ESET Endpoint Security

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r. o.

ESET Endpoint Security bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukovaná žiadnym prostriedkom ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti ESET, spol. s r. o.

ESET, spol. s r. o. si vyhradzuje právo zmeny programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 25.4.2023

1 ESET Endpoint Security 9 1
1.1 Aké novinky prináša táto verzia? 2
1.2 Systémové požiadavky 3
1.2 Podporované jazyky 4
1.3 Prevencia 5
1.4 Pomocník k programu 6
2 Dokumentácia pre koncové zariadenia spravované vzdialene 8
2.1 Predstavenie programu ESET PROTECT 8
2.2 Predstavenie programu ESET PROTECT Cloud 10
2.3 Ochrana nastavení heslom 10
2.4 Čo sú politiky? 11
2.4 Zlučovanie politík 12
2.5 Ako fungujú príznaky 12
3 Používanie programu ESET Endpoint Security samostatne 13
3.1 Metódy inštalácie 13
3.1 Inštalácia s použitím nástroja ESET AV Remover 14
3.1 ESET AV Remover 14
3.1 Odinštalovanie pomocou nástroja ESET AV Remover skončilo chybou 17
3.1 Inštalácia (.exe) 17
3.1 Zmena inštalačného priečinka (.exe) 19
3.1 Inštalácia (.msi) 19
3.1 Pokročilá inštalácia (.msi) 21
3.1 Minimálna inštalácia 23
3.1 Inštalácia cez príkazový riadok 23
3.1 Nasadenie pomocou GPO alebo SCCM 28
3.1 Prechod na novšiu verziu 30
3.1 Aktualizácie zaisťujúce bezpečnosť a stabilitu 31
3.1 Časté problémy pri inštalácii 31
3.1 Aktivácia nebola úspešná 31
3.2 Aktivácia produktu 32
3.3 Kontrola počítača 32
3.4 Začíname 32
3.4 Používateľské rozhranie 32
3.4 Nastavenie aktualizácií 36
3.4 Nastavenie zón 37
3.4 Nástroje webovej kontroly 38
4 Práca s programom ESET Endpoint Security 38
4.1 Počítač 40
4.1 Detekčné jadro 42
4.1 Detekčné jadro – pokročilé možnosti 46
4.1 Našla sa infiltrácia 47
4.1 Rezidentná ochrana súborového systému 49
4.1 Kontrola rezidentnej ochrany 50
4.1 Kedy meniť nastavenia rezidentnej ochrany 51
4.1 Čo robiť, ak nefunguje rezidentná ochrana 51
4.1 Kontrola počítača 52
4.1 Spustenie vlastnej kontroly 54
4.1 Priebeh kontroly 55
4.1 Protokol o kontrole počítača 57
4.1 Detekcia malvéru 57

4.1 Kontrola v nečinnosti ... 58
4.1 Profily kontroly ... 58
4.1 Ciele kontroly ... 59
4.1 Pokročilé možnosti kontroly ... 59
4.1 Správa zariadení ... 60
4.1 Pravidlá správy zariadení ... 61
4.1 Zistené zariadenia ... 62
4.1 Skupiny zariadení ... 62
4.1 Pridanie pravidiel správy zariadení ... 63
4.1 HIPS (Host-based Intrusion Prevention System) ... 65
4.1 Interaktívne okno HIPS ... 68
4.1 Bola zachytená potenciálna aktivita ransomvéru ... 69
4.1 Manažment pravidiel HIPS ... 69
4.1 Nastavenie pravidiel HIPS ... 70
4.1 Rozšírené nastavenia HIPS ... 72
4.1 Ovládače s povolením vždy sa načítať ... 73
4.1 Prezentačný režim ... 73
4.1 Kontrola pri štarte ... 74
4.1 Kontrola súborov spúšťaných pri štarte počítača ... 74
4.1 Ochrana dokumentov ... 75
4.1 Vylúčenia ... 75
4.1 Výkonnostné vylúčenia ... 76
4.1 Pridanie alebo úprava výkonnostných vylúčení ... 77
4.1 Formát vylúčenia cesty ... 78
4.1 Vylúčenia detekcií ... 79
4.1 Pridanie alebo úprava vylúčení detekcií ... 82
4.1 Sprievodca vytvorením vylúčenia detekcie ... 83
4.1 Vylúčenia (7.1 a staršie verzie) ... 83
4.1 Vylúčenia procesov ... 84
4.1 Pridanie alebo úprava vylúčení procesov ... 85
4.1 HIPS vylúčenia ... 85
4.1 Parametre ThreatSense ... 85
4.1 Úrovne liečenia ... 88
4.1 Prípony súborov vylúčené z kontroly ... 89
4.1 Doplňujúce parametre ThreatSense ... 89
4.2 Sieť ... 89
4.2 Firewall ... 91
4.2 Učiaci sa režim ... 93
4.2 Ochrana pred sieťovými útokmi ... 94
4.2 Ochrana pred útokmi hrubou silou ... 94
4.2 Pravidlá ... 95
4.2 Vylúčenia ... 97
4.2 Pokročilé možnosti filtrovania ... 97
4.2 IDS pravidlá ... 100
4.2 Zablokovaná podozrivá hrozba ... 101
4.2 Riešenie problémov ochrany siete ... 101
4.2 Pripojené siete ... 102
4.2 Známe siete ... 102
4.2 Editor známych sietí ... 103
4.2 Overenie siete – konfigurácia servera ... 105
4.2 Profily firewallu ... 106

4.2 Profily priradené k sieťovým adaptérom ... 106
4.2 Detekcia zmeny aplikácií ... 107
4.2 Vylúčenia z detekcie zmeny aplikácií ... 107
4.2 Ako nastaviť a používať pravidlá ... 108
4.2 Zoznam pravidiel firewallu ... 108
4.2 Pridanie alebo úprava pravidiel firewallu ... 109
4.2 Pravidlo firewallu – Lokálna strana ... 111
4.2 Pravidlo firewallu – Vzdialená strana ... 112
4.2 Dočasný blacklist IP adries ... 113
4.2 Dôveryhodná zóna ... 113
4.2 Nastavenie zón ... 114
4.2 Zóny firewallu ... 114
4.2 Protokol firewallu ... 114
4.2 Nadväzovanie spojenia – detekcia ... 115
4.2 Riešenie problémov s ESET Firewallom ... 116
4.2 Sprievodca riešením problémov ... 117
4.2 Vytváranie protokolov a pravidiel alebo výnimiek z protokolu ... 117
4.2 Vytvorenie pravidla z protokolu ... 117
4.2 Vytvorenie výnimky z oznámenia firewallu ... 117
4.2 Vytváranie rozšírených protokolov ochrany siete ... 118
4.2 Riešenie problémov s filtrovaním protokolov ... 118
4.3 Web a e-mail ... 119
4.3 Filtrovanie protokolov ... 121
4.3 Vylúčené aplikácie ... 121
4.3 Vylúčené IP adresy ... 122
4.3 SSL/TLS ... 123
4.3 Certifikáty ... 124
4.3 Šifrovaná sieťová komunikácia ... 125
4.3 Zoznam známych certifikátov ... 125
4.3 Zoznam SSL/TLS-filtrovaných aplikácií ... 126
4.3 Ochrana e-mailových klientov ... 127
4.3 E-mailové protokoly ... 128
4.3 Značenie e-mailov ... 129
4.3 Integrácia s e-mailovými klientmi ... 130
4.3 Panel nástrojov programu Microsoft Outlook ... 130
4.3 Panel nástrojov programu Outlook Express a Windows Mail ... 131
4.3 Potvrdzovacie dialógové okno ... 131
4.3 Opätovná kontrola správ ... 132
4.3 Antispamová ochrana ... 132
4.3 Zoznamy adries ... 133
4.3 Blacklist, whitelist a zoznam výnimiek ... 134
4.3 Pridanie a úprava položiek v blackliste, whiteliste a zozname výnimiek ... 135
4.3 Ochrana prístupu na web ... 136
4.3 Rozšírené nastavenia ochrany prístupu na web ... 138
4.3 Webové protokoly ... 138
4.3 Manažment URL adries ... 139
4.3 Zoznam URL adries ... 140
4.3 Vytvorenie nového zoznamu ... 141
4.3 Ako pridať URL masku ... 142
4.3 Antiphishingová ochrana ... 143
4.3 Rozšírené nastavenia pre zabezpečený prehliadač ... 144

4.3 Chránené stránky ... 145
4.3 Oznámenie v prehliadači ... 145
4.4 Webová kontrola ... 146
4.4 Pravidlá webovej kontroly ... 147
4.4 Pridanie pravidiel webovej kontroly ... 148
4.4 Skupiny kategórií ... 150
4.4 URL skupiny ... 151
4.4 Prispôsobenie správy zobrazenej pri blokovaní stránky ... 152
4.5 Aktualizácia programu ... 154
4.5 Nastavenie aktualizácií ... 158
4.5 Vrátenie zmien aktualizácií ... 161
4.5 Aktualizácie produktu ... 163
4.5 Možnosti pripojenia ... 163
4.5 Aktualizačný mirror ... 165
4.5 HTTP Server a SSL pre mirror ... 166
4.5 Aktualizácia z mirrora ... 167
4.5 Riešenie problémov pri aktualizácii z mirrora ... 168
4.5 Vytvorenie aktualizačnej úlohy ... 169
4.6 Nástroje ... 169
4.6 Protokoly ... 170
4.6 Filtrovanie protokolov ... 173
4.6 Konfigurácia zápisu do protokolov ... 174
4.6 Protokoly auditu ... 175
4.6 Plánovač ... 176
4.6 ESET SysInspector ... 178
4.6 Ochrana s podporou cloudu ... 179
4.6 Filter vylúčení pre ochranu s podporou cloudu ... 182
4.6 Spustené procesy ... 182
4.6 Správa o bezpečnosti ... 184
4.6 Sieťové pripojenia ... 186
4.6 ESET SysRescue Live ... 187
4.6 Odoslanie vzorky na analýzu ... 187
4.6 Vybrať vzorku na analýzu – Podozrivý súbor ... 188
4.6 Vybrať vzorku na analýzu – Podozrivá stránka ... 189
4.6 Vybrať vzorku na analýzu – Nesprávne detegovaný súbor ... 189
4.6 Vybrať vzorku na analýzu – Nesprávne detegovaná stránka ... 189
4.6 Vybrať vzorku na analýzu – Iné ... 190
4.6 Karanténa ... 190
4.6 Nastavenie Proxy servera ... 192
4.6 Časové intervaly ... 193
4.6 Aktualizácie Microsoft Windows ... 194
4.6 Interval kontroly licencie ... 195
4.7 Používateľské rozhranie ... 195
4.7 Prvky používateľského rozhrania ... 195
4.7 Nastavenia prístupu ... 197
4.7 Heslo na ochranu rozšírených nastavení ... 198
4.7 Ikona na paneli úloh ... 199
4.7 Kontextové menu ... 200
4.7 Pomocník a podpora ... 200
4.7 O ESET Endpoint Security ... 201
4.7 Odoslať systémové nastavenia ... 202

4.7 Technická podpora ... 202
4.8 Oznámenia ... 203
4.8 Stavy aplikácie ... 203
4.8 Oznámenia na ploche ... 204
4.8 Dialógové okno – Oznámenia na ploche ... 205
4.8 Prispôsobenie oznámení ... 205
4.8 Interaktívne upozornenia ... 205
4.8 Zoznam interaktívnych upozornení ... 207
4.8 Potvrdzovacie správy ... 208
4.8 Chyba (konflikt) v rámci rozšírených nastavení ... 209
4.8 Povoliť pokračovanie v predvolenom prehliadači ... 210
4.8 Vymeniteľné médiá ... 210
4.8 Vyžaduje sa reštart ... 211
4.8 Odporúča sa reštart ... 212
4.8 Preposielanie ... 213
4.8 Manažér profilov ... 216
4.8 Klávesové skratky ... 216
4.8 Diagnostika ... 217
4.8 Modul kontroly cez príkazový riadok ... 218
4.8 ESET CMD ... 221
4.8 Detekcia stavu nečinnosti ... 223
4.8 Import a export nastavení ... 223
4.8 Všetky nastavenia zmeniť na predvolené ... 224
4.8 Vrátiť späť predvolené nastavenia v tejto sekcii ... 224
4.8 Chyba pri ukladaní nastavení ... 225
4.8 Vzdialený monitoring a správa ... 225
4.8 Príkazový riadok pre vzdialený monitoring a správu (ERMM) ... 226
4.8 Zoznam ERMM JSON príkazov ... 227
4.8 get protection-status ... 228
4.8 get application-info ... 228
4.8 get license-info ... 231
4.8 get logs ... 231
4.8 get activation-status ... 232
4.8 get scan-info ... 233
4.8 get configuration ... 234
4.8 get update-status ... 235
4.8 start scan ... 236
4.8 start activation ... 236
4.8 start deactivation ... 237
4.8 start update ... 238
4.8 set configuration ... 238
5 Časté otázky ... 239
5.1 Časté otázky o automatických aktualizáciách ... 240
5.2 Ako aktualizovať ESET Endpoint Security ... 242
5.3 Ako aktivovať ESET Endpoint Security ... 243
5.3 Zadanie licenčného kľúča počas aktivácie ... 243
5.3 Prihlásenie do ESET Business Account ... 244
5.3 Ako aktivovať nový produkt ESET určený pre koncové zariadenia pomocou starších licenčných údajov ... 244
5.4 Ako odstrániť vírus z počítača ... 244
5.5 Ako povoliť komunikáciu pre určitú aplikáciu ... 245
5.6 Ako vytvoriť novú úlohu v Plánovači ... 245

5.6 Ako naplánovať pravidelnú týždňovú kontrolu počítača 246
5.7 Ako pripojiť ESET Endpoint Security k nástroju ESET PROTECT 247
5.7 Ako používať Režim prepísania 247
5.7 Ako aplikovať odporúčané politiky pre ESET Endpoint Security 249
5.8 Ako nastaviť funkciu mirror 251
5.9 Ako prejsť na Windows 10 s nainštalovaným produktom ESET Endpoint Security 251
5.10 Ako aktivovať vzdialený monitoring a správu produktu (RMM) 252
5.11 Ako blokovať stiahnutie určitých typov súborov z internetu 254
5.12 Ako minimalizovať používateľské rozhranie programu ESET Endpoint Security 255
5.13 Ako vyriešiť chybové hlásenie „Zabezpečený prehliadač nemohol byť presmerovaný na požadovanú webovú stránku“ 256
6 Licenčná dohoda s koncovým používateľom 257
7 Zásady ochrany osobných údajov 264

ESET Endpoint Security 9

ESET Endpoint Security 9 predstavuje nový prístup k integrovanej počítačovej bezpečnosti. Najnovšia verzia skenovacieho jadra ESET LiveGrid® spolu s naším vlastným firewallom a antispamovým modulom prináša rýchlu a presnú ochranu pre váš počítač. Výsledkom je inteligentný systém, ktorý je neustále v pohotovosti pred útokmi či škodlivým softvérom predstavujúcim potenciálnu hrozbu pre váš počítač.

ESET Endpoint Security 9 je komplexné bezpečnostné riešenie, ktoré je výsledkom dlhodobého úsilia spojiť maximálnu bezpečnosť s minimálnou záťažou systému. Pokročilé technológie založené na umelej inteligencii sú schopné proaktívne eliminovať prenikanie vírusov, spyvéru, trójskych koní, červov, advéru, rootkitov a ďalších internetových útokov bez toho, aby brzdili výkon systému alebo spôsobovali nefunkčnosť operačného systému počítača.

ESET Endpoint Security 9 je primárne navrhnutý pre pracovné stanice v menších firemných sieťach.

V sekcii Používanie ESET Endpoint Security samostatne nájdete jednotlivé časti pomocníka rozdelené do niekoľkých kapitol a podkapitol s cieľom poskytnúť lepšiu orientáciu a kontext. Nájdete tu aj informácie týkajúce sa stiahnutia, inštalácie a aktivácie.

Používanie programu ESET Endpoint Security spolu s nástrojom ESET PROTECT v podnikovom prostredí vám umožňuje jednoducho spravovať akýkoľvek počet klientskych pracovných staníc, zavádzať politiky a pravidlá, monitorovať detekcie a vzdialene konfigurovať klientske zariadenia z akéhokoľvek počítača v sieti.

Kapitola Časté otázky obsahuje niektoré z najčastejšie sa vyskytujúcich otázok a problémov, s ktorými sa môžete stretnúť.

Vlastnosti a výhody

Prepracované používateľské rozhranie	Používateľské rozhranie v novej verzii bolo značne vylepšené a zjednodušené na základe výsledkov používateľského testovania. Všetky popisy a oznámenia boli dôkladne skontrolované a rozhranie teraz navyše poskytuje podporu pre jazyky písané sprava doľava, ako sú hebrejčina a arabčina. Online pomocník je teraz integrovaný do ESET Endpoint Security a poskytuje dynamicky aktualizovaný podporný obsah pre používateľov.
Antivírusová a antispyvérová ochrana	Proaktívne deteguje a lieči známe i neznáme vírusy, červy, trójske kone a rootkity. Pokročilá heuristika odhaľuje dokonca aj doteraz neznáme hrozby a neutralizuje ich skôr, než môžu spôsobiť škodu vo vašom počítači. Ochrana prístupu na web a antiphishingová ochrana spočíva hlavne v monitorovaní komunikácie prehliadačov internetových stránok so vzdialenými servermi (vrátane SSL). Ochrana e-mailových klientov zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3(S) a IMAP(S).
Pravidelné aktualizácie	Pravidelné aktualizácie detekčného jadra (v predchádzajúcich verziách pod názvom „vírusová databáza“) a programových modulov sú základným predpokladom na zaistenie maximálnej úrovne zabezpečenia vášho počítača.
ESET LiveGrid® (cloudový reputačný systém)	Používateľ môže overiť reputáciu súborov a spustených procesov priamo v ESET Endpoint Security.

Vzdialená správa	ESET PROTECT vám umožňuje spravovať v sieťovom prostredí z jedného miesta všetky produkty ESET nainštalované na pracovných staniciach, serveroch a mobilných zariadeniach. Prostredníctvom ESET PROTECT Web Console (ESET PROTECT Web Console) môžete nasadiť bezpečnostné riešenia spoločnosti ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na vzdialených počítačoch.
Ochrana pred sieťovými útokmi	Analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Akákoľvek komunikácia, ktorá je považovaná za nebezpečnú, bude zablokovaná.
Webová kontrola (len v ESET Endpoint Security)	Webová kontrola vám umožňuje blokovať webové stránky, ktoré môžu obsahovať potenciálne nežiaduci obsah. Okrem toho môžu zamestnávatelia alebo systémoví administrátori zakázať prístup na 27 predvolených kategórií a 140 podkategórií webových stránok.

Aké novinky prináša táto verzia?

Produkt ESET Endpoint Security vo verzii 9 bol uvedený na trh a je k dispozícii na stiahnutie.

Automatické aktualizácie

- Automatické aktualizácie zabezpečujú, aby ste vždy používali najnovšiu verziu produktu.
- Šikovné riešenie, ktoré znižuje údržbu produktu ESET Endpoint Security na minimum.

- Funkcia je predvolene zapnutá a využíva aktualizáciu programových súčastí (microPCU).
- Nedochádza k preinštalovaniu produktu, ktoré so sebou nesie nevýhody v podobe odregistrovania zo systému a prenosu konfigurácie.
- Sťahuje sa menší objem dát (rozdielová aktualizácia).
- Používateľ je o aktualizácii informovaný oznámením, ktorého zobrazovanie je možné úplne potlačiť. Zaručená je tiež kompatibilita so spravovanými prostrediami.

Súvisiace zmeny a doplnenia licenčnej dohody s koncovým používateľom (EULA)

- Nová EULA sa zobrazuje nezávisle od procesu inštalácie pomocou informačného prvku v konzole alebo v používateľskom rozhraní programu ESET Endpoint Security.
- Zjednodušuje sa proces automatickej aktualizácie produktu a zvyšuje sa používateľský komfort, keďže už nebude potrebné odsúhlasiť licenčnú dohodu pri každej aktualizácii produktu ESET na novšiu verziu.

Ochrana pred útokmi hrubou silou

- Ochrana pred útokmi hrubou silou (ako súčasť prepracovanej ochrany pred sieťovými útokmi) kontroluje obsah sieťovej komunikácie a blokuje pokusy o uhádnutie hesiel.
- Sledujú sa opakované pokusy o zadanie hesla a zdrojová IP adresa sa zaznamená do dočasného blacklistu IP adries, čo pomáha lepšie monitorovať situáciu.
- Zdrojová IP adresa s takouto podozrivou aktivitou môže byť po určitom čase odstránená z blacklistu, ak sa pripojenie ukáže ako legitímne.
- Možnosť konfigurácie pre potreby veľkých sietí.

Natívna podpora pre ARM64

- Verzia 9 je k dispozícii aj pre zariadenia s procesorom ARM64.

Toto vydanie prináša rôzne opravy chýb a vylepšenia výkonu.

Ďalšie informácie o nových funkciách programu ESET Endpoint Security vrátane ilustračných obrázkov nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET:

- Aké novinky prináša verzia 9 programu ESET Endpoint Security?

Systémové požiadavky

Pre bezproblémový chod programu ESET Endpoint Security by systém mal spĺňať nasledujúce hardvérové a softvérové požiadavky:

Podporované procesory

Procesor Intel alebo AMD, 32-bitový (x86) s inštrukčnou súpravou SSE2 alebo 64-bitový (x64), 1 GHz alebo rýchlejší
Procesor založený na architektúre ARM64, 1 GHz alebo rýchlejší

Operačné systémy

Microsoft® Windows® 11

Microsoft® Windows® 10

Podrobný zoznam podporovaných verzií operačných systémov Microsoft® Windows® 10 a Microsoft® Windows® 11 nájdete v článku o prehľade podpory operačného systému Windows.

Podpora pre Azure Code Signing musí byť nainštalovaná na všetkých operačných systémoch Windows, aby bolo možné nainštalovať alebo aktualizovať produkty ESET vydané po júli 2023. Viac informácií

Microsoft® Windows® 8.1
Microsoft® Windows® 8

Microsoft® Windows® 7 SP1 s najnovšími aktualizáciami systému Windows (aspoň KB4474419 a KB4490628)

ESET Endpoint Security 9.1 je poslednou verziou, ktorá podporuje operačné systémy Windows 7 a Windows 8.1. Viac informácií

Windows XP a Windows Vista už nie sú podporované.

Operačný systém pravidelne aktualizujte.

Inštalátor produktu ESET Endpoint Security vytvorený v ESET PROTECT 8.1 a novších verziách podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 v režime viacerých relácií (multi-session).

Iné

- Splnené systémové požiadavky na operačný systém a iný softvér inštalovaný na počítači

- 0,3 GB voľnej systémovej pamäte (pozri Poznámku 1)
- 1 GB voľného miesta na disku (pozrite Poznámku 2)
- Minimálne rozlíšenie monitora 1024x768
- Internetové pripojenie alebo lokálne sieťové pripojenie na zabezpečenie produktových aktualizácií (pozrite Poznámku 3)
- Používanie dvoch antivírusových programov súčasne na jednom zariadení nevyhnutne vedie ku konfliktu pri prístupe k systémovým prostriedkom, čo sa prejaví spomalením systému a môže vyústiť až do stavu, keď zariadenie prestane pracovať.

Aj keď je možné inštalovať a využívať produkt na systémoch, ktoré nespĺňajú tieto požiadavky, odporúčame najprv vykonať používateľské testovanie v závislosti od konkrétnych systémových požiadaviek.

(1): Program môže spotrebovať viac systémovej pamäte v prípade ťažko infikovaného počítača (ak by táto pamäť nebola využívaná iným spôsobom) alebo v prípade importovania veľkého objemu dát do programu (napr. zoznamy dôveryhodných URL adries).
(2): Miesto na disku potrebné na stiahnutie inštalačného súboru, inštaláciu programu a uloženie kópie inštalačného balíka v programových dátach, ako aj na zálohy programových aktualizácií na podporu funkcie vrátenia zmien (tzv. rollback). Program môže mať väčšie požiadavky na miesto na disku pri odlišných nastaveniach (v prípade ukladania viacerých verzií zálohovania produktových aktualizácií, výpisov pamäte, alebo v prípade ukladania nadmerného počtu záznamov protokolov) alebo na infikovanom počítači (napríklad v dôsledku využívania funkcie karantény). Odporúčame zachovať dostatok voľného miesta na disku na účely aktualizácie operačného systému, ako aj na aktualizáciu samotného produktu ESET.
(3): Hoci sa to neodporúča, program je možné aktualizovať aj manuálne z vymeniteľného média.

Podporované jazyky

ESET Endpoint Security je k dispozícii na inštaláciu a stiahnutie v nasledujúcich jazykoch.

Jazyk	Kód jazyka	LCID
Angličtina (Spojené štáty)	en-US	1033
Arabčina (Egypt)	ar-EG	3073
Bulharčina	bg-BG	1026
Zjednodušená čínština	zh-CN	2052
Tradičná čínština	zh-TW	1028
Chorvátčina	hr-HR	1050
Čeština	cs-CZ	1029
Estónčina	et-EE	1061
Fínčina	fi-FI	1035
Francúzština (Francúzsko)	fr-FR	1036
Francúzština (Kanada)	fr-CA	3084
Nemčina (Nemecko)	de-DE	1031
Gréčtina	el-GR	1032
*Hebrejčina	he-IL	1037
Maďarčina	hu-HU	1038
*Indonézština	id-ID	1057
Taliančina	it-IT	1040

Jazyk	Kód jazyka	LCID
Japončina	ja-JP	1041
Kazaština	kk-KZ	1087
Kórejčina	ko-KR	1042
*Lotyština	lv-LV	1062
Litovčina	lt-LT	1063
Holandčina	nl-NL	1043
Nórčina	nb-NO	1044
Poľština	pl-PL	1045
Portugalčina (Brazília)	pt-BR	1046
Rumunčina	ro-RO	1048
Ruština	ru-RU	1049
Španielčina (Čile)	es-CL	13322
Španielčina (Španielsko)	es-ES	3082
Švédčina (Švédsko)	sv-SE	1053
Slovenčina	sk-SK	1051
Slovinčina	sl-SI	1060
Thajčina	th-TH	1054
Turečtina	tr-TR	1055
Ukrajinčina (Ukrajina)	uk-UA	1058
*Vietnamčina	vi-VN	1066

*ESET Endpoint Security je v tomto jazyku k dispozícii, ale online používateľská príručka k dispozícii nie je (dochádza k presmerovaniu na anglickú verziu).

Ak chcete zmeniť jazyk tejto online používateľskej príručky, pozrite si okno s výberom jazyka (v pravom hornom rohu).

Prevencia

Pri práci s počítačom, a to najmä pri prehliadaní internetu, majte na pamäti, že žiadny antivírusový systém na svete nedokáže úplne eliminovať riziko infiltrácií a vzdialených útokov. Pre zaistenie maximálnej úrovne ochrany a pohodlia je nevyhnutné správne používať vaše antivírusové riešenie a dodržiavať niekoľko užitočných pravidiel:

Pravidelná aktualizácia

Podľa štatistík z ESET LiveGrid® vznikajú denne tisíce nových unikátnych infiltrácií, ktoré sa snažia obísť existujúce bezpečnostné opatrenia a priniesť svojim tvorcom zisk na úkor ostatných používateľov. Vírusoví analytici spoločnosti ESET denne tieto hrozby analyzujú a vydávajú aktualizácie, ktoré zvyšujú úroveň ochrany používateľov antivírusového systému. Pri nesprávnom nastavení aktualizácie sa účinnosť antivírusového systému dramaticky znižuje. Pre podrobnejšie informácie o nastavení aktualizácie kliknite na nasledujúci odkaz: Nastavenie aktualizácie.

Sťahovanie bezpečnostných záplat

Tvorcovia škodlivého kódu s obľubou využívajú bezpečnostné zraniteľnosti a chyby v často používaných programoch, aby zvýšili účinnosť šírenia infiltrácie. Z toho dôvodu softvérové spoločnosti kladú dôraz na vyhľadávanie bezpečnostných zraniteľností vo svojich programoch a pravidelne vydávajú bezpečnostné záplaty, ktorými dané chyby opravujú a znižujú potenciálne riziko hrozby. Je dôležité tieto záplaty pravidelne inštalovať. Medzi takéto programy môžeme zaradiť napríklad operačný systém Microsoft Windows alebo internetový prehliadač Internet Explorer.

Zálohovanie dôležitých dát

Tvorcovia infiltrácií väčšinou neberú ohľad na potreby používateľa, a tak často nimi vytvorené infiltrácie môžu spôsobiť úplnú nefunkčnosť niektorých programov, operačného systému alebo stratu dát. Preto je kľúčové pravidelne zálohovať citlivé a dôležité dáta na externé úložisko, napríklad na DVD alebo externý pevný disk. Záloha vám výrazne uľahčí a urýchli obnovu systému po útoku do pôvodného stavu.

Pravidelná kontrola počítača

Detekcia známych či menej známych vírusov, červov, trójskych koní a rootkitov je zabezpečená pomocou Rezidentnej ochrany súborového systému. To znamená, že pri každom prístupe alebo otvorení súboru prebehne kontrola na prítomnosť malvéru. Napriek tomu odporúčame, aby ste spustili kontrolu počítača aspoň raz mesačne, pretože malvér je rôzny, dynamický a detekčné jadro sa aktualizuje každý deň.

Dodržiavanie základných bezpečnostných pravidiel

Jedným z najužitočnejších a najúčinnejších bezpečnostných opatrení je obozretnosť používateľa. V súčasnosti mnoho infiltrácií vyžaduje priame spustenie používateľom. Preto je veľmi dôležitá opatrnosť pri otváraní súborov. Ušetríte si tak mnoho problémov a čas strávený snahou o odstránenie infiltrácie z počítača. Medzi užitočné rady by sme mohli zahrnúť:

- Obmedziť návštevy podozrivých stránok, ktoré používateľa bombardujú otváraním okien s reklamnými ponukami a pod.
- Opatrnosť pri sťahovaní a inštalovaní voľne šíriteľných programov, kodekov atď. Odporúčame využívať iba overené programy a internetové stránky.
- Opatrnosť pri otváraní príloh e-mailov obzvlášť pri masovo posielaných e-mailoch alebo pri e-mailoch od neznámych odosielateľov.
- Nepoužívať na bežnú prácu na počítači účet s právami Administrátora.

Pomocník k programu

Vitajte v používateľskej príručke ESET Endpoint Security. Veríme, že informácie obsiahnuté v tejto príručke vám pomôžu pri práci s vaším produktom a urobia váš počítač bezpečnejším.

Ako začať

Pred začatím používania ESET Endpoint Security je potrebné mať na pamäti, že tento produkt môže byť používaný buď samostatne, alebo ho môžu používať používatelia pripojení prostredníctvom nástroja ESET PROTECT. Taktiež odporúčame, aby ste sa oboznámili s rôznymi typmi detekcií a vzdialenými útokmi, s ktorými sa môžete pri práci s počítačom stretnúť.

V časti Čo je nové nájdete informácie o funkciách predstavených v tejto verzii produktu ESET Endpoint Security. Pripravili sme pre vás aj sprievodcu, ktorý vám pomôže so základným nastavením ESET Endpoint Security.

Ako používať Pomocníka programu ESET Endpoint Security

Jednotlivé stránky Pomocníka sú pre lepšiu orientáciu logicky usporiadané do kapitol a podkapitol. To vám umožňuje nájsť súvisiace informácie jednoduchým prechádzaním tejto štruktúry.

Stlačením klávesu **F1** získate dodatočné informácie o akomkoľvek okne programu. Zobrazí sa Pomocník pre sekciu programu, ktorú máte otvorenú.

Pomocník umožňuje aj vyhľadávanie prostredníctvom kľúčových slov alebo pomocou vyhľadania slov a slovných spojení. Rozdiel medzi týmito dvomi typmi vyhľadávania je ten, že kľúčové slová sa viažu k stránkam pomocníka logicky, pričom samotné kľúčové slovo sa vôbec v texte nemusí vyskytovať. Vyhľadávanie pomocou slov a slovných spojení vyhľadá všetky stránky pomocníka, kde sa všetky hľadané slová súčasne nachádzajú priamo v texte.

Na zachovanie konzistencie, a aby sa zabránilo zámene, je terminológia použitá v tejto príručke založená na názvoch parametrov programu ESET Endpoint Security. Používame tiež jednotnú súpravu symbolov na zvýraznenie kapitol, ktoré sú zvlášť dôležité alebo sú iným spôsobom markantné.

Poznámka je len krátky postreh. Hoci poznámkam nemusí byť venovaná zvláštna pozornosť, môžu obsahovať cenné informácie, ako napr. špecifické funkcie alebo odkaz na súvisiacu kapitolu.

Informácie, ktoré si vyžadujú vašu pozornosť a neodporúča sa ich ignorovať. Zvyčajne nejde o mimoriadne závažné, avšak o podstatné informácie.

Ide o informáciu, ktorá vyžaduje zvýšenú pozornosť a opatrnosť. Upozornenia sú umiestnené tak, aby vás včas varovali a zároveň vám pomohli predísť chybám, ktoré by mohli mať negatívne následky. Prosím, dôkladne si prečítajte text ohraničený týmto označením, pretože sa týka vysoko citlivých systémových nastavení alebo upozorňuje na riziká.

Toto je prípad použitia alebo praktický príklad, ktorého cieľom je pomôcť vám lepšie porozumieť, ako využiť konkrétnu funkciu.

Konvencia	Význam
Tučné písmo	Pomenúva položky rozhrania, ako napr. polia a tlačidlá možností.
Kurzíva	Zástupné symboly pre údaje, ktoré máte poskytnúť. Napríklad, file name alebo path znamená, že máte zadať konkrétnu cestu alebo názov súboru.
`Courier New`	Príklady kódov alebo príkazov.
Hypertextové prepojenie	Poskytuje rýchly a jednoduchý prístup k súvisiacim prepojeným kapitolám alebo externým webovým lokalitám. Hypertextové prepojenia sú zvýraznené modrou farbou a môžu byť podčiarknuté.
%ProgramFiles%	Systémový adresár Windows, kde sú uložené programy inštalované na operačnom systéme Windows.

Online pomocník je hlavným zdrojom pomocného obsahu. Pri pripojení na internet je zobrazovaná vždy najnovšia verzia online pomocníka.

Dokumentácia pre koncové zariadenia spravované vzdialene

Firemné produkty ESET (vrátane ESET Endpoint Security) nainštalované na pracovných staniciach, serveroch a mobilných zariadeniach je možné spravovať v sieťovom prostredí z jedného miesta. Systémoví administrátori, ktorí spravujú viac ako 10 klientskych pracovných staníc, majú k dispozícii nástroje ESET určené na vzdialenú správu, prostredníctvom ktorých môžu nasadiť bezpečnostné riešenia ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na vzdialených počítačoch.

Nástroje spoločnosti ESET na vzdialenú správu

ESET Endpoint Security je možné spravovať vzdialene prostredníctvom ESET PROTECT alebo ESET Cloud Administrator.

- Predstavenie programu ESET PROTECT
- Predstavenie programu ESET PROTECT Cloud

Nástroje na vzdialenú správu tretích strán

- Vzdialený monitoring a správa (RMM)

Odporúčané postupy

- Pripojte všetky koncové zariadenia s produktom ESET Endpoint Security k nástroju ESET PROTECT
- Ochráňte na pripojených klientskych počítačoch prístup k Rozšíreným nastaveniam heslom a zabráňte neoprávneným zmenám v nastaveniach produktu
- Použite odporúčanú politiku na vynútenie dostupných bezpečnostných funkcií
- Obmedzte používateľské rozhranie – minimalizujte interakciu používateľa s ESET Endpoint Security

Ako na to

- Ako používať Režim prepísania
- Ako nasadiť ESET Endpoint Security prostredníctvom GPO alebo SCCM

Predstavenie programu ESET PROTECT

ESET PROTECT vám umožňuje spravovať v sieťovom prostredí z jedného miesta všetky produkty ESET nainštalované na pracovných staniciach, serveroch a mobilných zariadeniach.

Prostredníctvom ESET PROTECT Web Console môžete vzdialene nasadiť bezpečnostné riešenia ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na počítačoch. Prečítajte si tiež kapitoly Prehľad architektúry a infraštruktúry ESET PROTECT, Začíname s nástrojom ESET PROTECT Web Console a Podporované Desktop Provisioning prostredia.

ESET PROTECT pozostáva z nasledujúcich súčastí:

- ESET PROTECT Server – ESET PROTECT Server môže byť nainštalovaný na Windows aj Linux servery a môže

mať tiež podobu virtuálneho zariadenia. Riadi komunikáciu s agentmi a zhromažďuje a uchováva dáta aplikácií v databáze.

- ESET PROTECT Web Console – ESET PROTECT Web Console je hlavným rozhraním, ktoré vám umožňuje spravovať klientske počítače vo vašej sieti. Poskytuje prehľad stavu klientskych zariadení v sieti a dá sa použiť na vzdialenú inštaláciu produktov spoločnosti ESET na nespravované počítače. Po inštalácii ESET PROTECT Servera máte prístup do Web Console prostredníctvom vášho webového prehliadača. Ak sa rozhodnete sprístupniť webový server na internete, budete môcť používať ESET PROTECT z akéhokoľvek miesta a zariadenia pripojeného na internet.
- ESET Management Agent – ESET Management Agent sprostredkúva komunikáciu medzi ESET PROTECT Serverom a klientskymi počítačmi. Agent musí byť nainštalovaný na každom klientskom počítači, ktorý má komunikovať s ESET PROTECT Serverom. Keďže sa agent nachádza na klientskom počítači a dokáže uchovávať viaceré bezpečnostné scenáre, používanie ESET Management Agenta výrazne skracuje čas reakcie na nové detekcie. Pomocou ESET PROTECT Web Console môžete nasadiť ESET Management Agenta na nespravované počítače, ktoré boli identifikované prostredníctvom Active Directory alebo nástrojom ESET RD Sensor. V prípade potreby je možná aj manuálna inštalácia ESET Management Agenta.
- ESET Rogue Detection Sensor – ESET Rogue Detection Sensor deteguje nespravované počítače, ktoré sa nachádzajú v sieti. Informácie o týchto počítačoch sú odosielané na ESET PROTECT Server. To umožňuje jednoducho pridať nové klientske počítače do vašej zabezpečenej siete. RD Sensor si pamätá počítače, ktoré už boli nájdené a nebude odosielať rovnaké informácie dvakrát.
- Apache HTTP Proxy – je to služba, ktorá môže byť použitá v kombinácii s nástrojom ESET PROTECT na:
    - distribúciu aktualizácií na klientske počítače a distribúciu inštalačných balíkov na ESET Management Agenta,
    - presmerovanie komunikácie z ESET Management Agentov na ESET PROTECT Server.
- Mobile Device Connector – komponent, ktorý umožňuje správu mobilných zariadení pomocou nástroja ESET PROTECT. Umožňuje vám spravovať mobilné zariadenia (Android a iOS) a bezpečnostný produkt ESET Endpoint Security pre Android.
- Virtuálne zariadenie ESET PROTECT – ESET PROTECT VA je určené pre používateľov, ktorí chcú používať ESET PROTECT vo virtualizovanom prostredí.
- ESET PROTECT Virtual Agent Host – komponent programu ESET PROTECT, ktorý vytvára virtuálnych agentov, a umožňuje tak správu virtuálnych zariadení bez klasického agenta. Toto riešenie umožňuje automatizáciu, použitie dynamických skupín a správu úloh na rovnakej úrovni, ako tomu je pri klasických ESET Management Agentoch na fyzických počítačoch. Virtuálny agent zbiera informácie na virtuálnych počítačoch a odosiela ich na ESET PROTECT Server.
- Mirror Tool – tento nástroj sa používa na aktualizovanie programových modulov v offline prostredí. V prípade, že bezpečnostné produkty ESET na vašich klientskych počítačoch nemajú pripojenie na internet, môžete použiť nástroj Mirror Tool, ktorý sťahuje aktualizačné súbory z aktualizačných serverov spoločnosti ESET a ukladá ich lokálne.
- ESET Remote Deployment Tool – tento nástroj slúži na nasadenie all-in-one inštalačných balíkov vytvorených pomocou nástroja <%PRODUCT%> Web Console. Ponúka tak pohodlný spôsob distribúcie ESET Management Agenta s bezpečnostným produktom ESET na klientske počítače v sieti.
- ESET Business Account – nový licenčný portál určený pre firemné produkty ESET vám umožňuje spravovať licencie. Bližšie informácie o aktivácii produktu nájdete v kapitole ESET Business Account, prípadne si môžete prečítať používateľskú príručku k portálu ESET Business Account, kde nájdete podrobnejšie informácie o používaní ESET Business Account. Ak už máte prihlasovacie meno a heslo, ktoré vám boli vydané spoločnosťou ESET, môžete si ich skonvertovať na licenčný kľúč. Viac informácií nájdete v časti Konvertovanie licenčných prihlasovacích údajov na licenčný kľúč.
- ESET Inspect – komplexný systém detekcie a reakcie na hrozby na koncových zariadeniach (Endpoint Detection and Response – EDR), ktorý zahŕňa funkcie, ako napr. detekciu incidentov, riadenie a reakciu na incidenty, zozbieravanie údajov, detekciu indikátorov preukazujúcich narušenie zabezpečenia, detekciu

anomálií, detekciu správania, detekciu porušenia pravidiel atď.

Pomocou nástroja ESET PROTECT Web Console môžete nasadiť bezpečnostné riešenia spoločnosti ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na vzdialených počítačoch.

Viac informácií nájdete v online používateľskej príručke pre ESET PROTECT.

Predstavenie programu ESET PROTECT Cloud

ESET PROTECT Cloud vám umožňuje spravovať v sieťovom prostredí produkty spoločnosti ESET nainštalované na pracovných staniciach a serveroch z jedného miesta bez potreby fyzického alebo virtuálneho servera, ktorý je potrebný napríklad v prípade konzoly ESET PROTECT. Pomocou ESET PROTECT Cloud Web Console môžete nasadiť riešenia ESET, spravovať úlohy, vynucovať bezpečnostné politiky, monitorovať stav systému a rýchlo reagovať na problémy alebo hrozby na vzdialených počítačoch.

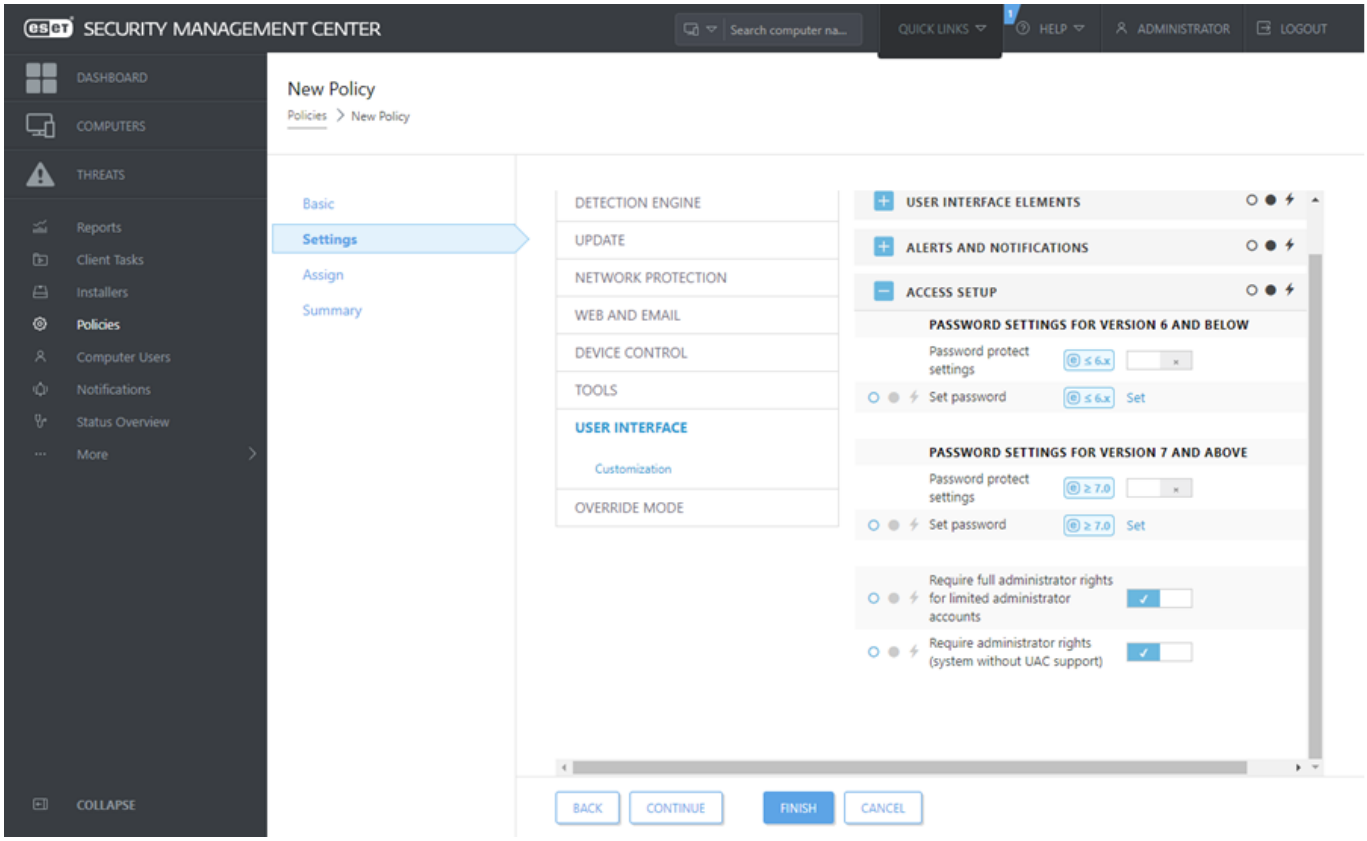
- Podrobnejšie informácie nájdete v online používateľskej príručke pre ESET PROTECT Cloud.

Ochrana nastavení heslom

Aby program ESET Endpoint Security mohol poskytovať maximálnu úroveň ochrany, je dôležitá jeho správna konfigurácia. Neoprávnené zmeny v nastaveniach môžu ohroziť bezpečnosť klientskeho počítača. Ak chcete ako správca obmedziť prístup koncového používateľa k rozšíreným nastaveniam programu, môžete ich chrániť pomocou hesla.

Správca môže vytvoriť politiku, na základe ktorej budú rozšírené nastavenia programu ESET Endpoint Security nainštalovaného na pripojenom klientskom počítači chránené heslom. Pre vytvorenie novej politiky postupujte nasledovne:

1. V ESET PROTECT Web Console kliknite v hlavnom menu vľavo na **Politiky**.
2. Kliknite na **Nová politika**.
3. Novú politiku pomenujte, prípadne k nej pridajte aj popis. Kliknite na **Pokračovať**.
4. Zo zoznamu produktov vyberte **ESET Endpoint pre Windows**.
5. V **Nastaveniach** kliknite na **Používateľské rozhranie** a rozbaľte sekciu **Nastavenia prístupu**.
6. Podľa verzie programu ESET Endpoint Security kliknite na prepínacie tlačidlo vedľa možnosti **Nastavenia chránené heslom**. Môžete si všimnúť, že produkty ESET určené pre koncové zariadenia vo verzii 7 a novšie ponúkajú dodatočné možnosti ochrany. Ak máte vo svojej sieti nainštalované produkty pre koncové zariadenia verzie 7 a novšie aj verzie 6, odporúčame vám vytvoriť si pre každú verziu samostatnú politiku s jedinečným heslom.
7. V zobrazenom okne zadajte nové heslo, potvrďte ho a kliknite na **OK**. Kliknite na **Pokračovať**.
8. Priraďte politiku ku klientom. Kliknite na **Priradiť** a vyberte počítače alebo skupiny počítačov, ktoré majú byť chránené heslom. Kliknite na **OK**.
9. Skontrolujte, či sú všetky želané klientske počítače zahrnuté v zozname, a kliknite na **Pokračovať**.
10. Skontrolujte nastavenia v sekcii Súhrn a kliknutím na **Dokončiť** uložte novú politiku.



Čo sú politiky?

Správca môže prostredníctvom politík v ESET PROTECT Web Console vzdialene aplikovať konkrétne nastavenia na bezpečnostné produkty ESET nainštalované na klientskych počítačoch. Politika môže byť aplikovaná priamo na individuálne počítače, ako aj na skupiny počítačov. Správca tiež môže k počítaču alebo skupine priradiť viacero politík.

Na vytvorenie novej politiky musí mať používateľ nasledujúce oprávnenia: Na čítanie zoznamu politík je potrebné povolenie na **čítanie**. Na priraďovanie politík k cieľovým zariadeniam je potrebné povolenie na **použitie**. Na vytváranie, zmenu a úpravu politík je potrebné povolenie na **zápis**.

Politiky sú aplikované v poradí podľa hierarchickej štruktúry statických skupín. Toto však neplatí pre dynamické skupiny, v prípade ktorých sú najskôr prechádzané podradené skupiny. Vďaka tomuto princípu môžete vytvárať globálne politiky pre statické skupiny, zatiaľ čo politiky so špecifickým nastavením môžete priraďovať k podskupinám. Použitím príznakov môže používateľ programu ESET Endpoint Security, ktorý má prístup do skupín nachádzajúcich sa vyššie v hierarchii, prepísať politiky nižších skupín. Algoritmus je podrobnejšie vysvetlený v online používateľskej príručke pre ESET PROTECT.

> Ku skupinám, ktoré sa nachádzajú vyššie v hierarchii, odporúčame priraďovať všeobecnejšie politiky (napr. nastavenia aktualizačného servera). Špecifickejšie politiky (napr. nastavenia správy zariadení) by mali byť priraďované hlbšie v stromovej štruktúre skupín. Politiky, ktoré sa nachádzajú v hierarchii nižšie, zvyčajne pri zlučovaní prepisujú nastavenia politík nachádzajúcich sa vyššie v hierarchii (ak nie je určené inak pomocou príznakov politík).

Zlučovanie politík

Politika aplikovaná na klienta je zvyčajne výsledkom zlúčenia viacerých politík do jednej finálnej politiky. Politiky sú zlučované po jednom. Pri zlučovaní politík je hlavným pravidlom, že nastavenia definované v neskoršej politike vždy nahrádzajú príslušné nastavenia definované predchádzajúcou politikou. Na zmenu tohto správania môžete použiť príznaky politík (dostupné pre každé nastavenie).

Pri vytváraní politík si môžete všimnúť, že pri niektorých nastaveniach je možné použiť ďalšie pravidlo (nahradiť/pripojiť na koniec/pripojiť na začiatok).

- **Nahradiť** – nahradený bude celý zoznam, predchádzajúce hodnoty budú odstránené a budú pridané nové hodnoty.
- **Pripojiť na koniec** – nové položky budú pridané na koniec aktuálne aplikovaného zoznamu (musí ísť o zoznam uplatňovaný na základe inej existujúcej politiky, keďže lokálny zoznam je vždy prepísaný).
- **Pripojiť na začiatok** – nové položky sú pridané na začiatok zoznamu (lokálny zoznam bude prepísaný).

ESET Endpoint Security podporuje zlučovanie lokálnych nastavení so vzdialenými politikami novým spôsobom. Ak je nastavenie zoznamom (napr. zoznam blokovaných webových stránok) a existuje konflikt medzi vzdialenou politikou a lokálnym nastavením, vzdialená politika dané lokálne nastavenie prepíše. Môžete si vybrať, ako kombinovať lokálne a vzdialené zoznamy. Rôzne pravidlá zlučovania môžete nastaviť pre:

- zlučovanie nastavení pre vzdialené politiky,
- zlučovanie vzdialených a lokálnych politík – zlučovanie lokálneho nastavenia s výslednou vzdialenou politikou.

Ak sa chcete o zlučovaní politík dozvedieť viac, prejdite do online používateľskej príručky pre ESET PROTECT a preskúmajte uvedený príklad.

Ako fungujú príznaky

Politika aplikovaná na klientsky počítač je zvyčajne výsledkom zlúčenia viacerých politík do jednej finálnej politiky. Proces zlučovania politík a očakávané správanie finálnej politiky, ktorá bude aplikovaná na klienta, je možné ovplyvniť použitím príznakov. Príznaky určujú, ako je s nastavením v politike zaobchádzané.

Pre každé nastavenie môžete zvoliť jeden z nasledujúcich príznakov:

Neaplikovať	Akékoľvek nastavenie s týmto príznakom nebude politikou aplikované. Keďže nastavenie nie je politikou uplatňované, môže byť neskôr zmenené inými politikami.
Aplikovať	Nastavenie s príznakom **Aplikovať** bude odoslané na klientske zariadenie. Pri zlučovaní politík však toto nastavenie môže byť prepísané neskoršou politikou. Ak je politika aplikovaná na klientsky počítač a určité nastavenie má tento príznak, dané nastavenie je zmenené bez ohľadu na to, čo bolo na klientskom počítači nakonfigurované lokálne. Keďže nastavenie nie je vynútené, môže byť neskôr zmenené inými politikami.
Vynútiť	Nastavenie s príznakom **Vynútiť** má vyššiu prioritu, čiže nemôže byť zmenené inou politikou (ani v prípade, že by neskoršia politika mala príznak **Vynútiť**). Týmto bude zaručené, že nastavenie nebude zmenené neskoršími politikami pri zlučovaní. Ak je politika aplikovaná na klientsky počítač a určité nastavenie má tento príznak, dané nastavenie je zmenené bez ohľadu na to, čo bolo na klientskom počítači nakonfigurované lokálne.

Situácia: *Správca* chce používateľovi s menom *John* povoliť vytvárať a upravovať politiky v jeho domácej skupine a zároveň mu umožniť vidieť všetky politiky vytvorené *správcom* vrátane politík obsahujúcich príznaky Vynútiť. *Správca* chce, aby *John* mohol vidieť všetky politiky, avšak nemohol upravovať existujúce politiky vytvorené *správcom*. Používateľ *John* bude môcť vytvárať alebo upravovať politiky iba vo svojej domácej skupine San Diego.
Riešenie:*Správca* musí vykonať nasledujúce kroky:
Vytvorenie statických skupín a súborov povolení
1. Vytvorte novú statickú skupinu s názvom *San Diego*.
2. Vytvorte nový súbor povolení s názvom *Politika – Všetko John* s prístupom k statickej skupine *Všetko* a s povolením na **čítanie** politík (kategória povolení **Politiky**).
3. Vytvorte nový súbor povolení s názvom *Politika John*, prístupom k statickej skupine *San Diego*, ako aj povolením na **zápis** v rámci kategórií **Skupiny a počítače** a **Politiky**. Tento súbor povolení umožňuje *Johnovi* vytvárať a upravovať politiky v jeho domácej skupine *San Diego*.
4. Vytvorte nového používateľa *John* a v sekcii **Súbory povolení** vyberte vytvorené súbory povolení *Politika – Všetko John* a *Politika John*.
Vytvorenie politík
5. Vytvorte novú politiku *Všetko – Zapnúť firewall*, rozbaľte sekciu **Nastavenia**, vyberte **ESET Endpoint pre Windows**, prejdite do sekcie **Personálny firewall** > **Základné** a pre všetky nastavenia použite príznak **Vynútiť**. Rozbaľte sekciu **Priradiť** a vyberte statickú skupinu *Všetko*.
6. Vytvorte novú politiku *Johnova skupina – Zapnúť firewall*, rozbaľte sekciu **Nastavenia**, vyberte **ESET Endpoint pre Windows**, prejdite do sekcie **Personálny firewall** > **Základné** a pre všetky nastavenia použite príznak **Aplikovať**. Rozbaľte sekciu **Priradiť** a vyberte statickú skupinu *San Diego*.
Výsledok
Politiky vytvorené *správcom* budú aplikované ako prvé z dôvodu použitia príznaku **Vynútiť**. Nastavenia s týmto príznakom majú vyššiu prioritu a nemôžu byť prepísané neskoršou politikou. Po politikách správcu budú aplikované politiky vytvorené používateľom *John*.
Na zobrazenie konečného poradia politík kliknite na **Viac** > **Skupiny** > **San Diego**. Kliknite na počítač a vyberte možnosť **Zobraziť podrobnosti**. V sekcii **Konfigurácia** kliknite na **Aplikované politiky**.

Používanie programu ESET Endpoint Security samostatne

Táto časť dokumentácie, ako aj časť Práca s programom ESET Endpoint Security je určená pre tých, ktorí používajú ESET Endpoint Security bez konzoly ESET PROTECT alebo ESET PROTECT Cloud. Dostupnosť všetkých funkcií produktu ESET Endpoint Security záleží od oprávnení používateľského účtu.

Metódy inštalácie

Existuje niekoľko spôsobov, ako nainštalovať ESET Endpoint Security 9.x na klientsku pracovnú stanicu, pokiaľ ESET Endpoint Security nenasadzujete vzdialene prostredníctvom konzoly ESET PROTECT alebo ESET PROTECT Cloud.

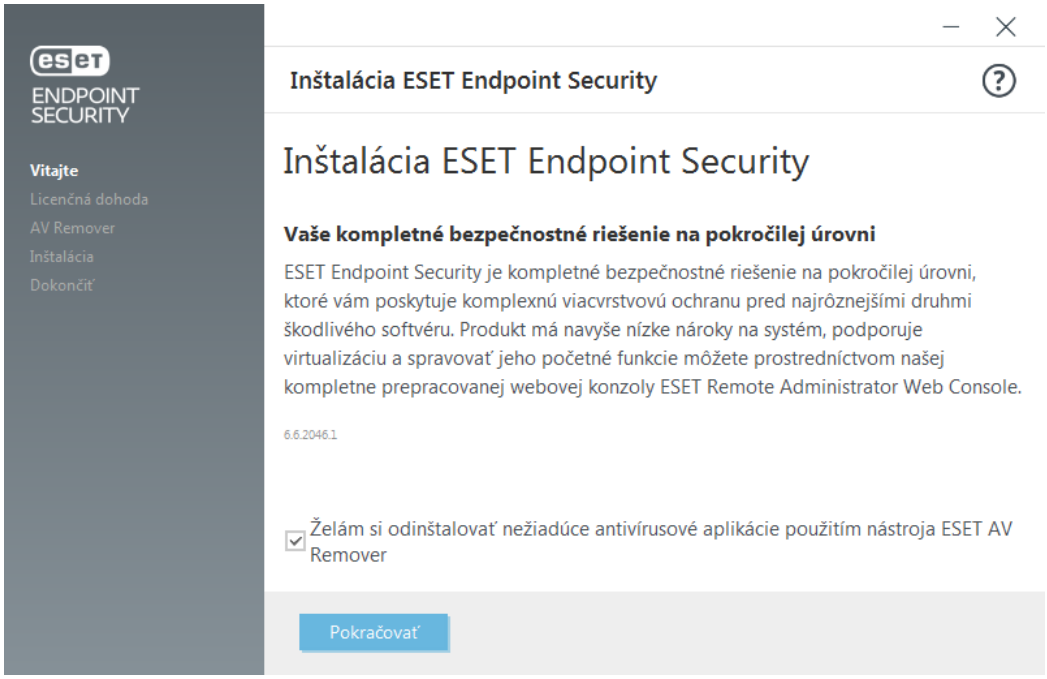
Metóda	Účel	Odkaz na stiahnutie
Inštalácia s použitím nástroja ESET AV Remover	ESET AV Remover je nástroj, ktorý vám pred pokračovaním v inštalácii pomôže odstrániť takmer akýkoľvek antivírusový softvér, ktorý už bol nainštalovaný vo vašom systéme.	Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu
Inštalácia (.exe)	Inštalácia bez použitia nástroja ESET AV Remover.	N/A

Metóda	Účel	Odkaz na stiahnutie
Inštalácia (.msi)	V podnikovom prostredí je inštalátor .msi preferovaným inštalačným balíkom. Je to najmä z dôvodu offline a vzdialených nasadení, ktoré sú vykonávané pomocou rôznych nástrojov, ako je napr. ESET PROTECT.	Stiahnuť 64-bitovú verziu Stiahnuť 32-bitovú verziu
Inštalácia cez príkazový riadok	ESET Endpoint Security je možné nainštalovať lokálne pomocou príkazového riadka alebo vzdialene prostredníctvom klientskej úlohy z konzoly ESET PROTECT.	N/A
Nasadenie pomocou GPO alebo SCCM	Na nasadenie ESET Management Agenta a ESET Endpoint Security na klientske pracovné stanice sú použité nástroje určené na správu, ako napr. GPO alebo SCCM.	N/A
Nasadenie pomocou RMM nástrojov	ESET DEM pluginy pre nástroj na vzdialenú správu a monitorovanie (RMM) vám umožňujú nasadiť ESET Endpoint Security na klientske pracovné stanice.	N/A

ESET Endpoint Security je k dispozícii vo viac ako 30 jazykoch.

Inštalácia s použitím nástroja ESET AV Remover

Skôr ako začnete s inštalačným procesom, je dôležité odinštalovať všetky ostatné antivírusové aplikácie z vášho počítača. Označte možnosť **Želám si odinštalovať nežiaduce antivírusové aplikácie použitím nástroja ESET AV Remover**, ak chcete, aby ESET AV Remover skontroloval systém a odstrániť ktorúkoľvek z podporovaných antivírusových aplikácií. Ak chcete nainštalovať ESET Endpoint Security bez spustenia nástroja ESET AV Remover, ponechajte túto možnosť neoznačenú a kliknite na **Pokračovať**.

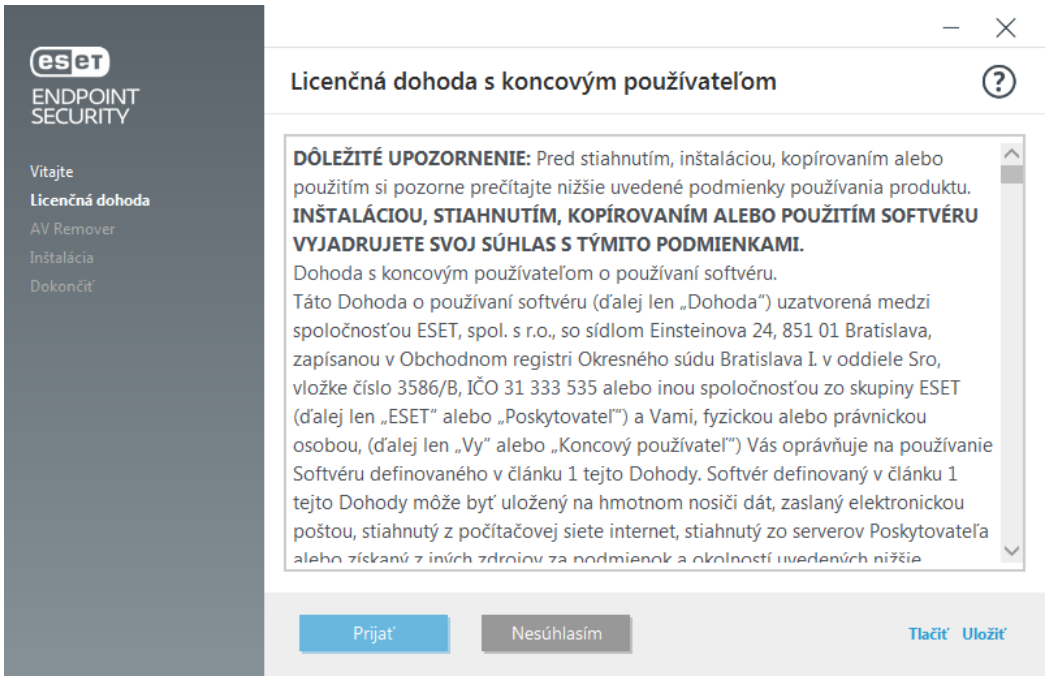


ESET AV Remover

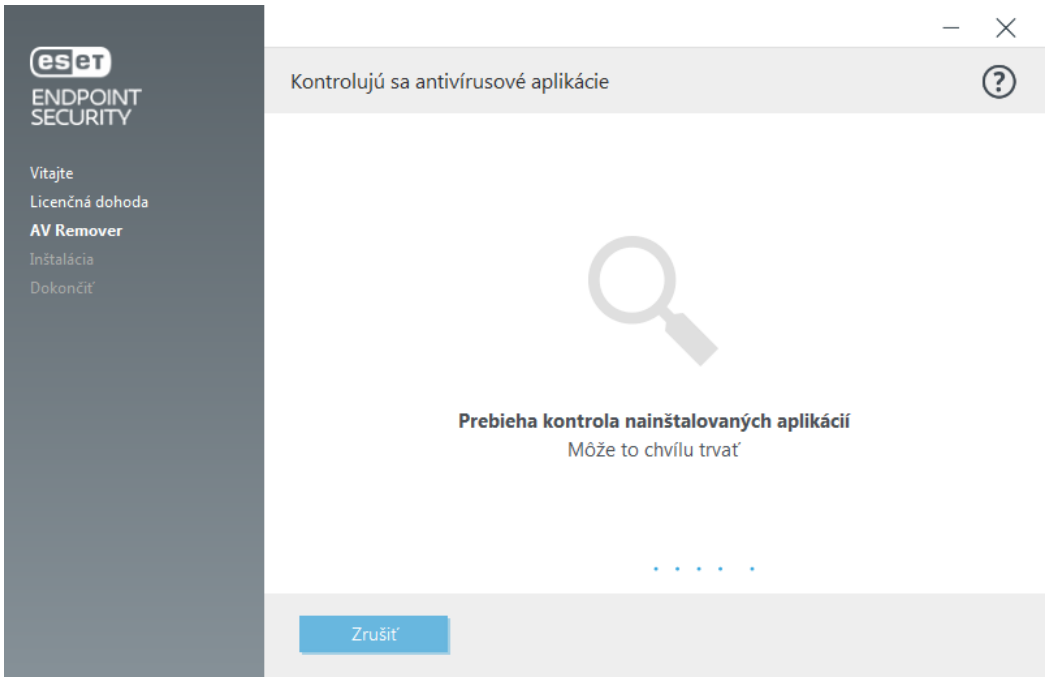
Nástroj ESET AV Remover vám pomôže odstrániť takmer akýkoľvek antivírusový softvér, ktorý už bol nainštalovaný vo vašom systéme. Na odstránenie existujúceho antivírusového programu pomocou nástroja ESET AV Remover postupujte podľa nasledujúcich inštrukcií:

1. Zoznam podporovaných antivírusových softvérov, ktoré dokáže ESET AV Remover odstrániť, nájdete v tomto článku Databázy znalostí spoločnosti ESET.

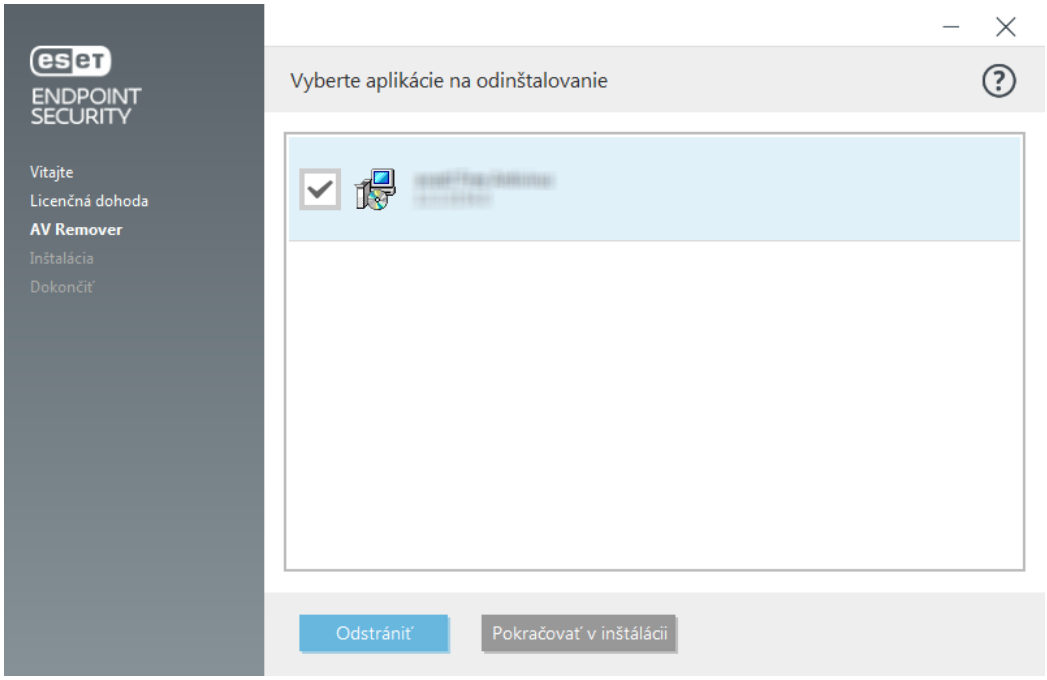
2. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA) a kliknutím na **Prijať** potvrďte svoj súhlas s uvedenými podmienkami. Kliknutím na **Nesúhlasím** budete pokračovať v inštalácii ESET Endpoint Security bez odstránenia existujúcej antivírusovej aplikácie z počítača.



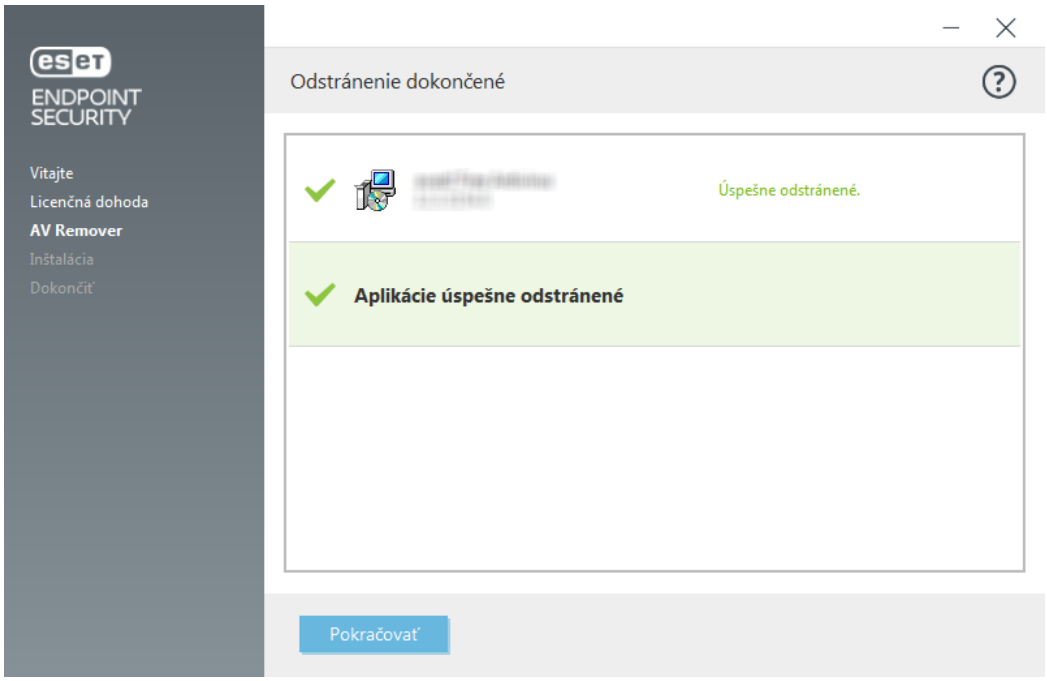
2. ESET AV Remover začne prehľadávať váš systém.



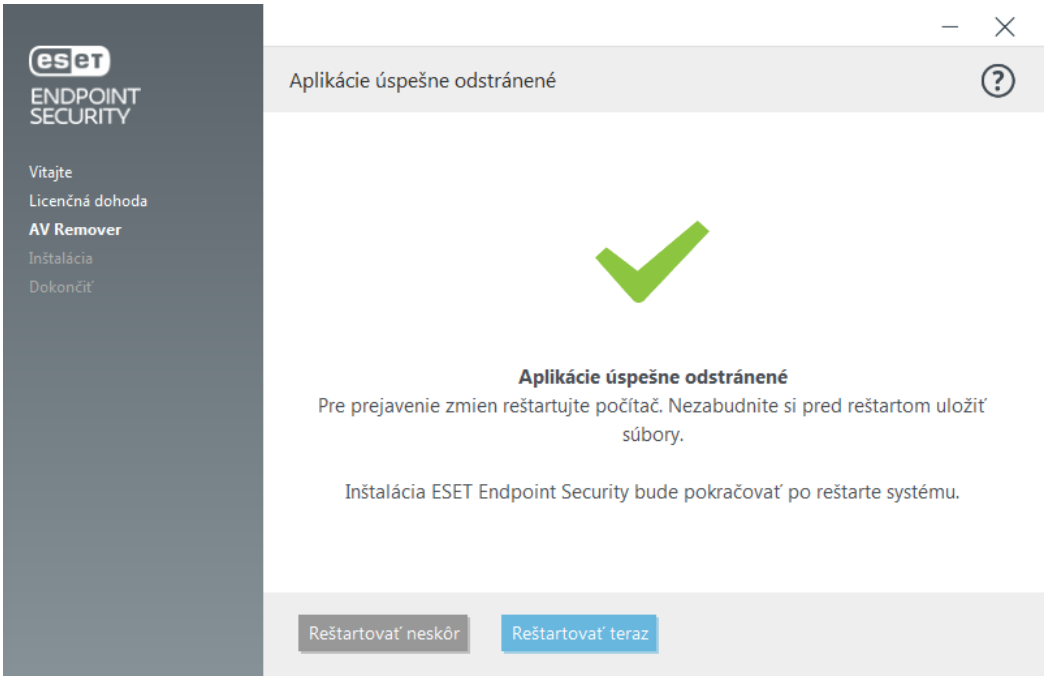
2. Zvoľte vybranú antivírusovú aplikáciu zo zoznamu a kliknite na **Odstrániť**. Odstránenie môže chvíľu trvať.



2. Po úspešnom odstránení kliknite na **Pokračovať**.



6. Reštartujte počítač, aby sa zmeny prejavili, a pokračujte v inštalácii programu ESET Endpoint Security. Ak bolo odinštalovanie neúspešné, pozrite si kapitolu Odinštalovanie pomocou nástroja ESET AV Remover skončilo chybou v tejto príručke.



Odinštalovanie pomocou nástroja ESET AV Remover skončilo chybou

Ak sa nepodarilo odstrániť antivírusový program použitím nástroja ESET AV Remover, zobrazí sa oznámenie, že aplikácia, ktorú sa pokúšate odstrániť, nie je podporovaná nástrojom ESET AV Remover. Pozrite si zoznam podporovaných produktov alebo odinštalátory pre bežné antivírusové programy pre systém Windows v Databáze znalostí spoločnosti ESET pre overenie možnosti odstránenia konkrétneho programu.

Ak bolo odinštalovanie bezpečnostného produktu neúspešné alebo bola niektorá jeho súčasť odinštalovaná len čiastočne, budete vyzvaný na vykonanie akcie **Reštartovať a skontrolovať znovu**. Potvrďte kontrolu používateľských kont (UAC) a pokračujte v prehľadávaní a procese odinštalovania.

Ak je to potrebné, kontaktujte technickú podporu spoločnosti ESET. Nezabudnite si pripraviť protokol **AppRemover.log**, ktorý pomôže pracovníkom technickej podpory pri riešení vášho problému. Súbor **AppRemover.log** sa nachádza v priečinku **eset**. Tento priečinok najľahšie otvoríte tak, že do prieskumníka napíšete *%TEMP%*. Pracovníci Technickej podpory spoločnosti ESET vás budú kontaktovať čo najskôr, aby vám pomohli vyriešiť váš problém.

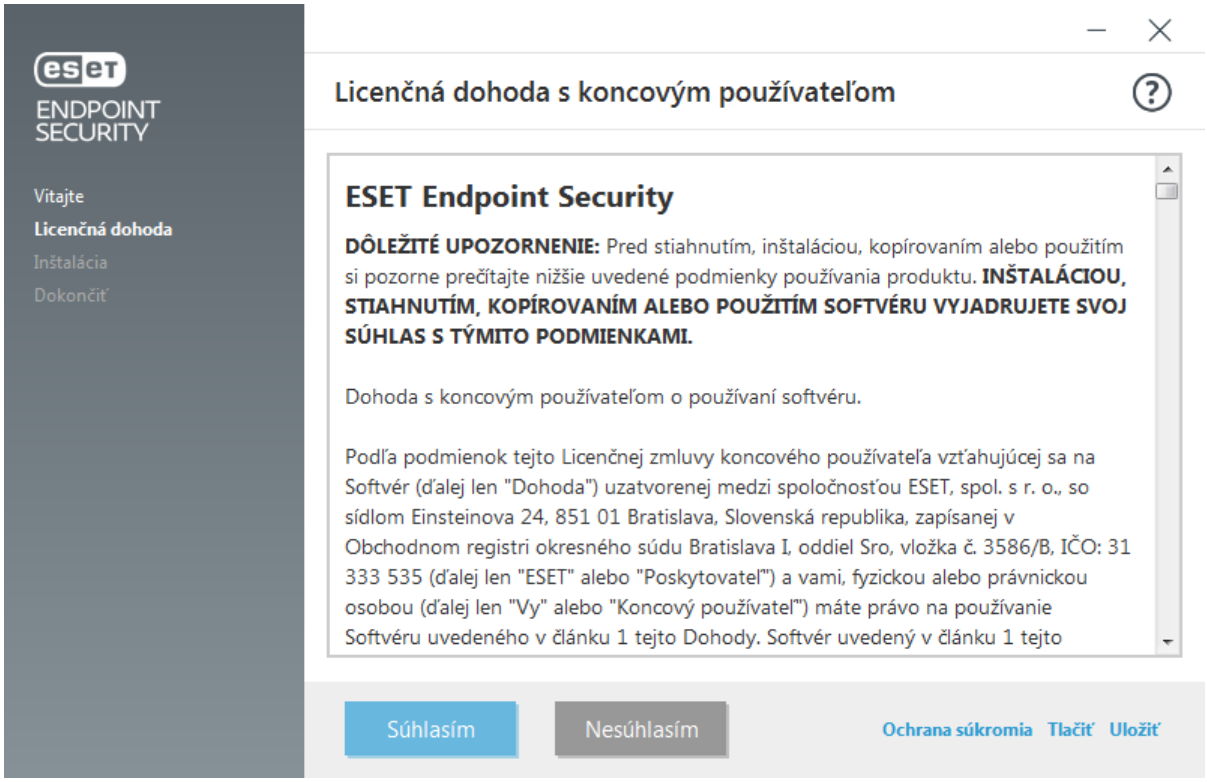
Inštalácia (.exe)

Po spustení .exe inštalátora vás sprievodca prevedie celým inštalačným procesom.

Uistite sa, že nemáte na počítači nainštalované žiadne iné antivírusové programy. Medzi dvoma antivírusovými programami môže dochádzať ku konfliktu. Odporúčame preto odinštalovať akýkoľvek iný antivírusový program zo systému. Viac informácií a zoznam odinštalátorov pre najbežnejšie antivírusové programy nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.



1. Prečítajte si Licenčnú dohodu s koncovým používateľom. Ak chcete nastaviť detekciu Potenciálne nechcených aplikácií a zapnúť Systém spätnej väzby ESET LiveGrid®, kliknite na **Povoliť všetko a pokračovať**. ESET LiveGrid® pomáha zaistiť, že ESET je okamžite a neustále informovaný o nových infiltráciách, čo nám umožňujú lepšie chrániť našich zákazníkov. Systém povoľuje odosielať nové druhy hrozieb do vírusového laboratória spoločnosti ESET, kde sú tieto hrozby analyzované a zapracovávané do aktualizácií detekčného jadra. Kliknite na tlačidlo **Pokračovať**, aby ste potvrdili váš súhlas s Licenčnou dohodou s koncovým používateľom. Ak chcete ESET Endpoint Security nainštalovať do iného ako predvoleného priečinka, kliknite na **Zmeniť inštalačný priečinok**.



2. Po dokončení inštalácie sa vám zobrazí výzva na aktiváciu ESET Endpoint Security.

Zmena inštalačného priečinka (.exe)

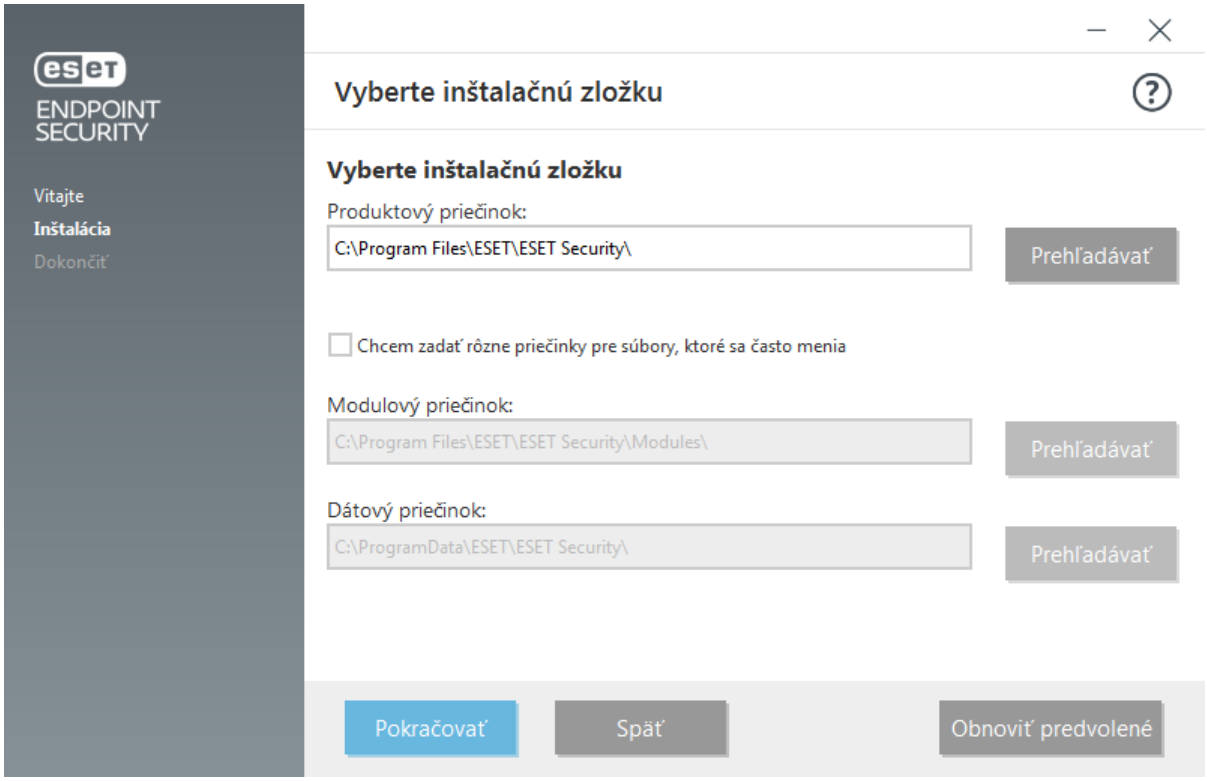
Po povolení/zakázaní detekcie potenciálne nechcených aplikácií a kliknutí na možnosť **Zmeniť inštalačný priečinok** budete vyzvaný zvoliť umiestnenie pre priečinok s inštalačnými súbormi programu ESET Endpoint Security. Predvolený inštalačný priečinok je nasledovný:

C:\Program Files\ESET\ESET Security

Je možné zadať umiestnenie pre moduly a dáta programu. Predvolene sa inštalujú do nasledujúcich priečinkov:

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

Ak chcete tieto umiestnenia zmeniť, kliknite na **Prehľadávať** (neodporúča sa).



Kliknite na **Späť** a potom pokračujte v inštalácii.

Inštalácia (.msi)

Po spustení inštalátora .msi vás sprievodca prevedie celým inštalačným procesom.

V podnikovom prostredí je inštalátor .msi preferovaným inštalačným balíkom. Je to najmä z dôvodu offline a vzdialených nasadení, ktoré sú vykonávané pomocou rôznych nástrojov, ako je napr. ESET PROTECT.

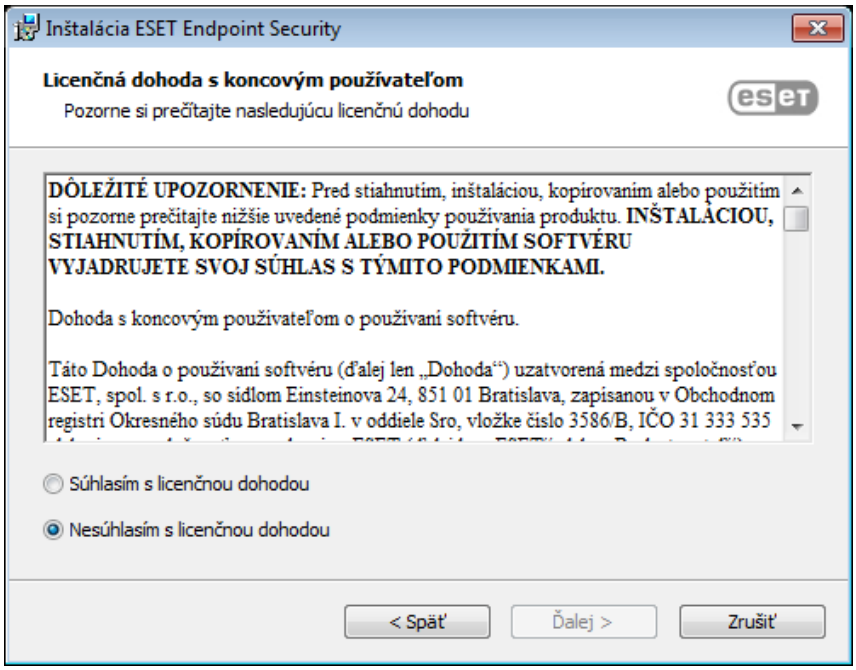
Uistite sa, že nemáte na počítači nainštalované žiadne iné antivírusové programy. Medzi dvoma antivírusovými programami môže dochádzať ku konfliktu. Odporúčame preto odinštalovať akýkoľvek iný antivírusový program zo systému. Viac informácií a zoznam odinštalátorov pre najbežnejšie antivírusové programy nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Inštalátor produktu ESET Endpoint Security vytvorený v ESET PROTECT 8.1 a novších verziách podporuje Windows 10 Enterprise for Virtual Desktops a Windows 10 v režime viacerých relácií (multi-session).

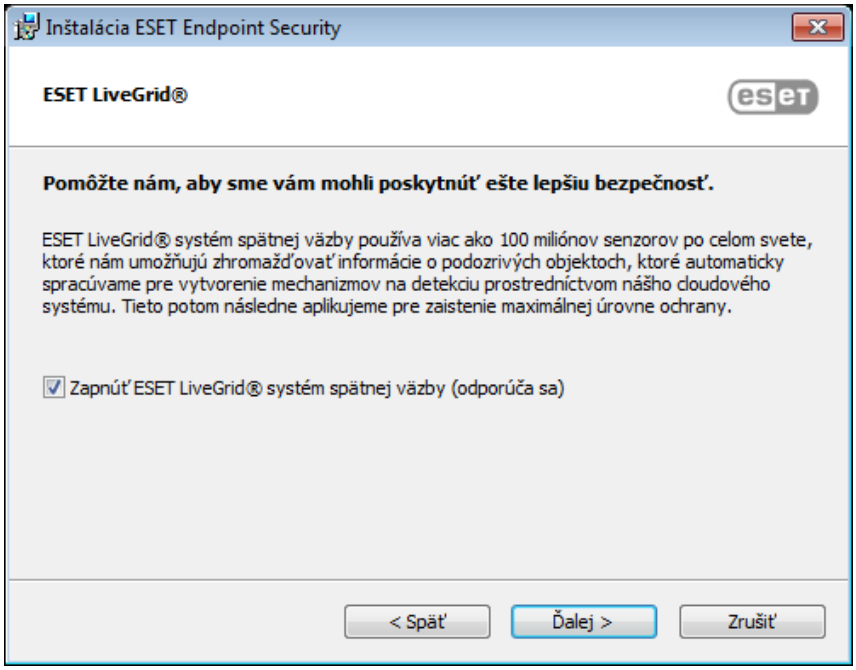
1. Vyberte požadovaný jazyk a kliknite na **Ďalej**.



2. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA) a potvrďte váš súhlas s uvedenými podmienkami kliknutím na **Súhlasím s licenčnou dohodou**. Následne kliknite na **Ďalej** pre pokračovanie v inštalácii.



3. Ďalej vyberte svoje preferencie pre systém ESET LiveGrid®. ESET LiveGrid® umožňuje, aby bola spoločnosť ESET pohotovo a neustále informovaná o nových infiltráciách s cieľom lepšie chrániť svojich zákazníkov. Systém povoľuje odosielať nové druhy hrozieb do vírusového laboratória spoločnosti ESET, kde sú tieto hrozby analyzované a zapracovávané do aktualizácií detekčného jadra. Ak si želáte pokračovať v pokročilej inštalácii (.msi), kliknite na **Rozšírené nastavenia**.



5. Posledným krokom je potvrdenie inštalácie kliknutím na **Inštalovať**. Po dokončení inštalácie sa vám zobrazí výzva na aktiváciu ESET Endpoint Security.

Pokročilá inštalácia (.msi)

Pokročilá inštalácia vám umožňuje nastaviť parametre, ktoré nie sú dostupné pri klasickej inštalácii.

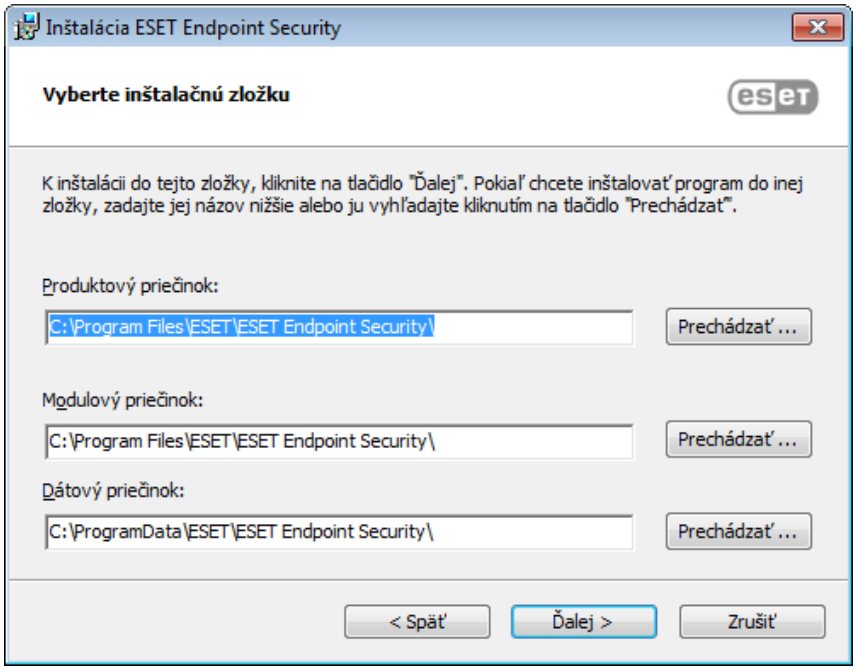
5. Po povolení/zakázaní detekcie potenciálne nechcených aplikácií a kliknutí na **Rozšírené nastavenia** bude potrebné zvoliť umiestnenie pre priečinok s inštalačnými súbormi ESET Endpoint Security. Predvolený inštalačný priečinok je nasledovný:

C:\Program Files\ESET\ESET Security

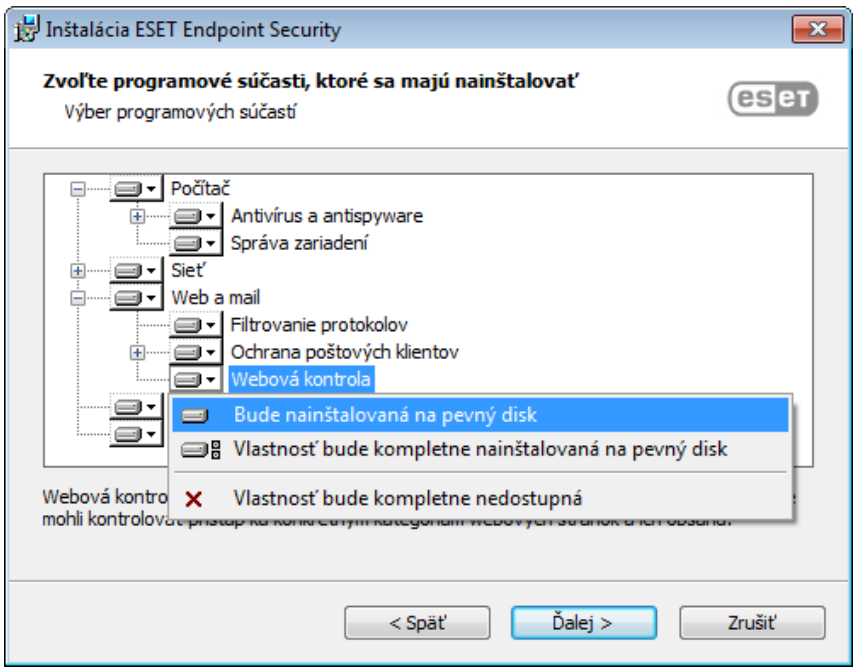
Je možné zadať umiestnenie pre moduly a dáta programu. Predvolene sa inštalujú do nasledujúcich priečinkov:

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

Ak chcete tieto umiestnenia zmeniť, kliknite na **Prehľadávať** (neodporúča sa).



6. V ďalšom okne môžete vybrať, ktoré programové súčasti budú nainštalované. V sekcii Počítač sú zahrnuté súčasti, ako napr. Rezidentná ochrana súborového systému, Kontrola počítača, Ochrana dokumentov a Správa zariadení. Moduly Rezidentná ochrana súborového systému a Kontrola počítača sú povinné a nevyhnutné pre správnu funkčnosť programu. Sekcia Sieť umožňuje nainštalovať ESET Firewall, ktorý monitoruje všetku prichádzajúcu a odchádzajúcu sieťovú komunikáciu a aplikuje pravidlá pre jednotlivé sieťové pripojenia. Firewall tiež poskytuje ochranu pred útokmi zo vzdialených počítačov. Ochrana pred sieťovými útokmi (IDS) analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Akákoľvek komunikácia, ktorá je považovaná za nebezpečnú, bude zablokovaná. Súčasti v sekcii Web a e-mail zabezpečujú ochranu pri prehliadaní internetu a komunikácii prostredníctvom e-mailu. Aktualizačný mirror môže byť použitý na aktualizáciu produktov ESET na ostatných počítačoch vo vašej sieti. Vzdialený monitoring a správa (RMM) je proces vzdialeného monitorovania a ovládania softvérových systémov pomocou agenta inštalovaného na koncové zariadenia. Bezpečnostné produkty spoločnosti ESET určené pre firmy podporujú RMM prostredníctvom nástrojov tretích strán.



7. Posledným krokom je potvrdenie inštalácie kliknutím na **Inštalovať**.

Minimálna inštalácia

S cieľom znížiť množstvo prenášaných dát v súvislosti s inštalátorom a tiež spotrebu systémových prostriedkov ponúkame inštalačný balík obsahujúci minimum potrebných modulov. Inštalátor tak zahŕňa iba najdôležitejšie moduly a všetky ostatné moduly sa stiahnu v priebehu prvotnej aktualizácie modulov, ktorá prebehne po aktivácii produktu. Výhodou je tak výrazné zníženie veľkosti inštalačného balíka, ako aj to, že pri aktivácii produktu ESET Endpoint Security sa stiahnu len najnovšie moduly aplikácie.

Inštalátor určený na minimálnu inštaláciu obsahuje nasledujúce moduly:

- Zavádzače (loader)
- Modul technológie Anti-Stealth
- Komunikačný modul Direct Cloud
- Modul jazykovej lokalizácie
- Modul konfigurácie
- SSL modul

Po aktivácii produktu sa zobrazí stav **Inicializuje sa ochrana**, ktorý vás informuje o tom, že prebieha inicializácia funkcií.

V prípade problému so sťahovaním modulov (napríklad z dôvodu chybného nastavenia proxy, nedostupnej siete atď.) sa stav aplikácie zmení na oranžový a zobrazí sa hlásenie **Vyžaduje sa vaša pozornosť**. V hlavnom okne programu kliknite na **Aktualizovať** > **Overiť dostupnosť aktualizácií**, aby ste znovu spustili aktualizačný proces.

Po niekoľkých neúspešných pokusoch sa stav aplikácie zmení na červený a zobrazí sa hlásenie **Ochranu sa nepodarilo nastaviť**.

Ak klientske počítače nemajú pripojenie na internet, prípadne sú v offline prostredí a potrebujú aktualizácie, môžete použiť jednu z nasledujúcich metód na sťahovanie aktualizačných súborov zo serverov ESET:

- Aktualizácia z mirrora
- Použitie nástroja Mirror Tool

Ak inicializačný proces zlyhá a nebudete môcť stiahnuť moduly, stiahnite plnohodnotné inštalátory MSI tu.

Inštalácia cez príkazový riadok

ESET Endpoint Security môžete nainštalovať lokálne pomocou príkazového riadka alebo vzdialene prostredníctvom klientskej úlohy z konzoly ESET PROTECT.

Podporované parametre

APPDIR=<path>

- Path – platná cesta k adresáru.
- Adresár, do ktorého bude aplikácia nainštalovaná.

APPDATADIR=<path>

- Path – platná cesta k adresáru.
- Adresár, do ktorého budú uložené dáta aplikácie.

MODULEDIR=<path>

- Path – platná cesta k adresáru.
- Adresár, do ktorého budú nainštalované moduly aplikácie.

ADDLOCAL=<list>

- Inštalácia súčastí – zoznam voliteľných funkcií, ktoré budú nainštalované lokálne.
- Použitie s ESET inštalačnými balíkmi .msi: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Viac informácií o parametri **ADDLOCAL** nájdete na webovej stránke http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx.

ADDEXCLUDE=<list>

- Zoznam ADDEXCLUDE je čiarkami oddelený zoznam názvov všetkých funkcií, ktoré nemajú byť nainštalované. Ide o náhradu za REMOVE.
- Pri výbere funkcie, ktorá nemá byť nainštalovaná, musí byť v zozname uvedená úplná cesta (t. j. vrátane všetkých podfunkcií) a súvisiace neviditeľné funkcie.
- Použitie s ESET inštalačnými balíkmi .msi: `ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **ADDEXCLUDE** nie je možné použiť spolu s **ADDLOCAL**.

Podrobnejšie informácie o tom, aké prepínače podporuje konkrétna verzia **msiexec**, nájdete v príslušnej dokumentácii.

Pravidlá

- **ADDLOCAL** je zoznam čiarkou oddelených funkcií, ktoré budú nainštalované.
- Pri výbere funkcie na inštaláciu musí byť v zozname uvedená celá cesta (vrátane všetkých rodičovských funkcií).
- Pre správne použitie pozrite ostatné pravidlá.

Súčasti a funkcie

> Inštalácia súčastí pomocou parametrov ADDLOCAL/ADDEXCLUDE nebude v prípade ESET Endpoint Antivirus fungovať.

Funkcie sú rozdelené do 4 kategórií:

- **Povinné** – funkcia bude nainštalovaná vždy.
- **Voliteľné** – pre takúto funkciu je možné zrušiť označenie a nenainštalovať ju.
- **Neviditeľné** – funkcia je povinná pre správne fungovanie inej funkcie.
- **Zástupný symbol** – funkcia, ktorá neovplyvňuje produkt, ale má iné funkcie.

Nižšie nájdete zoznam funkcií a komponentov ESET Endpoint Security:

Popis	Názov funkcie	Nadradená funkcia	Prítomnosť
Základné programové súčasti	Computer		Zástupný symbol
Detekčné jadro	Antivirus	Computer	Povinné
Detekčné jadro/Detekcia malvéru	Scan	Computer	Povinné
Detekčné jadro/Rezidentná ochrana súborového systému	RealtimeProtection	Computer	Povinné
Detekčné jadro/Detekcia malvéru/Ochrana dokumentov	DocumentProtection	Antivirus	Voliteľné
Správa zariadení	DeviceControl	Computer	Voliteľné
Ochrana siete	Network		Zástupný symbol
Ochrana siete/Firewall	Firewall	Network	Voliteľné
Ochrana siete/Ochrana pred sieťovými útokmi/...	IdsAndBotnetProtection	Network	Voliteľné
Zabezpečený prehliadač	OnlinePaymentProtection	WebAndEmail	Voliteľné
Web a e-mail	WebAndEmail		Zástupný symbol
Web a e-mail/Filtrovanie protokolov	ProtocolFiltering	WebAndEmail	Neviditeľné
Web a e□mail/Ochrana prístupu na web	WebAccessProtection	WebAndEmail	Voliteľné
Web a e-mail/Ochrana e-mailových klientov	EmailClientProtection	WebAndEmail	Voliteľné
Web a e-mail/Ochrana e-mailových klientov/E-mailové klienty	MailPlugins	EmailClientProtection	Neviditeľné
Web a e-mail/Ochrana e-mailových klientov/Antispamová ochrana	Antispam	EmailClientProtection	Voliteľné
Web and e-mail/Webová kontrola	WebControl	WebAndEmail	Voliteľné
Nástroje/ESET RMM	Rmm		Voliteľné
Aktualizácia/Profily/Aktualizačný mirror	UpdateMirror		Voliteľné
Plugin ESET Inspect	EnterpriseInspector		Neviditeľné

Skupiny funkcií:

Popis	Názov funkcie	Prítomnosť funkcie
Všetky povinné funkcie	_Base	Neviditeľné
Všetky dostupné funkcie	ALL	Neviditeľné

Ostatné pravidlá

- Ak bude vybraná na inštaláciu niektorá z funkcií v sekcii **WebAndEmail**, neviditeľná funkcia **ProtocolFiltering** musí byť zahrnutá v zozname.
- Názvy všetkých funkcií rozlišujú malé a veľké písmená, napríklad UpdateMirror sa nerovná UPDATEMIRROR.

Zoznam vlastností konfigurácie

Vlastnosť	Hodnota	Funkcia
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – vypnuté 1 – zapnuté	Detekcia potenciálne nechcených aplikácií (PUA)
CFG_LIVEGRID_ENABLED=	Pozrite nižšie	Pozrite sa nižšie na vlastnosť LiveGrid
FIRSTSCAN_ENABLE=	0 – vypnuté 1 – zapnuté	Naplánovanie a spustenie Kontroly počítača po inštalácii
CFG_PROXY_ENABLED=	0 – vypnuté 1 – zapnuté	Nastavenie proxy servera
CFG_PROXY_ADDRESS=	<ip>	IP adresa proxy servera
CFG_PROXY_PORT=	<port>	Číslo portu proxy servera
CFG_PROXY_USERNAME=	<username>	Používateľské meno pre overenie
CFG_PROXY_PASSWORD=	<password>	Heslo pre overenie
ACTIVATION_DATA=	Pozrite nižšie	Aktivácia produktu, licenčný kľúč alebo offline licenčný súbor
ACTIVATION_DLG_SUPPRESS=	0 – vypnuté 1 – zapnuté	Ak je nastavená možnosť „1“, okno aktivácie produktu sa pri prvom spustení nezobrazí
ADMINCFG=	<path>	Cesta k exportovanej XML konfigurácii (predvolená hodnota je *cfg.xml*)

Vlastnosti dostupné iba v ESET Endpoint Security

CFG_EPFW_MODE=	0 – Automatický (predvolené) 1 – Interaktívny 2 – Na základe politík 3 – Učiaci sa	Režim filtrovania firewallu
CFG_EPFW_LEARNINGMODE_ENDTIME=	<timestamp>	Koniec učiaceho sa režimu v unixovom čase

Vlastnosť LiveGrid®

Ak pri inštalácii ESET Endpoint Security použijete parameter CFG_LIVEGRID_ENABLED, výsledné nastavenie produktu bude nasledovné:

Funkcia	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
Reputačný systém ESET LiveGrid®	Zapnuté	Zapnuté
Systém spätnej väzby ESET LiveGrid®	Vypnuté	Zapnuté
Odosielať anonymné štatistiky	Vypnuté	Zapnuté

Vlastnosť ACTIVATION_DATA

Formát	Metóda
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	Aktivácia pomocou ESET licenčného kľúča (internetové pripojenie by malo byť aktívne)

Formát	Metóda
`ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf`	Aktivácia pomocou offline licenčného súboru

Vlastnosť jazyka

Jazyk ESET Endpoint Security (musíte zadať obidva parametre).

Vlastnosť	Hodnota
`PRODUCT_LANG=`	LCID desatinné číslo (Locale ID), napríklad 1033 pre angličtinu (Spojené štáty) – pozrite si zoznam jazykových kódov.
`PRODUCT_LANG_CODE=`	LCID reťazec (Language Culture Name) uvedený malými písmenami, napríklad en-us pre angličtinu (Spojené štáty) – pozrite si zoznam jazykových kódov.

Vlastnosti týkajúce sa reštartu počítača

Nasledujúce parametre môžete použiť na reštartovanie počítača po dokončení inštalácie:

Vlastnosť	Hodnota	Funkcia
`REBOOT_WHEN_NEEDED=`	0 – vypnuté 1 – zapnuté	Ak je táto možnosť zapnutá, po dokončení inštalácie sa počítač reštartuje.
`REBOOT_CANCELABLE=`	0 – vypnuté 1 – zapnuté	Ak je táto možnosť zapnutá, používateľ bude môcť zrušiť reštart počítača.
`REBOOT_POSTPONE=`	hodnota v sekundách	Maximálny časový interval v sekundách, počas ktorého môže používateľ odložiť reštart počítača.

Hodnoty REBOOT_CANCELABLE a REBOOT_POSTPONE sa berú do úvahy iba v prípade, keď je zapnutá možnosť REBOOT_WHEN_NEEDED.

Príklady inštalácie pomocou príkazového riadka

Pred inštaláciou sa uistite, že ste si prečítali Licenčnú dohodu s koncovým používateľom a máte oprávnenia správcu.

Vylúčenie sekcie **NetworkProtection** z inštalácie (je potrebné tiež definovať všetky podradené funkcie):
`msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection`

Ak chcete, aby sa váš produkt ESET Endpoint Security po inštalácii automaticky nakonfiguroval, môžete použiť základné parametre konfigurácie v inštalačnom príkaze.
Inštalácia ESET Endpoint Security so zapnutou funkciou ESET LiveGrid®:
`msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1`

Inštalácia do iného ako predvoleného priečinka.
`msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\`

Inštalácia a aktivácia ESET Endpoint Security pomocou licenčného kľúča ESET.
`msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE`

Tichá inštalácia s podrobným zapisovaním do protokolu (užitočné pri riešení problémov) a RMM s iba povinnými súčasťami:
`msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm`

Vynútená tichá úplná inštalácia s definovaným jazykom.
`msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us`

Možnosti ovládania produktu pomocou príkazového riadka

- ESET CMD – import konfiguračného .xml súboru alebo zapnutie/vypnutie bezpečnostnej funkcie
- Modul kontroly cez príkazový riadok – spustenie kontroly počítača z príkazového riadka

Nasadenie pomocou GPO alebo SCCM

Okrem priamej inštalácie programu ESET Endpoint Security na klientsky počítač môžete použiť aj nástroje určené na správu, ako napríklad Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris alebo Puppet.

Spravované prostredie (odporúčané)

V spravovaných prostrediach odporúčame najprv nainštalovať ESET Management Agenta a potom nasadiť ESET Endpoint Security cez ESET PROTECT. Konzola ESET PROTECT však už musí byť nainštalovaná vo vašej sieti.

1. Stiahnite si samostatný inštalátor pre ESET Management Agenta.
2. Pripravte si GPO/SCCM skript.
3. Nasaďte ESET Management Agenta pomocou GPO aleboSCCM.
4. Uistite sa, že klientske počítače boli pridané do ESET PROTECT.
5. Nasaďte a aktivujte ESET Endpoint Security na svoje klientske počítače.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Nasadenie ESET Management Agenta cez SCCM alebo GPO
- Nasadenie ESET Management Agenta pomocou GPO (Group Policy Object)

Nespravované prostredie

V nespravovaných prostrediach môžete nasadiť ESET Endpoint Security aj priamo na klientske stanice. Toto však neodporúčame, pretože nebudete môcť na pracovných staniciach monitorovať a vynucovať politiky svojich produktov ESET určených pre koncové zariadenia.

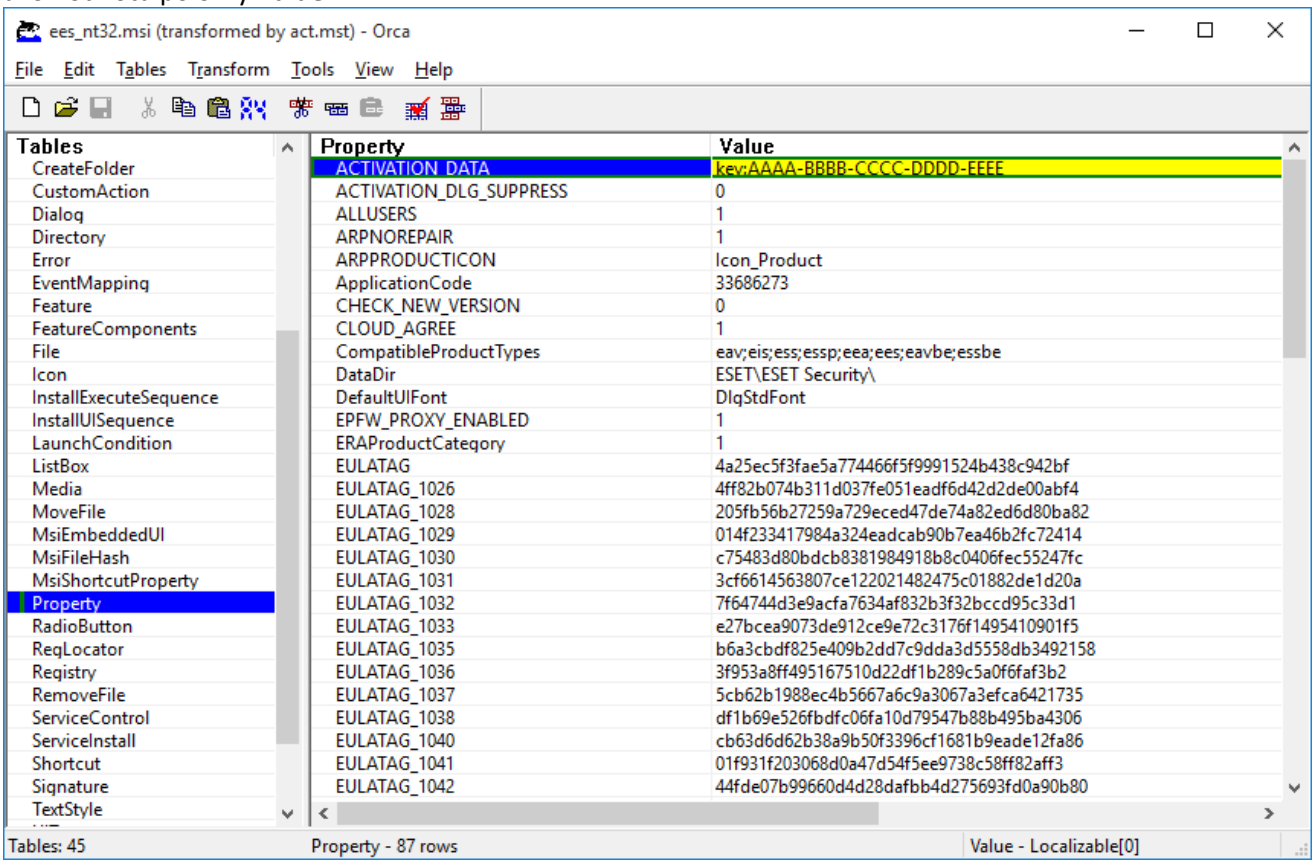
Štandardne produkt ESET Endpoint Security nie je po inštalácii aktivovaný, a preto nie je funkčný.

Možnosť č. 1 (inštalácia softvéru)

1. Stiahnite si .msi inštalátor pre ESET Endpoint Security.
2. Vytvorte transformačný balík .mst zo súboru .msi (napríklad pomocou nástroja Orca .msi Editor), ktorý bude obsahovať vlastnosť pre aktiváciu produktu (pozrite `ACTIVATION_DATA` v kapitole Inštalácia cez príkazový riadok).

Zobraziť kroky pre vytvorenie .mst v nástroji Orca

1. Otvorte Orca.
2. Načítajte .msi inštalátor kliknutím na **File** > **Open**.
3. Kliknite na **Transform** > **New Transform**.
4. Kliknite na **Property** v sekcii **Tables** a potom v menu **Tables** vyberte možnosť **Add row**.
5. V okne **Add Row** zadajte ACTIVATION_DATA ako hodnotu položky **Property** a licenčné informácie zadajte ako hodnotu položky **Value**.



6. Kliknite na **Transform** > **Generate Transform** pre uloženie .mst súboru.

1. Voliteľné: Ak chcete importovať svoj vlastný konfiguračný súbor .xml do produktu ESET Endpoint Security (napr. na povolenie RMM alebo kvôli konfigurácii proxy servera), umiestnite súbor cfg.xml do rovnakého umiestnenia ako .msi inštalátor.
2. Nasaďte .msi inštalátor spolu s .mst súborom vzdialene prostredníctvom GPO (inštalácia softvéru) alebo SCCM.

Možnosť č. 2 (pomocou plánovanej úlohy)

1. Stiahnite si .msi inštalátor pre ESET Endpoint Security.
2. Pripravte si skript pre inštaláciou pomocou príkazového riadka, ktorý bude obsahovať vlastnosť pre aktiváciu produktu (pozrite `ACTIVATION_DATA`).
3. Uistite sa, že k .msi inštalátoru a .cmd skriptu majú prístup všetky pracovné stanice v sieti.
4. Voliteľné: Ak chcete importovať svoj vlastný konfiguračný súbor .xml do produktu ESET Endpoint Security (napr. na povolenie RMM alebo kvôli konfigurácii proxy servera), umiestnite súbor cfg.xml do rovnakého umiestnenia ako .msi inštalátor.
5. Pripravený inštalačný skript použite prostredníctvom GPO alebo SCCM.
    - V prípade GPO použite Group Policy Preferences > Group Policy Schedule Tasks > Immediate task.

Ak nechcete používať ESET PROTECT na vzdialenú správu svojich bezpečnostných produktov ESET, ESET Endpoint Security obsahuje plugin ESET pre RMM, ktorý vám umožní spravovať a kontrolovať softvérové systémy pomocou lokálne nainštalovaného agenta, ku ktorému môže pristupovať poskytovateľ spravovaných riešení (MSP).
• Pre podrobnejšie informácie kliknite sem

Prechod na novšiu verziu

Nové verzie ESET Endpoint Security sú vydávané kvôli zabudovaným vylepšeniam produktu a opravám chýb, ktoré nie je možné opraviť v rámci automatickej aktualizácie programových modulov.

Je niekoľko spôsobov, ako aktualizovať produkt na novšiu verziu:

1. Automaticky prostredníctvom konzoly ESET PROTECT alebo ESET PROTECT Cloud. ESET Endpoint Security vo verzii 9 nie je možné spravovať prostredníctvom nástroja ESET Remote Administrator.
2. Automaticky prostredníctvom GPO alebo SCCM.
3. Automaticky prostredníctvom aktualizácie programu.
   Keďže aktualizácia programu je posielaná všetkým používateľom daného produktu a môže mať významný dopad na konfiguráciu systému, je uvoľnená až po dlhom období testovania v rôznych konfiguráciách, aby sa zaistila úplná funkčnosť pre všetky možné systémové konfigurácie. Ak potrebujete aktualizovať na najnovšiu verziu hneď po jej vydaní, použite niektorú z nasledujúcich dvoch metód.
   Uistite sa, že ste povolili **Režim aktualizácie** v sekcii **Rozšírené nastavenia** (F5) > **Aktualizácia** > **Profily** > **Aktualizácie produktu**.
4. Manuálne, stiahnutím a nainštalovaním novej verzie cez starú verziu programu pomocou inštalátora.

Odporúčané scenáre prechodu na novšiu verziu

Spravujem alebo chcem spravovať produkty ESET vzdialene

Ak spravujete viac ako desať produktov ESET určených pre koncové zariadenia, zvážte prechod na novšiu verziu prostredníctvom konzoly ESET PROTECT alebo ESET PROTECT Cloud.

Bližšie informácie nájdete v dokumentácii:

- ESET PROTECT | Aktualizácia softvéru ESET pomocou klientskej úlohy
- ESET PROTECT | Príručka pre malé a stredné podniky s maximálne 250 produktami ESET na koncových zariadeniach Windows
- Predstavenie programu ESET PROTECT Cloud

Manuálny prechod na novšiu verziu na klientskej pracovnej stanici

Neinštalujte verziu 9 cez verziu 4.x. Podobne, ak máte starší/nefunkčný produkt ESET Endpoint Security vo verzii 5.x alebo 6.x.

Ak chcete manuálne prejsť na novšiu verziu produktu na individuálnych klientskych staniciach:

1. Uistite sa, že váš operačný systém je podporovaný (Windows Vista aWindows XP nie sú podporované touto verziou produktu).

2. Stiahnite a nainštalujte novšiu verziu cez staršiu verziu programu.

Ak chcete maximálne zvýšiť pravdepodobnosť úspešného prechodu na najnovšiu verziu 9.x, prejdite na ňu z jednej z týchto verzií ESET Endpoint Security:
• 5.0.2272.x
• 6.5.2132.x
• 7.3.2044.x
V opačnom prípade najskôr odinštalujte ESET Endpoint Security. Ďalšie informácie o prechode na najnovšiu verziu ESET Endpoint Security na klientskej pracovnej stanici nájdete v našom článku Databázy znalostí spoločnosti ESET.

Aktualizácie zaisťujúce bezpečnosť a stabilitu

Pravidelné aktualizovanie produktu ESET Endpoint Security je základným predpokladom na zaistenie maximálnej bezpečnosti systému. Každá nová verzia ESET Endpoint Security prináša mnoho vylepšení aj opráv chýb. Dôrazne odporúčame pravidelne aktualizovať ESET Endpoint Security, aby ste si zaistili ochranu pred hrozbami a predišli možnému zneužitiu bezpečnostných zraniteľností. Tak ako na všetky produkty ESET aj na ESET Endpoint Security sa vzťahuje životný cyklus produktov určujúci úroveň poskytovanej podpory.

Viac informácií:
Politika životného cyklu produktov (pre firmy)
Aktualizácie produktu
Rýchle opravy zabezpečenia a stability
Ďalšie informácie o zmenách v produkte ESET Endpoint Security si môžete prečítať v Databáze znalostí.

Automatické aktualizácie zabezpečujú maximálnu bezpečnosť a stabilitu vášho produktu. Nie je preto možné vypnúť aktualizácie zaisťujúce bezpečnosť a stabilitu.

Časté problémy pri inštalácii

Pozrite si nasledujúci článok so zoznamom častých problémov pri inštalácii a ich riešením.

Aktivácia nebola úspešná

V prípade, že aktivácia ESET Endpoint Security nebola úspešná, pravdepodobne to bolo spôsobené niektorým z nasledujúcich problémov:

- Licenčný kľúč sa už používa.
- Neplatný licenčný kľúč. Chyba formulára aktivácie produktu.
- Dodatočné informácie potrebné pre aktiváciu chýbajú alebo sú neplatné.
- Zlyhala komunikácia s aktivačnou databázou. Skúste aktivovať produkt znova o 15 minút.
- Nie je dostupné alebo je vypnuté pripojenie k aktivačným serverom ESET.

Uistite sa, že ste zadali správny licenčný kľúč alebo vložili správnu offline licenciu a pokúste sa aktiváciu vykonať znova.

Ak sa vám nedarí aktivovať produkt, náš sprievodca vám poskytne odpovede na najčastejšie otázky, chyby a problémy týkajúce sa aktivácie a licencovania (dostupné v angličtine a niekoľkých ďalších jazykoch).

- Spustenie sprievodcu riešením problémov s aktiváciou produktu ESET

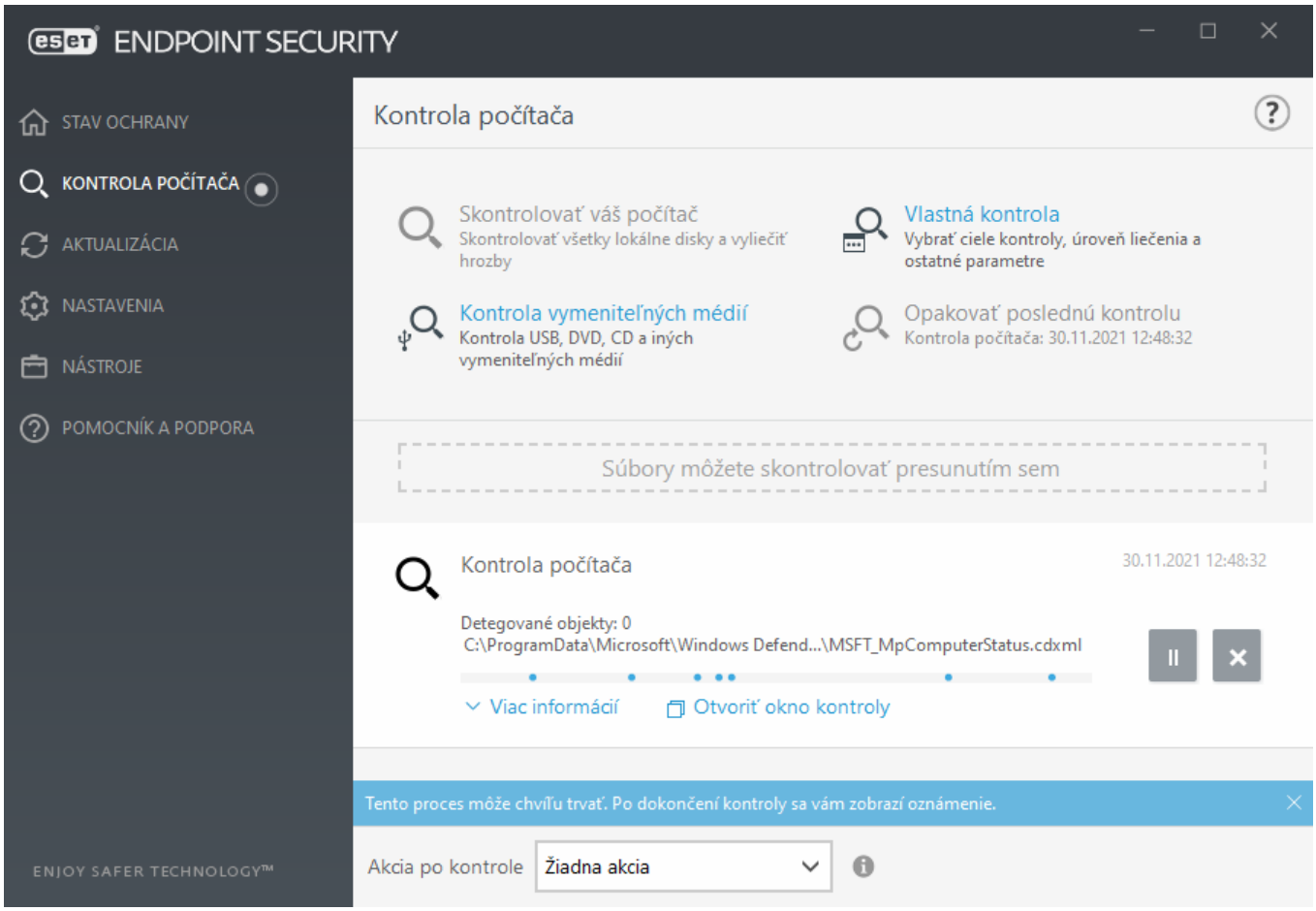
Aktivácia produktu

Po ukončení inštalácie sa zobrazí dialógové okno s výzvou na aktiváciu produktu.

Vyberte si jednu z dostupných metód aktivácie produktu ESET Endpoint Security. Viac informácií o aktivácii nájdete v kapitole Ako aktivovať ESET Endpoint Security.

Kontrola počítača

Odporúčame pravidelne spúšťať kontrolu počítača alebo si nastaviť pravidelnú kontrolu v Plánovači, aby bol váš počítač kontrolovaný na prítomnosť hrozieb na pravidelnej báze. V hlavnom okne programu kliknite na **Kontrola počítača** > **Skontrolovať váš počítač**. Podrobnejšie informácie o kontrolách počítača nájdete v kapitole Kontrola počítača.



Začíname

Táto kapitola poskytuje prvotný pohľad na ESET Endpoint Security a jeho základné nastavenia.

Používateľské rozhranie

Hlavné okno programu ESET Endpoint Security je rozdelené na dve základné časti. Časť vpravo zobrazuje informácie, ktoré podliehajú voľbe vybranej v hlavnom menu vľavo.

Hlavné menu v ľavej časti okna programu obsahuje nasledujúce položky:

Stav ochrany – v prehľadnej forme poskytne používateľovi informácie o stave ochrany počítača prostredníctvom programu ESET Endpoint Security.

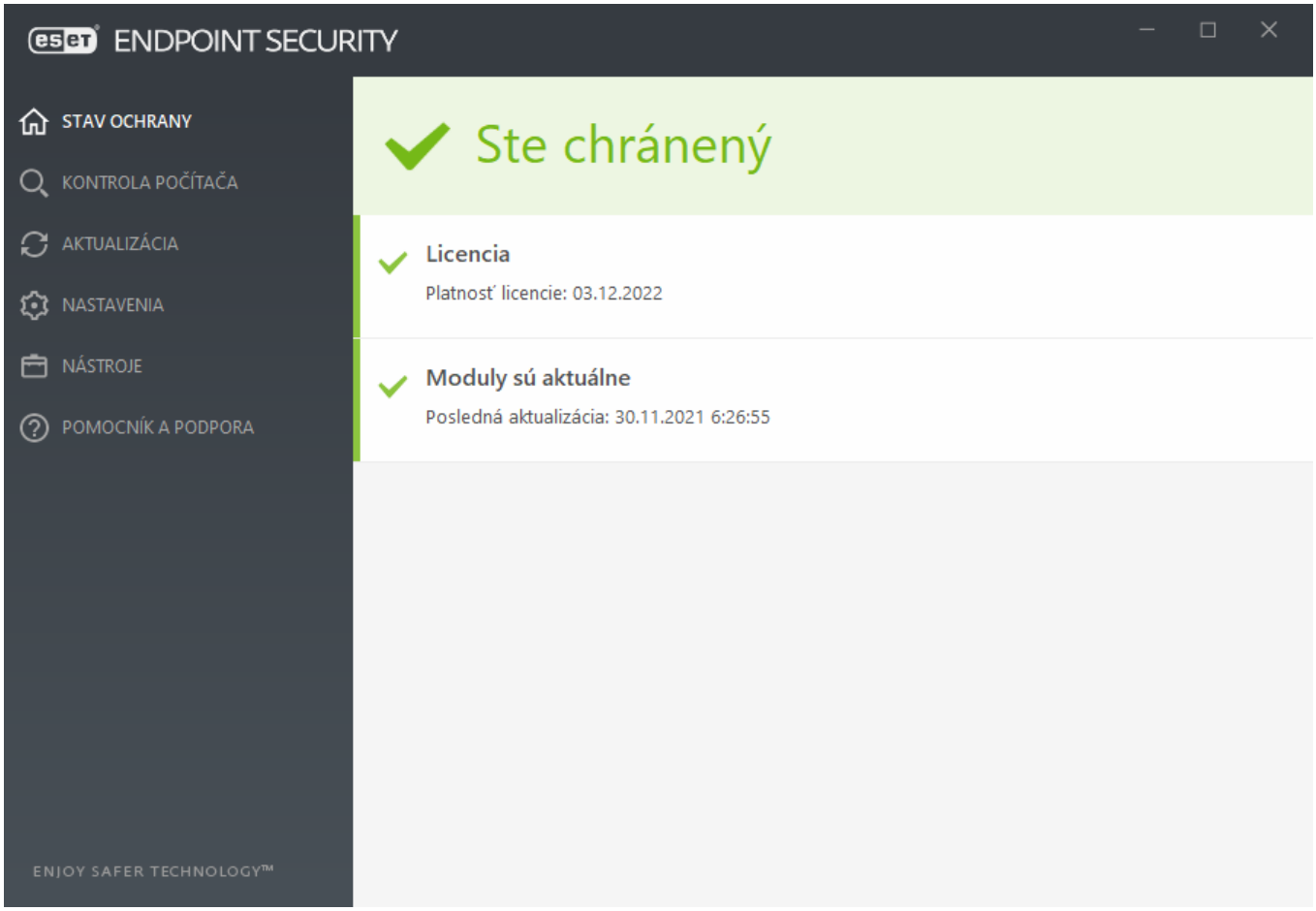
Kontrola počítača – v tejto časti môže používateľ nastaviť a spustiť kontrolu počítača, vlastnú kontrolu alebo kontrolu vymeniteľných médií. Tiež je možné zopakovať poslednú kontrolu.

Aktualizácia – zobrazuje informácie o aktuálnosti detekčného jadra a umožňuje manuálne si overiť, či nie sú dostupné nové aktualizácie.

Nastavenia – obsahuje možnosti nastavenia ochrany pre Počítač, Sieť alebo Web a e□mail.

Nástroje – poskytuje prístup k protokolom, štatistikám ochrany, sledovaniu aktivity, spusteným procesom, plánovaču, karanténe, sieťovým pripojeniam, ESET SysInspector a nástroju ESET SysRescue na vytvorenie CD alebo DVD určeného na obnovu. Môžete tiež odoslať vzorku na analýzu.

Pomocník a podpora – poskytuje prístup k stránkam pomocníka, Databáze znalostí spoločnosti ESET a webovej stránke spoločnosti ESET. Obsahuje tiež odkaz na online formulár slúžiaci na kontaktovanie technickej podpory, podporné nástroje a informácie o aktivácii produktu.

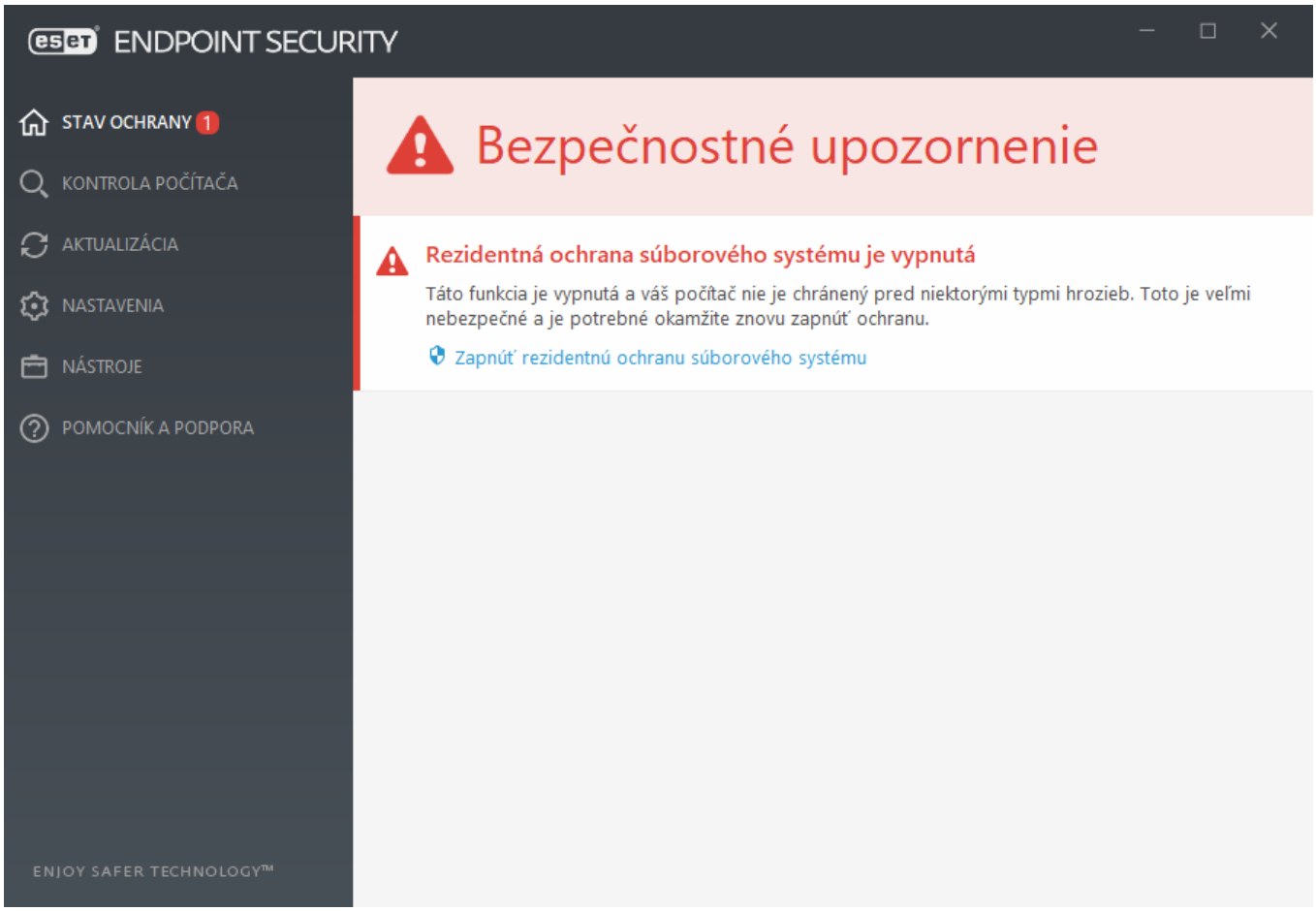


Na záložke **Stav ochrany** sú zobrazené informácie o aktuálnej úrovni ochrany vášho počítača. Zelený nápis **Maximálna ochrana** znamená, že je zaistená maximálna úroveň ochrany.

V okne stavu ochrany sa zobrazujú aj rýchle odkazy na najčastejšie používané funkcie programu ESET Endpoint Security a informácia o poslednej aktualizácii.

Čo robiť, ak program nepracuje správne?

Pri plnej funkčnosti ochrany majú jednotlivé programové moduly zelené symboly. Červený výkričník alebo oranžové oznámenie signalizuje, že modul ochrany si vyžaduje vašu pozornosť. Dodatočné informácie o module sú zobrazené vo vrchnej časti okna. Taktiež je zobrazené navrhované riešenie v prípade problému s modulom. Stav jednotlivých modulov je možné zmeniť kliknutím na **Nastavenia** v hlavnom okne a označením požadovaného modulu.



Červený výkričník (!) signalizuje, že ochrana vášho systému nie je zaručená v plnej miere. Možné príčiny sú:

- **Antivírusová a antispyvérová ochrana je pozastavená** – antivírusovú a antispyvérovú ochranu môžete opätovne aktivovať kliknutím na možnosť **Spustiť všetky moduly antivírusovej a antispyvérovej ochrany** v okne **Stav ochrany** alebo použite možnosť **Zapnúť antivírusovú a antispyvérovú ochranu** v časti **Nastavenia** v hlavnom okne programu.
- Antivírusová ochrana je nefunkčná – nepodarilo sa spustiť antivírusovú kontrolu. Väčšina modulov ESET Endpoint Security nebude fungovať správne.
- **Antiphishingová ochrana je nefunkčná** – táto funkcia nefunguje, pretože požadované programové moduly nie sú aktívne.
- **ESET Firewall je vypnutý** – tento problém je tiež signalizovaný červenou ikonou a bezpečnostným upozornením na paneli oznámení vedľa ikony siete. Kliknite na možnosť **Zapnúť režim filtrovania** pre opätovné povolenie ochrany siete.
- **Firewall sa nepodarilo spustiť** – firewall nie je aktívny pre problémy s integráciou do systému. Hneď ako to bude možné, reštartujte svoj počítač.
- **Detekčné jadro je neaktuálne** – toto chybové hlásenie sa zobrazí po niekoľkých neúspešných pokusoch o aktualizáciu detekčného jadra (predtým „vírusová databáza“). Odporúčame, aby ste skontrolovali

nastavenia aktualizácie. Najčastejším problémom sú nesprávne zadané autorizačné údaje alebo nesprávne nakonfigurované nastavenia pripojenia.

- **Produkt nie je aktivovaný** alebo **Platnosť licencie uplynula** – v tomto prípade ikona stavu ochrany zmení farbu na červenú. Po uplynutí platnosti licencie program nebude možné aktualizovať. Ak chcete licenciu obnoviť, odporúčame postupovať podľa pokynov vo výstražnom okne.
- **Systém HIPS je vypnutý** – tento problém je signalizovaný v prípade, že HIPS je deaktivovaný v Rozšírených nastaveniach. Odporúčame teda ochranu okamžite opäť povoliť kliknutím na možnosť **Zapnúť HIPS**.
- **ESET LiveGrid® je vypnutý** – tento problém je signalizovaný v prípade, že ESET LiveGrid® je v Rozšírených nastaveniach vypnutý.
- **Nie sú naplánované žiadne pravidelné aktualizácie** – ESET Endpoint Security nebude kontrolovať dostupnosť dôležitých aktualizácií ani ich prijímať, pokiaľ nenaplánujete úlohu na vykonanie aktualizácie.
- **Anti-Stealth je vypnutý** – ak chcete túto funkciu znova povoliť, kliknite na možnosť **Zapnúť Anti-Stealth**.
- **Prístup na sieť bol zablokovaný** – zobrazí sa v prípade, že pre danú pracovnú stanicu bola z ESET PROTECT spustená úloha pre klienta **Izolovať počítač od siete**. Pre viac informácií kontaktujte svojho správcu siete.
- **Rezidentná ochrana súborového systému je pozastavená** – rezidentná ochrana bola deaktivovaná používateľom. Váš počítač nie je chránený pred hrozbami. Ak chcete túto funkciu opäť povoliť, kliknite na Zapnúť rezidentnú ochranu.

 Oranžová ikona (i) signalizuje, že produkt ESET si vyžaduje vašu pozornosť, pretože sa vyskytol problém, ktorý však nie je kritický. Možné príčiny sú:

- **Ochrana prístupu na web je vypnutá** – ak chcete opätovne povoliť Ochranu prístupu na web, kliknite na bezpečnostné oznámenie a potom na **Zapnúť ochranu prístupu na web**.
- **Platnosť vašej licencie čoskoro uplynie** – v takomto prípade sa ikona stavu ochrany zmení na výkričník. Po skončení platnosti licencie nebude možné program aktualizovať a ikona stavu ochrany bude mať červenú farbu.
- **Ochrana pred botnetmi je pozastavená** – ak chcete túto funkciu opätovne povoliť, kliknite na **Zapnúť ochranu proti botnetom**.
- **Ochrana pred sieťovými útokmi (IDS) je pozastavená** – ak chcete túto funkciu opätovne povoliť, kliknite na **Zapnúť ochranu proti sieťovým útokom (IDS)**.
- **Antispamová ochrana je pozastavená** – ak chcete túto funkciu opätovne povoliť, kliknite na **Zapnúť antispamovú ochranu**.
- **Webová kontrola je pozastavená** – ak chcete túto funkciu opätovne povoliť, kliknite na **Zapnúť webovú kontrolu**.
- **Prepísanie politiky je aktívne** – konfigurácia stanovená politikou je dočasne prepísaná, pravdepodobne kým sa nevyriešia problémy. Prepísať politiku môže len používateľ, ktorý má na to dostatočné oprávnenia. Viac informácií nájdete v kapitole Ako používať Režim prepísania.
- **Správa zariadení je pozastavená** – ak chcete túto funkciu opätovne povoliť, kliknite na **Zapnúť správu zariadení**.

Ak chcete nastaviť, ktoré stavy ochrany sa majú zobrazovať priamo v produkte ESET Endpoint Security, prečítajte si kapitolu Stavy aplikácie.

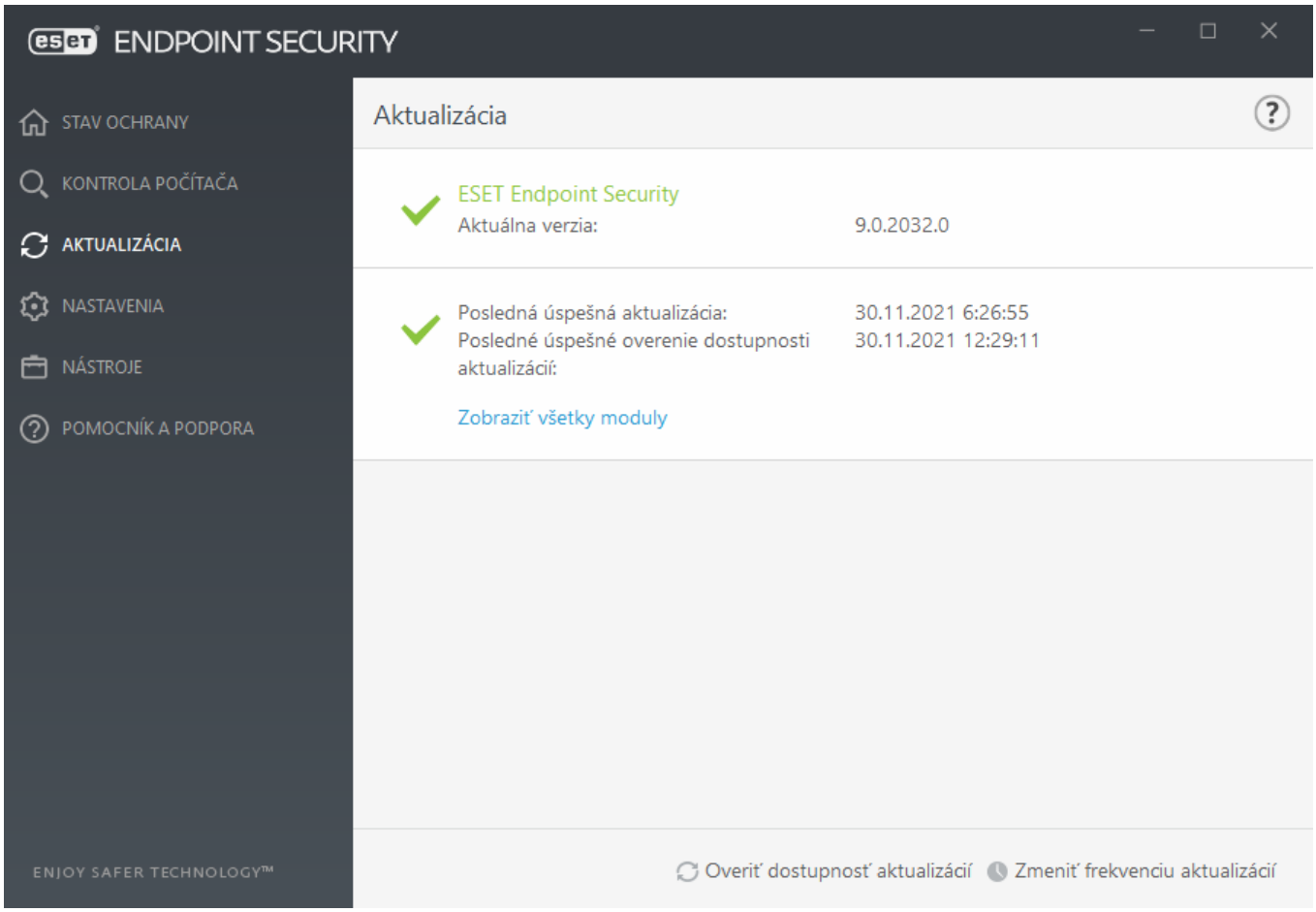
Ak sa vám nepodarí problém vyriešiť pomocou navrhnutých riešení, je potrebné použiť časť **Pomocník a podpora** alebo vyhľadať informácie o danom probléme v Databáze znalostí spoločnosti ESET. Ak aj napriek tomu potrebujete pomoc, môžete kontaktovať technickú podporu spoločnosti ESET. Špecialisti technickej podpory spoločnosti ESET reagujú na problémy rýchlo a efektívne vám pomôžu s riešením vášho problému.

Ak stav súvisí s funkciou, ktorá je blokovaná politikou nástroja ESET PROTECT, odkaz nebude funkčný (nebude dostupný).

Nastavenie aktualizácií

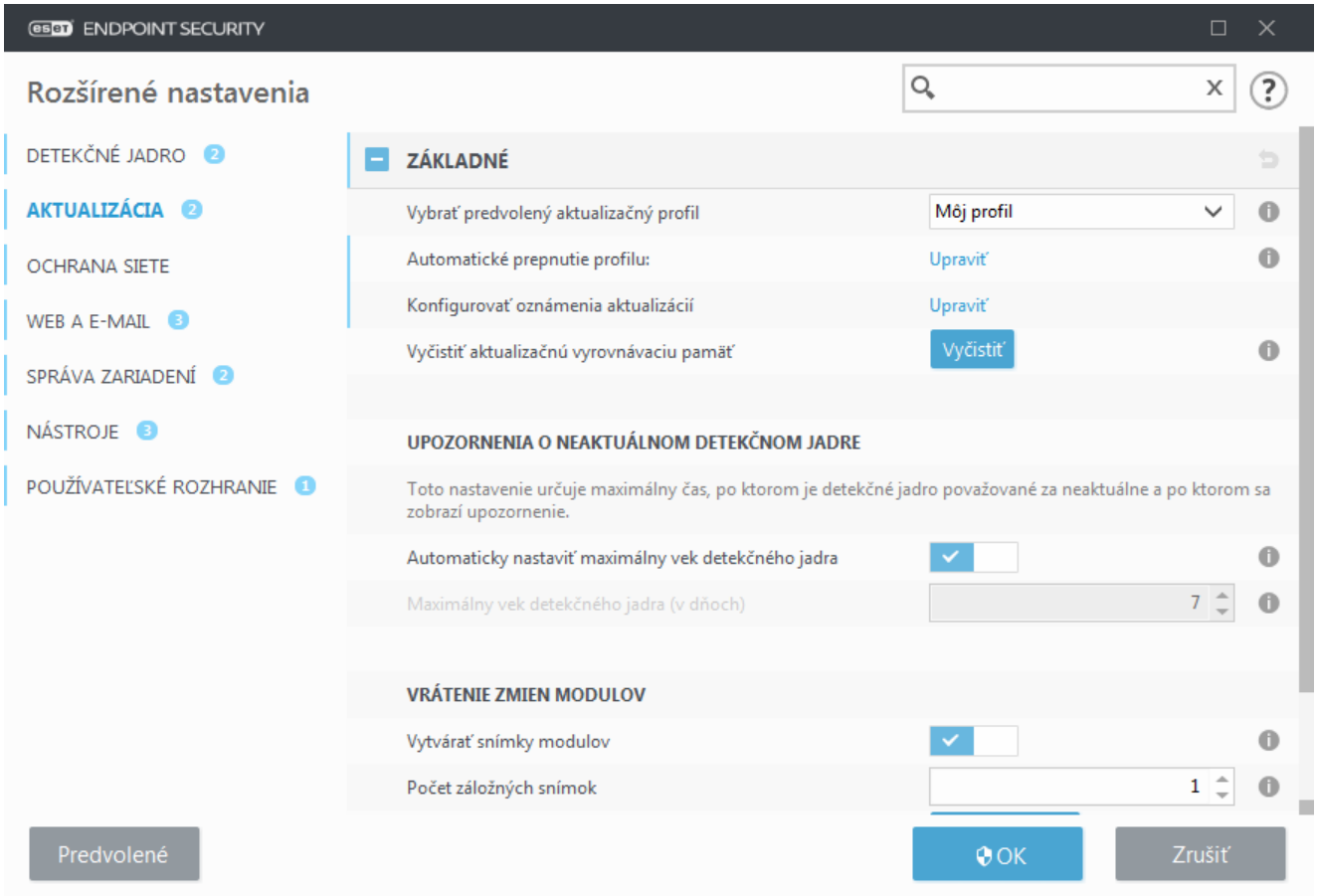
Aktualizovanie programových modulov je z pohľadu zaistenia komplexnej ochrany pred škodlivým kódom nevyhnutnosťou. Nastaveniu a priebehu aktualizácií preto treba venovať zvýšenú pozornosť. Pre skontrolovanie dostupnosti novej aktualizácie modulov kliknite v hlavnom okne programu na záložku **Aktualizácia** a následne na možnosť **Overiť dostupnosť aktualizácií**.

Ak do programu ešte nebol zadaný **licenčný kľúč**, k aktivácii vášho produktu budete vyzvaný práve teraz. Pokým nebude program aktivovaný, nebudú sa môcť sťahovať aktualizácie modulov.



Rozšírené nastavenia (prejdite do sekcie **Nastavenia** v hlavnom okne programu a kliknite na **Rozšírené nastavenia** alebo stlačte **F5** na klávesnici) obsahujú rozšírené nastavenia aktualizácií. Pre konfiguráciu rozšírených nastavení aktualizácií, ako je napríklad režim aktualizácie, prístup na proxy server, nastavenie LAN pripojenia a vytvárania kópie detekčného jadra, kliknite v okne Rozšírených nastavení na kartu **Aktualizácia**.

- V prípade problémov s aktualizovaním produktu kliknite na tlačidlo **Vyčistiť** a vyčistite vyrovnávaciu pamäť s dočasnými aktualizačnými súbormi.



- Predvolene ja zapnutá možnosť **Automatický výber servera** v sekcii **Profily** > **Aktualizácie** > **Aktualizácie modulov**. Ak pre získavanie aktualizácií produktu využívate aktualizačný server spoločnosti ESET, odporúčame vám ponechať túto možnosť aktívnu.
- Ak si neprajete, aby sa vám v pravom dolnom rohu obrazovky zobrazovali oznámenia o úspešnej aktualizácii produktu, rozbaľte sekciu **Profily** > **Aktualizácie**, kliknite na možnosť **Upraviť** vedľa popisu **Vyberte prichádzajúce aktualizačné upozornenia** a následne zrušte označenie pre typ upozornenia **Detekčné jadro bolo úspešne aktualizované**.

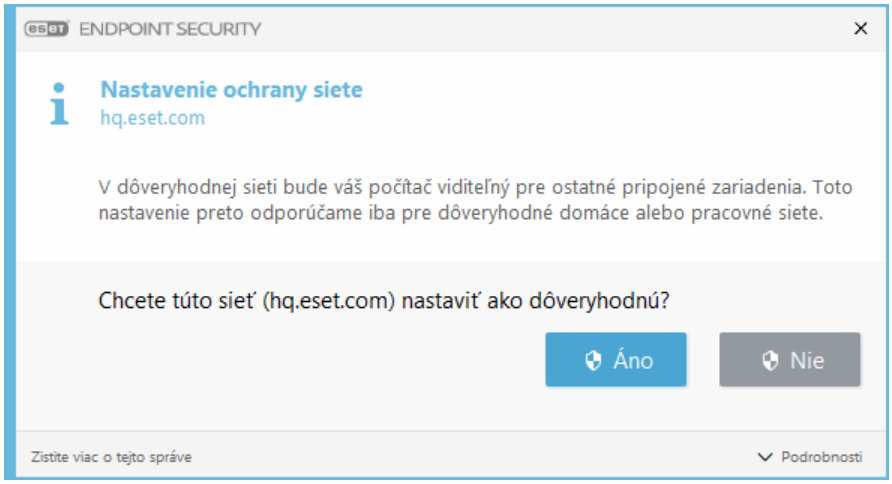
Pre úplnú funkčnosť programu je dôležité, aby bol pravidelne aktualizovaný. To však nie je možné bez zadaného **Licenčného kľúča** v sekcii **Pomocník a podpora** > **Aktivovať produkt**.

Ak ste nezadali **Licenčný kľúč** hneď po inštalácii, môžete tak spraviť aj neskôr. Podrobnejšie informácie o aktivácii nájdete v časti Ako aktivovať ESET Endpoint Security. Na aktiváciu programu je potrebné do príslušného okna zadať **licenčné údaje**, ktoré ste obdržali po zakúpení bezpečnostného produktu ESET.

Nastavenie zón

Pre ochranu počítača v sieti je potrebné nastaviť dôveryhodné zóny. Zadaním dôveryhodnej zóny umožníte zdieľanie a sprístupníte počítač iným používateľom v danej sieti. Nastavenia týkajúce sa dôveryhodných zón nájdete v **Rozšírených nastaveniach** (F5) > **Ochrana siete** > **Firewall** > **Pokročilé** > **Zóny**.

Automatická detekcia dôveryhodnej zóny sa vykoná po nainštalovaní programu ESET Endpoint Security alebo keď sa váš počítač pripojí k novej sieti. Vo väčšine prípadov preto nie je potrebné dodatočne tieto zóny definovať. Pri detekcii novej zóny je štandardne zobrazený dialóg s možnosťou definovania úrovne ochrany v tejto zóne.



Nesprávnym nastavením dôveryhodnej zóny vystavujete počítač potenciálnemu bezpečnostnému riziku.

Počítačom z dôveryhodnej zóny je predvolene povolený prístup k zdieľaným súborom a tlačiarňam, povolená prichádzajúca RPC komunikácia a dostupná služba zdieľania pracovnej plochy.

Podrobnejšie informácie o tejto funkcii nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET:

- Program ESET Endpoint Security zachytil nové sieťové pripojenie

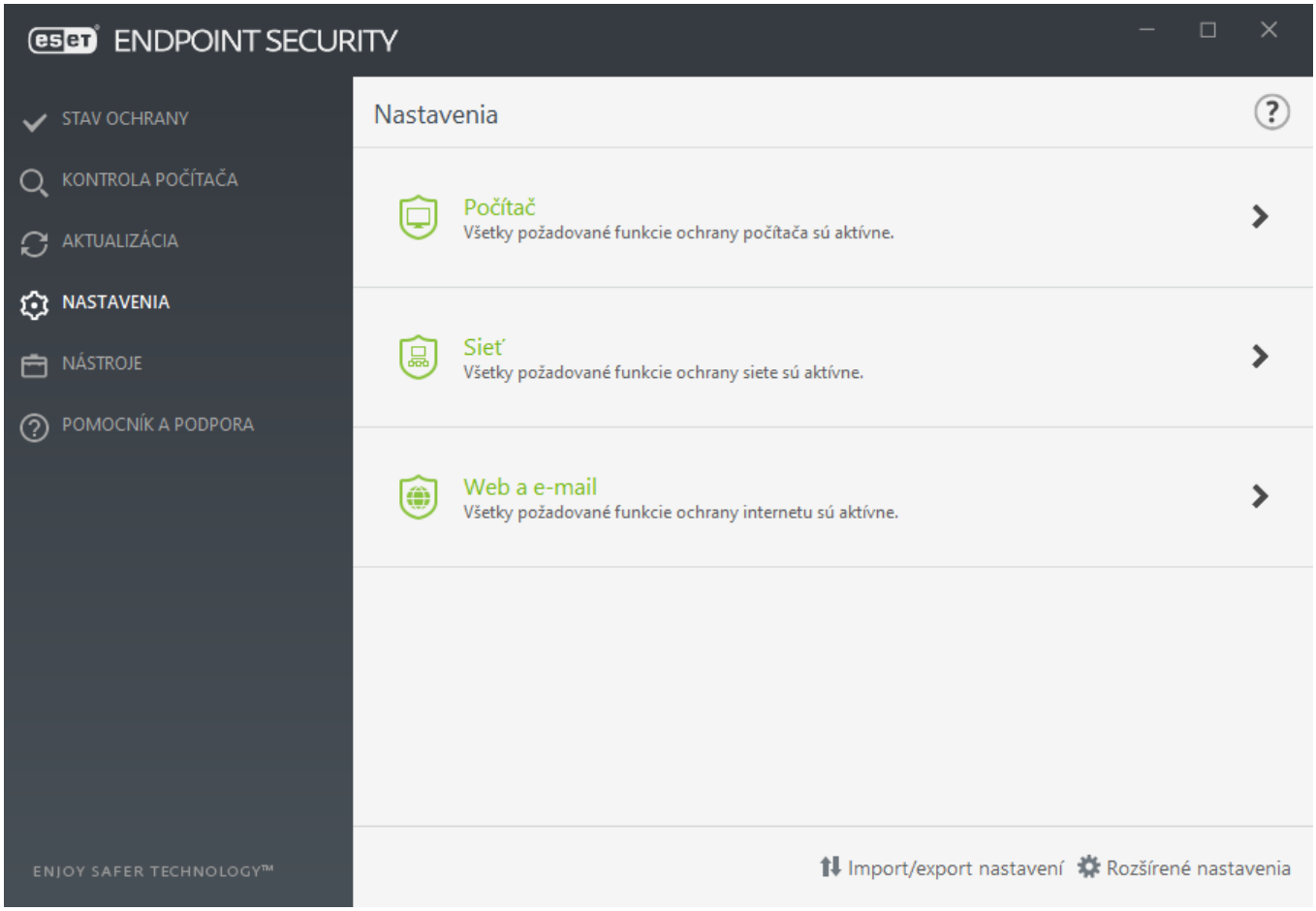
Nástroje webovej kontroly

Ak ste už aktivovali webovú kontrolu v programe ESET Endpoint Security, je potrebné ju ešte nastaviť pre používateľské účty, aby kontrola mohla fungovať správne. V kapitole Webová kontrola nájdete postup na vytvorenie špecifických pravidiel na ochranu pracovných staníc pred potenciálne nebezpečným alebo citlivým či neslušným obsahom.

Práca s programom ESET Endpoint Security

ESET Endpoint Security vám umožňuje nastaviť úroveň ochrany pre váš počítač, web, e-mail a sieť.

Pri vytváraní politiky z ESET PROTECT Web Console môžete určiť príznak pre každé nastavenie. Nastavenie s príznakom Vynútiť má vyššiu prioritu, čiže nemôže byť zmenené inou politikou (ani v prípade, že neskoršia politika má tiež príznak Vynútiť). Týmto bude zaručené, že nastavenie nebude zmenené (napr. používateľom alebo neskoršími politikami pri zlučovaní). Viac informácií nájdete v kapitole Online pomocníka o príznakoch v konzole ESET PROTECT.



Sekcia **Nastavenia** obsahuje nasledujúce časti:

- **Počítač**
- **Sieť**
- **Web a e-mail**

Sekcia Počítač obsahuje nasledujúce programové súčasti, ktoré môžete zapnúť alebo vypnúť:

- **Rezidentná ochrana súborového systému** – všetky súbory, ktoré sa v počítači otvárajú, vytvárajú a spúšťajú, sú kontrolované na prítomnosť škodlivého kódu.
- **Správa zariadení** – poskytuje automatickú správu zariadení (CD/DVD/USB/...). Tento modul umožňuje blokovať a nastaviť rozšírené prístupové práva a pravidlá na filtrovanie prístupu k zariadeniu.
- **Host Intrusion Prevention System (HIPS)** – HIPS monitoruje udalosti v operačnom systéme a reaguje na ne na základe stanovených pravidiel.
- **Pokročilá kontrola pamäte** – spolu s funkciou Exploit Blocker poskytuje lepšiu ochranu pred malvérom, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu bezpečnostných produktov. Pokročilá kontrola pamäte je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa dočítate v slovníku pojmov.
- **Exploit Blocker** – je navrhnutý na ochranu najčastejšie zneužívaných aplikácií, ako napríklad webových prehliadačov, softvéru na zobrazovanie PDF dokumentov, e-mailových klientov a komponentov MS Office. Exploit Blocker je v predvolených nastaveniach zapnutý. Viac o tomto type ochrany sa dočítate v slovníku pojmov.
- **Ransomware Shield** – predstavuje dodatočnú vrstvu ochrany zahrnutú v rámci funkcie HIPS. Aby mohol Ransomware Shield fungovať, je potrebné mať povolený systém ESET LiveGrid®. Viac o tomto type ochrany sa môžete dočítať tu.

- **Prezentačný režim** – funkcia určená pre používateľov, ktorí potrebujú neprerušovane používať svoj softvér a neželajú si byť vyrušovaní oznámeniami a dialógovými oknami, pričom taktiež požadujú minimálne vyťaženie procesora antivírusom. Po zapnutí prezentačného režimu sa zobrazí varovanie (potenciálne bezpečnostné riziko) a hlavné okno programu zmení farbu na oranžovú.

Sekcia **Sieť** umožňuje upraviť nastavenia pre Firewall, Ochranu pred sieťovými útokmi (IDS) a Ochranu pred botnetmi.

Sekcia **Web a e□mail** vám umožňuje nastaviť nasledujúce programové súčasti:

- **Zabezpečený prehliadač** – chráni vaše citlivé údaje pri surfovaní na internete (napríklad platobné údaje pri online transakciách).
- **Webová kontrola** – umožňuje vám blokovať webové stránky, ktoré môžu obsahovať potenciálne nežiaduci obsah. Okrem toho môže správca zakázať prístup na 27 predvolených kategórií web stránok.
- **Ochrana prístupu na web** – ak je zapnutá, všetka komunikácia cez HTTP alebo HTTPS je kontrolovaná na prítomnosť škodlivého kódu.
- **Ochrana e□mailových klientov** – zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3 a IMAP.
- **Antispamová ochrana** – kontroluje prítomnosť nevyžiadanej pošty.
- **Antiphishingová ochrana** – filtruje obsah webových stránok podozrivých z distribúcie obsahu určeného na manipuláciu používateľov, aby poskytli svoje osobné údaje (napr. heslá, bankové údaje atď.).

Ak chcete dočasne vypnúť jednotlivé moduly, kliknite na zelené tlačidlo vedľa príslušného modulu. Pozastavením ochrany vystavujete systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného komponentu kliknite na červené tlačidlo.

Ak je politika aplikovaná cez ESET PROTECT, vedľa príslušného komponentu uvidíte ikonu zámku. Politika aplikovaná cez ESET PROTECT môže byť prepísaná lokálne po overení prihláseným používateľom (napr. správcom). Viac informácií nájdete v Online pomocníkovi pre ESET PROTECT.

Ochrana pozastavená týmto spôsobom sa po reštarte znova zapne.

Ak chcete zobraziť podrobné nastavenia konkrétneho bezpečnostného komponentu, kliknite na ozubené koleso vedľa ktoréhokoľvek komponentu.

V dolnej časti okna sa nachádzajú dodatočné možnosti. Ak chcete načítať nastavenia zo súboru *.xml* alebo uložiť nastavenia do súboru, kliknite na možnosť **Import/export nastavení**. Viac informácií nájdete v kapitole Import a export nastavení.

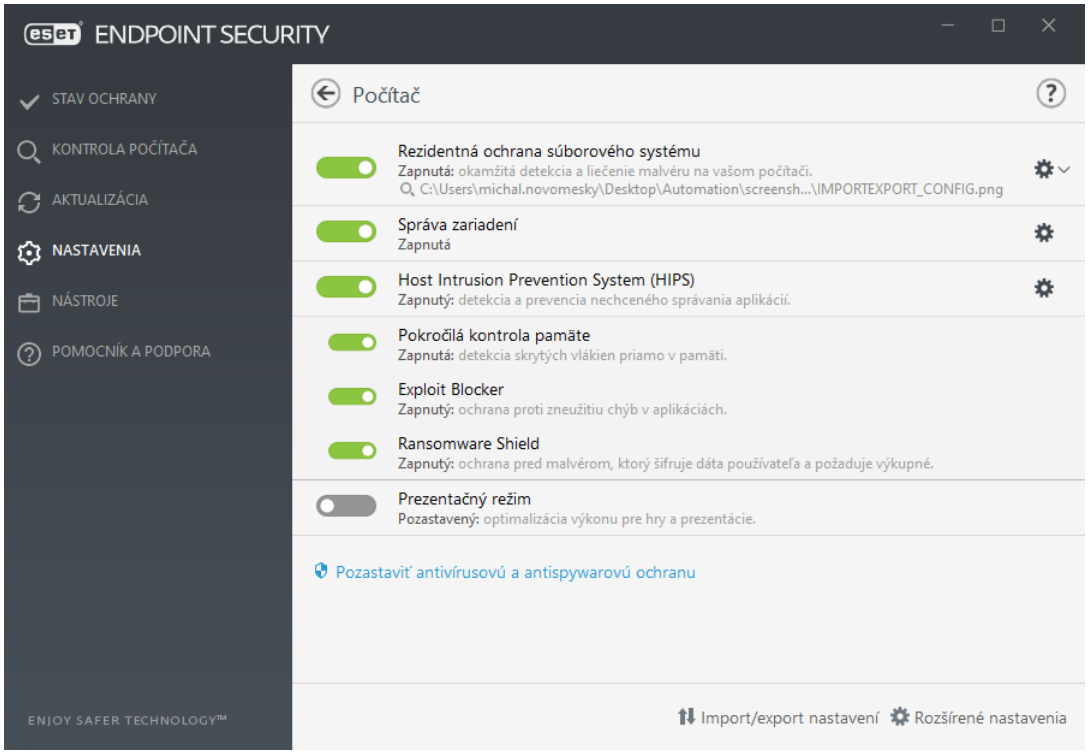
Podrobnejšie nastavenia zobrazíte kliknutím na **Rozšírené nastavenia** alebo stlačením klávesu **F5**.

Počítač

Modul **Počítač** sa nachádza v hlavnom okne programu v sekcii **Nastavenia** > **Počítač**. Zobrazuje prehľad modulov ochrany, o ktorých sa môžete dočítať viac v predchádzajúcej kapitole. V tejto sekcii sú dostupné tieto nastavenia:

Kliknite na ozubené koleso vedľa položky **Rezidentná ochrana súborového systému** a následne kliknite na možnosť **Nastaviť vylúčenia** pre otvorenie nastavení pre Vylúčenia, kde môžete vylúčiť z kontroly konkrétne súbory a priečinky. Ak chcete otvoriť rozšírené nastavenia **Rezidentnej ochrany súborového systému**, kliknite na

Konfigurovať.



Sekcia **Počítač** obsahuje nasledujúce programové súčasti, ktoré môžete zapnúť alebo vypnúť:

- **Rezidentná ochrana súborového systému** – všetky súbory, ktoré sa v počítači otvárajú, vytvárajú a spúšťajú, sú kontrolované na prítomnosť škodlivého kódu.
- **Správa zariadení** – poskytuje automatickú správu zariadení (CD/DVD/USB/...). Tento modul umožňuje blokovať a nastaviť rozšírené prístupové práva a pravidlá na filtrovanie prístupu k zariadeniu.
- **Host Intrusion Prevention System (HIPS)** – HIPS monitoruje udalosti v operačnom systéme a reaguje na ne na základe stanovených pravidiel.
- **Pokročilá kontrola pamäte** – spolu s funkciou Exploit Blocker poskytuje lepšiu ochranu pred malvérom, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu bezpečnostných produktov. Pokročilá kontrola pamäte je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa dočítate v slovníku pojmov.
- **Exploit Blocker** – je navrhnutý na ochranu najčastejšie zneužívaných aplikácií, ako napríklad webových prehliadačov, softvéru na zobrazovanie PDF dokumentov, e-mailových klientov a komponentov MS Office. Exploit Blocker je v predvolených nastaveniach zapnutý. Viac o tomto type ochrany sa dočítate v slovníku pojmov.
- **Ransomware Shield** – predstavuje dodatočnú vrstvu ochrany zahrnutú v rámci funkcie HIPS. Aby mohol Ransomware Shield fungovať, je potrebné mať povolený systém ESET LiveGrid®. Viac o tomto type ochrany sa môžete dočítať tu.
- **Prezentačný režim** – funkcia určená pre používateľov, ktorí potrebujú neprerušovane používať svoj softvér a neželajú si byť vyrušovaní oznámeniami a dialógovými oknami, pričom taktiež požadujú minimálne vyťaženie procesora antivírusom. Po zapnutí prezentačného režimu sa zobrazí varovanie (potenciálne bezpečnostné riziko) a hlavné okno programu zmení farbu na oranžovú.

Pozastaviť antivírusovú a antispyvérovú ochranu – z roletového menu vyberte časové obdobie, na ktoré chcete pozastaviť ochranu, a následne kliknite na **Použiť** pre potvrdenie akcie. Pre opätovné zapnutie pozastavenej ochrany kliknite na možnosť **Zapnúť antivírusovú a antispyvérovú ochranu**.

Detekčné jadro

Detekčné jadro chráni pred nebezpečnými útokmi na systém tým, že kontroluje súbory, e-maily a internetovú komunikáciu. Napríklad, ak zachytí objekt klasifikovaný ako malvér, začne sa proces nápravy. Detekčné jadro môže objekt eliminovať jeho zablokovaním a následným vyliečením, odstránením alebo presunutím do karantény.

Ak chcete konfigurovať nastavenia detekčného jadra, kliknite na možnosť **Rozšírené nastavenia** alebo stlačte kláves **F5**.

V tejto kapitole nájdete nasledujúce témy:

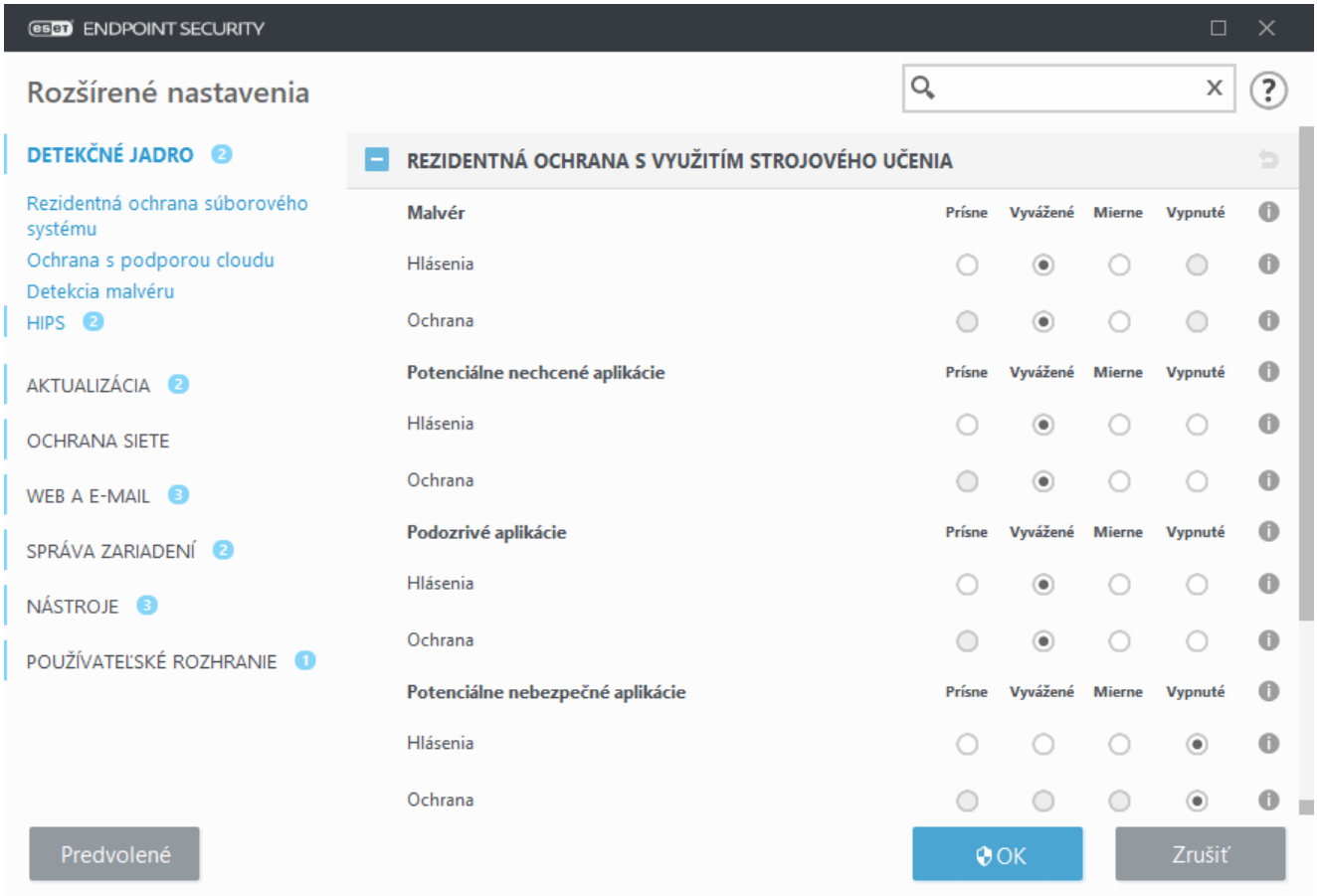
- Rezidentná ochrana s využitím strojového učenia a jej kategórie
- Detekcia malvéru
- Nastavenie hlásení
- Nastavenie ochrany
- Odporúčané postupy

> Počnúc verziou 7.2 sa v sekcii nastavení detekčného jadra už viac nepoužíva zapínanie/vypínanie pomocou prepínača ako vo verzii 7.1 a starších. Prepínacie tlačidlá sú nahradené štyrmi úrovňami nastavenia – „prísne“, „vyvážené“, „mierne“ a „vypnuté“.

Rezidentná ochrana s využitím strojového učenia a jej kategórie

Rezidentná ochrana s využitím strojového učenia pre všetky moduly ochrany (napr. Rezidentná ochrana súborového systému, Ochrana prístupu na web atď.) vám umožňuje nastaviť úroveň hlásenia a ochrany nasledujúcich kategórií:

- **Malvér** – počítačový vírus je škodlivý kód pripojený k existujúcim súborom na počítači. Termín „vírus“ sa však často používa nesprávne. Presnejším výrazom je „malvér“ (škodlivý softvér). Detekciu malvéru zabezpečuje modul detekčného jadra v kombinácii s komponentom strojového učenia.
  Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.
- **Potenciálne nechcené aplikácie** – grayware alebo tiež potenciálne nechcená aplikácia (PUA) je označenie pre širokú škálu softvéru, ktorý nie je jednoznačne škodlivý ako iné druhy malvéru, napríklad vírusy alebo trójske kone. Môže však na váš počítač nainštalovať ďalší nežiaduci softvér, zmeniť správanie zariadenia, vykonávať neočakávané operácie, prípadne akcie bez súhlasu používateľa.
  Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.
- **Potenciálne nebezpečné aplikácie** – predstavujú v prevažnej miere komerčný a legitímny softvér, avšak v nesprávnych rukách môže dôjsť k jeho zneužitiu na nekalé účely. Medzi potenciálne nebezpečné aplikácie môžeme zaradiť nástroje vzdialeného prístupu, nástroje na prelomenie hesiel a keyloggery (programy zapisujúce každé stlačenie klávesu používateľom).
  Prečítajte si viac o týchto typoch aplikácií v slovníku pojmov.
- **Podozrivé aplikácie** predstavujú programy komprimované packermi alebo protektormi. Autori malvéru tieto typy nástrojov často zneužívajú na zmarenie detekcie.



Pokročilé strojové učenie je teraz súčasťou detekčného jadra, pričom funguje ako pokročilá vrstva ochrany vylepšujúca detekciu na základe strojového učenia. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Detekcia malvéru

Nastavenia kontroly je možné nakonfigurovať samostatne pre rezidentnú ochranu a manuálnu kontrolu. Na základe predvolených nastavení je povolená možnosť **Použiť nastavenia rezidentnej ochrany**. Ak je táto možnosť povolená, príslušné nastavenia manuálnej kontroly sú prevzaté zo sekcie **Rezidentná ochrana s využitím strojového učenia**.

Nastavenie hlásení

Ak dôjde k detekcii (napr. sa nájde hrozba, ktorá je klasifikovaná ako malvér), informácie sa zaznamenajú do protokolu Detekcie a zobrazia sa Oznámenia na ploche v prípade, že sú nakonfigurované v programe ESET Endpoint Security.

Úroveň hlásenia sa nastavuje zvlášť pre každú kategóriu (ďalej len „KATEGÓRIA"):

1. Malvér
2. Potenciálne nechcené aplikácie
3. Potenciálne nebezpečné aplikácie
4. Podozrivé aplikácie

Pri hláseniach detegovaných objektov sa využíva detekčné jadro vrátane komponentu strojového učenia. V prípade hlásení pritom môžete nastaviť vyššiu úroveň (prah) ako pri ochrane. Tieto nastavenia hlásení neovplyvnia blokovanie, liečenie ani odstraňovanie objektov.

Pred zmenou prahu (úrovne) hlásenia pre jednotlivé KATEGÓRIE si prečítajte nasledujúce informácie:

Úroveň nastavenia (zvolený prah)	Vysvetlenie
Prísne	Hlásenia danej KATEGÓRIE sú nakonfigurované na maximálnu citlivosť. Je preto hlásený väčší počet detekcií. **Prísne** nastavenie môže objekty nesprávne identifikovať ako objekt danej KATEGÓRIE.
Vyvážené	Hlásenia danej KATEGÓRIE sú nakonfigurované ako vyvážené. Toto nastavenie je optimalizované pre dosiahnutie vyváženého pomeru medzi výkonom a presnosťou detekcie a počtom nesprávne identifikovaných objektov.
Mierne	Hlásenia danej KATEGÓRIE sú nakonfigurované tak, aby sa minimalizovali nesprávne identifikované objekty pri súčasnom zachovaní dostatočnej úrovne ochrany. Objekty sú hlásené iba v prípade vysokej pravdepodobnosti a zhody so správaním charakteristickým pre danú KATEGÓRIU.
Vypnuté	Hlásenia danej KATEGÓRIE nie sú aktívne a detekcie tohto typu nie sú zachytávané, hlásené ani liečené. Toto nastavenie preto vyvolá vypnutie ochrany pred daným typom detekcie. Úroveň „Vypnuté“ nie je dostupná pre hlásenia malvéru a zároveň je to predvolená hodnota pre kategóriu potenciálne nebezpečných aplikácií.

Dostupnosť modulov ochrany programu ESET Endpoint Security

Nasledujúca tabuľka zobrazuje dostupnosť (povolené alebo zakázané) daného modulu ochrany pre zvolený prah v rámci KATEGÓRIE:

	Prísne	Vyvážené	Mierne	Vypnuté**
Modul pokročilého strojového učenia*	✓ (prísny režim)	✓ (konzervatívny režim)	X	X
Modul detekčného jadra	✔	✔	✔	X
Iné moduly ochrany	✔	✔	✔	X

* Dostupné v programe ESET Endpoint Security vo verzii 7.2 a novších.
** Neodporúča sa.

Zistite verziu svojho produktu, verzie programových modulov a dátumy vydania

1. Kliknite na **Pomocník a podpora** > **O ESET Endpoint Security**.
2. Na obrazovke s názvom **O programe** sa v prvom riadku textu zobrazuje číslo verzie vášho bezpečnostného produktu ESET.
3. Kliknite na tlačidlo **Zobraziť moduly**, ak si chcete zobraziť informácie o konkrétnych moduloch.

Dôležité poznámky

Pokiaľ ide o nastavenie vhodnej úrovne (prahu) hlásenia a ochrany pre vaše prostredie, tu je ešte niekoľko dôležitých poznámok:

- **Vyvážené** nastavenie sa odporúča pre väčšinu situácií.
- **Mierne** nastavenie predstavuje porovnateľnú úroveň ochrany s predchádzajúcimi verziami ESET Endpoint Security (7.1 a nižšie). Táto možnosť sa odporúča pre prostredia, kde je prioritou minimalizovať počet nesprávne identifikovaných objektov bezpečnostným softvérom.
- Čím vyšší prah hlásenia zvolíte, tým vyššia bude úspešnosť detekcie, ale zároveň sa zvýši aj možnosť výskytu nesprávne identifikovaných objektov.
- Vzhľadom na dynamiku hrozieb v reálnom prostredí nie je možné zaručiť 100 % úspešnosť detekcie a rovnako ani 0 % možnosť nesprávnych kategorizácií bezpečných objektov ako malvér.
- Udržujte program ESET Endpoint Security a jeho moduly v aktuálnom stave, aby ste tak dosiahli čo najlepší balans medzi výkonnosťou a presnosťou detekcie a počtom nesprávne identifikovaných objektov.

Nastavenie ochrany

V prípade, že je zachytený objekt klasifikovaný ako KATEGÓRIA, program daný objekt zablokuje a následne ho vylieči, odstráni alebo presunie do karantény.

Pred zmenou prahu (úrovne) ochrany pre jednotlivé KATEGÓRIE si prečítajte nasledujúce informácie:

Úroveň nastavenia (zvolený prah)	Vysvetlenie
Prísne	Detekcie zachytené pri prísnej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu). Toto nastavenie sa odporúča, keď všetky koncové zariadenia prešli kontrolou pri prísnej úrovni nastavenia a nesprávne detegované objekty boli pridané do vylúčení detekcií.
Vyvážené	Detekcie zachytené pri vyváženej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).
Mierne	Detekcie zachytené pri miernej úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).
Vypnuté	Toto nastavenie je užitočné pre identifikáciu a vylúčenie nesprávne detegovaných objektov. Úroveň „Vypnuté“ nie je dostupná pre ochranu pred malvérom a zároveň je to predvolená hodnota pre kategóriu potenciálne nebezpečných aplikácií.

Konverzia ESET PROTECT politiky pre ESET Endpoint Security 7.1 a nižšie verzie

Editor politík v nástroji ESET PROTECT, ktoré slúžia na konfiguráciu kontroly, už viac neobsahuje prepínacie tlačidlá pre zapínanie/vypínanie pre jednotlivé KATEGÓRIE. Nasledujúca tabuľka ukazuje konverziu medzi prahom ochrany a konečným stavom prepínača v ESET Endpoint Security 7.1 a nižších verziách.

Nastavený prah pre KATEGÓRIU	Prísne	Vyvážené	Mierne	Vypnuté
Použitý stav prepínača pre KATEGÓRIU	✓	✓	✓	✗

Ak aktualizujete produkt z verzie 7.1 alebo nižších na verziu 7.2 alebo vyššie, nastavenie bude po aktualizácii vyzerať nasledovne:

Stav prepínača pre KATEGÓRIU pred aktualizáciou	✓	✗
Nastavený prah pre KATEGÓRIU po aktualizácii	Vyvážené	Vypnuté

Odporúčané postupy

NESPRAVOVANÉ PROSTREDIE (jednotlivé klientske pracovné stanice)

Odporúčame vám ponechať predvolené nastavenia nezmenené.

SPRAVOVANÉ PROSTREDIE

Tieto nastavenia sa zvyčajne aplikujú na pracovné stanice prostredníctvom politiky.

1. Počiatočná fáza

Táto fáza môže trvať aj týždeň.

- Pre všetky kategórie nastavte **hlásenia** na prahovú úroveň **Vyvážené**.
  POZNÁMKA: V prípade potreby použite **Prísne** nastavenie.
- Nastavte alebo ponechajte **ochranu** pred malvérom na úrovni **Vyvážené**.
- Nastavte **ochranu** pre ostatné KATEGÓRIE na úroveň **Mierne**.
  POZNÁMKA: V tejto fáze sa neodporúča nastavovať **ochranu** na úroveň **Prísne**, pretože liečenie by prebehlo na všetkých nájdených detekciách vrátane tých, ktoré boli nesprávne identifikované.
- Vyhľadajte nesprávne identifikované objekty v protokole Detekcie a pridajte ich medzi Vylúčenia detekcií.

2. Prechodná fáza

- „Produkčnú fázu“ najskôr v rámci testovania implementujte len na niektoré z pracovných staníc (nie na všetky pracovné stanice v sieti).

3. Produkčná fáza

- Pre všetky kategórie nastavte **ochranu** na prahovú úroveň **Vyvážené**.
- Ak ESET Endpoint Security na pracovných staniciach spravujete vzdialene, použite vhodnú preddefinovanú politiku s nastaveniami antivírusu.
- **Prísnu** úroveň ochrany nastavte v prípade, že vyžadujete najvyššiu úspešnosť detekcie, no zároveň pripúšťate výskyt nesprávne identifikovaných objektov.
- Skontrolujte protokol detekcie alebo ESET PROTECT reporty pre prípadné chýbajúce detekcie.

Detekčné jadro – pokročilé možnosti

Technológia Anti-Stealth je dômyselný systém určený na detekciu nebezpečných programov, akými sú napríklad rootkity, ktoré sú po aktivácii neviditeľné pre operačný systém a iné aplikácie vrátane antivírusových programov. Z tohto dôvodu ich nie je možné detegovať pomocou bežných techník kontroly.

Zapnúť rozšírenú kontrolu prostredníctvom AMSI – nástroj Microsoft Antimalware Scan Interface umožňuje vývojárom aplikácií vytvárať nové metódy ochrany pred malvérom (platí pre Windows 10 a 11).

Našla sa infiltrácia

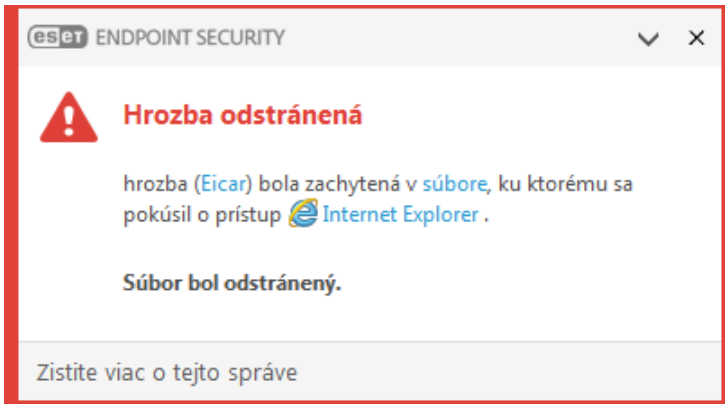
Infiltrácie sa môžu do systému dostať z rôznych zdrojov: z webových stránok, zo zdieľaných priečinkov, prostredníctvom e-mailu alebo z vymeniteľných médií (USB kľúče, externé disky, CD, DVD a pod.).

Štandardné správanie

V programe ESET Endpoint Security môžu byť infiltrácie zachytené pomocou nasledujúcich modulov:

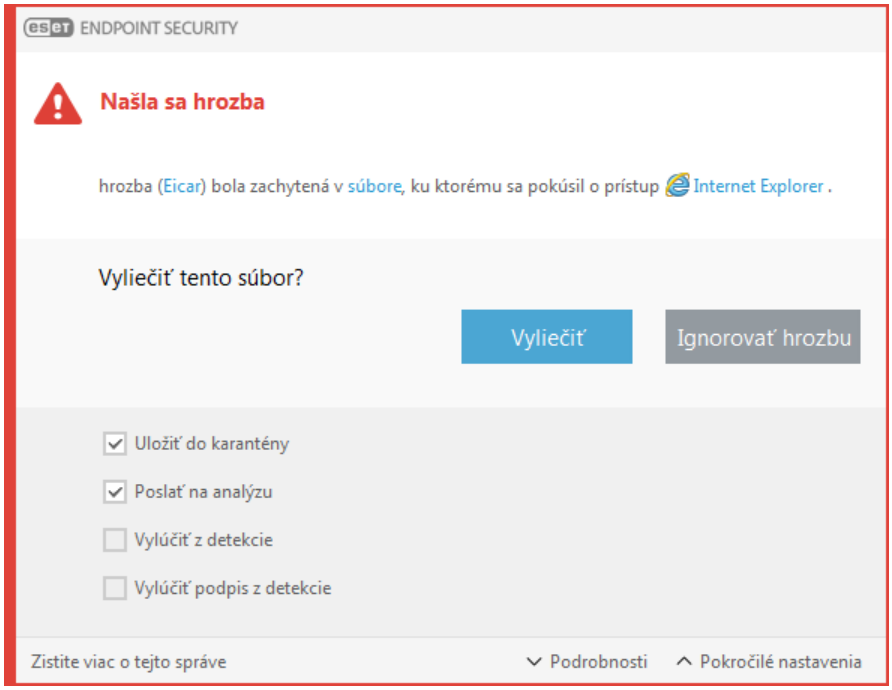
- Rezidentná ochrana súborového systému
- Ochrana prístupu na web
- Ochrana e-mailových klientov
- Manuálna kontrola počítača

Každý z týchto modulov používa prednastavenú úroveň liečenia a pokúsi sa súbor buď vyliečiť a presunúť do Karantény, alebo preruší spojenie. Notifikácie sa zobrazujú v paneli oznámení v pravej dolnej časti obrazovky. Podrobné informácie o zachytených/vyliečených objektoch nájdete v kapitole Protokoly. Pre viac informácií o jednotlivých úrovniach liečenia a správaní si prečítajte kapitolu Liečenie.



Liečenie a mazanie

Ak rezidentná ochrana súborového systému nevie vybrať akciu, vyzve vás pomocou výstražného okna, aby ste akciu vybrali sami. Na výber sú spravidla akcie **Liečiť**, **Odstrániť** a **Žiadna akcia**. Možnosť **Žiadna akcia** sa neodporúča, nakoľko infiltrácia zostáva na svojom pôvodnom mieste, a tak stále predstavuje potenciálnu hrozbu. Výnimkou je, ak máte úplnú istotu, že daný súbor bol ako infiltrácia detegovaný omylom.



Liečenie sa dá aplikovať v prípade, že do súboru bola zavedená časť, ktorá obsahuje škodlivý kód. V tomto prípade má zmysel pokúsiť sa infikovaný súbor liečiť a dostať ho tak do pôvodného stavu. Ak súbor pozostáva výlučne zo škodlivého kódu, bude celý súbor odstránený.

V prípade, že súbor s infiltráciou je „držaný“, napr. systémovým procesom, môže nastať situácia, že nebude vymazaný okamžite, ale až po jeho uvoľnení po reštarte počítača.

Obnovenie súborov z karantény

Karanténa je prístupná z hlavného okna programu ESET Endpoint Security po kliknutí na **Nástroje** > **Karanténa**.

Súbory presunuté do karantény možno obnoviť do ich pôvodného umiestnenia:

- Na tento účel použite funkciu **Obnoviť**, ktorá je k dispozícii v kontextovom menu po kliknutí pravým tlačidlom myši na daný súbor v karanténe.
- Ak je súbor označený ako potenciálne nechcená aplikácia, možnosť **Obnoviť a vylúčiť z kontroly** bude zapnutá. Prečítajte si tiež kapitolu Vylúčenia.
- Kontextové menu ponúka aj možnosť **Obnoviť do**, ktorá vám umožňuje obnoviť súbor do iného umiestnenia, než bolo to pôvodné, z ktorého bol súbor vymazaný.
- Funkcia obnovenia súborov nie je v niektorých prípadoch k dispozícii, napr. pri súboroch na zdieľanom mieste v sieti určených len na čítanie.

Viaceré hrozby

Ak pri kontrole počítača neboli niektoré infikované súbory vyliečené (prípadne úroveň liečenia bola nastavená na hodnotu **Neliečiť**), zobrazí sa okno s možnosťou výberu akcie pre jednotlivé súbory.

Mazanie súborov v archívoch

Pri štandardnej úrovni liečenia je archív vymazaný len v prípade, že obsahuje iba infikované súbory a žiadne iné bezpečné súbory. Archív teda nebude zmazaný, ak okrem infiltrácie obsahuje aj neškodné súbory. Obozretne postupujte pri nastavení prísnej úrovne liečenia, pretože v tomto prípade bude archív s infikovanými súbormi

odstránený vždy bez ohľadu na to, či jeho obsah tvoria aj zdravé súbory.

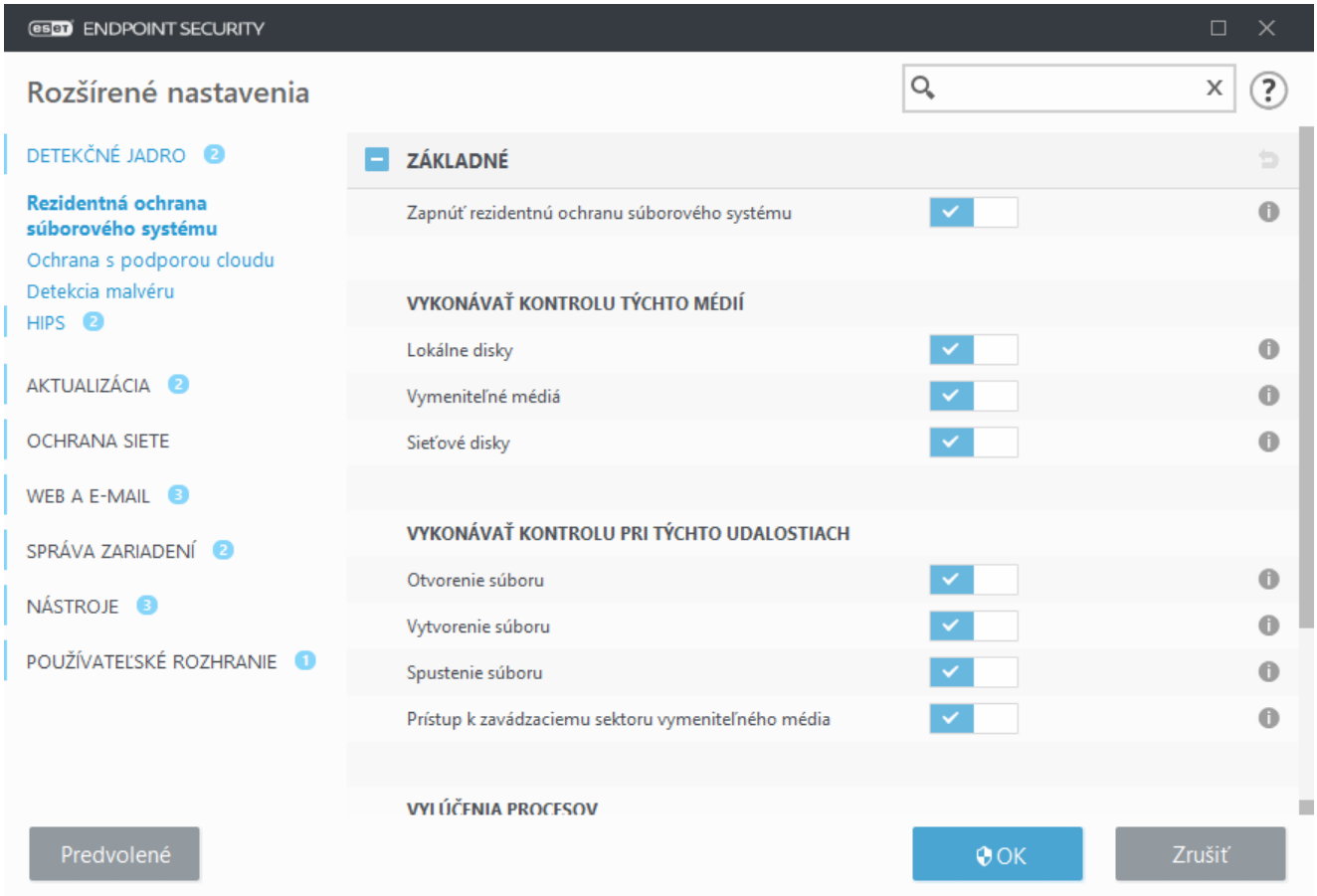
Ak má váš počítač príznaky infekcie škodlivým kódom, teda je pomalší, zamŕza a podobne, odporúčame nasledovné kroky:

- V hlavnom okne programu ESET Endpoint Security kliknite na Kontrola počítača.
- Kliknite na **Smart kontrola** (viac informácií nájdete v kapitole Kontrola počítača).
- Po ukončení kontroly preverte protokol so zoznamom skontrolovaných, infikovaných a vyliečených súborov.

Ak chcete skontrolovať len určité časti svojho počítača, vyberte možnosť **Vlastná kontrola** a označte ciele kontroly.

Rezidentná ochrana súborového systému

Rezidentná ochrana súborového systému kontroluje všetky súbory v systéme na prítomnosť škodlivého kódu pri ich otváraní, vytváraní a spúšťaní.



Na základe predvolených nastavení sa rezidentná ochrana súborového systému spustí pri štarte systému a následne poskytuje nepretržitú kontrolu. Neodporúčame vypínať rezidentnú ochranu zrušením výberu možnosti **Zapnúť rezidentnú ochranu súborového systému** v **Rozšírených nastaveniach** v sekcii **Detekčné jadro** > **Rezidentná ochrana súborového systému** > **Základné**.

Vykonávať kontrolu týchto médií

Predvolene je nastavená kontrola všetkých typov médií:

- **Lokálne disky** – kontroluje všetky systémové a pevné disky (napr.: *C:*\, *D:*\).
- **Vymeniteľné médiá** – kontroluje CD/DVD, USB úložisko, pamäťové karty atď.
- **Sieťové disky** – kontroluje všetky namapované sieťové disky (napr.: *H:*\ ako *store04*) alebo sieťové disky s priamym prístupom (napr.: *store08*).

Odporúčame používať predvolené nastavenia kontroly všetkých médií a meniť ich iba v špecifických prípadoch, napríklad keď pri kontrole určitého média vzniká výrazné spomalenie prenosu dát.

Vykonávať kontrolu pri týchto udalostiach

Na základe predvolených nastavení sa súbory kontrolujú pri otváraní, vytváraní a spúšťaní. Odporúčame vám ponechať tieto predvolené nastavenia bez zmeny, aby bola aj naďalej zabezpečená kontrola všetkého diania v počítači:

- **Otvorenie súboru** – kontroluje súbor pri jeho otvorení.
- **Vytvorenie súboru** – kontroluje novovytvorený alebo upravený súbor.
- **Spustenie súboru** – kontroluje súbor, keď dôjde k jeho spusteniu.
- **Prístup k zavádzaciemu sektoru vymeniteľného média** – ak k zariadeniu pripojíte vymeniteľné médium, ktoré obsahuje zavádzací sektor, prebehne okamžitá kontrola zavádzacieho sektora. Táto možnosť neslúži na povolenie kontroly súborov uložených na vymeniteľných médiách. Nastavenie kontroly súborov na vymeniteľných médiách nájdete v časti **Vykonávať kontrolu týchto médií** > **Vymeniteľné médiá**. Pre správne fungovanie **prístupu k zavádzaciemu sektoru vymeniteľného média** nechajte v sekcii Parametre ThreatSense povolenú možnosť **Zavádzacie sektory/UEFI**.

Zoznam procesov vylúčených z kontroly – viac o tomto type vylúčenia si môžete prečítať v kapitole Vylúčenia procesov.

Rezidentná ochrana súborového systému kontroluje rôzne typy médií, pričom kontrola je vykonávaná pri rôznych udalostiach, napríklad pri prístupe k súboru. Pomocou detekčných metód technológie ThreatSense (bližšie informácie nájdete v časti Parametre ThreatSense) môže byť rezidentná ochrana súborového systému nastavená tak, aby pracovala s novovytvorenými súbormi inak ako v prípade už dlhšie existujúcich súborov. Napríklad pri novovytvorených súboroch je možné nastaviť hlbšiu úroveň kontroly.

Pre zabezpečenie minimálnych systémových nárokov pri používaní rezidentnej ochrany nedochádza k opakovanej kontrole tých súborov, ktoré už boli skontrolované (pokiaľ neboli zmenené). Hneď po každej novej aktualizácii detekčného jadra sú súbory opätovne skontrolované na prítomnosť infiltrácií. Toto správanie je kontrolované pomocou **Smart optimalizácie**. Pokiaľ **Smart optimalizáciu** vypnete, všetky súbory budú kontrolované vždy vtedy, keď sa k nim pristupuje. Toto nastavenie nájdete v **Rozšírených nastaveniach** (F5) v sekcii **Detekčné jadro** > **Rezidentná ochrana súborového systému**. Kliknite na **Parametre ThreatSense** > **Iné** a pomocou prepínača vedľa položky **Zapnúť Smart optimalizáciu** povoľte alebo zakážte túto funkciu.

Kontrola rezidentnej ochrany

Funkčnosť rezidentnej ochrany a detekcie vírusov si môžete overiť pomocou testovacieho súboru zo stránky eicar.com. Ide o neškodný testovací súbor, ktorý by každý funkčný antivírusový program mal byť schopný detegovať. Súbor bol vytvorený spoločnosťou EICAR (European Institute for Computer Antivirus Research) na

otestovanie funkčnosti antivírusových programov.

Súbor je dostupný na stiahnutie na adrese http://www.eicar.org/download/eicar.com.
Keď túto URL adresu zadáte do prehliadača, mala by sa vám zobraziť správa o odstránení hrozby.

Kedy meniť nastavenia rezidentnej ochrany

Rezidentná ochrana súborového systému je najzákladnejším komponentom na udržanie bezpečnosti systému. Preto pri zmenách nastavení treba byť obozretný. Nastavenia rezidentnej ochrany odporúčame meniť len v špecifických prípadoch.

Po nainštalovaní ESET Endpoint Security sú všetky nastavenia optimalizované na zabezpečenie najvyššej úrovne ochrany systému používateľa. Pre obnovenie predvolených nastavení kliknite na tlačidlo v každej časti okna (**Rozšírené nastavenia** > **Detekčné jadro** > **Rezidentná ochrana súborového systému**).

Čo robiť, ak nefunguje rezidentná ochrana

V tejto kapitole sú popísané problémové stavy, ktoré môžu nastať v prípade rezidentnej ochrany, a tiež ich odporúčané riešenie.

Rezidentná ochrana je vypnutá

Ak používateľ omylom vypne rezidentnú ochranu súborového systému, je potrebné ju znova aktivovať. V takomto prípade otvorte hlavné okno programu a kliknite na **Nastavenia** > **Ochrana počítača** > **Rezidentná ochrana súborového systému**.

Ak sa rezidentná ochrana automaticky nespúšťa pri štarte systému, pravdepodobne je deaktivovaná možnosť **Zapnúť rezidentnú ochranu súborového systému**. Uistite sa, že je táto možnosť aktivovaná – otvorte okno **Rozšírené nastavenia** (stlačením klávesu **F5**) a kliknite na **Detekčné jadro** > **Rezidentná ochrana súborového systému**.

Rezidentná ochrana nedeteguje a nelieči infiltrácie

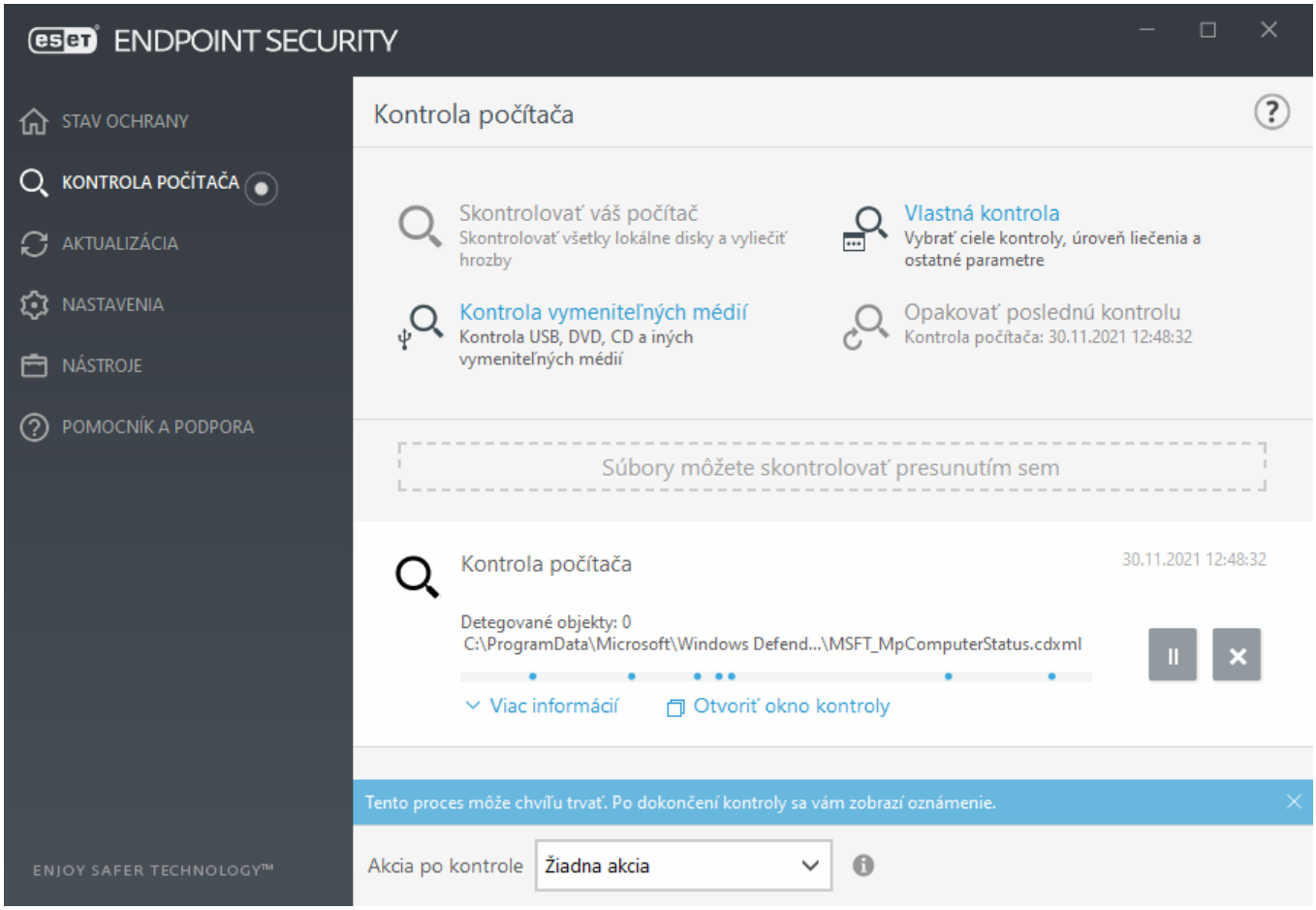
Uistite sa, že nemáte nainštalovaný antivírusový program od inej spoločnosti. Ak sú na počítači nainštalované dva antivírusové programy, medzi ich rezidentnými ochranami môže dochádzať ku konfliktu. Odporúčame preto pred inštaláciou produktu ESET zo systému odinštalovať akýkoľvek iný antivírusový program.

Rezidentná ochrana sa nespúšťa pri štarte

Ak sa rezidentná ochrana automaticky nespúšťa pri štarte systému (a možnosť **Zapnúť rezidentnú ochranu súborového systému** je aktivovaná), pravdepodobne dochádza ku konfliktu s iným programom. V takomto prípade odporúčame kontaktovať technickú podporu spoločnosti ESET. S vyriešením problému môže pomôcť vytvorenie protokolu nástroja ESET SysInspector a jeho zaslanie technickej podpore na analýzu. Viac informácií nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Kontrola počítača

Manuálna kontrola počítača je dôležitou súčasťou programu ESET Endpoint Security. Umožňuje kontrolu diskov, jednotlivých priečinkov a súborov v počítači. Z bezpečnostného hľadiska je potrebné, aby kontrola počítača bola spúšťaná nielen v prípade podozrenia výskytu infekcie, ale aj priebežne v rámci celkovej prevencie. Hĺbkovú kontrolu odporúčame vykonávať v pravidelných časových intervaloch (napr. raz mesačne), aby sa detegovali prípadné vírusy, ktoré v čase zápisu na disk neboli zachytené pomocou Rezidentnej ochrany súborového systému. Takáto situácia môže nastať, ak bola rezidentná ochrana v tom čase vypnutá alebo bolo detekčné jadro zastarané, prípadne v čase zápisu na disk program tento konkrétny vírus nedetegoval.



K dispozícii sú dva typy **kontroly počítača**. **Skontrolovať váš počítač** slúži na rýchle spustenie kontroly počítača bez nastavovania ďalších parametrov kontroly. **Vlastná kontrola**, naopak, umožňuje vybrať si z rôznych prednastavených profilov a určiť ciele kontroly.

Viac informácií nájdete v kapitole Priebeh kontroly.

Skontrolovať váš počítač

Smart kontrola je rýchla kontrola počítača, ktorá lieči infikované súbory bez potreby zásahu používateľa. Výhodou Smart kontroly je jej rýchle spustenie bez nutnosti nastavovania. Kontrolujú sa všetky súbory na lokálnych diskoch, pričom nájdené infiltrácie budú automaticky vyliečené alebo zmazané. Úroveň liečenia je automaticky nastavená na predvolenú hodnotu. Pre podrobnejšie informácie ohľadom typov liečenia si pozrite kapitolu Liečenie.

Vlastná kontrola

Vlastná kontrola je užitočná v prípade, že chcete vybrať konkrétne ciele a metódy kontroly. Výhodou je možnosť vlastného nastavenia parametrov kontroly. Tieto nastavenia sa dajú uložiť do tzv. profilov. To je užitočné, najmä ak chcete vykonávať pravidelnú vlastnú kontrolu počítača so svojimi obľúbenými nastaveniami.

Ak si želáte skontrolovať len špecifické súbory na disku, kliknite na **Kontrola počítača** > **Vlastná kontrola**, z roletového menu **Ciele kontroly** vyberte príslušnú možnosť, prípadne vyberte požadované ciele kontroly z adresárovej (stromovej) štruktúry. Cieľ kontroly môžete špecifikovať aj zadaním cesty k priečinku alebo súboru. Ak chcete spustiť výhradne len kontrolu systému bez následných akcií liečenia, vyberte možnosť **Kontrolovať bez liečenia**. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na **Nastaviť** > **Parametre ThreatSense** > **Liečenie**.

Používanie vlastnej kontroly je navrhnuté pre pokročilých používateľov, ktorí majú skúsenosti s antivírusovými programami.

Môžete tiež manuálne spustiť kontrolu konkrétneho súboru alebo priečinka jeho presunutím **(Drag & drop)** do vyznačeného priestoru – kliknite na daný súbor alebo priečinok a podržte tlačidlo myši stlačené, následne presuňte kurzor myši do vyznačeného priestoru a uvoľnite prst z tlačidla myši. Aplikácia sa následne presunie do popredia.

Kontrola vymeniteľných médií

Funguje podobne ako funkcia **Skontrolovať váš počítač**, keďže vám umožňuje okamžite spustiť kontrolu vymeniteľných médií aktuálne pripojených do počítača (ako napr. CD, DVD a USB). Toto môže byť užitočné v prípade, ak pripojíte USB kľúč do počítača a želáte si skontrolovať jeho obsah na prítomnosť malvéru alebo iných potenciálnych hrozieb.

Tento typ kontroly počítača je možné spustiť aj kliknutím na možnosť **Vlastná kontrola**, zvolením možnosti **Vymeniteľné médiá** v roletovom menu **Ciele kontroly** a kliknutím na **Kontrolovať**.

Opakovať poslednú kontrolu

Táto funkcia vám umožňuje rýchlo spustiť naposledy spustenú kontrolu s rovnakými nastaveniami.

Z roletového menu **Akcia po kontrole** môžete vybrať niektorú z nasledujúcich možností: **Žiadna akcia**, **Vypnúť**, **Reštartovať**, **Reštartovať v prípade potreby**, **Vynútiť reštart v prípade potreby** alebo **Vynútiť reštart**. Možnosti **Uspať** a **Prepnúť do režimu dlhodobého spánku** sú dostupné v závislosti od nastavení napájania a režimu spánku v rámci operačného systému alebo od možností vášho počítača/laptopu. Zvolená akcia sa spustí po dokončení všetkých prebiehajúcich kontrol. Ak ste zvolili akciu **Vypnúť**, zobrazí sa dialógové okno s výzvou na potvrdenie vypnutia počítača s 30□sekundovým odpočítavaním, v rámci ktorého je možné plánované vypnutie počítača zrušiť kliknutím na **Zrušiť**. Viac informácií nájdete v kapitole Pokročilé možnosti kontroly.

> Odporúčame, aby kontrola počítača prebehla aspoň raz za mesiac. Kontrola sa dá nastaviť ako jedna z plánovaných úloh v časti **Nástroje** > **Plánovač**. Ako naplánovať pravidelnú týždňovú kontrolu?

Spustenie vlastnej kontroly

Ak si želáte skontrolovať len špecifické súbory na disku, môžete použiť nástroj Vlastná kontrola. Kliknite na **Kontrola počítača** > **Vlastná kontrola** a z roletového menu > **Ciele kontroly** vyberte príslušnú možnosť, resp. príslušné cieľové umiestnenie z adresárovej (stromovej) štruktúry.

Ciele kontroly slúžia na výber objektov (pamäte, diskov, sektorov, súborov a adresárov), ktoré majú byť skontrolované na prítomnosť infiltrácií.

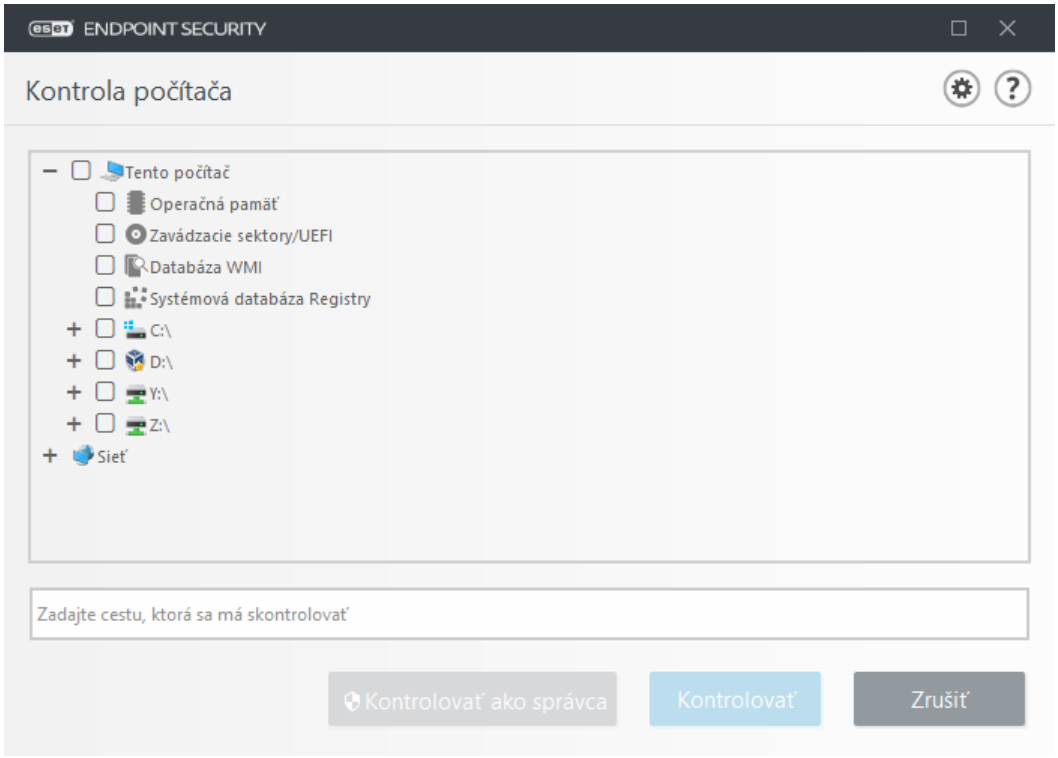
Roletové menu **Ciele kontroly** umožňuje vybrať na kontrolu preddefinované objekty.

- **Podľa nastavenia profilu** – vykoná výber cieľov uložených v profile.
- **Vymeniteľné médiá** – vyberie diskety, CD/DVD, USB kľúče atď.
- **Lokálne disky** – vyberie lokálne pevné disky v počítači.
- **Sieťové disky** – vyberie mapované sieťové disky.
- **Vlastný výber** – zruší celý predchádzajúci výber.

Adresárová (stromová) štruktúra tiež obsahuje konkrétne ciele kontroly.

- **Operačná pamäť** – skontrolujú sa všetky procesy a dáta aktuálne používané operačnou pamäťou.
- **Zavádzacie sektory/UEFI** – skontrolujú sa zavádzacie sektory a UEFI na prítomnosť malvéru. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
- **Databáza WMI** – skontroluje sa celá databáza služby Windows Management Instrumentation (WMI), všetky priestory názvov, inštancie triedy a vlastnosti. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta.
- **Systémová databáza Registry** – skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Ak chcete rýchlo prejsť k požadovanému cieľu kontroly (súbor alebo priečinok), zadajte jeho cestu do textového poľa pod stromovou štruktúrou. V ceste sa rozlišujú veľké a malé písmená. Označením políčka v stromovej štruktúre pridáte daný cieľ do zoznamu cieľov, ktoré sa majú skontrolovať.



Infikované objekty nie sú automaticky liečené. Kontrolu bez liečenia môžete využiť na získanie prehľadu o aktuálnom stave ochrany vášho systému a potrebách liečenia. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na **Rozšírené nastavenia** > **Detekčné jadro** > **Manuálna kontrola** > **Parametre ThreatSense** > **Liečenie**. Ak chcete spustiť výhradne len kontrolu systému bez následných akcií liečenia, vyberte možnosť **Kontrolovať bez liečenia**. História kontrol sa zaznamenáva do protokolu kontroly.

Ak je vybraná možnosť **Ignorovať vylúčenia**, súbory s príponami, ktoré boli predtým vylúčené z kontroly, budú kontrolované bez výnimky.

Profil, s ktorým bude vykonaná kontrola zvolených cieľov, môžete vybrať z roletového menu **Profil kontroly**. Predvolený profil je **Smart kontrola**. Sú dostupné aj ďalšie tri prednastavené profily: **Kontrola z kontextového menu**, **Hĺbková kontrola** a **Kontrola počítača**. Tieto profily používajú rôzne parametre ThreatSense. Dostupné možnosti nájdete v **Rozšírených nastaveniach** v sekcii **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > Parametre ThreatSense.

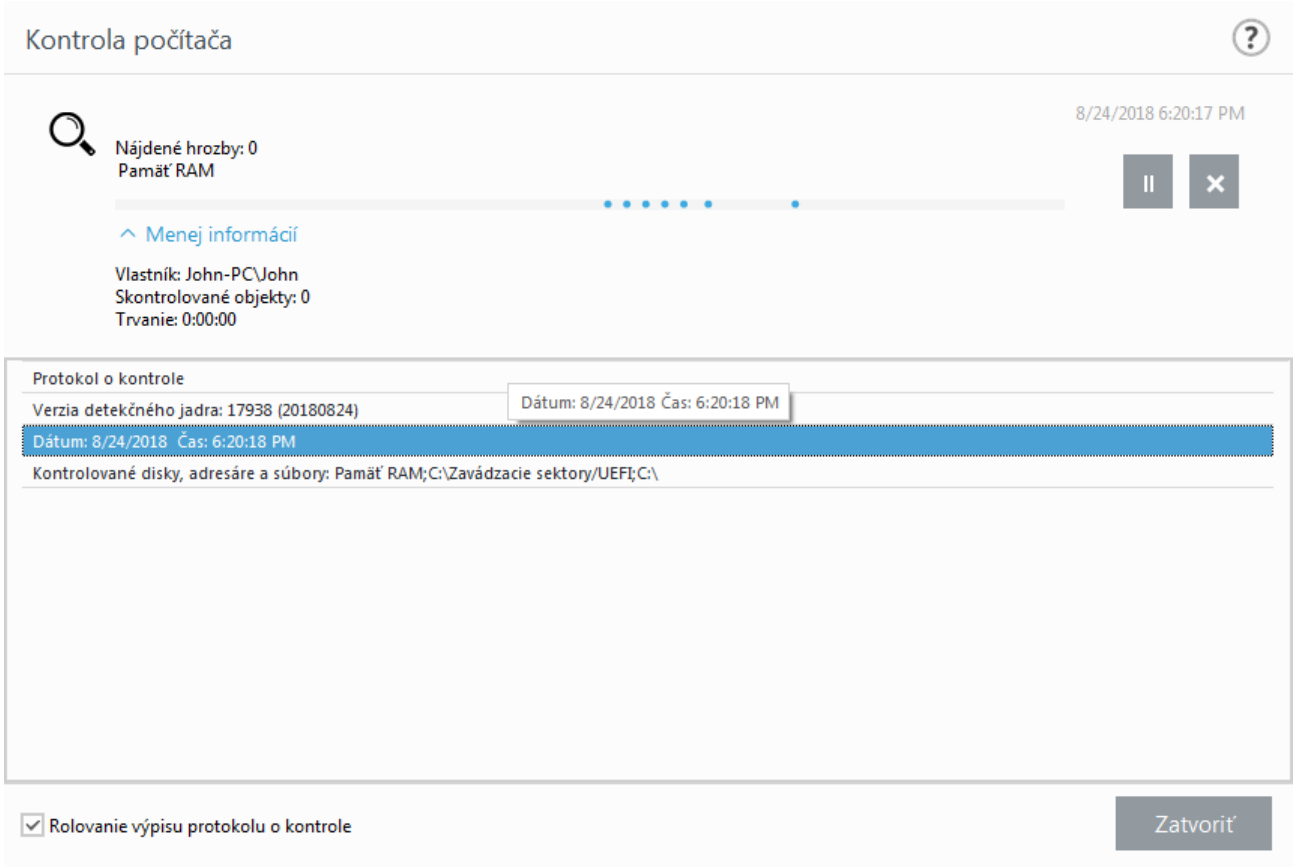
Kliknutím na **Kontrolovať** spustíte kontrolu počítača s parametrami, ktoré ste nastavili.

Kontrolovať ako správca spúšťa kontrolu počítača pod účtom správcu. Túto možnosť je vhodné použiť, ak prihlásený používateľ nemá dostatočné oprávnenia na prístup k súborom, ktoré sa majú kontrolovať. Táto možnosť nie je dostupná, ak aktuálne prihlásený používateľ nemôže vyvolať operácie UAC (kontroly používateľských kont) ako administrátor.

Po dokončení kontroly počítača môžete zobraziť protokol o kontrole kliknutím na **Zobraziť protokol**.

Priebeh kontroly

Okno priebehu kontroly ukazuje aktuálny stav kontroly a počet nájdených súborov, ktoré obsahujú škodlivý kód.



Je v poriadku, ak určité typy súborov, ako napríklad dáta chránené heslom alebo súbory využívané výhradne systémom (napr. *pagefile.sys* a niektoré súbory protokolov), nemôžu byť skontrolované.

Priebeh kontroly – indikátor priebehu kontroly zobrazuje stav pomeru skontrolovaných súborov oproti súborom, ktoré na kontrolu ešte čakajú. Stav je určovaný podľa celkového počtu objektov zahrnutých do kontroly.

Cieľ – názov aktuálne kontrolovaného súboru a jeho umiestnenie.

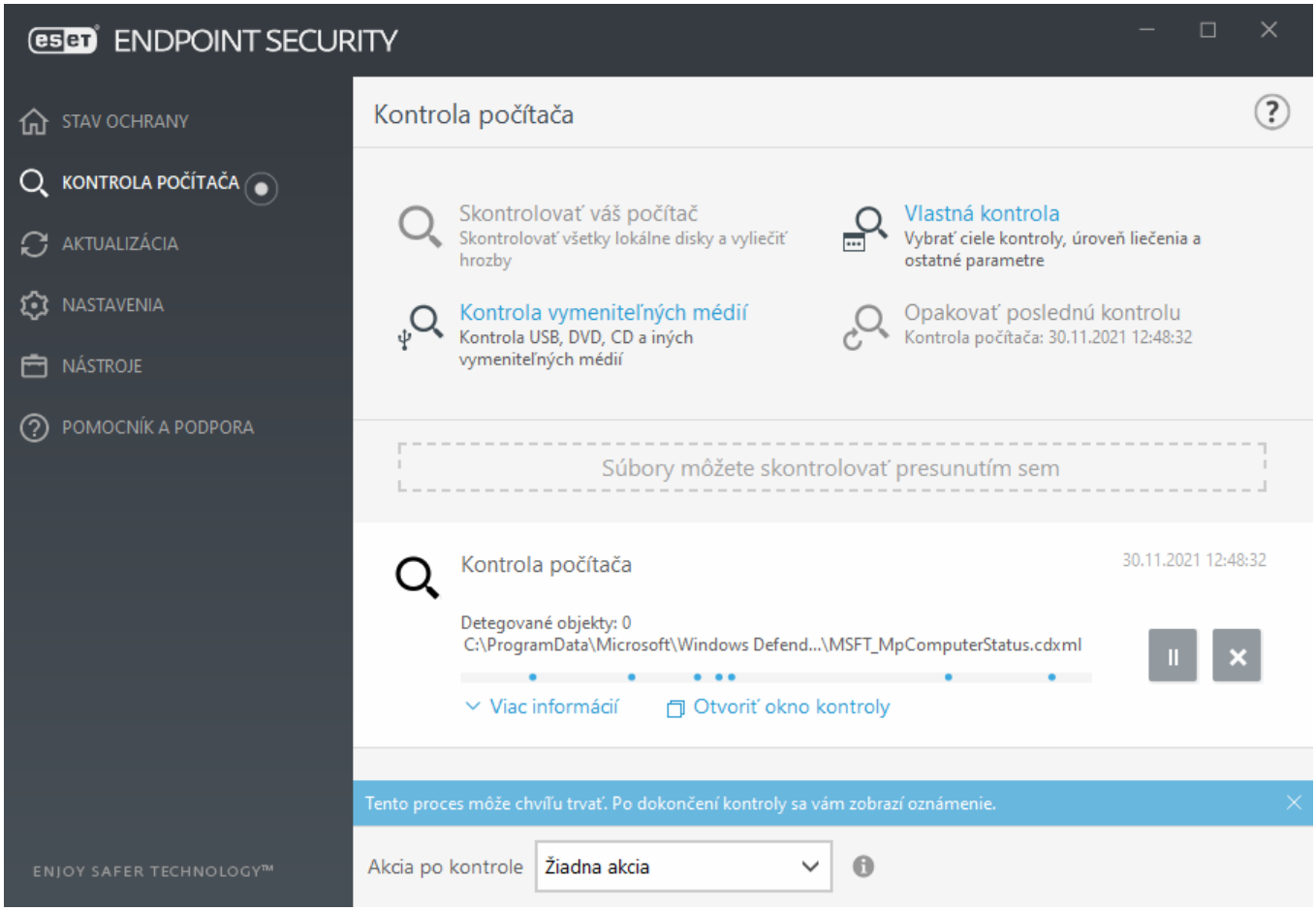
Nájdené hrozby – zobrazuje celkový počet hrozieb nájdených počas kontroly.

Pozastaviť – pozastaví kontrolu.

Pokračovať – táto možnosť sa zobrazí po pozastavení kontroly. Kliknite na **Pokračovať** pre pokračovanie v kontrole.

Zastaviť – preruší a ukončí kontrolu.

Rolovanie výpisu protokolu o kontrole – po zapnutí tejto možnosti uvidíte v okne kontroly vždy tie najnovšie záznamy o práve skontrolovaných objektoch.



Protokol o kontrole počítača

Protokol o kontrole počítača vám poskytuje všeobecné informácie o kontrole, ako napríklad:

- dátum a čas kontroly,
- kontrolované disky, priečinky a súbory,
- počet skontrolovaných objektov,
- počet nájdených hrozieb,
- čas ukončenia kontroly,
- celkový čas kontroly.

Detekcia malvéru

Sekcia **Detekcia malvéru** je dostupná v Rozšírených nastaveniach. Stlačte kláves **F5** a prejdite do sekcie **Detekčné jadro** > **Detekcia malvéru**, kde môžete nastaviť parametre kontroly. Táto sekcia obsahuje nasledujúce možnosti:

- **Aktívny profil** – určuje názov profilu, ktorého nastavenia sa použijú pri manuálne spustenej kontrole. Pridať nový profil je možné prostredníctvom tlačidla Upraviť v sekcii Zoznam profilov. Viac informácií nájdete v kapitole Profily kontroly.
- **Manuálna kontrola s využitím strojového učenia** – prečítajte si kapitolu Detekčné jadro (7.2 a novšie verzie).
- **Ciele kontroly** – ak si želáte skontrolovať len konkrétne súbory na disku, kliknite na **Upraviť** vedľa popisu **Ciele kontroly** a z roletového menu vyberte príslušnú možnosť, resp. príslušné cieľové umiestnenie z adresárovej štruktúry. Viac informácií nájdete v kapitole Ciele kontroly.

- **Parametre ThreatSense** – detailnejšie nastavenia kontroly, ako napr. typy súborov, ktoré si želáte kontrolovať, metódy detekcie a iné. Kliknutím na túto sekciu sa zobrazia podrobné nastavenia kontroly počítača.

Kontrola v nečinnosti

Kontrolu v nečinnosti môžete povoliť v **Rozšírených nastaveniach** v časti **Detekčné jadro** > **Detekcia malvéru** > **Kontrola v nečinnosti**.

Kontrola v nečinnosti

Ak chcete zapnúť kontrolu v nečinnosti, kliknite na prepínač vedľa popisu **Zapnúť kontrolu v nečinnosti**. Ak je počítač v nečinnosti, na pozadí sa spúšťa kontrola všetkých diskov počítača.

Na základe predvolených nastavení programu sa kontrola v nečinnosti nespúšťa, ak je počítač (laptop) napájaný z batérie. Toto nastavenie môžete prepísať aktivovaním funkcie **Spustiť, aj keď je počítač napájaný z batérie** v okne Rozšírených nastavení.

Kliknite na prepínacie tlačidlo **Vytvárať protokol** v sekcii Rozšírené nastavenia, ak chcete z kontroly v nečinnosti vytvárať protokol, ktorý nájdete v časti Protokoly (v hlavnom okne programu kliknite na **Nástroje** > **Protokoly** a potom vyberte možnosť **Kontrola počítača** z roletového menu **Protokoly**).

Detekcia stavu nečinnosti

O podmienkach spustenia kontroly v nečinnosti sa dočítate v kapitole Detekcia stavu nečinnosti.

Ak chcete upraviť parametre kontroly v stave nečinnosti (napr. metódy detekcie), prejdite na kapitolu Parametre ThreatSense.

Profily kontroly

ESET Endpoint Security ponúka 4 prednastavené profily kontroly:

- **Smart kontrola** – toto je predvolený profil pokročilej kontroly. Profil Smart kontroly využíva technológiu Smart optimalizácie na vylúčenie súborov, ktoré boli počas predchádzajúcej kontroly vyhodnotené ako neškodné a odvtedy neboli zmenené. Vďaka tomu je čas kontroly kratší, pričom vplyv na bezpečnosť systému je minimálny.
- **Kontrola z kontextového menu** – kontrolu ľubovoľného súboru môžete spustiť manuálne z kontextového menu. Profil Kontroly z kontextového menu umožňuje nastaviť konfiguráciu kontroly, ktorá bude použitá pri spustení kontroly.
- **Hĺbková kontrola** – profil Hĺbkovej kontroly štandardne nevyužíva Smart optimalizáciu, čo znamená, že ak použijete tento profil, z kontroly nebudú vylúčené žiadne súbory.
- **Kontrola počítača** – toto je predvolený profil použitý pri štandardnej kontrole počítača.

Preferované nastavenia kontroly je možné uložiť do profilov pre budúce použitie. Odporúčame vám, aby ste vždy vytvorili nový profil (s rôznymi cieľmi kontroly, metódami kontroly a ďalšími parametrami) pre každú pravidelne používanú kontrolu.

Pre vytvorenie nového profilu otvorte okno Rozšírené nastavenia (F5) a kliknite na **Detekčné jadro** > **Detekcia malvéru** > **Manuálna kontrola** > **Zoznam profilov**. Otvorí sa okno **Manažér profilov**, v ktorom sa nachádza roletové menu **Aktívny profil** obsahujúce zoznam existujúcich profilov kontroly, ako aj možnosť vytvoriť nový profil kontroly. Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite kapitolu Nastavenie parametrov skenovacieho jadra ThreatSense, ktorá obsahuje popis každého parametra kontroly.

Predpokladajme, že chcete vytvoriť vlastný profil kontroly a čiastočne vám vyhovujú nastavenia predvoleného profilu používaného v prípade funkcie **Skontrolovať váš počítač**. Nechcete však kontrolovať runtime archívy, potenciálne nebezpečné aplikácie a chcete tiež použiť **Prísne liečenie**. Zadajte názov nového profilu do okna **Manažér profilov** a kliknite na možnosť **Pridať**. Označte svoj nový profil v roletovom menu **Aktívny profil**, upravte ostatné parametre tak, aby vám vyhovovali, a profil uložte kliknutím na **OK**.

Ciele kontroly

Ciele kontroly slúžia na výber objektov (pamäte, diskov, sektorov, súborov a adresárov), ktoré majú byť skontrolované na prítomnosť infiltrácií.

Roletové menu **Ciele kontroly** umožňuje vybrať na kontrolu preddefinované objekty.

- **Podľa nastavenia profilu** – vykoná výber cieľov uložených v profile.
- **Vymeniteľné médiá** – vyberie diskety, CD/DVD, USB kľúče atď.
- **Lokálne disky** – vyberie lokálne pevné disky v počítači.
- **Sieťové disky** – vyberie mapované sieťové disky.
- **Vlastný výber** – zruší celý predchádzajúci výber.

Adresárová (stromová) štruktúra tiež obsahuje konkrétne ciele kontroly.

- **Operačná pamäť** – skontrolujú sa všetky procesy a dáta aktuálne používané operačnou pamäťou.
- **Zavádzacie sektory/UEFI** – skontrolujú sa zavádzacie sektory a UEFI na prítomnosť malvéru. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
- **Databáza WMI** – skontroluje sa celá databáza služby Windows Management Instrumentation (WMI), všetky priestory názvov, inštancie triedy a vlastnosti. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta.
- **Systémová databáza Registry** – skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadajú sa odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Ak chcete rýchlo prejsť k požadovanému cieľu kontroly (súbor alebo priečinok), zadajte jeho cestu do textového poľa pod stromovou štruktúrou. V ceste sa rozlišujú veľké a malé písmená. Označením políčka v stromovej štruktúre pridáte daný cieľ do zoznamu cieľov, ktoré sa majú skontrolovať.

Pokročilé možnosti kontroly

V tomto okne môžete meniť rozšírené nastavenia pre plánované úlohy kontroly počítača. Môžete nastaviť akciu, ktorá bude vykonaná automaticky po ukončení kontroly:

- **Vypnúť** – počítač sa po ukončení kontroly vypne.
- **Reštartovať** – počítač po ukončení kontroly zatvorí všetky spustené programy a reštartuje sa.

- **Reštartovať v prípade potreby** – počítač v prípade potreby po ukončení kontroly zatvorí všetky spustené programy a reštartuje sa.
- **Uspať** – vaša relácia bude uložená a počítač sa prepne do úsporného režimu, tak aby sa dal rýchlo zapnúť.
- **Prepnúť do režimu dlhodobého spánku** – bude uložená snímka stavu počítača a počítač sa vypne. Pri opätovnom zapnutí počítača sa načíta uložený stav.
- **Žiadna akcia** – po ukončení kontroly nebude vykonaná žiadna akcia.

> Berte na vedomie, že počítač, ktorý sa nachádza v stave spánku, je aj naďalej zapnutý. Takýto počítač má stále aktívne základné funkcie a naďalej spotrebúva elektrickú energiu, a to aj v prípade, že je napájaný z batérie. Pre šetrenie batérie, napríklad pri cestovaní mimo kancelárie, odporúčame použiť možnosť Prepnúť do režimu dlhodobého spánku.

Kliknite na možnosť **Akcia nemôže byť zrušená používateľom**, ak si prajete, aby neoprávnený používateľ nemohol zrušiť akciu po ukončení kontroly.

Nastavte hodnotu pre možnosť **Pozastaviť plánované kontroly o (min.)**, ak chcete umožniť používateľovi s obmedzenými oprávneniami pozastaviť kontrolu počítača na stanovený čas.

Viac informácií nájdete v časti Priebeh kontroly.

Správa zariadení

ESET Endpoint Security poskytuje automatickú kontrolu externých zariadení (CD/DVD/USB/...). Tento modul umožňuje blokovať a nastaviť rozšírené prístupové práva a pravidlá na filtrovanie prístupu k zariadeniu. Toto môže byť užitočné v prípade, že správca chce, aby používatelia nemohli používať externé zariadenia s nevyžiadaným obsahom.

Podporované externé zariadenia:

- Diskové úložisko (HDD, vymeniteľný USB disk)
- CD/DVD
- USB tlačiareň
- Úložisko FireWire
- Zariadenie Bluetooth
- Čítačka smart kariet
- Obrazové zariadenie
- Modem
- Port LPT/COM
- Prenosné zariadenie (zariadenia napájané z batérie, ako sú prehrávače médií, smartfóny, zariadenia typu plug-and-play atď.)
- Všetky typy zariadení

Nastavenia správy zariadení je možné meniť v **Rozšírených nastaveniach** (F5) > **Správa zariadení**.

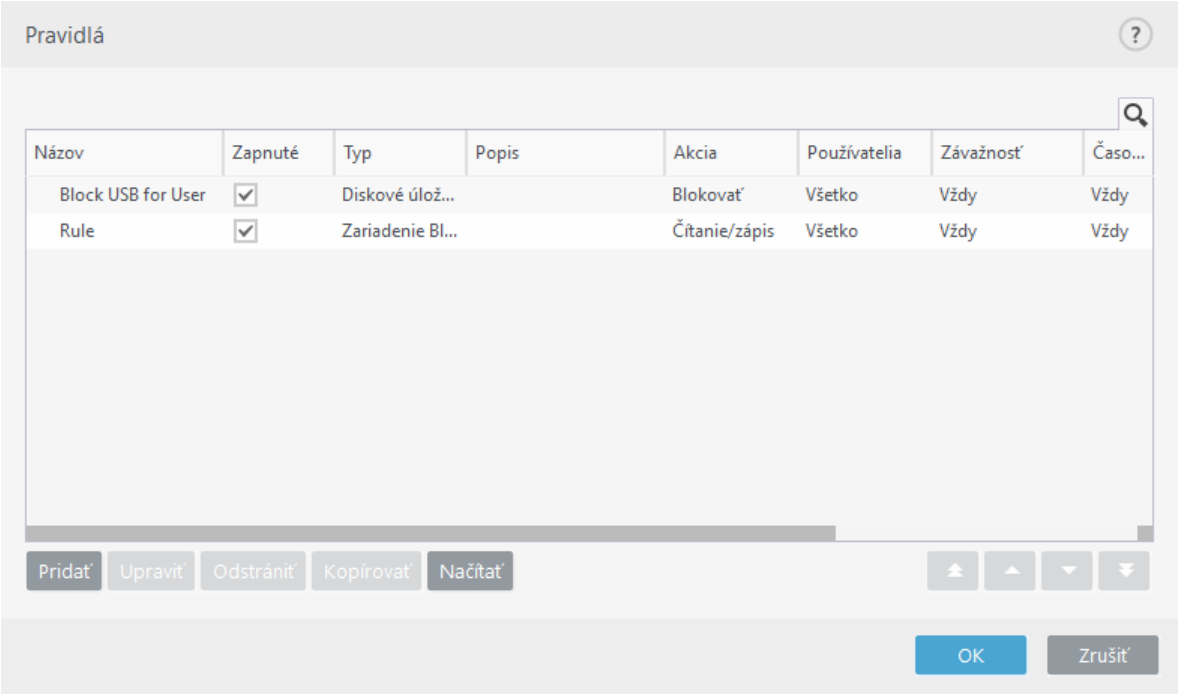
Možnosť **Zapnúť správu zariadení** aktivuje funkciu Správa zariadení v programe ESET Endpoint Security. Na dokončenie zmeny tejto konfigurácie bude potrebný reštart operačného systému. Následne sa aktivujú **Pravidlá** a budete môcť otvoriť Editor pravidiel.

Pri vložení zariadenia blokovaného existujúcim pravidlom sa zobrazí upozornenie a prístup na zariadenie nebude povolený.

Pravidlá správy zariadení

Editor pravidiel správy zariadení zobrazuje zoznam všetkých existujúcich pravidiel, ktoré vám umožňujú kontrolovať externé zariadenia pripájané k vášmu počítaču. Pozrite si tiež kapitolu Pridanie pravidiel správy zariadení.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Pridanie a úprava pravidiel správy zariadení pomocou produktov ESET pre koncové zariadenia



Konkrétne zariadenia môžu byť povolené alebo blokované vzhľadom na používateľa, skupinu používateľov alebo iné parametre, ktoré zadefinujete v konfigurácii pravidla. Zoznam pravidiel obsahuje popisné informácie ako názov, typ externého zariadenia, akcia, ktorá sa má vykonať po pripojení zariadenia k počítaču, a rozsah vytvorených protokolov.

Kliknutím na **Pridať** alebo **Upraviť** pridáte či upravíte pravidlo. Zrušte označenie možnosti **Zapnuté**, ak chcete pravidlo dočasne deaktivovať (táto možnosť je užitočná, ak nechcete pravidlo zmazať, ale len dočasne zakázať). Ak chcete pravidlo odstrániť natrvalo, kliknite na **Odstrániť**.

Kopírovať – môžete vytvoriť nové pravidlo s prednastavenými možnosťami použitými pre iné vybrané pravidlo.

Na automatické vyplnenie parametrov zo zariadenia pripojeného k vášmu počítaču kliknite na možnosť **Načítať**.

Pravidlá sú zoradené podľa priority, pričom pravidlá s najvyššou prioritou sú navrchu. Pravidlá môžete jednotlivo alebo v skupinách premiestňovať kliknutím na tlačidlá  **Navrch/Vyššie/Nižšie/Naspodok**.

Do protokolu správy zariadení sa zaznamenávajú informácie o všetkých akciách modulu Správy zariadení. Tieto záznamy sú prístupné z hlavného okna programu ESET Endpoint Security v sekcii **Nástroje** > **Protokoly**.

Zistené zariadenia

Tlačidlo **Načítať** zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné.

Zvolením konkrétneho zariadenia zo zoznamu Zistené zariadenia a kliknutím na tlačidlo **OK** môžete pridať nové pravidlo správy zariadení s preddefinovanými hodnotami (zobrazené hodnoty je možné upraviť).

Zariadenia v režime nízkej spotreby (režim spánku) sú označené ikonou výkričníka . Ak chcete pre takéto zariadenie pridať pravidlo a aktivovať tlačidlo **OK**, postupujte nasledovne:

- Odpojte a znovu pripojte zariadenie.
- Použite zariadenie (napríklad spustite aplikáciu Fotoaparát v systéme Windows na prebudenie webovej kamery).

Skupiny zariadení

Zariadenia pripojené k vášmu počítaču môžu predstavovať bezpečnostné riziko.

Okno Skupiny zariadení je rozdelené na dve časti. Po pravej strane sa nachádza zoznam zariadení patriacich do skupiny, ktorých zoznam je na ľavej strane okna. Na pravej strane vyberte skupinu zariadení, ktorej zariadenia chcete zobraziť.

Ak otvoríte okno Skupiny zariadení a označíte vytvorenú skupinu, môžete pridať alebo odstrániť zariadenia zo zoznamu. Ďalším spôsobom, ako pridať zariadenia do skupiny, je importovať zoznam zariadení zo súboru. Môžete prípadne kliknúť na tlačidlo **Načítať** a všetky zariadenia pripojené k vášmu počítaču sa zobrazia v okne **Zistené zariadenia**. Vyberte zariadenie z načítaného zoznamu a pridajte ho do skupiny kliknutím na **OK**.

Ovládacie prvky

Pridať – môžete pridať skupiny zariadení alebo zariadenia do existujúcej skupiny (môžete prípadne zadať ďalšie podrobnosti, ako napr. výrobcu, model a sériové číslo zariadenia).

Upraviť – môžete zmeniť názov vybranej skupiny alebo parametre pre vybrané zariadenie (výrobcu, model, sériové číslo).

Odstrániť – odstráni vybranú skupinu alebo zariadenie.

Import – importuje zoznam zariadení z textového súboru. Súbor musí spĺňať nasledujúci formát:

- Každé zariadenie začína na novom riadku.
- Pre každé zariadenie musí byť uvedený **Výrobca**, **Model** a **Sériové číslo**, pričom tieto informácie sú oddelené čiarkou.

Príklad obsahu textového súboru:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Export – vyexportuje zoznam zariadení do súboru.

Tlačidlo **Načítať** zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ

zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné.

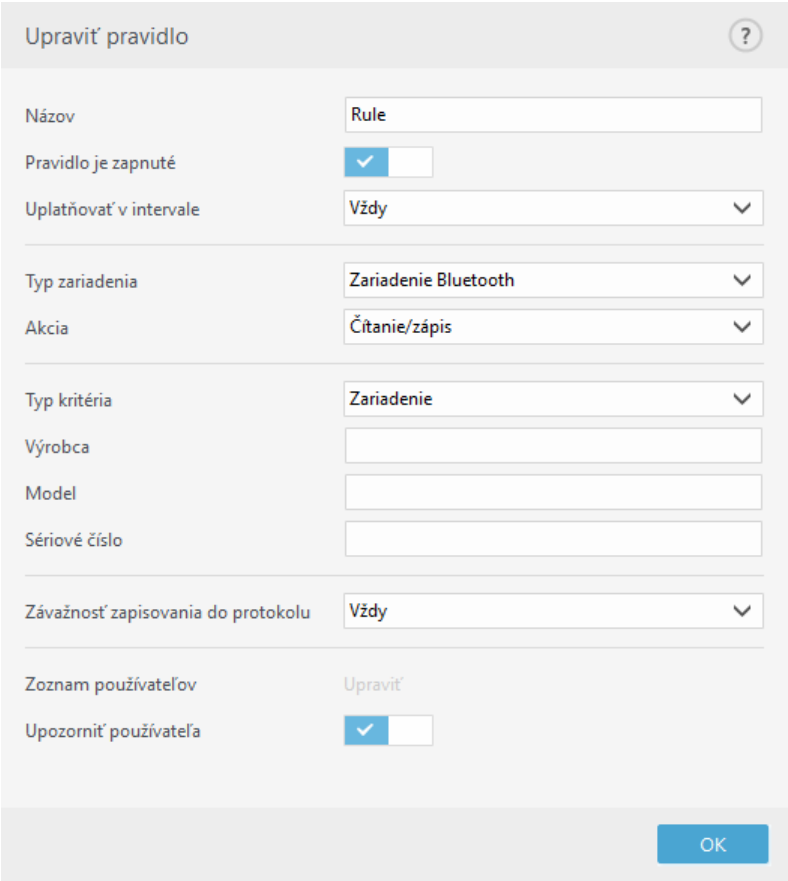
Zmeny potvrdíte kliknutím na **OK**. Ak chcete opustiť okno **Skupiny zariadení** bez uloženia zmien, kliknite na **Zrušiť**.

> Môžete vytvoriť viacero skupín zariadení, na ktoré môžete aplikovať rozdielne pravidlá. Môžete tiež vytvoriť len jednu skupinu dôveryhodných zariadení, na ktorú aplikujete pravidlo na **Čítanie/Zápis** alebo **Iba na čítanie**. Vďaka tomu bude zaručené blokovanie neznámych zariadení pripojených k vášmu počítaču.

Majte na pamäti, že pre niektoré typy zariadení nemusia byť dostupné všetky akcie (povolenia). V prípade úložného zariadenia sú dostupné všetky štyri akcie. Ak ide o zariadenie, ktoré neslúži na ukladanie dát, sú k dispozícii len tri akcie (napríklad akcia **Iba na čítanie** nie je dostupná pri Bluetooth zariadeniach, takže tieto zariadenia sa dajú len povoliť, blokovať alebo na ne upozorniť).

Pridanie pravidiel správy zariadení

Pravidlo správy zariadení definuje akciu, ktorá bude vykonaná pri pripojení zariadenia spĺňajúceho kritériá v pravidle.



Do poľa **Názov** zadajte popis pravidla na jeho lepšiu identifikáciu. Tlačidlo **Pravidlo je zapnuté** aktivuje alebo deaktivuje konkrétne pravidlo, čo je užitočné v prípade, že si neželáte vymazať pravidlo natrvalo.

Uplatňovať v intervale – umožňuje vám uplatňovať vytvorené pravidlo len počas určitého časového úseku. Z roletového menu stačí vybrať vytvorený časový interval. Prečítajte si viac o časových intervaloch.

Typ zariadenia

Z roletového menu vyberte typ externého zariadenia (disk, prenosné zariadenie, Bluetooth, FireWire atď.). Informácia o type zariadenia je prevzatá od operačného systému a je uvedená v systémovom Správcovi zariadení (Device manager), ak je zariadenie pripojené k počítaču. Úložné zariadenia zahŕňajú externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Čítačky smart kariet zahŕňajú čítačky kariet s integrovaným obvodom, ako sú napríklad SIM karty alebo overovacie karty. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty, ktoré neposkytujú informácie o používateľovi, ale iba o akciách. Keďže neposkytujú informácie o používateľovi, ale iba o akciách, môžu byť blokované len globálne pre všetkých používateľov.

> Zoznam používateľov nie je dostupný pre modemy. Pravidlo bude použité pre všetkých používateľov a súčasný zoznam používateľov bude vymazaný.

Akcia

Prístupové práva k zariadeniam bez úložiska môžu byť povolené/blokované. Na druhej strane v rámci prístupových práv k úložným zariadeniam môžete vybrať jednu z nasledujúcich možností:

- **Čítanie/Zápis** – bude povolený úplný prístup k zariadeniu.
- **Blokovať** – prístup k zariadeniu bude blokovaný.
- **Iba na čítanie** – povolený bude prístup k zariadeniu len na čítanie, nie na zápis.
- **Upozorniť** – pri pripojení zariadenia k počítaču, bude používateľ informovaný, či je zariadenie povolené alebo blokované, a táto informácia sa tiež zaznamená do protokolu. Program si zariadenia nepamätá, čo znamená, že príslušné oznámenie sa zobrazí aj pri opätovnom pripojení rovnakého zariadenia.

Majte na pamäti, že pre niektoré typy zariadení nemusia byť dostupné všetky akcie (povolenia). V prípade úložného zariadenia sú dostupné všetky štyri akcie. Ak ide o zariadenie, ktoré neslúži na ukladanie dát, sú k dispozícii len tri akcie (napríklad akcia **Iba na čítanie** nie je dostupná pri Bluetooth zariadeniach, takže tieto zariadenia sa dajú len povoliť, blokovať alebo na ne upozorniť).

Typ kritéria

Zvoľte **Zariadenie** alebo **Skupinu zariadení**.

Nasledujúce parametre môžu byť použité na vyladenie pravidla tak, aby bolo platné pre vybrané zariadenie. V parametroch sa rozlišujú veľké a malé písmená:

- **Výrobca** – filtrovanie podľa názvu výrobcu alebo ID.
- **Model** – názov daného zariadenia.
- **Sériové číslo** – externé zariadenia zvyčajne majú svoje vlastné sériové číslo. V prípade CD/DVD ide o sériové číslo daného média, nie CD mechaniky.

> Ak sú vyššie uvedené údaje prázdne, pravidlo bude tieto polia ignorovať. Parametre vo všetkých poliach okna rozlišujú malé a veľké písmená a nepodporujú zástupné znaky (*, ?).

> Na zistenie parametrov zariadenia pripojeného k počítaču najprv vytvorte pravidlo pre daný typ zariadenia a po pripojení zariadenia k počítaču zistite jeho parametre v Protokole správy zariadení.

Závažnosť zapisovania do protokolu

- **Vždy** – zaznamenáva všetky udalosti.
- **Diagnostické** – zaznamenáva do protokolu informácie dôležité pre ladenie programu.
- **Informácie** – zaznamenáva informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky záznamy vyššie.
- **Upozornenia** – zaznamenáva varovné správy a kritické chyby a informuje o nich ERA Server.
- **Žiadne** – nebudú vytvárané žiadne protokoly.

Pravidlo môže byť obmedzené len na určitých používateľov alebo skupiny používateľov ich pridaním do **Zoznamu používateľov**:

- **Pridať** – otvorí sa okno **Vybrať objekty typu: Používatelia alebo Skupiny**, kde je možné vybrať konkrétnych používateľov.
- **Odstrániť** – vybraný používateľ bude odstránený z filtra.

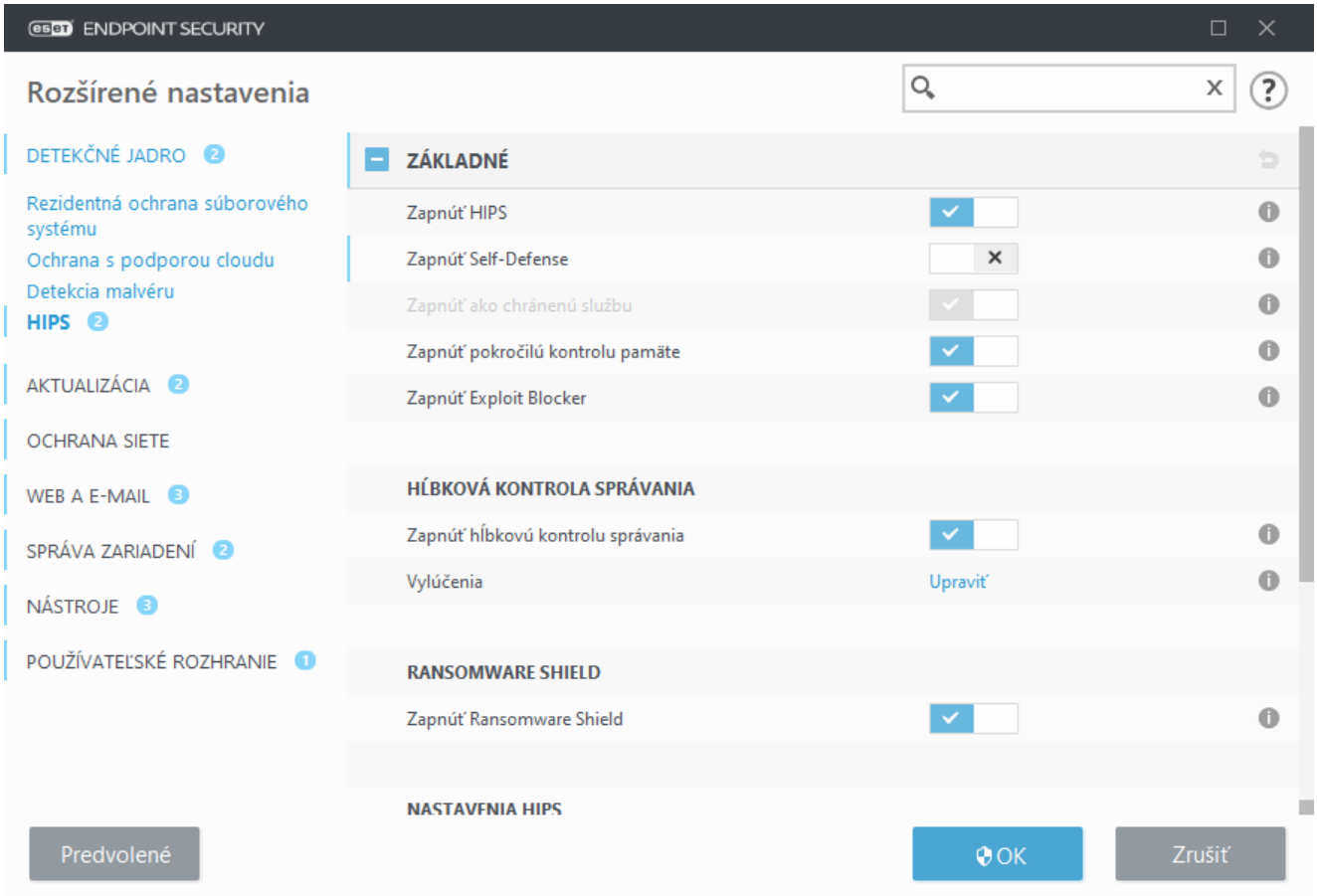
Berte, prosím, na vedomie, že nie všetky zariadenia je možné filtrovať podľa pravidiel používateľa (napr. zobrazovacie zariadenia neposkytujú informácie o používateľoch, ale len o akciách).

HIPS (Host-based Intrusion Prevention System)

Zmeny v nastaveniach systému HIPS odporúčame robiť len skúseným používateľom. Nesprávne nastavenia v sekcii HIPS môžu spôsobiť nestabilitu systému.

Host-based Intrusion Prevention System (HIPS) chráni pred malvérom a nechcenou aktivitou, ktorá môže negatívne pôsobiť na systém. Používa pokročilú analýzu správania, ktorá spolu s detekčnými schopnosťami sieťového filtra zabezpečuje efektívne sledovanie spustených procesov, súborov a záznamov v registroch, čo umožňuje aktívne blokovať takéto pokusy a predchádzať im. HIPS pracuje oddelene od firewallu a rezidentnej ochrany súborového systému, pričom sleduje len procesy spustené v rámci operačného systému.

Nastavenia systému HIPS sa nachádzajú v **Rozšírených nastaveniach** (F5) v časti **Detekčné jadro** > **HIPS** > **Základné**. Stav modulu HIPS (zapnutý/vypnutý) je zobrazený v hlavnom okne programu ESET Endpoint Security v časti **Nastavenia** > **Počítač**.



Základné

Zapnúť HIPS – HIPS je v ESET Endpoint Security predvolene zapnutý. Vypnutie systému HIPS spôsobí vypnutie aj jeho funkcií, ako napr. Exploit Blocker.

Zapnúť Self-Defense – ESET Endpoint Security má ako súčasť systému HIPS vstavanú technológiu **Self-Defense**, ktorej cieľom je zabrániť škodlivému softvéru narušiť alebo deaktivovať antivírusovú a antispyvérovú ochranu. Self-Defense chráni dôležité procesy v rámci systému a programu ESET, súbory a záznamy v databáze Registry pred neoprávnenými zmenami. Chránený je taktiež ESET Management Agent v prípade, že je nainštalovaný.

Zapnúť ako chránenú službu – povoľuje ochranu pre službu ESET (ekrn.exe). Ak je táto možnosť povolená, služba je spustená ako zabezpečený proces systému Windows s cieľom poskytnúť ochranu pred malvérom. Táto možnosť je dostupná na systémoch Windows 8.1 a Windows 10.

Zapnúť pokročilú kontrolu pamäte – spolu s funkciou Exploit Blocker poskytuje lepšiu ochranu pred malvérom, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu bezpečnostných produktov. Pokročilá kontrola pamäte je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Exploit Blocker – je navrhnutý na ochranu najčastejšie zneužívaných aplikácií, ako napríklad webových prehliadačov, softvéru na zobrazovanie PDF dokumentov, e-mailových klientov a komponentov MS Office. Exploit Blocker je v predvolených nastaveniach zapnutý. Viac o tomto type ochrany sa dočítate v slovníku pojmov.

Hĺbková kontrola správania

Zapnúť hĺbkovú kontrolu správania – dodatočná vrstva ochrany, ktorá funguje ako súčasť funkcie HIPS. Jej úlohou je analyzovať správanie všetkých procesov spustených na počítači a upozorniť vás na zachytené škodlivé

správanie.

HIPS vylúčenia z hĺbkovej kontroly správania vám umožňujú nastaviť procesy, ktoré nemajú byť podrobené analýze. Aby bola zaručená kontrola všetkých procesov na prítomnosť hrozieb, neodporúčame vylúčenia vytvárať, ak to nie je naozaj nevyhnutné.

Ransomware Shield

Zapnúť Ransomware Shield – dodatočná vrstva ochrany, ktorá funguje ako súčasť funkcie HIPS. Aby mohol Ransomware Shield fungovať, je potrebné mať povolený systém ESET LiveGrid®. Viac o tomto type ochrany sa môžete dočítať tu.

Povoliť režim auditu – Ransomware Shield neblokuje automaticky všetky nájdené detekcie, ale dochádza k ich zapísaniu do protokolu formou upozornenia a následnému odoslaniu do konzoly na správu s príznakom „REŽIM AUDITU“. Správca môže buď vylúčiť takúto detekciu s cieľom predísť ďalšej detekcii, alebo ju ponechať aktívnu, čo znamená, že po skončení režimu auditu bude zablokovaná a odstránená. Zapnutie/vypnutie režimu auditu sa zaznamená aj v programe ESET Endpoint Security. Táto možnosť je k dispozícii len prostredníctvom editora určeného na konfiguráciu politík v konzole ESET PROTECT.

Nastavenia HIPS

Režim filtrovania umožňuje nastaviť filtrovanie do jedného z nasledujúcich režimov:

Režim filtrovania	Popis
Automatický režim	Operácie budú povolené s výnimkou takých, ktoré sú blokované prednastavenými pravidlami chrániacimi systém.
Smart režim	Používateľ bude upozornený len v prípade skutočne podozrivých udalostí v systéme.
Interaktívny režim	Používateľ bude vyzvaný na potvrdenie operácií.
Režim politík	Blokuje všetky operácie, ktoré nie sú definované konkrétnym pravidlom, ktoré ich povoľuje.
Učiaci sa režim	Operácie sú povolené a zároveň sa po každej operácii vytvorí pravidlo. Pravidlá vytvorené v tomto režime sú viditeľné v editore **pravidiel HIPS**, ale majú nižšiu prioritu ako pravidlá vytvorené manuálne alebo v automatickom režime. Keď z roletového menu **Režim filtrovania** vyberiete možnosť **Učiaci sa režim**, sprístupní sa nastavenie s popisom **Učiaci sa režim skončí**, ktoré vám umožňuje definovať dátum a čas ukončenia tohto režimu. Nastavte obdobie, počas ktorého bude zapnutý učiaci sa režim (maximálne 14 dní). Po uplynutí nastaveného časového obdobia budete vyzvaný na úpravu pravidiel, ktoré boli vytvorené počas učiaceho sa režimu. Môžete tiež zvoliť iný režim filtrovania alebo oddialiť svoje rozhodnutie a používať učiaci sa režim aj naďalej.

Režim, ktorý sa nastaví po skončení učiaceho sa režimu – vyberte režim filtrovania, ktorý bude aktivovaný po ukončení učiaceho sa režimu. Možnosť **Spýtať sa používateľa** vyžaduje oprávnenia správcu, ak chcete vykonávať zmeny režimu filtrovania HIPS.

Systém HIPS monitoruje udalosti vnútri operačného systému a reaguje na ne podľa pravidiel, ktoré sú štruktúrou podobné pravidlám firewallu. Kliknutím na **Upraviť** vedľa položky **Pravidlá** otvoríte editor **pravidiel HIPS**. V tomto okne môžete označiť, pridať, upraviť alebo odstrániť pravidlá. Viac informácií o vytváraní pravidiel a operáciách HIPS nájdete v kapitole Úprava pravidla HIPS.

Interaktívne okno HIPS

Notifikačné okno HIPS vám umožňuje vytvoriť pravidlo na základe nových akcií, ktoré HIPS deteguje, a definovať podmienky, za ktorých bude konkrétna akcia povolená alebo zakázaná.

Pravidlá vytvorené pomocou notifikačného okna sú rovnocenné pravidlám vytvoreným manuálne. Pravidlo vytvorené z notifikačného okna môže byť menej špecifické ako pravidlo, ktoré vyvolalo dané dialógové okno. To znamená, že po vytvorení pravidla v dialógovom okne môže rovnaká operácia vyvolávať rovnaké okno. Viac informácií nájdete v kapitole Manažment pravidiel HIPS.

Ak je akcia v pravidle nastavená na **Vždy sa opýtať**, po spustení pravidla sa zobrazí dialógové okno s výberom možností. Operáciu môžete buď **Zakázať**, alebo **Povoliť**. Ak používateľ nezvolí odpoveď vo vyhradenom čase, vyberie sa na základe pravidiel nová akcia.

Možnosť **Zapamätať si do ukončenia aplikácie** spôsobí, že zvolená akcia (**Povoliť/Zakázať**) bude platná a používaná len do najbližšej zmeny pravidiel, režimu filtrovania, aktualizácie HIPS modulu alebo reštartu systému. Po vykonaní ktorejkoľvek z týchto akcií budú dočasné pravidlá zmazané.

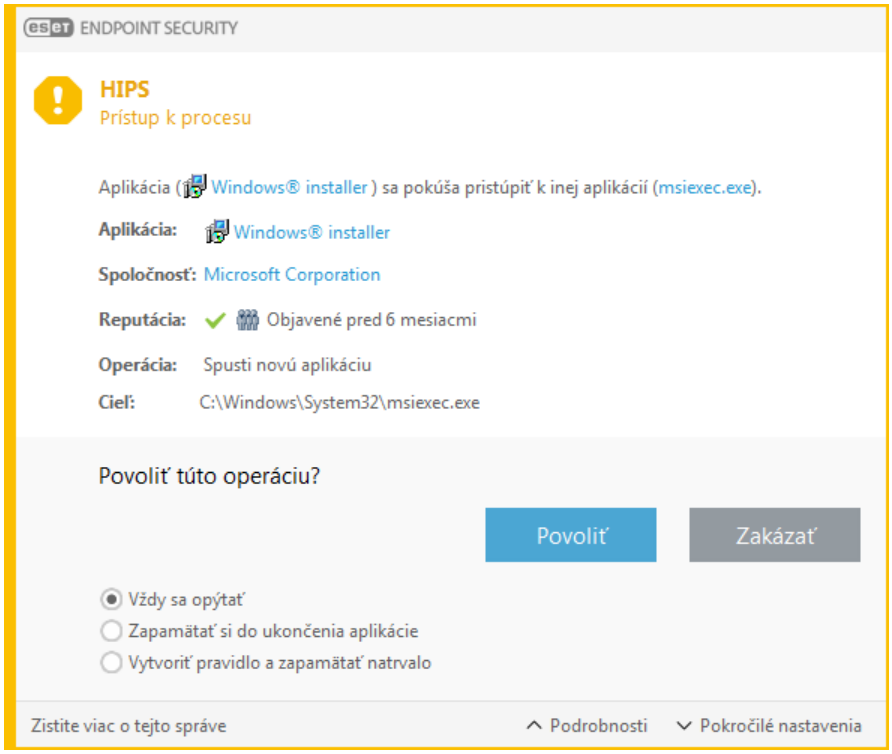
Možnosť **Vytvoriť pravidlo a zapamätať natrvalo** vytvorí nové pravidlo HIPS, ktoré môže byť neskôr zmenené v sekcii Manažment pravidiel HIPS (toto si vyžaduje oprávnenia správcu).

Kliknutím na **Podrobnosti** v dolnej časti zistíte, ktorá aplikácia spúšťa operáciu, aká je reputácia súboru, prípadne aký typ operácie sa chystáte povoliť alebo zakázať.

Nastavenia podrobnejších parametrov pravidla sú dostupné po kliknutí na **Pokročilé možnosti**. Ak vyberiete možnosť **Vytvoriť pravidlo a zapamätať natrvalo**, budú dostupné nasledujúce nastavenia:

- **Pravidlo sa bude týkať len tejto aplikácie** – ak zrušíte označenie tejto možnosti, pravidlo sa vytvorí pre všetky zdrojové aplikácie.
- **Len pre operáciu** – vyberte operáciu pre súbor/aplikáciu/databázu Registry. Popis všetkých operácií HIPS nájdete tu.
- **Len pre cieľ** – vyberte, či bude pravidlo uplatnené pre súbor/aplikáciu/databázu Registry.

Ak chcete zastaviť zobrazovanie oznámení, zmeňte režim filtrovania na **Automatický režim** v časti **Rozšírené nastavenia** (F5) > **Detekčné jadro** > **HIPS** > **Základné**.



Bola zachytená potenciálna aktivita ransomvéru

Toto interaktívne okno sa zobrazí v prípade, že bola zachytená potenciálna aktivita ransomvéru. Operáciu môžete buď **Zakázať**, alebo **Povoliť**.

Kliknutím na **Podrobnosti** zobrazíte konkrétne parametre detekcie. Pomocou dialógového okna môžete súbor **odoslať na analýzu** alebo ho **vylúčiť z detekcie**.

Aby mohla ochrana pred ransomvérom správne fungovať, musí byť aktivovaná služba ESET LiveGrid®.

Manažment pravidiel HIPS

Toto je zoznam používateľských a automaticky vytvorených pravidiel systému HIPS. Viac informácií o vytváraní pravidiel a operáciách HIPS nájdete v kapitole Nastavenie pravidiel HIPS. Prečítajte si tiež kapitolu HIPS (Host-based Intrusion Prevention System).

Stĺpce

Pravidlo – používateľom definovaný alebo automaticky zvolený názov pravidla.

Povolené – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.
Akcia – Pravidlo bližšie špecifikuje akcia – **Povoliť**, **Blokovať** alebo **Spýtať sa** – ktorá bude vykonaná, ak budú splnené podmienky.

Zdroje – pravidlo sa použije iba v prípade, ak bude udalosť spustená aplikáciou.

Ciele – pravidlo sa použije iba v prípade, ak je operácia spojená s konkrétnym súborom, aplikáciou alebo položkou databázy Registry.

Závažnosť zapisovania do protokolu – ak aktivujete túto možnosť, budú informácie o danom pravidle zapisované do protokolu HIPS.

Oznamovať – po každej zodpovedajúcej udalosti sa v pravom dolnom rohu automaticky otvorí malé informačné okno.

Ovládacie prvky

Pridať – pridanie nového pravidla.

Upraviť – úprava zvolených položiek.

Odstrániť – odstránenie zvolených položiek.

Priorita pravidiel HIPS

Nie je možné nastaviť či meniť prioritu HIPS pravidiel pomocou šípok alebo tlačidiel pre zmenu poradia nahor/nadol (ako napr. v prípade pravidiel firewallu, ktoré sú spúšťané smerom zhora nadol).

- Všetky pravidlá, ktoré vytvoríte, majú rovnakú prioritu.
- Čím je pravidlo konkrétnejšie, tým vyššia je jeho priorita (napr. pravidlo pre konkrétnu aplikáciu má vyššiu prioritu ako pravidlo pre všetky aplikácie).
- Interne HIPS obsahuje pravidlá s vyššou prioritou, ku ktorým však nemáte prístup (napr. nie je možné prepísať definované pravidlá Self-Defense).
- Ak vytvoríte pravidlo, ktoré môže spôsobiť zamŕzanie vášho operačného systému, takéto pravidlo sa nebude aplikovať (bude mať najnižšiu prioritu).

Nastavenie pravidiel HIPS

Skôr ako začnete nastavovať pravidlá HIPS, prečítajte si kapitolu Manažment pravidiel HIPS.

Názov pravidla – názov zadaný používateľom alebo automaticky zvolený názov pravidla.

Akcia – špecifikuje akciu (Povoliť, Blokovať alebo Spýtať sa), ktorá sa vykoná, ak budú splnené podmienky pravidla.

Ovplyvnené operácie – vyberte typ operácií, pre ktoré bude pravidlo aplikované. Pravidlo sa uplatní len pre tento typ operácie a pre zvolený cieľ.

Zapnuté – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.

Závažnosť zapisovania do protokolu – ak aktivujete túto možnosť, budú informácie o danom pravidle zapisované do protokolu HIPS.

Upozorniť používateľa – po každej zodpovedajúcej udalosti sa v pravom dolnom rohu automaticky otvorí malé informačné okno.

Pravidlo pozostáva z častí, ktoré popisujú podmienky, za ktorých sa pravidlo spustí:

Zdrojové aplikácie – pravidlo sa uplatní len v prípade, že udalosť vyvolajú vybrané aplikácie. Ak chcete vybrať určité aplikácie, z roletového menu zvoľte **Konkrétne aplikácie** a kliknite na **Pridať**. Ak chcete pridať všetky aplikácie, z roletového menu vyberte **Všetky aplikácie**.

Cieľové súbory – pravidlo sa uplatní len v prípade, že sa operácia týka vybraného cieľa. Ak chcete vybrať určité súbory alebo priečinky, z roletového menu zvoľte **Konkrétne súbory** a kliknite na **Pridať**. Ak chcete pridať všetky súbory, z roletového menu vyberte **Všetky súbory**.

Aplikácie – pravidlo sa uplatní len v prípade, že sa operácia týka tohto cieľa. Ak chcete pridať nové súbory alebo priečinky, z roletového menu vyberte **Konkrétne aplikácie** a kliknite na **Pridať**. Ak chcete pridať všetky aplikácie, z roletového menu vyberte **Všetky aplikácie**.

Položky databázy Registry – pravidlo sa uplatní len v prípade, že sa operácia týka tohto cieľa. Z roletového menu zvoľte **Konkrétne položky** a kliknite na **Pridať** pre pridanie jednotlivých kľúčov databázy Registry. Ak chcete pridať všetky kľúče, vyberte z roletového menu **Všetky položky**.

Niektoré operácie špecifických pravidiel prednastavených modulom HIPS nemôžu byť zablokované a sú na základe predvolených nastavení povolené. Rovnako platí, že HIPS nemonitoruje všetky systémové operácie. HIPS monitoruje tie operácie, ktoré môžu byť nebezpečné.

Pri zadaní cesty C:\example sa pravidlo aplikuje na akcie súvisiace s priečinkom. Zadaním C:\example*.* aplikujete pravidlo na všetky súbory v priečinku.

Aplikačné operácie

- **Ladiť inú aplikáciu** – pripojí ladiaci nástroj (debugger) k procesu. Pri ladení aplikácie sa dá pozorovať alebo meniť jej správanie. Tiež je možné pristupovať k jej dátam.
- **Zachytávať udalosti inej aplikácie** – zdrojová aplikácia sa pokúša zachytiť udalosti cieľovej aplikácie (napríklad, ak sa keylogger snaží zachytiť aktivitu webového prehliadača).
- **Ukončiť/pozastaviť inú aplikáciu** – pozastavenie, obnovenie alebo ukončenie procesu (môže byť vyvolané priamo cez Process Explorer alebo zo záložky Procesy).
- **Spustiť novú aplikáciu** – spustenie novej aplikácie alebo procesu.
- **Zmeniť stav inej aplikácie** – zdrojová aplikácia sa pokúša zapisovať do pamäte cieľovej aplikácie, prípadne sa snaží spustiť kód v jej mene. Táto funkcionalita je užitočná na ochranu dôležitej aplikácie, ak ju nastavíte ako cieľovú aplikáciu pri pravidle, ktoré blokuje tieto operácie.

Na 64-bitových operačných systémoch Windows XP nie je možné zachytávať operácie jednotlivých aplikácií.

Operácie s databázou Registry

- **Zmena nastavení spustenia** – všetky zmeny v nastaveniach definujúcich, ktoré aplikácie budú spúšťané pri štarte operačného systému Windows. Tieto možno vyhľadať napríklad zadaním kľúča Run do vyhľadávania v databáze Registry systému Windows.
- **Vymazanie z databázy Registry** – zmazanie kľúča alebo hodnoty v danom kľúči.
- **Premenovanie kľúča databázy Registry** – premenovanie konkrétneho kľúča.
- **Úprava v databáze Registry** – vytváranie nových hodnôt kľúčov alebo zmena dát asociovaných s hodnotou, zmena umiestnenia dát v rámci stromu databázy a nastavovanie používateľských alebo skupinových práv daného kľúča.

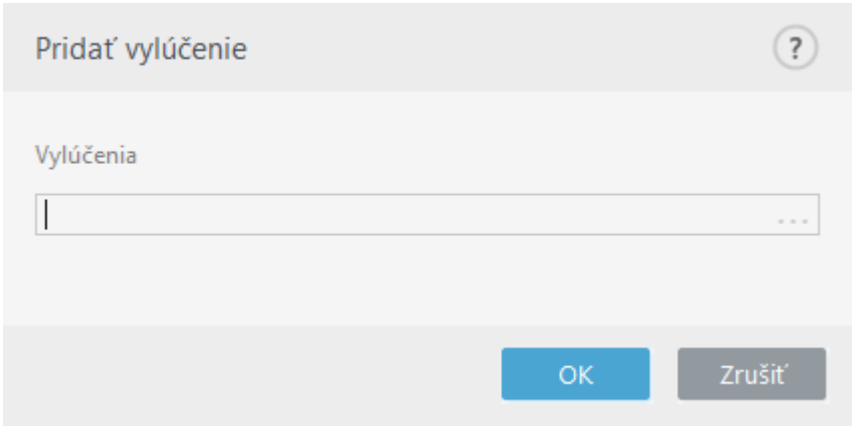
Použitie zástupných znakov v pravidlách
Hviezdičku je možné v pravidlách použiť len na nahradenie konkrétneho kľúča, napr. Hviezdičku je možné v pravidlách použiť len na nahradenie konkrétneho kľúča, napr. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start. Iné spôsoby využitia zástupných znakov nie sú podporované.

Vytváranie pravidiel s kľúčom HKEY_CURRENT_USER
Tento kľúč je len odkazom na príslušný podkľúč v rámci HKEY_USERS, ktorý prislúcha konkrétnemu používateľovi podľa identifikátora SID. Ak chcete vytvoriť pravidlo len pre aktuálneho používateľa, namiesto cesty k HKEY_CURRENT_USER použite cestu k HKEY_USERS\%SID%. Ako SID môžete použiť hviezdičku, čím docielite, aby sa pravidlo aplikovalo na všetkých používateľov.

Ak vytvoríte príliš všeobecné pravidlo, zobrazí sa príslušné upozornenie.

V nasledujúcom príklade si ukážeme, ako obmedziť neželané správanie konkrétnej aplikácie:

1. Zadajte názov pravidla a vyberte možnosť **Blokovať** (alebo **Spýtať sa**, ak si želáte vybrať akciu neskôr) z roletového menu **Akcia**.
2. Zvoľte možnosť **Upozorniť používateľa** pre zobrazenie upozornenia v prípade, že sa pravidlo použije.
3. Vyberte aspoň jednu operáciu v sekcii **Ovplyvnené operácie**, pre ktorú bude pravidlo aplikované.
4. Kliknite na tlačidlo **Ďalej**.
5. V okne **Zdrojové aplikácie** vyberte z roletového menu možnosť **Všetky aplikácie**, aby sa nové pravidlo uplatnilo pre všetky aplikácie, ktoré sa pokúšajú vykonať jednu zo zvolených operácií na vami vybraných aplikáciách.
6. Kliknite na **Pridať**, pomocou **...** následne vyberte cestu ku konkrétnej aplikácii a kliknite na **OK**. V prípade potreby pridajte ďalšie aplikácie.
   Napríklad: *C:\Program Files (x86)\Untrusted application\application.exe*
7. Vyberte operáciu **Zapísať do súboru**.
8. Z roletového menu vyberte možnosť **Všetky súbory**. Týmto sa zablokujú akékoľvek pokusy o zápis do súborov aplikáciou zvolenou v predchádzajúcom kroku.
9. Kliknite na **Dokončiť** pre uloženie pravidla.



Rozšírené nastavenia HIPS

Nasledujúce možnosti sú užitočné pre ladenie (debugovanie) a analýzu správania aplikácií:

Ovládače s povolením vždy sa načítať – vybrané ovládače majú vždy povolené načítanie bez ohľadu na zvolený režim filtrovania, pokiaľ nie sú blokované špecifickým používateľským pravidlom.

Zapisovať všetky zablokované operácie do protokolu – všetky zablokované operácie sa zapíšu do protokolu HIPS. Vzhľadom na značnú veľkosť protokolu a spomalenie počítača pri jeho vytváraní použite túto možnosť, len ak vás na to vyzval pracovník technickej podpory spoločnosti ESET.

Upozorňovať na zmeny v zozname aplikácií automaticky spúšťaných pri štarte – ak pribudne alebo ubudne aplikácia zo zoznamu aplikácií spúšťaných pri štarte, zobrazí sa upozornenie.

Ovládače s povolením vždy sa načítať

Ovládače v tomto zozname majú vždy povolené načítanie bez ohľadu na zvolený HIPS režim filtrovania, pokiaľ nie sú blokované špecifickým používateľským pravidlom.

Pridať – pridať nový ovládač.

Upraviť – upraviť zvolený ovládač.

Zmazať – odstrániť ovládač zo zoznamu.

Obnoviť – načítať len zoznam systémových ovládačov.

Kliknite na **Obnoviť** pre odstránenie ovládačov pridaných používateľom. Táto možnosť je užitočná, ak ste pridali väčší počet ovládačov a neviete ich odstrániť zo zoznamu manuálne.

Prezentačný režim

Prezentačný režim je funkcia určená pre používateľov, ktorí chcú svoj softvér používať neprerušovane a neželajú si byť vyrušovaní oznámeniami a dialógovými oknami, pričom taktiež požadujú minimálne vyťaženie procesora antivírusom. Prezentačný režim je možné použiť aj pri prezentáciách, ktoré nesmú byť prerušené aktivitou antivírusového programu. Po zapnutí prezentačného režimu bude zobrazovanie všetkých notifikácií programu zakázané a naplánované úlohy nebudú spúšťané. Samotná ochrana systému naďalej prebieha na pozadí, ale nevyžaduje žiadne zásahy používateľa.

Kliknite na **Nastavenia** > **Počítač** a potom manuálne zapnite prezentačný režim kliknutím na **Prezentačný režim.** V **Rozšírených nastaveniach** (F5) kliknite na **Nástroje** > **Prezentačný režim** a povoľte možnosť **Automaticky zapnúť prezentačný režim pri spúšťaní aplikácií na celú obrazovku**. ESET Endpoint Security odteraz spustí prezentačný režim vždy, keď sa spustí aplikácia na celú obrazovku. Zapnutie prezentačného režimu môže predstavovať potenciálne bezpečnostné riziko, a preto sa ikonka ochrany na lište zmení na oranžovú. Zobrazí sa tiež oranžové varovné hlásenie v hlavnom okne: **Prezentačný režim je zapnutý**.

Po zvolení možnosti **Automaticky zapnúť prezentačný režim pri spúšťaní aplikácií na celú obrazovku** sa prezentačný režim automaticky zapne po spustení aplikácie na celú obrazovku a po jej zatvorení sa vypne. Táto možnosť je užitočná pre okamžité spustenie prezentačného režimu po spustení aplikácie na celú obrazovku alebo začatí prezentácie.

Môžete tiež označiť možnosť **Automaticky vypnúť prezentačný režim po určenom čase** a zadať požadované časové obdobie (v minútach), po uplynutí ktorého sa Prezentačný režim automaticky vypne.

Ak je firewall v interaktívnom režime a zapnete prezentačný režim, môžu sa vyskytnúť problémy s pripojením na internet. To môže byť problematické, ak napríklad spustíte hru, ktorá sa pripája na internet. Je to spôsobené tým, že za bežných okolností by si firewall vyžiadal používateľské potvrdenie pripojenia (ak nie sú definované žiadne pravidlá alebo výnimky pre spojenia), ale v prezentačnom režime sú všetky vyskakovacie okná vypnuté. Riešením je definovanie pravidiel komunikácie pre každú aplikáciu, ktorá by mohla byť v konflikte s týmto správaním alebo zvoliť iný Režim filtrovania v sekcii Firewall. Majte tiež na pamäti, že ak pri zapnutom prezentačnom režime pracujete s aplikáciou alebo stránkou, ktorá predstavuje potenciálne riziko, bude zablokovaná. Nezobrazí sa však žiadne vysvetlenie alebo varovanie, pretože sú vypnuté všetky akcie vyžadujúce zásah používateľa.

Kontrola pri štarte

Na základe predvolených nastavení programu sa pri štarte systému a počas aktualizácií modulov programu automaticky vykonáva kontrola súborov spúšťaných pri štarte. Táto kontrola závisí od nastavení plánovača a úloh.

Nastavenia tejto kontroly sú súčasťou plánovanej úlohy s názvom **Kontrola súborov spúšťaných pri štarte počítača**. Pre zmenu týchto nastavení kliknite na **Nástroje** > **Plánovač**, označte položku **Kontrola súborov spúšťaných pri štarte počítača** a kliknite na **Upraviť**. V poslednom kroku sa zobrazí okno Kontrola súborov spúšťaných pri štarte počítača (viac informácií nájdete v nasledujúcej kapitole).

Podrobné inštrukcie týkajúce sa vytvárania a správy plánovaných úloh nájdete v časti o vytváraní nových úloh.

Kontrola súborov spúšťaných pri štarte počítača

Pri vytváraní úlohy Kontrola súborov spúšťaných pri štarte počítača v plánovači máte na výber nasledujúce možnosti:

V roletovom menu **Cieľ kontroly** sa určuje hĺbka kontroly súborov spúšťaných pri štarte operačného systému. Ich poradie je určené podľa počtu kontrolovaných súborov:

- **Všetky registrované súbory** (najviac kontrolovaných súborov)
- **Zriedkavo používané súbory**
- **Bežne používané súbory**
- **Často používané súbory**
- **Iba najčastejšie používané súbory** (najmenej kontrolovaných súborov)

Patria sem aj dve špeciálne skupiny:

- **Súbory spúšťané pred prihlásením používateľa** – obsahuje množstvo súborov z umiestnení, z ktorých sa môžu spúšťať súbory bez toho, aby bol používateľ prihlásený (zahŕňa takmer všetky startup lokácie, ako napr. služby, pomocné objekty prehľadávača, winlogon notify, položky plánovača systému Windows, známe dll súbory atď.).
- **Súbory spúšťané po prihlásení používateľa** – obsahuje menšie množstvo súborov z umiestnení, z ktorých sa spúšťajú súbory po prihlásení používateľa (zahŕňa súbory, ktoré sa spúšťajú iba pre daného používateľa, napr. *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Zoznamy súborov na kontrolu sú pre každú skupinu pevne definované.

Priorita kontroly – priorita, s ktorou bude spustená kontrola:

- **Počas nečinnosti** – v momente, keď nie sú vykonávané žiadne iné činnosti.
- **Najnižší** – zaťaženie systému je najnižšie možné,
- **Nižší** – zaťaženie systému je nižšie,
- **Normálny** – zaťaženie systému je normálne,

Ochrana dokumentov

Modul ochrany dokumentov kontroluje dokumenty Microsoft Office pred ich otvorením a kontroluje objekty pri automatickom sťahovaní pomocou programu Internet Explorer, napríklad prvky Microsoft ActiveX. Ochrana dokumentov poskytuje dodatočnú vrstvu ochrany k modulu Rezidentnej ochrany súborového systému. Ochranu dokumentov možno vypnúť s cieľom zvýšiť výkon na systémoch, kde sa nepracuje s veľkým počtom dokumentov balíka Microsoft Office.

Ak chcete aktivovať Ochranu dokumentov, otvorte okno **Rozšírené nastavenia** (stlačením klávesu **F5**), kliknite na **Detekčné jadro** > **Detekcia malvéru** > **Ochrana dokumentov** a kliknite na prepínacie tlačidlo **Zapnúť ochranu dokumentov**.

Tento modul pracuje iba s aplikáciami, ktoré podporujú rozhranie Microsoft Antivirus API (napríklad Microsoft Office 2000 a vyššie verzie alebo Microsoft Internet Explorer 5.0 a vyššie verzie).

Vylúčenia

Vylúčenia vám umožňujú vylúčiť konkrétne objekty z detekčného jadra. Aby bola zabezpečená kontrola všetkých objektov, neodporúčame túto možnosť používať, ak to nie je naozaj nevyhnutné. Môžu však nastať situácie, keď je potrebné niektoré objekty z kontroly vylúčiť, napríklad v prípade veľkých databázových súborov, ktorých kontrola by mohla spomaľovať počítač, prípadne niektorých programov, ktoré by mohli byť v konflikte s priebehom kontroly.

Výkonnostné vylúčenia vám umožňujú vybrať súbory a priečinky, ktoré nemajú byť podrobené kontrole. Výkonnostné vylúčenia sú užitočné, ak chcete z kontroly vylúčiť herné aplikácie na úrovni konkrétnych súborov, ak pri kontrole dochádza k nezvyčajnému správaniu systému, prípadne ak chcete týmto spôsobom zvýšiť výkon.

Vylúčenia detekcií vám umožňujú vylúčiť objekty z liečenia podľa názvu detekcie, cesty k objektu alebo hodnoty hash. Vylúčenia detekcií na rozdiel od výkonnostných vylúčení neslúžia na vylúčenie súborov a priečinkov z kontroly. Vylúčenia detekcií vylúčia iba objekty zachytené detekčným jadrom, pre ktoré sa v zozname vylúčení nachádza zodpovedajúce pravidlo.

Vylúčenia vo verzii 7.1 a starších verziách v sebe zahŕňajú výkonnostné vylúčenia aj vylúčenia detekcií.

Spomenuté vylúčenia si nezamieňajte ani s ďalšími typmi vylúčení:

- Vylúčenia procesov – z kontroly sú vylúčené všetky operácie so súbormi, ktoré sa týkajú vylúčených aplikačných procesov (toto môže byť užitočné pre zvýšenie rýchlosti zálohovania a zlepšenie dostupnosti služieb).
- Prípony súborov vylúčené z kontroly
- HIPS vylúčenia
- Filter vylúčení pre ochranu s podporou cloudu

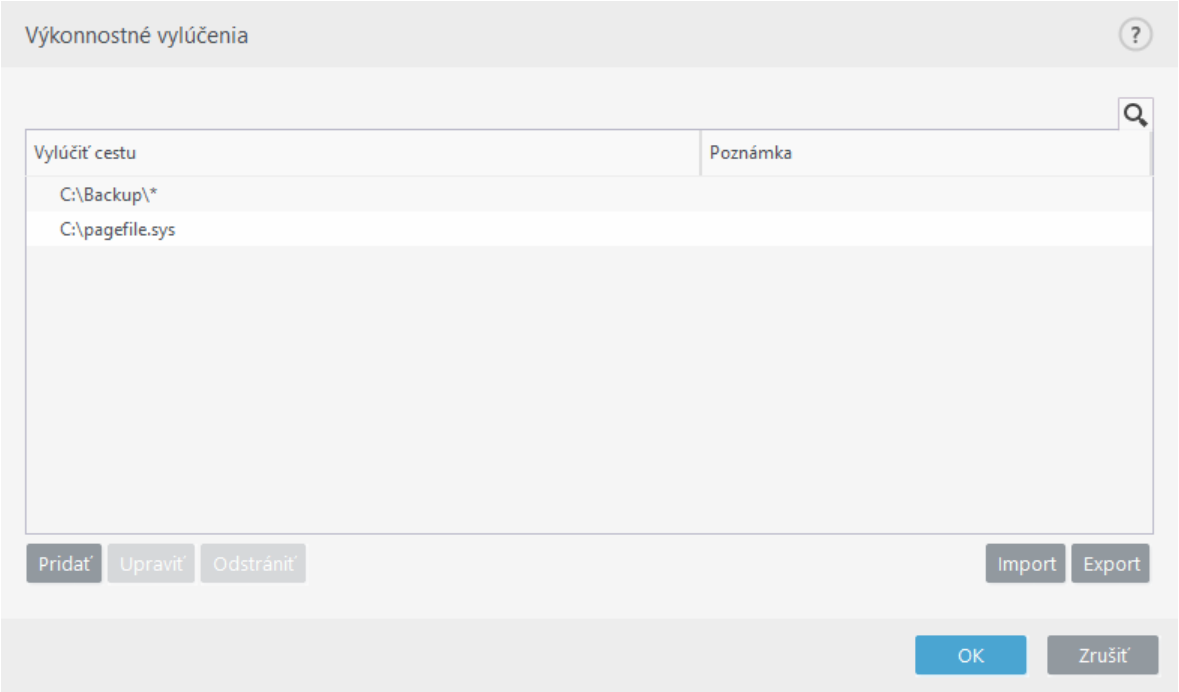
Výkonnostné vylúčenia

Výkonnostné vylúčenia vám umožňujú vybrať súbory a priečinky, ktoré nemajú byť podrobené kontrole.

Za normálnych okolností sa neodporúča nastavovať vylúčenia z kontroly, ak si chcete byť istý, že všetky objekty budú skontrolované na prítomnosť hrozieb. Môžu nastať situácie, keď je potrebné niektoré objekty z kontroly vylúčiť. Napríklad kontrola veľkých databázových súborov môže spomaliť počítač alebo databázový softvér môže byť v konflikte s priebehom kontroly.

Do zoznamu vylúčení môžete pridať súbory a priečinky, a to v sekcii **Rozšírené nastavenia** (F5) > **Detekčné jadro** > **Vylúčenia** > **Výkonnostné vylúčenia** > **Upraviť**.

Ak chcete vylúčiť objekt (cesta: súbor alebo priečinok) z kontroly, kliknite na **Pridať** a zadajte cestu k objektu, prípadne ho označte v stromovej štruktúre.



Ak súbor spĺňa kritériá vylúčenia z kontroly, moduly **Rezidentná ochrana súborového systému** a **Kontrola počítača** nebudú hrozbu v takomto súbore detegovať.

Ovládacie prvky

- **Pridať** – pridanie novej položky do zoznamu objektov vylúčených z kontroly.
- **Upraviť** – úprava zvolených položiek.
- **Odstrániť** – odstránenie zvolených položiek (pri podržaní klávesu CTRL môžete kliknutím označiť viacero položiek).
- **Import/Export** – import a export výkonnostných vylúčení je užitočný napríklad pri zálohovaní aktuálnych vylúčení, ku ktorým sa chce používateľ neskôr vrátiť. Export nastavení ďalej určite ocenia používatelia v nespravovaných prostrediach, ktorí potrebujú použiť jednotné nastavenia na viacerých počítačoch, kde do nainštalovaného programu jednoducho importujú súbor .txt s nastaveniami.
  Príklad formátu súboru na import/export

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManageme
nt.PerformanceExclusions","columns":["Path","Description"]}

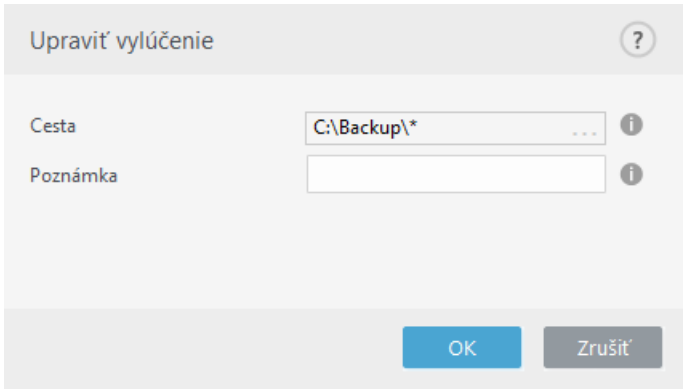
C:\Backup\*,custom comment

C:\pagefile.sys
```

Pridanie alebo úprava výkonnostných vylúčení

V tomto dialógovom okne môžete vylúčiť konkrétnu cestu (k súboru alebo adresáru) v rámci počítača.

Požadovanú cestu zvolíte kliknutím na **...** v poli **Cesta**.
V prípade manuálneho zadávania si pozrite príklady formátov vylúčení uvedené nižšie.



Pri vylúčení súborov z kontroly môžu byť použité zástupné znaky pre pokrytie skupiny súborov. Otáznik (*?*) slúži na nahradenie jedného ľubovoľného znaku a hviezdička (***) nahrádza ľubovoľný reťazec v dĺžke nula až niekoľko znakov.

- Ak chcete vylúčiť vo zvolenom adresári všetky súbory a podpriečinky, zadajte cestu k adresáru a použite masku ***
- V prípade vylúčenia všetkých súborov .doc použite masku **.doc*
- Ak má názov spustiteľného súboru určitý počet znakov a vy viete s istotou len začiatočný znak (napr. „D“), použite nasledujúci formát:
D????.exe (otázniky zastupujú chýbajúce/neznáme znaky)

Príklady:
- *C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (*), ak má označovať, že ide o priečinok a všetok jeho obsah (súbory a podpriečinky) bude vylúčený.
- *C:\Tools*.** – funguje rovnako ako *C:\Tools**
- *C:\Tools* – priečinok *Tools* nebude vylúčený. Z pohľadu kontroly by totiž *Tools* mohol byť aj názov súboru.
- *C:\Tools*.dat* – budú vylúčené súbory .dat v priečinku *Tools*.
- *C:\Tools\sg.dat* – bude vylúčený tento konkrétny súbor v danom umiestnení.

Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné ako *%PROGRAMFILES%*.
• Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%** (nezabudnite na spätnú lomku a hviezdičku na konci).
• Ak chcete vylúčiť všetky súbory a priečinky v konkrétnom podadresári v rámci *%PROGRAMFILES%*, použite cestu *%PROGRAMFILES%\Vyluceny_podadresar**

Rozbaliť zoznam podporovaných systémových premenných

Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nie sú podporované premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*).

Používanie zástupných znakov uprostred zadávanej cesty (napríklad *C:\Tools*\Data\file.dat*), môže fungovať, ale pre výkonnostné vylúčenia nie je oficiálne podporované. Prečítajte si náš článok Databázy znalostí, kde nájdete podrobnejšie informácie.
V prípade vylúčení detekcií neplatia žiadne obmedzenia pre používanie zástupných znakov uprostred zadávanej cesty.

Poradie vylúčení:
• Prioritu vylúčení nie je možné nastaviť či meniť pomocou šípok alebo tlačidiel nahor/nadol (ako napr. v prípade pravidiel firewallu, ktoré sú spúšťané smerom zhora nadol).
• Keď sa pri kontrole uplatní prvé zodpovedajúce pravidlo, ďalšie pravidlo nebude vyhodnocované.
• Čím menej pravidiel, tým lepší výkon kontroly.
• Vyhnite sa vytváraniu súbežných pravidiel.

Formát vylúčenia cesty

Pri vylúčení súborov z kontroly môžu byť použité zástupné znaky pre pokrytie skupiny súborov. Otáznik (*?*) slúži na nahradenie jedného ľubovoľného znaku a hviezdička (***) nahrádza ľubovoľný reťazec v dĺžke nula až niekoľko znakov.

• Ak chcete vylúčiť vo zvolenom adresári všetky súbory a podpriečinky, zadajte cestu k adresáru a použite masku *
• V prípade vylúčenia všetkých súborov .doc použite masku **.doc*
• Ak má názov spustiteľného súboru určitý počet znakov a vy viete s istotou len začiatočný znak (napr. „D“), použite nasledujúci formát:
D????.exe (otázniky zastupujú chýbajúce/neznáme znaky)
Príklady:
• *C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (*), ak má označovať, že ide o priečinok a všetok jeho obsah (súbory a podpriečinky) bude vylúčený.
• *C:\Tools*.** – funguje rovnako ako *C:\Tools**
• *C:\Tools* – priečinok *Tools* nebude vylúčený. Z pohľadu kontroly by totiž *Tools* mohol byť aj názov súboru.
• *C:\Tools*.dat* – budú vylúčené súbory .dat v priečinku *Tools*.
• *C:\Tools\sg.dat* – bude vylúčený tento konkrétny súbor v danom umiestnení.

Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné ako *%PROGRAMFILES%*.
• Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%** (nezabudnite na spätnú lomku a hviezdičku na konci).
• Ak chcete vylúčiť všetky súbory a priečinky v konkrétnom podadresári v rámci *%PROGRAMFILES%*, použite cestu *%PROGRAMFILES%\Vyluceny_podadresar**

Rozbaliť zoznam podporovaných systémových premenných

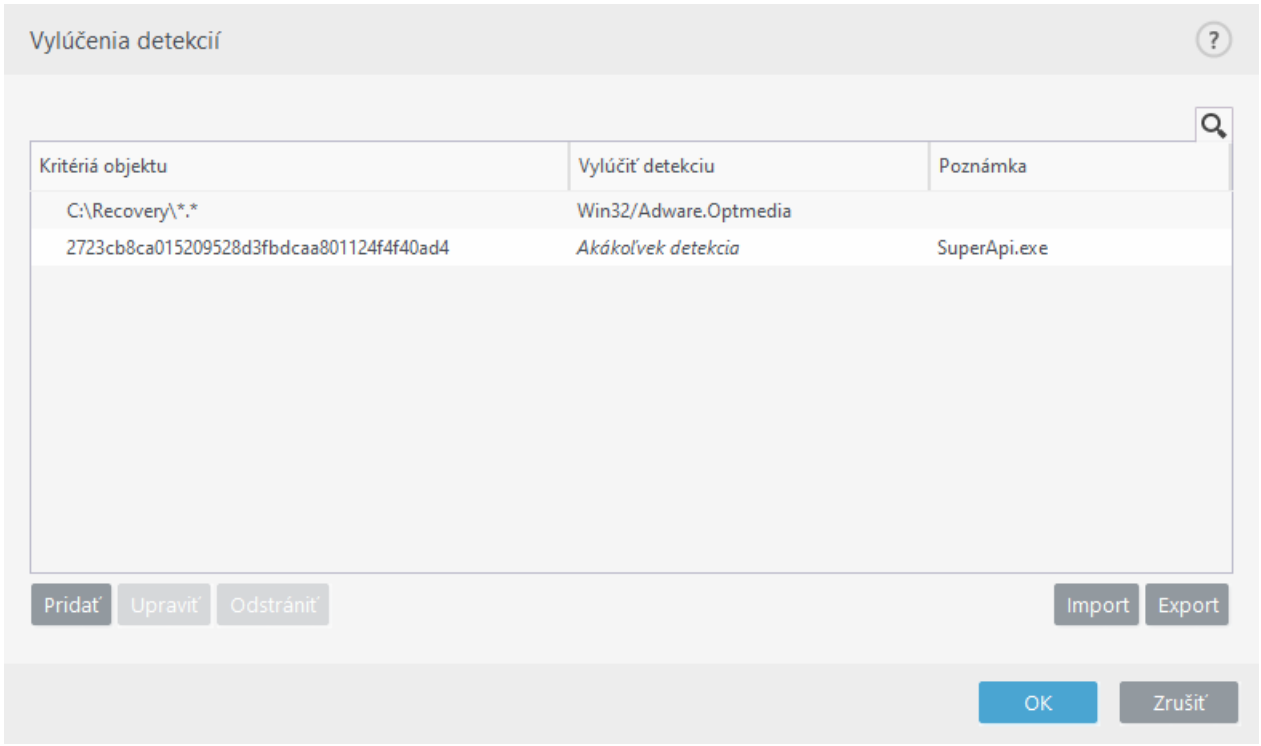
Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:
• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nie sú podporované premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*).

Vylúčenia detekcií

Vylúčenia detekcií umožňujú vylúčiť objekty z liečenia filtrovaním názvu detekcie, cesty k objektu alebo hodnoty hash.

Vylúčenia detekcií na rozdiel od výkonnostných vylúčení neslúžia na vylúčenie súborov a priečinkov z kontroly. Vylúčenia detekcií vylúčia iba objekty zachytené detekčným jadrom, pre ktoré sa v zozname vylúčení nachádza zodpovedajúce pravidlo.
Napríklad podľa prvého riadku na obrázku nižšie, ak je objekt detegovaný ako Win32/Adware.Optmedia a cesta k detegovanému súboru je *C:\Recovery\file.exe*, tento súbor bude vylúčený z detekčného jadra. Druhý riadok znamená, že každý súbor, ktorý má zhodujúci sa hash SHA-1, bude vždy vylúčený bez ohľadu na názov detekcie.



Aby bolo zabezpečené zachytávanie všetkých hrozieb, odporúčame vylúčenia detekcií vytvárať len v tom prípade, že je to naozaj nevyhnutné.

Ak chcete do zoznamu vylúčení pridať súbory a priečinky, prejdite do sekcie **Rozšírené nastavenia** (F5) > **Detekčné jadro** > **Vylúčenia** > **Vylúčenia detekcií** > **Upraviť**.

Ak chcete vylúčiť objekt (podľa názvu detekcie alebo hodnoty hash) z liečenia, kliknite na **Pridať**.

Pre potenciálne nechcené aplikácie a potenciálne nebezpečné aplikácie je možné vytvoriť vylúčenie podľa názvu detekcie aj nasledujúcim spôsobom:

- Vo výstražnom okne informujúcom o detekcii kliknite na **Zobraziť pokročilé možnosti** a vyberte možnosť **Vylúčiť z detekcie**.
- V kontextovom menu v okne Protokoly použite Sprievodcu vytvorením vylúčenia detekcie.
- V hlavnom okne programu v časti **Nástroje** > **Karanténa** kliknite pravým tlačidlom myši na súbor v karanténe a v kontextovom menu označte možnosť **Obnoviť a vylúčiť z kontroly**.

Kritériá pre vylúčenie detegovaného objektu

- **Cesta** – umožňuje obmedziť vylúčenie len na konkrétnu cestu.
- **Názov detekcie** – ak je vedľa vylúčeného súboru zobrazený názov detekcie, znamená to, že súbor je vylúčený z kontroly len pre danú detekciu, nie ako celok. Ak by teda došlo k infikovaniu takto vylúčeného súboru iným malvérom, ten bude detekčným jadrom riadne zachytený.
- **Hash** – môžete vylúčiť konkrétny súbor na základe jeho hashu (SHA-1) bez ohľadu na typ súboru, umiestnenie, názov alebo súborovú príponu.

Ovládacie prvky

- **Pridať** – pridanie novej položky do zoznamu objektov vylúčených z liečenia.

- **Upraviť** – úprava zvolených položiek.
- **Odstrániť** – odstránenie zvolených položiek (pri podržaní klávesu CTRL môžete kliknutím označiť viacero položiek).
- **Import/Export** – import a export vylúčení detekcií je užitočný napríklad pri zálohovaní aktuálnych vylúčení, ku ktorým sa chce používateľ neskôr vrátiť. Export nastavení ďalej určite ocenia používatelia v nespravovaných prostrediach, ktorí potrebujú použiť jednotné nastavenia na viacerých počítačoch, kde do nainštalovaného programu jednoducho importujú súbor .txt s nastaveniami.
  Príklad formátu súboru na import/export

```
# {"product":"endpoint","version":"9.1.2060","path":"Settings.ExclusionsManageme
nt.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileH
ash"]}

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

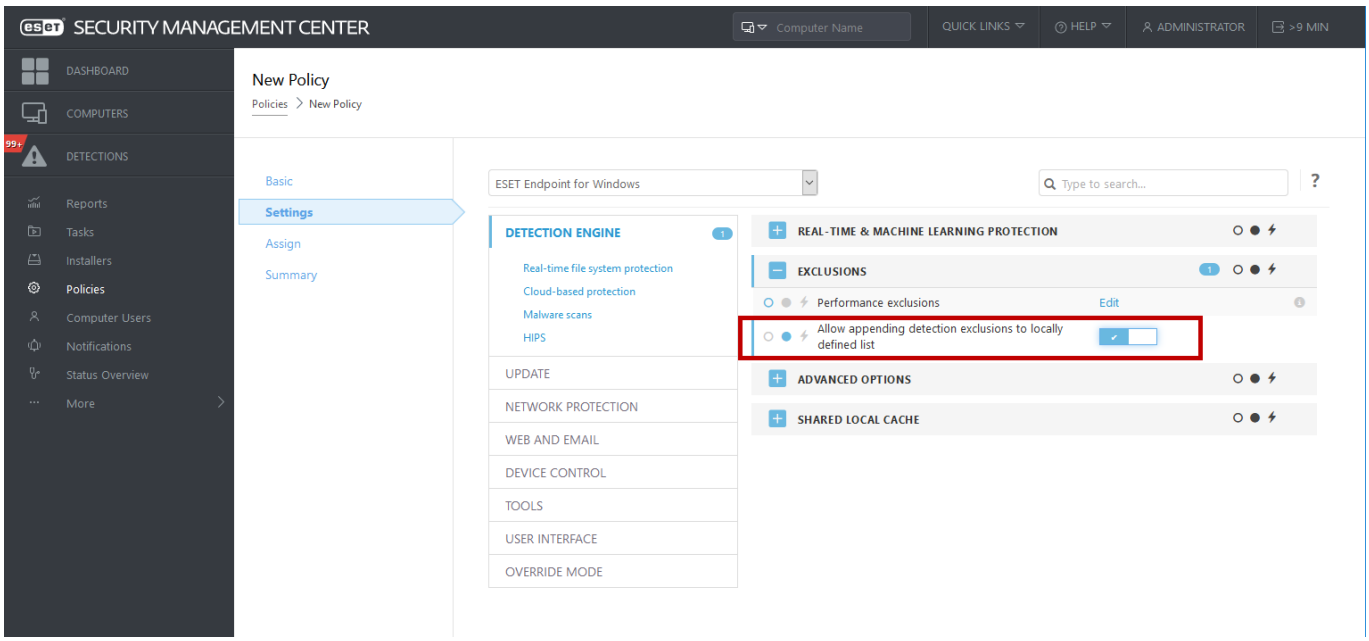
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

Nastavenie vylúčenia detekcie v ESET PROTECT

ESET PROTECT 8.0 obsahuje nového sprievodcu na spravovanie vylúčení detekcií – umožňuje vytvoriť vylúčenie detekcie a uplatniť ho na viacero počítačov/skupín.

Možné prepísanie vylúčení detekcií z ESET PROTECT

Ak na pracovnej stanici existuje lokálny zoznam vylúčení detekcií, správca musí použiť politiku s nastavením **Povoliť pridanie vylúčení detekcií do lokálnych zoznamov**. Až následne bude pridávanie vylúčení detekcií z ESET PROTECT fungovať podľa očakávaní.

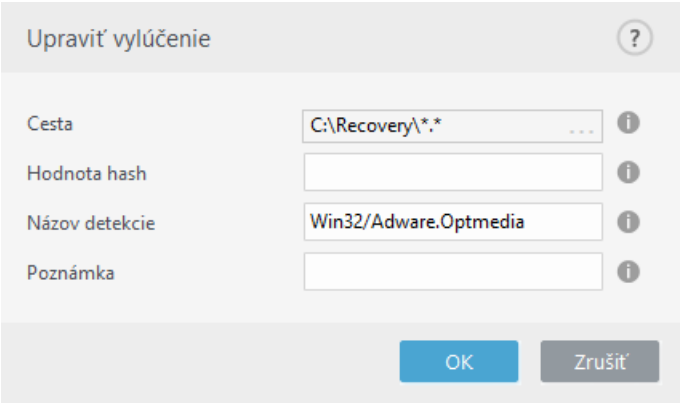


Pridanie alebo úprava vylúčení detekcií

Vylúčenie detekcie

Mali by ste zadávať platný názov, pod ktorým ESET zachytil detekciu. Tento názov nájdete v sekcii Protokoly po zvolení možnosti **Detekcie** z roletového menu Protokoly. Takéto vylúčenie môže byť užitočné napríklad v prípade, že v programe ESET Endpoint Security dôjde k nesprávnej detekcii vzorky (falošný poplach). Vylúčenie skutočných infiltrácií je však veľmi nebezpečné, zvážte preto vylúčenie len zasiahnutých súborov/adresárov kliknutím na **...** v poli **Cesta** a/alebo vytvorte vylúčenie len na dočasné obdobie. Vylúčenia je možné vytvárať aj pre potenciálne nechcené aplikácie, potenciálne nebezpečné aplikácie a podozrivé aplikácie.

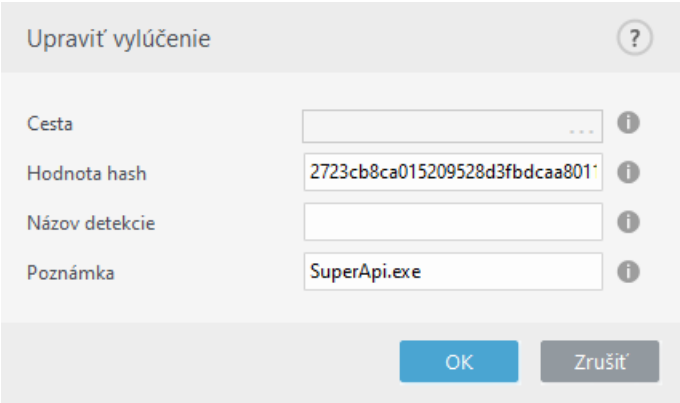
Prečítajte si tiež Formát vylúčenia cesty.



Pozrite si tiež príklad vylúčenia detekcie nižšie.

Vylúčiť hash

Umožní vám vylúčiť konkrétny súbor na základe jeho hashu (SHA-1) bez ohľadu na typ súboru, umiestnenie, názov alebo súborovú príponu.



Ak chcete vylúčiť konkrétnu detekciu podľa jej názvu, zadajte platný názov danej detekcie: *Win32/Adware.Optmedia*
Ak vytvárate vylúčenie detekcie z okna upozornenia, ktoré zobrazil ESET Endpoint Security, môžete použiť aj nasledujúci formát:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Ovládacie prvky

- **Pridať** – pridanie objektu na vylúčenie z detekcie.
- **Upraviť** – úprava zvolených položiek.
- **Odstrániť** – odstránenie zvolených položiek (pri podržaní klávesu CTRL môžete kliknutím označiť viacero položiek).

Sprievodca vytvorením vylúčenia detekcie

Vylúčenie detekcie je možné vytvoriť aj z kontextového menu v okne Protokoly (táto možnosť nie je dostupná pre detekcie malvéru):

1. V hlavnom okne programu kliknite na **Nástroje** > **Protokoly**.
2. Kliknite pravým tlačidlom myši na zvolený detegovaný objekt v protokole s názvom **Detekcie**.
3. Kliknite v kontextovom menu na možnosť **Vytvoriť vylúčenie**.

Pre vylúčenie jednej alebo viacerých detekcií na základe **Kritérií vylúčenia** kliknite na možnosť **Zmeniť kritériá**:

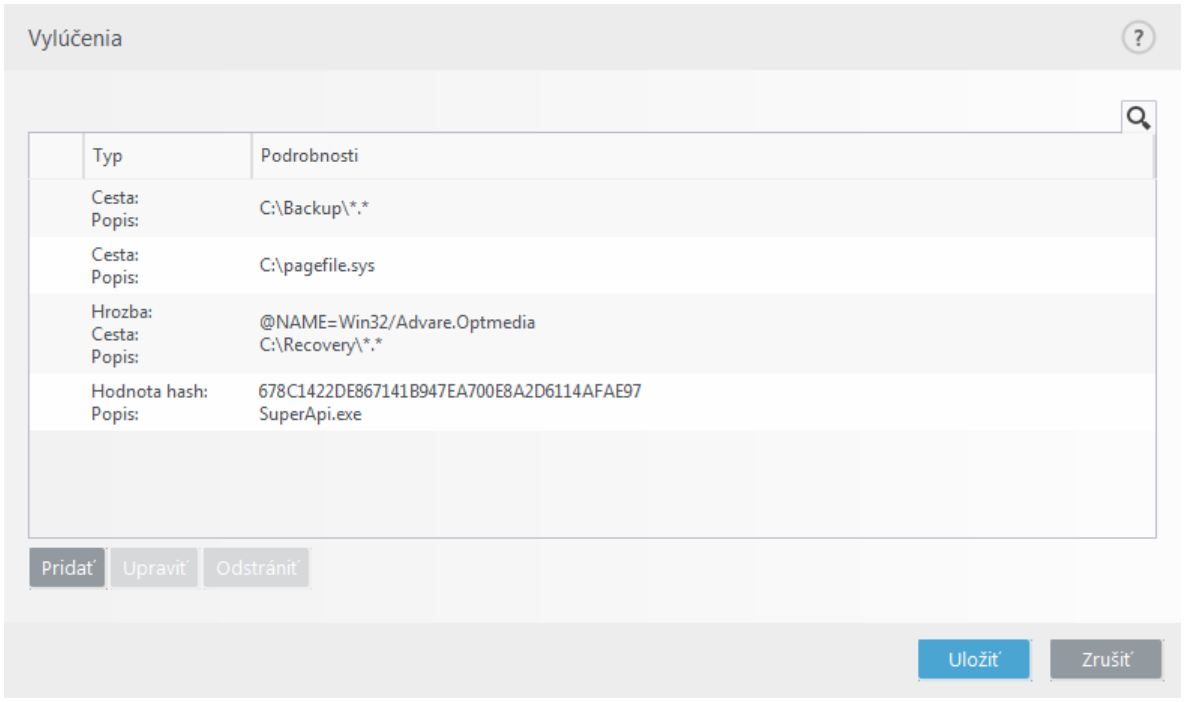
- **Konkrétne súbory** – vylúči sa každý súbor podľa jeho hodnoty SHA-1 hash.
- **Detekcia** – vylúči sa každý súbor podľa názvu detekcie.
- **Cesta + detekcia** – vylúči sa každý súbor podľa názvu detekcie a cesty vrátane názvu súboru (napr. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Odporúčaná možnosť je prednastavená na základe typu detekcie.

Pred kliknutím na tlačidlo **Vytvoriť vylúčenie** môžete voliteľne pridať aj **Poznámku**.

Vylúčenia (7.1 a staršie verzie)

Vylúčenia vo verzii 7.1 a starších verziách v sebe zahŕňajú výkonnostné vylúčenia aj vylúčenia detekcií.



Vylúčenia procesov

Funkcia Vylúčenia procesov vám umožňuje vylúčiť procesy aplikácií z Rezidentnej ochrany súborového systému. Na zvýšenie rýchlosti zálohovania a vylepšenie integrity procesov a dostupnosti služieb sa počas zálohovania používajú niektoré techniky, ktoré sú v konflikte s antimalvérovou ochranou súborového systému. Podobné problémy môžu nastať pri živej migrácii virtuálnych počítačov. Jediným efektívnym riešením v oboch prípadoch je deaktivácia antimalvérového softvéru. Vylúčením konkrétneho procesu (napr. procesu zálohovacieho riešenia) budú všetky jeho operácie so súbormi ignorované a považované za bezpečné, čím sa minimalizuje interferencia s procesom zálohovania. Pri vytváraní vylúčení odporúčame byť opatrný – zálohovací nástroj, ktorý bol vylúčený, môže pristupovať k infikovaným súborom bez toho, aby sa spustilo upozornenie, čo je dôvod, prečo sú rozšírené povolenia povolené iba v module rezidentnej ochrany.

Vylúčenia procesov pomáhajú minimalizovať riziko potenciálnych konfliktov a zvýšiť výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie príslušného spustiteľného súboru (*.exe*).

Spustiteľné súbory môžete pridať do zoznamu vylúčených procesov cez **Rozšírené nastavenia** (F5) > **Detekčné jadro** > **Rezidentná ochrana súborového systému** > **Vylúčenia procesov**.

Táto funkcia bola navrhnutá tak, aby vylúčila z kontroly zálohovacie nástroje. Vylúčenie procesu zálohovacieho nástroja z kontroly nielen zabezpečuje stabilitu systému, ale taktiež nemá negatívny vplyv na rýchlosť zálohy, keďže počas spustenia zálohy nedochádza k jej spomaľovaniu.

Kliknite na **Upraviť** pre otvorenie okna **Vylúčenia procesov**, v ktorom môžete pridať vylúčenie a vyhľadať spustiteľný súbor (napr. *Backup-tool.exe*), ktorý chcete vylúčiť z kontroly.
Hneď ako pridáte súbor *.exe* do vylúčení, aktivita príslušného procesu viac nebude monitorovaná programom ESET Endpoint Security a nebudú kontrolované žiadne operácie so súbormi, ktoré tento proces vykoná.

Ak pri výbere spustiteľného súboru nepoužijete funkciu určenú na prehľadávanie, budete musieť k danému súboru manuálne zadať úplnú cestu. V opačnom prípade vylúčenie nebude fungovať správne a HIPS môže hlásiť chyby.

Existujúce vylúčené procesy môžete **upravovať** alebo ich **odstrániť** z vylúčení.

Ochrana prístupu na web neberie takéto vylúčenie do úvahy, preto v prípade, že vylúčite z kontroly spustiteľný súbor vášho webového prehliadača, sťahované súbory budú aj naďalej kontrolované. Vďaka tomu je stále možné zachytiť prípadné infiltrácie. Tento scenár slúži len ako príklad a neodporúčame vytvárať vylúčenia pre webové prehliadače.

Pridanie alebo úprava vylúčení procesov

Toto dialógové okno vám umožňuje **pridať** procesy, ktoré majú byť vylúčené z kontroly detekčným jadrom. Vylúčenia procesov pomáhajú minimalizovať riziko potenciálnych konfliktov a zvýšiť výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie príslušného spustiteľného súboru (*.exe*).

Nastavte cestu k spustiteľnému súboru aplikácie, ktorú chcete vylúčiť z kontroly, kliknutím na ... (napr. *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
Hneď ako pridáte súbor *.exe* do vylúčení, aktivita príslušného procesu viac nebude monitorovaná programom ESET Endpoint Security a nebudú kontrolované žiadne operácie so súbormi, ktoré tento proces vykoná.

Ak pri výbere spustiteľného súboru nepoužijete funkciu určenú na prehľadávanie, budete musieť k danému súboru manuálne zadať úplnú cestu. V opačnom prípade vylúčenie nebude fungovať správne a HIPS môže hlásiť chyby.

Existujúce vylúčené procesy môžete **upravovať** alebo ich **odstrániť** z vylúčení.

HIPS vylúčenia

Tieto vylúčenia vám umožňujú vyňať konkrétne procesy z hĺbkovej behaviorálnej kontroly v rámci systému HIPS.

Pre vylúčenie objektu kliknite na **Pridať** a zadajte cestu k objektu, prípadne ho označte v stromovej štruktúre. Môžete tiež **Upraviť** alebo **Odstrániť** vybrané položky.

Prečítajte si kapitolu Vylúčenia.

Parametre ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácií. Táto technológia je proaktívna, takže poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. K odhaleniu hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické signatúry, generické a vírusové definície), čím efektívne spája ich výhody. Detekčné jadro je schopné kontrolovať niekoľko dátových tokov paralelne, a tak maximalizovať rýchlosť a účinnosť detekcie. Technológia ThreatSense dokáže úspešne eliminovať aj rootkity.

Nastavenia ThreatSense vám umožňujú špecifikovať viacero parametrov kontroly:

- typy súborov a prípony, ktoré sa majú kontrolovať,
- kombinácie rôznych metód detekcie,
- úrovne liečenia atď.

Pre zobrazenie okna s nastaveniami kliknite na **Parametre ThreatSense** v Rozšírených nastaveniach príslušných modulov využívajúcich technológiu ThreatSense (pozrite nižšie). Pre rôzne druhy ochrany sa používa rôzna úroveň nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

- Rezidentná ochrana súborového systému
- Kontrola v nečinnosti
- Kontrola pri štarte
- Ochrana dokumentov
- Ochrana e mailových klientov
- Ochrana prístupu na web
- Kontrola počítača

Parametre ThreatSense sú pre každý modul odlišné. Zmeny v nastavení týchto parametroch môžu výrazne ovplyvniť celkový výkon systému. Príkladom môže byť povolenie pokročilej heuristiky v rámci modulu rezidentnej ochrany súborového systému a voľba vždy kontrolovať runtime archívy, čo môže viesť k spomaleniu systému (pri predvolenom nastavení sú pri týchto metódach kontrolované iba novovytvorené súbory). Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky moduly ochrany okrem Kontroly počítača.

Objekty na kontrolu

Sekcia Objekty na kontrolu umožňuje nastaviť, ktoré komponenty počítača a súborového systému budú testované na prítomnosť infiltrácie.

Operačná pamäť – slúži na kontrolu prítomnosti hrozieb, ktoré môžu byť zavedené v operačnej pamäti počítača.

Zavádzacie sektory/UEFI – kontroluje zavádzacie sektory na prítomnosť malvéru v hlavnom zavádzacom zázname. Viac o UEFI sa dočítate v slovníku pojmov.

E-mailové súbory – program podporuje nasledujúce prípony súborov: DBX (Outlook Express) a EML.

Archívy – program podporuje nasledujúce prípony: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a mnoho ďalších.

Samorozbaľovacie archívy – archívy, ktoré nepotrebujú pre svoje rozbalenie iné programy. Ide o SFX (self-extracting) archívy.

Runtime archívy – runtime archívy sa na rozdiel od štandardných archívov po spustení rozbalia v pamäti počítača. Okrem štandardných statických archívov (UPX, yoda, ASPack, FSG atď.) dokáže program rozpoznať vďaka emulácii kódu aj veľa iných typov archívov.

Možnosti kontroly

V tejto sekcii môžete nastaviť, ktoré metódy detekcie sa použijú pri kontrole systému na prítomnosť infiltrácií. K dispozícii sú nasledujúce možnosti:

Heuristika – heuristika je algoritmus, ktorý analyzuje (škodlivú) aktivitu programov. Výhodou heuristiky je schopnosť odhaliť aj taký škodlivý softvér, ktorý v dobe poslednej aktualizácie modulu detekčného jadra programu ešte neexistoval alebo nebol pokrytý. Nevýhodou je (veľmi malá) pravdepodobnosť „falošného poplachu“.

Pokročilá heuristika/DNA vzorky – pokročilá heuristika je jedinečný algoritmus vyvinutý spoločnosťou ESET, ktorý je optimalizovaný pre odhaľovanie počítačových červov a trójskych koní písaných vo vyšších programovacích jazykoch. Použitie pokročilej heuristiky značne zvyšuje možnosti rozpoznávania vírusov a malvéru. Vzorky umožňujú spoľahlivo odhaliť a identifikovať nové vírusy. Vďaka pravidelnej aktualizácii sú nové

vzorky k dispozícii zvyčajne už do niekoľkých hodín od objavenia hrozby. Nevýhodou je, že táto metóda odhaľuje iba vírusy na základe známych vzoriek, prípadne ich čiastočne pozmenené verzie.

Liečenie

Nastavenia liečenia určujú správanie programu ESET Endpoint Security pri čistení infikovaných súborov.

Vylúčenia

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Iné

V rámci konfigurácie parametrov ThreatSense pre Manuálnu kontrolu počítača sú v sekcii **Iné** k dispozícii aj nasledujúce možnosti:

Kontrolovať alternatívne dátové prúdy (ADS) – alternatívne dátové prúdy používané systémom NTFS sú asociácie k súborom a adresárom, ktoré sú pre bežné spôsoby kontroly neviditeľné. Veľký počet vírusov ich preto využíva na svoje maskovanie a ukrytie sa pred prípadným odhalením.

Kontroly na pozadí vykonávať s nízkou prioritou – každá kontrola počítača využíva isté množstvo systémových prostriedkov. Ak práve pracujete s programami náročnými na výkon počítača, presunutím kontroly na pozadie jej môžete priradiť nižšiu prioritu a získať tým viac systémových prostriedkov pre svoje aplikácie.

Zapisovať všetky objekty do protokolu – protokol kontroly zobrazí všetky skontrolované súbory v samorozbaľovacích archívoch, a to aj súbory, ktoré neboli infikované (môže tak dochádzať ku generovaniu veľkého množstva dát a viesť k veľkému súboru protokolu kontroly).

Zapnúť Smart optimalizáciu – pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia na zabezpečenie najefektívnejšej úrovne kontroly pri zachovaní najvyššej možnej rýchlosti kontroly. Moduly ochrany pri kontrole dômyselne využívajú rozdielne metódy kontroly na rôzne typy súborov. Ak je Smart optimalizácia vypnutá, pri kontrole sú použité len používateľské nastavenia jadra ThreatSense pre konkrétne moduly.

Zachovať čas posledného prístupu k súborom – pri kontrole súboru nebude zmenený čas prístupu, ale bude ponechaný pôvodný (vhodné pri používaní zálohovacích systémov).

Obmedzenia

V sekcii Obmedzenia nastavíte maximálnu veľkosť kontrolovaných objektov a maximálnu hĺbku kontroly v archívoch.

Nastavenie objektov

Maximálna veľkosť objektu – definuje maximálnu veľkosť skenovaného objektu. Daný modul antivírusu bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame meniť len pokročilým používateľom, ktorí chcú veľké objekty z určitého dôvodu vylúčiť z kontroly. Predvolená hodnota: neobmedzené.

Maximálny čas kontroly objektu (v sekundách) – definuje maximálny povolený čas na kontrolu súborov v objekte kontajnera (napr. archívy RAR/ZIP alebo e□mail s viacerými prílohami). Toto nastavenie sa netýka samostatných

súborov. Ak používateľ zadefinuje určitú hodnotu, po prekročení uvedeného času sa prebiehajúca kontrola skončí bez ohľadu na to, či bol skontrolovaný každý súbor v objekte kontajnera. V prípade archívu s veľkými súbormi sa kontrola zastaví až po extrahovaní súboru z archívu (napríklad keď používateľ zadefinuje premennú 3 sekundy, ale extrakcia súboru trvá 5 sekúnd). Po uplynutí tohto času sa zostávajúce súbory v archíve nebudú kontrolovať. Na obmedzenie času kontroly (aj v prípade väčších archívov) použite možnosť **Maximálna veľkosť objektu** a **Maximálna veľkosť súboru v archíve** (neodporúča sa z dôvodu možných bezpečnostných rizík). Predvolená hodnota: neobmedzené.

Nastavenie kontroly archívov

Úroveň vnorenia archívov – špecifikuje maximálny počet vnorených archívov, do ktorého bude prebiehať antivírusová kontrola. Predvolená hodnota: 10.

Maximálna veľkosť súboru v archíve – špecifikuje maximálnu veľkosť rozbaleného súboru v archíve, ktorý sa má kontrolovať. Maximálna hodnota je 3 GB.

Neodporúčame meniť predvolené hodnoty, za normálnych okolností nie je žiadny dôvod na ich zmenu.

Úrovne liečenia

Nastavenia úrovne liečenia pre požadovaný modul ochrany sú dostupné v sekcii **Parametre ThreatSense** (napríklad v rámci **Rezidentnej ochrany súborového systému**) > **Liečenie**.

Rezidentná ochrana a ďalšie moduly ochrany ponúkajú nasledujúce úrovne liečenia.

Liečenie v produkte ESET Endpoint Security 9

Úroveň liečenia	Popis
Vždy vyriešiť detekciu	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých zriedkavých prípadoch (napríklad pri systémových súboroch), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení. **Vždy vyriešiť detekciu** je odporúčané predvolené nastavenie pre spravované prostredia.
Vyriešiť detekciu a ak to nie je možné, ponechať ju	Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany koncového používateľa. V niektorých prípadoch (napríklad pri systémových súboroch alebo archívoch s infikovanými aj neškodnými súbormi), keď liečenie nie je možné vykonať, sa detegovaný objekt ponechá v pôvodnom umiestnení.
Vyriešiť detekciu a ak to nie je možné, spýtať sa	Program sa pokúsi o liečenie detegovaného objektu. V niektorých prípadoch, keď nie je možné vykonať žiadnu akciu, sa koncovému používateľovi zobrazí interaktívne upozornenie, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Toto nastavenie sa odporúča vo väčšine prípadov.
Vždy sa spýtať koncového používateľa	Koncovému používateľovi sa pri liečení objektov zobrazí interaktívne okno, v ktorom si musí zvoliť požadovanú akciu (napríklad odstrániť alebo ignorovať detegovaný objekt). Táto úroveň liečenia je určená pre pokročilých používateľov, ktorí vedia, ako postupovať pri detekciách.



Prípony súborov vylúčené z kontroly

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense zvolíte, ktoré typy súborov budú kontrolované.

Spomenuté vylúčenia si nezamieňajte s ďalšími typmi vylúčení.

Prednastavená je kontrola všetkých súborov bez ohľadu na príponu. Do zoznamu súborov vylúčených z kontroly môže byť pridaná akákoľvek prípona.

Vylúčenie prípony z kontroly je rozumné použiť napr. vtedy, keď kontrola určitého typu súboru spôsobuje nesprávne fungovanie daného programu. Odporúča sa napríklad vylúčiť súborové prípony `.edb`, `.eml` a `.tmp` v prípade, že používate Microsoft Exchange server.

Ak chcete pridať novú príponu do zoznamu, kliknite na **Pridať**. Zadajte príponu (napr. `tmp`) a kliknite na tlačidlo **OK**. Ak označíte možnosť **Zadať viaceré hodnoty**, môžete do textového poľa zadať viacero prípon oddelených riadkami, čiarkami alebo bodkočiarkami (z roletového menu pre oddeľovač viacerých hodnôt vyberte napríklad **Bodkočiarku** a zadajte prípony v tvare `edb;eml;tmp`).
Môžete použiť aj špeciálny znak ? (otáznik). Otáznik nahrádza akýkoľvek znak (napríklad `?db`).

Ak chcete vidieť presnú príponu konkrétneho súboru na operačnom systéme Windows, musíte zrušiť výber možnosti **Skryť prípony známych súborov** v časti **Ovládací panel** > **Možnosti priečinka** > karta **Zobrazenie** a aplikovať túto zmenu.

Doplňujúce parametre ThreatSense

Doplňujúce parametre ThreatSense pre vytvárané a menené súbory – pravdepodobnosť napadnutia novovytvorených alebo upravovaných súborov je vyššia ako u existujúcich súborov. To je dôvod, prečo program tieto súbory kontroluje s prídavnými parametrami. Využívajú sa metódy kontroly na základe detekčných signatúr spoločne s pokročilou heuristikou, vďaka ktorej možno zachytiť nové hrozby skôr, ako vyjde aktualizácia detekčného jadra. Okrem novovytvorených súborov sa kontrolujú aj samorozbaľovacie archívy (.sfx) a runtime archívy (interne komprimované spustiteľné súbory). Štandardne sú archívy kontrolované do desiatej úrovne vnorenia a bez ohľadu na ich veľkosť. Ak chcete zmeniť nastavenia kontroly archivovaných súborov, zrušte označenie možnosti **Predvolené nastavenie archívov**.

Viac informácií o runtime archívoch, samorozbaľovacích archívoch a pokročilej heuristike nájdete v kapitole Parametre ThreatSense.

Doplňujúce parametre ThreatSense pre spúšťané súbory – predvolene sa pokročilá heuristika používa pri spúšťaní súborov. Ak je zapnutá, odporúčame ponechať zapnutú aj Smart optimalizáciu a ESET LiveGrid®, čím zmiernite vplyv na výkon systému.

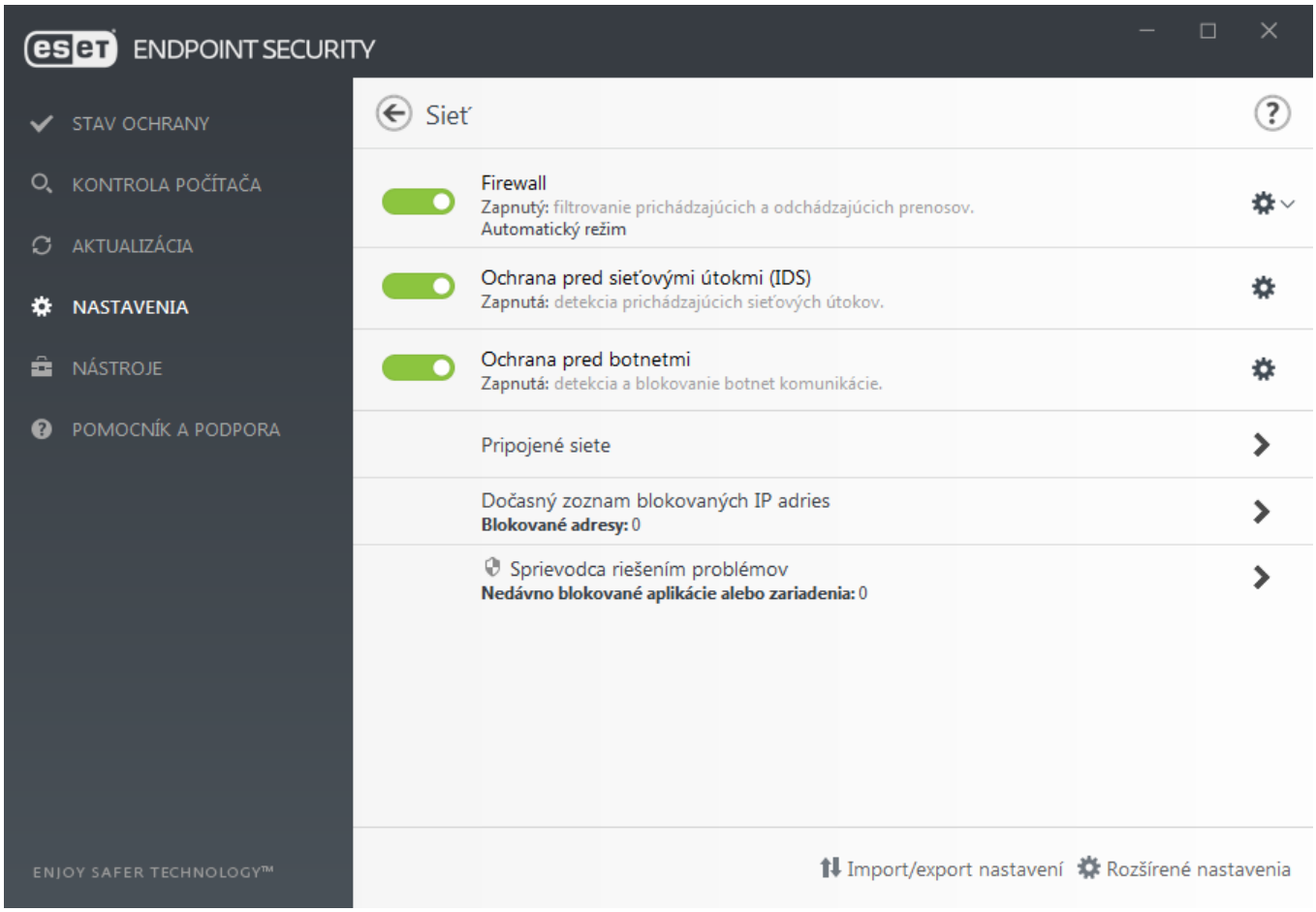
Sieť

Sekcia **Sieť** vám ponúka rýchly prístup k nasledujúcim súčastiam alebo **rozšíreným nastaveniam**:

- **Firewall** – v tejto časti si môžete zvoliť režim filtrovania pre ESET Firewall. Pre prístup k podrobnejším nastaveniam kliknite na ikonu ozubeného kolesa > **Konfigurovať** vedľa položky **Firewall** alebo stlačte

kláves **F5**, čím otvoríte sekciu **Rozšírené nastavenia**.

- **Ochrana pred sieťovými útokmi (IDS)** – analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Zablokovaná bude každá škodlivá sieťová komunikácia. ESET Endpoint Security vás upozorní, ak sa pripojíte k nezabezpečenej bezdrôtovej sieti alebo k sieti so slabou ochranou.
- **Ochrana pred botnetmi** – rýchlo a presne odhaľuje malvér v systéme. Ak chcete ochranu pred botnetmi na určitý čas vypnúť, kliknite na (neodporúča sa).
- **Pripojené siete** – zobrazuje siete, ku ktorým sú pripojené sieťové adaptéry. Kliknite na ikonu ozubeného kolesa a vyberte typ ochrany pre sieť, na ktorú ste pripojený. Ak si chcete zobraziť jednotlivé sieťové adaptéry spolu s priradeným profilom firewallu a dôveryhodnou zónou, kliknite na **Pripojené siete** > **Sieťové adaptéry**. Viac informácií sa nachádza v kapitole Sieťové adaptéry.
- **Dočasný zoznam blokovaných IP adries** – zoznam IP adries, ktoré boli identifikované ako zdroje útokov. Tieto IP adresy boli pridané do zoznamu dočasne blokovaných IP adries a zároveň je pre ne na určitý čas prerušená komunikácia. Viac informácií získate kliknutím na túto možnosť a stlačením F1.
- **Sprievodca riešením problémov** – pomáha pri riešení problémov so sieťovým spojením, ktoré môžu byť zapríčinené ESET Firewallom. Viac informácií nájdete v kapitole Sprievodca riešením problémov.



Po kliknutí na ozubené koleso vedľa položky **Firewall** sa zobrazia nasledujúce možnosti:

- **Konfigurovať** – rozšírené nastavenia firewallu, kde môžete určiť, akým spôsobom bude firewall spravovať sieťovú komunikáciu.
- **Zablokovať všetku komunikáciu** – každá prichádzajúca a odchádzajúca komunikácia bude firewallom bez upozornenia používateľa zablokovaná. Použiť tento spôsob blokovania je vhodné napríklad pri podozrení na možné kritické bezpečnostné riziká, kedy je nutné odpojiť systém od siete. Ak je v rámci filtrovania sieťovej komunikácie nastavená možnosť **Zablokovať všetku komunikáciu**, kliknutím na **Zastaviť blokovanie všetkej komunikácie** prepnete firewall do štandardného režimu.
- **Pozastaviť firewall (povoliť všetku komunikáciu)** – pomocou tejto možnosti môžete pozastaviť kontrolu

siete firewallom. Pri použití tejto možnosti je filtrovanie spojení firewallom úplne vypnuté a všetky prichádzajúce aj odchádzajúce spojenia sú povolené. Ak chcete znova zapnúť firewall, keď je filtrovanie sieťovej komunikácie v tomto režime, kliknite na možnosť **Zapnúť firewall**.

- **Automatický režim** – (ak je povolený iný režim filtrovania) – kliknutím na túto možnosť sa režim filtrovania zmení na automatický (s pravidlami nastavenými používateľom).
- **Interaktívny režim** (ak je povolený iný režim filtrovania) – kliknutím na túto možnosť sa režim filtrovania zmení na interaktívny.

Firewall

Firewall zabezpečuje kontrolu všetkých spojení medzi sieťou a daným systémom. Na základe definovaných pravidiel jednotlivé spojenia povoľuje alebo blokuje. Chráni pred útokmi zo vzdialených počítačov a umožňuje blokovanie niektorých potenciálne nebezpečných služieb.

Základné

Zapnúť firewall

Na zaistenie maximálnej ochrany vášho systému vám odporúčame ponechať túto možnosť povolenú. Pri zapnutom firewalle je komunikácia na sieti kontrolovaná v oboch smeroch.

Vyhodnotiť aj pravidlá z Windows Firewall

Pri automatickom režime bude povolená aj prichádzajúca komunikácia, ktorá je povolená pravidlami Windows Firewallu, pokiaľ nie je blokovaná existujúcimi pravidlami ESET.

Nevyhodnocujú sa pravidlá z Windows Firewallu nakonfigurované skupinovou politikou (GPO).

Režim filtrovania

Správanie firewallu sa mení podľa zvoleného režimu filtrovania. Režimy filtrovania tiež určujú, do akej miery bude potrebná interakcia používateľa.

Firewall programu ESET Endpoint Security môže pracovať v štyroch režimoch filtrovania:

Režim filtrovania	Popis
Automatický režim	Ide o predvolený režim. Je vhodný pre používateľov, ktorí preferujú pohodlné používanie firewallu bez potreby vytvárania pravidiel. Vlastné používateľské pravidlá môžu byť vytvorené aj v **automatickom režime**, no nie sú povinné. Povoľuje všetku odchádzajúcu komunikáciu z daného systému a blokuje väčšinu novej prichádzajúcej komunikácie (okrem komunikácie z dôveryhodnej zóny, ktorá je nastavená v časti IDS a pokročilé možnosti/Povolené služby) a prichádzajúcej komunikácie odpovedajúcej na nedávnu odchádzajúcu komunikáciu.

Režim filtrovania	Popis
Interaktívny režim	Predstavuje komfortnú možnosť nastavenia firewallu podľa požiadaviek používateľa. V prípade zistenia akejkoľvek komunikácie, na ktorú nie je možné aplikovať žiadne existujúce pravidlo, je používateľovi zobrazené informačné okno o zachytení neznámeho spojenia. Následne je možné túto komunikáciu povoliť alebo zamietnuť, pričom toto rozhodnutie môže byť uložené ako nové pravidlo firewallu. V prípade vytvorenia pravidla bude každá komunikácia tohto typu v budúcnosti povolená alebo zablokovaná podľa daného pravidla.
Režim politík	Blokuje každé spojenie, pre ktoré neexistuje povoľujúce pravidlo. Skúsený používateľ tak môže nastaviť pravidlá firewallu tak, aby boli povolené len želané a bezpečné spojenia. Firewall bude blokovať všetku ostatnú neznámu komunikáciu.
Učiaci sa režim	Automaticky vytvára a ukladá pravidlá. Tento režim je vhodný na prvotné nastavenie firewallu, no nemal by zostávať aktívny na dlhšie časové obdobie. Vytvorenie pravidiel prebehne bez interakcie používateľa, keďže ESET Endpoint Security ukladá pravidlá na základe prednastavených parametrov. Tento režim odporúčame používať len dovtedy, kým sa nevytvoria všetky pravidlá pre bežnú komunikáciu. Vyhnete sa tak bezpečnostným rizikám.

Profily sú ďalším účinným nástrojom, ako si správanie firewallu v programe ESET Endpoint Security prispôsobiť vlastným potrebám, keďže pre rozličné situácie môžete mať zadefinovaný iný súbor pravidiel.

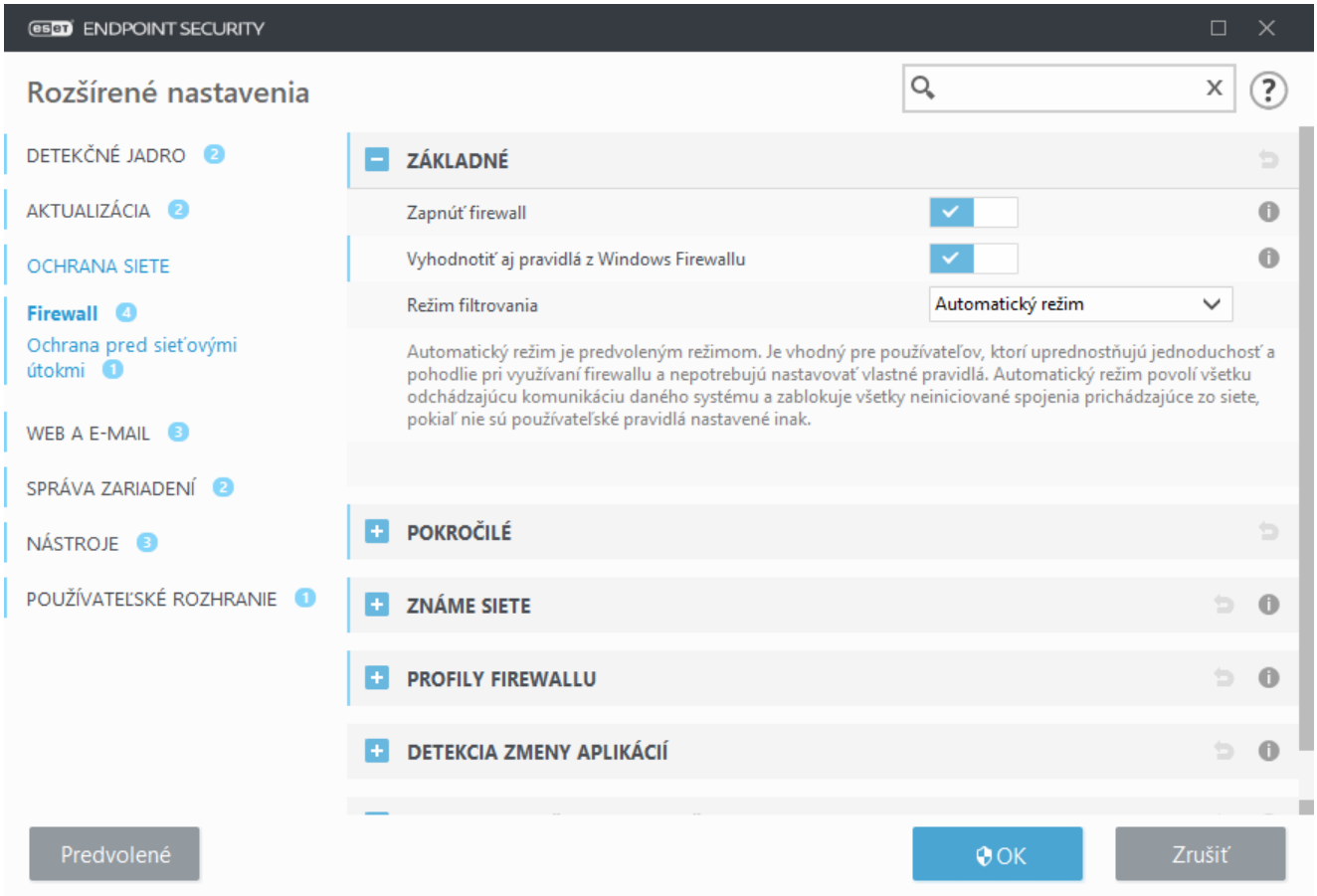
Pokročilé

Pravidlá

Nastavenie pravidiel umožňuje prezeranie všetkých pravidiel, ktorými sa riadi komunikácia jednotlivých aplikácií v rámci dôveryhodných zón a internetu.

Zóny

Zóny predstavujú zoskupenia sieťových adries, ktoré spolu tvoria jednu logickú skupinu.



Môžete vytvoriť IDS pravidlo pri Botnet útoku na váš počítač. Pravidlo je možné upravovať v sekcii **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Ochrana pred sieťovými útokmi** > **IDS pravidlá** po kliknutí na **Upraviť**.

Učiaci sa režim

Učiaci sa režim automaticky vytvorí a uloží pre každú komunikáciu zodpovedajúce pravidlo. Vytvorenie pravidiel prebehne bez interakcie s používateľom, keďže ESET Endpoint Security uloží pravidlá na základe prednastavených parametrov.

Používanie tohto režimu môže vystaviť váš systém riziku a odporúča sa len v prípade potreby prvotného nastavenia firewallu.

Učiaci sa režim môžete zapnúť v **Rozšírených nastaveniach** (F5) v časti **Firewall** > **Základné** zvolením možnosti **Učiaci sa režim** z roletového menu **Režim filtrovania**, čím aktivujete **Nastavenia učiaceho sa režimu**. Táto sekcia obsahuje nasledujúce možnosti:

V učiacom sa režime firewall nefiltruje komunikáciu. Všetka odchádzajúca a prichádzajúca komunikácia je povolená. Váš počítač v tomto režime nie je plne chránený pomocou firewallu.

Režim, ktorý sa nastaví po skončení učiaceho sa režimu – táto možnosť určuje, ktorý režim filtrovania bude v rámci firewallu programu ESET Endpoint Security použitý po skončení učiaceho sa režimu. Prečítajte si viac o režimoch filtrovania. Možnosť Spýtať sa používateľa vyžaduje oprávnenia správcu, ak chcete vykonávať zmeny režimu filtrovania firewallu.

Typ komunikácie – pomocou tejto možnosti môžete zvoliť osobitné zásady vytvárania pravidiel pre každý typ

komunikácie. Učiaci sa režim rozlišuje štyri typy komunikácie:

- **Prichádzajúca komunikácia z dôveryhodnej zóny** – príklad prichádzajúcej komunikácie z dôveryhodnej zóny: Vzdialený počítač z dôveryhodnej zóny sa pokúša komunikovať s lokálnou aplikáciou bežiacou na vašom počítači.

- **Odchádzajúca komunikácia do dôveryhodnej zóny** – lokálna aplikácia sa pokúša nadviazať spojenie s iným počítačom v rámci lokálnej siete alebo inej siete v dôveryhodnej zóne.

- **Prichádzajúca internetová komunikácia** – vzdialený počítač sa pokúša komunikovať s aplikáciou bežiacou na počítači.

- **Odchádzajúca internetová komunikácia** – lokálna aplikácia sa pokúša nadviazať spojenie s iným počítačom.

Definovanie parametrov, ktoré sa pridajú do vytváraných pravidiel:

Pridať lokálny port – číslo lokálneho portu sieťového spojenia. Pre odchádzajúcu komunikáciu sa generujú náhodné čísla. Preto je vhodné tento parameter definovať len pri kontrole prichádzajúcich spojení.

Pridať aplikáciu – názov lokálnej aplikácie. Túto možnosť odporúčame použiť vtedy, ak chcete do pravidla zahrnúť kompletnú komunikáciu špecifikovanej aplikácie. Napríklad môžete povoliť komunikáciu iba pre webový prehliadač, e-mailového klienta atď.

Pridať vzdialený port – číslo vzdialeného portu sieťovej komunikácie. Napríklad môžete povoliť/zakázať konkrétnu službu so štandardným číslom portu (napr. HTTP – 80, POP3 – 110 a pod.).

Pridať vzdialenú IP adresu/dôveryhodnú zónu – vzdialená IP adresa alebo celá zóna adries môže byť použitá ako parameter pre nové pravidlá, ktoré sa aplikujú na všetky sieťové spojenia medzi lokálnym systémom a vzdialenou adresou/zónou. Túto možnosť je vhodné použiť v prípade, že chcete definovať akcie pre konkrétny počítač alebo skupinu počítačov v sieti.

Maximálny počet pravidiel pre jednu aplikáciu – pokiaľ aplikácia komunikuje viacerými smermi (z rôznych portov, na rôzne IP adresy a pod.), firewall v učiacom sa režime pre ňu vytvára zodpovedajúci počet pravidiel. Pomocou tejto možnosti je možné limitovať počet pravidiel, ktoré môžu byť vytvorené pre jednu aplikáciu.

Ochrana pred sieťovými útokmi

Zapnúť ochranu pred sieťovými útokmi (IDS) – analyzuje obsah sieťovej komunikácie a chráni pred sieťovými útokmi. Akákoľvek komunikácia, ktorá je považovaná za nebezpečnú, bude zablokovaná.

Zapnúť ochranu pred botnetmi – deteguje a blokuje komunikáciu s riadiacimi C&C servermi rozpoznávaním charakteristík, ktoré naznačujú, že počítač je infikovaný a bot sa pokúša komunikovať. Viac o ochrane pred botnetmi sa dočítate v slovníku pojmov.

IDS pravidlá – v tejto časti môžete nastaviť pokročilé možnosti filtrovania a detekcie rôznych typov zraniteľností a útokov, ktoré môžu byť namierené na váš počítač.

Ochrana pred útokmi hrubou silou

Ochrana pred útokmi hrubou silou blokuje pokusy o uhádnutie hesiel pre služby SMB a RDP. Útok hrubou silou je metóda systematického testovania možných kombinácií písmen, číslic a symbolov s cieľom prelomiť heslo. Ak

chcete upraviť nastavenia ochrany pred útokmi hrubou silou, v hlavnom okne programu kliknite na **Nastavenia** > **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Ochrana pred sieťovými útokmi** > **Ochrana pred útokmi hrubou silou**.

Zapnúť ochranu pred útokmi hrubou silou – ESET Endpoint Security kontroluje obsah sieťovej komunikácie a blokuje pokusy o uhádnutie hesiel.

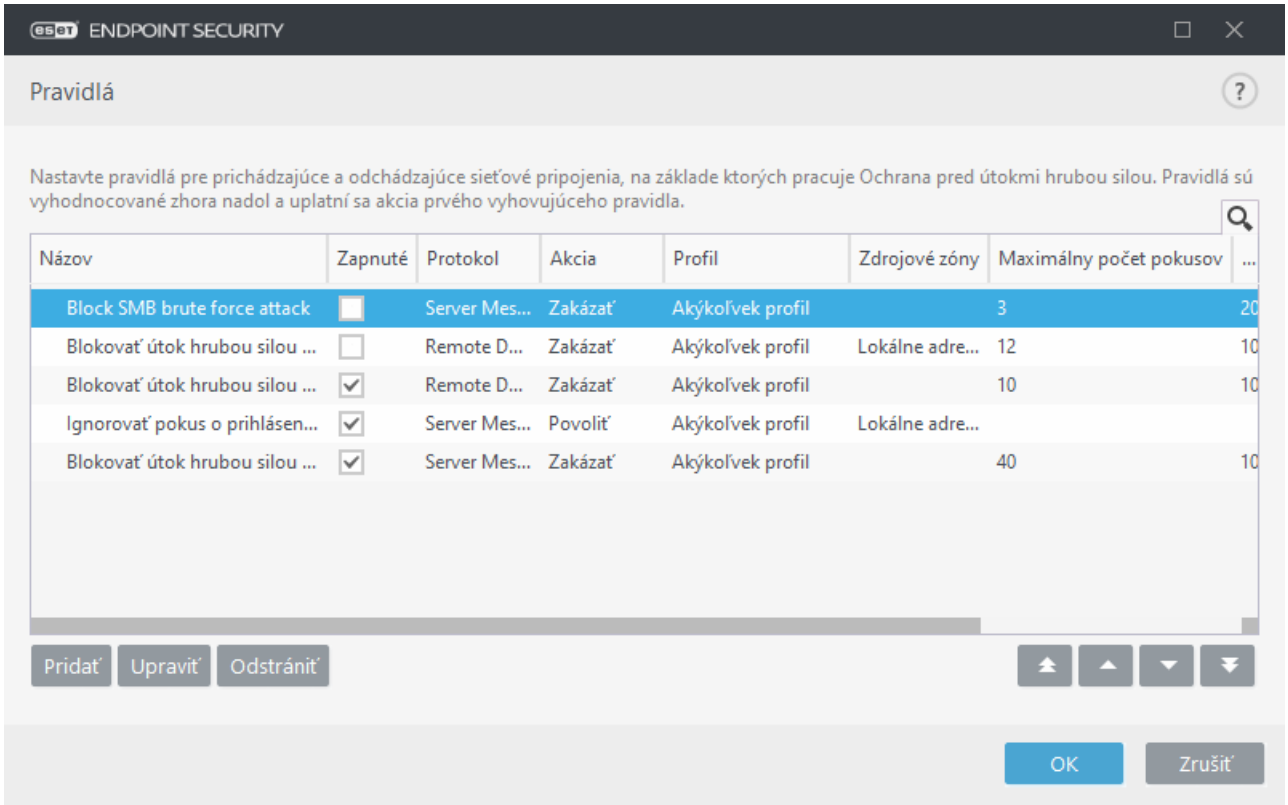
Pravidlá – umožňujú vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia. Viac informácií nájdete v kapitole Pravidlá.

Vylúčenia – zoznam vylúčených detekcií definovaných na základe IP adresy alebo cesty k aplikácii. Vylúčenia môžete vytvárať a upravovať vo svojej konzole ESET PROTECT. Viac informácií nájdete v kapitole Vylúčenia.

Pravidlá

V okne s pravidlami ochrany pred útokmi hrubou silou môžete vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia. Prednastavené pravidlá nie je možné upraviť ani odstrániť.

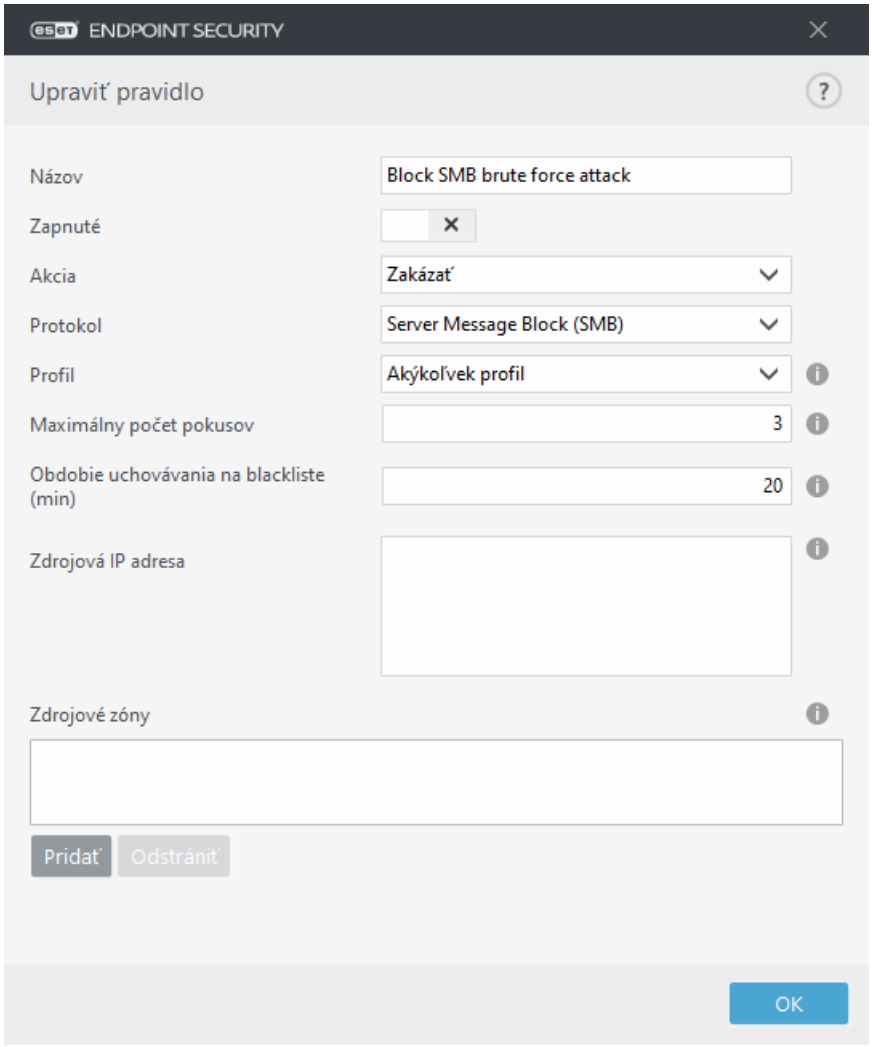
Správa pravidiel ochrany pred útokmi hrubou silou



- **Pridať** – vytvorenie nového pravidla ochrany pred útokmi hrubou silou.
- **Upraviť** – zmena existujúceho pravidla ochrany pred útokmi hrubou silou.
- **Odstrániť** – odstránenie označeného IDS pravidla zo zoznamu.
- **Navrch/Vyššie/Nižšie/Naspodok** – šípky, ktoré vám jednoducho umožňujú meniť prioritu pravidiel v zozname.

V záujme maximálnej ochrany sa blokovacie pravidlo s najnižšou hodnotou nastavenou pre **Maximálny počet pokusov** použije aj vtedy, keď je v zozname pravidiel nižšie v poradí a podmienkam detekcie vyhovuje viacero pravidiel blokovania.

Editor pravidiel



Názov – názov pravidla.

Zapnuté – deaktivujte túto možnosť, ak pravidlo nechcete používať, no želáte si ho ponechať v zozname.

Akcia – zvoľte, či sa má pri splnení pravidlom definovaných podmienok spojenie **Zakázať** alebo **Povoliť**.

Protokol – komunikačný protokol, pre ktorý má pravidlo platiť.

Profil – pre konkrétne profily možno nastaviť a použiť vlastné pravidlá.

Maximálny počet pokusov – maximálny povolený počet pokusov o opakovanie útoku, pokým IP adresa nebude zablokovaná a pridaná na blacklist.

Obdobie uchovávania na blackliste (min) – nastaví čas odstránenia IP adresy z blacklistu.

Zdrojová IP adresa – zoznam IP adries, rozsahov alebo podsietí. Viaceré adresy musia byť oddelené čiarkou.

Zdrojové zóny – kliknutím na **Pridať** môžete pridať preddefinované alebo novovytvorené zóny so zvoleným

rozsahom IP adries.

Vylúčenia

Vylúčenia útokov hrubou silou možno použiť na potlačenie detekcií útokov hrubou silou podľa konkrétnych kritérií. Tieto vylúčenia sa vytvárajú cez ESET PROTECT na základe detekcií útokov hrubou silou.

Stĺpce

- **Detekcia** – typ detekcie.
- **Aplikácia** – nastavte cestu k vylúčenej aplikácii kliknutím na ... (napríklad *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
- **Vzdialená IP** – zoznam vzdialených IPv4 alebo IPv6 adries/rozsahov/podsietí. Viaceré adresy musia byť oddelené čiarkou.

Správa vylúčení

Vylúčenia sa zobrazia v tom prípade, že správca vytvorí vylúčenia útokov hrubou silou v ESET PROTECT Web Console. Vylúčenia môžu obsahovať iba povoľujúce pravidlá a sú vyhodnocované ešte pred IDS pravidlami.

Pokročilé možnosti filtrovania

Sekcia Firewall a sekcia Ochrana pred sieťovými útokmi vám umožňujú nastaviť pokročilé možnosti filtrovania a detekcie rôznych typov zraniteľností a útokov, ktoré môžu byť namierené na váš počítač.

V určitých prípadoch sa nezobrazí výstražné oznámenie o zablokovanej komunikácii. Postup zobrazenia všetkých blokovaných komunikácií nájdete v kapitole Vytváranie protokolov a pravidiel alebo výnimiek z protokolu.

Dostupnosť jednotlivých možností v sekcii **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Firewall** a v sekcii **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Ochrana pred sieťovými útokmi** môže závisieť od typu alebo verzie vášho modulu firewallu, ako aj od verzie vášho operačného systému.

Povolené služby

Nastavenia v tejto skupine majú zjednodušiť konfiguráciu prístupu k službám tohto počítača z dôveryhodnej zóny. Viaceré z nich povoľujú/zakazujú predvolené pravidlá firewallu.

- **Umožniť zdieľanie súborov a tlačiarní v dôveryhodnej zóne** – zabezpečuje, že vzdialené počítače, ktoré sú zaradené do dôveryhodnej zóny, budú môcť pristupovať k vašim zdieľaným súborom a tlačiarňam.
- **Povoliť UPNP pre systémové služby v dôveryhodnej zóne** – povoľuje odchádzajúce a prichádzajúce požiadavky protokolu UPnP pre systémové služby v dôveryhodnej zóne. UPnP (Universal Plug and Play alebo Microsoft Network Discovery) sa používa od verzie operačného systému Windows Vista.
- **Povoliť prichádzajúcu RPC komunikáciu v dôveryhodnej zóne** – povoľuje TCP komunikáciu z dôveryhodnej zóny používanú na prístup k službám MS RPC Portmapper a RPC/DCOM.
- **Povoliť vzdialenú plochu v dôveryhodnej zóne** – povoľuje pripojenia cez Microsoft Remote Desktop Protocol (RDP) a počítačom v dôveryhodnej zóne povoľuje pripojenie na váš počítač prostredníctvom programu využívajúceho RDP (napr. funkcie Pripojenie vzdialenej pracovnej plochy). Prečítajte si tiež, ako

povoliť pripojenia cez RDP mimo dôveryhodnej zóny.

- **Povoliť prihlasovanie do rozosielacích skupín cez IGMP** – umožňuje komunikáciu pomocou protokolov IGMP a UDP, napríklad video streamu vytvoreného určitým programom cez protokol IGMP (Internet Group Management Protocol).
- **Povoliť komunikáciu nepatriacu danému počítaču (most)** – v prípade komunikácie typu most (bridge) táto nebude firewallom blokovaná. Premostenie umožňuje pripájanie virtuálnych počítačov k sieti pomocou adaptéra siete Ethernet hostiteľského počítača. Ak používate most, virtuálny počítač má prístup k iným zariadeniam v sieti a naopak, akoby išlo o fyzický počítač.
- **Povoliť automatické zisťovanie webových služieb (WSD) v dôveryhodnej zóne pre systémové služby** – povoľuje prichádzajúce požiadavky protokolu WSD z dôveryhodnej zóny cez firewall. WSD (Web Service Discovery) je protokol používaný na zisťovanie služieb v lokálnej sieti.
- **Povoliť preklad rozosielacích adries v dôveryhodnej zóne (LLMNR)** – LLMNR (Link-local Multicast Name Resolution) je protokol založený na DNS paketoch umožňujúci preklad názvov IPv4 a IPv6 hostiteľov na rovnakom lokálnom segmente bez potreby DNS servera či konfigurácie DNS klienta. Táto možnosť povoľuje prichádzajúce multicastové DNS požiadavky z dôveryhodnej zóny cez firewall.
- **Podpora pre Windows domácu skupinu** – zapne podporu pre domácu skupinu na operačnom systéme Windows 7 a novších. Pomocou HomeGroup je možné zdieľať súbory a tlačiarne v rámci domácej siete. Nastavenia je možné nájsť v ponuke **Štart** > **Ovládací panel** > **Sieť a Internet** > **Domáca skupina**.

Detekcia útokov

- **Protokol SMB** – deteguje a blokuje rôzne zraniteľnosti v SMB protokole:
- **Detekcia útoku škodlivého servera challenge autentifikáciou** – chráni pred útokom prebiehajúcim pri prihlasovaní sa a odosielaní prihlasovacích údajov na server.
- **Detekcia úniku IDS počas otvárania pomenovaného presmerovania** – detekcia únikových techník pri otváraní pomenovaných kanálov MSRPCS v protokole SMB.
- **CVE detekcie** (Common Vulnerabilities and Exposures) – implementované metódy detekcie rôznych útokov, foriem, bezpečnostných dier a zneužití cez protokol SMB. Viac informácií nájdete na webovej stránke CVE: cve.mitre.org.
- **Protokol RPC** – deteguje a blokuje rôzne zraniteľnosti (CVE) v RPC protokole, ktorý bol navrhnutý pre Distributed Computing Environment (DCE).
- **Protokol RDP** – deteguje a blokuje rôzne zraniteľnosti (CVE) v RDP protokole (pozri popis vyššie).
- **Detekcia útoku ARP Poisoning** – detekcia útokov typu ARP poisoning spôsobených útokmi typu man in the middle a detekcia tzv. sniffingu na sieťovom prepínači. Protokol ARP (Address Resolution Protocol) je sieťovými aplikáciami alebo zariadeniami využívaný na zistenie Ethernet adresy.
- **Detekcia útoku skenovaním portov TCP/UDP** – zabraňuje útokom softvéru, ktorý sa pokúša nájsť otvorené porty hostiteľského zariadenia posielaním požiadaviek na určitý rozsah adries portov za účelom nájdenia aktívneho portu, ktorý je možné zneužiť na napadnutie systému. Viac o tomto type útoku sa môžete dočítať v slovníku pojmov.
- **Blokovať nebezpečnú adresu po detekcii útoku** – ak je zistený útok z určitej adresy, všetka komunikácia z nej bude na určitý čas blokovaná.
- **Zobraziť oznámenie po detekcii útoku** – pri zachytení útoku program zobrazí upozornenie v pravom dolnom rohu obrazovky.
- **Zobraziť upozornenie pri pokusoch o zneužitie bezpečnostných dier** – program zobrazí upozornenie, ak bude zachytený útok na bezpečnostné diery alebo pokus o preniknutie do systému týmto spôsobom.

Kontrola paketov

- **Povoliť prichádzajúce spojenie k správcovským zdieľaným položkám cez SMB protokol** – správcovské zdieľané položky (admin shares) sú predvolené zdieľané položky na sieti, ktoré zdieľajú oddiely pevného disku (*C$*, *D$* atď.) spolu so systémovým priečinkom (*ADMIN$*). Zakázanie prístupu k správcovským zdieľaným položkám výrazne znižuje bezpečnostné riziká. Napríklad červ Conficker vykonáva slovníkové (dictionary) útoky v snahe získať prístup k týmto položkám.

- **Zakázať staré (nepodporované) SMB dialekty** – zakáže SMB reláciu so starým dialektom SMB, ktorý nepodporuje IDS. Najnovšie operačné systémy Windows podporujú staré dialekty SMB kvôli spätnej kompatibilite so staršími operačnými systémami, ako napríklad Windows 95. Útočník môže použiť starší dialekt SMB s úmyslom vyhnúť sa kontrole packetov. Zakážte staré SMB dialekty, ak váš počítač nepotrebuje zdieľať súbory so staršími verziami operačného systému Windows.
- **Zakázať relácie SMB bez bezpečnostných rozšírení** – bezpečnostné rozšírenia môžu byť použité počas nadväzovania SMB relácie na zaistenie bezpečnejšieho mechanizmu autentifikácie ako v prípade LAN Manager Challenge/Response (LM). Schéma LM je považovaná za slabú a neodporúča sa ju používať.
- **Zakázať otvorenie spustiteľného súboru na serveroch mimo dôveryhodnej zóny cez SMB protokol** – zabraňuje komunikácii v prípade, že sa používateľ snaží otvoriť spustiteľný súbor (.exe, .dll) zo zdieľaného priečinka na serveri, ktorý nie je v dôveryhodnej zóne firewallu. Kopírovanie spustiteľných súborov z dôveryhodných zdrojov je v poriadku, táto funkcionalita by však mala obmedziť nebezpečenstvo otvorenia spustiteľného súboru zo škodlivých serverov.
- **Zakázať NTLM overenie cez SMB protokol pri pripojení na server v/mimo dôveryhodnej zóny** – protokoly používajúce autentifikačnú schému NTLM (obe verzie) sú ohrozené útokmi, ktorých cieľom je preposielanie prihlasovacích údajov (v prípade SMB protokolu známe ako SMB Relay útoky). Zakázaním autentifikácie NTLM so servermi mimo dôveryhodnej zóny sa zníži riziko preposlania prihlasovacích údajov škodlivým serverom mimo dôveryhodnej zóny. Tiež môžete zakázať aj autentifikáciu NTLM so servermi v dôveryhodnej zóne.

- **Povoliť komunikáciu so službou Security Account Manager** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SAMR].

- **Povoliť komunikáciu so službou Local Security Authority** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-LSAD] a [MS-LSAT].

- **Povoliť komunikáciu so službou Remote Registry** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-RRP].

- **Povoliť komunikáciu so službou Service Control Manager** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SCMR].

- **Povoliť komunikáciu so službou Server** – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SRVS].
- **Povoliť komunikáciu s ostatnými službami** – ostatné MSRPC služby. MSRPC je implementáciou DCE RPC mechanizmu v systéme Microsoft Windows. MSRPC môže na prenos (ncacn_np) používať pomenované kanály v rámci SMB protokolu. Služby MSRPC poskytujú rozhranie na vzdialenú správu systémov Windows. V systéme MSRPC bolo objavených mnoho zraniteľných miest (tieto zraniteľnosti zneužíva napr. červ Conficker, červ Sasser atď.). Zakázaním komunikácie so službami MSRPC, ktoré nepotrebujete, predídete mnohým bezpečnostným rizikám (ako napríklad vzdialené spúšťanie kódu alebo zlyhávanie služieb kvôli útoku).

IDS pravidlá

V niektorých situáciách môže systém na detekciu narušenia (IDS) zaznamenať komunikáciu medzi routermi alebo inými internými sieťovými zariadeniami ako potenciálny útok. Môžete napríklad pridať známu bezpečnú adresu do Adries vylúčených z aktívnej ochrany IDS, a tak obísť IDS.

Berte, prosím, na vedomie, že nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Vytvorenie IDS pravidiel na klientskych pracovných staniciach v programe ESET Endpoint Security
- Vytvorenie IDS pravidiel pre klientske pracovné stanice v konzole ESET PROTECT

Stĺpce

- **Detekcia** – typ detekcie.
- **Aplikácia** – nastavte cestu k vylúčenej aplikácii kliknutím na ... (napríklad *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
- **Vzdialená IP** – zoznam vzdialených IPv4 alebo IPv6 adries/rozsahov/podsietí. Viaceré adresy musia byť oddelené čiarkou.
- **Blokovať** – každý systémový proces má vlastné predvolené správanie a priradenú akciu (blokovať alebo povoliť). Pre zmenu predvoleného správania produktu ESET Endpoint Security vyberte z roletového menu možnosť áno alebo nie.
- **Oznámiť** – ak chcete zapnúť zobrazovanie oznámení na ploche, označte možnosť Áno. Ak nechcete, aby sa zobrazovali oznámenia na ploche, označte možnosť Nie. Dostupné hodnoty sú Predvolená/Áno/Nie.
- **Zapísať do protokolu** – ak chcete zaznamenávať udalosti do protokolu produktu ESET Endpoint Security, označte možnosť **Áno**. Ak nechcete zaznamenávať udalosti do protokolu produktu, označte možnosť **Nie**. Dostupné hodnoty sú **Predvolená**/**Áno**/**Nie**.

Záložka Vylúčenia sa zobrazí v tom prípade, že správca vytvorí IDS vylúčenia v ESET PROTECT Web Console. IDS vylúčenia môžu obsahovať iba povoľujúce pravidlá a sú vyhodnocované ešte pred IDS pravidlami.

Spravovanie IDS pravidiel

- **Pridať** – vytvorenie nového IDS pravidla.
- **Upraviť** – zmena existujúceho IDS pravidla.
- **Odstrániť** – odstránenie označeného IDS pravidla zo zoznamu.
-  **Navrch/Vyššie/Nižšie/Naspodok** – šípky, ktoré vám jednoducho umožňujú meniť prioritu položiek v zozname (pravidlá sú vyhodnocované zhora nadol).

Ak chcete, aby sa pri každom výskyte konkrétnej udalosti zobrazilo oznámenie a bol vytvorený protokol:
1. Kliknite na **Pridať** a pridajte nové IDS pravidlo.
2. Z roletového menu **Detekcia** vyberte konkrétny typ detekcie.
3. Kliknite na **...** a zadajte cestu k aplikácii, pre ktorú sa majú zobrazovať oznámenia.
4. V roletovom menu **Blokovať** ponechajte možnosť **Predvolená**. Takto bude vykonaná akcia, ktorá je predvolená produktom ESET Endpoint Security.
5. V roletovom menu **Oznámiť** a **Zapísať do protokolu** vyberte možnosť **Áno**.
6. Kliknite na **OK**, aby sa oznámenie uložilo.

Ak chcete, aby sa prestali opakovane zobrazovať oznámenia pre typ detekcie, ktorú nepovažujete za hrozbu:
1. Kliknite na **Pridať** a pridajte novú IDS výnimku.
2. Z roletového menu **Detekcia** vyberte konkrétny typ detekcie, napr. **Relácia SMB bez bezpečnostných rozšírení** alebo **Útok skenovaním portov TCP**.
3. V prípade prichádzajúcej komunikácie vyberte z roletového menu Smer možnosť **Dnu**.
4. V roletovom menu **Oznámiť** vyberte možnosť **Nie**.
5. V roletovom menu **Zapísať do protokolu** vyberte možnosť **Áno**.
6. Pole **Aplikácia** nechajte prázdne.
7. Ak komunikácia neprichádza z konkrétnej IP adresy, pole **Vzdialená IP adresa** nechajte prázdne.
8. Kliknite na **OK**, aby sa oznámenie uložilo.

Zablokovaná podozrivá hrozba

Táto situácia môže nastať v prípade, ak sa niektorá aplikácia na vašom počítači pokúša neštandardne komunikovať s iným počítačom v sieti, zneužiť bezpečnostnú dieru alebo sa niekto pokúša skenovať porty vo vašej sieti.

Hrozba – názov hrozby.

Zdroj – zdrojová sieťová adresa.

Cieľ – cieľová sieťová adresa.

Zastaviť blokovanie – vytvorenie IDS pravidla pre podozrivú hrozbu s nastaveniami pre povolenie komunikácie.

Pokračovať v blokovaní – zablokovanie detegovanej hrozby. Ak chcete vytvoriť IDS pravidlo s nastaveniami pre blokovanie komunikácie pre túto hrozbu, vyberte možnosť **Viac neupozorňovať**.

Informácia zobrazená v okne oznámení sa môže líšiť v závislosti od typu zachytenej hrozby.
Viac informácií o hrozbách a ďalších súvisiacich pojmoch nájdete v časti Typy vzdialených útokov alebo Typy detekcií.

Riešenie problémov ochrany siete

Sprievodca riešením problémov vám umožňuje riešiť problémy s pripojením, ktoré môžu vznikať pri používaní ESET Firewallu. Z roletového menu vyberte časové obdobie, v ktorom bola sieťová komunikácia zablokovaná. Zoznam nedávno blokovanej komunikácie vám poskytuje prehľad o typoch aplikácií alebo zariadení, reputácii a celkovom počte aplikácií a zariadení blokovaných v danom časovom období. Pre viac informácií o konkrétnej blokovanej komunikácii kliknite na **Podrobnosti**. Ďalším krokom je odblokovanie aplikácie alebo zariadenia, pri ktorom dochádza k problému.

Po kliknutí na tlačidlo **Odblokovať** bude povolená všetka doteraz blokovaná komunikácia. Ak problémy s aplikáciou pretrvávajú alebo vaše zariadenie nefunguje podľa očakávania, kliknite na **Aplikácia stále nefunguje** a všetka predtým blokovaná komunikácia bude povolená. Ak problém napriek tomu pretrváva, reštartujte počítač.

Kliknutím na **Zobraziť zmeny** zobrazíte pravidlá vytvorené pomocou sprievodcu. Pravidlá vytvorené sprievodcom nájdete aj v okne **Rozšírené nastavenia** > **Ochrana siete** > **Firewall** > **Pokročilé** > **Pravidlá**.

Po kliknutí na **Odblokovať iný** môžete pokračovať v riešení problémov s ďalším zariadením alebo aplikáciou.

Pripojené siete

Sekcia **Pripojené siete** je dostupná z hlavného okna programu ESET Endpoint Security kliknutím na **Nastavenia** > **Sieť** > **Pripojené siete**.

Zobrazuje siete, na ktoré sú pripojené sieťové adaptéry. Po kliknutí na odkaz pod názvom siete sa zobrazí výzva, aby ste vybrali typ ochrany (blokovať alebo povoliť) pre sieť, na ktorú ste pripojený cez sieťový adaptér. Prípadne môžete kliknúť na ozubené koleso a zmeniť tieto nastavenia v **Rozšírených nastaveniach**. Tieto nastavenia určujú, ako veľmi prístupný je váš počítač pre ostatné počítače v sieti.

Môžete sa pripojiť k trom typom sietí:

- **Nedôveryhodná sieť** – tento typ siete je určený pre verejné miesta a nie je dôveryhodný. Vaše zariadenie nebude v sieti viditeľné a ani vy nebudete môcť vidieť ostatné zariadenia vo svojej sieti. Zisťovanie siete je v tomto prípade predvolene vypnuté.
- **Dôveryhodná sieť** – na rozdiel od verejnej siete môžete zdieľať zdroje s ostatnými počítačmi v súkromnej sieti LAN. **Dôveryhodnú sieť** vyberte vtedy, keď zariadenia v sieti poznáte a dôverujete im.
- **Doménová sieť** – tento typ sieťového umiestnenia spravuje správca siete, takže ho nie je možné vybrať ani zmeniť. Doménová sieť je detegovaná, ak je lokálny počítač členom Active Directory Domain Services. Lokálny počítač sa môže autentifikovať voči doménovému radiču v rámci jedného zo svojich sieťových pripojení.

Výberom sieťového umiestnenia môžete zaistiť vhodnú úroveň zabezpečenia svojho počítača.

Po kliknutí na **Sieťové adaptéry** v pravom dolnom rohu okna môžete zobraziť všetky sieťové adaptéry svojho počítača a k nim pridelené profily firewallu a dôveryhodné zóny. Viac informácií sa nachádza v kapitole Sieťové adaptéry.

> Ak povolíte možnosť **Použiť nastavenia Windows**, okno sa nebude zobrazovať a sieť, ku ktorej ste pripojený, bude automaticky označená podľa vašich nastavení Windows. Toto nastavenie spôsobí, že niektoré funkcie (napr. zdieľanie súborov a vzdialená plocha) budú dostupné z iných sietí.

Známe siete

Pri častom používaní počítača, ktorý je stále pripojený na verejné siete mimo vašej domácnosti alebo pracoviska, vám odporúčame overiť dôveryhodnosť siete, na ktoré sa pripájate. Po nastavení sietí dokáže ESET Endpoint Security rozpoznať dôveryhodné siete (domáce/pracovné) pomocou nastavení v časti **Identifikácia siete**. Počítače sa často pripájajú do sietí s IP adresami podobnými dôveryhodnej zóne. V takých prípadoch môže ESET Endpoint Security označiť neznámu sieť ako dôveryhodnú (domácu alebo pracovnú). Aby ste takéto prípady eliminovali, odporúčame vám používať **Overenie siete**.

Keď sa sieťový adaptér počítača pripojí na sieť alebo dôjde k zmene sieťových nastavení, ESET Endpoint Security sa pokúsi v zozname známych sietí vyhľadať záznam zodpovedajúci novej sieti. V prípade, že **Identifikácia siete** a **Overenie siete** (nepovinné) budú vyhovovať záznamu, sieť bude označená ako pripojená. Ak nebola nájdená žiadna zhoda so známou sieťou, konfigurácia identifikácie siete vytvorí nové sieťové pripojenie na identifikáciu siete, keď sa na ňu znova pripojíte. Pre nové siete sa predvolene použije typ ochrany **Verejná sieť**. Zobrazí sa dialógové okno s oznámením **Zistené pripojenie do novej siete**, v ktorom budete mať možnosť zvoliť pre sieť jeden z nasledujúcich typov ochrany: **Nedôveryhodná sieť**, **Dôveryhodná sieť** alebo **Použiť nastavenia Windows**. Ak sa sieťový adaptér pripojí na známu sieť, ktorá je označená ako **Dôveryhodná**, budú do dôveryhodnej zóny

automaticky pridané lokálne podsiete.

Typ ochrany nových sietí – určuje, ktorá z nasledujúcich možností bude predvolene použitá pre nové siete: Použiť nastavenia Windows, Spýtať sa používateľa alebo Označiť ako verejné.

> Ak povolíte možnosť **Použiť nastavenia Windows,** dialógové okno sa nebude zobrazovať a sieť, ku ktorej ste pripojený, bude automaticky označená podľa vašich nastavení Windows. To spôsobí, že niektoré funkcie (napr. zdieľanie súborov a vzdialená plocha) budú dostupné z iných sietí.

Nastavenia známych sietí sú dostupné v okne Editor známych sietí.

Editor známych sietí

Nastavenie známych sietí je dostupné cez **Rozšírené nastavenia** > **Ochrana siete** > **Základné** > **Známe siete** po kliknutí na tlačidlo **Upraviť** vedľa nastavenia **Známe siete**.

Stĺpce

Názov – názov známej siete.

Typ ochrany – zobrazuje, či je pre sieť nastavená možnosť **Dôveryhodná sieť**, **Nedôveryhodná sieť** alebo **Použiť nastavenia Windows**.

Profil firewallu – pomocou roletového menu **Zobrazovať pravidlá aktívne v profile** môžete filtrovať záznamy pravidiel podľa vybraného profilu.

Aktualizačný profil – umožňuje aplikovať vytvorený aktualizačný profil pri pripojení k danej sieti.

Ovládacie prvky

Pridať – vytvorenie novej známej siete.

Upraviť – zmena existujúcej siete.

Odstrániť – vyberte sieť a kliknutím na **Odstrániť** ju odstráňte zo zoznamu známych sietí.

 **Presunúť: Na vrch/Vyššie/Nižšie/Na spodok** – šípky, ktoré vám jednoducho umožňujú meniť poradie položiek v zozname.

Rozšírené nastavenia pri pridaní alebo zmene známej siete sú rozdelené do nasledujúcich záložiek:

Sieť

Na tejto karte môžete zadať **Názov siete** a vybrať **Typ ochrany** (Nedôveryhodná sieť, Dôveryhodná sieť, Použiť nastavenia Windows) pre danú sieť. V roletovom menu **Profil firewallu** môžete vybrať profil pre túto sieť. Ak je nastavená **Dôveryhodná sieť**, všetky priamo pripojené podsiete sú zahrnuté do dôveryhodnej zóny. Napríklad ak má sieťový adaptér pre túto sieť IP adresu 192.168.1.5 a masku podsiete 255.255.255.0, podsieť 192.168.1.0/24 bude pridaná do dôveryhodnej zóny daného adaptéra. Ak má adaptér viac adries/podsietí, všetky budú dôveryhodné bez ohľadu na nastavenia **Identifikácie siete**.

Adresy, ktoré pridáte do **Dodatočných dôveryhodných adries,** sú vždy považované za dôveryhodné (bez ohľadu

na typ ochrany siete).

Upozorniť na slabé šifrovanie WiFi – ESET Endpoint Security vás upozorní na možné bezpečnostné riziko, ak sa pripojíte do nezabezpečenej alebo slabo zabezpečenej bezdrôtovej siete.

Profil firewallu – vyberte profil firewallu, ktorý sa použije pri pripojení k danej sieti.

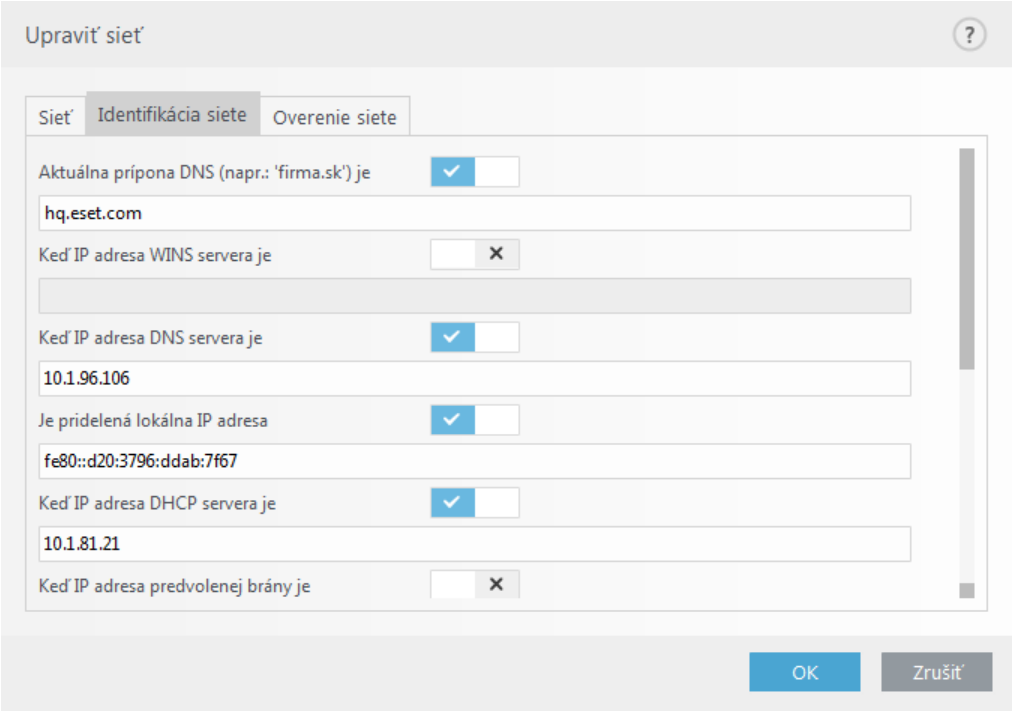
Aktualizačný profil – vyberte aktualizačný profil, ktorý sa použije pri pripojení k danej sieti.

Nasledujúce podmienky musia byť splnené, aby bola sieť pridaná do zoznamu pripojených sietí:

- **Identifikácia siete** – všetky vyplnené parametre musia byť totožné s parametrami aktívneho pripojenia.
- **Overenie siete** – ak je zvolený autentifikačný server, musí dôjsť k úspešnému overeniu voči ESET Authentication Serveru.

Identifikácia siete

Sieťová identifikácia prebieha na základe parametrov lokálneho sieťového adaptéra. Všetky nastavené parametre sú porovnávané so skutočnými parametrami aktívneho sieťového pripojenia. Sú povolené IPv4 aj IPv6 adresy.



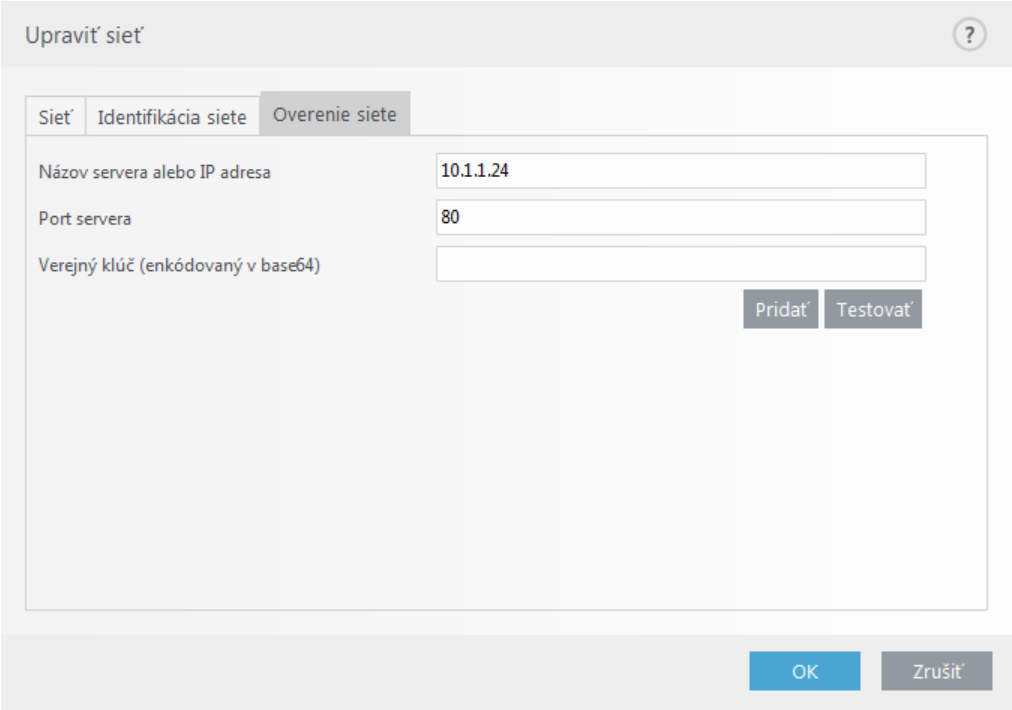
Overenie siete

Sieťová autentifikácia vyhľadáva špecifický server na sieti a používa asymetrické šifrovanie (RSA) na autentifikáciu s týmto serverom. Názov siete, ktorá je overovaná, musí byť zhodný s názvom zóny nastaveným v nastaveniach autentifikačného servera. Názov rozlišuje veľké a malé písmená. Pri nastavení autentifikačného servera je potrebné zadať jeho názov, port na ktorom počúva a verejný kľúč zodpovedajúci tajnému privátnemu kľúču servera (bližšie informácie nájdete v časti Autentifikácia zóny – nastavenie serverovej časti). Za názvom servera vo forme IP adresy, DNS alebo NetBios názvu môže nasledovať cesta upresňujúca umiestnenie kľúča na serveri (napr. "nazov_servera_/adresar1/adresar2/autentifikacia"). Môžete zadať alternatívne servery oddelené bodkočiarkou.

Stiahnite si nástroj ESET Authentication Server.

Verejný kľúč môže byť vložený v nasledujúcich typoch:

- PEM šifrovaný verejný kľúč (.pem) – tento typ kľúča je generovaný pomocou nástroja ESET Authentication Server (bližšie informácie nájdete v časti Autentifikácia zóny – nastavenie serverovej časti).
- Šifrovaný verejný kľúč
- Verejný certifikát (.crt)



Kliknite na **Testovať** pre otestovanie nastavení. Ak bola autentifikácia úspešná, objaví sa oznámenie Overenie servera bolo úspešné. Ak nie je autentifikácia nastavená správne, môže sa objaviť jedno z nasledujúcich chybových hlásení:

Overenie servera nebolo úspešné. Neplatný alebo nezhodujúci sa podpis.
Podpis servera sa nezhoduje so zadaným verejným kľúčom.

Overenie servera nebolo úspešné. Názov siete sa nezhoduje.
Nastavený názov siete sa nezhoduje s názvom zóny nastavenom na autentifikačnom serveri. Overte názvy a uistite sa, že sú zhodné.

Overenie servera nebolo úspešné. Neplatná alebo žiadna odpoveď zo servera.
Nie je prijatá odpoveď zo servera, server nie je spustený alebo je nedostupný. Neplatná odpoveď môže byť spôsobená iným HTTP serverom spusteným na nastavenej adrese.

Zadaný neplatný verejný kľúč.
Uistite sa, že zadaný súbor verejného kľúča nie je poškodený.

Overenie siete – konfigurácia servera

Autentifikáciu vykonáva ľubovoľný počítač/server pripojený do siete, ktorá má byť autentifikovaná. Aplikácia ESET Authentication Server by mala byť nainštalovaná na počítači/serveri, ktorý je neustále dostupný, aby bolo možné vykonať autentifikáciu kedykoľvek pri pripojení klienta do siete. Inštalačný súbor aplikácie ESET Authentication Server je možné stiahnuť z webovej stránky spoločnosti ESET.

Po nainštalovaní sa zobrazí riadiace dialógové okno autentifikačného servera, ktoré je možné neskôr kedykoľvek

vyvolať cez ponuku **Štart** > **Všetky programy** > **ESET** > **ESET Authentication Server**).

Na konfiguráciu autentifikačného servera zadajte názov autentifikovanej siete, port, na ktorom bude server počúvať (štandardne 80), a cestu k adresáru, do ktorého sa uloží vygenerovaný súkromný a verejný kľúč. Ďalej vygenerujte verejný a súkromný kľúč, ktoré budú použité v autentifikačnom procese. Súkromný kľúč ostáva nastavený na serveri, verejný kľúč je treba použiť na klientskej strane v rozšírených nastaveniach firewallu pri nastavovaní siete v sekcii Overenie siete.

Profily firewallu

Globálny predvolený profil – ak nie je k dispozícii žiaden profil ani zo siete, ani z konfigurácie sieťového adaptéra, potom sa použije globálny predvolený profil.

Zoznam profilov – profily slúžia na ovládanie správania firewallu v programe ESET Endpoint Security. Pri vytváraní alebo upravovaní pravidiel firewallu môžete pravidlo priradiť k určitému profilu alebo ho priradiť ku všetkým profilom. Ak je aktívny konkrétny profil firewallu, budú použité len globálne pravidlá (pravidlá bez priradeného profilu) a pravidlá, ktoré boli priradené priamo k danému profilu. Používateľ môže vytvoriť viacero profilov s rôznymi priradenými pravidlami (pre sieťové adaptéry alebo siete), vďaka čomu môže jednoducho meniť správanie firewallu.

Profily priradené k sieťovým adaptérom – sieťový adaptér môže byť nastavený tak, aby používal pri pripojení k špecifickej sieti k nej priradený profil.

Priradiť profil k sieti je možné v sekcii **Rozšírené nastavenia** (F5) > **Firewall** > **Známe siete**. V okne **Známe siete** vyberte požadovanú sieť, kliknite na **Upraviť** a z roletového menu **Profil firewallu** vyberte profil, ktorý chcete k danej sieti priradiť. Ak k sieti nie je priradený žiadny profil, bude použitý predvolený profil adaptéra. Ak je sieťový adaptér nastavený tak, aby nepoužíval sieťový profil, jeho predvolený profil bude použitý bez ohľadu na to, do akej siete je pripojený. Ak nie je vytvorený žiadny profil pre sieť alebo sieťový adaptér, bude použitý globálny prednastavený profil. Pre priradenie profilu k sieťovému adaptéru vyberte sieťový adaptér, kliknite na možnosť **Upraviť** vedľa položky **Profily priradené k sieťovým adaptérom**, vyberte profil z roletového menu **Predvolený profil firewallu** a kliknite na **OK**.

Keď sa firewall z aktívneho profilu prepne na iný profil, zobrazí sa oznámenie v pravom dolnom rohu obrazovky pri hodinách.

Profily priradené k sieťovým adaptérom

Zmenou profilu sa dá rýchlo zmeniť správanie firewallu. Pre každý profil je možné nastaviť vlastné pravidlá. Všetky sieťové adaptéry v počítači sú automaticky pridané do zoznamu **Sieťové adaptéry**.

Stĺpce

Názov – názov sieťového adaptéra.

Predvolený profil firewallu – profil, do ktorého sa firewall prepne pri pripojení na sieť, ktorá nemá nastavený vlastný profil, prípadne ak je sieťový adaptér nakonfigurovaný tak, aby nepoužíval profil siete.

Uprednostniť profil siete – sieťový adaptér bude používať profil firewallu nakonfigurovaný pre známu sieť, na ktorú je pripojený. Ak daná sieť nemá nakonfigurovaný profil, potom sa použije predvolený profil adaptéra. Ak je adaptér nastavený tak, aby nepoužíval profil siete, vždy sa miesto toho použije predvolený profil adaptéra,

nezávisle od pripojenej siete.

Ovládacie prvky

Pridať – pridá nový sieťový adaptér.

Upraviť – umožňuje zmeniť existujúci sieťový adaptér.

Odstrániť – odstráni vybraný sieťový adaptér zo zoznamu.

OK/Zrušiť – kliknite na **OK** pre uloženie zmien alebo na **Zrušiť**, ak zmeny uložiť nechcete.

Detekcia zmeny aplikácií

Detekcia zmeny aplikácií umožňuje zobraziť upozornenie na zmenu aplikácie (pre ktorú je vytvorené pravidlo firewallu) v momente, keď sa zmenená aplikácia pokúsi nadviazať sieťové spojenie. Táto funkcionalita predchádza tomu, aby pravidlo firewallu vytvorené pre určitú aplikáciu bolo zneužité škodlivým programom, ktorý dočasne alebo natrvalo nahradí pôvodný spustiteľný súbor aplikácie iným súborom, prípadne pozmení pôvodný spustiteľný súbor aplikácie za účelom škodlivej aktivity.

Prosím, majte na pamäti, že táto funkcia nie je určená na detekciu zmien všetkých aplikácií. Cieľom tejto funkcie je zabrániť zneužitiu existujúcich pravidiel firewallu, preto sú monitorované len aplikácie, pre ktoré existujú pravidlá.

Sledovať zmenu aplikácií – program bude sledovať, či nedošlo k zmene aplikácií (či sa aplikácia aktualizovala, infikovala alebo inak zmenila). Firewall zobrazí upozornenie na zmenu aplikácie v momente, keď sa zmenená aplikácia pokúsi nadviazať sieťové spojenie.

Povoliť zmenu podpísaných (dôveryhodných) aplikácií – používateľ nebude informovaný o zmene aplikácie v prípade, že daná aplikácia má rovnaký digitálny podpis pred aj po zistenej zmene.

Zoznam aplikácií vylúčených z kontroly – v tomto zozname je možné pridávať alebo odoberať aplikácie, ktoré budú vylúčené z detekcie zmien. V prípade zmeny týchto aplikácií sa používateľovi nezobrazí žiadne upozornenie.

Vylúčenia z detekcie zmeny aplikácií

Firewall v programe ESET Endpoint Security umožňuje monitorovať stav aplikácií a odhaliť, ak sa ich škodlivý kód pokúsi modifikovať (pozri kapitolu Detekcia zmeny aplikácií).

Z rôznych dôvodov sa môže vyskytnúť stav, keď je pri špecifickej aplikácii táto funkcionalita nežiaduca a je potrebné danú aplikáciu z kontroly firewallom vylúčiť.

Pridať – zobrazí sa okno, v ktorom môžete vybrať aplikáciu, ktorú chcete pridať do zoznamu aplikácií vylúčených z detekcie zmien. Aplikáciu môžete vybrať zo zoznamu aplikácií, ktoré sa spúšťajú v systéme a pre ktoré vo firewalle existuje pravidlo, prípadne môžete cestu k aplikácii zadať manuálne.

Upraviť – zobrazí sa okno, v ktorom môžete upraviť umiestenie aplikácie, ktorá je na zozname aplikácií vylúčených z detekcie zmien. Inú aplikáciu môžete vybrať zo zoznamu aplikácií, ktoré sa spúšťajú v systéme a pre ktoré vo firewalle existuje pravidlo, prípadne môžete umiestnenie aplikácie zmeniť manuálne.

Odstrániť – umožňuje odobrať položky zo zoznamu aplikácií vylúčených z detekcie zmien.

Ako nastaviť a používať pravidlá

Pravidlá predstavujú zoznam podmienok, podľa ktorých sú testované všetky sieťové pripojenia, a zároveň sú uplatnené definované akcie. Môžeme teda definovať, aká akcia sa má vykonať s pripojením spĺňajúcim podmienky daného pravidla. Pravidlá filtrovania sa nachádzajú v **Rozšírených nastaveniach** (F5) > **Ochrana siete** > **Firewall** > **Pokročilé**. Niektoré z predvolených pravidiel sa dajú vypnúť len pomocou prepínača v sekcii **Povolené služby** (Povolené služby a pokročilé možnosti).

Vyhodnocovanie pravidiel firewallu bolo v novej verzii programu ESET Endpoint Security pozmenené – priorita pravidiel v zozname je teraz posudzovaná zhora nadol. To znamená, že pri každom testovanom sieťovom spojení bude uplatnená akcia prvého pravidla, ktorého podmienky boli splnené. Je to dôležitá zmena oproti predchádzajúcej verzii programu, v ktorej bola priorita pravidiel posudzovaná automaticky a podrobnejšie zadefinované pravidlá mali väčšiu prioritu.

Z pohľadu smeru komunikácie je možné sieťové spojenia rozdeliť na prichádzajúce a odchádzajúce. Prichádzajúce spojenie je inicializované na vzdialenej strane, keď sa vzdialený počítač snaží nadviazať spojenie s lokálnym systémom (lokálnou stranou). V prípade odchádzajúceho spojenia je situácia opačná, teda lokálna strana nadväzuje spojenie so vzdialenou.

V prípade zistenia neznámej komunikácie je potrebné zvážiť, či ju povoliť alebo zamietnuť. Nevyžiadané, nezabezpečené alebo úplne neznáme spojenia predstavujú pre systém bezpečnostné riziko. Pri takejto komunikácii je vhodné venovať pozornosť hlavne vzdialenej strane a aplikácii, ktorá sa pokúša nadviazať spojenie s vaším počítačom. Mnohé infiltrácie sa snažia získať a odoslať súkromné dáta alebo sťahujú iné škodlivé aplikácie na používateľské pracovné stanice. Práve tieto skryté spojenia je možné pomocou firewallu odhaliť a zakázať.

Zoznam pravidiel firewallu

Zoznam pravidiel firewallu je dostupný cez **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Firewall** > **Základné** po kliknutí na tlačidlo **Upraviť** vedľa popisu **Pravidlá**.

Stĺpce

Názov – názov pravidla.

Zapnutý – zobrazuje, či je pravidlo aktívne alebo neaktívne; príslušným prepínacím tlačidlom je možné aktivovať a deaktivovať pravidlo.

Protokol – internetový protokol, pre ktorý je pravidlo platné.

Profil – profil firewallu, pre ktorý je pravidlo platné.

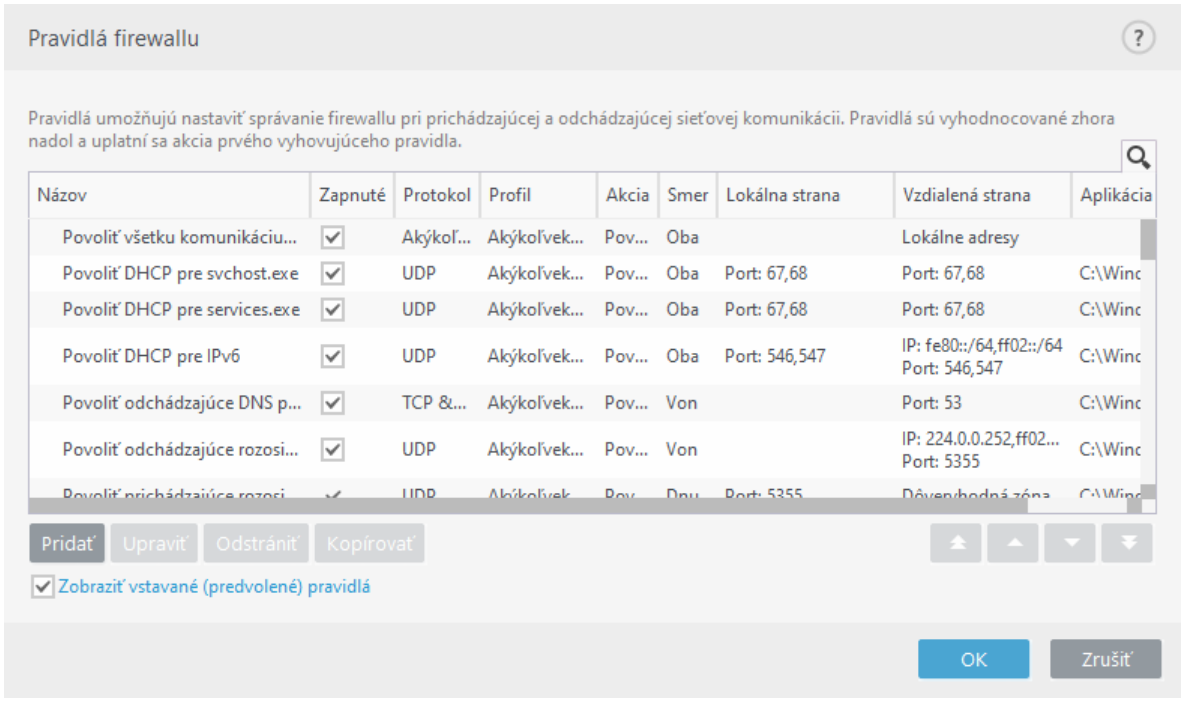
Akcia – zobrazuje stav komunikácie po uplatnení pravidla (povolené/zakázané/pýtať sa).

Smer – zobrazuje smer komunikácie (dnu/von/oba).

Lokálna strana – IPv4 alebo IPv6 adresa/rozsah adries/podsieť a port lokálneho počítača.

Vzdialená strana – IPv4 alebo IPv6 adresa/rozsah adries/podsieť a port vzdialeného počítača.

Aplikácie – aplikácia, pre ktorú bude pravidlo platiť.



Ovládacie prvky

Pridať – pridanie nového pravidla.

Upraviť – úprava existujúceho pravidla.

Odstrániť – odstránenie existujúceho pravidla.

Kopírovať – vytvorenie kópie vybraného pravidla.

Zobraziť vstavané (predvolené) pravidlá – pravidlá prednastavené programom ESET Endpoint Security, ktoré povoľujú alebo blokujú konkrétne komunikácie. Tieto pravidlá môžete deaktivovať, ale nemôžete ich zmazať.

Navrch/Vyššie/Nižšie/Naspodok – šípky, ktoré vám jednoducho umožňujú meniť prioritu pravidiel v zozname (pravidlá sú uplatňované odhora smerom nadol).

Kliknite na ikonu lupy vpravo hore pre vyhľadanie pravidla podľa názvu, protokolu alebo portu.

Pridanie alebo úprava pravidiel firewallu

Pridanie alebo úprava pravidiel firewallu môžu byť potrebné v prípade zmeny sieťových nastavení (napríklad pri zmene sieťovej adresy vzdialenej strany alebo čísla portu) s cieľom zabezpečiť správne fungovanie aplikácie, ktorú ovplyvňuje pravidlo.

Berte, prosím, na vedomie, že nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Ako vytvoriť alebo upraviť pravidlo firewallu v produkte ESET Endpoint Security
- Ako vytvoriť alebo upraviť pravidlá firewallu pre klientske pracovné stanice v nástroji ESET PROTECT

V hornej časti okna sa nachádzajú tri záložky:

- **Všeobecné** – zadajte názov, smer, akciu (**Povoliť**, **Zakázať**, **Spýtať sa**), protokol a profil, pre ktorý bude pravidlo platné.

- **Lokálna strana** – zobrazuje informácie o lokálnej strane komunikácie, vrátane čísla portu alebo rozsahu portov a názov komunikujúcej aplikácie. Po kliknutí na **Pridať** si môžete vybrať z preddefinovaných zón alebo si vytvoriť novú zónu so zvoleným rozsahom IP adries.
- **Vzdialená strana** – informácie o vzdialenom porte alebo rozsahu portov. Taktiež môžete zadať zoznam IP adries alebo zón pre dané pravidlo. Po kliknutí na **Pridať** si môžete vybrať z preddefinovaných zón alebo si vytvoriť novú zónu so zvoleným rozsahom IP adries.

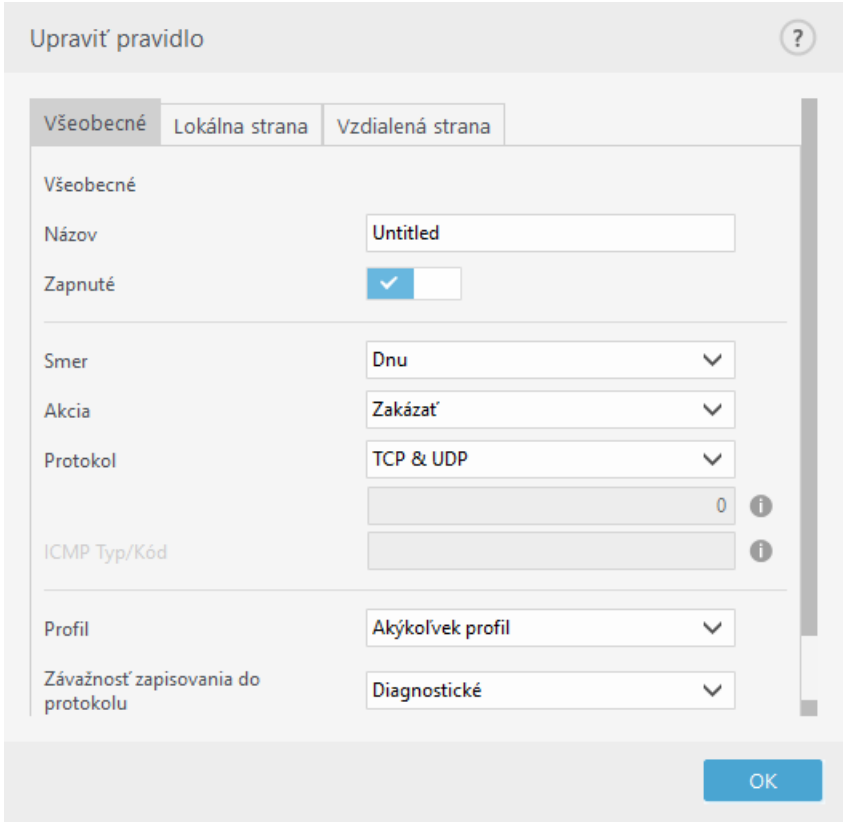
Pri vytváraní pravidla musíte zadať meno pravidla do poľa **Názov**. Z roletového menu **Smer** vyberte smer, ktorý sa vzťahuje na pravidlo, a z roletového menu **Akcia** vyberte akciu, ktorá bude vykonaná, ak bude komunikácia v súlade s príslušným pravidlom.

Protokol je komunikačný protokol použitý pri komunikácii. Vyberte protokol, ktorý bude použitý pre dané pravidlo.

ICMP Typ/Kód predstavuje číslo ICMP správy (napríklad 0 predstavuje správu „Echo Reply“).

Štandardne je každé pravidlo platné pre **Akýkoľvek profil**. Môžete prípadne vybrať aj vlastný profil firewallu z roletového menu **Profil**.

V prípade nastavenia **Závažnosti zapisovania do protokolu** bude aktivita súvisiaca s pravidlom zaznamenávaná do protokolu. Funkcia **Upozorniť používateľa** zobrazí oznámenie v prípade, že sa pravidlo použije.



Protokoly firewallu s akciou **Zakázať** a úrovňou závažnosti nastavenou na **Upozornenie** môžu byť zozbierané prostredníctvom konzoly ESET PROTECT.

V tomto príklade si vytvoríme nové pravidlo, ktoré povolí webovému prehliadaču Firefox pristupovať k webovým stránkam na Internete/lokálnej sieti:
1. Na karte **Všeobecné** povoľte odchádzajúcu komunikáciu cez protokoly TCP a UDP.
2. Kliknite na kartu **Lokálna strana**.
3. Zadajte cestu k vášmu webovému prehliadaču kliknutím na **...** (napr. *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
4. Na karte **Vzdialená strana** povoľte porty číslo 80 a 443, ak chcete povoliť štandardné prehliadanie internetu.

Prednastavené pravidlá je možné upravovať len v obmedzenej miere.

Pravidlo firewallu – Lokálna strana

Umožňuje zadať lokálnu aplikáciu a port/porty, pre ktoré má byť pravidlo uplatnené.

Port – čísla lokálnych portov. Ak nie je zadaný žiaden port, pravidlo sa týka celej komunikácie. Zadajte čísla portov alebo ich rozsah.

IP – pridanie adresy, rozsahu adries alebo podsiete, pre ktorú sa uplatňuje pravidlo. Ak nie je zadaná žiadna IP adresa, pravidlo sa týka celej komunikácie.

Zóny – zoznam pridaných zón.

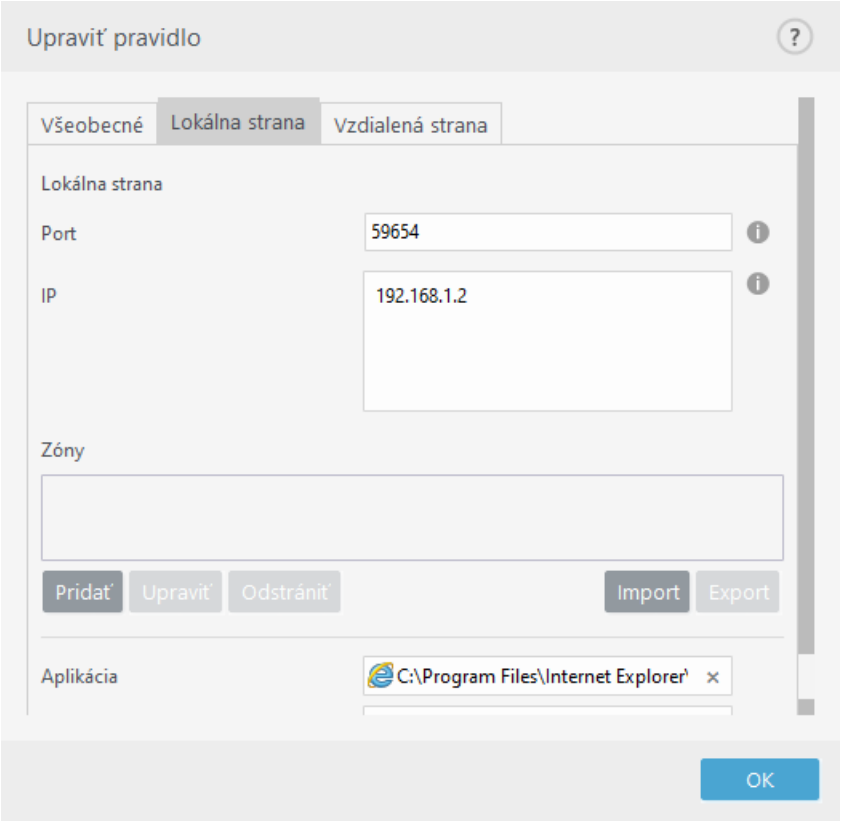
Pridať – pridá zónu označenú z roletového menu. Zónu možno vytvoriť v časti Zóny firewallu.

Odstrániť – odstráni zónu zo zoznamu.

Aplikácia – aplikácia, pre ktorú bude platiť pravidlo. Zadajte cestu k lokálnej aplikácii, pre ktorú bude pravidlo platiť.

Služba – roletové menu so zoznamom systémových služieb.

Môžete napríklad vytvoriť pravidlo pre nástroj mirror, ktorý poskytuje aktualizácie cez komunikáciu na porte 2221 pomocou služby EHttpSrv.



Pravidlo firewallu – Vzdialená strana

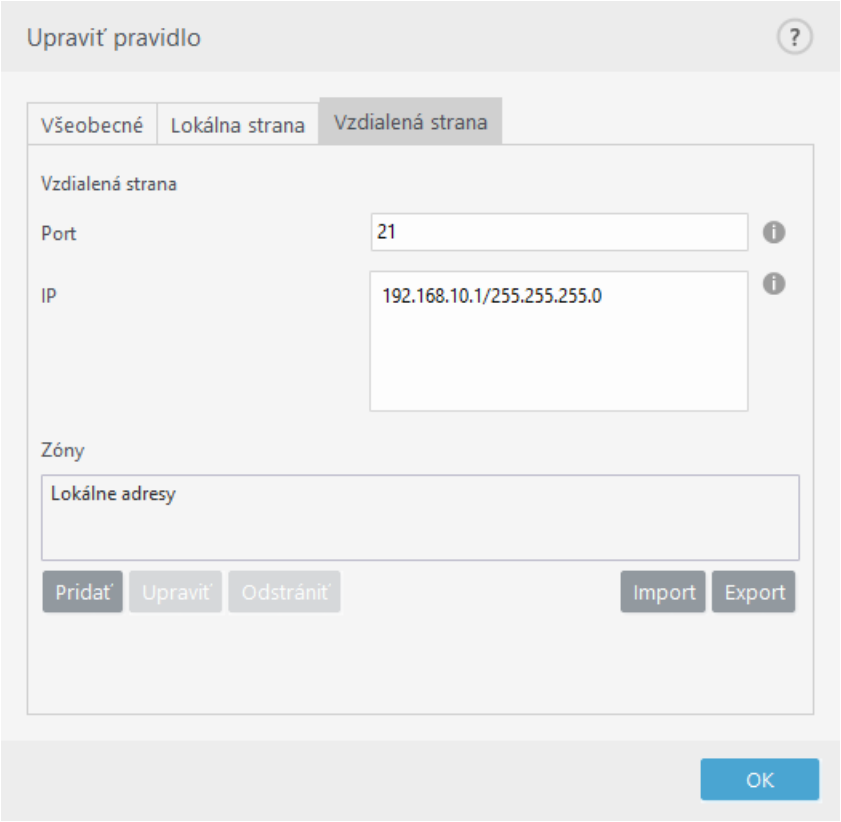
Port – čísla portov komunikácie so vzdialenou stranou. Ak nie je zadaný žiaden port, pravidlo sa týka celej komunikácie. Zadajte čísla portov alebo ich rozsah.

IP – umožňuje pridanie adresy, rozsahu adries alebo podsiete vzdialenej strany. Zadajte adresu, rozsah, podsieť alebo vzdialenú zónu, pre ktorú sa uplatňuje pravidlo. Ak nie je zadaná žiadna IP adresa, pravidlo sa týka celej komunikácie.

Zóny – zoznam pridaných zón.

Pridať – pridá zónu označenú z roletového menu. Zónu možno vytvoriť v časti Zóny firewallu.

Odstrániť – odstráni zónu zo zoznamu.



Dočasný blacklist IP adries

Ak chcete zobraziť IP adresy, ktoré boli zachytené ako zdroj útokov a pridané na blacklist s cieľom zablokovať na určitý čas spojenie, prejdite v ESET Endpoint Security do časti **Nastavenia** > **Sieť** > **Dočasný blacklist IP adries**. Dočasne blokované IP adresy sú blokované jednu hodinu.

Stĺpce

IP adresa – zobrazuje IP adresu, ktorá bola zablokovaná.

Dôvod blokovania – typ útoku, ktorému bolo zabránené (napríklad útok skenovaním portov TCP).

Časový limit – zobrazuje čas a dátum, kedy bude adresa vyradená zo zoznamu.

Ovládacie prvky

Odstrániť – kliknite pre odobratie adresy z blacklistu skôr, ako uplynie časový limit.

Odobrať všetky – kliknite pre odobratie všetkých adries z blacklistu.

Pridať výnimku – kliknite pre pridanie výnimky do IDS filtrovania firewallu.

Dôveryhodná zóna

Dôveryhodná zóna predstavuje skupinu sieťových adries, z ktorých firewall povolí prichádzajúcu komunikáciu. Nastavenia pre funkcie, ako napr. zdieľanie súborov na sieti alebo vzdialená plocha v dôveryhodnej zóne, nájdete v sekcii Povolené služby a pokročilé možnosti.

Skutočná dôveryhodná zóna je vytváraná dynamicky a samostatne pre každý sieťový adaptér na základe toho, v akej sieti je práve počítač pripojený. Adresy, ktoré patria alebo sú pridané do dôveryhodnej zóny, budú vždy považované za bezpečné. Ak sa sieťový adaptér pripojí na známu sieť, do zoznamu známych sietí sú automaticky pridané **Dodatočné dôveryhodné adresy** nastavené pre túto sieť. Ak je sieť domáca/pracovná, všetky priamo pripojené podsiete sú zahrnuté do dôveryhodnej zóny. Nastavenia dôveryhodnej zóny pre sieťový adaptér sa nachádzajú v hlavnom okne programu v sekcii **Nastavenia** na karte **Sieť** > **Sieťové adaptéry**.

Nastavenie zón

Zóna predstavuje súbor sieťových adries, ktoré vytvárajú jednu logickú skupinu IP adries. Zóny sú užitočné, ak potrebujete použiť rovnakú skupinu IP adries vo viacerých pravidlách. Na každú adresu danej skupiny sa následne aplikujú rovnaké pravidlá, definované spoločne pre celú skupinu. Príkladom takejto skupiny je napríklad **Dôveryhodná zóna**. Dôveryhodná zóna predstavuje skupinu sieťových adries bez akéhokoľvek blokovania firewallom. Nastavenie zón je dostupné cez **Rozšírené nastavenia** > **Ochrana siete** > **Základné** > **Zóny** kliknutím na tlačidlo **Upraviť** vedľa popisu **Zóny**. Ak chcete pridať zónu, kliknite na tlačidlo **Pridať**, zadajte **Názov** zóny a **Popis** a následne zadajte IP adresu do poľa **Vzdialená adresa počítača (IPv4, IPv6, rozsah, maska)**. Prečítajte si aj kapitolu Zóny firewallu.

Zóny firewallu

Viac informácií o zónach nájdete v kapitole Nastavenie zón.

Stĺpce

Názov – názov skupiny vzdialených počítačov.

IP adresy – vzdialené IP adresy, ktoré patria do konkrétnej zóny.

Ovládacie prvky

Ak ste sa rozhodli **pridať** alebo **upraviť** zónu, budú dostupné nasledujúce polia:

Názov – názov skupiny vzdialených počítačov.

Popis – všeobecný popis skupiny.

Vzdialená adresa počítača (IPv4, IPv6, rozsah, maska) – pridanie vzdialenej adresy, rozsahu adries alebo podsiete.

Odstrániť – odstránenie zóny zo zoznamu.

Berte, prosím, na vedomie, že prednastavené zóny nemôžu byť odstránené.

Protokol firewallu

Firewall v programe ESET Endpoint Security ukladá všetky dôležité udalosti do protokolov, ktoré si môžete zobraziť priamo z hlavného menu programu. Kliknite na **Nástroje** > **Protokoly** a z roletového menu **Protokoly** vyberte možnosť **Ochrana siete**. Ak chcete povoliť vytváranie rozšírených protokolov firewallu, prejdite do sekcie

Rozšírené nastavenia > **Nástroje** > **Protokoly** a nastavte minimálnu úroveň podrobnosti protokolov na možnosť **Diagnostické**. Do protokolu sa tak budú zapisovať všetky zablokované spojenia.

Súbory protokolov môžete použiť na riešenie problémov a odhalenie prienikov do systému. Protokoly modulu ESET Firewall obsahujú nasledujúce údaje:

- **Čas** – dátum a čas udalosti.
- **Udalosť** – názov udalosti.
- **Zdroj** – zdrojová sieťová adresa.
- **Cieľ** – cieľová sieťová adresa.
- **Protokol** – komunikačný protokol.
- **Názov pravidla/červa** – aplikované pravidlo alebo názov červa, ak bol identifikovaný.
- **Aplikácia** – názov komunikujúcej aplikácie.
- **Používateľ** – meno používateľa, ktorý bol prihlásený v systéme v čase zachytenia hrozby.

Podrobná analýza týchto údajov môže pomôcť odhaliť pokusy o narušenie bezpečnosti systému. Potenciálne bezpečnostné riziká a hrozby môžete včas odhaliť aj sledovaním rozličných faktorov. Napríklad, príliš časté spojenia z rôznych neznámych lokalít, hromadné pokusy o nadviazanie spojenia, komunikujúce neznáme aplikácie či nezvyčajné čísla portov môžu pomôcť v odhalení útoku a minimalizovaní jeho následkov.

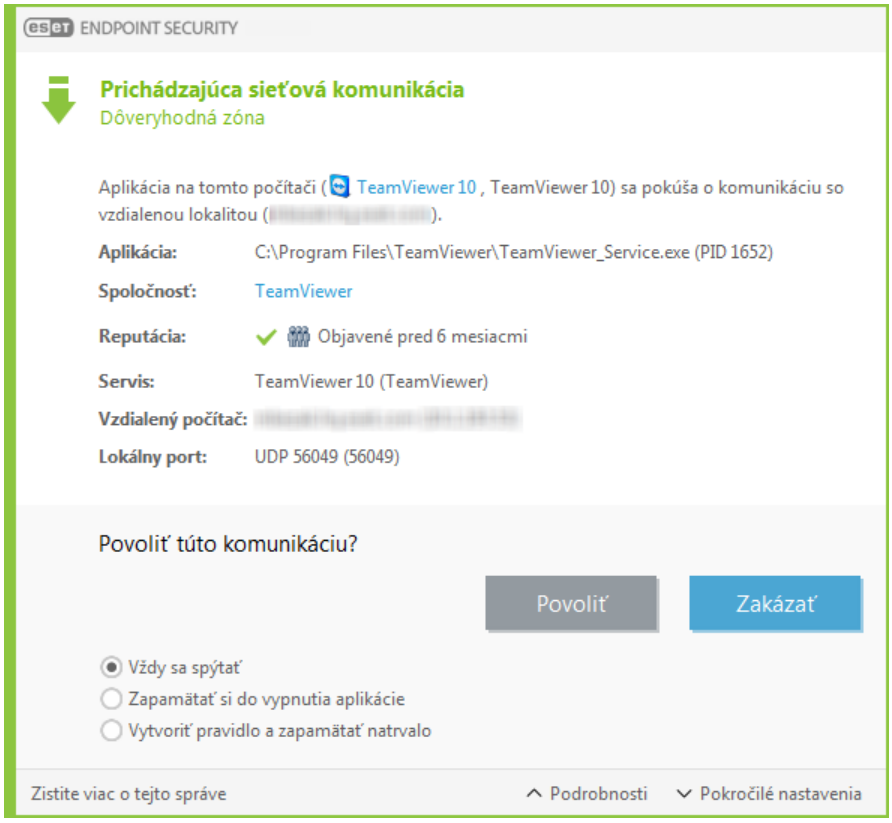
> **i** Správa o zneužití bezpečnostnej chyby je zaznamenaná do protokolu aj v tom prípade, že je už konkrétna zraniteľnosť opravená. Pokus o zneužitie je totiž zachytený a zablokovaný na úrovni siete ešte predtým, ako by mohlo dôjsť k samotnému zneužitiu bezpečnostnej zraniteľnosti.

Nadväzovanie spojenia – detekcia

Firewall deteguje každé nové sieťové spojenie. Nastavenie režimu filtrovania určuje, aké akcie sa vykonajú v prípade nového sieťového spojenia. Pri **Automatickom režime** alebo **Režime politík** firewall pracuje na základe prednastavených pravidiel a bez interakcie používateľa.

V prípade interaktívneho režimu sa pri každom novom sieťovom spojení zobrazí dialógové okno, ktoré informuje o zachytení nového sieťového spojenia a poskytuje podrobné informácie o danom spojení. Používateľ má možnosť toto spojenie povoliť alebo odmietnuť (zablokovať). V prípade, že opakovane povoľujete rovnaké sieťové spojenie, odporúčame vám vytvoriť pre toto spojenie nové pravidlo. V zobrazenom dialógovom okne označte možnosť **Zapamätať si akciu (vytvoriť pravidlo)**, čím sa zvolená akcia uloží do nastavení firewallu ako nové pravidlo. V prípade, že firewall v budúcnosti zachytí rovnaké spojenie, bez potreby interakcie používateľa naň aplikuje už existujúce pravidlo.

Možnosť **Dočasne si zapamätať akciu pre tento proces** spôsobí, že zvolená akcia (**Povoliť**/**Zakázať**) bude platná len dovtedy, kým aplikáciu nereštartujete, nezmeníte pravidlo alebo režim filtrovania, prípadne neaktualizujete modul firewallu alebo nereštartujete systém. Po vykonaní ktorejkoľvek z týchto akcií budú dočasné pravidlá zmazané.



Pri detekcii neznámych spojení a vytváraní príslušných pravidiel treba postupovať obozretne a povoľovať len tie spojenia, ktoré sú bezpečné. Firewall pri povolení všetkých spojení stráca svoje opodstatnenie. Dôležité parametre sieťových spojení:

- **Vzdialená strana** – povoľujte len spojenia na dôveryhodné a známe adresy.
- **Lokálna aplikácia** – neodporúčame povoliť spojenia neznámym aplikáciám a procesom.
- **Lokálny port** – komunikácia na známych portoch (napr. web – port číslo 80) je zvyčajne bezpečná.

Infiltrácie pre svoje šírenie vo veľkej miere využívajú internet a skryté spojenia, pomocou ktorých sú schopné infikovať vzdialené počítačové systémy. Správnym nastavením pravidiel firewallu je možné ochrániť systém pred rôznymi útokmi škodlivého kódu.

Riešenie problémov s ESET Firewallom

Ak máte pri používaní programu ESET Endpoint Security problémy so sieťovým spojením, existuje niekoľko spôsobov, ako zistiť, či tieto problémy zapríčiňuje ESET Firewall. ESET Firewall vám navyše umožňuje vytvoriť nové pravidlá alebo výnimky na vyriešenie problémov s pripojením.

Viac informácií o riešení problémov s ESET Firewallom nájdete v nasledujúcich kapitolách:

- Sprievodca riešením problémov
- Vytváranie protokolov a pravidiel alebo výnimiek z protokolu
- Vytvorenie výnimky z oznámenia firewallu
- Vytváranie rozšírených protokolov ochrany siete
- Riešenie problémov s filtrovaním protokolov

Sprievodca riešením problémov

Sprievodca riešením problémov monitoruje všetky blokované spojenia a pomôže vám pri riešení problémov firewallu s určitou aplikáciou alebo zariadením. Sprievodca vám navrhne nové pravidlá pre zlepšenie problémového stavu. **Sprievodcu riešením problémov** nájdete v hlavnom okne programu v sekcii **Nastavenia** > **Sieť**.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Pridanie výnimky firewallu pomocou Sprievodcu riešením problémov

Vytváranie protokolov a pravidiel alebo výnimiek z protokolu

Štandardne ESET Firewall nevytvára protokol o blokovaní sieťových spojení. Pre zobrazenie spojení blokovaných firewallom zapnite rozšírené protokoly ochrany siete v sekcii **Diagnostika** v **Rozšírených nastaveniach** po kliknutí na **Nástroje** > **Diagnostika**. Ak vo vytvorenom protokole nájdete spojenie, ktoré blokovať nechcete, môžete pre toto spojenie vytvoriť pravidlo alebo IDS pravidlo kliknutím pravým tlačidlom myši na daný záznam a výberom možnosti **Neblokovať podobné udalosti v budúcnosti**. Je potrebné mať na pamäti, že blokované spojenia môžu obsahovať tisíce údajov a môže byť veľmi ťažké nájsť špecifické spojenie, ktoré spôsobuje problém. Po vyriešení problému môžete vytváranie protokolov znova vypnúť.

Viac informácií o protokoloch nájdete v kapitole Protokoly.

Vo vytvorenom protokole je možné vidieť poradie, v akom firewall zablokoval konkrétne sieťové spojenia. Vytváranie pravidiel priamo z protokolu vám umožňuje prispôsobiť pravidlá presne podľa vašich potrieb.

Vytvorenie pravidla z protokolu

Nová verzia ESET Endpoint Security vám umožňuje vytvoriť pravidlo priamo z protokolu. V hlavnom okne programu kliknite na **Nástroje** > **Protokoly**. Z roletového menu vyberte položku **Ochrana siete**, pravým tlačidlom myši kliknite na protokol a z kontextového menu vyberte možnosť **Neblokovať podobné udalosti v budúcnosti**. Zobrazí sa oznámenie o vytvorení nového pravidla.

Aby bolo možné vytvárať pravidlá z protokolu, program ESET Endpoint Security musí byť nastavený nasledovne:

- V sekcii **Rozšírené nastavenia** (F5) > **Nástroje** > **Protokoly** nastavte minimálnu úroveň podrobnosti protokolov na možnosť **Diagnostický**.
- Povoľte možnosť **Zobraziť upozornenia aj pre prichádzajúce útoky na bezpečnostné diery** v sekcii **Rozšírené nastavenia** (F5) > **Ochrana siete** > **Ochrana pred sieťovými útokmi** > **Pokročilé možnosti** > **Detekcia útokov**.

Vytvorenie výnimky z oznámenia firewallu

Keď ESET Firewall deteguje škodlivú aktivitu na sieti, zobrazí oznámenie s popisom udalosti. Toto oznámenie obsahuje odkaz, ktorý vám umožňuje vytvoriť výnimku.

Ak sieťová aplikácia alebo zariadenie nespĺňa sieťové štandardy, môže dôjsť k opakovanému oznámeniu tej istej udalosti. Takýmto oznámeniam sa dá predísť vytvorením výnimky priamo z oznámenia na obrazovke.

Vytváranie rozšírených protokolov ochrany siete

Táto funkcionalita je navrhnutá na komplexné vytváranie protokolov pre technickú podporu spoločnosti ESET. Vzhľadom na značnú veľkosť protokolov a spomalenie počítača pri ich vytváraní použite túto možnosť, len ak vás na to vyzval pracovník technickej podpory spoločnosti ESET.

1. Prejdite do časti **Rozšírené nastavenia** > **Nástroje** > **Diagnostika** a povoľte možnosť **Zapnúť rozšírené protokoly ochrany siete**.
2. Potom sa pokúste znova vyvolať váš problém.
3. Vypnite rozšírené protokoly ochrany siete.
4. Vytvorené rozšírené PCAP protokoly ochrany siete nájdete v rovnakom adresári, do ktorého sa generujú aj diagnostické výpisy pamäte: *C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics*

Riešenie problémov s filtrovaním protokolov

Ak ste zaznamenali problémy s vaším webovým prehliadačom alebo e-mailovým klientom, v prvom rade treba zistiť, či je problém spôsobený kontrolou protokolov. Pre overenie tejto možnosti skúste dočasne vypnúť kontrolu protokolov v rozšírených nastaveniach (nezabudnite kontrolu znova zapnúť, keď skončíte, v opačnom prípade ostanú webové prehliadače a e-mailové klienty nechránené). Ak sa po vypnutí kontroly protokolov váš problém viac neprejavuje, je možné, že ide o jeden z nasledujúcich problémov:

Problémy aktualizácie alebo zabezpečenia komunikácie

Ak aplikácia hlási problém s aktualizáciou alebo so zabezpečením komunikačných kanálov:

- Ak je zapnuté filtrovanie protokolu SSL, skúste ho dočasne vypnúť. Ak to pomôže, môžete toto filtrovanie naďalej používať a umožniť aktualizáciu vytvorením výnimky pre problémovú komunikáciu:
  Prepnite filtrovanie protokolu SSL na interaktívny režim. Spustite znova aktualizáciu. Malo by sa zobraziť dialógové okno o šifrovanej komunikácii. Uistite sa, že aplikácia v okne je tá, ktorej problém riešite, a že certifikát pochádza z aktualizačného servera. Označte možnosť Zapamätať si akciu pre tento certifikát a vyberte Ignorovať. Ak sa nezobrazia ďalšie relevantné dialógové okná, môžete prepnúť režim filtrovania späť na automatický a problém by mal byť vyriešený.
- Ak aplikácia nie je webový prehliadač alebo e-mailový klient, môžete ju kompletne vylúčiť z kontroly protokolov (ak vylúčite z kontroly e-mailový klient alebo webový prehliadač, vystavíte tým váš počítač riziku infiltrácie). Aplikácie, ktorých komunikácia už bola predtým filtrovaná kontrolou protokolov, by už mali byť v zozname dostupnom pri pridávaní výnimky, takže manuálne pridanie by už nemalo byť potrebné.

Problém s prístupom na sieťové zariadenie

Ak nemáte prístup k funkcionalitám zariadení na vašej sieti (napríklad otváranie webovej stránky webkamery alebo prehranie videa na domácom multimediálnom prehrávači), skúste pridať Ipv4 a Ipv6 adresy do zoznamu vylúčených adries.

Problém s konkrétnou webovou stránkou

Pre vylúčenie webstránky z kontroly protokolov použite manažment URL adries. Napríklad, ak nemáte prístup k stránke https://www.gmail.com/intl/en/mail/help/about.html, skúste pridať *gmail.com* do zoznamu webových stránok vylúčených z kontroly.

Chyba "Niektoré podporované aplikácie na import koreňového certifikátu sú ešte spustené.“

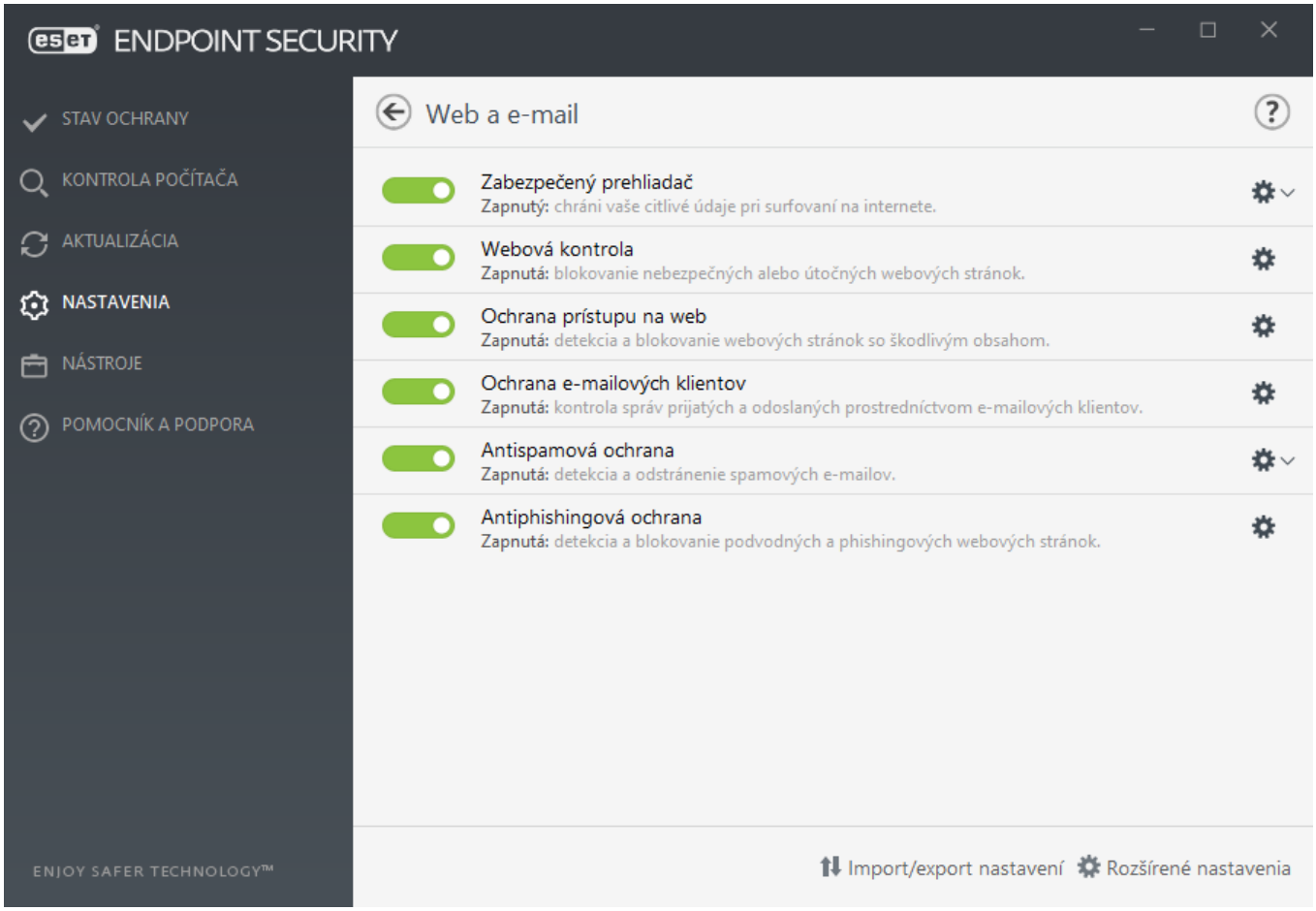
Ak povolíte kontrolu protokolu SSL, ESET Endpoint Security sa postará, aby nainštalované aplikácie dôverovali spôsobu kontroly protokolov SSL naimportovaním certifikátu do ich úložného priestoru certifikátov. Pri niektorých aplikáciách to nie je možné vykonať za behu. Napríklad ani v aplikáciách Firefox a Opera. Uistite sa preto, že nie sú spustené (napríklad cez Správcu úloh – skontrolujte, či sa v zozname Procesy nenachádza firefox.exe alebo opera.exe) a skúste znova.

Chyba o nedôveryhodnom vydavateľovi alebo neplatnom podpise certifikátu

Toto oznámenie znamená, že import certifikátu popísaný vyššie zlyhal. V prvom rade sa uistite, že žiadna zo zmienených aplikácií nebeží. Potom vypnite kontrolu protokolu SSL a následne ju zapnite. Tento postup znova spustí import.

Web a e-mail

Nastavenia webu a e□mailov je možné nájsť v sekcii **Nastavenia** > **Web a e□mail**. Odtiaľto môžete tiež pristupovať k podrobnejším nastaveniam programu.



Zabezpečený prehliadač chráni vaše citlivé údaje pri surfovaní na internete.

Modul **Webová kontrola** poskytuje správcom automatizované nástroje slúžiace na ochranu pracovných staníc a nastavenie obmedzení pri prehliadaní internetu. Funkcia webovej kontroly zabraňuje prístupu na webové stránky s nevhodným alebo škodlivým obsahom. Viac si môžete prečítať v kapitole Webová kontrola.

Internetové pripojenie patrí do štandardnej výbavy osobných počítačov. Bohužiaľ sa stalo aj hlavným médiom prenosu škodlivého softvéru. Preto je veľmi dôležité venovať zvýšenú pozornosť **Ochrane prístupu na web**.

Ochrana e□mailových klientov zabezpečuje kontrolu e□mailovej komunikácie prijímanej prostredníctvom protokolov POP3(S) a IMAP(S). Pomocou doplnku (pluginu) do e□mailových klientov zabezpečuje ESET Endpoint Security kontrolu všetkej komunikácie týchto klientov.

Antispamová ochrana zabezpečuje filtrovanie nevyžiadaných e-mailových správ.

Po kliknutí na ikonu ozubeného kolesa vedľa položky Antispamová ochrana sa zobrazia nasledujúce možnosti:

Konfigurovať – otvoria sa rozšírené nastavenia pre antispamovú ochranu e□mailových klientov.

Používateľský zoznam adries – zobrazí sa dialógové okno, kde môžete pridať/odobrať/upraviť e□mailové adresy, ktoré považujete za dôveryhodné alebo nedôveryhodné. Na základe týchto pravidiel budú e□maily z adries uvedených v príslušných zoznamoch buď vynechané z kontroly, alebo označené ako spam. Ak chcete pridať, upraviť alebo odstrániť e□mailové adresy, ktoré môžu byť falošné a zneužívané na odosielanie nevyžiadaných správ, kliknite na Používateľský zoznam výnimiek. Správy prijaté z týchto adries budú vždy skontrolované na prítomnosť spamu.

Antiphishingová ochrana predstavuje dodatočnú bezpečnostnú vrstvu, ktorá chráni pred podvodnými webovými stránkami pokúšajúcimi sa z používateľov vylákať heslá a iné citlivé informácie. Nastavenia antiphishingovej

ochrany je možné nájsť v menu Nastavenia > Web a e-mail. Pre viac informácií si prečítajte kapitolu Antiphishingová ochrana.

Modul webovej/e-mailovej/antiphishingovej/antispamovej ochrany môžete dočasne vypnúť pomocou prepínača .

Filtrovanie protokolov

Antivírusovú ochranu aplikačných protokolov zabezpečuje skenovacie jadro ThreatSense, v ktorom sú sústredené všetky pokročilé metódy detekcie malvéru. Filtrovanie protokolov prebieha automaticky a nezávisle od použitého internetového prehliadača alebo e□mailového klienta. Meniť nastavenia SSL je možné v **Rozšírených nastaveniach** (F5) v sekcii **Web a e□mail** > **SSL/TLS**.

Zapnúť kontrolu obsahu aplikačných protokolov – zapne/vypne filtrovanie protokolov. Viaceré súčasti programu ESET Endpoint Security (Ochrana prístupu na web, Ochrana e-mailových klientov, Antiphishingová ochrana, Webová kontrola) sú závislé na tomto nastavení a po vypnutí filtrovania protokolov nebudú funkčné.

Vylúčené aplikácie – umožňuje vylúčenie aplikácie z filtrovania protokolov. Odporúčame použiť v prípade, že filtrovanie protokolov obmedzuje spojenie.

Vylúčené IP adresy – umožňuje vylúčenie vzdialenej adresy z filtrovania protokolov. Odporúčame použiť v prípade, že filtrovanie protokolov obmedzuje spojenie.

IPv4 adresy a masky:
• *192.168.0.10* – IP adresa individuálneho počítača, pre ktorý sa má uplatniť pravidlo.
• *192.168.0.1* až *192.168.0.99* – začiatočná a koncová IP adresa na stanovenie rozsahu IP adries (skupiny počítačov), pre ktoré sa má uplatniť pravidlo.
• Podsieť (skupina počítačov) definovaná IP adresou a maskou. Napríklad *255.255.255.0* je maska podsiete pre prefix *192.168.1.0/24*, čo znamená rozsah adries od *192.168.1.1* do 192.168.1.254.
IPv6 adresy a masky:
• *2001:718:1c01:16:214:22ff:fec9:ca5* – IPv6 adresa individuálneho počítača, pre ktorý sa má uplatniť pravidlo.
• *2002:c0a8:6301:1::1/64* – IPv6 adresa s dĺžkou predpony 64 bitov, čo znamená *2002:c0a8:6301:0001:0000:0000:0000:0000 až 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

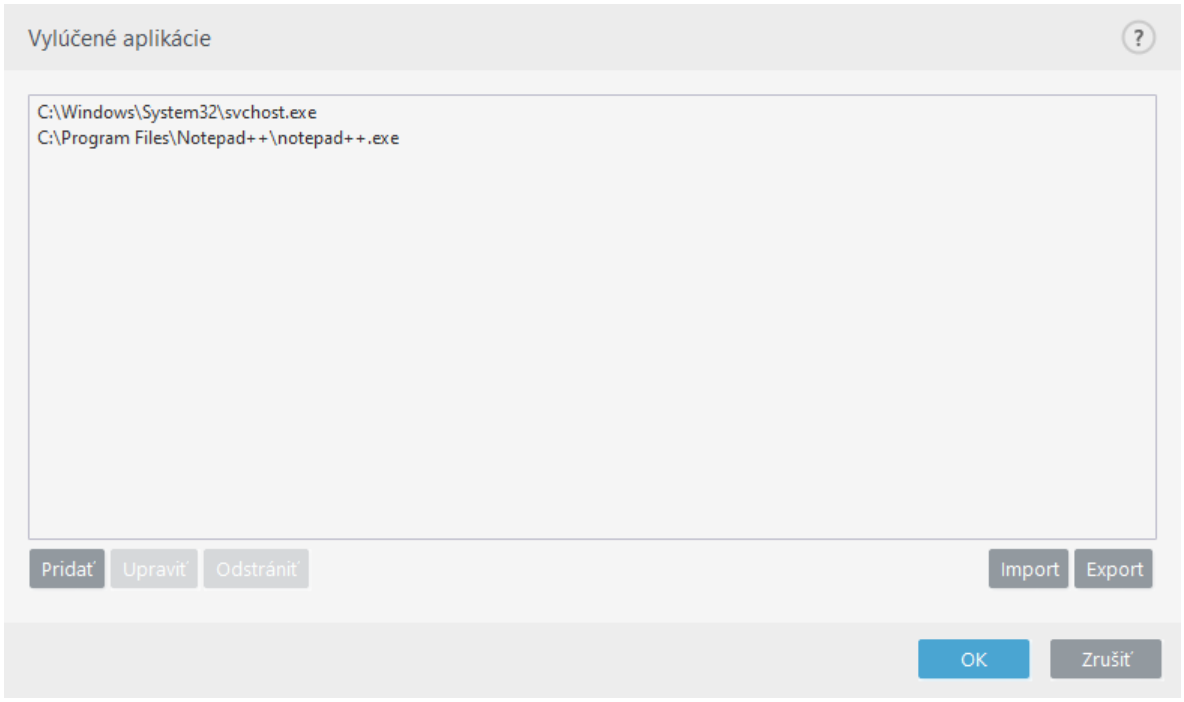
Vylúčené aplikácie

Ak chcete vylúčiť aplikácie z kontroly protokolov, pridajte ich do tohto zoznamu. Po pridaní do zoznamu nebude HTTP, POP3, či IMAP komunikácia označených aplikácií kontrolovaná na prítomnosť škodlivého kódu. Odporúčame používať túto možnosť iba v prípade aplikácií, ktoré by so zapnutou kontrolou protokolov nefungovali správne.

Aplikácie a služby, ktoré sú ovplyvnené kontrolou protokolov, sa automaticky zobrazia po kliknutí na tlačidlo **Pridať**.

Upraviť – umožňuje upravovať zvolené položky v zozname.

Odstrániť – umožňuje odstrániť zvolené položky zo zoznamu.



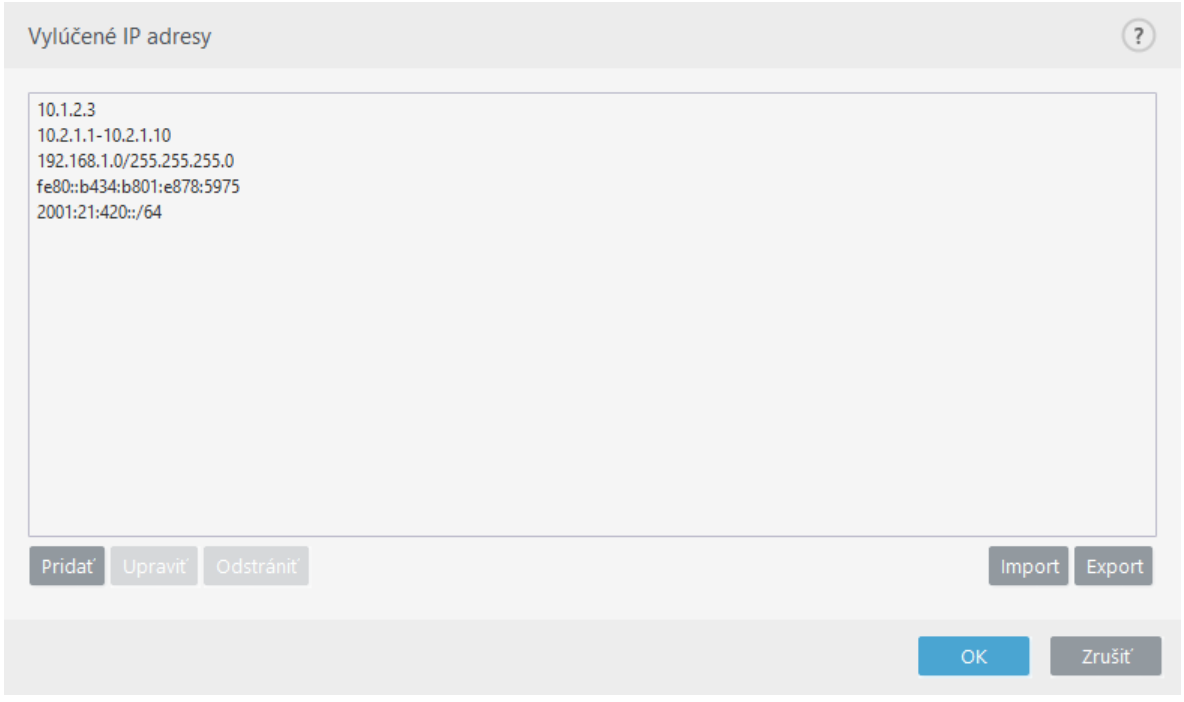
Vylúčené IP adresy

IP adresy uvedené v zozname budú vylúčené z filtrovania obsahu protokolov. HTTP/POP3/IMAP komunikácia z/na zvolené adresy nebude kontrolovaná na prítomnosť hrozieb. Odporúčame používať túto možnosť iba v prípade dôveryhodných IP adries.

Pridať – umožňuje pridať IP adresu, rozsah adries alebo podsieť vzdialeného bodu, na ktorý je uplatnené pravidlo.

Upraviť – umožňuje upravovať zvolené položky v zozname.

Odstrániť – umožňuje odstrániť zvolené položky zo zoznamu.



SSL/TLS

ESET Endpoint Security umožňuje kontrolu komunikácií využívajúcich protokol SSL. Kontrolu možno prispôsobiť podľa toho, či certifikát využívaný danou komunikáciou SSL je dôveryhodný, neznámy alebo je v zozname certifikátov, ktoré sú vylúčené z kontroly komunikácie chránenej protokolom SSL.

Zapnúť filtrovanie protokolu SSL/TLS – filtrovanie protokolov je predvolene zapnuté. Filtrovanie protokolu SSL/TLS môžete vypnúť v **Rozšírených nastaveniach** po kliknutí na **Web a e□mail** > **SSL/TLS** alebo prostredníctvom politiky. Ak je filtrovanie protokolov vypnuté, program nebude kontrolovať komunikáciu cez SSL.

K dispozícii sú tieto **režimy filtrovania protokolov SSL/TLS**:

Režim filtrovania	Popis
Automatický režim	Predvolený režim, ktorý bude kontrolovať len vybrané aplikácie, ako sú webové prehliadače a e□mailové klienty. V prípade potreby môžete kedykoľvek rozšíriť zoznam aplikácií, ktorých komunikáciu chcete kontrolovať.
Interaktívny režim	Pri prístupe k novej webovej stránke chránenej protokolom SSL- (s neznámym certifikátom) sa zobrazí okno s možnosťou výberu akcie. Tento režim vám umožňuje vytvoriť zoznam certifikátov/aplikácií SSL, ktoré budú z kontroly vylúčené.
Režim politiky	Vyberte tento režim, ak chcete kontrolovať všetku komunikáciu chránenú protokolom SSL okrem komunikácie chránenej certifikátmi vylúčenými z kontroly. Pri nadviazaní novej komunikácie využívajúcej zatiaľ neznámy certifikát, ktorý je dôveryhodne podpísaný, nebude používateľ upozornený a komunikácia sa bude automaticky filtrovať. Ak používateľ pristupuje na server používajúci nedôveryhodný certifikát, pričom bol tento používateľom označený ako dôveryhodný (zaradený do zoznamu dôveryhodných certifikátov), komunikácia so serverom bude povolená a prenášaný obsah bude filtrovaný.

Zoznam SSL/TLS-filtrovaných aplikácií môžete použiť na prispôsobenie správania programu ESET Endpoint Security pre konkrétne aplikácie.

Zoznam známych certifikátov vám umožňuje nastaviť správanie programu ESET Endpoint Security pre konkrétne SSL certifikáty.

Vylúčiť komunikáciu s dôveryhodnými doménami – ak je táto možnosť povolená, komunikácia s dôveryhodnými doménami bude vylúčená z kontroly. Dôveryhodnosť domény sa určuje na základe integrovaného whitelistu.

Blokovať šifrovanú komunikáciu používajúcu zastaraný protokol SSL v2 – komunikácia cez staršiu verziu protokolu SSL bude automaticky zablokovaná.

> Adresy nebudú filtrované v prípade, že je aktívne nastavenie **Vylúčiť komunikáciu s dôveryhodnými doménami** a daná doména je považovaná za dôveryhodnú.

Koreňový certifikát

Koreňový certifikát – pre správne fungovanie SSL komunikácie v danom prehliadači/e□mailovom kliente je nevyhnutné, aby do jeho zoznamu známych koreňových certifikátov (vydavateľov) bol pridaný aj certifikát spoločnosti ESET, spol. s r. o. Možnosť **Pridať koreňový certifikát do známych prehliadačov** by teda mala ostať označená. Táto možnosť by mala byť aktívna, aby sa zabezpečilo automatické pridanie certifikátu do známych prehliadačov (napr. Opera, Firefox). Do prehliadačov využívajúcich úložisko systémových certifikátov je certifikát pridaný automaticky (napr. Internet Explorer).

V prípade nepodporovaných prehliadačov môžete certifikát exportovať kliknutím na **Zobraziť certifikát** > **Podrobnosti** > **Kopírovať do súboru** a následne manuálne importovať do prehliadača.

Platnosť certifikátu

Akcia v prípade nemožnosti overiť dôveryhodnosť certifikátu – v niektorých prípadoch sa dôveryhodnosť certifikátu webovej stránky nedá overiť pomocou úložiska koreňových certifikátov vydaných dôveryhodnými certifikačnými autoritami (TRCA). Môže ísť napríklad o certifikát s uplynutou platnosťou, nedôveryhodný certifikát, certifikát neplatný pre konkrétnu doménu alebo podpis, ktorý je možné overiť, ale certifikát ním nie je správne podpísaný. Legitímne webové stránky vždy používajú dôveryhodné certifikáty. Ak stránka takýto certifikát nemá, môže to znamenať, že útočník dešifruje vašu komunikáciu alebo má stránka technické problémy.

Ak je označená možnosť **Spýtať sa používateľa na platnosť certifikátu** (predvolené nastavenie), budete v prípade nadviazania šifrovanej komunikácie vyzvaný na výber akcie, ktorá sa má vykonať. Zobrazí sa okno, kde je možné označiť daný certifikát ako dôveryhodný alebo ho vylúčiť z kontroly dôveryhodnosti. V prípade, že certifikát nie je v zozname TRCA, okno je červené. V opačnom prípade je okno zelené.

Ak zvolíte možnosť **Zablokovať komunikáciu využívajúcu daný certifikát**, komunikácia s webovou stránkou využívajúcou nedôveryhodný certifikát sa vždy zablokuje.

Akcia v prípade poškodeného certifikátu – poškodený certifikát znamená, že certifikát používa formát, ktorý program ESET Endpoint Security nevie rozpoznať, alebo už bol prijatý v poškodenom stave (napríklad bol prepísaný náhodnými údajmi). V tomto prípade odporúčame ponechať označenú možnosť **Zablokovať komunikáciu využívajúcu daný certifikát**. Ak je zvolená možnosť **Spýtať sa používateľa na platnosť certifikátu**, pri nadviazaní šifrovanej komunikácie bude používateľ vyzvaný na výber akcie.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Oznámenia produktu ESET týkajúce sa certifikátov
- Pri návšteve webovej stránky sa zobrazilo upozornenie na nedôveryhodný certifikát

Certifikáty

Pre správne fungovanie SSL komunikácie v danom prehliadači/e-mailovom kliente je nevyhnutné, aby do jeho zoznamu známych koreňových certifikátov (vydavateľov) bol pridaný aj certifikát spoločnosti ESET, spol. s r. o. Možnosť **Pridať koreňový certifikát do známych prehliadačov** by teda mala ostať označená. Táto možnosť zabezpečuje jeho automatické pridanie do známych prehliadačov (napr. Opera, Firefox). Do prehliadačov, ktoré používajú ukladací priestor systémových certifikátov, bude certifikát pridaný automaticky (napr. Internet Explorer). Pre nepodporované prehliadače môže byť certifikát vyexportovaný cez tlačidlo **Zobraziť certifikát** > **Podrobnosti** > **Kopírovať do súboru** a následne manuálne naimportovaný do prehliadača.

V niektorých prípadoch sa nedá overiť platnosť certifikátu pomocou certifikačných autorít (napr. VeriSign). To znamená, že certifikát je niekým samostatne podpísaný (napr. administrátorom webového servera alebo malou firmou) a považovanie tohto certifikátu za dôveryhodný nemusí vždy predstavovať riziko. Väčšina veľkých obchodných spoločností (napr. banky) používajú certifikát podpísaný certifikačnou autoritou (TRCA – Trusted Root Certification Authorities). Ak je označená možnosť **Spýtať sa používateľa na platnosť certifikátu** (predvolená), používateľ bude v prípade nadviazania šifrovanej komunikácie upozornený na výber akcie. Zobrazí sa okno, kde je možné rozhodnúť, či označiť daný certifikát ako dôveryhodný, alebo sa vylúči z kontroly dôveryhodnosti. V prípade, že certifikát nie je v zozname TRCA, okno je červené. V opačnom prípade je okno zelené.

Pomocou možnosti **Zablokovať komunikáciu využívajúcu daný certifikát** sa vždy zablokuje komunikácia s web

stránkou využívajúcou neoverený certifikát.

Ak je certifikát neplatný alebo poškodený, znamená to, že mu uplynula platnosť alebo bol nesprávne podpísaný. V tomto prípade sa odporúča zakázať komunikáciu využívajúcu daný certifikát.

Šifrovaná sieťová komunikácia

Ak je počítač nastavený na kontrolu protokolu SSL, v nasledujúcich dvoch situáciách sa zobrazí dialógové okno s výzvou vybrať si želanú akciu:

Prvá situácia nastáva, ak stránka používa neoveriteľný alebo neplatný certifikát a program ESET Endpoint Security je v takýchto prípadoch nastavený pýtať sa používateľa (predvolene len pri neoveriteľných certifikátoch). Zobrazí sa dialógové okno s možnosťami **Blokovať** alebo **Povoliť** spojenie. Certifikát je považovaný za nedôveryhodný, ak sa nenachádza v úložisku koreňových certifikátov vydaných dôveryhodnými certifikačnými autoritami (Trusted Root Certification Authorities store – TRCA).

Druhá situácia nastáva, ak je **Režim filtrovania protokolu SSL** nastavený na **Interaktívny režim**. V takomto prípade sa používateľovi zobrazí dialógové okno pre každú webovú stránku s možnosťami **Kontrolovať** alebo **Ignorovať** danú sieťovú komunikáciu. Niektoré aplikácie kontrolujú, či ich SSL komunikácia nie je zmenená alebo sledovaná inou aplikáciou, v takomto prípade musí ESET Endpoint Security ignorovať komunikáciu týchto aplikácií, aby nedošlo k obmedzeniu ich funkčnosti.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
- Oznámenia produktu ESET týkajúce sa certifikátov
- Pri návšteve webovej stránky sa zobrazilo upozornenie na nedôveryhodný certifikát

V oboch hore uvedených prípadoch môže používateľ označiť, aby si program zapamätal zvolenú akciu. Zapamätané akcie sú uložené v Zozname známych certifikátov.

Zoznam známych certifikátov

Pomocou **Zoznamu známych certifikátov** môžete prispôsobiť správanie ESET Endpoint Security pre konkrétne SSL certifikáty, ako aj zapamätanie akcií zvolených pri **Interaktívnom režime** nastavenom v časti **Režim filtrovania protokolu SSL/TLS**. Upravovanie zoznamu je možné v sekcii **Rozšírené nastavenia** (klávesová skratka F5) > **Web a e-mail** > **SSL/TLS** > **Zoznam známych certifikátov**.

V okne **Zoznam známych certifikátov** sú dostupné nasledujúce možnosti:

Stĺpce

Názov – názov certifikátu.

Vydavateľ certifikátu – meno autora certifikátu.

Predmet certifikátu – identifikuje entitu asociovanú s verejným kľúčom uloženým v poli predmet verejného kľúča.

Prístup – ako Akciu prístupu zvoľte **Povoliť** alebo **Blokovať** na povolenie alebo blokovanie komunikácie zabezpečenej certifikátom bez ohľadu na jeho dôveryhodnosť. Vyberte možnosť **Automaticky** na povolenie dôveryhodných certifikátov a pýtanie sa na nedôveryhodné certifikáty. Ak vyberiete možnosť **Spýtať sa**, pri

každej komunikácii sa zobrazí okno s výberom akcie.

Kontrolovať – vyberte **Kontrolovať** alebo **Ignorovať** ako **Akciu kontroly** podľa toho, či chcete kontrolovať alebo ignorovať komunikáciu zabezpečenú týmto certifikátom. K dispozícii je aj možnosť **Automaticky**, ktorá spustí kontrolu v automatickom režime a zobrazí výzvu na výber akcie v interaktívnom režime. Ak vyberiete možnosť **Spýtať sa**, pri každej komunikácii sa zobrazí okno s výberom akcie.

Ovládacie prvky

Pridať – certifikát môže byť načítaný manuálne ako súbor s príponou *.cer*, *.crt* alebo *.pem*. Kliknite na **Súbor**, ak chcete nahrať lokálny certifikát, alebo na **URL** a zadajte presnú adresu online certifikátu.

Upraviť – označte certifikát, ktorý chcete konfigurovať, a kliknite na **Upraviť**.

Odstrániť – označte certifikát a kliknite na **Odstrániť** pre jeho odstránenie.

OK/Zrušiť – kliknite na **OK** pre uloženie zmien v nastavení alebo na **Zrušiť**, ak chcete okno zatvoriť bez uloženia vykonaných zmien.

Zoznam SSL/TLS-filtrovaných aplikácií

Zoznam SSL/TLS-filtrovaných aplikácií môžete použiť na prispôsobenie správania programu ESET Endpoint Security pre konkrétne aplikácie, ako aj na zapamätanie zvolených akcií pri **Interaktívnom režime** nastavenom v sekcii **Režim filtrovania protokolu SSL/TLS**. Tento zoznam môžete nájsť v časti **Rozšírené nastavenia** (klávesová skratka F5) > **Web a e-mail** > **SSL/TLS** > **Zoznam SSL/TLS-filtrovaných aplikácií**.

V okne **Zoznam SSL/TLS-filtrovaných aplikácií** sú dostupné nasledujúce možnosti:

Stĺpce

Aplikácia – vyberte spustiteľný súbor zo stromovej štruktúry, kliknutím na **...** alebo cestu k súboru aplikácie zadajte manuálne.

Akcia kontroly – vyberte **Kontrolovať** alebo **Ignorovať**. K dispozícii je aj možnosť **Automaticky**, ktorá spustí kontrolu v automatickom režime a zobrazí výzvu na výber akcie v interaktívnom režime. Ak vyberiete možnosť **Spýtať sa**, pri každej komunikácii sa zobrazí okno s výberom akcie.

Ovládacie prvky

Pridať – pridajte filtrovanú aplikáciu.

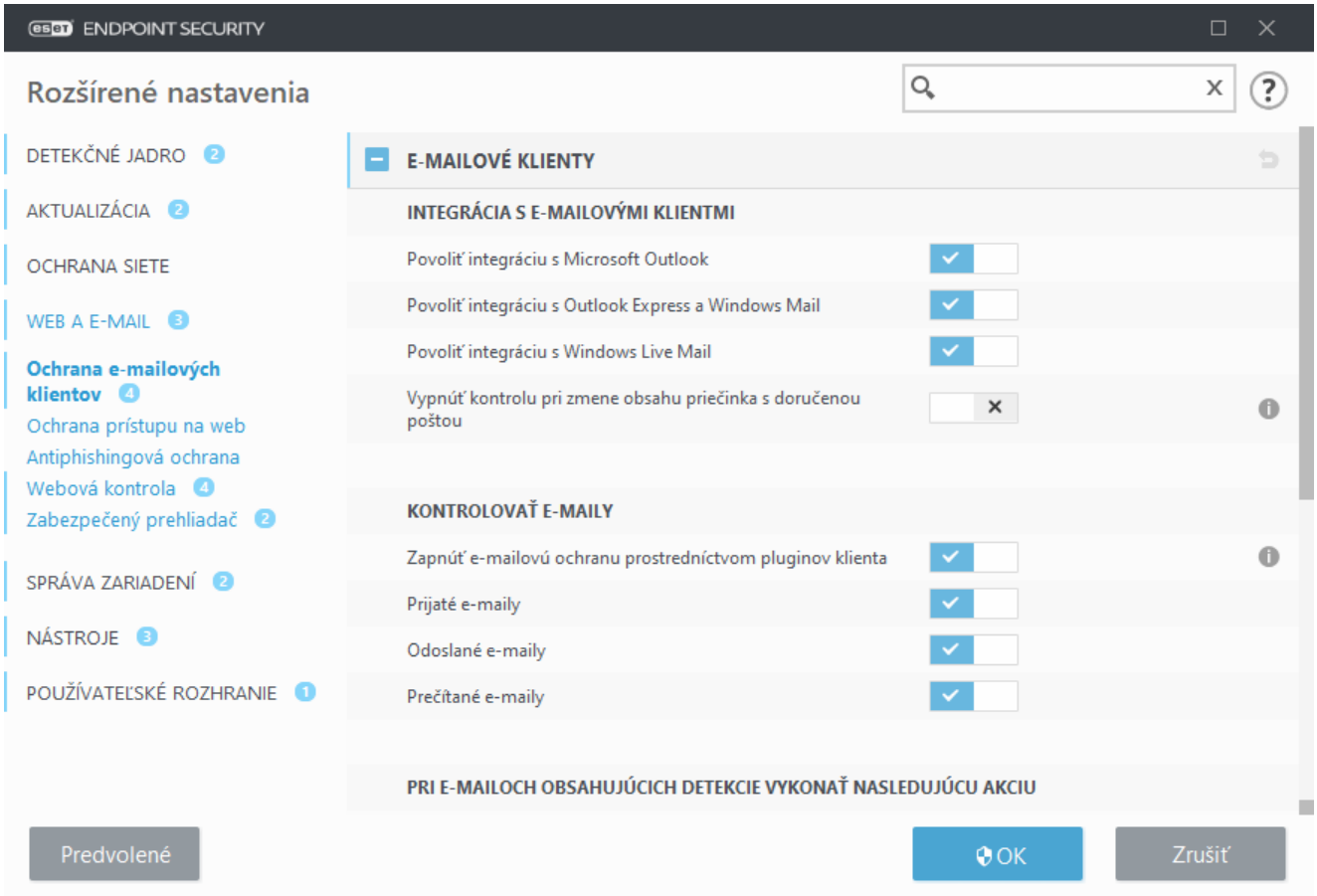
Upraviť – označte certifikát, ktorý chcete konfigurovať, a kliknite na **Upraviť**.

Odstrániť – označte certifikát a kliknite na **Odstrániť** pre jeho odstránenie.

OK/Zrušiť – kliknite na **OK** pre uloženie zmien v nastavení alebo na **Zrušiť**, ak chcete okno zatvoriť bez uloženia vykonaných zmien.

Ochrana e-mailových klientov

Integrácia programu ESET Endpoint Security s vaším e-mailovým klientom zlepšuje aktívnu ochranu pred škodlivým kódom v e-mailových správach. V prípade, že je daný e-mailový klient podporovaný, je možné povoliť integráciu v programe ESET Endpoint Security. Pri integrácii dochádza k vloženiu panela nástrojov ESET Endpoint Security priamo do e-mailového klienta, čo prispieva k účinnejšej kontrole e-mailových správ. Nastavenia integrácie sú dostupné cez **Rozšírené nastavenia** (F5) > **Web a e-mail** > **Ochrana e-mailových klientov** > **E-mailové klienty**.



Kontrolovať e-maily

Zapnúť e-mailovú ochranu prostredníctvom pluginov klienta – ak je táto možnosť deaktivovaná, ochrana prostredníctvom pluginov e-mailového klienta je vypnutá.

Prijaté emaily – ak je funkcia zapnutá, kontroluje prijaté e-mailové správy.

Odoslané emaily – ak je funkcia zapnutá, kontroluje odoslané e-mailové správy.

Prečítané emaily – ak je funkcia zapnutá, kontroluje prečítané e-mailové správy.

> Odporúčame ponechať možnosť **Zapnúť e-mailovú ochranu prostredníctvom pluginov klienta** aktívnu. V prípade, že integrácia nie je povolená alebo funkčná, bude e-mailová komunikácia stále chránená filtrovaním protokolov (IMAP/IMAPS a POP3/POP3S).

Pri e-mailoch obsahujúcich detekcie vykonať nasledujúcu akciu

Žiadna akcia – ak je táto možnosť povolená, program nájde e-mailové správy s infikovanými prílohami, no nevykoná s nimi žiadnu akciu.

Odstrániť email – program upozorní používateľa na infikované prílohy a odstráni celú e-mailovú správu.

Presunúť e-mail do priečinka vymazaných správ – program bude automaticky presúvať infikované správy do priečinka Vymazané správy.

Presunúť e-mail do priečinka (predvolená akcia) – program bude automaticky presúvať infikované správy do zadaného priečinka.

Priečinok – priečinok, do ktorého bude program presúvať správy, v ktorých boli zachytené infiltrácie.

Opakovať kontrolu po aktualizácii – ak je táto možnosť povolená, program opätovne skontroluje infikované správy po aktualizácii detekčného jadra.

Zohľadniť výsledky kontroly z iných modulov – modul emailovej ochrany bude môcť namiesto opätovnej kontroly využívať výsledky kontroly vykonanej iným modulom ochrany.

E-mailové protokoly

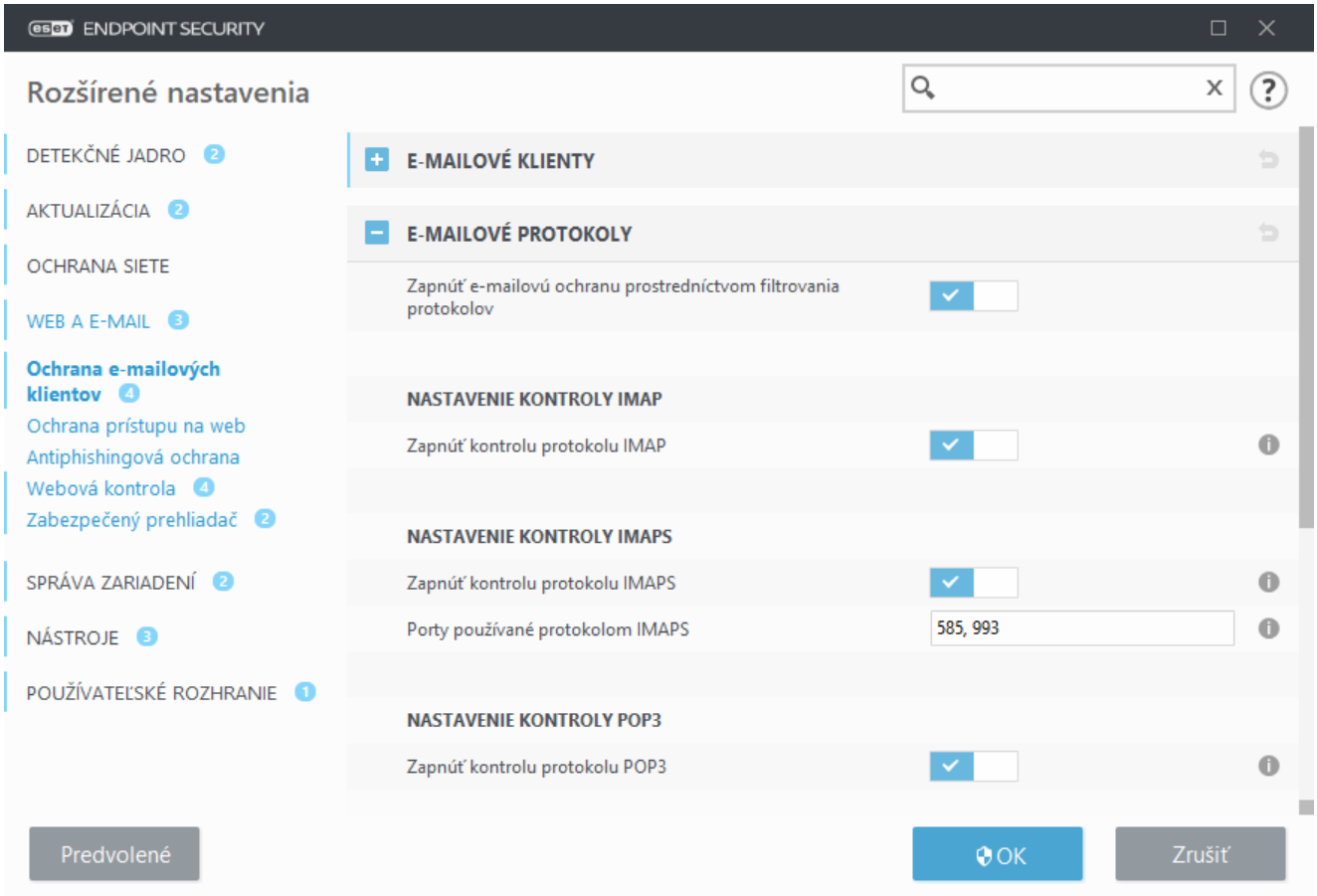
IMAP a POP3 sú najrozšírenejšie protokoly slúžiace na príjem e□mailovej komunikácie prostredníctvom e□mailového klienta. IMAP (Internet Message Access Protocol) je internetový protokol na prijímanie e□mailov. V porovnaní s protokolom POP3 má niekoľko výhod, napríklad umožňuje viacerým klientom naraz pripojiť sa k tej istej e-mailovej schránke a zachovávať informácie o stave správy (napríklad, či správa bola prečítaná, odstránená alebo či na ňu bolo odpovedané). Modul zabezpečujúci kontrolu sa zavádza pri štarte operačného systému a počas celej doby je zavedený v pamäti.

ESET Endpoint Security zabezpečuje ochranu týchto protokolov nezávisle od používaného e□mailového klienta a bez potreby zmeny jeho konfigurácie. Predvolene je všetka komunikácia prostredníctvom protokolov POP3 a IMAP kontrolovaná, bez ohľadu na predvolené čísla portov POP3/IMAP.
Protokol MAPI nie je kontrolovaný. Komunikáciu s Microsoft Exchange Serverom je však možné kontrolovať prostredníctvom modulu integrácie v e□mailových klientoch, ako je Microsoft Outlook.

Odporúčame ponechať možnosť **Zapnúť e□mailovú ochranu prostredníctvom filtrovania protokolov** aktívnu. Nastavenia kontroly protokolov IMAP/IMAPS a POP3/POP3S sú dostupné cez Rozšírené nastavenia > **Web a e□mail** > **Ochrana e□mailových klientov** > **E□mailové protokoly**.

ESET Endpoint Security podporuje aj kontrolu komunikácie cez protokoly IMAPS (585, 993) a POP3S (995). Pri tejto komunikácii sú prenášané údaje medzi serverom a klientom zašifrované. ESET Endpoint Security kontroluje komunikáciu využívajúcu protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovať komunikáciu len na portoch definovaných v poli **Porty používané protokolom IMAP/POP3**, pričom nezáleží na verzii operačného systému. V prípade potreby môžu byť pridané aj ďalšie komunikačné porty. Čísla portov musia byť oddelené čiarkou.

Šifrovaná komunikácia je predvolene kontrolovaná. Na zobrazenie nastavení kontroly prejdite do časti SSL/TLS v Rozšírených nastaveniach. Kliknite na **Web a e□mail** > **SSL/TLS** a aktivujte možnosť **Zapnúť filtrovanie protokolu SSL/TLS**.



Značenie e-mailov

Nastavenia pre túto funkcionalitu sú dostupné cez **Rozšírené nastavenia (F5) > Web a e-mail** > **Ochrana e-mailových klientov** > **Upozornenia a udalosti**.

Program umožňuje pridávať do skontrolovaných e-mailov oznámenie s informáciami o výsledku kontroly. Používateľ môže zvoliť, či chce **Pridávať poznámku do prijatých a prečítaných e-mailov** alebo tiež **Pridávať poznámku do odosielaných e-mailov**. Na tieto poznámky o výsledku kontroly sa nemožno úplne spoliehať, nakoľko nemusia byť doplnené do problematických HTML správ a taktiež môžu byť sfalšované malvérom. Pridávanie poznámok možno nastaviť zvlášť pre prijaté a prečítané e-maily a zvlášť pre odosielané e-maily, prípadne pre všetky e-maily. Na výber sú tieto možnosti:

- **Nikdy** – do správ nebudú pridávané žiadne poznámky s informáciou o výsledku kontroly.
- **Pri zachytení detekcie** – program bude pridávať poznámky len do infikovaných správ (predvolené nastavenie).
- **Do všetkých skontrolovaných e-mailov** – program bude pridávať poznámky do všetkých skontrolovaných e-mailov.

Upraviť predmet odosielaných e-mailov – umožňuje programu pridať do predmetu infikovaných e-mailov upozornenie na vírus. Táto funkcia sa dá využiť na jednoduché filtrovanie infikovaných správ podľa predmetu, pokiaľ to e-mailový klient umožňuje. Upozornenie tiež vzbudzuje dôveryhodnosť u adresáta správy a v prípade zachytenej infiltrácie poskytuje hodnotnú informáciu o bezpečnosti správy.

Text pridaný do predmetu e-mailu – túto šablónu upravte v prípade, ak si želáte zmeniť formát predpony predmetu infikovaného e-mailu. Táto funkcia nahradí predmet správy „Ahoj“ nasledujúcim formátom: „[detekcia %DETECTIONNAME%] Ahoj“. Premenná %DETECTIONNAME% predstavuje detekciu.

Integrácia s e-mailovými klientmi

V tomto okne je možné aktivovať integráciu s podporovanými e-mailovými klientmi, ktorými v súčasnej verzii sú: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. E-mailová ochrana funguje v rámci týchto klientov prostredníctvom pluginu. Hlavnou výhodou je nezávislosť od použitého protokolu. V prípade šifrovanej komunikácie program takto od e-mailového klienta dostáva na kontrolu už dešifrované správy. Kompletný zoznam podporovaných e-mailových klientov a ich verzií nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Špeciálne nastavenia

Optimalizovať spracovanie príloh – ak je optimalizácia vypnutá, všetky prílohy budú ihneď skontrolované. Týmto sa môže spomaliť výkon e-mailového klienta.

Pokročilé spracovanie e-mailovými klientmi – vypnite túto možnosť, ak ste zaznamenali spomalenie systému pri práci s e-mailovým klientom.

Panel nástrojov programu Microsoft Outlook

Ochrana programu Microsoft Outlook je vykonávaná prostredníctvom doplnku. Po inštalácii ESET Endpoint Security pribudne v programe Microsoft Outlook nový antivírusový/antispamový panel s funkciami pre ovládanie modulu:

Spam – vybrané správy označí ako spam. Po označení sa pošle „odtlačok“ správy na centrálny server s databázou charakteristík nevyžiadanej pošty. V prípade, že rovnaký „odtlačok“ pošle väčší počet ľudí, bude sa takáto správa v budúcnosti vyhodnocovať ako spam.

Nie spam – vybrané správy označí ako „nie spam“.

Spamová adresa (blacklist, zoznam spamových adries) – pridá adresu odosielateľa vybraných správ na blacklist. Správy z týchto adries budú automaticky označované ako spam.

> ⚠ Vyhýbajte sa spoofingu – pri odosielaní nevyžiadanej pošty sa využíva tzv. spoofing, keď sa skutočný odosielateľ maskuje za inú e-mailovú adresu.

Dôveryhodná adresa (whitelist, zoznam dôveryhodných adries) – pridá adresu odosielateľa na whitelist. Správy z týchto adries nebudú nikdy automaticky označované ako spam.

ESET Endpoint Security – kliknutím na ikonu sa otvorí program ESET Endpoint Security.

Opätovná kontrola správ – umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete určiť správy, ktoré majú byť skontrolované, a môžete tiež aktivovať opätovné prekontrolovanie už skontrolovaných správ. Viac informácií nájdete v kapitole Ochrana e-mailových klientov.

Nastavenie antivírusu – otvorí okno s nastaveniami Ochrany e-mailových klientov.

Nastavenia antispamu – otvorí okno s nastaveniami Antispamovej ochrany.

Zoznamy adries – otvorí okno antispamovej ochrany, ktoré vám umožní prístup k zoznamom vylúčených, dôveryhodných a spamových adries.

Panel nástrojov programu Outlook Express a Windows Mail

Ochrana programu Outlook Express alebo Windows Mail je vykonávaná prostredníctvom doplnku. Po inštalácii ESET Endpoint Security pribudne v programoch Outlook Express a Windows Mail nový antivírusový/antispamový panel s funkciami pre ovládanie modulu:

Spam – Vybrané správy označí ako spam. Po označení sa pošle „odtlačok“ správy na centrálny server s databázou charakteristík nevyžiadanej pošty. V prípade, že rovnaký „odtlačok“ pošle väčší počet ľudí, bude sa takáto správa v budúcnosti vyhodnocovať ako spam.

Nie spam – vybrané správy označí ako „nie spam“.

Spamová adresa – pridá adresu odosielateľa vybraných správ na blacklist. Správy z týchto adries budú automaticky označované ako spam.

Vyhýbajte sa spoofingu – pri odosielaní nevyžiadanej pošty sa využíva tzv. spoofing, keď sa skutočný odosielateľ maskuje za inú e-mailovú adresu.

Dôveryhodná adresa – pridá adresu odosielateľa vybraných správ na whitelist. Správy z týchto adries nebudú nikdy automaticky označované ako spam.

ESET Endpoint Security – kliknutím na ikonu sa otvorí program ESET Endpoint Security.

Opätovná kontrola správ – umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete určiť správy, ktoré majú byť skontrolované, a môžete tiež aktivovať opätovné prekontrolovanie už skontrolovaných správ. Viac informácií nájdete v kapitole Ochrana e-mailových klientov.

Nastavenie antivírusu – otvorí okno s nastaveniami Ochrany e-mailových klientov.

Nastavenia antispamu – otvorí okno s nastaveniami Antispamovej ochrany.

Používateľské rozhranie

Prispôsobiť vzhľad – umožňuje upraviť vzhľad panela nástrojov v e□mailovom kliente. Vzhľad panela je možné meniť nezávisle od nastavení e□mailového klienta.

Zobrazovať text – zobrazuje popis pod ikonami.

Text vpravo – popisy sú presunuté na pravú stranu vedľa ikony.

Veľké ikony – zobrazí veľké ikony pre položky menu.

Potvrdzovacie dialógové okno

Dialóg s možnosťou potvrdenia alebo zamietnutia zvolenej akcie slúži ako ubezpečenie sa, že používateľ chce danú akciu naozaj vykonať, čo slúži na obmedzenie možných omylov.

Dialóg ponúka aj možnosť vypnúť zobrazovanie potvrdzovacích správ úplne.

Opätovná kontrola správ

Integrovaný ovládací panel produktu ESET Endpoint Security v e-mailovom kliente umožňuje používateľom nastaviť rôzne druhy kontroly e-mailových správ. Prostredníctvom možnosti **Opätovná kontrola správ** je možné zvoliť dva režimy kontroly:

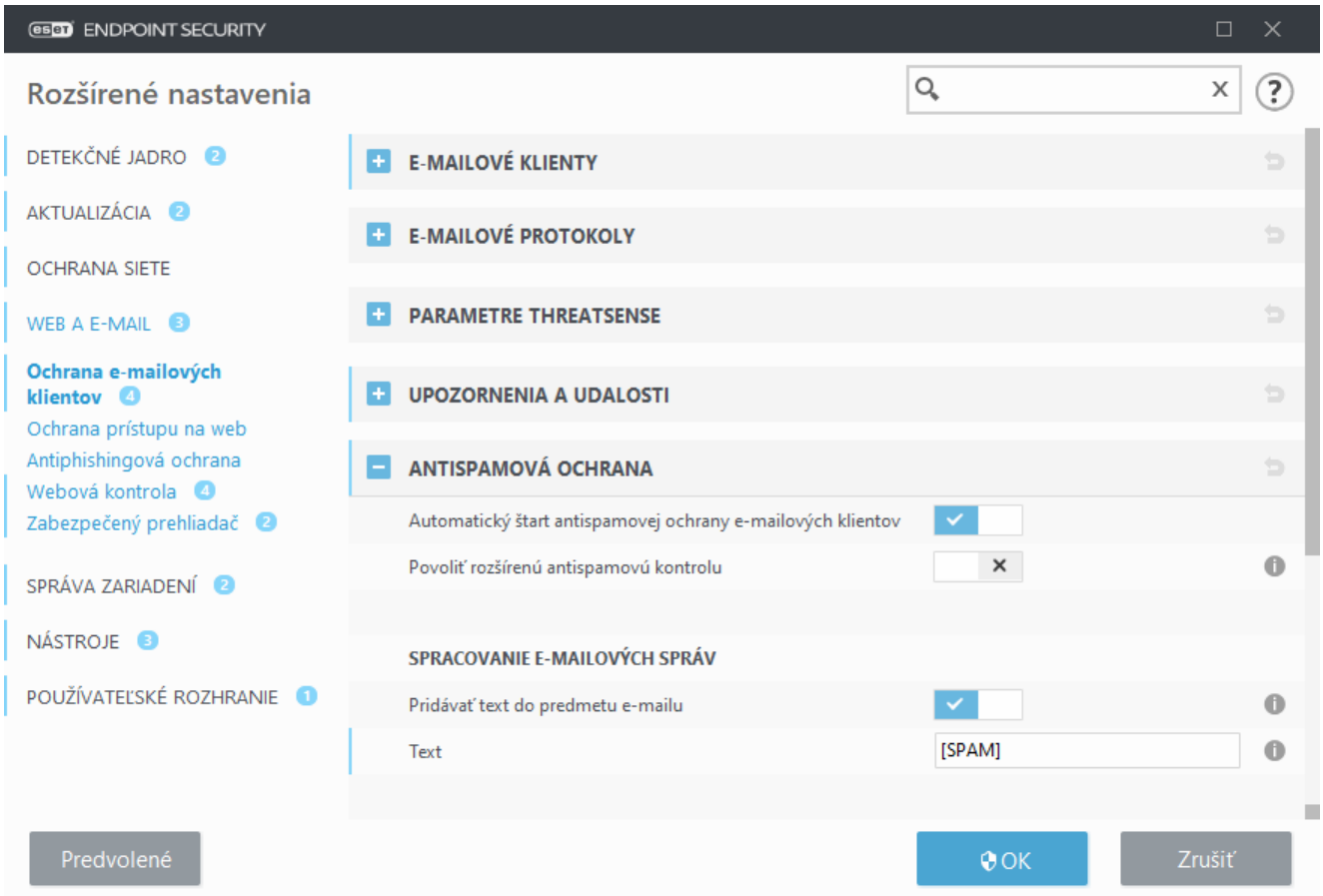
Všetky správy v aktuálnom priečinku – budú kontrolované všetky správy v priečinku, ktorý je aktuálne zobrazený.

Iba vybrané správy – kontrole budú podliehať len správy, ktoré používateľ priamo označil.

Položka **Kontrolovať aj správy, ktoré už boli prekontrolované** zabezpečí, aby sa do kontroly zahrnuli aj správy, ktoré už boli v minulosti prekontrolované.

Antispamová ochrana

V súčasnosti sa medzi najväčšie problémy e-mailovej komunikácie radí nevyžiadaná pošta – spam. Spam tvorí až 50 % všetkej e-mailovej komunikácie. Antispamová ochrana slúži na ochranu pred týmto problémom. Zahŕňa kombináciu viacerých účinných princípov zabezpečujúcich dokonalé filtrovanie nevyžiadanej pošty.



Základnou metódou rozpoznávania nevyžiadanej pošty je schopnosť jej rozpoznania na základe vopred definovaných dôveryhodných (whitelist) a spamových adries (blacklist). Do whitelistu sú automaticky zaradené všetky adresy z vášho zoznamu kontaktov a adresy, ktoré označíte ako bezpečné.

Hlavným princípom je rozpoznávanie spamu na základe vlastností emailových správ. Prijatá správa je preverená

podľa základných pravidiel (vzorky správ, štatistická heuristika, rozpoznávacie algoritmy a ďalšie unikátne metódy) a podľa výsledku sa určí, či ide o spam, alebo nie.

Automatický štart antispamovej ochrany e-mailových klientov – ak je táto možnosť povolená, antispamová ochrana sa bude automaticky spúšťať pri štarte počítača.

Povoliť rozšírenú antispamovú kontrolu – zlepší schopnosti a výsledky antispamovej ochrany, keďže sa budú pravidelne sťahovať dodatočné antispamové dáta.

Antispamová ochrana produktu ESET Endpoint Security povoľuje nastaviť rôzne parametre pre prácu so zoznamami adries. Sú dostupné nasledujúce nastavenia:

Spracovanie e-mailových správ

Pridávať text do predmetu e-mailu – umožňuje pridať vlastný text do predmetu e-mailovej správy klasifikovanej ako spam. Prednastavený text je [SPAM].

Presúvať správy do spamového priečinka – ak je táto možnosť zapnutá, spamové správy budú presunuté do predvoleného priečinka pre nevyžiadanú poštu a správy preklasifikované ako „nie spam“ budú presunuté do priečinka prijatých správ. Keď na e-mailovú správu kliknete pravým tlačidlom myši a z kontextového menu označíte možnosť ESET Endpoint Security, zobrazia sa vám dostupné možnosti pre danú správu.

Použiť vlastný priečinok – priečinok, kam chcete presúvať infikované e□maily, ktoré program zachytí.

SPAM správy označovať ako prečítané – umožní automatické označovanie spamových správ ako prečítané. Pomôže vám to sústrediť sa na legitímne neprečítané správy.

Preklasifikované správy označovať ako neprečítané – správy pôvodne označené ako spam, no neskôr prehodnotené a označené ako legitímne, sa zobrazia ako neprečítané správy.

Zapisovať hodnotenie antispamovej ochrany do protokolu – antispamové jadro ESET Endpoint Security priraďuje každej skontrolovanej správe skóre. Správa bude zaznamenaná v antispamovom protokole (**ESET Endpoint Security** > **Nástroje** > **Protokoly** > **Antispamová ochrana**).

- **Žiadne** – hodnotenie antispamovej kontroly nebude do protokolu zaznamenané.
- **Preklasifikované a označené ako SPAM** – zvoľte túto možnosť, ak si želáte zapisovať do protokolu spamové hodnotenie pre správy označené ako SPAM.
- **Všetko** – všetky správy budú mať zaznamenané spamové hodnotenie.

Po kliknutí na správu v priečinku nevyžiadanej pošty môžete vybrať možnosť **Preklasifikovať vybrané správy ako NIE SPAM** a správa bude presunutá do priečinka prijatých správ. Po kliknutí na správu v priečinku prijatých správ môžete vybrať možnosť **Preklasifikovať označené správy ako SPAM** a správa bude presunutá do priečinka nevyžiadanej pošty. Môžete označiť viacero správ a vykonať akciu pre všetky správy naraz.

ESET Endpoint Security podporuje antispamovú ochranu pre Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail.

Zoznamy adries

Antispamová ochrana programu ESET Endpoint Security umožňuje nastaviť rôzne parametre pre prácu so zoznamami adries.

Zoznamy adries

Povoliť používateľské zoznamy adries – zapnite túto možnosť na aktiváciu adresára vytvoreného používateľom v rámci jeho vlastného e-mailového klienta.

Povoliť globálne zoznamy adries – táto možnosť povolí používanie globálneho zoznamu adries, ktorý je spoločný pre všetkých používateľov na danej pracovnej stanici. Globálny zoznam adries obsahuje informácie o všetkých používateľoch e-mailu, distribučných skupinách a zdrojoch.

Whitelist používateľa – zoznam kontaktov, v ktorom môžete pridať/odstrániť/upraviť e-mailové adresy, ktoré považujete za dôveryhodné a z ktorých chcete prijímať e-maily.

Používateľský blacklist – zoznam kontaktov, v ktorom môžete pridať/odobrať/upraviť e-mailové adresy, ktoré považujete za nedôveryhodné a z ktorých nechcete prijímať e-maily.

Používateľský zoznam výnimiek – zoznam e-mailových adries, ktoré sú podozrivé z odosielania nevyžiadaných správ (spamu) a ktoré majú byť vždy kontrolované na prítomnosť spamu. Viac informácií nájdete v kapitole Zoznam výnimiek.

Globálny whitelist/blacklist/zoznam výnimiek – tieto zoznamy sa používajú na uplatnenie antispamových politík pre všetkých používateľov programu ESET Endpoint Security na danej pracovnej stanici. Ak je ESET Endpoint Security spravovaný vzdialene, politika z nástroja ESET PROTECT/ECA sa aplikuje na všetky k nej priradené pracovné stanice.

Automatické pridávanie do whitelistu používateľa

Pridávať adresy z adresára – existujúce kontakty z adresára budú pridané do používateľského whitelistu.

Pridávať adresy príjemcov z odosielaných správ – do používateľského whitelistu budú pridané adresy príjemcov správ.

Pridávať adresy odosielateľov zo správ preklasifikovaných ako NIE SPAM – do používateľského whitelistu budú pridané adresy odosielateľov správ, ktoré boli preklasifikované ako NIE SPAM.

Automatické pridávanie do používateľského zoznamu výnimiek

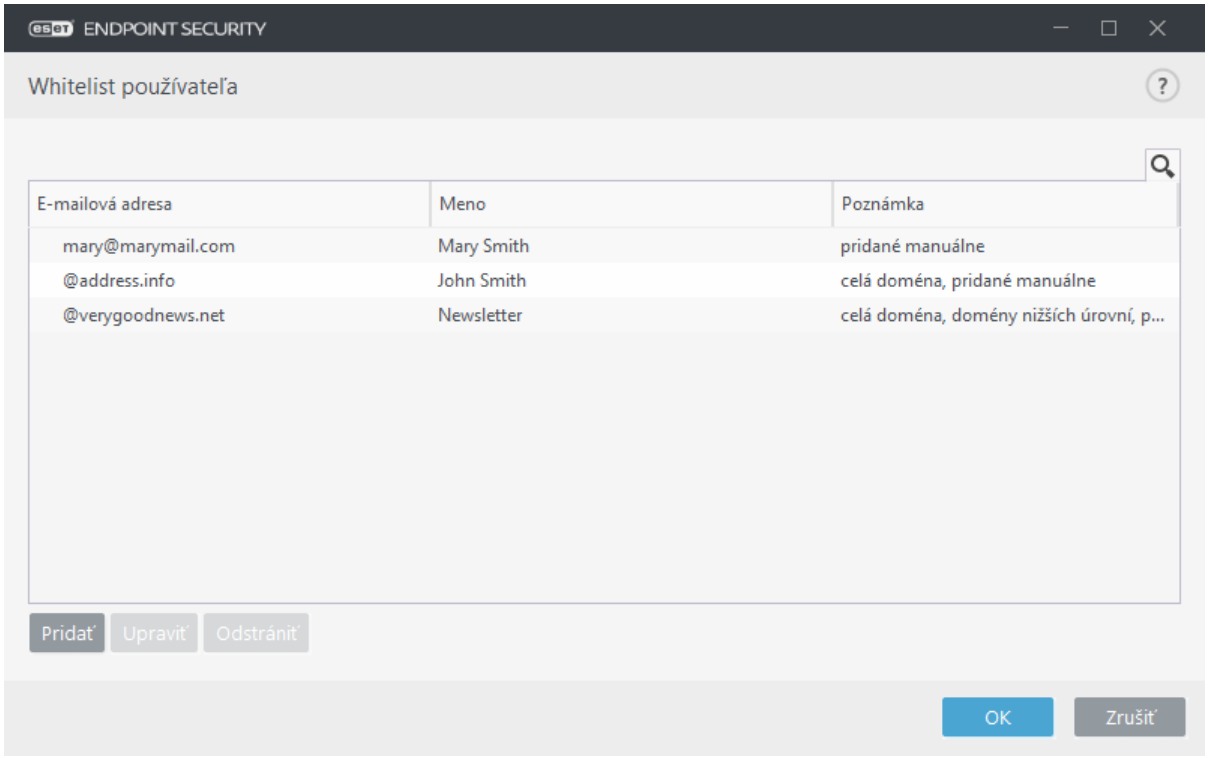
Pridávať adresy z vlastných účtov – do zoznamu výnimiek budú pridané e-mailové adresy z existujúcich účtov e-mailového klienta.

Blacklist, whitelist a zoznam výnimiek

Na zabezpečenie ochrany pred nevyžiadanými e□mailmi vám ESET Endpoint Security umožňuje triediť e□mailové adresy do špecializovaných zoznamov. Whitelist obsahuje e-mailové adresy, ktoré sú bezpečné. Správy prijaté z týchto adries budú vždy v priečinku prijatej pošty. Blacklist obsahuje e-mailové adresy, ktoré sú nebezpečné/rozširujú nevyžiadanú poštu. Všetky správy prijaté z týchto adries budú označené ako Spam a presunuté do príslušného priečinka. Zoznam výnimiek obsahuje e□mailové adresy, ktoré sa vždy kontrolujú na prítomnosť spamu, ale môže tiež obsahovať adresy z nevyžiadaných e□mailových správ, ktoré nemusia byť zo začiatku rozpoznané ako spam.

Všetky zoznamy sú prístupné z hlavného okna programu ESET Endpoint Security cez **Rozšírené nastavenia** > **Web**

a e-mail > **Ochrana e-mailových klientov** > **Zoznamy adries**. Pomocou tlačidiel **Pridať**, **Upraviť** a **Odstrániť** môžete upravovať každý zo zoznamov. Zoznamy sú prístupné aj z hlavného okna programu v sekcii **Nastavenia** > **Web a e-mail** po kliknutí na ikonu ozubeného kolesa vedľa položky **Antispamová ochrana**.



Štandardne ESET Endpoint Security pridá všetky vaše kontakty z e-mailového klienta do zoznamu dôveryhodných adries (whitelist). Zoznam blokovaných adries (blacklist) je predvolene prázdny. Sekcia Zoznam výnimiek obsahuje len e-mailové adresy používateľa.

Pridanie a úprava položiek v blackliste, whiteliste a zozname výnimiek

V tomto okne môžete pridať alebo upraviť položky vo whiteliste alebo blackliste. Otvorte hlavné okno programu ESET Endpoint Security > **Rozšírené nastavenia** > **Web a e-mail** > **Ochrana e-mailových klientov** > **Zoznamy adries**.

E-mailová adresa – e-mailová adresa, ktorá má byť pridaná/upravená.

Meno – pomenovanie položky.

Celá doména – pri zvolení tejto možnosti sa bude položka uplatňovať na celú doménu (teda nielen pre adresu zadanú v poli E-mailová adresa, ale napríklad pre všetky adresy domény *adresa.sk*).

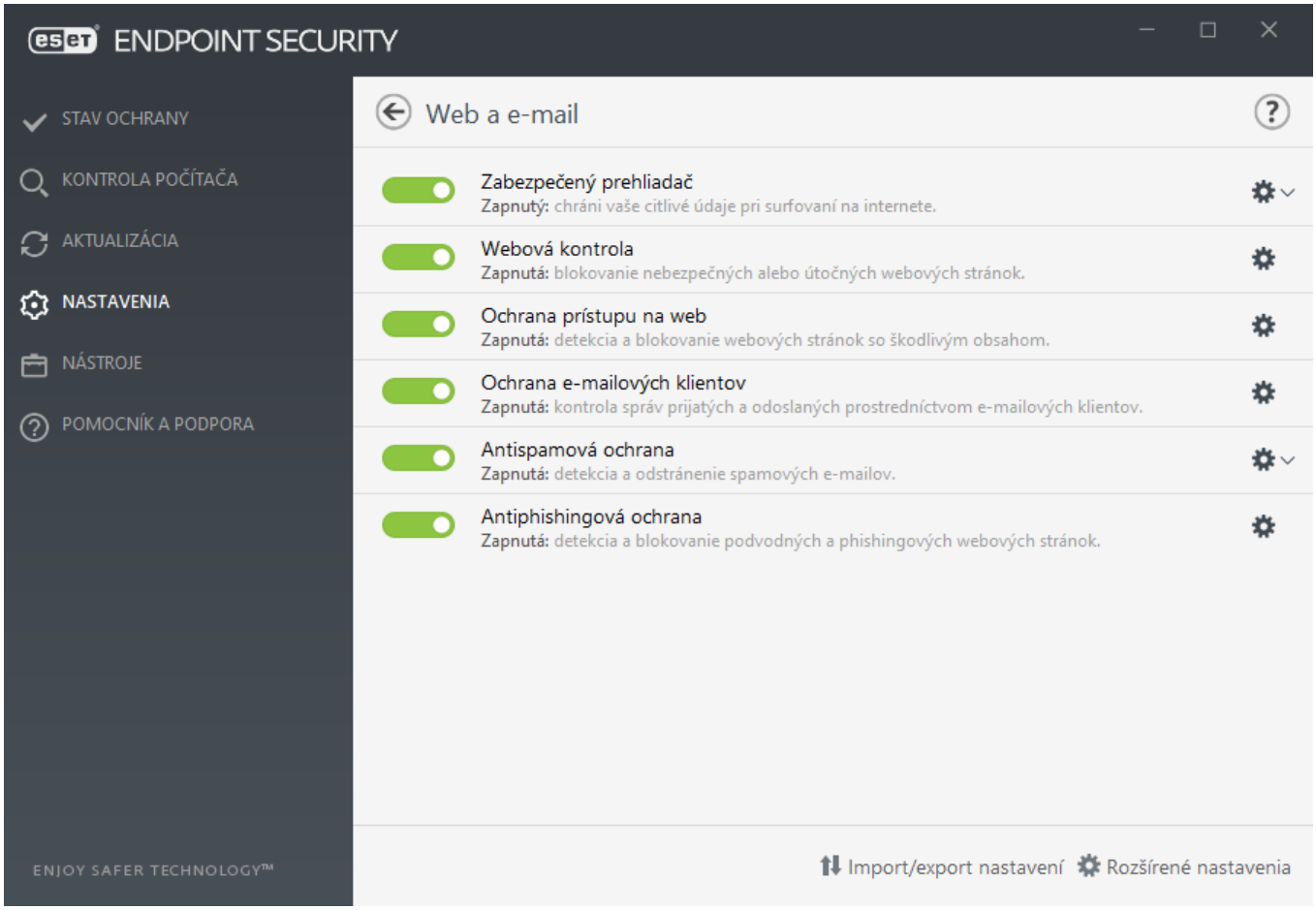
Domény nižších úrovní – ak sa e-mailová adresa skladá aj z domén nižších úrovní, je možné označením tejto voľby zaradiť takéto adresy do zoznamu (všetky subdomény domény, napr. *adresa.sk* je doména a *moja.adresa.sk* je subdoména).

Ochrana prístupu na web

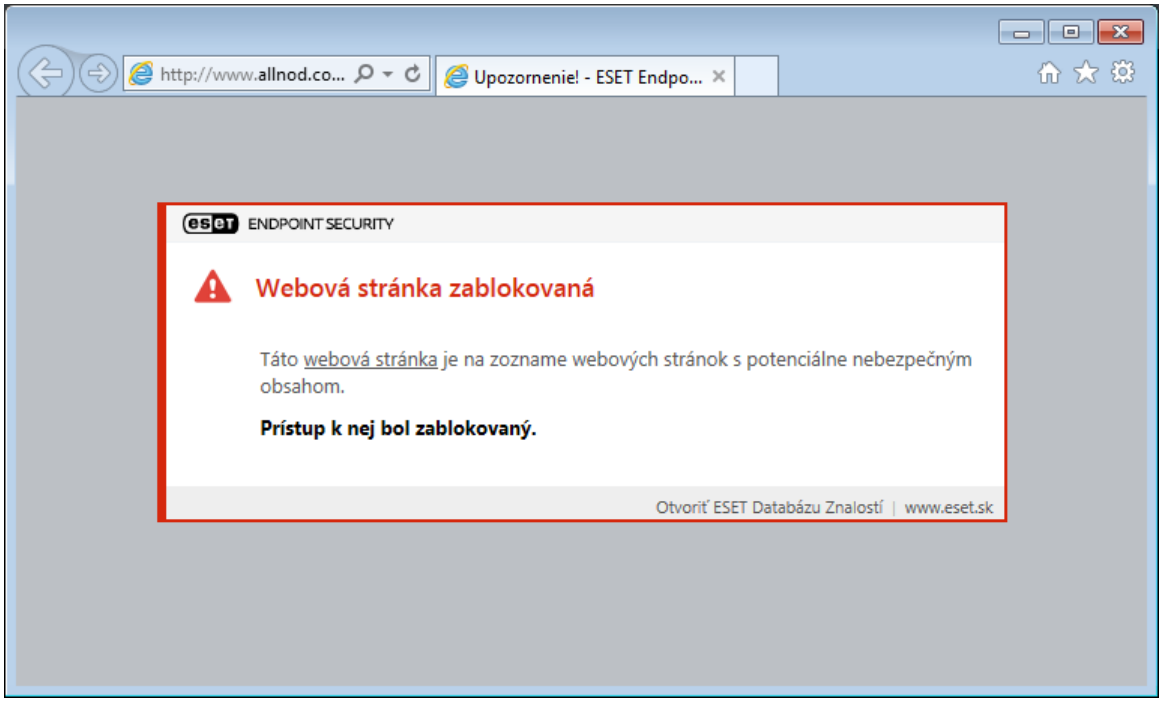
Internetové pripojenie patrí do štandardnej výbavy osobných počítačov. Zároveň sa stalo aj hlavným médiom prenosu škodlivého softvéru. Ochrana prístupu na web spočíva hlavne v monitorovaní komunikácie prehliadačov internetových stránok so servermi, ktorá prebieha podľa pravidiel protokolu HTTP a HTTPS.

Prístup na webové stránky, ktoré sú známe nebezpečným obsahom, je vždy blokovaný skôr, ako je obsah stiahnutý. Všetky ostatné webové stránky sú kontrolované technológiou ThreatSense pri ich načítaní, a ak obsahujú škodlivý obsah, sú zablokované. Ochrana prístupu na web obsahuje dve ochranné vrstvy, blokovanie podľa blacklistu a blokovanie podľa obsahu.

Odporúčame zapnúť Ochranu prístupu na web na zabezpečenie ochrany pred internetovými hrozbami. Nastavenia webovej ochrany sú prístupné z hlavného okna ESET Endpoint Security v sekcii **Nastavenia** > **Ochrana internetu** > **Ochrana prístupu na web**.



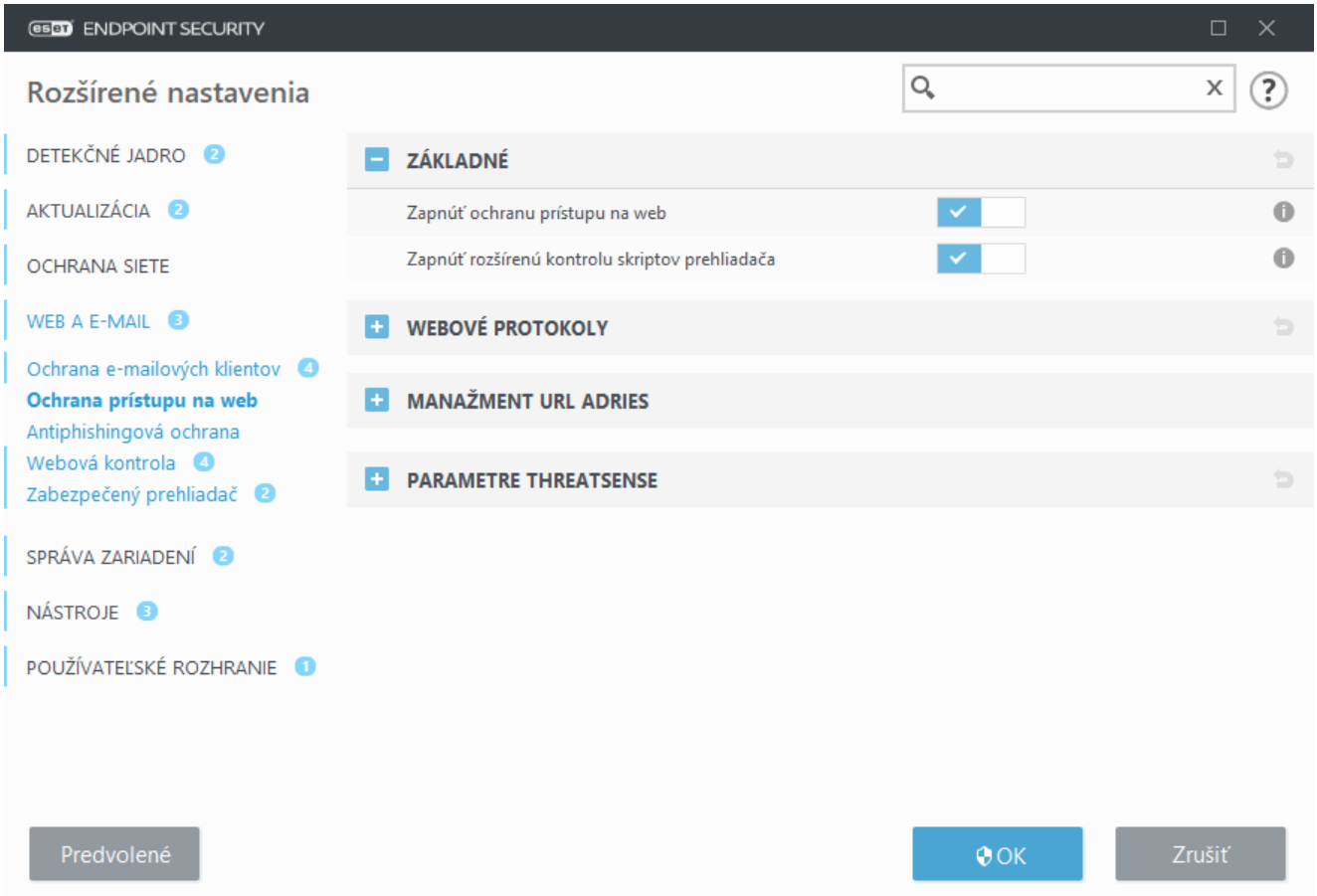
Ak dôjde k zablokovaniu webovej stránky, Ochrana prístupu na web zobrazí vo vašom prehliadači nasledujúcu správu:



Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
• Ako v programe ESET Endpoint Security **odblokovať bezpečnú webovú stránku na konkrétnej pracovnej stanici**

V sekcii **Rozšírené nastavenia** (F5) > **Web a e-mail** > **Ochrana prístupu na web** sú k dispozícii nasledujúce možnosti:

- **Základné** – umožňuje zapnúť alebo vypnúť túto funkciu v Rozšírených nastaveniach.
- **Webové protokoly** – umožňuje nastaviť kontrolu pre štandardné protokoly, ktoré využíva väčšina internetových prehliadačov.
- **Manažment URL adries** – umožňuje definovať zoznamy URL adries, ktoré budú blokované, povolené alebo vylúčené z kontroly.
- **Parametre ThreatSense** – pokročilé možnosti nastavenia kontroly, ako napr. typy objektov, ktoré si želáte kontrolovať (e-maily, archívy atď.), metódy detekcie pre Ochranu prístupu na web a pod.



Rozšírené nastavenia ochrany prístupu na web

V sekcii **Rozšírené nastavenia** (F5) > **Web a e-mail** > **Ochrana prístupu na web** > **Základné** sú k dispozícii nasledujúce možnosti:

Zapnúť ochranu prístupu na web – ak je táto možnosť vypnutá, ochrana prístupu na web a antiphishingová ochrana nebudú fungovať.

Zapnúť rozšírenú kontrolu skriptov prehliadača – ak je táto možnosť zapnutá, detekčné jadro bude kontrolovať všetky programy využívajúce JavaScript, ktoré sú spúšťané webovými prehliadačmi.

Dôrazne odporúčame ponechať Ochranu prístupu na web zapnutú.

Webové protokoly

Štandardne je ESET Endpoint Security nakonfigurovaný na monitorovanie protokolov HTTP používaných vo väčšine internetových prehliadačov.

Nastavenie kontroly HTTP

Komunikácia cez protokol HTTP sa vždy kontroluje na všetkých portoch a pre všetky aplikácie.

Nastavenie kontroly HTTPS

ESET Endpoint Security podporuje aj kontrolu komunikácie cez protokol HTTPS. Pri tejto komunikácii sú prenášané údaje medzi serverom a klientom zašifrované. ESET Endpoint Security kontroluje aj komunikáciu využívajúcu protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovať len komunikáciu na portoch definovaných v časti **Porty používané protokolom HTTPS** (443, 0-65535), pričom nezáleží na verzii operačného systému.

Šifrovaná komunikácia je predvolene kontrolovaná. Na zobrazenie nastavení kontroly prejdite do časti SSL/TLS v Rozšírených nastaveniach. Kliknite na **Web a e□mail** > **SSL/TLS** a aktivujte možnosť **Zapnúť filtrovanie protokolu SSL/TLS**.

Manažment URL adries

Manažment URL adries vo svojich nastaveniach umožňuje definovať zoznamy HTTP adries webových stránok, ktoré budú blokované, povolené alebo vylúčené z kontroly.

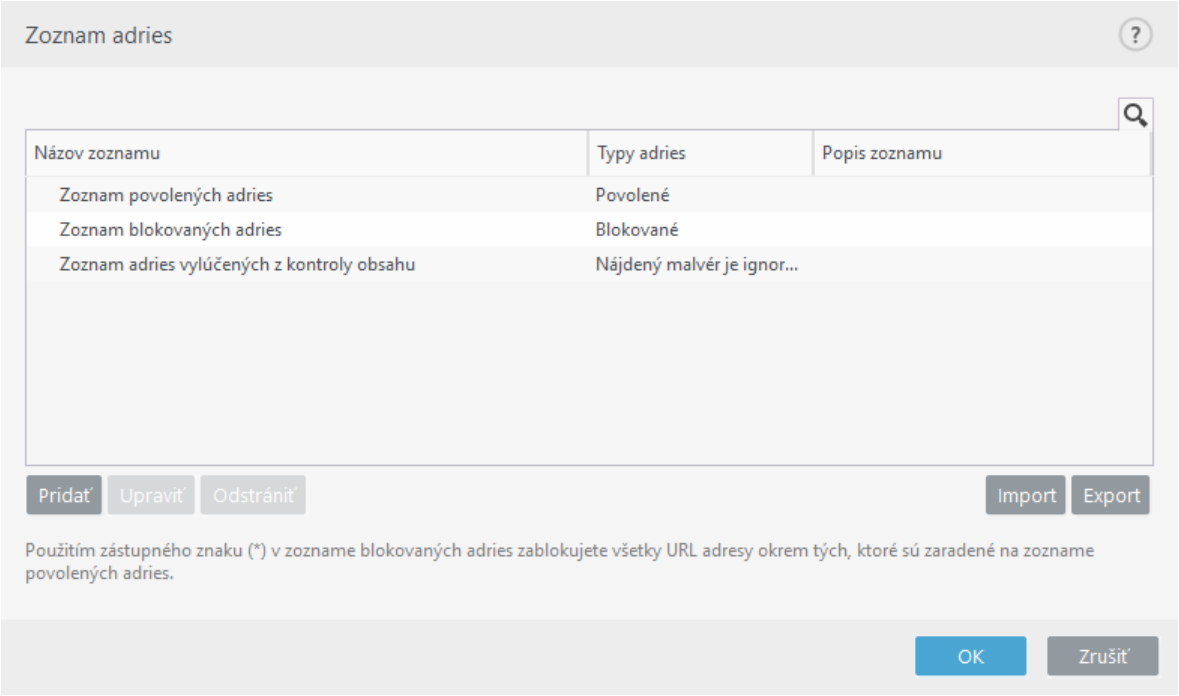
Možnosť **Zapnúť filtrovanie protokolu SSL/TLS** musí byť aktivovaná, ak chcete okrem HTTP adries filtrovať aj adresy HTTPS. V opačnom prípade budú pridané len domény HTTPS stránok, ktoré ste navštívili, a celé URL adresy nebudú pridané.

Webové stránky na **zozname blokovaných adries** nebudú prístupné, na rozdiel od stránok na **zozname povolených adries**. Webové stránky na **zozname adries vylúčených z kontroly obsahu** nebudú pri prístupe kontrolované na prítomnosť škodlivého kódu.

Ak chcete zablokovať všetky HTTP adresy okrem adries zaradených na **Zozname povolených adries**, pridajte znak hviezdičky (*) do **Zoznamu blokovaných adries**.

Je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Hviezdička nahrádza ľubovoľný reťazec znakov a otáznik nahrádza ľubovoľný znak. Odporúčame zvýšenú opatrnosť pri zadávaní vylúčených URL adries. Rovnako je potrebné dbať na opatrnosť pri používaní špeciálnych znakov (* a ?) v tomto zozname. Viac informácií o tom, ako bezpečne pomocou masky zadefinovať celú doménu vrátane všetkých subdomén, nájdete v kapitole Pridanie HTTP adresy/masky domény. Pre aktivovanie zoznamu kliknite na možnosť **Zoznam je aktívny**. Ak chcete byť upozornený na zadanie adresy zo zoznamu, zvoľte možnosť **Upozorniť pri použití adresy zo zoznamu**.

Adresy nebudú filtrované v prípade, že možnosť **Web a e-mail** > **SSL/TLS** > **Vylúčiť komunikáciu s dôveryhodnými doménami** je zapnutá a doména je považovaná za dôveryhodnú.



Ovládacie prvky

Pridať – pridanie nového zoznamu k vopred zadefinovaným. Toto môže byť užitočné, ak chcete logicky rozdeliť niekoľko skupín adries. Napríklad, jeden zoznam blokovaných adries môže obsahovať adresy z externého verejného blacklistu a ďalší zoznam môže obsahovať váš vlastný blacklist, čo umožňuje aktualizáciu externých zoznamov, pričom nenaruší váš používateľský zoznam.

Upraviť – zmena existujúceho zoznamu. Použite túto možnosť na pridanie alebo odstránenie adresy zo zoznamu.

Odstrániť – odstránenie existujúceho zoznamu. Dostupné len pre zoznamy pridané cez tlačidlo **Pridať**, nie pre predvolené zoznamy.

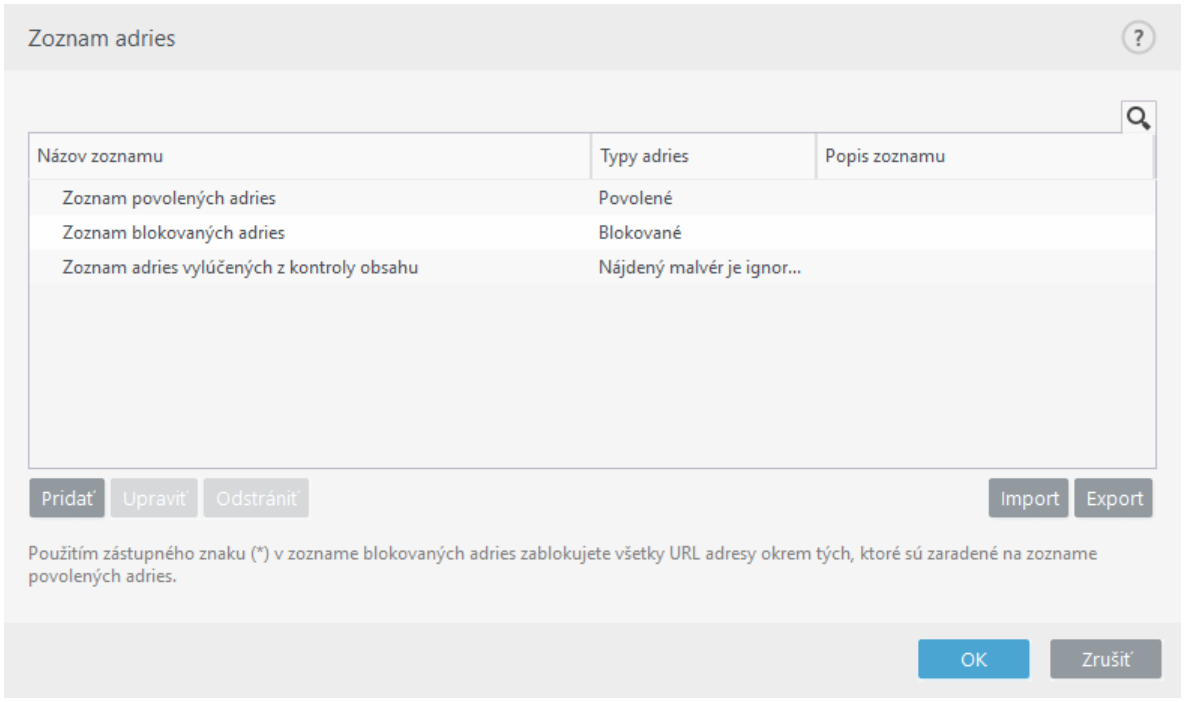
Zoznam URL adries

V tejto sekcii môžete definovať zoznamy HTTP adries, ktoré budú blokované, povolené alebo vylúčené z kontroly.

Na základe predvolených nastavení sú k dispozícii tri zoznamy:

- **Zoznam adries vylúčených z kontroly obsahu** – adresy v tomto zozname nebudú kontrolované na prítomnosť škodlivého kódu.
- **Zoznam povolených adries** – pokiaľ je aktívna voľba Povoliť prístup iba na HTTP adresy zaradené do zoznamov povolených adries a zoznam blokovaných adries obsahuje zástupný znak * (takže všetko), používateľovi bude umožnený prístup iba na adresy v tomto zozname. Adresy v tomto zozname budú povolené aj v tom prípade, ak sa nachádzajú aj v zozname blokovaných adries.
- **Zoznam blokovaných adries** – na adresy v tomto zozname nebude používateľovi povolený prístup, ak sa zároveň nenachádzajú aj v zozname povolených adries.

Kliknite na **Pridať** pre vytvorenie nového zoznamu. Pre zmazanie zoznamu kliknite na **Odstrániť**.



Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
• Ako v programe ESET Endpoint Security **odblokovať bezpečnú webovú stránku na konkrétnej pracovnej stanici**

Viac informácií nájdete v kapitole Manažment URL adries.

Vytvorenie nového zoznamu

Toto dialógové okno vám umožňuje nastaviť nový zoznam URL adries/masiek, ktoré budú blokované, povolené alebo vylúčené z kontroly.

Je možné nastaviť:

Typ zoznamu adries – k dispozícii sú tri typy zoznamov:

- **Nájdený malvér je ignorovaný** – adresy v tomto zozname nebudú kontrolované na prítomnosť škodlivého kódu.
- **Zoznam blokovaných adries** – na adresy v tomto zozname nebude povolený prístup.
- **Zoznam povolených adries** – na adresy v tomto zozname bude povolený prístup. Adresy v tomto zozname budú povolené aj v tom prípade, ak sa nachádzajú aj v zozname blokovaných adries.

Názov zoznamu – zadajte názov nového zoznamu. Toto pole nebude dostupné v prípade zmeny nastavení niektorého z preddefinovaných zoznamov.

Popis zoznamu – zadajte krátky popis zoznamu (nepovinné). Toto pole nebude dostupné v prípade zmeny nastavení niektorého z preddefinovaných zoznamov.

Pre aktivovanie zoznamu kliknite na možnosť **Zoznam je aktívny**. Pri aplikovaní adresy z konkrétneho zoznamu je možné nastaviť upozornenie o tejto udalosti prostredníctvom voľby **Upozorniť pri aplikovaní**. Napríklad pri prístupe na blokovanú alebo povolenú stránku zo zoznamu sa zobrazí oznámenie na ploche. Oznámenie bude obsahovať názov zoznamu.

Závažnosť zapisovania do protokolu – z roletového menu vyberte úroveň závažnosti zapisovania do protokolu. Záznamy, pre ktoré je úroveň závažnosti zapisovania do protokolu nastavená na Upozornenie, môžu byť zozbierané prostredníctvom konzoly ESET PROTECT.

Úroveň závažnosti zapisovania do protokolu nastavená na Informácie a Upozornenie je dostupná len pre pravidlá, ktoré obsahujú aspoň dve zložky bez zástupných znakov v rámci domény. Napríklad:
- *.domain.com/*
- *www.domain.com/*

Ovládacie prvky

Pridať – pridanie novej URL adresy do zoznamu (na pridanie viacerých adries použite oddeľovač).

Upraviť – úprava už existujúcej adresy v zozname. Táto možnosť je dostupná len pre adresy vytvorené pomocou tlačidla **Pridať**.

Odstrániť – odstránenie adries zo zoznamu. Táto možnosť je dostupná len pre adresy vytvorené pomocou tlačidla **Pridať**.

Importovať – import textového súboru s URL adresami (formát súboru *.txt – jedna adresa v riadku a kódovanie UTF-8).

Viac informácií nájdete v kapitole Ako pridať URL masku.

Ako pridať URL masku

Prosím, prečítajte si pred zadávaním masky adresy/domény inštrukcie uvedené v tomto okne.

ESET Endpoint Security umožňuje používateľovi blokovať prístup na konkrétne webové stránky a zabrániť tomu, aby prehliadač zobrazoval ich obsah. Tiež umožňuje používateľovi špecifikovať adresy, ktoré majú byť vylúčené z kontroly. V prípade, že nepoznáte celý názov vzdialeného servera alebo chcete špecifikovať celú skupinu vzdialených serverov, je možné použiť tzv. masky. V tomto prípade sú povolené špeciálne znaky ? a *, pričom:

- znak ? nahrádza ľubovoľný symbol,
- znak * nahrádza ľubovoľný reťazec textu.

Napríklad *.c?m bude platiť pre všetky adresy, kde posledná časť adresy začína znakom c, končí znakom m a v strede je ľubovoľný znak (.com, .cam a pod.).

Napríklad maska *x? predstavuje ľubovoľnú adresu, kde predposledným znakom je „x“. Ak chcete v maske zahrnúť celú doménu, použite formát **.domain.com/**. Určenie predpony protokolu (*http://*, *https://*) nie je povinné. Ak ju vynecháte, maska sa použije pre akýkoľvek protokol. Ak je sekvencia „*.“ použitá na začiatku názvu domény, je posudzovaná špecificky. Po prvé zástupný znak „*“ v tomto prípade nepokrýva lomku („/“). Zabráni sa tak obchádzaniu masky – napríklad pomocou masky **.domain.com* sa nebude vyhodnocovať adresa *http://anydomain.com/anypath#.domain.com* (takáto prípona môže byť pripojená k ľubovoľnej URL adrese bez toho, aby ovplyvnila sťahovanie). Po druhé sekvencia „*.“ v tomto špeciálnom prípade tiež pokrýva prázdny reťazec. To umožňuje použiť jednotnú masku pre celú doménu vrátane jej subdomén. Napríklad maskou **.domain.com* bude vyhodnotená aj adresa *http://domain.com*. Použitie masky **domain.com* by bolo nesprávne, pretože by to mohlo tiež zodpovedať adrese *http://anotherdomain.com*.

Úroveň závažnosti zapisovania do protokolu nastavená na Informácie a Upozornenie je dostupná len pre pravidlá, ktoré obsahujú aspoň dve zložky bez zástupných znakov v rámci domény. Napríklad:
- *.domain.com/*
- *www.domain.com/*

Antiphishingová ochrana

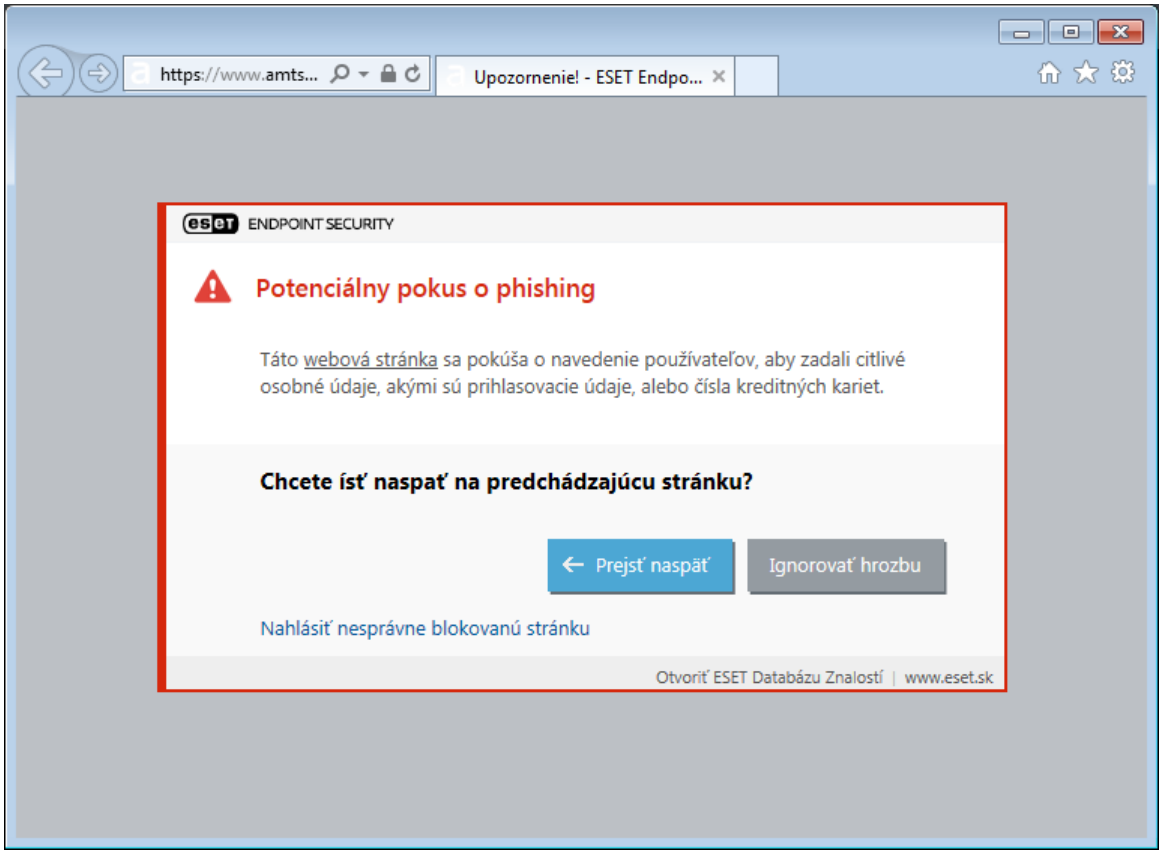
Termín phishing označuje kriminálnu aktivitu, ktorá používa techniky sociálneho inžinierstva (manipulovanie používateľov na získanie dôverných informácií). Jej cieľom je získať prístup k citlivým dátam, ako sú heslá k bankovým účtom, PIN kódy a iné detaily. Viac o tomto type aktivity sa môžete dočítať v slovníku pojmov. ESET Endpoint Security má zabudovanú ochranu pred phishingom, vďaka ktorej sú známe webové stránky s týmto typom obsahu blokované.

Antiphishingová ochrana je na základe predvolených nastavení zapnutá. Toto nastavenie je prístupné z hlavného okna programu cez **Rozšírené nastavenia** (F5) > **Web a e□mail** > **Antiphishingová ochrana**.

Viac informácií o Antiphishingovej ochrane v programe ESET Endpoint Security nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Prístup na phishingovú stránku

Ak navštívite phishingovú stránku, otvorí sa vám v prehliadači nasledujúce upozornenie. Ak aj napriek tomu chcete prejsť na stránku, kliknite na **Ignorovať hrozby** (neodporúča sa).



Povolenie potenciálnej phishingovej stránky horeuvedeným spôsobom vyprší v produkte po niekoľkých hodinách. Ak chcete konkrétnu webovú stránku povoliť natrvalo, použite nástroj Manažment URL adries. V strome **Rozšírených nastavení** (F5) kliknite na **Web a e-mail** > **Ochrana prístupu na web** > **Manažment URL adries**, v časti **Zoznam adries** kliknite na **Upraviť** a pridajte požadovanú webovú stránku do zoznamu.

Nahlasovanie phishingových stránok

Na stránke Nahlásiť phishingovú web stránku môžete spoločnosti ESET na účely analýzy nahlásiť webové stránky s phishingovým alebo malvérovým obsahom.

Skôr ako pošlete stránku do spoločnosti ESET na analýzu, uistite sa, že spĺňa aspoň jedno z nasledujúcich kritérií:
• webová stránka ešte nie je v programe detegovaná,
• webová stránka sa nesprávne deteguje ako hrozba. V takom prípade kliknite na odkaz Nahlásiť nesprávne detegovanú phishingovú stránku.

Webovú stránku môžete odoslať na analýzu aj prostredníctvom e-mailu. V takom prípade ju pošlite na adresu samples@eset.com. Nezabudnite uviesť výstižný predmet správy a čo najviac informácií o webovej stránke (napr. URL adresa, z ktorej ste sa na túto stránku dostali, ako ste sa o nej dozvedeli a pod.).

Rozšírené nastavenia pre zabezpečený prehliadač

Nastavenia sú k dispozícii v sekcii **Rozšírené nastavenia** (F5) > **Web a e-mail** > **Zabezpečený prehliadač**.

Základné

Zapnúť zabezpečený prehliadač – povolením tejto možnosti aktivujete zoznam chránených webových stránok, ktorý si budete môcť otvoriť v samostatnom okne.

Presmerovanie webových stránok

Zapnúť presmerovanie chránených stránok – ak je táto možnosť povolená, stránky uvedené na zozname chránených webových stránok a internom zozname stránok internetového bankovníctva budú vždy automaticky presmerované do zabezpečeného prehliadača.

Chránené stránky – zoznam webových stránok, pre ktoré môžete zvoliť, či budú otvárané v zabezpečenom alebo bežnom prehliadači. Ako znamenie, že váš prehliadač je chránený, sa v ráme prehliadača zobrazí logo spoločnosti ESET.

Zabezpečenie platobných stránok a online bankovníctva – toto nastavenie je predvolene vypnuté. Po zapnutí budú okrem stránok v zozname Chránené stránky do zabezpečeného prehliadača presmerované aj stránky v internom zozname spoločnosti ESET. Webové stránky identifikované spoločnosťou ESET sa pravidelne aktualizujú.

Zabezpečený prehliadač

Rozšírená ochrana pamäte – ak je táto možnosť povolená, pamäť zabezpečeného prehliadača bude chránená pred prístupom iných procesov.

Ochrana klávesnice – ak je táto možnosť povolená, informácie zadané na klávesnici do zabezpečeného prehliadača budú skryté pred ostatnými aplikáciami. Týmto sa zvyšuje ochrana pred keyloggermi.

Zelené orámovanie prehliadača – ak je táto možnosť vypnutá, zelené orámovanie okna prehliadača a príslušné oznámenie v prehliadači sa zobrazia len na chvíľu pri spustení prehliadača a potom zmiznú. Zelené orámovanie značí, že váš prehliadač je plne chránený.

Nastaviť interaktívne upozornenia zabezpečeného prehliadača – po kliknutí na túto možnosť sa zobrazí dialógové okno Interaktívne upozornenia.

> V niektorých situáciách sa interaktívne upozornenie zobrazí len vtedy, keď nastane chyba pri spustení zabezpečeného prehliadača. Viac informácií nájdete v kapitole Interaktívne upozornenia.

Chránené stránky

ESET Endpoint Security obsahuje zoznam vopred zadefinovaných webových stránok, ktoré spúšťajú zabezpečený prehliadač. Webové stránky môžete pridávať do zoznamu a upravovať v nastaveniach programu.

Zoznam **Chránené stránky** si môžete zobraziť a upravovať v sekcii **Rozšírené nastavenia** (F5) > **Web a e-mail** > **Zabezpečený prehliadač** > **Základné** > **Chránené stránky** > **Upraviť**.

Okno pozostáva z nasledujúcich častí:

Stĺpce

Webová stránka – chránená webová stránka.

Zabezpečený prehliadač – ako znamenie, že váš prehliadač je chránený, sa v ráme prehliadača zobrazí logo spoločnosti ESET.

Obyčajný prehliadač – vyberte túto možnosť, ak chcete pre stránku používať predvolený webový prehliadač (napríklad pri internetovom bankovníctve).

Ovládacie prvky

Pridať – pridanie adresy webovej stránky.

Upraviť – úprava existujúcej položky.

Odstrániť – odstránenie zvolených položiek.

Oznámenie v prehliadači

Zabezpečený prehliadač vás informuje o aktuálnom stave prostredníctvom oznámení v prehliadači a farby orámovania okolo okna prehliadača.

Oznámenia v prehliadači sa zobrazujú na karte na pravej strane okna prehliadača.



Kliknutím na ikonu ESET rozbalíte aktuálne oznámenie v prehliadači. Ak chcete oznámenie minimalizovať, kliknite na text oznámenia. Oznámenie môžete zatvoriť kliknutím na ikonu .

Oznámenia v prehliadači

Typ oznámenia	Stav
Informatívne oznámenie a zelené orámovanie prehliadača	Zabezpečená je maximálna ochrana a oznámenie v prehliadači je predvolene minimalizované.
Upozornenie a oranžové orámovanie prehliadača	Zabezpečený prehliadač si vyžaduje vašu pozornosť z dôvodu problému, ktorý však nie je kritický. Pre viac informácií o probléme a jeho riešení postupujte podľa pokynov uvedených priamo v oznámení v prehliadači.
Bezpečnostné upozornenia a červené orámovanie prehliadača	Prehliadač nie je chránený Ochranou online platieb od spoločnosti ESET. Reštartujte prehliadač, aby sa ochrana aktivovala. V prípade konfliktu so súbormi načítanými v prehliadači kontaktujte technickú podporu spoločnosti ESET podľa inštrukcií v tomto článku Databázy znalostí.

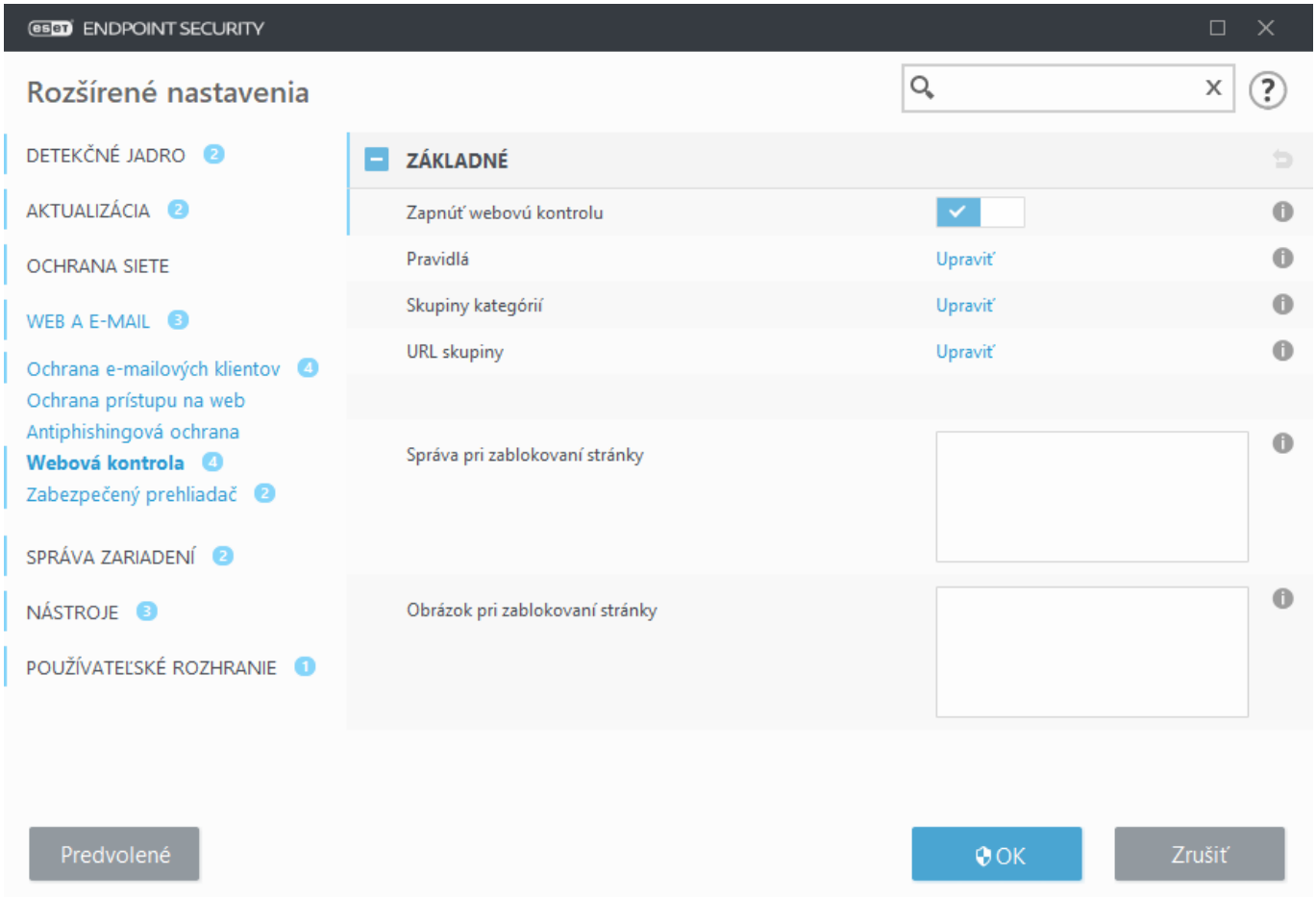
Webová kontrola

Webová kontrola vám umožňuje konfigurovať nastavenie, ktoré chráni firmu pred rizikom právnej zodpovednosti. Webová kontrola riadi prístup k webovým stránkam, ktoré môžu obsahovať potenciálne neprístojný obsah alebo môžu porušovať intelektuálne vlastníctvo iných osôb/spoločností. Jej cieľom je zamedziť zamestnancom prístup na tieto stránky, ako aj na stránky, ktoré môžu negatívne ovplyvniť ich produktivitu.

Webová kontrola vám umožňuje blokovať webové stránky, ktoré môžu obsahovať potenciálne nežiaduci obsah. Okrem toho môžu zamestnávatelia alebo systémoví administrátori zakázať prístup na 27 predvolených kategórií a 140 podkategórií webových stránok.

V predvolenom nastavení je modul Webovej kontroly vypnutý. Aktivovať ju môžete nasledovne:

1. Stlačte kláves **F5** pre zobrazenie okna **Rozšírených nastavení** a kliknite na **Web a e-mail** > **Webová kontrola**.
2. Zvoľte možnosť **Zapnúť webovú kontrolu**, čím aktivuje Webovú kontrolu v programe ESET Endpoint Security.
3. Pre nastavenie prístupu ku konkrétnym webovým stránkam kliknite na možnosť **Upraviť** vedľa popisu **Pravidlá**, čím otvoríte okno Editora pravidiel webovej kontroly.

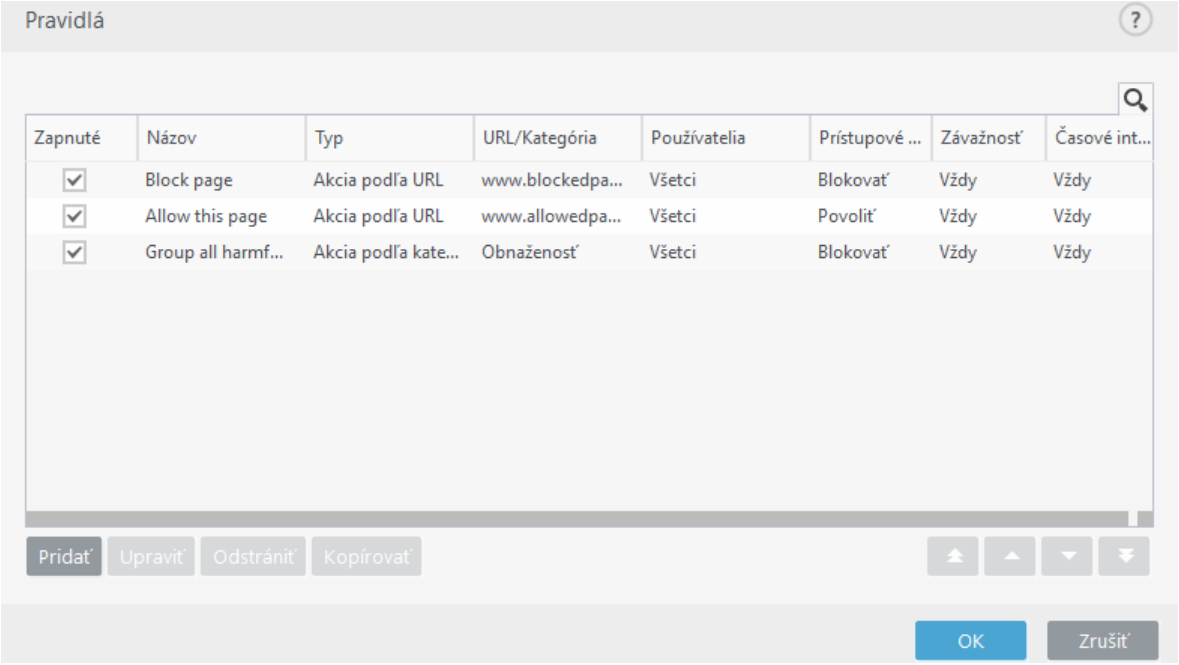


Polia **Správa pri zablokovaní stránky** a **Grafika pri zablokovaní stránky** vám umožňujú jednoducho si prispôsobiť správu, ktorá sa zobrazí v prípade, že dôjde k zablokovaniu webovej stránky.

> V prípade, že chcete blokovať všetky webové stránky a ponechať prístupné len konkrétne výnimky, použite Manažment URL adries.

Pravidlá webovej kontroly

Okno **Pravidlá** zobrazuje existujúce pravidlá pre URL adresy a webové kategórie.



Zoznam pravidiel pozostáva z niekoľkých parametrov, ako sú názov, typ blokovania, akcia vykonaná pri zhode s pravidlom Webovej kontroly a závažnosť zapisovania do protokolu.

Kliknutím na **Pridať** alebo **Upraviť** pridáte či upravíte pravidlo. Kliknutím na **Kopírovať** môžete vytvoriť nové pravidlo s predvolenými možnosťami použitými v inom zvolenom pravidle. Podržaním klávesu **CTRL** a kliknutím na pravidlá môžete hromadne označiť viacero položiek v zozname a následne takto označené pravidlá odstrániť. Možnosť **Zapnuté** aktivuje alebo deaktivuje konkrétne pravidlo, čo môže byť užitočné v prípade, ak si neželáte pravidlo odstrániť natrvalo, aby ste ho mohli v budúcnosti ešte použiť.

Pravidlá sú zoradené podľa priority, navrchu sa nachádzajú pravidlá s najvyššou prioritou. Ak chcete prioritu pravidla zmeniť, vyberte dané pravidlo a kliknite na šípku pre nastavenie vyššej alebo nižšej priority. Kliknutím na dvojitú šípku môžete pravidlo presunúť úplne na začiatok alebo koniec zoznamu.

Prečítajte si viac o vytváraní pravidiel.

Pridanie pravidiel webovej kontroly

Okno pravidiel webovej kontroly vám umožňuje manuálne vytvoriť alebo upraviť pravidlá webovej kontroly.

Názov

Do poľa **Názov** zadajte popis pravidla na jeho lepšiu identifikáciu.

Zapnuté

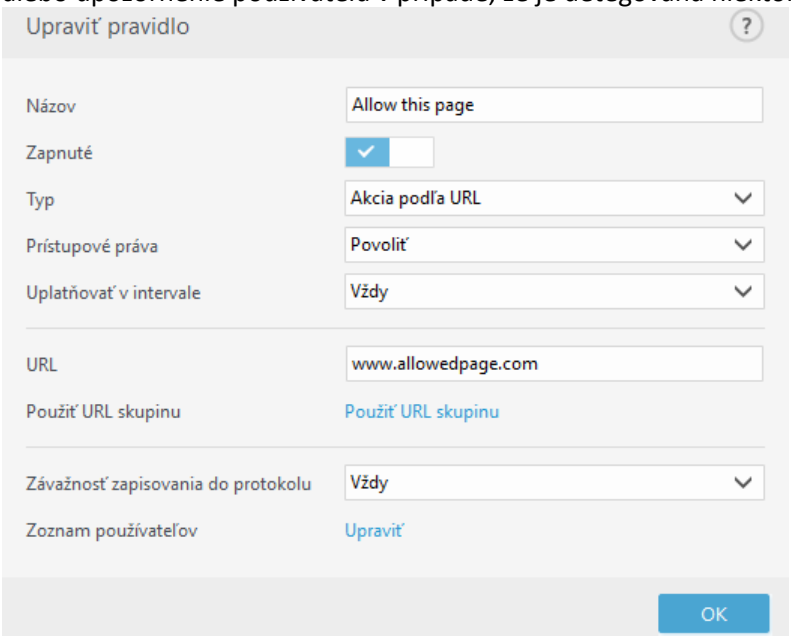
Kliknite na prepínač **Zapnuté** pre vypnutie alebo zapnutie pravidla. Toto môže byť užitočné v prípade, že si neželáte pravidlo odstrániť natrvalo.

Akcia

Vyberte si možnosť **Akcia podľa URL** alebo **Akcia podľa kategórie**:

Akcia podľa URL

Táto akcia je určená pre pravidlá, ktoré regulujú prístup na určitú webovú stránku – zadajte URL adresu do poľa **URL**.
Špeciálne znaky * (hviezdička) a? (otáznik) nie je možné použiť v zozname URL adries. Pri vytváraní URL skupiny, ktorá obsahuje webovú stránku s viacerými doménami najvyššej úrovne (top-level domain – TLD), musí byť každá doména pridaná samostatne. Keď pridáte doménu do skupiny, celý obsah nachádzajúci sa na danej doméne vrátane všetkých subdomén (napríklad *sub.examplepage.com*) bude blokovaný alebo povolený na základe vášho nastavenia akcie podľa URL.
URL alebo **Použiť URL skupinu** – použitie URL odkazu alebo skupiny URL odkazov na povolenie, blokovanie alebo upozornenie používateľa v prípade, že je detegovaná niektorá z daných URL adries.



Akcia podľa kategórie

Po zvolení tejto možnosti vyberte kategóriu webových stránok z roletového menu.
URL kategória alebo **Použiť skupinu** – použitie kategórie webových stránok alebo skupín kategórií na povolenie, blokovanie alebo upozornenie používateľa v prípade, že je detegovaná niektorá z daných skupín.

Prístupové práva

- **Povoliť** – prístup na URL adresu/kategóriu bude povolený.
- **Upozorniť** – pri prístupe na URL adresu/kategóriu bude používateľ upozornený.
- **Vždy upozorniť** – pri prístupe na URL adresu/kategóriu bude používateľ upozornený. Môže pokračovať na stránku, avšak správca bude upovedomený.
- **Blokovať** – prístup na URL adresu/kategóriu bude blokovaný.

Uplatňovať v intervale

Umožňuje vám aplikovať vytvorené pravidlo len počas určitého časového úseku. Z roletového menu stačí vybrať vytvorený časový interval.

- Viac informácií o časových intervaloch

Závažnosť zapisovania do protokolu

- **Vždy** – zaznamenáva do protokolu všetky online komunikácie.
- **Diagnostické** – zaznamenáva do protokolu informácie dôležité pre ladenie programu.
- **Informácie** – zaznamenáva informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky záznamy vyššie.
- **Upozornenie** – zaznamenáva kritické chyby a varovné správy.
- **Žiadne** – nebudú vytvárané žiadne protokoly.

Závažnosť zapisovania do protokolu môže byť nastavená osobitne pre každý zoznam. Protokoly, ktoré majú stav **Upozornenie**, môžu byť zozbierané prostredníctvom nástroja ESET PROTECT.

Zoznam používateľov

- **Pridať** – zobrazí okno **Zoznam používateľov**, kde je možné vybrať konkrétnych používateľov. Ak nie je zadaný žiadny používateľ, pravidlo je aplikované na všetkých používateľov.
- **Odstrániť** – vybraný používateľ bude odstránený z filtra.

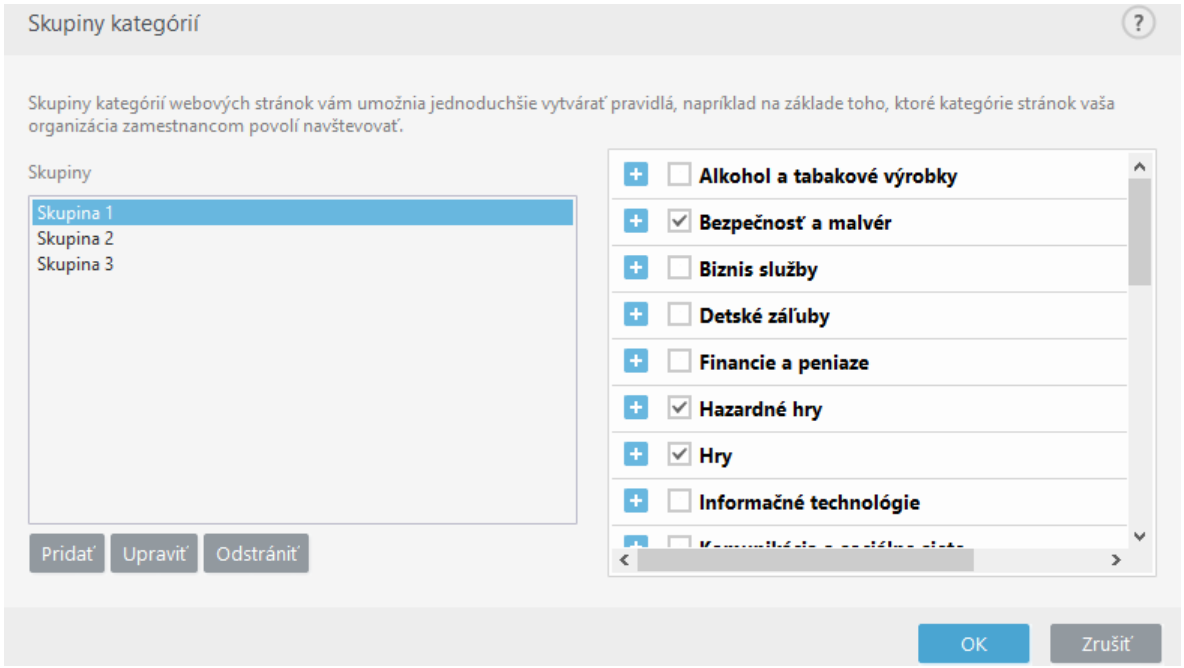
Skupiny kategórií

Okno Skupiny kategórií je rozdelené na dve časti. Ľavá časť okna obsahuje zoznam skupín kategórií.

- **Pridať** – vytvorenie novej skupiny kategórií.
- **Upraviť** – zmena existujúcej skupiny kategórií.
- **Odstrániť** – odstránenie označenej skupiny kategórií zo zoznamu.

Pravá časť okna obsahuje zoznam kategórií a podkategórií. V zozname vyberte kategóriu, ktorej podkategórie chcete zobraziť. Každá skupina obsahuje kategórie a podkategórie, ktoré zahŕňajú všeobecne prípustný obsah, ako aj obsah pre dospelých a/alebo všeobecne nevhodný obsah. Po otvorení okna Skupiny kategórií a kliknutí na prvú skupinu môžete pridávať alebo odoberať kategórie/podkategórie zo zoznamu skupín, napríklad Násilie alebo Zbrane. Vytvorením pravidla je možné webové stránky s nevhodným obsahom buď úplne blokovať, alebo sa používateľovi pri prístupe na stránku zobrazí upozornenie o nevhodnom obsahu stránky.

Použite začiarkavacie políčka na pridanie alebo odstránenie podkategórie z danej skupiny.



Nižšie nájdete niektoré príklady kategórií (skupín):

Rôzne – zvyčajne privátne (lokálne) IP adresy, ako napr. intranet, 192.168.0.0/16 a podobne. Ak sa zobrazí chybový kód 403 alebo 404, takáto webová stránka taktiež spadá do tejto kategórie.

Nevyriešené – táto kategória zahŕňa webové stránky, ktoré nebolo možné zaradiť kvôli chybe, ktorá nastala pri pokuse pripojiť sa na databázu webovej kontroly.

Nekategorizované – neznáme webové stránky, ktoré ešte neboli pridané do databázy webovej kontroly.

Proxy servery – webové stránky, ako napr. anonymizér, presmerovávač alebo verejné proxy, môžu byť použité na prístup k webovým stránkam, ktoré sú zakázané webovou kontrolou.

Zdieľanie súborov – tieto webové stránky obsahujú veľké množstvo dát, ako napr. fotky, videá alebo elektronické knihy. Existuje riziko, že tieto súbory majú nevhodný obsah.

Podkategória môže patriť pod akúkoľvek skupinu. Niektoré podkategórie nie sú zahrnuté vo vopred definovaných skupinách (napríklad Hry). Ak chcete zaistiť filtrovanie určitej podkategórie webových stránok, je potrebné pridať danú podkategóriu do konkrétnej skupiny.

URL skupiny

URL skupiny umožňujú vytváranie skupín, ktoré obsahujú niekoľko URL odkazov, pre ktoré môžete vytvoriť pravidlo (povoliť/zakázať konkrétnu webovú stránku).

Vytvorenie novej URL skupiny

Ak chcete vytvoriť novú URL skupinu, kliknite na **Pridať** a zadajte názov novej URL skupiny.

Použitie URL skupiny môže byť užitočné v prípade, ak chce správca vytvoriť pravidlo pre viacero webových stránok (blokovať alebo povoliť podľa vášho výberu).

Pridanie URL adries do zoznamu URL skupín – manuálne

Ak chcete pridať novú URL adresu do zoznamu, označte URL skupinu a kliknite na **Pridať** v pravom dolnom rohu okna.

Špeciálne znaky * (hviezdička) a? (otáznik) nie je možné použiť v zozname URL adries.

Nie je potrebné zadať úplný názov domény s http:// alebo https://.

Keď pridáte doménu do skupiny, celý obsah nachádzajúci sa na danej doméne vrátane všetkých subdomén (napríklad *sub.examplepage.com*) bude blokovaný alebo povolený na základe vášho nastavenia akcie podľa URL.

Ak existuje konflikt medzi dvoma pravidlami v zmysle, že prvé pravidlo blokuje doménu a druhé pravidlo povoľuje rovnakú doménu, daná doména alebo IP adresa bude zablokovaná. Podrobnejšie informácie o vytváraní pravidiel nájdete tu.

Pridanie URL adries do zoznamu URL skupín – import pomocou súboru .txt

Kliknite na **Import** pre importovanie súboru obsahujúceho zoznam URL adries (v každom riadku musí byť osobitná hodnota, môže ísť napríklad o .txt súbor s kódovaním UTF-8). Špeciálne znaky * (hviezdička) a? (otáznik) nie je možné použiť v zozname URL adries.

Používanie URL skupín vo Webovej kontrole

Ak chcete nastaviť akciu, ktorá má byť vykonaná pre konkrétnu URL skupinu, otvorte Editor pravidiel webovej kontroly, vyberte svoju URL skupinu pomocou roletového menu, upresnite ostatné parametre a kliknite na **OK**.

> Blokovanie alebo povolenie konkrétnych webových stránok môže byť podstatne presnejšie než blokovanie alebo povolenie celej kategórie. Pri zmene nastavení a pri pridávaní kategórie do zoznamu buďte opatrný.

Prispôsobenie správy zobrazenej pri blokovaní stránky

Polia **Správa pri zablokovaní stránky** a **Grafika pri zablokovaní stránky** vám umožňujú jednoducho si prispôsobiť správu, ktorá sa zobrazí v prípade, že dôjde k zablokovaniu webovej stránky.

Toto je predvolená správa a dizajn oznámenia zobrazeného v prehliadači v prípade, že sa používateľ pokúsi navštíviť blokovanú stránku:

Použitie

V tomto príklade si ukážeme, ako blokovať webové stránky z kategórie „Zbrane“.

Znenie správy zobrazenej pri pokuse o prístup k blokovanej webovej stránke môže byť napríklad nasledovné:

```
Webová stránka %URL_OR_CATEGORY% bola zablokovaná, pretože je považovaná za nevhodn
ú alebo sa na nej nachádza škodlivý obsah.
Pre bližšie informácie sa obráťte na správcu siete.
```

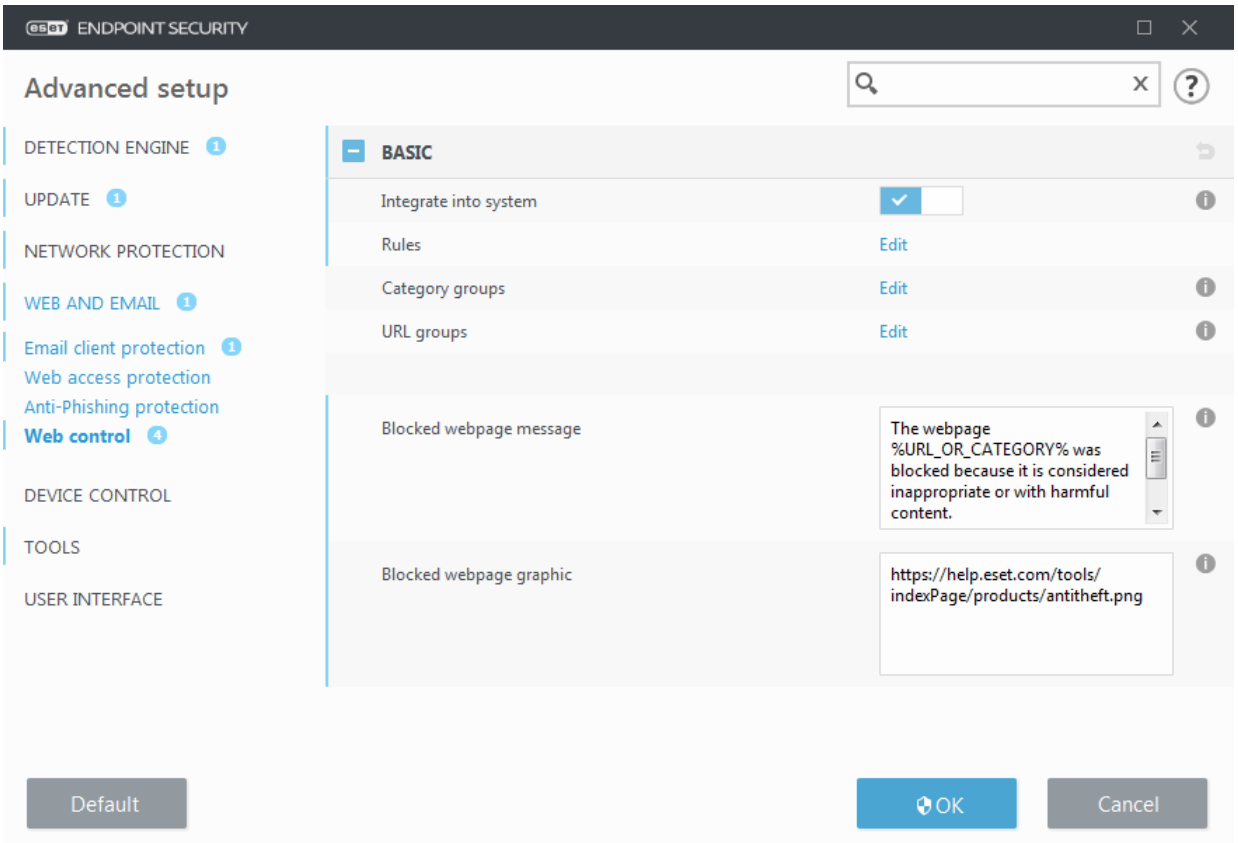
Premenná	Popis
%CATEGORY%	Blokovaná kategória v rámci Webovej kontroly.
%URL_OR_CATEGORY%	Blokovaná webová stránka alebo blokovaná kategória stránok (závisí od pravidla blokovania v rámci Webovej kontroly).
%STR_GOBACK%	Hodnota tlačidla „Prejsť naspäť“.
%product_name%	Názov produktu ESET (ESET Endpoint Security)
%product_version%	Verzia produktu ESET.

Príklad grafiky zobrazenej pri zablokovaní webovej stránky:

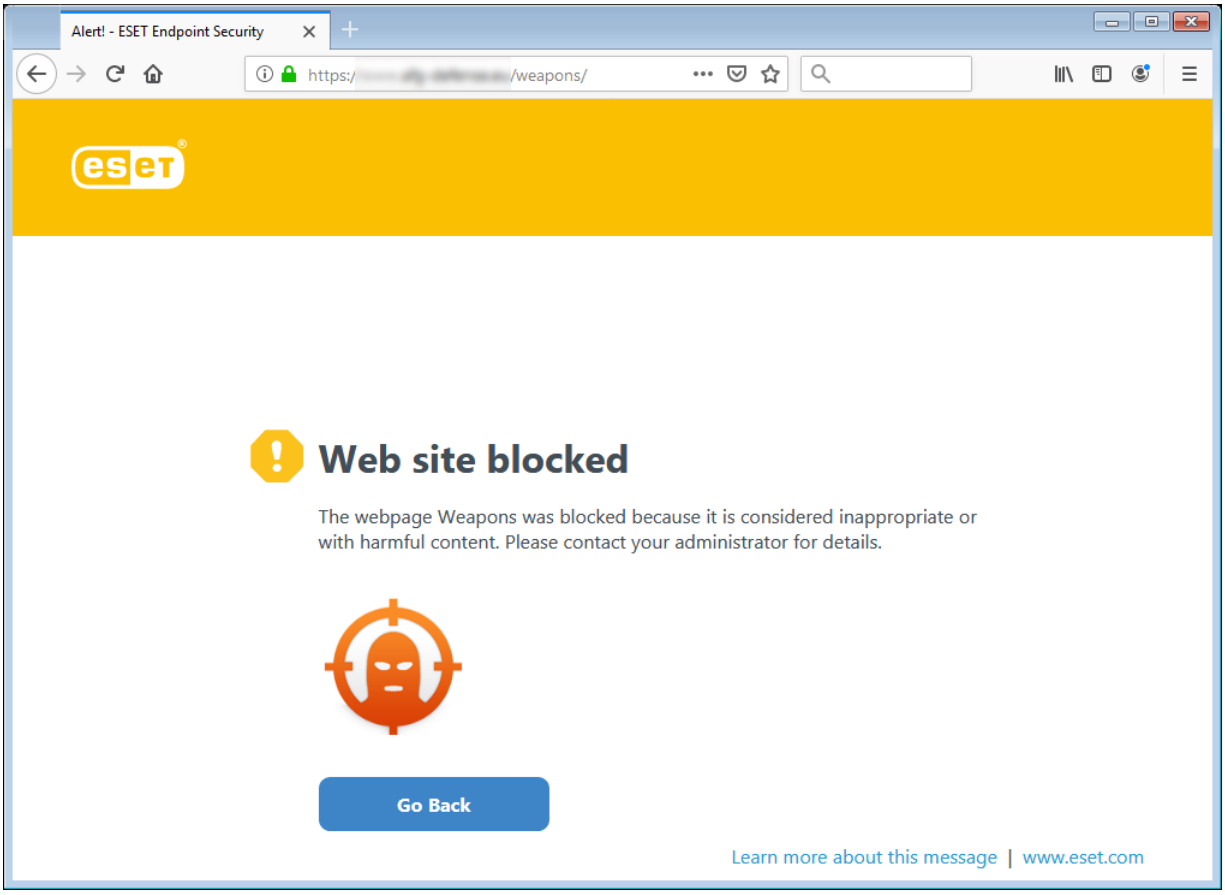
```
https://help.eset.com/tools/indexPage/products/antitheft.png
```

Ak je veľkosť obrázka (šírka/výška) priveľká, automaticky sa upraví.

Nastavenie v programe ESET Endpoint Security bude vyzerať nasledovne:



Správa, ktorá sa zobrazí v prehliadači, keď sa používateľ pokúsi o prístup k blokovanej webovej stránke, bude vyzerať nasledovne:



Aktualizácia programu

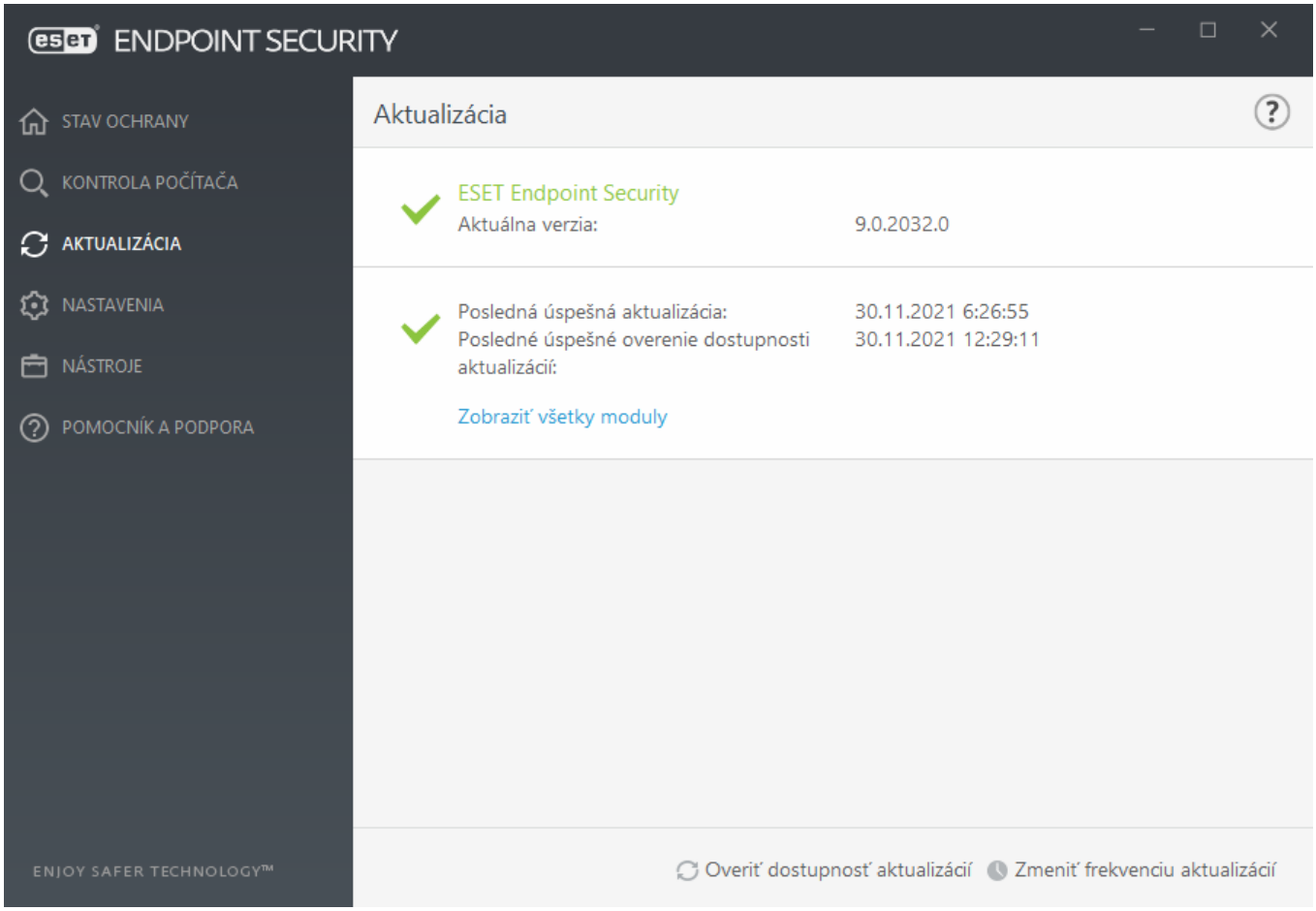
Pravidelná aktualizácia programu ESET Endpoint Security je základným predpokladom na zaistenie maximálnej úrovne ochrany vášho počítača. Modul aktualizácií zabezpečuje, aby bol program vždy aktuálny, čo zahŕňa aktualizáciu detekčného jadra a programových súčastí. Po aktivácii programu začnú aktualizácie prebiehať automaticky na základe predvoleného nastavenia.

V sekcii **Aktualizácia** v hlavnom okne programu je zobrazený aktuálny stav aktualizácie vrátane informácie o dátume a čase poslednej úspešnej aktualizácie, prípadne aj o dostupnosti novej aktualizácie. Po kliknutí na možnosť **Zobraziť všetky moduly** sa zobrazí zoznam nainštalovaných modulov programu, v ktorom tiež nájdete číslo verzie každého modulu a dátum jeho poslednej úspešnej aktualizácie.

Možnosť **Overiť dostupnosť aktualizácií** vám umožňuje manuálne spustiť proces aktualizácie. Aktualizovanie programových súčastí a detekčného jadra je z pohľadu zaistenia komplexnej ochrany pred škodlivým kódom nevyhnutnosťou. Nastaveniu a priebehu aktualizácií preto treba venovať zvýšenú pozornosť. Ak ste svoje licenčné údaje nezadali počas inštalácie, kliknite na možnosť **Aktivovať produkt** a zadajte svoj licenčný kľúč, aby ste zabezpečili prístup programu k aktualizačným serverom spoločnosti ESET.

Ak ste aktivovali ESET Endpoint Security pomocou offline registrácie bez prihlasovacieho mena a hesla, pri pokuse o aktualizáciu zo serverov ESET sa zobrazí chybové hlásenie **Aktualizácia modulov nebola úspešná**. V tomto prípade môžete aktualizácie sťahovať len z mirrora.

Licenčný kľúč ste od spoločnosti ESET dostali po zakúpení produktu ESET Endpoint Security.



Aktuálna verzia – číslo verzie vášho programu ESET Endpoint Security.

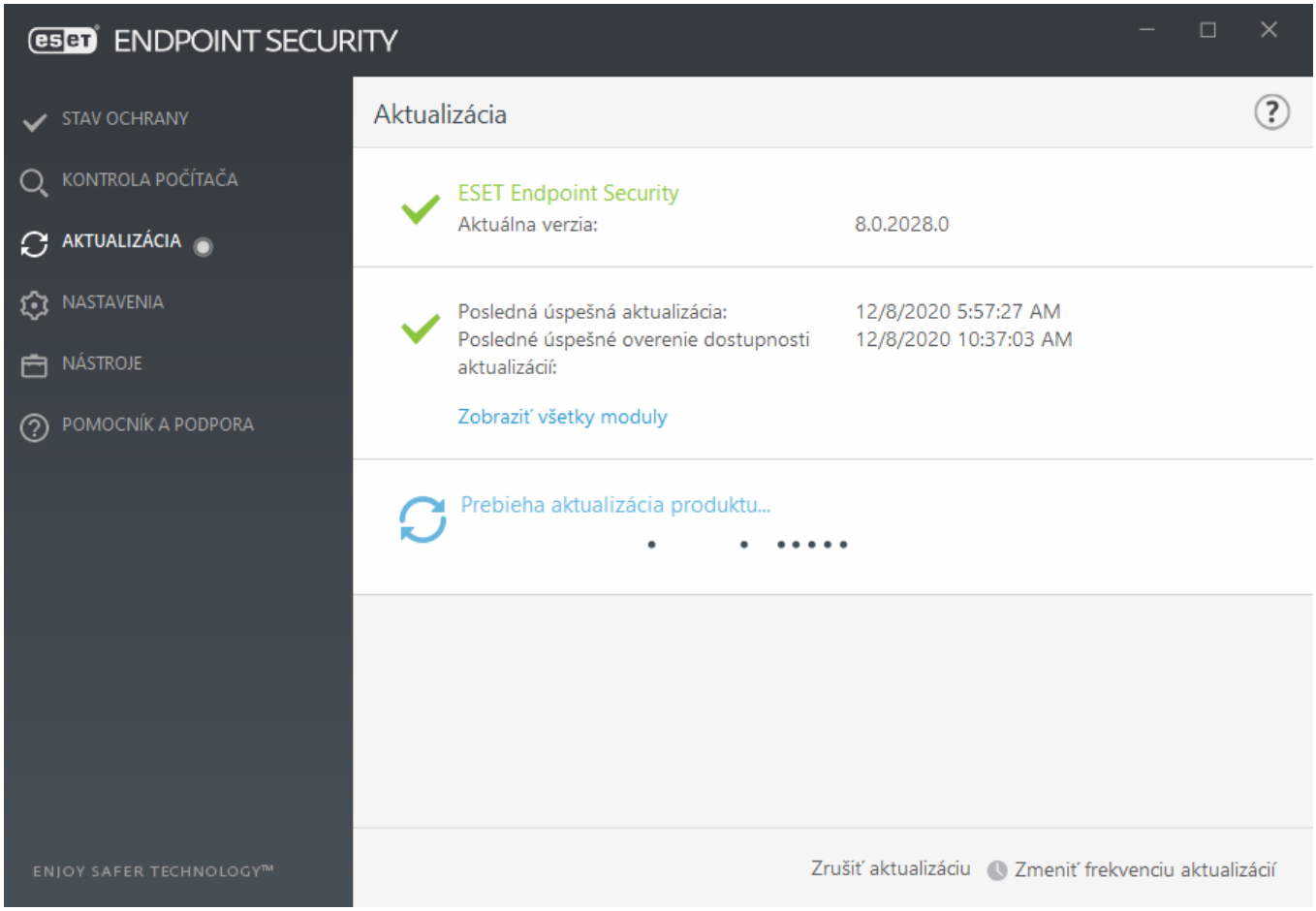
Posledná aktualizácia – dátum a čas poslednej úspešnej aktualizácie. Ak nie je zobrazený aktuálny dátum, detekčné jadro môže byť zastarané.

Posledné úspešné overenie dostupnosti aktualizácií – dátum a čas posledného úspešného pokusu o aktualizáciu modulov.

Zobraziť všetky moduly – zobrazí sa zoznam nainštalovaných modulov programu, v ktorom tiež nájdete číslo verzie každého modulu a dátum jeho poslednej úspešnej aktualizácie.

Priebeh aktualizácie

Po kliknutí na možnosť **Overiť dostupnosť aktualizácií** sa spustí proces sťahovania aktualizácií. Zároveň sa zobrazí indikátor priebehu sťahovania a zostávajúci čas do konca procesu. Ak chcete aktualizáciu zastaviť, môžete kliknúť na tlačidlo **Zrušiť aktualizáciu**.

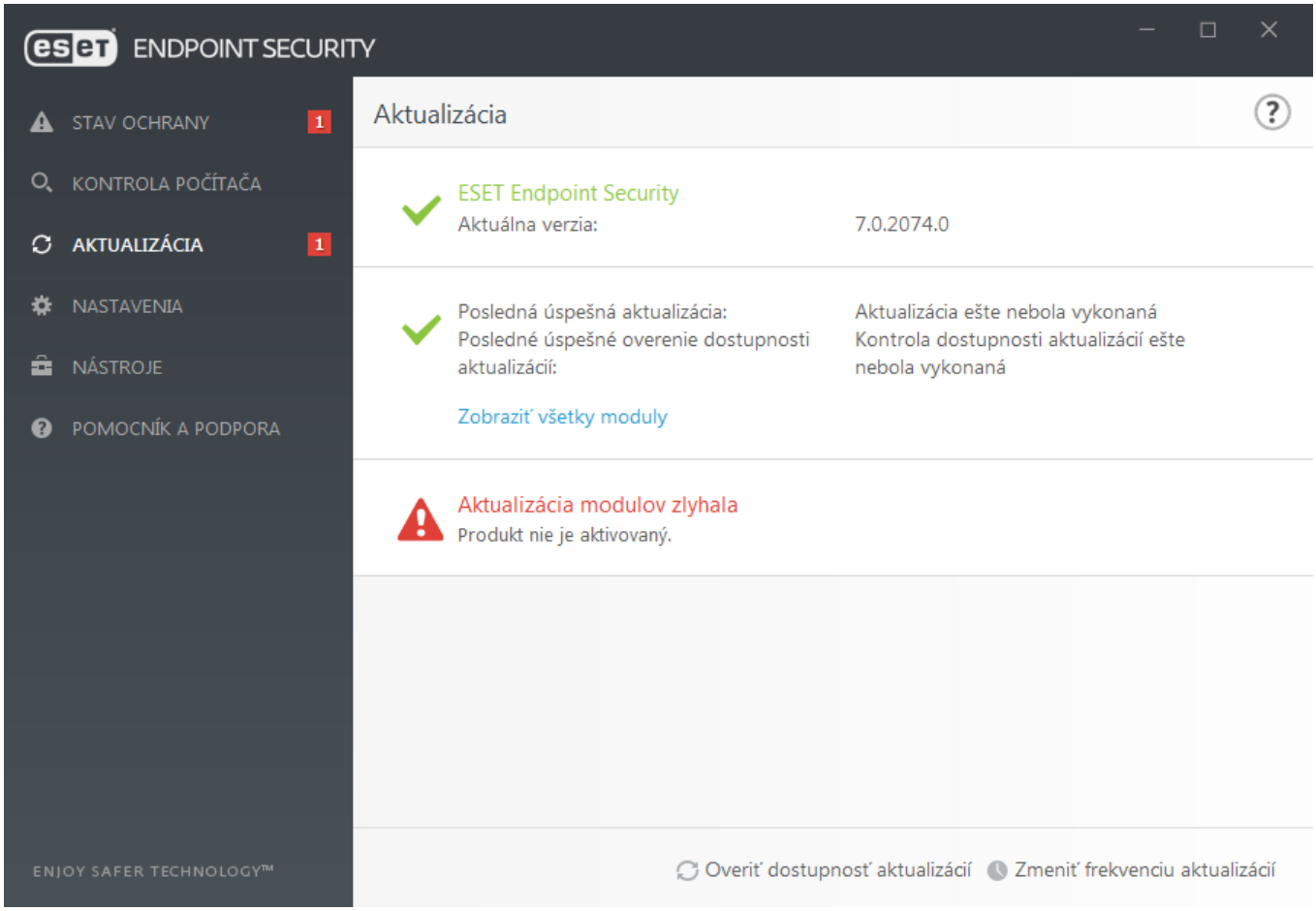


Za normálnych okolností sa moduly aktualizujú niekoľkokrát za deň. Ak tomu tak nie je, program nie je aktualizovaný a zvyšuje sa riziko napadnutia škodlivým kódom. Odporúčame vám v takomto prípade modul čo najskôr aktualizovať.

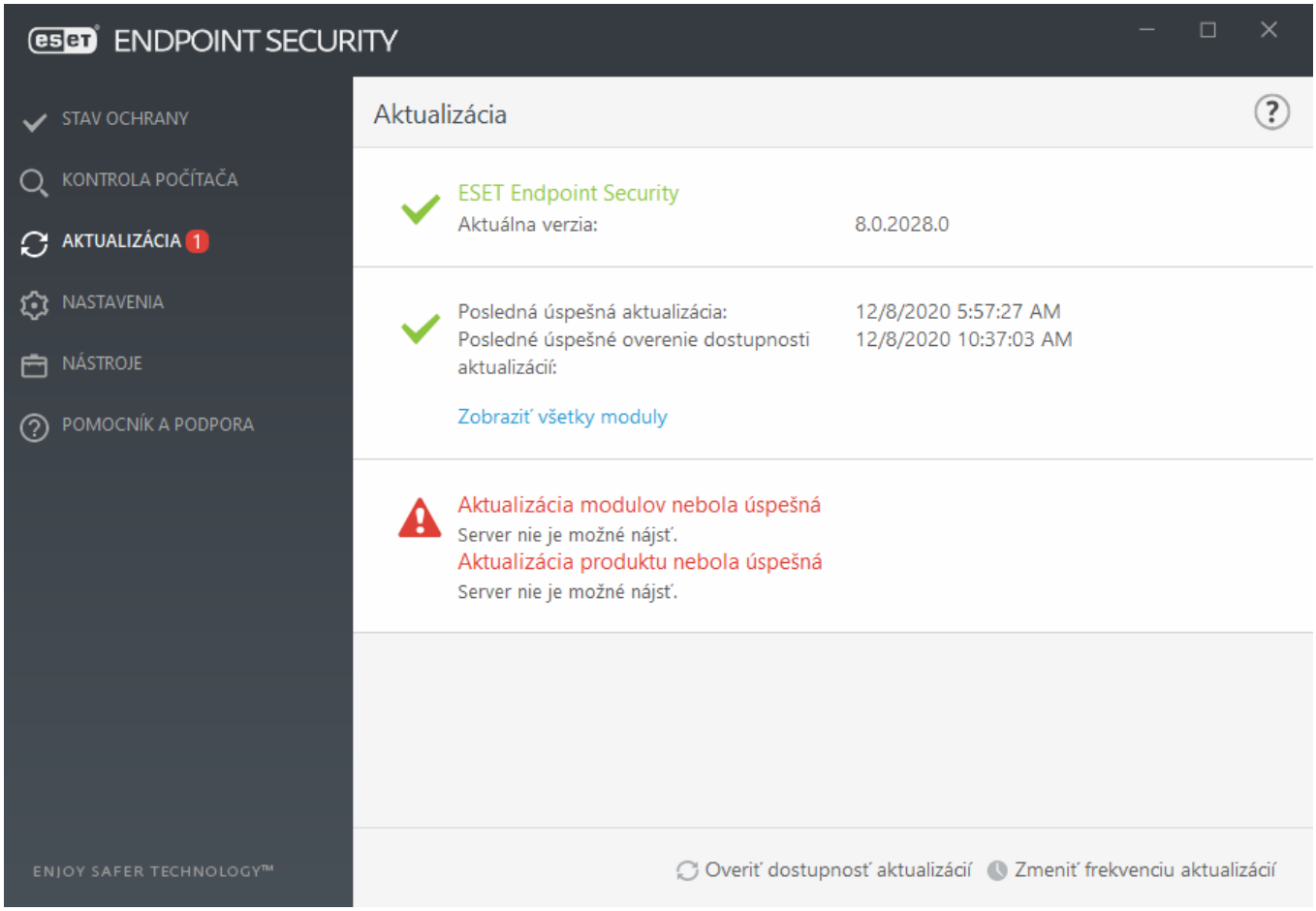
Detekčné jadro je neaktuálne – toto chybové hlásenie sa zobrazí po niekoľkých neúspešných pokusoch o aktualizáciu modulov. Odporúčame, aby ste skontrolovali nastavenia aktualizácie. Najčastejším problémom sú nesprávne zadané autorizačné údaje alebo nesprávne nakonfigurované nastavenia pripojenia.

V prípade neúspešnej aktualizácie sa zobrazí chybové hlásenie **Aktualizácia modulov nebola úspešná**, a to z nižšie uvedených dôvodov:

1. **Neplatná licencia** – licenčný kľúč bol zadaný nesprávne. Odporúčame, aby ste skontrolovali zadané licenčné údaje. Rozšírené nastavenia (prejdite do sekcie **Nastavenia** v hlavnom okne programu a kliknite na **Rozšírené nastavenia** alebo stlačte F5 na klávesnici) obsahujú rozšírené nastavenia aktualizácií. V hlavnom okne programu kliknite na **Pomocník a podpora** > **Zmeniť licenciu** a opätovne zadajte svoj licenčný kľúč.



2. **Pri sťahovaní aktualizačných súborov nastala chyba** – najčastejším problémom je nesprávne nastavenie internetového pripojenia. Odporúčame, aby ste si skontrolovali pripojenie na internet (otvorením akejkoľvek webovej stránky v internetovom prehliadači). Ak sa webová stránka nenačíta, počítač pravdepodobne nie je pripojený na internet alebo má problémy s pripojením. Uistite sa tiež, že váš poskytovateľ internetových služieb nemá výpadok pripojenia.



Viac informácií nájdete v nasledujúcom článku databázy znalostí spoločnosti ESET.

Nastavenie aktualizácií

Konfigurácia aktualizácie je dostupná v **Rozšírených nastaveniach** (F5) v časti **Aktualizácia**. Nastavenie aktualizácie pozostáva zo špecifikácie zdroja aktualizácie, teda z nastavenia aktualizačných serverov a autentifikácie voči týmto serverom.

Pre správne fungovanie aktualizácií je nevyhnutné mať všetky parametre nastavené správne. Ak používate firewall, treba zaistiť, aby mal program ESET povolenú komunikáciu cez internet (napríklad HTTPS komunikáciu).

Základné

Aktualizačný profil, ktorý je momentálne aktívny, je zobrazený v roletovom menu **Vybrať predvolený aktualizačný profil**.

Na vytvorenie nového profilu prejdite do sekcie Profily.

Automatické prepínanie profilu – priradí aktualizačný profil podľa Známych sietí v sekcii Firewall. Táto funkcia umožňuje, aby sa profil automaticky prepínal v závislosti od siete a nastavení v Plánovači. Viac informácií nájdete na stránkach pomocníka.

Konfigurovať oznámenia o aktualizáciách – kliknite na možnosť Upraviť, aby ste mohli vybrať, ktoré oznámenia aplikácie sa majú zobrazovať a ktoré nie. Môžete tiež zvoliť, či sa oznámenia majú Zobraziť na ploche a/alebo

Odoslať e-mailom.

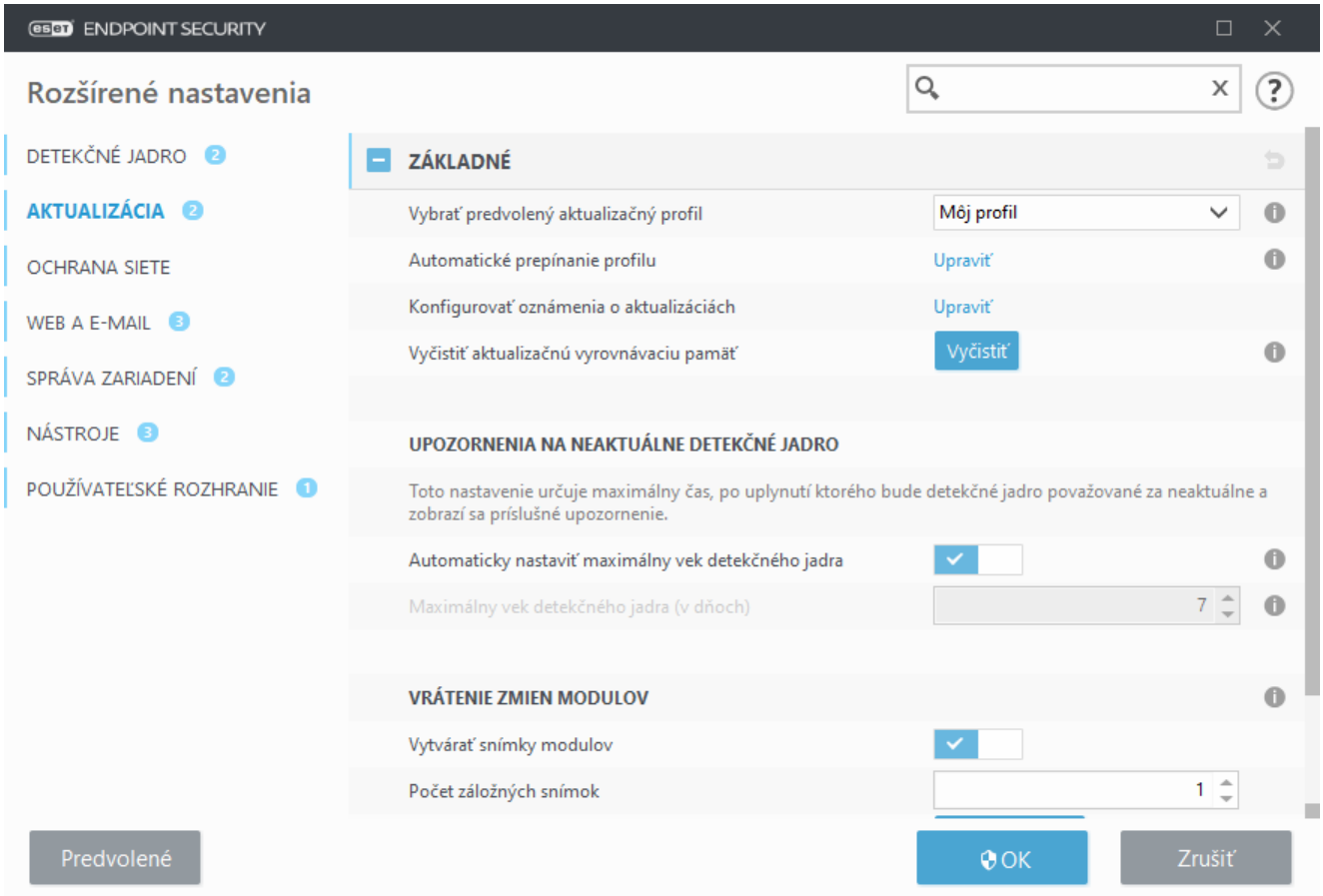
Ak sa vyskytnú problémy so sťahovaním aktualizácií modulov, kliknite na **Vyčistiť** vedľa možnosti **Vyčistiť aktualizačnú vyrovnávaciu pamäť** na vymazanie dočasných aktualizačných súborov/vyčistenie vyrovnávacej pamäte.

Upozornenia na neaktuálne detekčné jadro

Automaticky nastaviť maximálny vek detekčného jadra – táto možnosť umožňuje nastavenie maximálneho časového obdobia (v dňoch), po ktorom je detekčné jadro považované za neaktuálne a používateľovi sa zobrazí upozornenie. Predvolená hodnota pre **Maximálny vek detekčného jadra (v dňoch)** je 7.

Vrátenie zmien modulov

Ak máte podozrenie, že nová aktualizácia detekčného jadra alebo programových modulov môže byť nestabilná alebo poškodená, môžete program vrátiť späť do predchádzajúceho stavu a zakázať aktualizácie na určený časový interval.



Profily

V prípade potreby si môžete vytvoriť pre každú situáciu samostatný aktualizační profil s rozdielnou konfiguráciou. Možnosť vytvorenia alternatívneho profilu aktualizácie je užitočná predovšetkým pre používateľov, ktorí veľa cestujú a pripájajú sa do rozdielnych sietí.

Roletové menu **Vyberte profil na úpravu** zobrazuje momentálne vybraný profil. Predvolenou možnosťou je **Môj profil**.

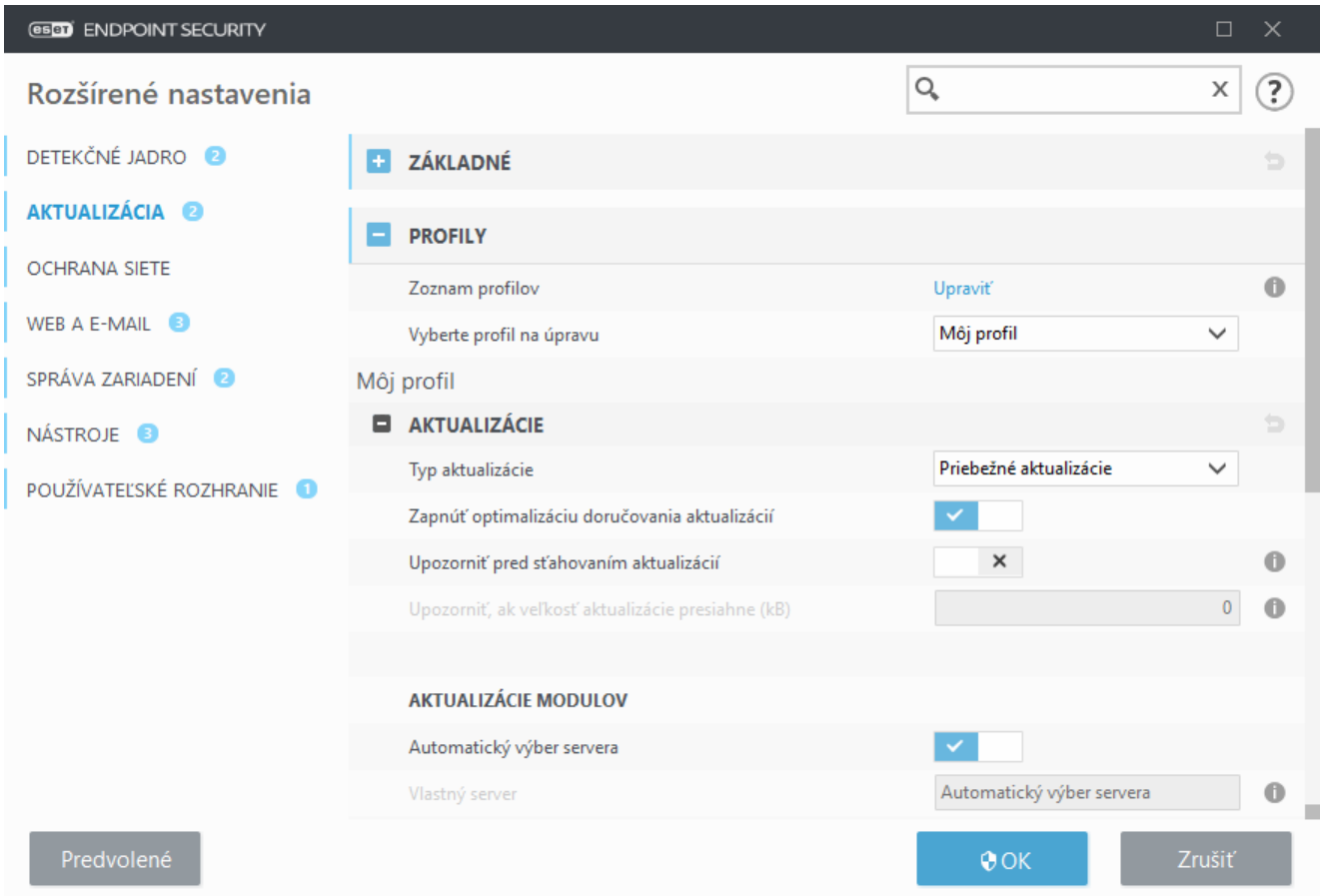
Vytvoriť nový profil je možné prostredníctvom tlačidla **Upraviť** vedľa položky **Zoznam profilov**. Zadajte **Názov profilu** a kliknite na **Pridať**.

Aktualizácie

Predvolenou možnosťou v roletovom menu Typ aktualizácie sú Priebežné aktualizácie, ktoré zabezpečujú priebežné sťahovanie aktualizačných súborov zo serverov spoločnosti ESET tak, aby pritom čo najmenej zaťažovali sieť. Predbežné aktualizácie sú aktualizácie, ktoré prešli dôkladným interným testovaním a budú čoskoro dostupné širokej verejnosti. Výhodou povolenia predbežných aktualizácií je možnosť prístupu k najnovším metódam detekcie a rôznym opravám. Treba však mať na pamäti, že predbežné aktualizácie nemusia byť vždy dostatočne stabilné a v žiadnom prípade by preto NEMALI byť používané na produkčných serveroch a pracovných staniciach, pri ktorých sa vyžaduje maximálna stabilita a dostupnosť. Oneskorená aktualizácia umožňuje sťahovanie aktualizácií zo špeciálnych aktualizačných serverov poskytujúcich nové verzie detekčného jadra s oneskorením najmenej X hodín (tzn. databázy testované v reálnom prostredí, ktoré sú považované za stabilné).

Zapnúť optimalizáciu doručovania aktualizácií – ak je táto možnosť povolená, aktualizačné súbory je možné sťahovať z CDN (sieť na doručovanie obsahu). Vypnutie tohto nastavenia môže spôsobiť prerušenie a spomalenie pri sťahovaní v prípade, že sú vyhradené aktualizačné servery ESET preťažené. Vypnutie je užitočné, ak je firewall nastavený na prístup výhradne k IP adresám aktualizačného servera ESET alebo ak pripojenie k CDN službám nefunguje.

Upozorniť pred sťahovaním aktualizácií – v prípade dostupnosti aktualizácie program zobrazí upozornenie, v ktorom môžete stiahnutie aktualizačných súborov potvrdiť alebo zamietnuť. Ak veľkosť aktualizácie presiahne hodnotu zadanú v poli Upozorniť, ak veľkosť aktualizácie presiahne (kB), program zobrazí potvrdzovacie dialógové okno. Ak je veľkosť aktualizačného súboru nastavená na 0 kB, program bude dialógové okno zobrazovať vždy.



Aktualizácie modulov

Predvolene je zapnutá možnosť **Automatický výber servera**. Možnosť **Vlastný server** predstavuje umiestnenie, kde sú uložené aktualizácie. Ak používate aktualizačný server spoločnosti ESET, odporúčame ponechať predvolené nastavenia.

Povoliť častejšie aktualizácie detekčných signatúr – umožňuje kratší časový interval medzi aktualizáciami detekčného jadra. Vypnutie tohto nastavenia môže mať negatívny vplyv na účinnosť detekcie.

Povoliť aktualizáciu modulov z vymeniteľných médií – umožňuje aktualizáciu z vymeniteľného média, ak dané médium obsahuje vytvorený mirror. Ak je zvolená možnosť Automatický, aktualizácia bude prebiehať na pozadí. Ak chcete, aby sa zobrazovali aktualizačné dialógové okná, vyberte možnosť Vždy sa spýtať.

Ak ako aktualizačný mirror používate lokálny HTTP server, zadajte aktualizačný server v tomto formáte: *http://nazov_pocitaca_alebo_jeho_IP_adresa:2221*

Ak používate lokálny HTTP server s SSL, zadajte aktualizačný server v tomto formáte: *https://nazov_pocitaca_alebo_jeho_IP_adresa:2221*

Ak ako aktualizačný mirror používate zdieľaný sieťový priečinok, zadajte aktualizačný server v tomto formáte: *nazov_pocitaca_alebo_jeho_IP_adresa**zdielany_priecinok*

> Číslo portu HTTP servera použité v príkladoch vyššie bude závisieť od toho, na ktorom porte počúva váš HTTP/HTTPS server.

Aktualizácie produktu

Prečítajte si kapitolu Aktualizácie produktu.

Možnosti pripojenia

Prečítajte si kapitolu Možnosti pripojenia.

Aktualizačný mirror

Prečítajte si kapitolu Aktualizačný mirror.

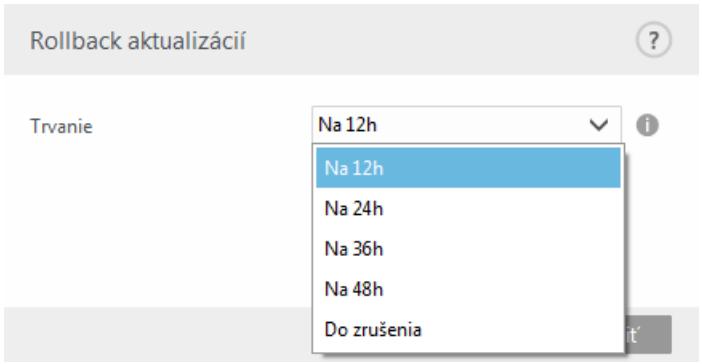
Vrátenie zmien aktualizácií

Ak máte podozrenie, že nová verzia detekčného jadra alebo programových modulov môže byť nestabilná alebo poškodená, môžete sa vrátiť na predchádzajúcu verziu a dočasne pozastaviť pravidelné aktualizácie. V tejto sekcii tiež môžete povoliť pravidelné aktualizácie, ktoré ste predtým odložili na neurčito.

ESET Endpoint Security vytvára záložné snímky programových modulov a detekčného jadra, ktoré môžu byť následne použité pri vrátení zmien na predchádzajúcu verziu (tzv. rollback). Pre vytváranie záložných snímok ponechajte možnosť **Vytvárať snímky modulov** označenú. Keď je vytváranie snímok modulov aktívne, prvá snímka sa vytvorí počas prvej aktualizácie. Ďalšia sa vytvorí po 48 hodinách. Pole **Počet záložných snímok** určuje počet snímok predošlých verzií modulov a detekčného jadra uložených na lokálnom disku počítača.

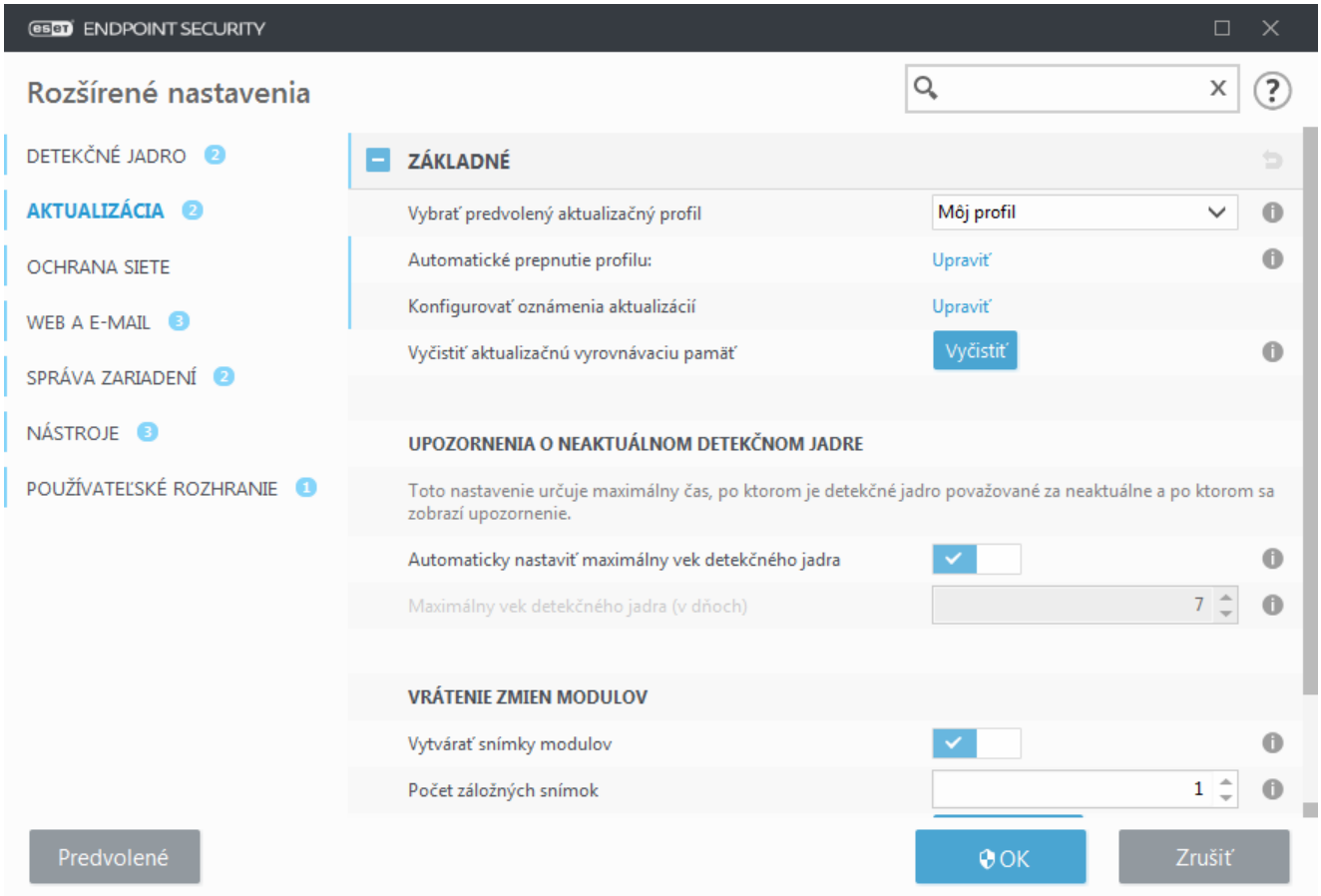
> Po dosiahnutí maximálneho počtu vytvorených záložných snímok (napr. troch) dôjde každých 48 hodín k nahradeniu najstaršej záložnej snímky novou. ESET Endpoint Security pri vrátení zmien vždy vráti späť najstaršiu záložnú snímku aktualizácie programových modulov a detekčného jadra.

Ak kliknete na tlačidlo **Vrátenie zmien** (**Rozšírené nastavenia** (F5) > **Aktualizácia** > **Základné** > **Vrátenie zmien modulov**), je potrebné z roletového menu **Trvanie** vybrať časový interval, počas ktorého budú pravidelné aktualizácie programových súčastí a detekčného jadra pozastavené.



Ak si želáte pravidelné aktualizácie odložiť na neurčito, až pokým ich neskôr manuálne nepovolíte, vyberte možnosť **Do zrušenia**. Keďže táto možnosť predstavuje potenciálne bezpečnostné riziko, jej výber neodporúčame.

Po vykonaní vrátenia zmien sa tlačidlo **Vrátenie zmien** zmení na tlačidlo s názvom **Povoliť aktualizácie**. Bez manuálneho povolenia aktualizácií sa počas vami stanoveného časového intervalu nebudú sťahovať ani inštalovať žiadne aktualizácie. Detekčné jadro sa vráti späť na verziu, ktorá je uložená na disku počítača ako záložná snímka a je najstaršia.



Uveďme si príklad, v ktorom najaktuálnejšia verzia detekčného jadra má číslo 22700. Na pevnom disku počítača sú uložené snímky verzií 22698 a 22696. Všimnite si, že 22697 nie je k dispozícii, pretože počítač bol napríklad istú dobu vypnutý a počas tohto obdobia vznikla už novšia aktualizácia, ktorá bola stiahnutá. Ak bolo v poli **Počet záložných snímok** nastavené číslo 2, po kliknutí na tlačidlo **Vrátenie zmien** sa detekčné jadro (vrátane programových modulov) obnoví na verziu s číslom 22696. Tento proces môže chvíľu trvať. Vrátenie detekčného jadra na staršiu verziu sa dá overiť v hlavnom okne programu v časti Aktualizácia.

Aktualizácie produktu

V sekcii **Aktualizácie produktu** sa nachádzajú nastavenia súvisiace s aktualizáciami produktu. Program vám umožňuje prednastaviť želané správanie v prípade, že sú k dispozícii nové aktualizácie produktu.

Aktualizácie produktu prinášajú do programu nové alebo upravujú už existujúce funkcie z predchádzajúcich verzií. Môžu prebiehať automaticky bez zásahu používateľa alebo s informovaním a výzvou na ich potvrdenie od používateľa. Po aktualizácii produktu sa môže vyžadovať reštart počítača.

Automatické aktualizácie – pozastavenie automatických aktualizácií pre konkrétne aktualizačné profily dočasne vypne funkciu automatických aktualizácií produktu pri pripojení na internet prostredníctvom iných sietí alebo pripojenia účtovaného podľa objemu údajov. Ak chcete mať neustály prístup k najnovším funkciám a najvyššej úrovni ochrany, ponechajte toto nastavenie zapnuté. Viac informácií o automatických aktualizáciách nájdete v kapitole Časté otázky o automatických aktualizáciách.

Na základe predvolených nastavení sa aktualizácie produktu sťahujú zo serverov repozitára ESET. Vo veľkých firemných prostrediach alebo offline prostrediach môžete využiť možnosť ukladania súborov produktu do internej vyrovnávacej pamäte.

Ako nastaviť vlastný server s aktualizáciami programových súčastí

1. V poli **Vlastný server** zadefinujte cestu k aktualizáciám produktu.
Zadať môžete cestu k HTTP(S) serveru, cestu k zdieľanému sieťovému umiestneniu SMB, cestu k lokálnemu disku alebo vymeniteľnému médiu. V prípade sieťového disku použite cestu UNC namiesto priradeného písmena disku.
2. Polia **Prihlasovacie meno** a **Heslo** ponechajte prázdne, ak sa tieto prístupové údaje nevyžadujú.
Ak sú prístupové údaje naopak potrebné, zadajte meno a heslo do príslušných polí pre HTTP overenie na vlastnom webovom serveri.
3. Potvrďte zmeny a overte dostupnosť aktualizácií produktu pomocou štandardnej aktualizácie produktu ESET Endpoint Security.

Vhodnosť použitia jednotlivých volieb pre aktualizáciu programových komponentov je závislá od počítača, na ktorom budú uvedené nastavenia aplikované. Nezabúdajte na rozdiely medzi pracovnými stanicami a servermi. Napríklad pri serveroch môže byť ich automatický reštart po aktualizácii produktu nežiaduci, pretože by mohol firme spôsobiť závažné problémy či škody.

Možnosti pripojenia

Pre prístup k nastaveniam proxy servera pre daný aktualizačný profil kliknite na položku **Aktualizácia** v **Rozšírených nastaveniach** (F5) a potom kliknite na **Profily** > **Aktualizácie** > **Možnosti pripojenia**.

Proxy server

Kliknite na roletové menu vedľa popisu **Režim proxy** a označte jednu z nasledujúcich možností:

- Nepoužívať proxy server
- Pripojenie prostredníctvom proxy servera
- Použiť globálne nastavenie proxy servera

Po označení možnosti **Použiť globálne nastavenie proxy servera** budú použité globálne nastavenia, ktoré sa

nachádzajú v rozšírených nastaveniach v sekcii **Nástroje** > **Proxy server**.

Po označení možnosti **Nepoužívať proxy server** používateľ explicitne definuje, že pri aktualizácii ESET Endpoint Security nemá byť použitý žiadny proxy server.

Možnosť **Pripojenie prostredníctvom proxy servera** označte v týchto prípadoch:

- Na aktualizáciu produktu ESET Endpoint Security sa používa iný proxy server ako ten, ktorý je zadefinovaný v časti Nástroje > **Proxy server**. Pri tejto konfigurácii by mali byť údaje nového proxy servera špecifikované v príslušných poliach. Je potrebné zadať adresu **Proxy servera**, komunikačný **Port** (predvolene 3128), prípadne tiež **Prihlasovacie meno** a **Heslo**.
- Proxy server používaný pri aktualizácii ESET Endpoint Security je iný ako globálne nastavený proxy server.
- Váš počítač je pripojený na internet cez proxy server. Nastavenia sú prevzaté z prehliadača počas inštalácie programu, no ak dôjde po čase k zmene v nastaveniach proxy servera (napríklad v dôsledku zmeny sprostredkovateľa internetového pripojenia – ISP), bude potrebné skontrolovať nastavenia proxy v tejto sekcii. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií z aktualizačných serverov.

Pri štandardnej inštalácii je prednastavená možnosť **Použiť globálne nastavenie proxy servera**.

Použiť priame pripojenie, ak proxy nie je k dispozícii – ak bude proxy nedostupné, bezpečnostný produkt ESET sa automaticky pokúsi pripojiť k aktualizačným serverom bez použitia proxy.

Zdieľané lokality systému Windows

Pri aktualizácii z lokálneho servera s verziou operačného systému Windows NT sa pre každé sieťové spojenie predvolene vyžaduje autorizácia.

Pre nastavenie overovaného účtu vyberte v roletovom menu **Pre pripojenie do LAN vystupovať ako** jednu z nasledujúcich možností:

- **Systémový účet (predvolený)**,
- **Aktuálny používateľ**,
- **Určený používateľ**.

Ak sa chcete autorizovať svojím systémovým účtom, vyberte možnosť **Systémový účet (predvolený)**. Za normálnych okolností autorizácia nebude vykonaná, ak nie sú nastavené autorizačné údaje v hlavných nastaveniach aktualizácie.

Ak sa použije možnosť **Aktuálny používateľ**, program sa bude autorizovať pod účtom aktuálne prihláseného používateľa. Nevýhodou v prípade tohto nastavenia je, že program sa nemôže pripojiť na aktualizačný server, ak nie je na počítači prihlásený žiadny používateľ.

Ak sa použije možnosť **Určený používateľ**, autorizácia bude vykonaná pod zadaným používateľom. Túto možnosť odporúčame v prípade, že zlyhá spojenie pod lokálnym systémovým účtom. Je však potrebné dbať na to, aby mal určený používateľský účet práva na prístup k adresáru s aktualizačnými súbormi, ktorý sa nachádza na lokálnom serveri. V opačnom prípade sa spojenie nepodarí vytvoriť a nestiahne sa aktualizácia.

Nastavenia **Prihlasovacieho mena** a **Hesla** sú voliteľné.

Pri použití možností **Aktuálny používateľ** a **Určený používateľ** môže nastať chyba pri zmene identity programu na požadovaného používateľa. Z toho dôvodu odporúčame pri pripojení do LAN nastaviť autorizačné údaje v hlavných nastaveniach aktualizácie. V týchto nastaveniach je potrebné uviesť údaje v nasledovnom tvare: *názov_domény\používateľ* (v prípade pracovnej skupiny – workgroup je to *názov_pracovnej_skupiny\používateľ*) a heslo. Pri aktualizácii cez HTTP nie je štandardne potrebné zadávať autorizačné údaje.

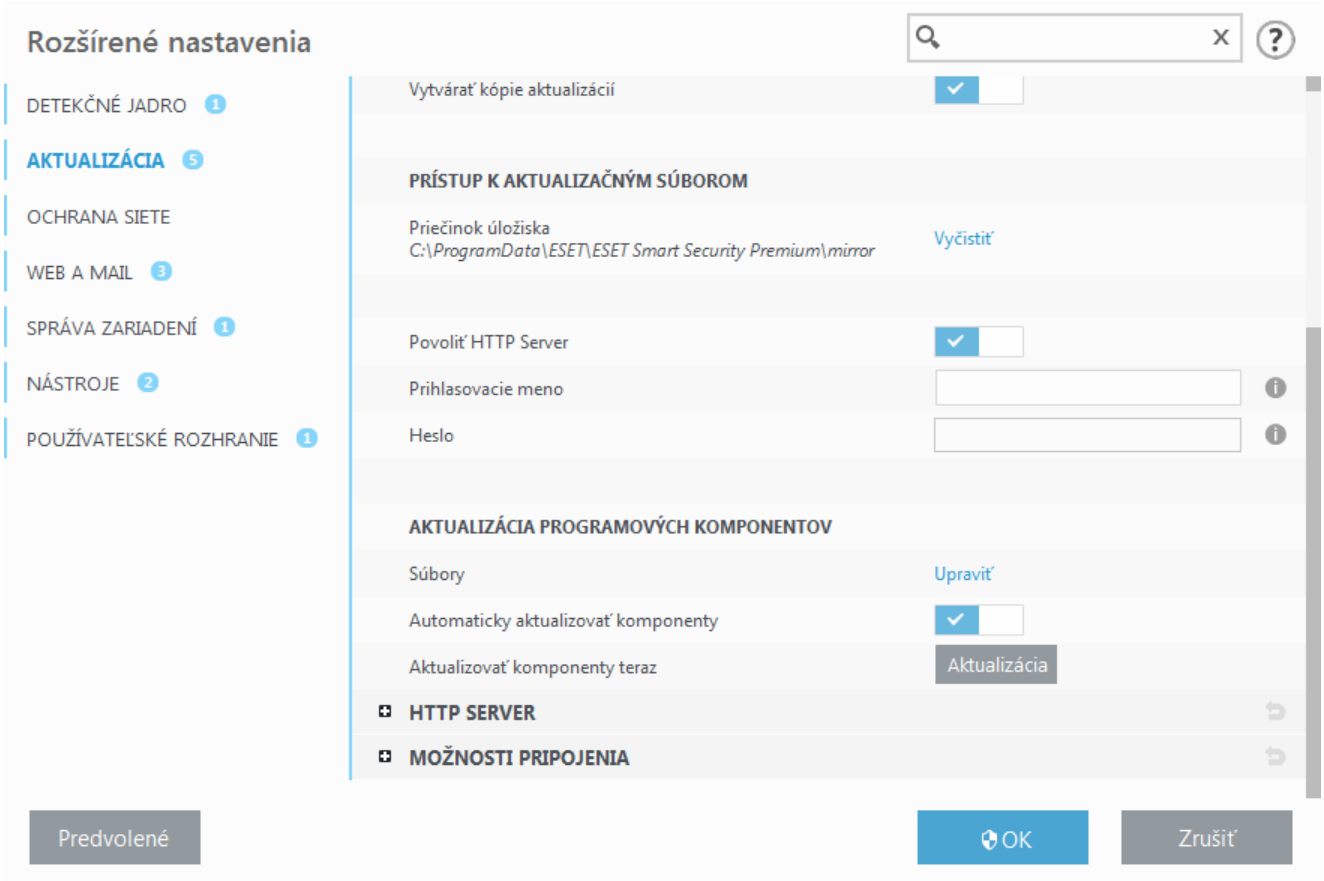
V prípade, že pripojenie na server zostáva aktívne aj po stiahnutí aktualizácie, odporúčame vynútiť ukončenie spojenia výberom možnosti Po dokončení aktualizácie **odpojiť** zo servera.

Aktualizačný mirror

ESET Endpoint Security umožňuje vytváranie kópií aktualizačných súborov (tzv. mirror), ktoré je možné následne použiť na aktualizáciu iných počítačov v sieti. Mirror je výhodné použiť najmä pri väčších sieťach, kde by sťahovanie aktualizácií z internetu každým počítačom samostatne spôsobovalo prenos väčšieho množstva dát. Preto je odporúčané aktualizovať len jeden objekt v sieti priamo z aktualizačných serverov na internete a následne aktualizáciu sprístupniť pomocou mirrora ostatným objektom v lokálnej sieti. Aktualizácia pracovných staníc z mirrora zabezpečuje rozloženie zaťaženia siete a šetrí spotrebu dát stiahnutých z internetu.

V sieťach, kde sa používa ESET PROTECT na správu veľkého množstva klientov, odporúčame na zníženie objemu sťahovaných dát z internetu uprednostniť Apache HTTP Proxy pred konfiguráciou mirrora na niektorom z klientov. Apache HTTP Proxy je možné nainštalovať spolu s ESET PROTECT pomocou all-in-one inštalátora alebo ako samostatný komponent. Viac informácií a prehľad rozdielov medzi Apache HTTP Proxy, nástrojom Mirror Tool a priamym pripojením nájdete v Online pomocníkovi pre ESET PROTECT.

Možnosti konfigurácie lokálneho mirrora nájdete v Rozšírených nastaveniach v sekcii **Aktualizácia**. Stlačte kláves **F5** pre otvorenie Rozšírených nastavení, kliknite na **Aktualizácia** > **Profily a rozbaľte časť Aktualizačný mirror**.



Pre vytvorenie mirrora na klientskej pracovnej stanici povoľte možnosť **Vytvárať kópie aktualizácií**. Po aktivovaní tejto možnosti sa sprístupnia ďalšie nastavenia mirrora, predovšetkým spôsob prístupu k aktualizačným súborom a definovanie adresára, do ktorého sa budú ukladať aktualizačné súbory vytváraného mirrora.

Prístup k aktualizačným súborom

Povoliť HTTP Server – po aktivovaní začne program poskytovať aktualizačné súbory pomocou HTTP servera, pričom nebude potrebné zadávať prihlasovacie údaje.

Spôsoby sprístupnenia mirrora sú podrobne popísané v kapitole Aktualizácia z mirrora. Existujú dva základné spôsoby sprístupnenia mirrora, a to buď prostredníctvom zdieľaného sieťového priečinka, alebo sprístupnením kópie aktualizácie cez HTTP server.

Priečinok, do ktorého sa budú ukladať aktualizačné súbory vytváraného mirrora, zadajte do poľa **Priečinok na ukladanie aktualizačných súborov**. Ak chcete vybrať iný priečinok, kliknutím na **Vyčistiť** odstráňte prednastavený priečinok *C:\ProgramData\ESET\ESET Endpoint Security\mirror* a kliknutím na **Upraviť** vyhľadajte priečinok v lokálnom počítači alebo zdieľaný sieťový priečinok. V prípade, že je na prístup a zápis do zvoleného priečinka nevyhnutná autorizácia, je potrebné zadať autorizačné údaje do polí **Prihlasovacie meno** a **Heslo**. Ak je vybraný súbor umiestnený na sieťovom disku, pričom operačným systémom je Windows NT/2000/XP, zadané prihlasovacie meno a heslo používateľa musí mať práva na zápis do zvoleného priečinka. Prihlasovacie meno zadávajte vo formáte *Doména/Používateľ* alebo *Pracovná_skupina/Používateľ*. Nezabudnite tiež na príslušné heslo.

HTTP Server a SSL pre mirror

V sekcii **HTTP Server** na karte **Mirror** môžete nastaviť **Port servera** a metódu **Overenia**, ktorú bude využívať váš HTTP server. V predvolených nastaveniach je port servera nastavený na **2221**.

Pomocou možnosti **Overenie** zvoľte metódu autorizácie pre prístup k aktualizačným súborom. K dispozícii sú nasledujúce možnosti: **Žiadne**, **Základné** a **NTLM**. Zvolením možnosti **Základné** zaistíte, že prihlasovacie meno a heslo bude šifrované použitím jednoduchej metódy kódovania base64. Možnosť **NTLM** zabezpečí kódovanie prostredníctvom bezpečnej metódy. Pre overenie sa používajú používatelia vytvorení na stanici zdieľajúcej aktualizačné súbory. Prednastavená je možnosť **Žiadne**, ktorá sprístupňuje aktualizačné súbory bez potreby overenia.

Autentifikačné údaje ako **Prihlasovacie meno** a **Heslo** slúžia na prístup k mirror HTTP serveru. Vyplňte ich len v prípade, že server vyžaduje ich zadanie.

Vyberte **Súbor s reťazcom certifikátov** alebo vygenerujte certifikát s vlastným podpisom, ak chcete prevádzkovať HTTP server s podporou SSL. Sú dostupné tieto **typy certifikátov**: ASN, PEM a PFX. Pre dodatočné zabezpečenie môžete na poskytovanie aktualizačných súborov na stiahnutie použiť protokol HTTPS. Pri použití tohto protokolu je takmer nemožné vystopovať prihlasovacie údaje a prenosy dát. Typ **súkromného kľúča** je predvolene nastavený ako **Integrovaný** (preto je možnosť **Súbor obsahujúci súkromný kľúč** nedostupná). To znamená, že súkromný kľúč je súčasťou reťazca certifikátu.

Certifikáty s vlastným podpisom pre HTTPS mirror
Ak používate HTTPS mirror server, je potrebné importovať jeho certifikát do dôveryhodného koreňového úložiska na všetkých klientskych počítačoch. Viac informácií nájdete v článku spoločnosti Microsoft o inštalácii dôveryhodného koreňového certifikátu v systéme Windows.

Aktualizácia z mirrora

Existujú dva základné spôsoby sprístupnenia mirrora, ktorý predstavuje repozitár pre klienty na sťahovanie aktualizácií. Adresár s aktualizačnými súbormi môže byť buď zdieľaný sieťový adresár, alebo HTTP server.

Sprístupnenie mirrora prostredníctvom HTTP servera

Je použité automaticky ako preddefinované nastavenie pri predvolenej konfigurácii programu. Pre sprístupnenie mirrora prostredníctvom HTTP servera prejdite do časti **Rozšírené nastavenia** > **Aktualizácia** > **Profily** > **Aktualizačný mirror** a vyberte možnosť **Vytvárať kópie aktualizácií**.

V sekcii **HTTP Server** na karte **Mirror** môžete nastaviť **Port servera** a metódu **Overenia**, ktorú bude využívať váš HTTP server. V predvolených nastaveniach je port servera nastavený na **2221**.

Pomocou možnosti **Overenie** zvoľte metódu autorizácie pre prístup k aktualizačným súborom. K dispozícii sú nasledujúce možnosti: **Žiadne**, **Základné** a **NTLM**. Zvolením možnosti **Základné** zaistíte, že prihlasovacie meno a heslo bude šifrované použitím jednoduchej metódy kódovania base64. Možnosť **NTLM** zabezpečí kódovanie prostredníctvom bezpečnej metódy. Pre overenie sa používajú používatelia vytvorení na stanici zdieľajúcej aktualizačné súbory. Prednastavená je možnosť **Žiadne**, ktorá sprístupňuje aktualizačné súbory bez potreby overenia.

Pri sprístupnení aktualizačných súborov prostredníctvom HTTP servera musí byť mirror priečinok umiestnený na rovnakom počítači ako ESET Endpoint Security, ktorý mirror vytvára.

Chybové hlásenie **Nesprávne meno alebo heslo** sa zobrazí po niekoľkých neúspešných pokusoch o aktualizáciu prostredníctvom mirrora. Odporúčame v sekcii **Rozšírené nastavenia** > **Aktualizácia** > **Profily** > **Aktualizačný mirror** skontrolovať prihlasovacie meno a heslo. Najčastejším problémom sú nesprávne zadané autorizačné údaje.

Po nastavení mirrora nastavte na klientskych pracovných staniciach nový aktualizačný server. Postupujte takto:

- Otvorte **Rozšírené nastavenia** (F5) a prejdite do sekcie **Aktualizácia** > **Profily** > **Aktualizácie** > **Aktualizácie modulov**.
- Vypnite **Automatický výber servera** a pridajte nový server do poľa **Aktualizačný server** v jednom z nasledujúcich formátov:
  http://IP_adresa_vášho_servera:2221
  https://IP_adresa_vášho_servera:2221 (v prípade používania SSL)

Sprístupnenie mirrora prostredníctvom zdieľaného adresára

Ako prvý krok je potrebné na lokálnom, či sieťovom disku vytvoriť zdieľaný adresár. Pri vytváraní adresára pre mirror je potrebné dbať na to, aby používateľ, ktorý do neho bude zapisovať, mal práva na „zápis“. Používatelia, ktorí budú aktualizovať ESET Endpoint Security z mirrora, musia mať práva na „čítanie“ z mirror adresára.

Nastavte prístup k mirroru v časti **Rozšírené nastavenia** > **Aktualizácia** > **Profily** > **Aktualizačný mirror** zakázaním možnosti **Povoliť HTTP server**. Táto možnosť je v predvolených nastaveniach zakázaná.

V prípade umiestnenia zdieľaného adresára na iný počítač v sieti je potrebné nastaviť autorizáciu voči tejto stanici. Autorizáciu nastavíte v programe ESET Endpoint Security cez **Rozšírené nastavenia** (**F5**) > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia** > **Zdieľané lokality systému Windows** > **Pre pripojenie do LAN vystupovať**

ako. Toto nastavenie je rovnaké ako pri aktualizácii a je popísané v kapitole Pre pripojenie do LAN vystupovať ako.

Pre prístup k mirror adresáru je potrebný rovnaký účet ako ten, ktorý sa používa pre prihlásenie do počítača, na ktorom je mirror vytvorený. V prípade, že daný počítač je v doméne, použite používateľské meno v tvare „doména\používateľ“. Ak počítač nie je v doméne, použite tvar „IP_adresa_servera\používateľ“ alebo „názov hostiteľa\používateľ“.

Po konfigurácii mirrora je potrebné na staniciach nastaviť *UNC**PATH* ako nový aktualizačný server podľa nasledujúceho postupu:

1. Otvorte **Rozšírené nastavenia** programu ESET Endpoint Security a kliknite na **Aktualizácia** > **Profily** > **Aktualizácie**.
2. Vypnite **Automatický výber servera** v sekcii **Aktualizácie modulov** a pridajte nový server do poľa **Aktualizačný server** vo formáte *UNC**PATH*.

Pri zadávaní cesty k aktualizačnému serveru je dôležité, aby bola použitá cesta UNC. V opačnom prípade nemusia aktualizácie z mapovaných diskov správne fungovať.

Vytvorenie mirrora pomocou nástroja Mirror Tool
Nástroj Mirror Tool vytvára štruktúru priečinkov odlišnú od tej, ktorú vytvára funkcia mirror v samotnom produkte. Každý priečinok obsahuje aktualizačné súbory pre konkrétnu skupinu produktov. Je teda potrebné v nastaveniach aktualizácie zadať úplnú cestu k správnemu priečinku.
Napríklad, ak chcete aktualizovať ESET PROTECT z mirrora, nastavte aktualizačný server na hodnotu (podľa umiestnenia koreňa vášho HTTP servera):
`http://your_server_address/mirror/eset_upd/era6`

Posledné nastavenie v tejto časti je nastavenie aktualizácie programových súčastí (PCU). Predvolene je táto možnosť zapnutá. Ak je možnosť **Aktualizácie produktu** zapnutá, nemusíte viac klikať na **Aktualizovať**, pretože súbory sú skopírované do lokálneho mirrora automaticky hneď, ako sú dostupné. Viac informácií o aktualizáciách produktu nájdete v časti Režim aktualizácie.

Riešenie problémov pri aktualizácii z mirrora

Vo väčšine prípadov sú problémy pri aktualizácii z mirrora spôsobené nesprávnym nastavením niektorého z nastavení v rámci záložky Mirror, nesprávnym nastavením práv prístupu k aktualizačnému adresáru Mirror, nesprávnym nastavením lokálnej stanice pokúšajúcej sa aktualizovať z mirrora alebo kombináciou viacerých z vyššie spomenutých príčin. Prinášame prehľad najbežnejších problémov, ktoré môžu nastať pri aktualizácii z mirrora:

ESET Endpoint Security nevie nadviazať spojenie s mirrorom – pravdepodobnou príčinou je nesprávne zadaný aktualizačný server (sieťová cesta k adresáru mirror), z ktorého si má lokálna stanica stiahnuť aktualizáciu. Správnosť adresára overíte tak, že kliknete na **Štart** > **Spustiť**, zadáte názov adresára a kliknete na **OK**. Mal by sa zobraziť obsah adresára.

ESET Endpoint Security vyžaduje prihlasovacie meno a heslo – pravdepodobnou príčinou sú nesprávne zadané autorizačné údaje (prihlasovacie meno a heslo) v nastaveniach Aktualizácie. Tie slúžia na prístup na aktualizačný server, z ktorého sa má program ESET na lokálnej pracovnej stanici aktualizovať. Uistite sa, že autorizačné údaje sú správne a zadané v správnom formáte, napr. Doména/Prihlasovacie meno alebo Pracovná skupina/Prihlasovacie meno a prislúchajúce heslo. Ak je mirror sprístupnený pre „Everyone” (t. j. pre každého používateľa), neznamená to, že prístup bude mať akýkoľvek neoprávnený používateľ. Znamená to, že priečinok bude prístupný pre všetkých používateľov domény. Preto aj keď je priečinok takto sprístupnený, stále bude

potrebné zadať doménové používateľské meno a heslo v nastaveniach Aktualizácie.

ESET Endpoint Security nevie nadviazať spojenie s mirrorom – nie je povolená komunikácia na porte, ktorý bol nastavený pre sprístupnenie mirrora cez HTTP server.

ESET Endpoint Security zaznamenal chybu pri sťahovaní súboru aktualizácie – pravdepodobne spôsobené nesprávnym zadaním aktualizačného servera (sieťovej cesty k adresáru mirror), z ktorého si má lokálna pracovná stanica sťahovať aktualizácie.

Vytvorenie aktualizačnej úlohy

Aktualizáciu môžete spustiť manuálne kliknutím na tlačidlo **Overiť dostupnosť aktualizácií** na záložke **Aktualizácia** v hlavnom okne programu.

Aktualizácie sa dajú spúšťať aj ako plánované úlohy. Tie možno nastaviť po kliknutí na **Nástroje** > **Plánovač**. V programe ESET Endpoint Security sú predvolene aktivované nasledujúce aktualizačné úlohy:

- **Pravidelná automatická aktualizácia**
- **Automatická aktualizácia po modemovom pripojení**
- **Automatická aktualizácia po prihlásení používateľa**

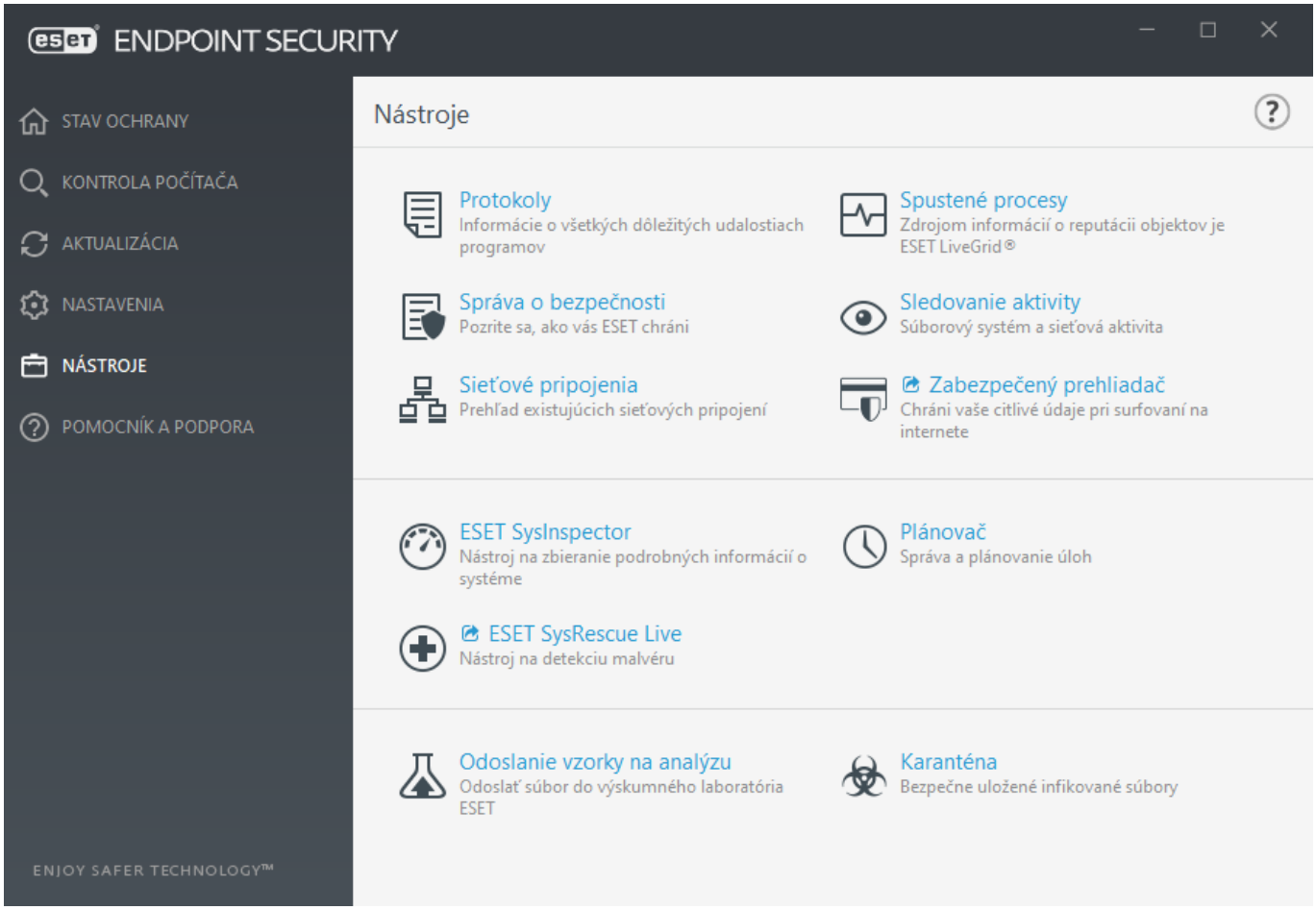
Každú z vyššie uvedených aktualizačných úloh môžete upravovať podľa vašich potrieb. Okrem predvolených aktualizačných úloh môžete vytvoriť nové plánované úlohy s vlastným nastavením. Pre bližší popis vytvárania a nastavenia aktualizačných úloh si pozrite kapitolu Plánovač.

Nástroje

Menu **Nástroje** obsahuje moduly, ktoré pomáhajú zjednodušiť správu programu a ponúkajú doplňujúce nastavenia pre pokročilých používateľov.

K dispozícii máte nasledujúce nástroje:

- Protokoly
- Spustené procesy (ak je povolený ESET LiveGrid® v ESET Endpoint Security)
- Správa o bezpečnosti (pre nespravované koncové zariadenia)
- Sieťové pripojenia (ak je v ESET Endpoint Security povolený Firewall)
- Zabezpečený prehliadač (v ESET Endpoint Security je predvolene vypnutý)
- ESET SysInspector
- Plánovač
- ESET SysRescue Live – presmeruje vás na webovú stránku ESET SysRescue Live, z ktorej si môžete stiahnuť súbor .iso obsahujúci ESET SysRescue Live.
- Odoslanie vzorky na analýzu – umožňuje vám odoslať podozrivé súbory na analýzu do výskumného laboratória ESET (tento nástroj nemusí byť k dispozícii v závislosti od konfigurácie ESET LiveGrid®).
- Karanténa



Protokoly

Protokoly obsahujú informácie o všetkých systémových udalostiach a poskytujú prehľad zistených ohrození. Predstavujú silný nástroj systémovej analýzy, odhaľovania problémov a rizík a v neposlednom rade hľadania riešení. Vytváranie protokolov prebieha aktívne na pozadí bez akejkoľvek interakcie zo strany používateľa. Informácie sú zaznamenávané na základe nastavenej úrovne podrobnosti zápisu do protokolov. Prezeranie protokolov a textových správ je možné priamo z prostredia ESET Endpoint Security. Rovnako je tieto protokoly možné archivovať.

Protokoly sú dostupné z hlavného okna programu po kliknutí na položku **Nástroje** > **Protokoly**. Zvoľte názov protokolu a vyberte akciu z roletového menu **Protokoly**. Dostupné sú nasledujúce protokoly:

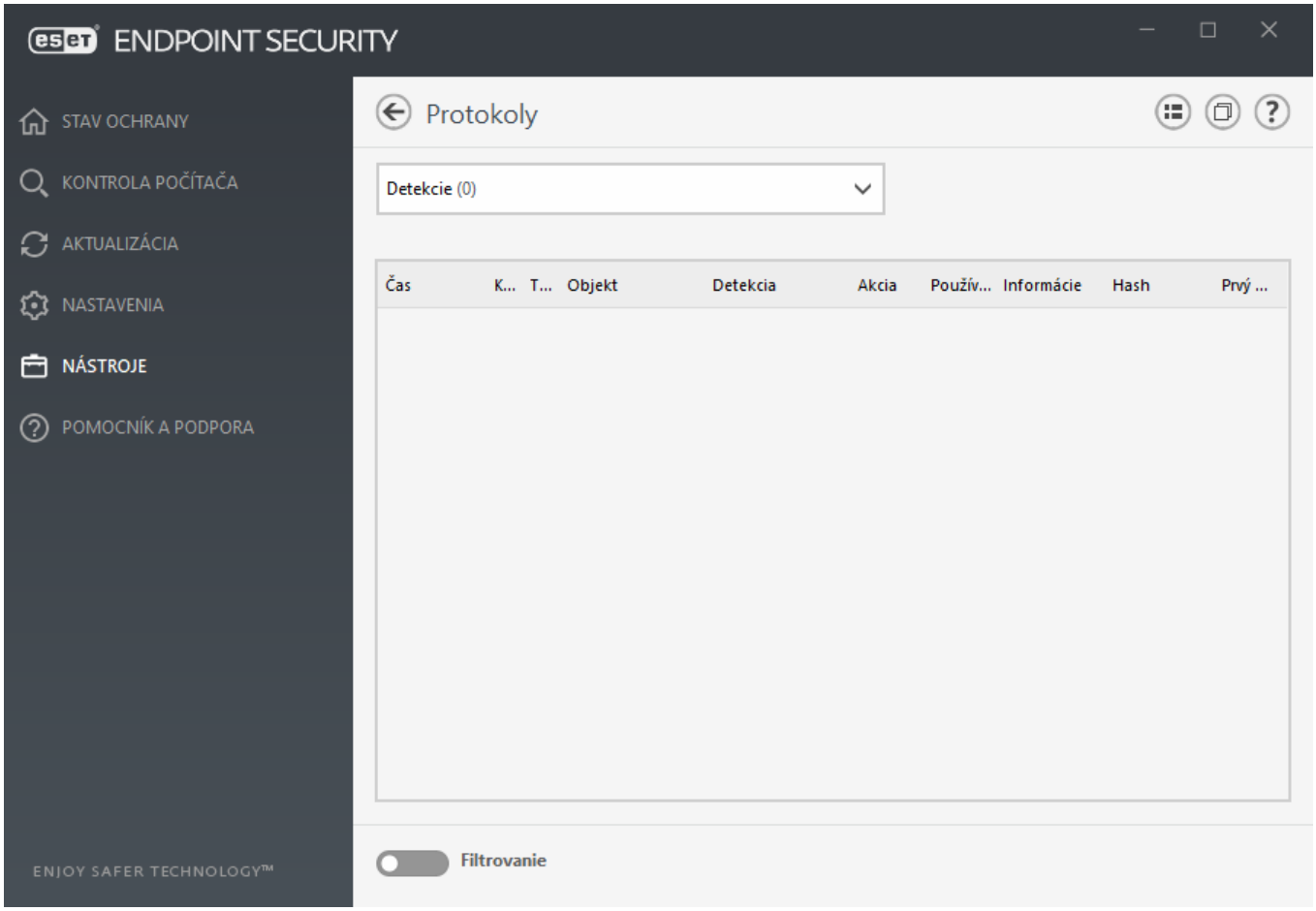
- **Detekcie** – tento protokol ponúka podrobné informácie o detekciách a infiltráciách zachytených pomocou modulov ESET Endpoint Security. Informácie v protokoloch zahŕňajú čas detekcie, názov detekcie, umiestnenie, vykonanú akciu a meno používateľa prihláseného v čase, kedy bola detegovaná infiltrácia. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte jej podrobnosti v osobitnom okne. Nevyliečené infiltrácie sú vždy označené červeným textom na svetločervenom pozadí, zatiaľ čo vyliečené infiltrácie sú označené žltým textom na bielom pozadí. Nevyliečené potenciálne nebezpečné a nechcené aplikácie sú označené žltým textom na bielom pozadí.
- **Udalosti** – v tomto protokole sú zaznamenané všetky dôležité operácie vykonané programom ESET Endpoint Security. Protokol udalostí obsahuje informácie o udalostiach v programe a chybách, ktoré sa vyskytli. Je navrhnutý tak, aby pomáhal správcom systémov a používateľom pri riešení problémov. Informácie získané z tohto protokolu vám často pomôžu nájsť príčiny problémov, prípadne ich riešenie.
- **Kontrola počítača** – tento protokol obsahuje výsledky všetkých vykonaných kontrol. Každý riadok prináleží samostatnej kontrole. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte podrobnosti príslušnej

kontroly.

- **Blokované súbory** – tento protokol obsahuje záznamy o blokovaných súboroch, ku ktorým bol zamietnutý prístup pri prepojení so službou ESET Enterprise Inspector. V protokole je uvedená príčina zablokovania a programový modul, ktorý súbor zablokoval, ako aj aplikácia a používateľ, ktorý súbor spustil. Viac informácií nájdete v online používateľskej príručke pre ESET Enterprise Inspector.
- **Odoslané súbory** – tento protokol obsahuje záznamy o súboroch, ktoré boli odoslané do ESET LiveGrid® alebo ESET LiveGuard na analýzu.
- **Protokoly auditu** – každý protokol obsahuje dátum a čas vykonanej zmeny, informácie o type zmeny, zdroji a používateľovi, ako aj popis. Pre viac informácií si prečítajte kapitolu Protokoly auditu.
- **HIPS** – tento protokol obsahuje záznamy konkrétnych pravidiel systému HIPS označených na zaznamenávanie. V protokole je zobrazená aplikácia, ktorá danú operáciu vyvolala, výsledok (tzn. či bolo pravidlo povolené alebo zakázané), prípadne aj názov vytvoreného pravidla.
- **Ochrana siete** – tento protokol zobrazuje všetky vzdialené útoky zachytené Ochranou pred sieťovými útokmi alebo Firewallom. Nájdete tu informácie o všetkých útokoch na váš počítač. V stĺpci Udalosť je typ zisteného útoku. V stĺpci Zdroj sú podrobnejšie informácie o útočníkovi. V stĺpci Protokol je uvedený komunikačný protokol použitý pri útoku. Analýzou tohto protokolu ochrany siete je možné včas odhaliť pokusy o prienik do systému. Viac informácií o sieťových útokoch nájdete v časti IDS a pokročilé možnosti.

- **Filtrované stránky** – Tento zoznam je užitočný v prípade, ak si želáte vidieť webové stránky, ktoré boli blokované modulom Ochrana prístupu na web alebo modulom Webová kontrola. V tomto protokole môžete vidieť čas, adresu URL, používateľa a aplikáciu, ktorá vytvorila spojenie s príslušnou webovou stránkou.

- **Antispamová ochrana** – obsahuje záznamy súvisiace s e-mailovými správami, ktoré boli označené ako spam.
- **Webová kontrola** – protokol zobrazuje povolené alebo blokované URL adresy a podrobnosti o tom, ako sú kategorizované. V stĺpci Vykonaná akcia sú podrobnejšie informácie o pravidle, ktoré bolo použité.
- **Správa zariadení** – záznamy o vymeniteľných médiách alebo zariadeniach, ktoré boli pripojené k počítaču. Do protokolu sú zaznamenávané len zariadenia s vytvoreným pravidlom. Ak sa na pripojené zariadenie nevzťahuje žiadne pravidlo, záznam v protokole sa pre zariadenie nevytvorí. Môžete tu tiež vidieť podrobnosti o zariadeniach, ako napríklad typ zariadenia, sériové číslo, názov výrobcu a veľkosť pamäte média (ak je dostupná).



Označte obsah akéhokoľvek protokolu a stlačením klávesovej kombinácie `Ctrl + C` **ho skopírujte do schránky**. Podržaním klávesov `Ctrl + Shift` označíte viaceré položky.

Kliknutím na **Filtrovanie** otvoríte okno Filtrovanie protokolov, kde môžete nastaviť podmienky filtrovania zoznamu protokolov.

Kliknite pravým tlačidlom na konkrétny záznam pre otvorenie kontextového menu. V kontextovom menu sú dostupné nasledujúce možnosti:

- **Zobraziť** – zobrazia sa podrobnejšie informácie o označenom protokole v novom okne.
- **Filtrovať rovnaké záznamy** – po aktivácii tohto filtra sa zobrazia protokoly rovnakého typu (diagnostické, varovania atď.).
- **Filtrovať** – po kliknutí na túto možnosť môžete v okne Filtrovanie protokolov definovať kritériá filtrovania pre konkrétne položky protokolu.
- **Zapnúť filter** – zapne filter, ktorý ste nastavili v okne Filtrovanie protokolov.
- **Zrušiť filter** – vypne aktivovaný filter.
- **Kopírovať/Kopírovať všetky** – kopíruje len označené alebo všetky protokoly z okna.
- **Odstrániť/Odstrániť všetko** – odstráni označené alebo všetky protokoly z okna – na vykonanie tejto akcie sú potrebné práva správcu.
- **Exportovať** – exportuje informácie o protokoloch vo formáte XML.
- **Exportovať všetko** – exportuje informácie o všetkých protokoloch vo formáte XML.
- **Hľadať/Hľadať ďalší/Hľadať predošlý** – po kliknutí na túto možnosť môžete v okne Filtrovanie protokolov definovať kritériá filtrovania pre konkrétne položky protokolu.
- **Vytvoriť vylúčenie** – umožňuje vytvoriť nové vylúčenie detekcie pomocou sprievodcu (táto možnosť nie je dostupná pre detekcie malvéru).

Filtrovanie protokolov

Na definovanie kritérií filtrovania kliknite na **Filtrovanie** v sekcii **Nástroje** > **Protokoly**.

Funkcia filtrovania protokolov vám pomôže nájsť informácie, ktoré hľadáte, a to najmä v prípade, ak sa v protokoloch nachádza veľký počet záznamov. Umožňuje vám zúžiť záznamy protokolov napríklad vtedy, keď hľadáte konkrétny typ udalosti, stav alebo časové obdobie. Záznamy protokolov môžete filtrovať použitím konkrétnych možností vyhľadávania. V okne Protokoly sa následne zobrazia len tie záznamy, ktoré zodpovedajú zadaným kritériám vyhľadávania.

Do poľa **Hľadať text** zadajte kľúčové slovo, ktoré chcete vyhľadať. Pre upresnenie vyhľadávania použite roletové menu **Hľadať v stĺpcoch**. V roletovom menu **Typy záznamov** vyberte jeden alebo viacero záznamov. Upresnite **Časové obdobie**, pre ktoré chcete zobraziť výsledky. Môžete použiť aj ďalšie možnosti vyhľadávania, ako napr. **Hľadať iba celé slová** alebo **Rozlišovať veľké a malé písmená**.

Hľadať text

Zadajte reťazec (slovo alebo časť slova). Zobrazia sa iba záznamy, ktoré obsahujú tento reťazec. Ostatné záznamy budú vynechané.

Hľadať v stĺpcoch

Vyberte stĺpce, ktoré budú pri vyhľadávaní brané do úvahy. Môžete označiť jeden alebo viacero stĺpcov.

Typy záznamov

Z roletového menu vyberte jeden alebo viacero typov záznamov:

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informačné** – zaznamenávané budú informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Varovania** – zaznamenávané budú varovné správy a kritické chyby.
- **Chyby** – zaznamenávané budú chyby typu „Chyba pri preberaní súboru“ a kritické chyby.
- **Kritické** – zaznamenávané budú len kritické chyby (nespustenie antivírusovej ochrany).

Časové obdobie

Zadajte časové obdobie, pre ktoré chcete zobraziť výsledky:

- **Nešpecifikované** (predvolené) – vyhľadávanie nebude vykonané pre konkrétne časové obdobie, ale bude prehľadaný celý protokol.
- **Posledný deň**
- **Posledný týždeň**
- **Posledný mesiac**
- **Vlastné** – môžete nastaviť konkrétne časové obdobie (od – do), v ktorom chcete filtrovať záznamy.

Hľadať iba celé slová

Túto možnosť použite v prípade, ak si želáte vyhľadávať celé slová a zobraziť tak presnejšie výsledky.

Rozlišovať veľké a malé písmená

Túto možnosť **použite** v prípade, ak je pri filtrovaní dôležité rozlišovať veľké a malé písmená. Po nastavení filtrovania/vyhľadávania kliknite na **OK** pre zobrazenie filtrovaných záznamov protokolu, prípadne kliknite na Hľadať pre spustenie vyhľadávania. Protokoly sú prehľadávané zhora nadol, počnúc vašou aktuálnou pozíciou (záznam, ktorý je zvýraznený). Vyhľadávanie sa zastaví pri nájdení prvého zodpovedajúceho záznamu. Stlačením **F3** vyhľadáte ďalší záznam, prípadne kliknite pravým tlačidlom myši a vyberte možnosť **Hľadať** pre upresnenie vyhľadávania.

Konfigurácia zápisu do protokolov

Nastavenie možností zapisovania protokolov produktu ESET Endpoint Security je dostupné cez hlavné okno programu. Kliknite na **Nastavenia** > **Rozšírené nastavenia** > **Nástroje** > **Protokoly**. Nastavenia protokolov umožňujú špecifikovať spôsoby manažovania protokolov. Manažment protokolov automaticky vymazáva staré protokoly, čím sa šetrí miesto na disku. Je možné definovať tieto vlastnosti protokolov:

Ukladať záznamy od úrovne – úroveň, od ktorej sa budú zaznamenávať udalosti do protokolov.

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informatívne** – zaznamenávané budú informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Upozornenia** – zaznamenávané budú varovné správy a kritické chyby.
- **Chyby** – zaznamenávané budú chyby typu „Chyba pri preberaní súboru“ a kritické chyby.
- **Kritické** – zaznamenávané budú len kritické chyby (chyba pri spustení antivírusovej ochrany, firewallu atď.).

Ak vyberiete **diagnostickú** úroveň podrobnosti protokolov, všetky blokované pripojenia budú zaznamenávané.

Protokoly staršie ako nastavená hodnota v poli **Automaticky mazať záznamy protokolov staršie ako (dní)** budú automaticky zmazané.

Automaticky optimalizovať protokoly – umožňuje automatickú defragmentáciu protokolov, ak počet nevyužitých záznamov prekročí špecifikovaný pomer v percentách nastavený v poli **Ak počet nepoužívaných záznamov prekročí (%)**.

Kliknite na **Optimalizovať** teraz pre spustenie defragmentácie protokolov. Defragmentácia odstraňuje prázdne záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi. Viditeľné zlepšenie práce s protokolmi po optimalizácii je očividné hlavne pri väčších množstvách záznamov v protokoloch.

Funkcia **Zapnúť textový protokol** umožňuje okrem klasického ukladania v sekcii Protokoly ukladať súbory protokolov aj v ďalšom formáte:

- **Cieľový priečinok** – vyberte priečinok, do ktorého budú ukladané protokoly (platí len pre text/CSV). Môžete skopírovať cestu alebo označiť iný priečinok kliknutím na možnosť **Vyčistiť**. Každá skupina protokolov má vlastný súbor s predvoleným názvom (napríklad, *virlog.txt* sú protokoly skupiny **Zachytené infiltrácie**).
- **Typ** – ak zvolíte formát **Text**, protokoly sa budú ukladať do textového súboru, pričom údaje budú oddelené tabulátorom. To isté platí pre formát **CSV**, avšak v tomto prípade budú údaje oddelené čiarkami. Ak vyberiete možnosť **Udalosť**, protokoly budú ukladané v denníku udalostí systému Windows, ktorý si môžete prezrieť cez Zobrazovač denníka udalostí (Event Viewer) v Ovládacom paneli.

- **Odstrániť všetky protokoly** – vymaže všetky uložené protokoly označené v roletovom menu **Typ**. Zobrazí sa vám tiež oznámenie o úspešnom odstránení protokolov.

Zaznamenávať zmeny v konfigurácii do protokolu auditu – poskytuje informácie o každej zmene v konfigurácii. Viac sa dozviete v časti Protokoly auditu.

> Pre urýchlenie riešenia problémov môžete byť technickou podporou spoločnosti ESET vyzvaný na zaslanie protokolov z vášho počítača. Nástroj ESET Log Collector zjednodušuje zozbieranie potrebných protokolov. Viac informácií o nástroji ESET Log Collector nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Protokoly auditu

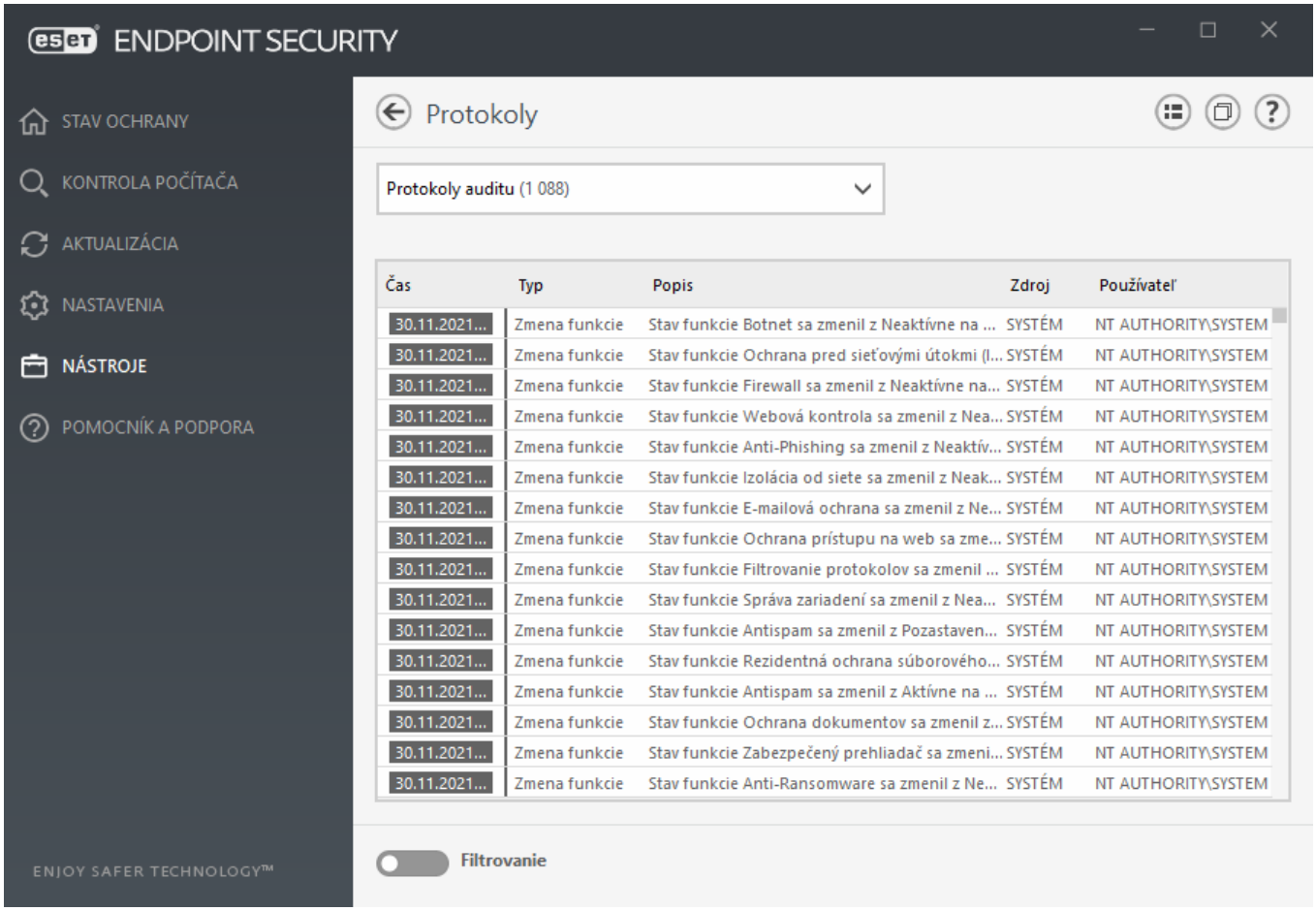
V podnikovom prostredí zvyčajne majú viacerí používatelia pridelené prístupové práva, ktoré im umožňujú konfigurovať koncové zariadenia. Keďže úpravy konfigurácie produktu môžu dramaticky ovplyvniť jeho fungovanie, je nevyhnutné, aby správcovia sledovali zmeny vykonané používateľmi a mohli tak rýchlo identifikovať, vyriešiť a tiež zabrániť rovnakým alebo podobným problémom v budúcnosti.

Protokoly auditu v rámci produktu ESET Endpoint Security vo verzii 7.1 prinášajú nový typ zapisovania do protokolu, pričom pomáhajú identifikovať príčiny problému. Sledujú zmeny v konfigurácii alebo stave ochrany a vytvárajú záznamy pre neskoršie použitie.

Ak chcete zobraziť **Protokol auditu**, v hlavnom menu kliknite na **Nástroje**, následne kliknite na **Protokoly** a z roletového menu vyberte **Protokoly auditu**.

Protokol auditu obsahuje nasledujúce informácie:

- Čas – kedy bola zmena vykonaná.
- Typ – aký typ nastavenia alebo funkcie sa zmenil.
- Popis – čo presne sa zmenilo, ktorá časť nastavenia bola upravená a počet zmenených nastavení.
- Zdroj – čo bolo zdrojom zmeny.
- Používateľ – kto zmenu spravil.



V okne Protokoly pravým tlačidlom myši kliknite medzi protokolmi auditu na ktorýkoľvek zo záznamov typu **Zmena nastavení** a z kontextovej ponuky vyberte možnosť **Zobraziť zmeny**, čím si zobrazíte podrobné informácie o vykonanej zmene. Zmenu nastavenia tiež môžete vrátiť späť kliknutím v kontextovej ponuke na možnosť **Obnoviť** (táto možnosť nie je dostupná, ako je produkt spravovaný cez ESET PROTECT). Ak z kontextovej ponuky vyberiete možnosť **Odstrániť všetko**, vytvorí sa protokol s informáciami o tejto akcii.

Ak máte v **Rozšírených nastaveniach** v sekcii **Nástroje** > **Protokoly** povolenú možnosť **Automaticky optimalizovať protokoly**, protokol auditu bude automaticky defragmentovaný ako iné protokoly.

Ak máte v **Rozšírených nastaveniach** v sekcii **Nástroje** > **Protokoly** povolenú možnosť **Automaticky odstraňovať záznamy protokolov staršie ako (dni)**, protokoly staršie ako nastavená hodnota v danom poli budú automaticky zmazané.

Plánovač

Plánovač zjednodušuje prácu s programovým balíkom automatizáciou často používaných operácií prostredníctvom vytvorenia plánovaných úloh.

Je prístupný z menu hlavného okna programu ESET Endpoint Security v sekcii **Nástroje** > **Plánovač**. **Plánovač** obsahuje prehľadný zoznam všetkých plánovaných úloh, ich nastavení a vlastností, ktoré sa vykonávajú v stanovený čas s použitím zadefinovaných profilov.

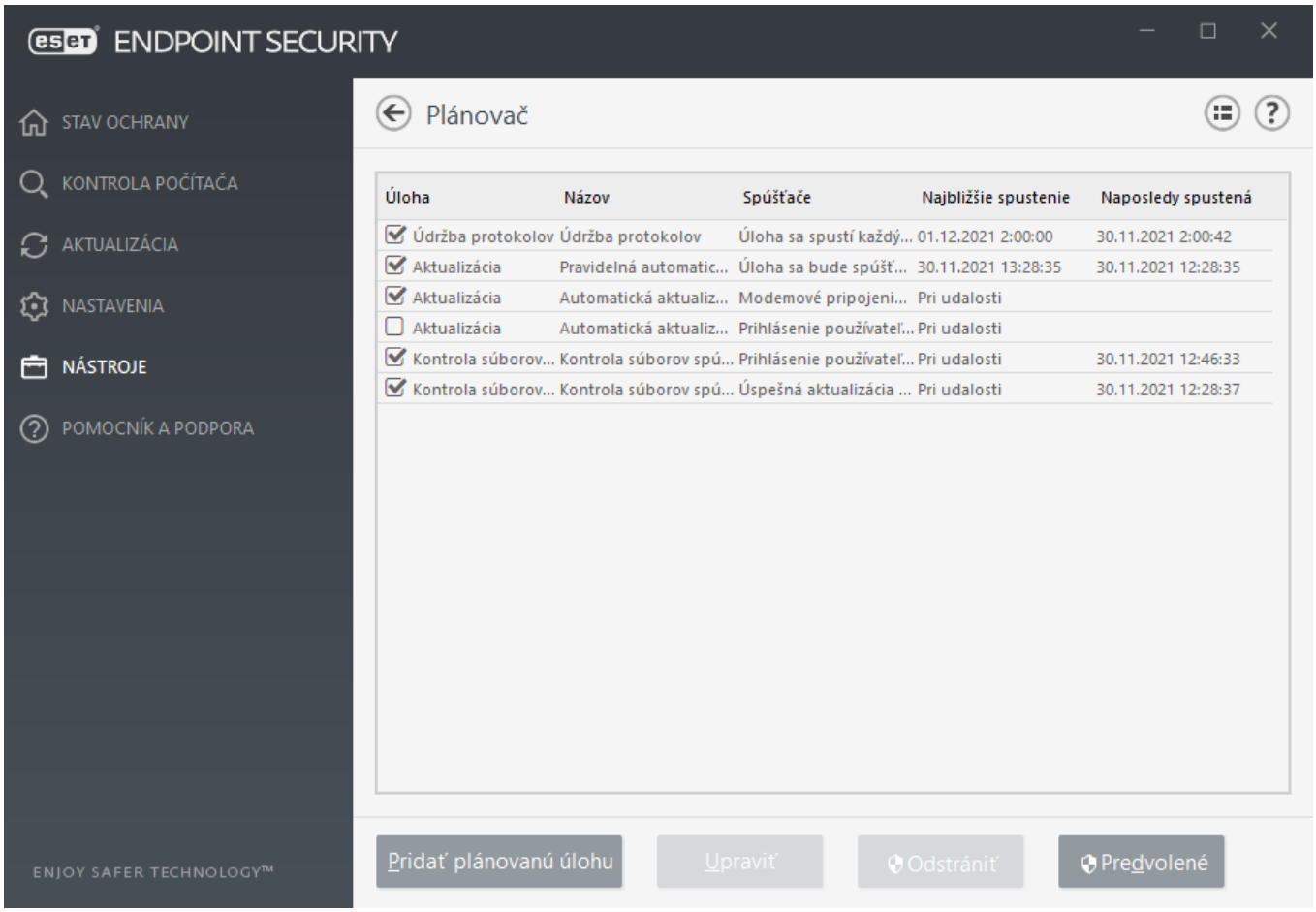
Slúži na plánovanie úloh, ako je napr. aktualizácia detekčného jadra, kontrola počítača, kontrola súborov spúšťaných pri štarte počítača či pravidelná údržba protokolov. Priamo z hlavného okna Plánovača môžete pridať alebo vymazať úlohu kliknutím na príslušné tlačidlo v dolnej časti okna (tlačidlá **Pridať plánovanú úlohu**

a **Odstrániť**). Kontextové menu, ktoré sa otvorí po kliknutí pravým tlačidlom myši v okne plánovača, umožňuje nasledovné akcie: zobrazenie detailných informácií o úlohe, okamžité vykonanie úlohy, pridanie novej úlohy, úpravu, resp. odstránenie už existujúcej úlohy. Zaškrtávacím políčkom pri úlohe je úlohu možné vypnúť/zapnúť.

V predvolenom nastavení **Plánovača** sú dostupné nasledujúce úlohy:

- **Údržba protokolov**
- **Pravidelná automatická aktualizácia**
- **Automatická aktualizácia po modemovom pripojení**
- **Automatická aktualizácia po prihlásení používateľa**
- **Kontrola súborov spúšťaných pri štarte počítača** (po prihlásení používateľa)
- **Kontrola súborov spúšťaných pri štarte počítača** (po úspešnej aktualizácii modulov programu)

Nastavenia existujúcich plánovaných úloh (a to tak preddefinovaných, ako aj vlastných) je možné meniť cez kontextové menu zvolením možnosti **Upraviť** alebo výberom príslušného riadku v zozname úloh a kliknutím na tlačidlo **Upraviť**.



Pridanie plánovanej úlohy

1. Kliknite na **Pridať plánovanú úlohu** v spodnej časti okna.
2. Zadajte názov úlohy.
3. Z roletového menu vyberte požadovanú úlohu:

- **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.
- **Údržba protokolov** – v protokoloch môžu zostávať stopy po vymazaných záznamoch. Táto úloha pravidelne optimalizuje záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi.

- **Kontrola súborov spúšťaných pri štarte počítača** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.
- **Vytvorenie záznamu o stave počítača** – vytvára záznam o stave počítača cez nástroj ESET SysInspector, ktorý slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.
- **Manuálna kontrola počítača** – vykoná kontrolu diskov, jednotlivých priečinkov a súborov na počítači.
- **Aktualizácia** – zabezpečuje aktualizáciu detekčného jadra a programových modulov.

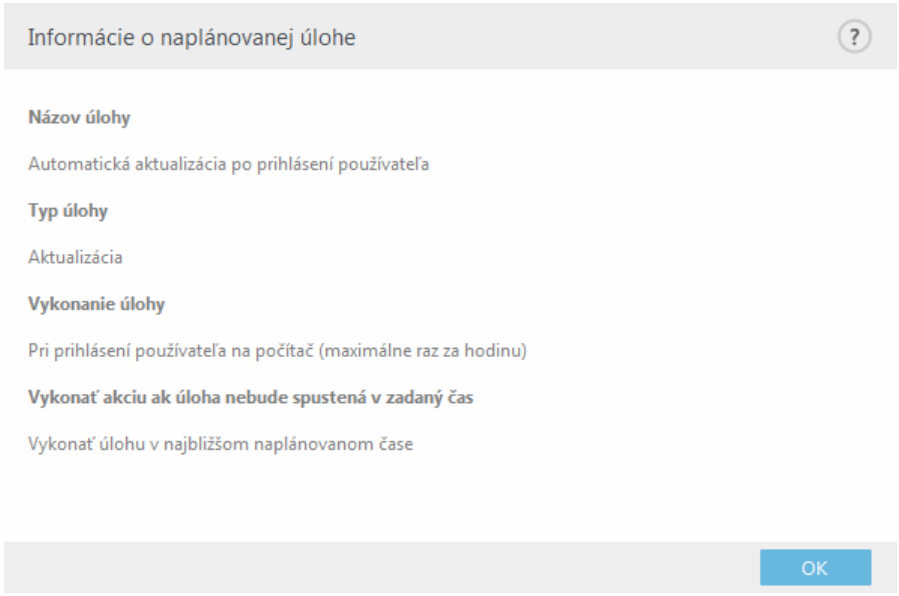
4. Na zapnutie úlohy potvrďte možnosť **Zapnuté** (môžete tak urobiť aj neskôr začiarknutím políčka v zozname naplánovaných úloh), kliknite na **Ďalej** a nastavte načasovanie úlohy:

- **Raz** – úloha sa vykoná iba raz v presne určený deň a čas.
- **Opakovane** – úloha bude vykonávaná opakovane v určenom časovom intervale.
- **Denne** – úloha bude vykonávaná opakovane každý deň v určenom čase.
- **Týždenne** – úloha sa bude vykonávať týždenne vo zvolené dni a v určený čas.
- **Pri udalosti** – úloha sa bude vykonávať pri určitej udalosti.

5. **Možnosť Nespúšťať úlohu, ak je počítač napájaný z batérie** je dobré použiť, ak prenosný počítač nie je zapojený do elektrickej siete a chcete v tomto čase minimalizovať jeho systémové prostriedky. Zadajte čas/dátum alebo interval, v ktorom bude úloha vykonaná, do poľa **Vykonanie úlohy**. V prípade, že sa naplánovanú úlohu nepodarí vykonať v určenom čase, môžete nastaviť, kedy sa má opätovne spustiť:

- **V najbližšom naplánovanom čase**
- **Hneď ako to bude možné**
- **Okamžite, ak od posledného naplánovaného spustenia uplynul stanovený časový interval v hodinách** (pričom interval je možné definovať priamo pri potvrdení tejto voľby v poli **Čas od posledného spustenia**)

Pre zobrazenie prehľadu nastavení úlohy kliknite pravým tlačidlom na myši a z menu vyberte možnosť **Zobraziť informácie**.



ESET SysInspector

ESET SysInspector je aplikácia slúžiaca na dôkladné preskúmanie stavu vášho počítača, ktorá je schopná zhromažďovať údaje o nainštalovaných ovládačoch a programoch, sieťových pripojeniach či dôležitých položkách databázy Registry a zobraziť úroveň rizika jednotlivých komponentov systému v jednoduchej čitateľnej forme.

Tieto informácie vám môžu pomôcť zistiť príčiny podozrivého správania systému, či už vplyvom nekompatibility alebo infekcie škodlivým kódom. Prečítajte si aj online používateľskú príručku pre ESET SysInspector.

V okne SysInspector sa nachádzajú nasledujúce informácie o vytvorených protokoloch:

- **Čas** – čas vytvorenia.
- **Komentár** – stručný komentár.
- **Používateľ** – meno používateľa, ktorý vytvoril protokol.
- **Stav** – stav vytvorenia.

Sú dostupné tieto akcie:

- **Zobraziť** – otvorí vytvorený protokol. Môžete tiež kliknúť pravým tlačidlom na konkrétny protokol a z kontextového menu vybrať možnosť **Zobraziť**.
- **Vytvoriť** – vytvorí nový protokol. Vždy počkajte na dokončenie protokolu nástroja ESET SysInspector (stav protokolu bude označený ako **Vytvorený**).
- **Odstrániť** – odstráni označený protokol zo zoznamu.

Nasledujúce položky budú dostupné z kontextového menu, ak je označený jeden alebo viacero protokolov:

- **Zobraziť** – otvorí zvolený protokol v nástroji ESET SysInspector (rovnako ako pri dvojitom kliknutí na protokol).
- **Vytvoriť** – vytvorí nový protokol. Vždy počkajte na dokončenie protokolu nástroja ESET SysInspector (stav protokolu bude označený ako **Vytvorený**).
- **Odstrániť** – Odstráni vybraný protokol.
- **Odstrániť všetko** – vymaže všetky protokoly.
- **Exportovať** – uloží protokol do súboru .xml alebo do skomprimovaného súboru .zip.

Ochrana s podporou cloudu

ESET LiveGrid® (založený na pokročilom systéme včasného varovania ThreatSense.Net) pracuje s dátami získanými od používateľov bezpečnostných produktov ESET z celého sveta a tieto dáta zasiela do výskumného laboratória spoločnosti ESET. Vďaka prijatým vzorkám podozrivého softvéru a príslušným metadátam nám ESET LiveGrid® umožňuje okamžite reagovať na najnovšie hrozby, ako aj na požiadavky našich zákazníkov.

K dispozícii sú tri možnosti:

1. možnosť: Zapnite reputačný systém ESET LiveGrid®

Reputačný systém ESET LiveGrid® poskytuje možnosť cloudového whitelistingu a blacklistingu.

Reputáciu súborov a spustených procesov môžete skontrolovať priamo z používateľského prostredia programu alebo z kontextového menu, cez ktoré je možné získať podrobnejšie informácie zo systému ESET LiveGrid®.

2. možnosť: Zapnite systém spätnej väzby ESET LiveGrid®

Na rozdiel od reputačného systému ESET LiveGrid®, systém spätnej väzby ESET LiveGrid® zozbiera z vášho počítača len tie informácie, ktoré sa týkajú novej hrozby. Môže ísť o vzorku alebo kópiu súboru, v ktorom sa infiltrácia objavila, cestu k danému súboru, názov súboru, informáciu o dátume a čase detekcie, spôsob, akým sa

hrozba dostala do vášho počítača, a informáciu o operačnom systéme.

Na základe predvolených nastavení ESET Endpoint Security odosiela podozrivé vzorky na analýzu do výskumného laboratória spoločnosti ESET. Súbory s niektorými príponami, napríklad *.doc* alebo *.xls*, sa nikdy neodosielajú. Medzi výnimky môžete doplniť aj ďalšie prípony súborov, pri ktorých sa špeciálne chcete vyhnúť možnosti odoslania.

3. možnosť: Nezapínajte ESET LiveGrid®

Neprídete tým o žiadnu funkcionalitu programu, avšak pri zapnutom systéme ESET LiveGrid® dokáže ESET Endpoint Security v niektorých prípadoch na nové hrozby reagovať skôr, ako dôjde k aktualizácii detekčného jadra.

> Viac o technológii ESET LiveGrid® sa dočítate v slovníku pojmov.
> Prečítajte si naše ilustrované inštrukcie (dostupné v angličtine a niekoľkých ďalších jazykoch) týkajúce sa zapnutia a vypnutia funkcie ESET LiveGrid® v ESET Endpoint Security.

Nastavenia ochrany s podporou cloudu v Rozšírených nastaveniach

Ak chcete prejsť na nastavenia systému ESET LiveGrid®, stlačte **F5**, čím otvoríte okno Rozšírených nastavení, a rozbaľte sekciu **Detekčné jadro** > **Ochrana s podporou cloudu**.

Zapnúť reputačný systém ESET LiveGrid® (odporúčané) – reputačný systém ESET LiveGrid® zvyšuje efektivitu antimalvérových riešení spoločnosti ESET pomocou porovnávania kontrolovaných súborov s cloudovou databázou dôveryhodných a blokovaných súborov.

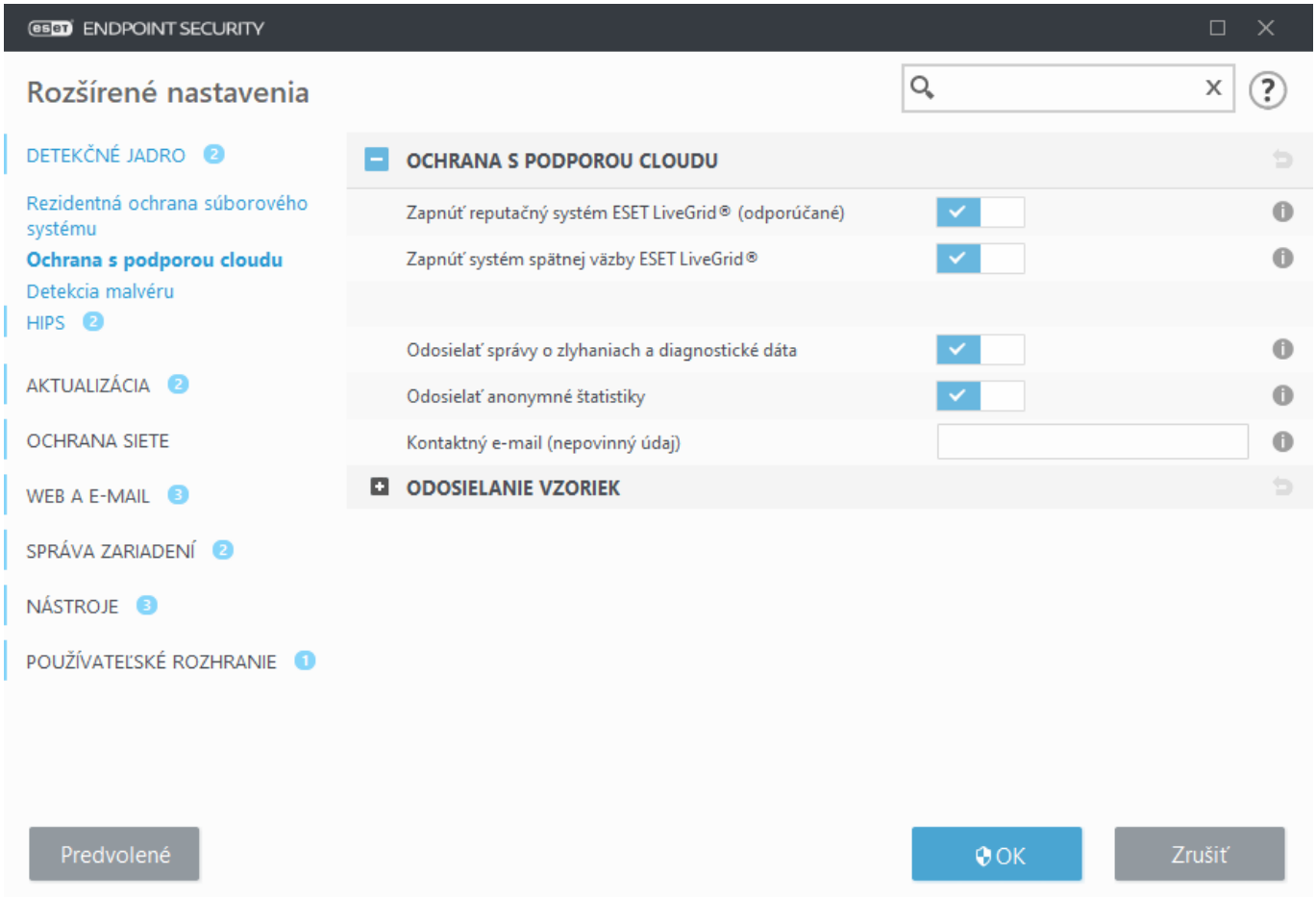
Zapnúť systém spätnej väzby ESET LiveGrid® – odosiela do výskumného laboratória spoločnosti ESET na ďalšiu analýzu relevantné údaje o vzorkách (popísané nižšie v sekcii **Odosielanie vzoriek**) spolu so správami o zlyhaní a štatistikami.

Zapnúť ESET LiveGuard (nie je viditeľné v programe ESET Endpoint Security) – ESET LiveGuard je platenou službou spoločnosti ESET. Predstavuje dodatočnú vrstvu ochrany osobitne navrhnutú na zmiernenie účinkov nových, dosiaľ neznámych druhov hrozieb. Podozrivé súbory sú automaticky odoslané do cloudu ESET. Tam sú analyzované našimi pokročilými nástrojmi na detekciu malvéru. Používateľ, ktorý vzorku poskytol, dostane správu o správaní pozorovanej vzorky.

Odosielať správy o zlyhaniach a diagnostické dáta – do spoločnosti ESET sa budú odosielať diagnostické dáta súvisiace so systémom ESET LiveGrid®, ako sú správy o zlyhaniach a výpisy pamäte modulov. Pomôže nám to diagnostikovať problémy, ako aj zlepšovať naše produkty a ochranu koncových používateľov.

Odosielať anonymné štatistiky – povoľte spoločnosti ESET zbierať informácie o novonájdených hrozbách, ako ich názov, čas detekcie, spôsob detekcie a súvisiace metadáta, verziu a nastavenie produktu a informácie o vašom systéme.

Kontaktný e⍰mail (nepovinný údaj) – zadaný kontaktný e⍰mail bude môcť byť odoslaný spoločne s podozrivým súborom a môže byť použitý na vyžiadanie ďalších informácií. Spoločnosť ESET vás bude prostredníctvom e-mailu kontaktovať len vtedy, keď bude potrebné získať ďalšie informácie.



Odosielanie vzoriek

Manuálne odosielanie vzoriek – aktivuje možnosť manuálne odosielať vzorky na analýzu do spoločnosti ESET priamo z kontextového menu, karantény alebo sekcie Nástroje > Odoslanie vzorky na analýzu.

Automatické odosielanie zachytených vzoriek

Vyberte, ktoré typy vzoriek budú zasielané spoločnosti ESET na analýzu s cieľom zlepšiť detekciu v budúcnosti. K dispozícii sú nasledujúce možnosti:

- **Všetky zachytené vzorky** – všetky objekty zachytené detekčným jadrom (vrátane potenciálne nechcených aplikácií, ak je to povolené v nastaveniach kontroly).
- **Všetky vzorky okrem dokumentov** – všetky zachytené objekty okrem **dokumentov** (pozri nižšie).
- **Neposielať** – zachytené objekty sa nebudú odosielať spoločnosti ESET.

Automatické odosielanie podozrivých vzoriek

Tieto vzorky sa budú do spoločnosti ESET zasielať aj v prípade, že ich detekčné jadro nezachytilo. Ide napríklad o vzorky, ktoré tesne unikli detekcii alebo ktoré niektorý z modulov ochrany ESET Endpoint Security považuje za podozrivé, prípadne o vzorky s nejasným správaním.

- **Spustiteľné súbory** – zahŕňa typy súborov ako .exe, .dll, .sys.
- **Archívy** – zahŕňa typy súborov ako .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skripty** – zahŕňa typy súborov ako .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Iné** – zahŕňa typy súborov ako .jar, .reg, .msi, .sfw, .lnk.
- **Potenciálne spamové e□maily** – táto voľba umožní odosielanie častí alebo celých potenciálnych

spamových e-mailov s prílohami do spoločnosti ESET na ďalšiu analýzu. Povolenie tejto možnosti nám umožňuje zlepšovať globálnu detekciu spamu a zároveň vám osobne prinášať lepšiu detekciu spamu v budúcnosti.

- **Dokumenty** – zahŕňa dokumenty Microsoft Office alebo PDF s aktívnym obsahom aj bez neho.
  Rozbaliť zoznam všetkých zahrnutých typov súborov

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

Vylúčenia

Pomocou filtra vylúčení môžete z odosielania vylúčiť určité súbory/adresáre (toto môže byť užitočné pri súboroch obsahujúcich dôverné či citlivé informácie, ako sú dokumenty alebo tabuľky). Súbory pridané do vylúčení nebudú nikdy odoslané na analýzu do laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód. Najbežnejšie typy súborov sú predvolene vylúčené (napr. súbory s príponou .doc). Do zoznamu vylúčení môžete pridávať ľubovoľné typy súborov.

Ak chcete vylúčiť súbory stiahnuté z download.domain.com, prejdite na **Rozšírené nastavenia** > **Ochrana s podporou cloudu** > **Odosielanie vzoriek** > **Vylúčenia** a pridajte vylúčenie *download.domain.com*.

ESET LiveGuard

Ak chcete zistiť, ako aktivovať službu ESET LiveGuard na klientskom počítači cez ESET PROTECT Web Console, prečítajte si článok Konfigurácia služby ESET LiveGuard pre ESET Endpoint Security.

Ak ste mali zapnutý ESET LiveGrid® a neskôr ste ho vypli, môže sa stať, že v počítači sú už pripravené dátové balíky na odoslanie. Tieto balíky budú odoslané spoločnosti ESET aj po vypnutí systému. Po odoslaní všetkých aktuálnych informácií sa už ďalšie balíky nevytvoria.

Filter vylúčení pre ochranu s podporou cloudu

Filter vylúčení umožňuje nastaviť súbory a priečinky, ktoré nemajú byť odosielané ako vzorky. Súbory pridané do vylúčení nebudú nikdy odoslané na analýzu do laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód. Bežné typy súborov (napríklad .doc) sú predvolene vylúčené.

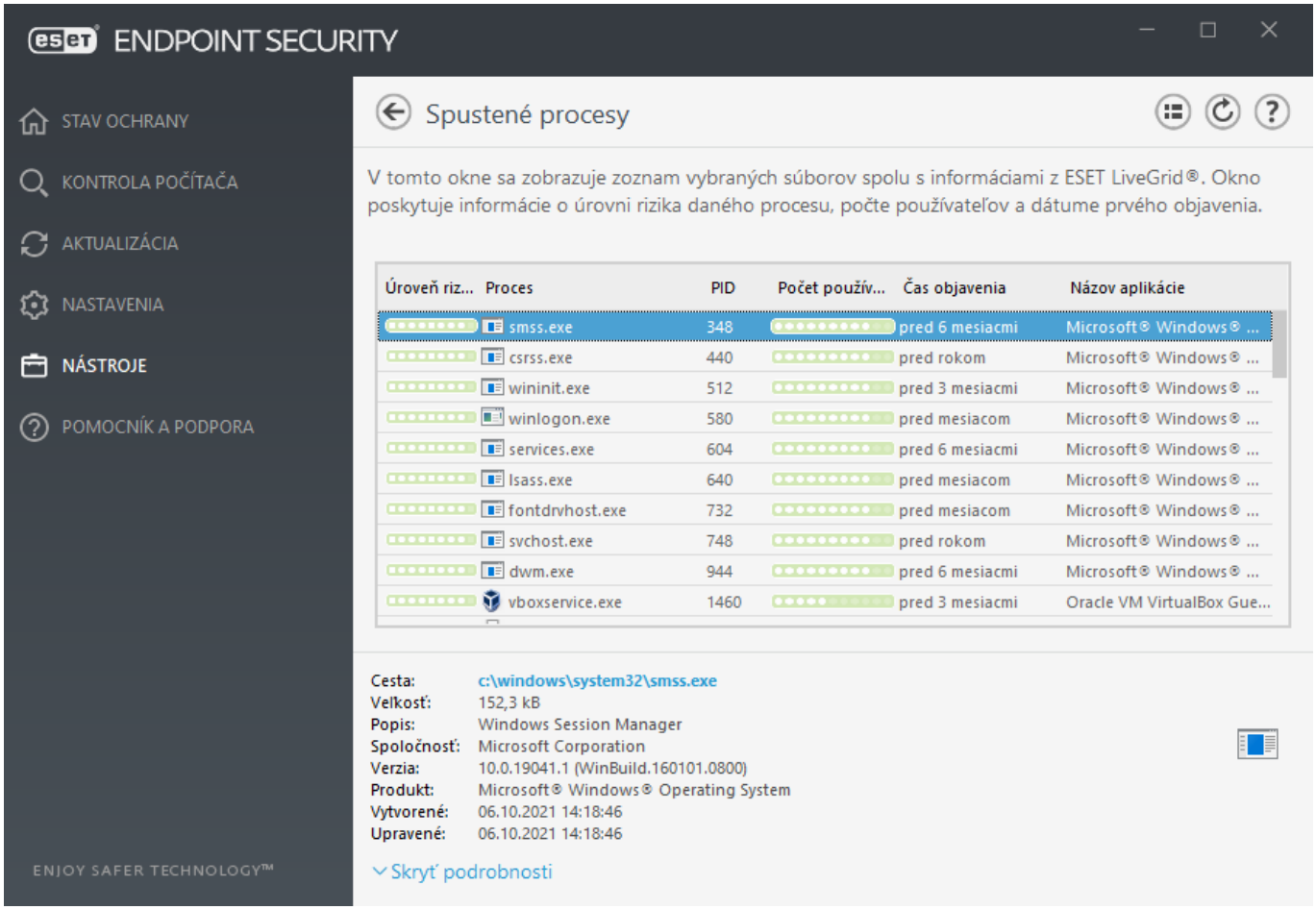
Táto funkcia je užitočná pri vylúčení súborov, v ktorých sa zvyčajne nachádzajú dôverné informácie, napríklad textové dokumenty a tabuľkové hárky.

Ak chcete vylúčiť súbory stiahnuté z download.domain.com, prejdite na **Rozšírené nastavenia** > **Ochrana s podporou cloudu** > **Odosielanie vzoriek** > **Vylúčenia** a pridajte vylúčenie *download.domain.com*.

Spustené procesy

Okno Spustené procesy zobrazuje programy a procesy, ktoré sú spustené vo vašom počítači. Umožňuje tiež, aby bola spoločnosť ESET pohotovo a neustále informovaná o nových infiltráciách. Pri povolenej technológii ESET

LiveGrid® ESET Endpoint Security poskytuje podrobné informácie o spustených procesoch s cieľom chrániť používateľov.



Úroveň rizika – vo väčšine prípadov ESET Endpoint Security pomocou technológie ESET LiveGrid® priradí objektom (súborom, procesom, kľúčom databázy Registry atď.) určitý stupeň rizika na základe heuristických pravidiel, ktoré preskúmajú každý objekt a vyhodnotia pravdepodobnosť nebezpečnej aktivity. Podľa výsledkov heuristiky sa objektom pridelí úroveň rizika od 9 – najlepšia reputácia (zelenou farbou) až po 0 – najhoršia reputácia (červenou farbou).

Proces – názov aplikácie alebo procesu, ktorý je momentálne spustený na počítači. Pre lepší prehľad o všetkých procesoch použite Správcu úloh (MS Windows). Správcu úloh môžete otvoriť kliknutím pravým tlačidlom myši kdekoľvek na systémovom paneli úloh a vybratím možnosti Spustiť správcu úloh, prípadne pomocou klávesovej skratky **Ctrl** + **Shift** + **Esc**.

PID – je identifikačné číslo procesu spusteného v operačnom systéme Windows.

Známe aplikácie označené zelenou farbou nepredstavujú riziko a sú bezpečné. Budú preto vyňaté z kontroly, čím sa zvyšuje rýchlosť kontroly počítača a rezidentnej ochrany súborového systému na vašom počítači.

Počet používateľov – počet používateľov, ktorí používajú danú aplikáciu. Táto informácia sa získava prostredníctvom technológie ESET LiveGrid®.

Čas objavenia – čas, ktorý ubehol od prvého zachytenia aplikácie technológiou ESET LiveGrid®.

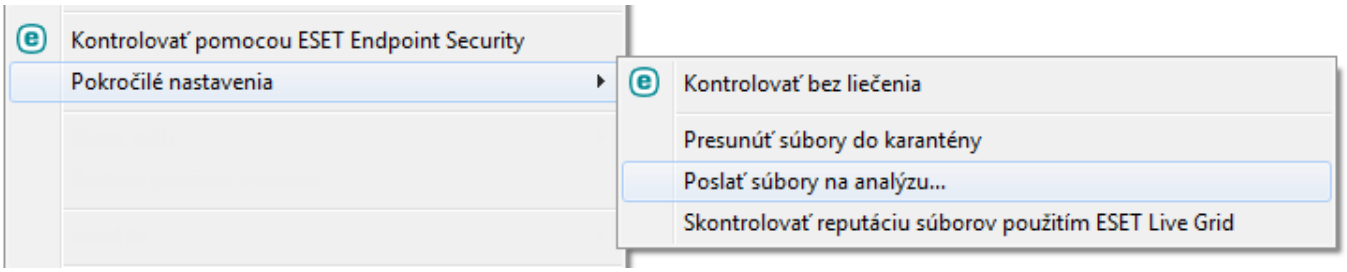
Aj v prípade, že je aplikácia označená ako Neznáma (oranžová), nemusí to znamenať, že obsahuje škodlivý kód. Obvykle je to nová aplikácia. Ak si nie je používateľ istý, či je tomu skutočne tak, má možnosť Odoslať súbor na analýzu do vírusového laboratória spoločnosti ESET. Ak sa ukáže, že ide o nebezpečnú aplikáciu, jej detekcia bude pridaná do niektorej z najbližších aktualizácií detekčného jadra.

Názov aplikácie – názov aplikácie alebo procesu.

Po kliknutí na jednotlivé aplikácie sa v dolnej časti okna zobrazia nasledujúce informácie:

- **Cesta** – umiestnenie aplikácie vo vašom počítači.
- **Veľkosť** – veľkosť v kB (kilobajtoch) alebo MB (megabajtoch).
- **Popis** – charakteristika súboru vychádzajúca z popisu daného súboru operačným systémom.
- **Spoločnosť** – názov vydavateľa aplikácie alebo procesu.
- **Verzia** – táto informácia pochádza od vydavateľa aplikácie alebo procesu.
- **Produkt** – názov aplikácie, zvyčajne obchodné meno.
- **Vytvorené** – dátum a čas, keď bola aplikácia vytvorená.
- **Upravené** – dátum a čas, kedy bola aplikácia naposledy upravená.

Reputácia môže byť použitá aj pri súboroch, ktoré sa nesprávajú ako spustené programy/procesy – označte súbor, ktorý chcete skontrolovať, kliknite naň pravým tlačidlom myši a z kontextového menu zvoľte možnosť **Pokročilé možnosti** > **Skontrolovať reputáciu súborov použitím ESET LiveGrid®**.



Správa o bezpečnosti

Táto funkcia vám poskytuje štatistické údaje o činnosti programu rozdelené do nasledujúcich kategórií:

Zablokovaných webových stránok – zobrazuje počet zablokovaných webových stránok (URL adresa na blackliste z dôvodu PUA, phishingu, hacknutého routera, IP alebo certifikátu).

Zachytených infikovaných e-mailových objektov – zobrazuje počet infikovaných e-mailových objektov, ktoré boli programom detegované.

Zablokovaných webových stránok vo webovej kontrole – zobrazuje počet stránok zablokovaných webovou kontrolou.

Zachytených potenciálne nechcených aplikácií – zobrazuje počet potenciálne nechcených aplikácií (PUA), ktoré boli programom detegované.

Zachytených spamových e-mailov – zobrazuje počet spamových e-mailov, ktoré boli programom detegované.

Skontrolovaných dokumentov – zobrazuje počet skontrolovaných dokumentov.

Skontrolovaných aplikácií – zobrazuje počet skontrolovaných spustiteľných objektov.

Skontrolovaných iných objektov – zobrazuje počet iných skontrolovaných objektov.

Skontrolovaných objektov webových stránok – zobrazuje počet skontrolovaných objektov webových stránok.

Skontrolovaných e-mailových objektov – zobrazuje počet skontrolovaných e-mailových objektov.

Poradie uvedených kategórií sa dynamicky mení, pričom na začiatku je vždy zobrazená kategória s najvyššou číselnou hodnotou a na konci s najnižšou. Kategórie s nulovými hodnotami sa nezobrazujú. Pre zobrazenie skrytých kategórií kliknite na možnosť **Zobraziť viac**.

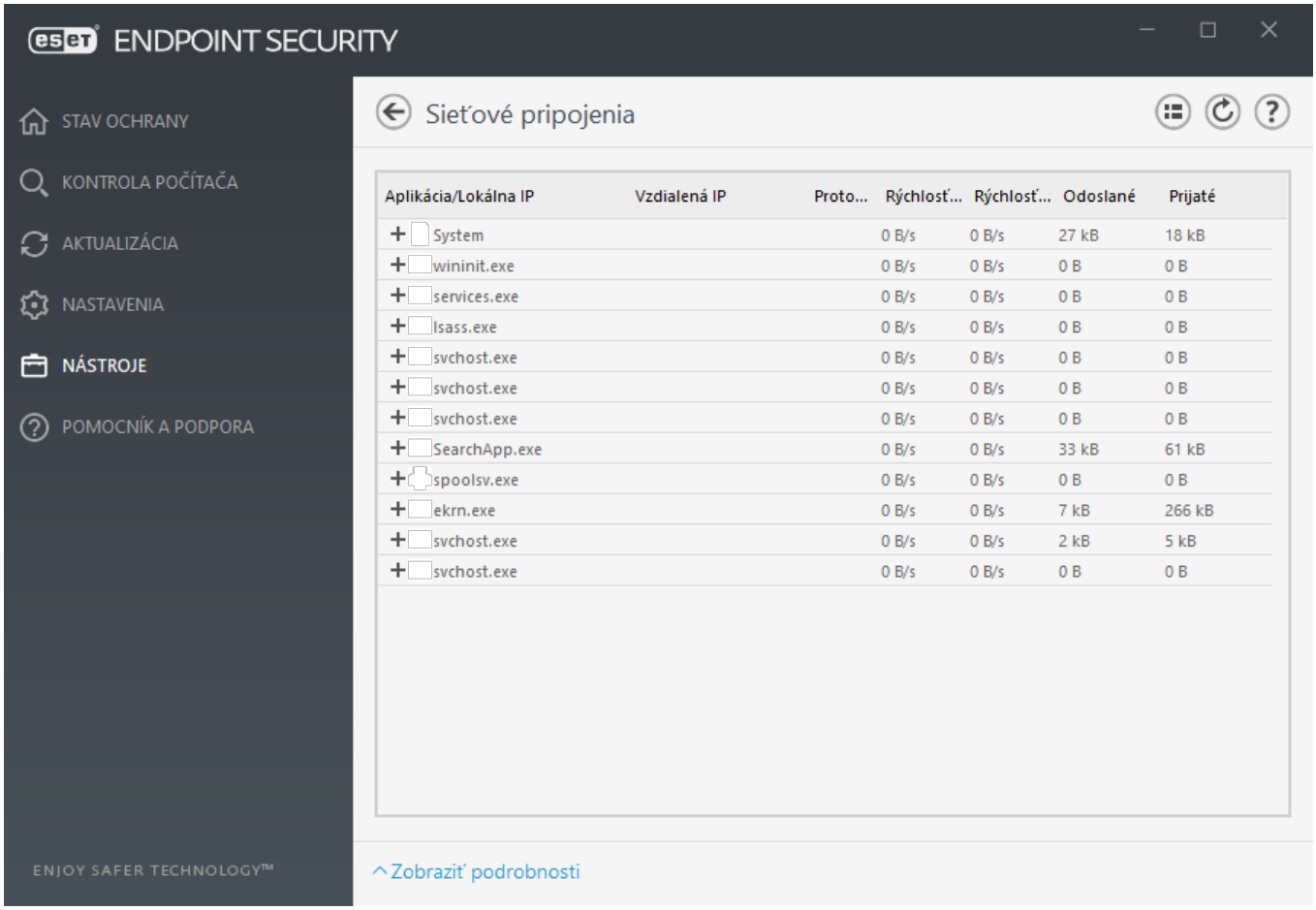
Kliknutím na ikonu ozubeného kolesa v pravom hornom rohu môžete **Zapnúť/Vypnúť oznámenia správy o bezpečnosti** a taktiež si zvoliť, či sa majú zobrazovať dáta za posledných 30 dní alebo od aktivácie produktu. Ak ste program ESET Endpoint Security nainštalovali pred menej ako 30 dňami, zvoliť bude možné len počet dní, ktoré uplynuli od inštalácie. Predvolenou nastavenou hodnotou je 30 dní.



Pomocou možnosti **Vynulovať dáta** odstránite všetky štatistiky a existujúce dáta zo Správy o bezpečnosti. Táto akcia si bude vyžadovať vaše potvrdenie v prípade, že ste predtým nezrušili označenie možnosti **Spýtať sa pred vynulovaním štatistiky** v **Rozšírených nastaveniach** v sekcii **Oznámenia** > **Interaktívne upozornenia** > **Potvrdzovacie správy**.

Sieťové pripojenia

V sekcii Sieťové pripojenia môžete vidieť zoznam aktívnych alebo čakajúcich spojení. Získate tak prehľad o aplikáciách, ktoré komunikujú so vzdialenou stranou.



Prvý riadok zobrazuje meno aplikácie a rýchlosť dátového prenosu. Pre zobrazenie zoznamu spojení pre danú aplikáciu (a viac podrobnejších informácií), kliknite na **+**.

Stĺpce

Aplikácia/Lokálna IP – názov aplikácie, lokálna IP adresa a komunikačný port.

Vzdialená IP – IP adresa a komunikačný port vzdialenej strany.

Protokol – komunikačný protokol.

Rýchlosť nahrávania/Rýchlosť sťahovania – zobrazuje rýchlosť prichádzajúcej/odchádzajúcej komunikácie.

Odoslané/Prijaté – objem dát, ktorý je prenesený v rámci spojenia.

Zobraziť podrobnosti – zobrazí podrobnosti o vybranom spojení.

Označte aplikáciu alebo IP adresu v zozname Sieťové pripojenia a kliknite pravým tlačidlom pre zobrazenie kontextového menu s nasledovnými možnosťami:

Prekladať IP adresy na mená – pokiaľ je to možné, sieťové adresy sú uvádzané v DNS forme a nie v číselnej podobe IP adresy.

Zobrazovať iba pripojenia TCP – v zozname sa zobrazia iba tie pripojenia, ktoré patria pod protokol TCP.

Zobrazovať počúvajúce pripojenia – zobrazia sa iba spojenia, pri ktorých neprebieha komunikácia, systém však má otvorený port a čaká na spojenie.

Zobrazovať pripojenia v rámci počítača – zobrazia sa iba pripojenia, ktoré majú ako vzdialenú stranu použitý lokálny systém. Týka sa to tzv. localhost pripojení.

Pravým tlačidlom myši kliknite na pripojenie a zobrazia sa vám doplňujúce možnosti:

Zablokovať komunikáciu pre dané pripojenie – zablokuje nadviazané spojenie. Táto možnosť je dostupná len pri aktívnych spojeniach.

Rýchlosť obnovovania – frekvencia, s akou sa budú obnovovať informácie o aktívnych pripojeniach.

Obnoviť teraz – obnovia sa informácie v okne Sieťové pripojenia.

Nasledujúce možnosti sú dostupné len po kliknutí na aplikáciu alebo proces, nie na aktívne spojenie:

Dočasne zablokovať komunikáciu pre daný proces – Zablokuje nadviazané spojenie pre danú aplikáciu/proces. V prípade vytvorenia nového spojenia firewall použije vopred definované pravidlo. Viac informácií nájdete v kapitole Nastaviť pravidlá a zóny.

Dočasne povoliť komunikáciu pre daný proces – povolí nadviazané spojenie pre danú aplikáciu. V prípade vytvorenia nového spojenia firewall použije vopred definované pravidlo. Viac informácií nájdete v kapitole Nastaviť pravidlá a zóny.

ESET SysRescue Live

ESET SysRescue Live je bezplatný nástroj, ktorý umožňuje vytvoriť spúšťací (tzv. bootovací) disk CD/DVD alebo USB. Spustenie infikovaného počítača z takto vytvoreného záchranného média vám poskytuje možnosť skontrolovať počítač na prítomnosť malvéru a liečiť infikované súbory.

Hlavnou výhodou ESET SysRescue Live je, že beží nezávisle od operačného systému počítača, pričom má priamy prístup k disku a celému súborovému systému. Toto umožňuje odstrániť hrozby, ktoré za normálnych prevádzkových podmienok nie je možné odstrániť (napríklad, ak je operačný systém spustený a pod.).

- Online pomocník pre ESET SysRescue Live

Odoslanie vzorky na analýzu

Ak vo svojom počítači nájdete súbor s podozrivým správaním alebo na internete narazíte na podozrivú stránku, môžete takéto vzorky poslať na analýzu do výskumného laboratória ESET (táto možnosť nemusí byť dostupná v závislosti od konfigurácie ESET LiveGrid®).

Vzorku pošlite do spoločnosti ESET na analýzu len v tom prípade, že spĺňa aspoň jednu z nasledujúcich podmienok:
• Vzorka nie je vaším produktom ESET vôbec detegovaná.
• Vzorka je nesprávne detegovaná ako hrozba.
• Súkromné súbory (ktoré by ste chceli nechať spoločnosťou ESET skontrolovať na prítomnosť malvéru) neprijímame ako vzorky (výskumné laboratórium spoločnosti ESET nevykonáva kontroly používateľských súborov na vyžiadanie).
• Pri zasielaní vzorky na analýzu uveďte výstižný predmet správy a poskytnite čo najviac informácií o vzorke (napr. snímka obrazovky alebo webová stránka, z ktorej ste podozrivý súbor stiahli).

Odoslať súbor alebo webovú stránku do spoločnosti ESET na analýzu môžete jedným z nasledujúcich spôsobov:

1. Pomocou dialógového okna určeného na odoslanie vzorky, ktoré nájdete v časti **Nástroje** > **Odoslanie vzorky na analýzu**.
2. Vzorku na analýzu môžete odoslať aj prostredníctvom e-mailu. V takom prípade súbor zabaľte do archívu pomocou WinRAR/ZIP, zabezpečte heslom „infected“ a následne ho odošlite na adresu samples@eset.com.
3. Ak chcete nahlásiť spam alebo, naopak, e-mail nesprávne zaradený medzi spam, prípadne nesprávne kategorizované webové stránky v module webovej kontroly, prečítajte si náš článok Databázy znalostí spoločnosti ESET.

Keď už máte otvorené okno **Vybrať vzorku na analýzu**, z roletového menu **Dôvod odoslania vzorky** vyberte popis, ktorý najlepšie zodpovedá podozreniu:

- **Podozrivý súbor**
- **Podozrivá stránka** **(stránka infikovaná malvérom)**
- **Nesprávne detegovaný súbor** (súbor, ktorý je detegovaný ako hrozba, no v skutočnosti infikovaný nie je)
- **Nesprávne detegovaná stránka**
- **Iné**

Súbor/Stránka – cesta k súboru alebo webovej stránke, ktorú chcete odoslať na analýzu.

Kontaktný e□mail – kontaktný e□mail bude odoslaný spolu s podozrivým súborom do spoločnosti ESET, aby v prípade potreby mohol byť použitý na vyžiadanie dodatočných informácií nevyhnutných k analýze. Zadanie kontaktného e□mailu nie je povinné. Ak svoju adresu zadať nechcete, označte možnosť **Odoslať anonymne**.

Odpoveď na vami zaslanú vzorku vám zo spoločnosti ESET príde len v tom prípade, že budú pracovníci výskumného laboratória pri analýze potrebovať viac informácií. Každý deň používatelia na naše servery odošlú tisícky súborov, preto nie je možné každému odpovedať.
Ak sa analýzou vzorky preukáže, že ide o nebezpečnú aplikáciu alebo webovú stránku, jej detekcia bude zahrnutá do najbližšej aktualizácie.

Vybrať vzorku na analýzu – Podozrivý súbor

Pozorované náznaky a symptómy infikovania malvérom – uveďte čo najpodrobnejší popis správania podozrivého súboru v systéme pre jeho presnejšiu analýzu.

Pôvod súboru (URL adresa alebo výrobca aplikácie) – uveďte zdroj, prostredníctvom ktorého ste sa k súboru dostali.

Poznámky a ďalšie doplňujúce informácie – do tohto poľa môžete zadať všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a analýze súboru.

Povinné je len pole **Pozorované náznaky a symptómy infikovania malvérom**, avšak poskytnutím doplňujúcich informácií výrazne pomôžete našim laboratóriám pri identifikácii a spracovaní vzoriek.

Vybrať vzorku na analýzu – Podozrivá stránka

Prosím, označte jednu z nasledujúcich možností z roletového menu **Aký je problém so stránkou?**:

- **Infikovaná stránka** – webová stránka, ktorá obsahuje alebo rôznymi spôsobmi rozširuje vírusy a iný malvér.
- **Phishingová stránka** – cieľom je získať citlivé údaje, ako napríklad heslá k bankovým účtom, PIN kódy a iné detaily. Viac o tomto type útoku sa môžete dočítať v slovníku pojmov.
- **Podvodná stránka** – podvodná webová stránka, ktorej cieľom je rýchly zisk pomocou zavádzania jej návštevníkov.
- Označte **Iné** ak stránka nespĺňa žiadnu z predošlých vlastností.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri analýze podozrivej webovej stránky.

Vybrať vzorku na analýzu – Nesprávne detegovaný súbor

Prosíme vás, aby ste nám posielali súbory, ktoré boli vyhodnotené ako infikované, ale v skutočnosti infikované nie sú. Pomôžete nám tým vylepšiť naše antivírusové a antispyvérové jadro a zvýšiť tak účinnosť ochrany pre ostatných používateľov. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétneho súboru zhoduje so vzorom obsiahnutým v detekčnom jadre.

Názov a verzia aplikácie – názov aplikácie a jej verzia (napr. číslo či alias).

Pôvod súboru (URL adresa alebo výrobca aplikácie) – uveďte pôvod súboru (zdroj) a popíšte, ako ste sa k danému súboru dostali.

Účel aplikácie – uveďte účel a typ aplikácie (napr. prehliadač, prehrávač médií atď.) pre rýchlejšie zaradenie a identifikáciu.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivého súboru.

Prvé tri parametre sú povinné z dôvodu lepšej identifikácie legitímnej aplikácie a jej odlíšenia od škodlivého kódu. Poskytnutím doplňujúcich informácií pomôžete významnou mierou našim laboratóriám pri identifikácii a spracovaní vzoriek.

Vybrať vzorku na analýzu – Nesprávne detegovaná stránka

Prosíme vás, aby ste nám posielali webové stránky, ktoré boli vyhodnotené ako infikované, podvodné či phishingové, avšak v skutočnosti neobsahujú žiaden škodlivý obsah. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétneho súboru zhoduje so vzorom obsiahnutým v

detekčnom jadre. Zaslaním nesprávne detegovanej stránky nám umožníte vylepšiť naše antivírusové a antiphishingové jadro a zvýšiť tak účinnosť ochrany pre ostatných používateľov.

Poznámky a dodatočné informácie – všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivej webovej stránky.

Vybrať vzorku na analýzu – Iné

Tento formulár sa používa v prípade, že súbor nie je možné kategorizovať ako **Podozrivý súbor** ani ako **Nesprávne detegovaný súbor**.

Dôvod odoslania súboru – Uveďte dôvod odoslania súboru a čo najpresnejší popis súboru

Karanténa

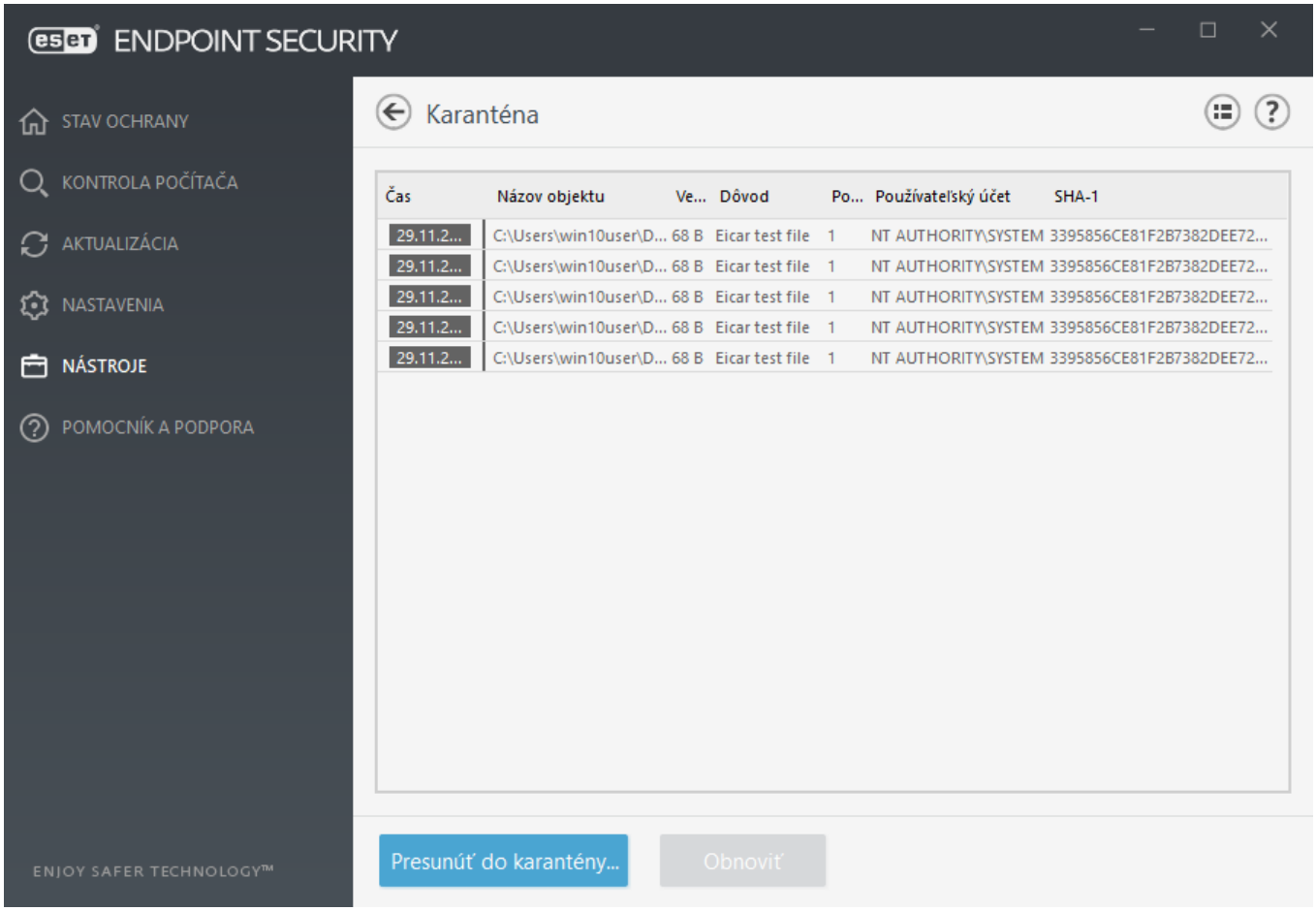
Hlavnou funkciou karantény je bezpečné uloženie detegovaných objektov (napríklad malvéru, infikovaných súborov alebo potenciálne nechcených aplikácií).

Karanténa je prístupná z hlavného okna programu ESET Endpoint Security po kliknutí na **Nástroje** > **Karanténa**.

Súbory uložené v karanténe si môžete prezrieť v prehľadnej tabuľke, ktorá obsahuje tieto informácie:

- dátum a čas presunutia súboru do karantény,
- cesta k pôvodnému umiestneniu súboru,
- veľkosť súboru v bytoch,
- dôvod (napr. objekt pridaný používateľom),
- počet detekcií (napr. opakovaná detekcia toho istého súboru alebo archív obsahujúci viacero infiltrácií).

- Vzdialene spravujem karanténu na klientskych pracovných staniciach



Presunutie súborov do karantény

ESET Endpoint Security automaticky presunie odstránené súbory do karantény (ak ste túto možnosť nedeaktivovali v okne s upozornením).

Ďalšie súbory by mali byť presunuté do karantény, ak:

a. ich nie je možné vyliečiť,
b. nie je bezpečné alebo vhodné ich odstrániť,
c. sú nesprávne detegované programom ESET Endpoint Security,
d. sa správajú podozrivo, ale nie sú detegované antivírusovým skenerom.

Súbory môžete presunúť do karantény viacerými spôsobmi:

a. manuálne presuniete súbor do karantény tak, že naň kliknete a podržíte tlačidlo myši stlačené, potom presuniete kurzor myši do vyznačeného priestoru a uvoľníte prst. Aplikácia sa následne presunie do popredia.
b. V hlavnom okne programu kliknite na **Presunúť do karantény**.
c. Na tento účel môžete použiť aj kontextové menu. V okne **Karanténa** kliknite pravým tlačidlom myši a z kontextového menu vyberte **Presunúť do karantény**.

Obnovenie súborov z karantény

Súbory presunuté do karantény možno obnoviť do ich pôvodného umiestnenia:

- Na tento účel použite funkciu **Obnoviť**, ktorá je k dispozícii v kontextovom menu po kliknutí pravým

tlačidlom myši na daný súbor v karanténe.

- Ak je súbor označený ako potenciálne nechcená aplikácia, možnosť **Obnoviť a vylúčiť z kontroly** bude zapnutá. Prečítajte si tiež kapitolu Vylúčenia.
- Kontextové menu ponúka aj možnosť **Obnoviť do**, ktorá vám umožňuje obnoviť súbor do iného umiestnenia, než bolo to pôvodné, z ktorého bol súbor vymazaný.
- Funkcia obnovenia súborov nie je v niektorých prípadoch k dispozícii, napr. pri súboroch na zdieľanom mieste v sieti určených len na čítanie.

Odstránenie súborov z karantény

Kliknite pravým tlačidlom na danú položku a vyberte možnosť **Odstrániť z karantény** alebo vyberte položku, ktorú chcete odstrániť, a stlačte kláves **Delete**. Môžete označiť a vymazať viac položiek naraz. Odstránené položky budú natrvalo vymazané z vášho zariadenia a z karantény.

Posielanie súboru z karantény na analýzu

Ak máte v karanténe uložený podozrivý súbor, ktorý program nedetegoval alebo ho detegoval nesprávne (napr. prostredníctvom heuristickej analýzy kódu) a následne presunul do karantény, pošlite jeho vzorku na analýzu do výskumného laboratória ESET. Súbor odošlete tak, že naň kliknete pravým tlačidlom a z kontextového menu vyberiete **Poslať na analýzu**.

Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:

- Spravovanie karantény v konzole ESET PROTECT
- Môj produkt ESET ma upozornil na detekciu. Čo mám robiť?

Nastavenie proxy servera

V prostredí, kde sa používa rozsiahlejšia lokálna sieť, môže byť pripojenie na internet zabezpečované pomocou tzv. proxy servera. V takomto prípade musia byť nastavenia proxy servera správne špecifikované. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií. Nastavenie proxy servera je možné vESET Endpoint Security definovať na dvoch odlišných miestach v rámci štruktúry Rozšírených nastavení.

Prvým miestom, kde nájdete nastavenia proxy servera, je okno **Rozšírených nastavení** > sekcia **Nástroje** > **Proxy server**. Proxy server zadaný v tejto sekcii bude použitý programom ESET Endpoint Security ako globálne nastavenie proxy servera. Danými nastaveniami sa budú riadiť všetky moduly vyžadujúce prístup na internet.

Nastavenie proxy servera aktivujete potvrdením možnosti **Používať proxy server**. Ďalej zadajte adresu proxy servera do poľa **Proxy server** a číslo portu do poľa **Port**.

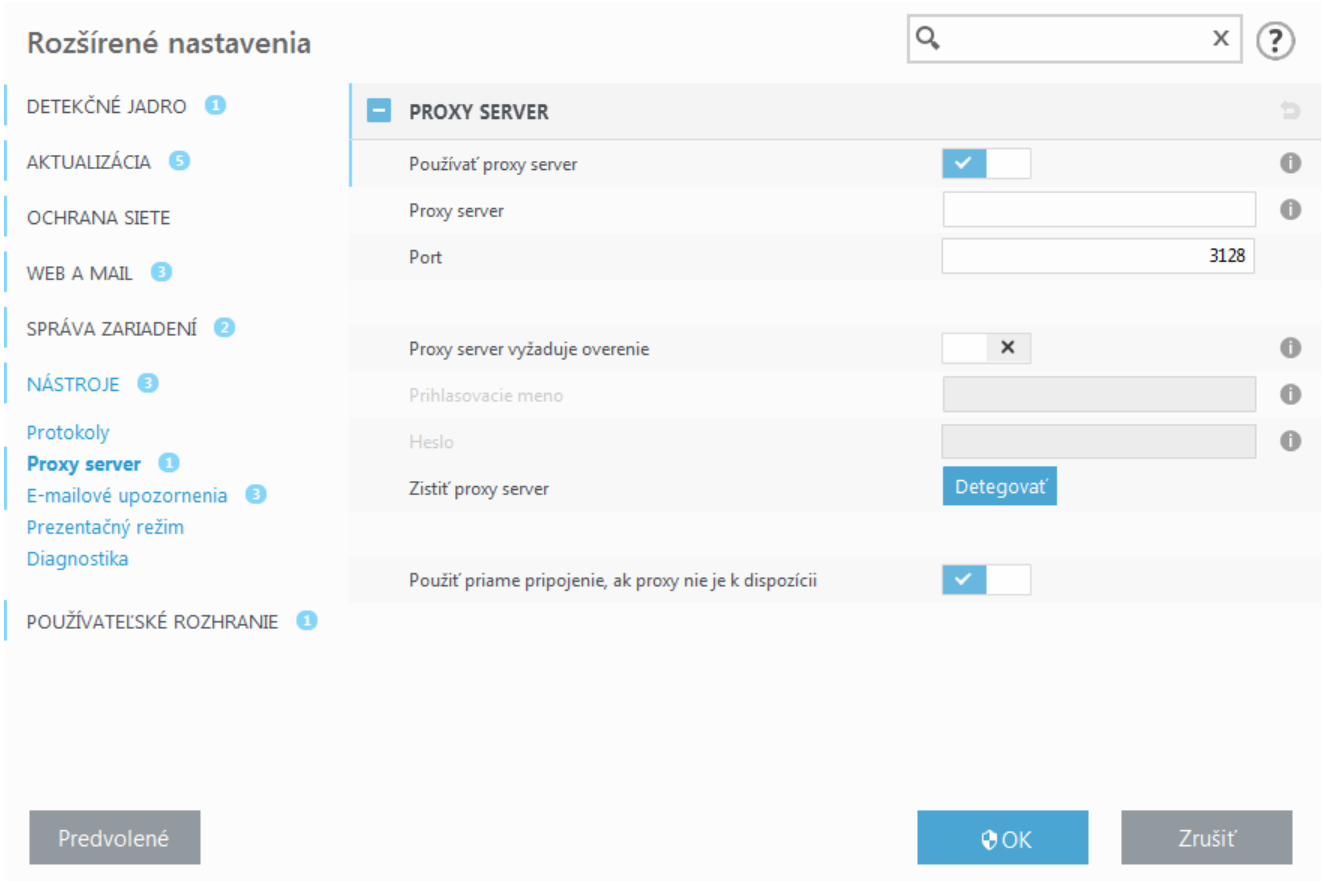
V prípade, že si komunikácia s proxy serverom vyžaduje overenie, vyberte možnosť **Proxy server vyžaduje overenie** a zadajte **prihlasovacie meno** a **heslo** do príslušných polí. Pre automatické zistenie nastavení proxy servera kliknite na tlačidlo **Vyhľadať proxy server**. Týmto sa prenesie nastavenie z operačného systému. Ak chcete nájsť nastavenia proxy servera v operačnom systéme, stlačte kombináciu klávesov **Windows + I** a potom kliknite na **Sieť a internet** > **Proxy**.

Budete musieť manuálne zadať vaše prihlasovacie meno a heslo v sekcii **Proxy server**.

Použiť priame pripojenie, ak proxy nie je k dispozícii – ak je produkt ESET Endpoint Security nakonfigurovaný tak, aby sa pripájal cez proxy, no proxy nie je dostupné, ESET Endpoint Security sa pokúsi pripojiť na servery

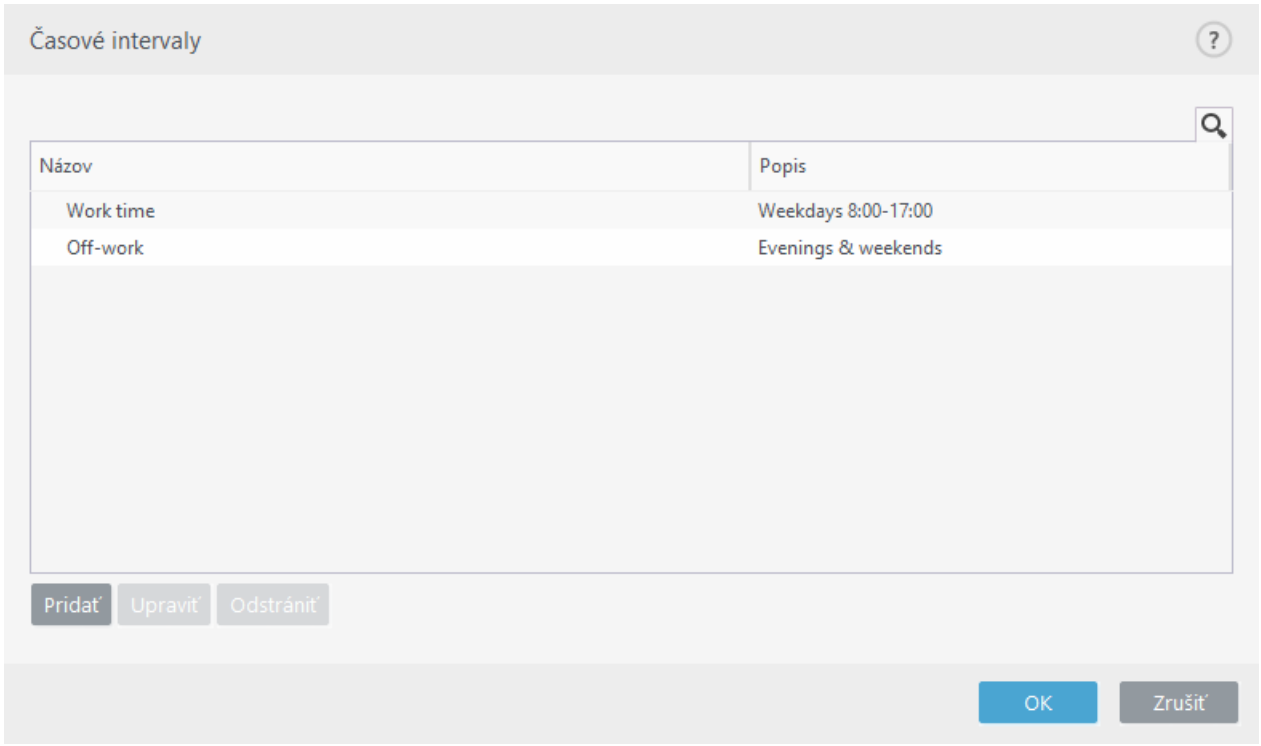
spoločnosti ESET priamo.

Nastavenia proxy servera môžete špecifikovať aj v rámci rozšírených nastavení aktualizácie (**Rozšírené nastavenia** > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia** > možnosť **Pripojenie prostredníctvom proxy servera** v roletovom menu **Režim proxy**). Toto nastavenie je platné pre konkrétny profil aktualizácie a je vhodné ho nastaviť, ak ide o prenosný počítač, ktorý vykonáva aktualizáciu detekčného jadra z rôznych vzdialených miest. Viac informácií nájdete v kapitole Pokročilé nastavenia aktualizácie.



Časové intervaly

Časové intervaly je možné vytvoriť a následne priraďovať k pravidlám **Správy zariadení** a **Webovej kontroly**. **Časové intervaly** môžete nastaviť v okne **Rozšírených nastavení** v časti **Nástroje**. Týmto spôsobom tak nezmeníte časové rozmedzie platnosti pre všetky pravidlá, ale len pre tie pravidlá, ktoré si zvolíte. Časové intervaly je možné použiť pri všetkých relevantných typoch pravidiel, ktoré podporujú kontrolu na základe času.



Pre vytvorenie časového intervalu postupujte nasledovne:

1. Kliknite na **Upraviť** > **Pridať**.
2. Zadajte názov a **popis** časového intervalu a kliknite na **Pridať**.
3. Zadefinuje deň a čas začiatku a konca vytváraného intervalu, prípadne vyberte možnosť **Celý deň**.
4. Kliknite na **OK**.

V rámci jedného časového intervalu môžete nastaviť viacero časových rozmedzí na základe dní a časov. Vytvorený časový interval sa bude zobrazovať v roletovom menu **Uplatňovať v intervale** v okne editora pravidiel Správy zariadení alebo v okne editora pravidiel Webovej kontroly.

Aktualizácie Microsoft Windows

Aktualizácie operačného systému predstavujú dôležitú súčasť zabezpečenia ochrany používateľov pred zneužitím bezpečnostných zraniteľností a možným infikovaním systému. Preto je dôležité inštalovať aktualizácie systému Microsoft Windows hneď, ako sú dostupné. ESET Endpoint Security vás informuje o chýbajúcich systémových aktualizáciách na úrovni, ktorú je možné nastaviť. Sú dostupné tieto úrovne:

- **Žiadne aktualizácie** – Nebudú ponúkané žiadne aktualizácie.
- **Voliteľné aplikácie** – Budú ponúkané aktualizácie s nízkou prioritou a všetky nasledovné.
- **Odporúčané aktualizácie** – Budú ponúkané bežné aktualizácie a všetky nasledovné.
- **Dôležité aktualizácie** – Budú ponúkané dôležité aktualizácie a všetky nasledovné.
- **Kritické aktualizácie** – Budú ponúkané len kritické aktualizácie.

Kliknite na **OK** pre uloženie zmien. Zobrazenie okna dostupných aktualizácií prebehne po overení stavu na aktualizačnom serveri. Samotné zobrazenie dostupných aktualizácií preto nemusí nutne prebehnúť hneď po uložení zmien.

Interval kontroly licencie

ESET Endpoint Security sa potrebuje pripájať k serverom spoločnosti ESET automaticky. Pre zmenu tohto nastavenia prejdite do sekcie **Rozšírené nastavenia (F5)** > **Nástroje** > **Licencia**. Predvolene je **Interval kontroly** nastavený na možnosť **Automatický** a licenčný server spoločnosti ESET kontroluje produkt niekoľkokrát za hodinu. V prípade zvýšenej sieťovej komunikácie zmeňte toto nastavenie na možnosť **Obmedzený**, aby ste znížili zaťaženie siete. Ak je zvolená možnosť **Obmedzený**, ESET Endpoint Security skontroluje licenčný server iba jedenkrát za deň, prípadne keď sa počítač reštartuje.

Ak je **Interval kontroly** nastavený na možnosť **Obmedzený**, môže trvať aj do jedného dňa, kým sa všetky zmeny týkajúce sa licencie, ktoré vykonáte cez nástroj ESET Business Account/ESET MSP Administrator, prejavia v nastaveniach produktu ESET Endpoint Security.

Používateľské rozhranie

Sekcia **Používateľské rozhranie** umožňuje nastaviť správanie programových GUI (grafické používateľské rozhranie) prvkov.

V sekcii Prvky používateľského rozhrania môžete nastaviť vizuálnu stránku programu a použité efekty.

Na zabezpečenie maximálnej ochrany bezpečnostného softvéru môžete zabrániť neoprávneným zmenám nastavení pomocou hesla v časti Nastavenia prístupu.

Nastavením Upozornení a okien správ a Oznámení môžete zmeniť správanie upozornení pri detekcii a správanie systémových oznámení. Nastavenia môžu byť zmenené tak, aby vyhovovali vašim požiadavkám.

Ak sa rozhodnete nezobrazovať určité upozornenia, budú zobrazené v časti **Prvky používateľského rozhrania** > **Stavy aplikácie**. Môžete kontrolovať ich stav, zobraziť viac informácií alebo ich odstrániť.

Integrácia kontextového menu sa zobrazuje po kliknutí pravým tlačidlom myši na vybrané objekty. Táto funkcionalita slúži na integráciu ovládacích prvkov ESET Endpoint Security do kontextového menu systému.

Prezentačný režim je funkcia určená pre používateľov, ktorí chcú neprerušovane používať svoj softvér a neželajú si byť vyrušovaní oznámeniami a dialógovými oknami, taktiež požadujú minimálne vyťaženie procesora a pamäte antivírusom.

Prečítajte si aj kapitolu Ako minimalizovať používateľské rozhranie programu ESET Endpoint Security (užitočné v prípade spravovaných prostredí).

Prvky používateľského rozhrania

ESET Endpoint Security umožňuje meniť nastavenia pracovného prostredia programu podľa potreby. Nastavenia používateľského rozhrania sa nachádzajú v Rozšírených nastaveniach programu ESET Endpoint Security v časti **Používateľské rozhranie** > **Prvky používateľského rozhrania**.

V časti **Prvky používateľského rozhrania** môžete meniť nastavenia grafického rozhrania programu. V roletovom menu **Režim spustenia** sú na výber nasledujúce možnosti:

Úplný – zobrazuje sa kompletné grafické rozhranie.

Minimálny – grafické rozhranie je spustené, avšak používateľovi sa zobrazujú len oznámenia.

Manuálny – grafické rozhranie nie je spustené automaticky pri prihlásení. Môže byť manuálne spustené ktorýmkoľvek používateľom.

Tichý – nezobrazujú sa žiadne oznámenia ani upozornenia. Grafické rozhranie môže spustiť iba správca. Tento režim môže byť užitočný v prípade spravovaných prostredí alebo v situáciách, keď je potrebné šetriť systémovými prostriedkami.

> Po zvolení Minimálneho režimu a reštartovaní počítača sa budú zobrazovať oznámenia, no grafické rozhranie nie. Ak chcete obnoviť režim úplného grafického rozhrania, spustite program ako správca z ponuky Štart v časti **Všetky programy** > **ESET** > ESET Endpoint Security, prípadne použite politiku v nástroji ESET PROTECT.

Ak chcete zrušiť zobrazovanie úvodnej obrazovky programu ESET Endpoint Security, deaktivujte možnosť **Zobrazovať úvodný obrázok pri štarte**.

Ak si prajete, aby program ESET Endpoint Security signalizoval dôležité udalosti v systéme pomocou zvukových efektov (napríklad pri nájdení hrozieb pri kontrole počítača alebo pri dokončení kontroly), aktivujte nastavenie **Používať zvukové upozornenia**.

Pridať do kontextového menu – integruje ovládacie prvky ESET Endpoint Security do kontextového menu systému.

Stavy

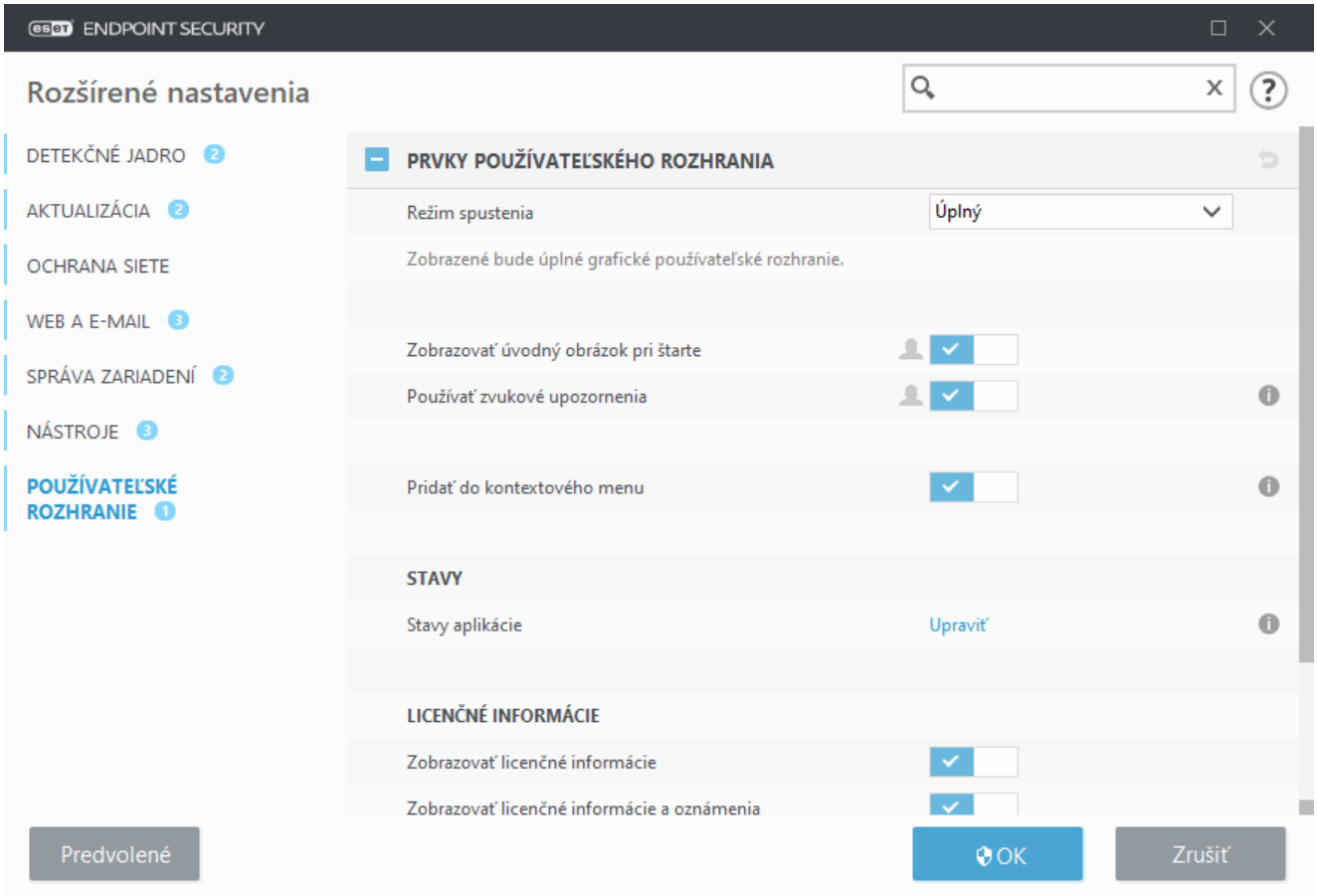
Stavy aplikácie – kliknutím na **Upraviť** môžete spravovať (zakázať) stavy, ktoré sa zobrazujú v hlavnom okne programu v časti **Stav ochrany**.

Licenčné informácie

Zobraziť licenčné informácie – ak je táto možnosť vypnutá, v hlavnom okne v časti **Stav ochrany** a **Pomocník a podpora** nebudú zobrazené informácie o platnosti licencie.

Zobraziť licenčné informácie a oznámenia – ak je táto možnosť vypnutá, oznámenia a správy sa budú zobrazovať len v prípade, že platnosť licencie uplynula.

> Nastavenia týkajúce sa licenčných informácií sú aplikované, ale nie dostupné pre produkt ESET Endpoint Security aktivovaný pomocou licencie MSP.



Nastavenia prístupu

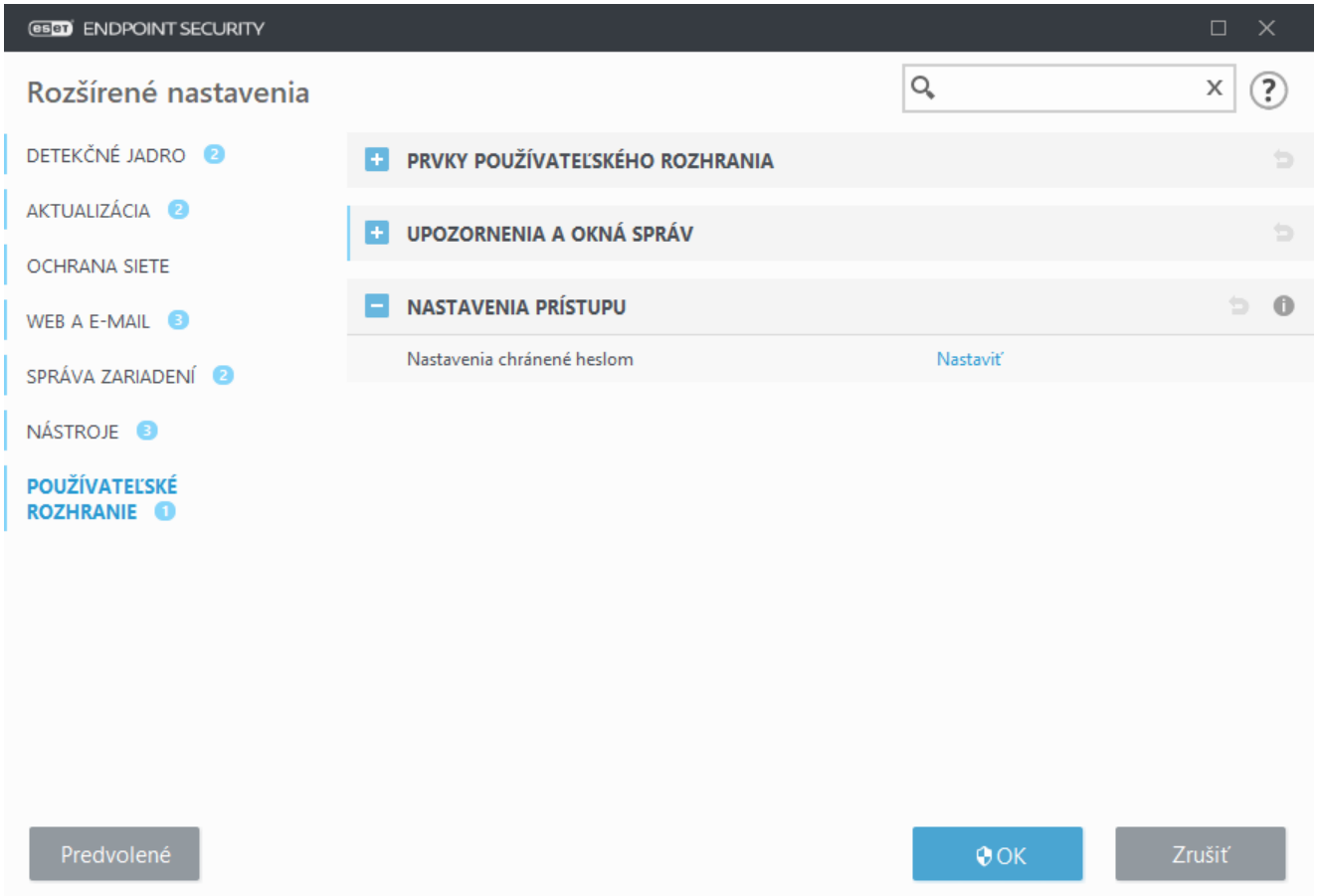
Na zaistenie maximálnej úrovne ochrany pre váš systém je kľúčové správne nastavenie programu ESET Endpoint Security. Neoprávnené zmeny nastavení môžu vystaviť systém nebezpečenstvu, prípadne spôsobiť stratu dát. Aby ste predišli neoprávneným zmenám nastavení, môžete rozšírené nastavenia programu ESET Endpoint Security ochrániť heslom.

Spravované prostredia

Správca môže vytvoriť politiku, ktorá bude vyžadovať pomocou hesla chrániť nastavenia ESET Endpoint Security na pripojených klientskych počítačoch. Pre vytvorenie novej politiky si prečítajte kapitolu Ochrana nastavení heslom.

Nespravované prostredie

Konfigurovať ochranu nastavení heslom môžete v okne **Rozšírených nastavení** (**F5**) v časti **Používateľské rozhranie** > **Nastavenia prístupu**.



Ochrana nastavení heslom – udáva, či je nastavené heslo. Po kliknutí sa otvorí okno Nastavenie hesla.

Ak chcete nastaviť alebo zmeniť heslo, kliknite na **Nastaviť**.

Heslo na ochranu rozšírených nastavení

Pre ochranu parametrov nastavení produktu ESET Endpoint Security pred neoprávnenými zmenami je potrebné nastaviť nové heslo.

Spravované prostredia

Správca môže vytvoriť politiku, ktorá bude vyžadovať pomocou hesla chrániť nastavenia ESET Endpoint Security na pripojených klientskych počítačoch. Pre vytvorenie novej politiky si prečítajte kapitolu Ochrana nastavení heslom.

Nespravované prostredie

V prípade, že chcete zmeniť existujúce heslo:

1. Zadajte vaše pôvodné heslo do poľa **Staré heslo**.
2. Zadajte vaše nové heslo do polí **Nové heslo** a **Potvrdiť heslo**.
3. Kliknite na tlačidlo **OK**.

Toto heslo sa bude vyžadovať pri akýchkoľvek budúcich úpravách nastavení ESET Endpoint Security.

Ak zabudnete svoje heslo, prístup k rozšíreným nastaveniam je možné obnoviť.

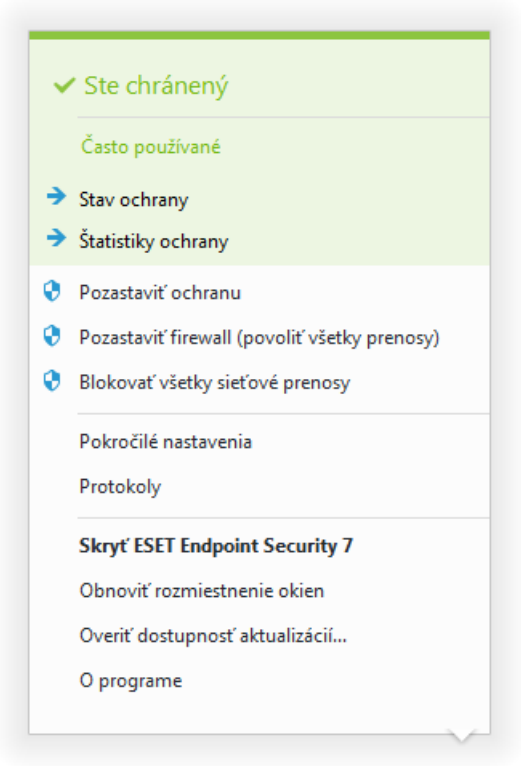
- Obnovenie pomocou metódy „Obnoviť heslo“ (verzia 7.1 a novšie)
- Obnovenie pomocou nástroja ESET Unlock Tool (verzia 7.0 a staršie)

Prečítajte si tento článok, ak ste zabudli svoj licenčný kľúč, dátum skončenia platnosti licencie alebo iné informácie týkajúce sa vašej licencie na ESET Endpoint Security.

Ikona na paneli úloh

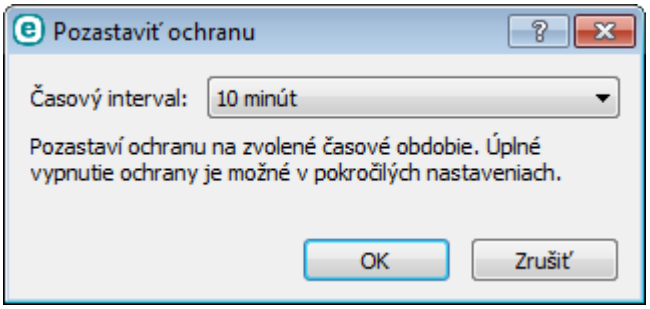
Niektoré dôležité nastavenia a funkcie sú dostupné v menu, ktoré sa zobrazí po kliknutí pravým tlačidlom na ikonu programu na paneli úloh.

> Pre zobrazenie menu po kliknutí na ikonu programu na paneli úloh je potrebné mať pre Prvky používateľského rozhrania nastavený úplný režim spustenia.



Pozastaviť ochranu – zobrazí sa potvrdzovacie dialógové okno, pomocou ktorého vypnete Detekčné jadro, ktoré chráni váš počítač pred útokmi prostredníctvom kontroly súborov, webu a e-mailovej komunikácie.

Roletové menu **Časový interval** predstavuje časové obdobie, počas ktorého bude ochrana vypnutá.



Pozastaviť firewall (povoliť všetku komunikáciu) – firewall sa prepne do neaktívneho režimu. Viac informácií nájdete v časti Sieť.

Blokovať všetku sieťovú komunikáciu – firewall bude blokovať všetku prichádzajúcu/odchádzajúcu sieťovú komunikáciu. Obnoviť sieťovú komunikáciu môžete kliknutím na možnosť **Zastaviť blokovanie všetkej sieťovej komunikácie**.

Rozšírené nastavenia – zvolením tejto možnosti prejdete do **Rozšírených nastavení** programu. Okno s rozšírenými nastaveniami je možné otvoriť aj stlačením klávesu F5 alebo z hlavného okna programu kliknutím na **Nastavenia** > **Rozšírené nastavenia**.

Protokoly – Protokoly obsahujú informácie o dôležitých udalostiach v programe a poskytujú prehľad všetkých detekcií.

Otvoriť ESET Endpoint Security – otvorí hlavné okno programu ESET Endpoint Security z ikony na paneli úloh.

Obnoviť rozmiestnenie okien – obnoví prednastavenú veľkosť a umiestnenie okna ESET Endpoint Security na obrazovke.

Overiť dostupnosť aktualizácií – spustí aktualizáciu programových modulov na zabezpečenie maximálnej ochrany pred škodlivým kódom.

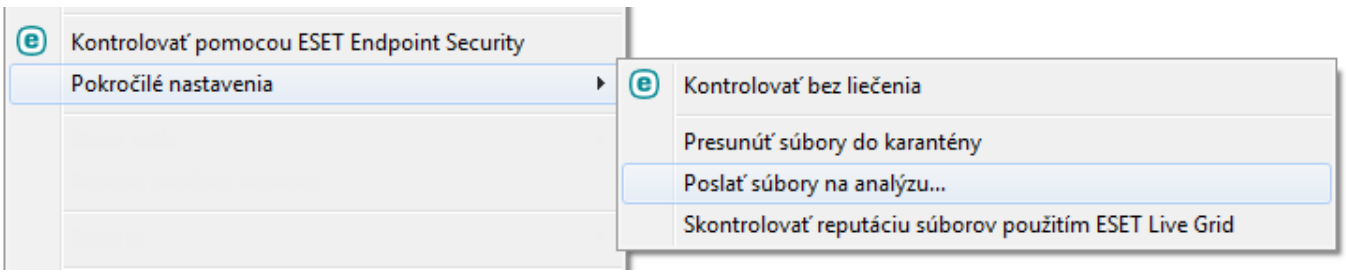
O programe – poskytuje základné informácie o systéme, podrobnosti o nainštalovanej verzii programu ESET Endpoint Security a informácie o nainštalovaných moduloch, ako aj dátum skončenia platnosti vašej licencie. Informácie o operačnom systéme a systémových prostriedkoch sú zobrazené v dolnej časti okna.

Kontextové menu

Kontextové menu sa zobrazuje po kliknutí pravým tlačidlom myši na súbor v prieskumníkovi. Obsahuje zoznam akcií, ktoré možno so súborom vykonať.

Ovládacie prvky ESET Endpoint Security je možné integrovať do kontextového menu systému. Podrobnejšie nastavenia tejto funkcionality sú dostupné v Rozšírených nastaveniach v časti **Používateľské rozhranie** > **Prvky používateľského rozhrania**.

Pridať do kontextového menu – integruje ovládacie prvky ESET Endpoint Security do kontextového menu systému.



Pomocník a podpora

ESET Endpoint Security obsahuje podporné informácie a nástroje poskytujúce pomoc pri riešení problémov, s ktorými sa pri používaní produktu môžete stretnúť.

**Nainštalovaný produkt**

- **O ESET Endpoint Security** – zobrazuje informácie o vašej kópii programu ESET Endpoint Security.
- **Riešenie problémov s produktom** – po kliknutí na tento odkaz sa otvorí kapitola pomocníka, ktorá sa venuje riešeniu najčastejších problémov s produktom.
- **Riešenie problémov s licenciou** – po kliknutí na tento odkaz sa otvorí kapitola pomocníka, ktorá sa venuje riešeniu problémov s aktiváciou alebo zmenou licencie.
- **Zmeniť licenciu** – kliknutím na túto možnosť otvoríte okno na aktiváciu produktu.

**Stránka pomocníka** – kliknutím na tento odkaz otvoríte pomocníka pre ESET Endpoint Security.

**Technická podpora**

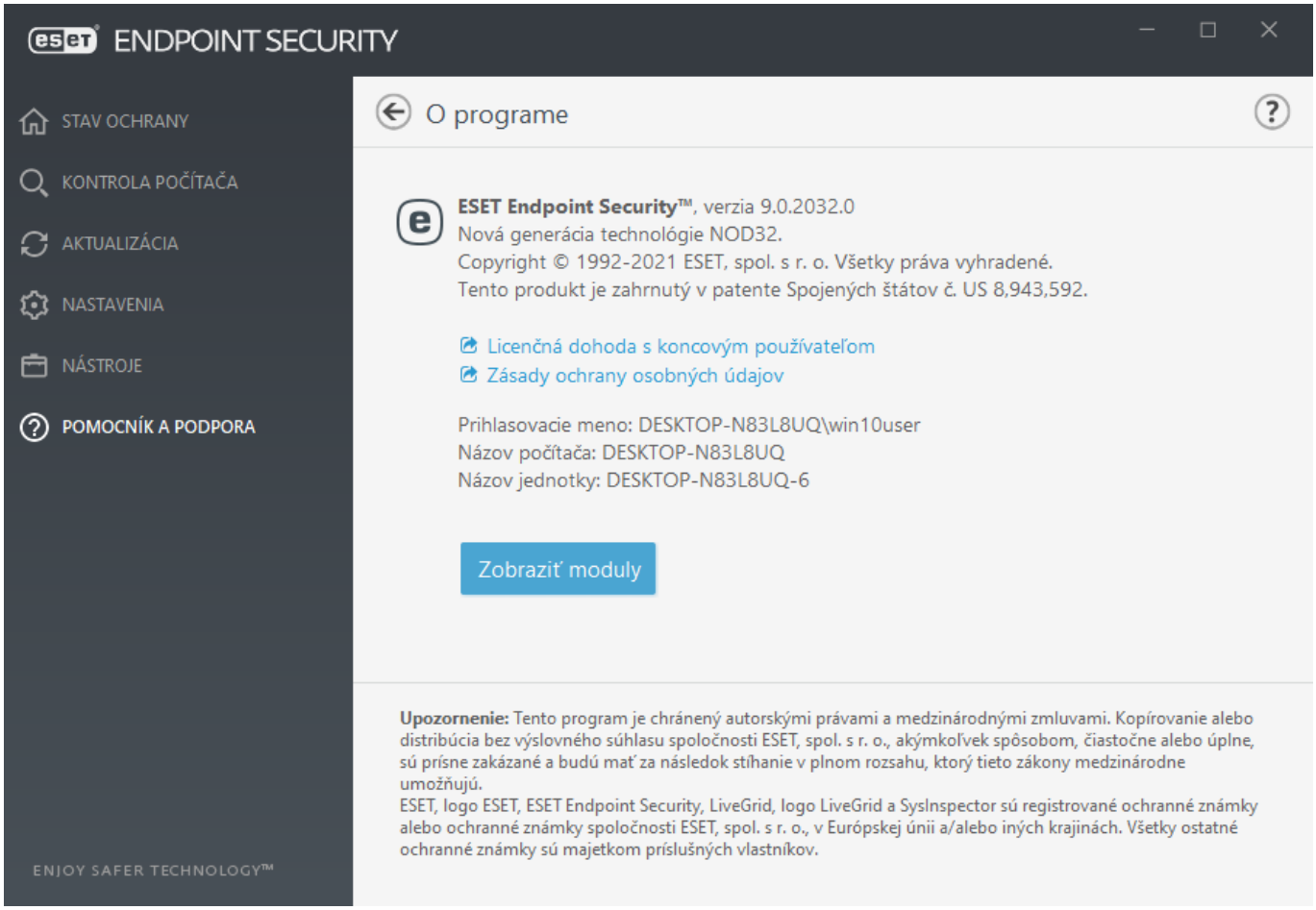
- **Požiadať o technickú podporu** – v prípade problému, na ktorý nenájdete odpoveď, je možné kontaktovať oddelenie technickej podpory prostredníctvom formulára na webovej stránke spoločnosti ESET. V závislosti od konfigurácie programu sa ešte pred vyplnením webového formulára zobrazí okno s možnosťou odoslať údaje o systémových nastaveniach.
- **Podrobnosti pre technickú podporu** – po výzve môžete skopírovať a odoslať informácie technickej podpore spoločnosti ESET (napr. názov produktu, verzia produktu, operačný systém a typ procesora).
- **ESET Log Collector** – odkaz na článok Databázy znalostí spoločnosti ESET, kde si môžete stiahnuť nástroj ESET Log Collector, ktorý slúži na zhromaždenie informácií a protokolov z počítača pre rýchlejšie riešenie problémov. Bližšie informácie nájdete v online príručke pre ESET Log Collector.
- Na vytvorenie podrobných protokolov pre všetky dostupné funkcie programu aktivujte možnosť Vytváranie rozšírených protokolov. Takéto protokoly našim vývojárom uľahčia diagnostiku problému a jeho následné riešenie. Úroveň podrobnosti zaznamenávaných informácií je v tomto prípade nastavená na hodnotu Diagnostické. Vytváranie rozšírených protokolov sa automaticky vypne po dvoch hodinách, ak tak nespravíte skôr kliknutím na Prestať zapisovať do rozšírených protokolov. Po vytvorení všetkých protokolov sa zobrazí okno oznámenia, v ktorom nájdete odkaz pre priamy prístup k priečinku s diagnostickými protokolmi.

**Databáza znalostí spoločnosti ESET** – Databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najefektívnejší nástroj na riešenie rozličných problémov.

O ESET Endpoint Security

V tomto okne nájdete podrobné informácie o nainštalovanej verzii ESET Endpoint Security, vašom operačnom systéme a systémových prostriedkoch.

Kliknutím na tlačidlo **Zobraziť moduly** zobrazíte zoznam načítaných programových modulov spolu s číslom ich verzie. Tieto informácie môžete skopírovať do schránky kliknutím na **Kopírovať**. Ide o informácie, ktoré môžu byť užitočné pri riešení problémov alebo pri kontaktovaní technickej podpory.



Odoslať systémové nastavenia

V záujme poskytnutia čo možno najrýchlejšej a najpresnejšej pomoci bude od vás spoločnosť ESET vyžadovať informácie o konfigurácii vášho produktu ESET Endpoint Security, podrobné systémové informácie, spustené procesy (protokol nástroja ESET SysInspector) a tiež údaje z databázy Registry. Spoločnosť ESET použije tieto informácie len na účely poskytnutia technickej podpory.

Ak posielate tieto informácie cez webový formulár, vaše systémové nastavenia budú odoslané spoločnosti ESET. Zvoľte možnosť **Vždy odoslať tieto informácie**, ak chcete, aby si program výber tejto akcie zapamätal. Ak chcete odoslať formulár bez odoslania akýchkoľvek dát, zvoľte možnosť **Neodoslať informácie** a môžete kontaktovať technickú podporu spoločnosti ESET prostredníctvom online formulára.

Tieto nastavenia môžu byť tiež upravené v časti **Rozšírené nastavenia** > **Nástroje** > **Diagnostika** > **Technická podpora**.

Ak ste sa rozhodli odoslať systémové nastavenia, je potrebné vyplniť a odoslať webový formulár, v opačnom prípade vaša požiadavka na technickú podporu nebude vytvorená.

Technická podpora

Kontaktovať technickú podporu

Požiadať o technickú podporu – v prípade problému, na ktorý nenájdete odpoveď, je možné kontaktovať

oddelenie technickej podpory spoločnosti ESET prostredníctvom formulára na webovej stránke. V závislosti od konfigurácie programu sa ešte pred vyplnením webového formulára zobrazí okno s možnosťou odoslať údaje o systémových nastaveniach.

Získať informácie pre technickú podporu

Podrobnosti pre technickú podporu – použite túto možnosť, ak vás technická podpora spoločnosti ESET požiada o skopírovanie a zaslanie základných informácií (zahŕňa napríklad podrobnosti o licencii, názov produktu, verziu produktu, operačný systém a informácie o počítači).

ESET Log Collector – odkaz na článok Databázy znalostí spoločnosti ESET, kde si môžete stiahnuť nástroj ESET Log Collector, ktorý slúži na zhromaždenie informácií a protokolov z počítača pre rýchlejšie riešenie problémov. Bližšie informácie nájdete v online príručke pre ESET Log Collector.

Na vytvorenie podrobných protokolov pre všetky dostupné funkcie programu aktivujte možnosť **Vytváranie rozšírených protokolov**. Takéto protokoly našim vývojárom uľahčia diagnostiku problému a jeho následné riešenie. Úroveň podrobnosti zaznamenávaných informácií je v tomto prípade nastavená na hodnotu **Diagnostické**. Vytváranie rozšírených protokolov sa automaticky vypne po dvoch hodinách, ak tak nespravíte skôr kliknutím na **Prestať zapisovať do rozšírených protokolov**. Po vytvorení všetkých protokolov sa zobrazí okno oznámenia, v ktorom nájdete odkaz pre priamy prístup k priečinku s diagnostickými protokolmi.

Oznámenia

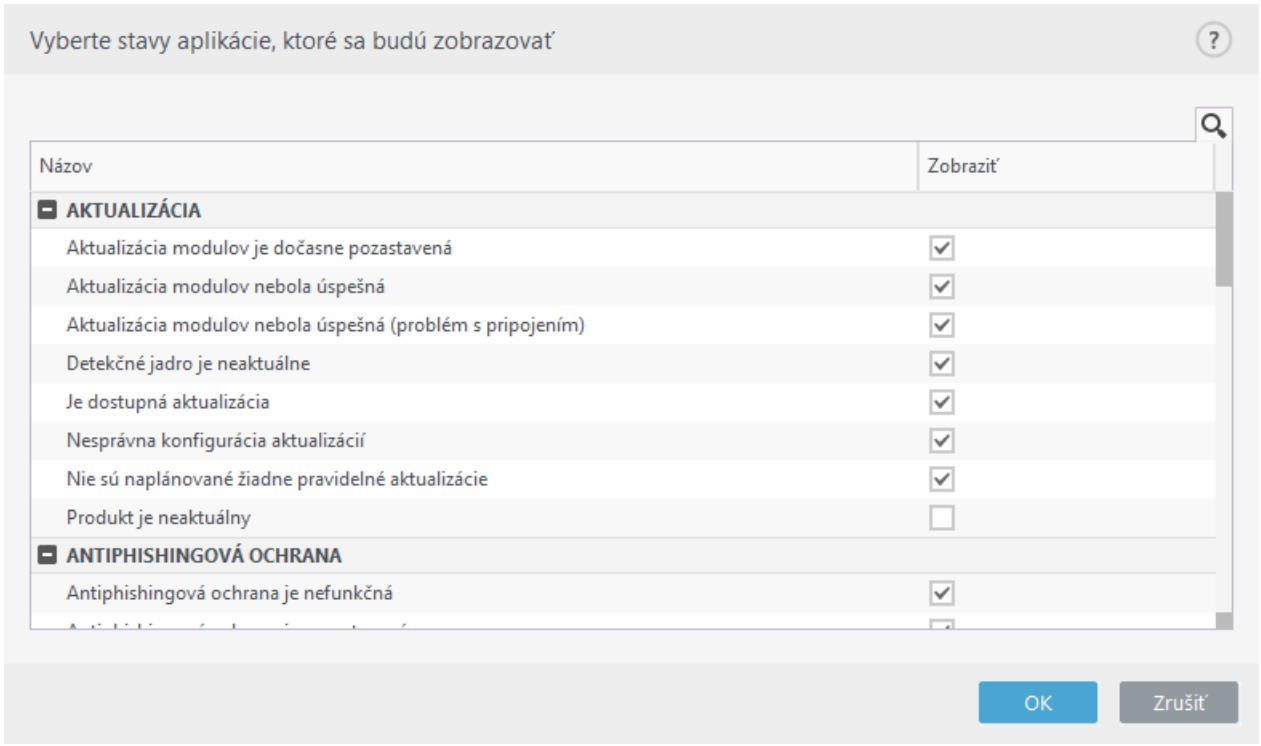
Nastavenia oznámení produktu ESET Endpoint Security môžete spravovať v sekcii **Rozšírené nastavenia** (F5) > **Oznámenia**. Konfigurovať môžete nasledujúce typy oznámení:

- Stavy aplikácie – po kliknutí na možnosť **Upraviť** môžete vybrať, ktoré stavy aplikácie sa budú zobrazovať v hlavnom okne programu v sekcii Domov.
- Oznámenia na ploche – oznámenia, ktoré sa zobrazujú v podobe malého kontextového okna vedľa systémového panela úloh.
- Prispôsobenie oznámení – umožňuje vám pridať vlastnú správu napríklad do oznámenia na ploche.
- Interaktívne upozornenia – výstražné upozornenia a okná správ, ktoré si vyžadujú interakciu používateľa.
- Preposielanie (e-mailové oznámenia) – oznámenia zasielané na vopred špecifikovanú e-mailovú adresu.

Stavy aplikácie

Ak chcete nastaviť, ktoré stavy aplikácie budú zobrazované (napríklad, ak pozastavíte antivírusovú a antispyvérovú ochranu alebo ak spustíte herný režim), otvorte **Rozšírené nastavenia** (F5) > **Oznámenia** a kliknite na tlačidlo **Upraviť**. V zobrazenom okne si môžete vybrať, ktoré stavy aplikácie sa budú zobrazovať v hlavnom okne programu v sekcii Domov.

Stav aplikácie bude zobrazený aj v prípade, že váš produkt nie je aktivovaný alebo vašej licencii uplynula platnosť. Toto nastavenie je možné zmeniť prostredníctvom politík v nástroji ESET PROTECT.



Oznámenia na ploche

Oznámenia na ploche sa zobrazujú v podobe malého kontextového okna vedľa systémového panela úloh. Na základe predvolených nastavení sa okno oznámenia zobrazí na 10 sekúnd, potom pomaly zmizne. Toto je hlavný spôsob, ako ESET Endpoint Security komunikuje s používateľom, aby ho informoval o úspešných aktualizáciách produktu, nových pripojených zariadeniach, dokončených antivírusových kontrolách alebo nájdených hrozbách.

Zobrazovať oznámenia na ploche – odporúčame ponechať túto možnosť zapnutú, aby vás mohol produkt informovať o nových udalostiach.

Oznámenia na ploche – ak chcete zapnúť alebo vypnúť konkrétne oznámenia na ploche, kliknite na možnosť **Upraviť**.

Nezobrazovať oznámenia pri spúšťaní aplikácií na celú obrazovku – táto možnosť vám umožňuje potlačiť zobrazovanie všetkých oznámení, ktoré nevyžadujú interakciu používateľa, pri spúšťaní aplikácií v režime na celú obrazovku.

Časový limit v sekundách – umožňuje nastaviť, ako dlho bude oznámenie zobrazené na ploche. Hodnota musí byť v rozmedzí 3 – 30 sekúnd.

Priehľadnosť – umožňuje nastaviť priehľadnosť okna s oznámením. Podporované je rozmedzie od 0 (nepriehľadné okno) do 80 (veľmi vysoká priehľadnosť).

Zobrazovať udalosti od úrovne – umožňuje nastaviť, od akej úrovne závažnosti sa majú oznámenia zobrazovať. Z roletového menu vyberte jednu z týchto možností:

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informatívne** – zaznamenávané budú informatívne správy, napríklad o neobvyklých sieťových aktivitách alebo o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Upozornenia** – zaznamenávané budú kritické chyby a upozornenia (Anti-Stealth nepracuje správne alebo

zlyhala aktualizácia).
- **Chyby** – zaznamenávané budú chyby (ochrana dokumentov nie je spustená) a kritické chyby.
- **Kritické** – zaznamenávané budú len kritické chyby (nespustenie antivírusovej ochrany, infikovaný systém atď.).

Vo viacpoužívateľskom prostredí zobrazovať oznámenia tomuto používateľovi – umožňuje vybrať účet, ktorému sa budú zobrazovať oznámenia na ploche. Ak napríklad na počítači nepoužívate správcovský účet, zadajte celý názov používateľského účtu, ktorému sa majú oznámenia zobrazovať. Oznámenia na ploche môže dostávať len jeden používateľský účet.

Povoliť oznámeniam zobrazovať sa v popredí – oznámenia sa budú zobrazovať v popredí obrazovky a budú dostupné pomocou klávesovej skratky Alt+Tab.

Dialógové okno – Oznámenia na ploche

Ak chcete upraviť zobrazovanie oznámení na ploche (v pravom dolnom rohu obrazovky), prejdite v **Rozšírených nastaveniach** (F5) do sekcie **Oznámenia** > **Oznámenia na ploche**. Kliknite na **Upraviť** vedľa popisu **Oznámenia na ploche** a v stĺpci **Zobraziť na ploche** označte príslušné políčka jednotlivých oznámení.

> Ak si chcete nastaviť oznámenia **Súbor skontrolovaný** a **Súbor nebol skontrolovaný** súvisiace s posielaním vzoriek do služby ESET LiveGuard, v sekcii Proaktívna ochrana musíte mať nastavenú možnosť **Blokovať spustenie súboru do doručenia výsledku analýzy**.

Prispôsobenie oznámení

V tomto okne môžete prispôsobiť správy v oznámeniach.

Predvolená správa v oznámeniach – predvolená správa, ktorá sa zobrazí v spodnej časti oznámenia.

Detekcie

Povoľte možnosť **Automaticky nezatvárať oznámenia o malvéri**, ak chcete, aby upozornenia na malvér zostali zobrazené, až kým nebudú zatvorené manuálne.

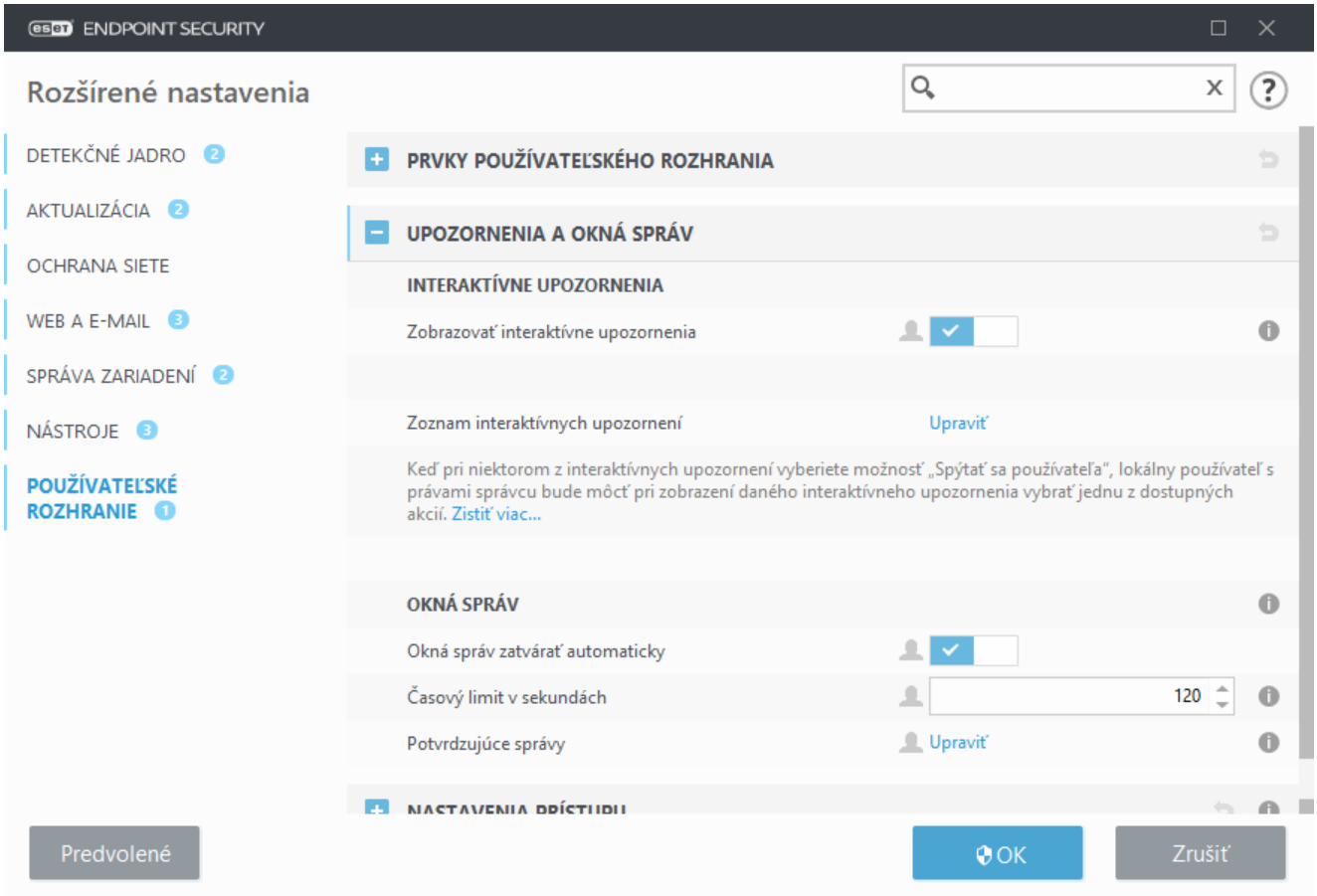
Zrušte možnosť **Použiť predvolenú správu** a zadajte vlastnú správu do poľa **Správa upozorňujúca na detekciu**.

Interaktívne upozornenia

Hľadáte informácie o častých upozorneniach a oznámeniach?

- Našla sa hrozba
- Adresa bola zablokovaná
- Produkt nie je aktivovaný
- Aktualizácia je k dispozícii
- Informácie o aktualizáciách nie sú konzistentné
- Riešenie chybového hlásenia „Aktualizácia modulov nebola úspešná“
- „Súbor je poškodený“ alebo „Nepodarilo sa premenovať súbor“
- Certifikát webovej stránky bol zrušený
- Sieťová hrozba bola zablokovaná
- Súbor je blokovaný z dôvodu analýzy

Interaktívne upozornenia v sekcii **Oznámenia** vám umožňujú nastaviť, ako má ESET Endpoint Security pracovať s detekciami v prípade, že je potrebná interakcia používateľa (napr. potenciálne phishingové stránky).



Interaktívne upozornenia

Interaktívne okná upozornení sa zobrazujú, ak dôjde k detekcii alebo ak sa vyžaduje zásah používateľa.

Zobrazovať interaktívne upozornenia

- V prípade nespravovaných používateľov odporúčame túto možnosť ponechať v predvolenom nastavení (zapnutá).
- V prípade spravovaných používateľov ponechajte túto možnosť zapnutú a vyberte preddefinovanú akciu v zozname interaktívnych upozornení.

Vypnutím možnosti **Zobrazovať interaktívne upozornenia** sa skryjú všetky okná upozornení a dialógové okná

prehliadača. Automaticky bude zvolená preddefinovaná akcia (napr. „potenciálna phishingová stránka“ bude zablokovaná).

Okná správ

Ak si želáte, aby sa informatívne okná zatvárali automaticky po uplynutí určitého času, vyberte možnosť **Okná správ zatvárať automaticky**. Po uplynutí nastaveného času sa okno oznámenia zatvorí, ak tak neurobí používateľ sám.

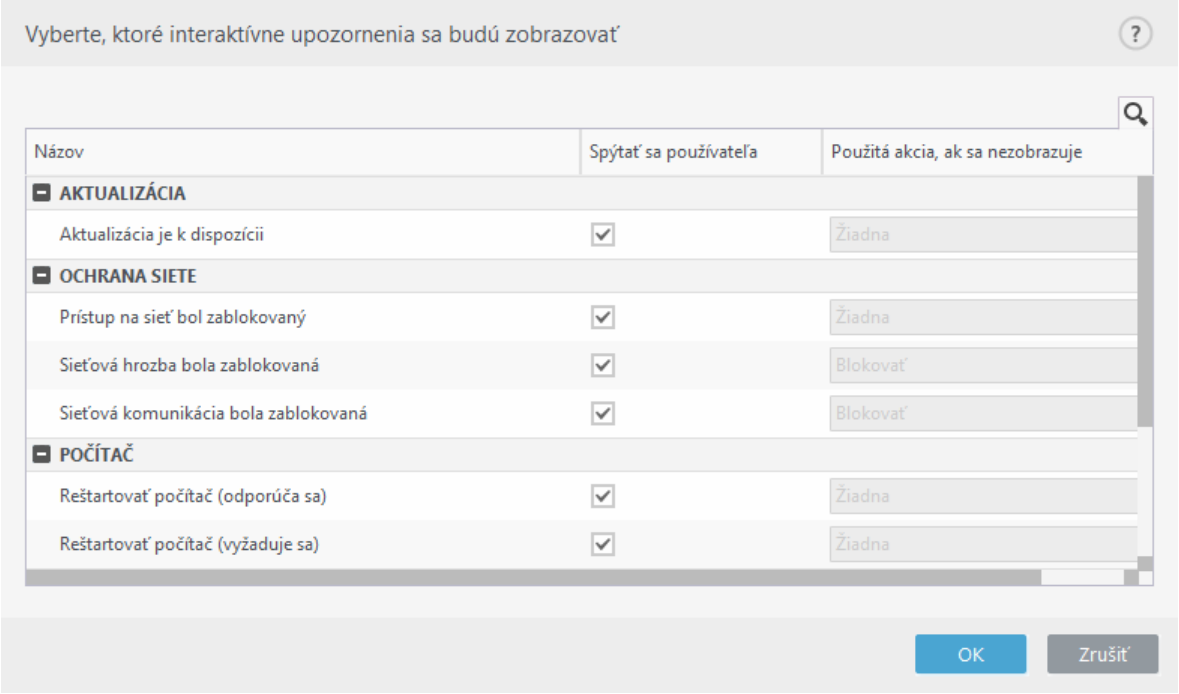
Potvrdzovacie správy – zobrazí vám zoznam potvrdzovacích správ, pre ktoré môžete zvoliť, či sa majú alebo nemajú zobrazovať.

Zoznam interaktívnych upozornení

Táto sekcia popisuje niekoľko interaktívnych upozornení, ktoré ESET Endpoint Security zobrazí pred vykonaním akejkoľvek akcie.

Ak chcete prispôsobiť správanie interaktívnych upozornení, prejdite v Rozšírených nastaveniach programu ESET Endpoint Security do sekcie **Oznámenia** > **Interaktívne upozornenia** > a kliknite na **Upraviť**.

Užitočné pre spravované prostredia, kde môže správca zrušiť výber možnosti **Spýtať sa používateľa** v celom zozname upozornení a vybrať preddefinovanú akciu, ktorá sa má použiť.
Pozrite si tiež kapitolu Stavy aplikácie.



Pozrite si ďalšie kapitoly Pomocníka, ktoré sa venujú jednotlivým interaktívnym upozorneniam:

Vymeniteľné médiá

- Rozpoznané nové zariadenie

Zabezpečený prehliadač

- Povoliť pokračovanie v predvolenom prehliadači

Ochrana siete

- Upozornenie Prístup na sieť bol zablokovaný sa zobrazí v prípade, že pre danú pracovnú stanicu bola z ESET PROTECT spustená úloha pre klienta **Izolovať počítač od siete**.
- Bola zablokovaná sieťová komunikácia
- Sieťová hrozba bola zablokovaná

Upozornenia internetového prehliadača

- Našiel sa potenciálne nechcený obsah
- Webová stránka bola zablokovaná z dôvodu phishingu

Počítač

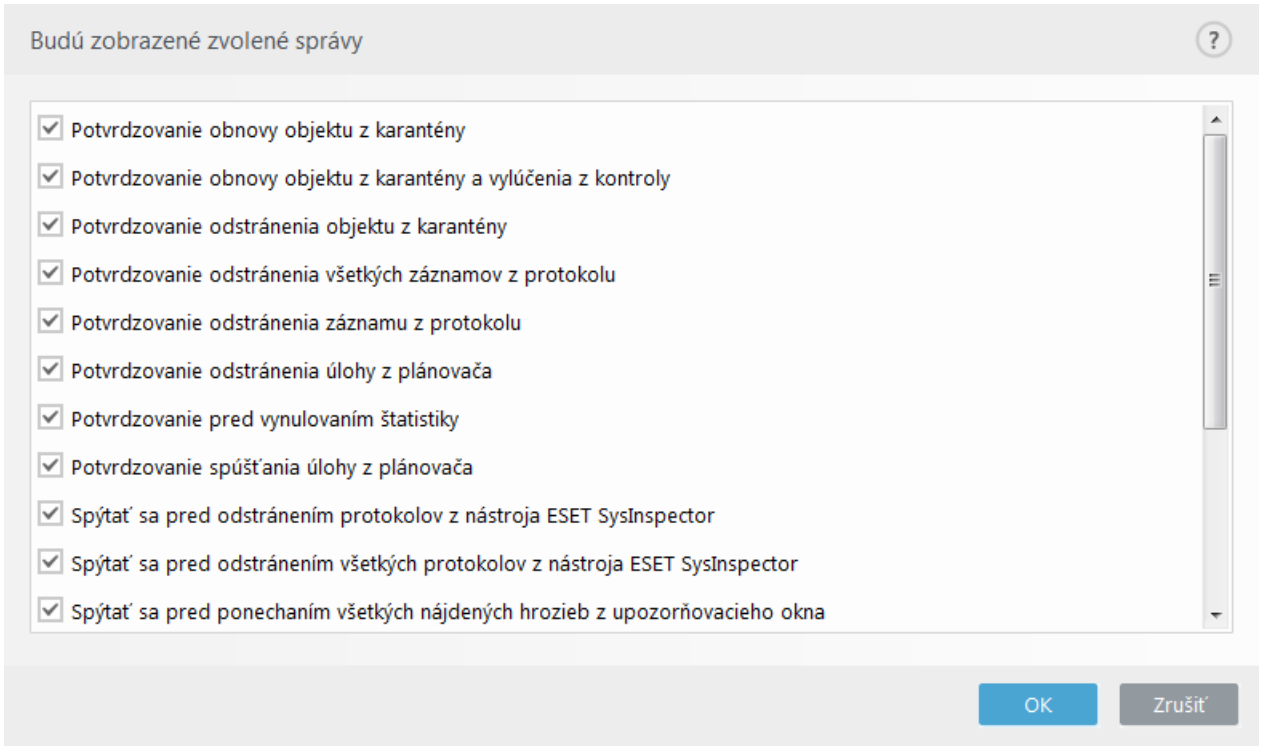
Prítomnosť týchto upozornení zmení farbu používateľského rozhrania na oranžovú:

- Reštartovať počítač (vyžaduje sa)
- Reštartovať počítač (odporúčané)

> Pod interaktívne upozornenia v tejto sekcii nespadajú interaktívne okná súvisiace s Detekčným jadrom, HIPS či firewallom, keďže ich správanie môže byť individuálne nakonfigurované v rámci nastavení k danej funkcii.

Potvrdzovacie správy

Pre prístup k nastaveniu potvrdzovacích správ prejdite v Rozšírených nastaveniach programu ESET Endpoint Security do sekcie **Používateľské rozhranie** > **Upozornenia a okná správ** > **Potvrdzovacie správy** a kliknite na tlačidlo **Upraviť**.



Potvrdzovacie správy sa zobrazujú v programe ESET Endpoint Security pred vykonaním akcií. Môžete označiť začiarkavacie políčka vedľa jednotlivých potvrdzovacích správ, ak chcete ich zobrazovanie povoliť, alebo ak ich zobrazovanie chcete naopak zakázať, zrušte ich označenie.

Na nasledujúcich odkazoch nájdete viac informácií o jednotlivých funkciách, ktorých sa potvrdzovacie správy týkajú:

- Spýtať sa pred odstránením protokolov z nástroja ESET SysInspector
- Spýtať sa pred odstránením všetkých protokolov z nástroja ESET SysInspector
- Spýtať sa pred odstránením objektu z karantény
- Spýtať sa pred zrušením vykonaných zmien v rozšírených nastaveniach
- Spýtať sa pred zatvorením okna s oznámením o nájdených a nevyriešených hrozbách
- Spýtať sa pred odstránením záznamu z protokolu
- Spýtať sa pred odstránením úlohy z plánovača
- Spýtať sa pred odstránením všetkých záznamov z protokolu
- Spýtať sa pred vynulovaním štatistiky
- Spýtať sa pred obnovením objektu z karantény
- Spýtať sa pred obnovením objektov z karantény a ich vylúčením z kontroly
- Spýtať sa pred spustením úlohy z plánovača
- Zobraziť oznámenia o výsledku antispamovej kontroly
- Zobraziť oznámenia o výsledku antispamovej kontroly pre e-mailové klienty
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailové klienty Outlook Express a Windows Mail
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailového klienta Windows Live Mail
- Zobraziť potvrdzovacie dialógové okná produktu pre e-mailového klienta Microsoft Outlook

Chyba (konflikt) v rámci rozšírených nastavení

Táto chyba sa môže vyskytnúť v prípade, že niektorý komponent (napr. HIPS alebo Firewall) a zároveň aj používateľ vytvorí pravidlá v interaktívnom alebo učiacom sa režime v rovnakom čase.

Ak chcete vytvárať vlastné pravidlá, odporúčame zmeniť režim filtrovania na predvolený **Automatický režim**. Viac informácií o učiacom sa režime ESET firewallu nájdete v tejto kapitole. Viac informácií o technológii HIPS a režimoch filtrovania HIPS nájdete v tejto kapitole.

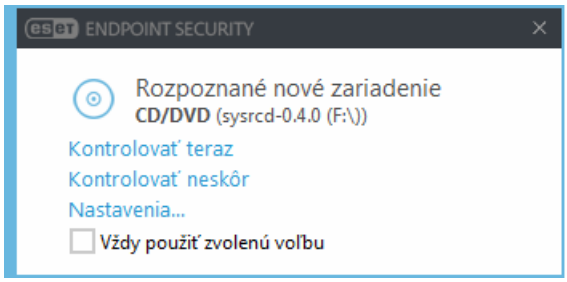
Povoliť pokračovanie v predvolenom prehliadači

Interaktívne upozornenie sa zobrazí len vtedy, keď nastane chyba pri spustení zabezpečeného prehliadača.

Vymeniteľné médiá

ESET Endpoint Security poskytuje automatickú kontrolu vložených alebo pripojených vymeniteľných médií (CD/DVD/USB...). Toto môže byť užitočné v prípade, že chce správca zabrániť používateľom vložiť alebo pripojiť do počítača vymeniteľné médium s nežiaducim obsahom.

Ak je v produkte ESET Endpoint Security nastavená akcia **Zobraziť možnosti kontroly**, po vložení alebo pripojení vymeniteľného média sa zobrazí nasledujúce okno:



Toto dialógové okno ponúka nasledujúce možnosti:

- **Kontrolovať teraz** – spustí sa kontrola vymeniteľného média.
- **Nekontrolovať** – nevykoná sa žiadna akcia.

ESET Endpoint Security navyše obsahuje funkciu Správa zariadení, ktorá vám umožňuje vytvárať pravidlá pre používanie externých zariadení na danom počítači. Viac informácií nájdete v kapitole Správa zariadení.

Nastavenia kontroly vymeniteľných médií sú dostupné v Rozšírených nastaveniach (**F5**) v sekcii **Používateľské rozhranie** > **Upozornenia a okná správ** > **Interaktívne upozornenia** > **Zoznam interaktívnych upozornení** > **Upraviť** > **Rozpoznané nové zariadenie**.

Ak nie je vybraná možnosť **Spýtať sa používateľa**, vyberte požadovanú akciu po vložení alebo pripojení vymeniteľného média do počítača:

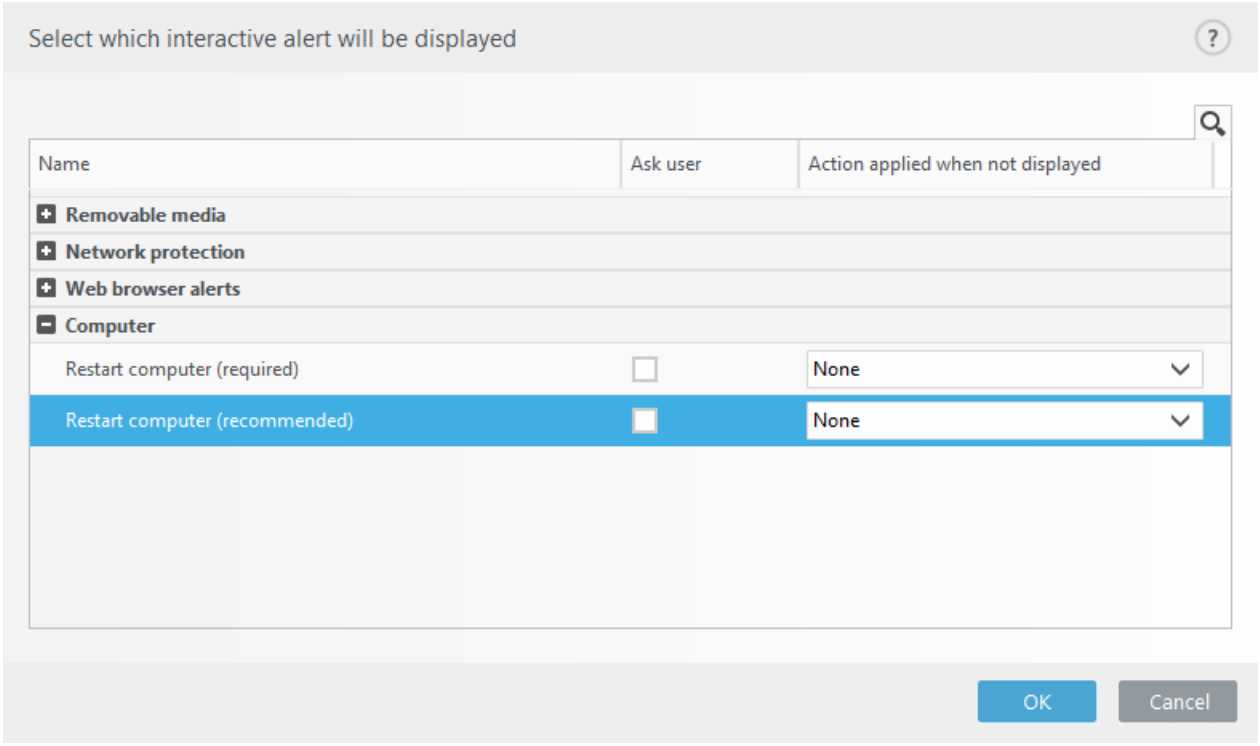
- **Nekontrolovať** – nevykoná sa žiadna akcia a okno **Rozpoznané nové zariadenie** sa neotvorí.
- **Automaticky skontrolovať zariadenie** – spustí sa kontrola vloženého zariadenia.
- **Vynútená kontrola zariadenia** – spustí sa kontrola vloženého zariadenia a nebude možné ju zrušiť.
- **Zobraziť možnosti kontroly** – otvorí sekciu **Interaktívne upozornenia**.

Vyžaduje sa reštart

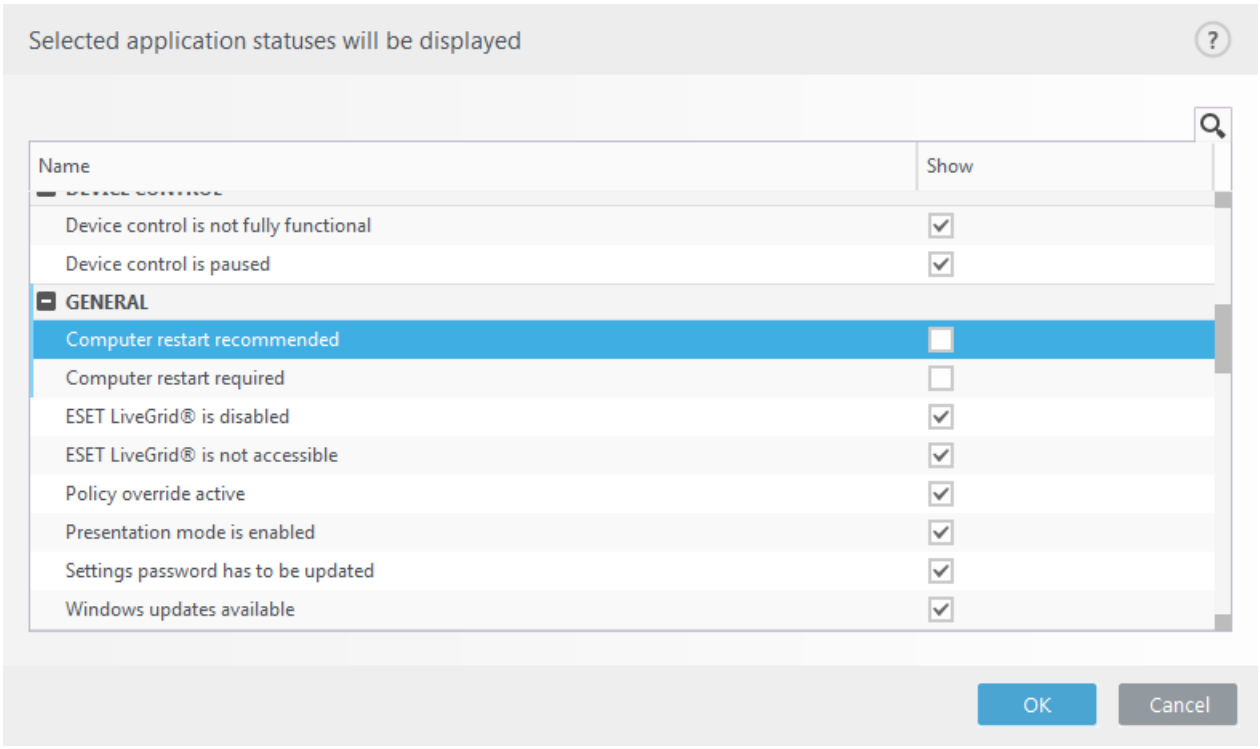
Ak sa na koncových pracovných staniciach zobrazuje červené upozornenie „Vyžaduje sa reštart“, máte možnosť zobrazovanie týchto upozornení vypnúť.

Ak chcete vypnúť zobrazovanie upozornení „Vyžaduje sa reštart“ a „Odporúča sa reštart“, postupujte podľa nasledujúcich krokov:

1. Stlačte kláves **F5** pre otvorenie okna Rozšírených nastavení a rozbaľte sekciu **Upozornenia a okná správ**.
2. Kliknite na možnosť **Upraviť** vedľa položky **Zoznam interaktívnych upozornení**. V sekcii **Počítač** zrušte označenie políčok **Reštartovať počítač (povinné)** a **Reštartovať počítač (odporúčané)**.



3. V oboch otvorených oknách kliknite na tlačidlo **OK** pre uloženie zmien.
4. Príslušné upozornenia sa na koncovej pracovnej stanici už viac nebudú zobrazovať.
5. (Voliteľný krok) Ak chcete vypnúť aj zobrazovanie príslušných stavov v hlavnom okne programu ESET Endpoint Security, v okne so zoznamom stavov aplikácie zrušte označenie políčok **Vyžaduje sa reštart počítača** a **Odporúča sa reštart počítača**.

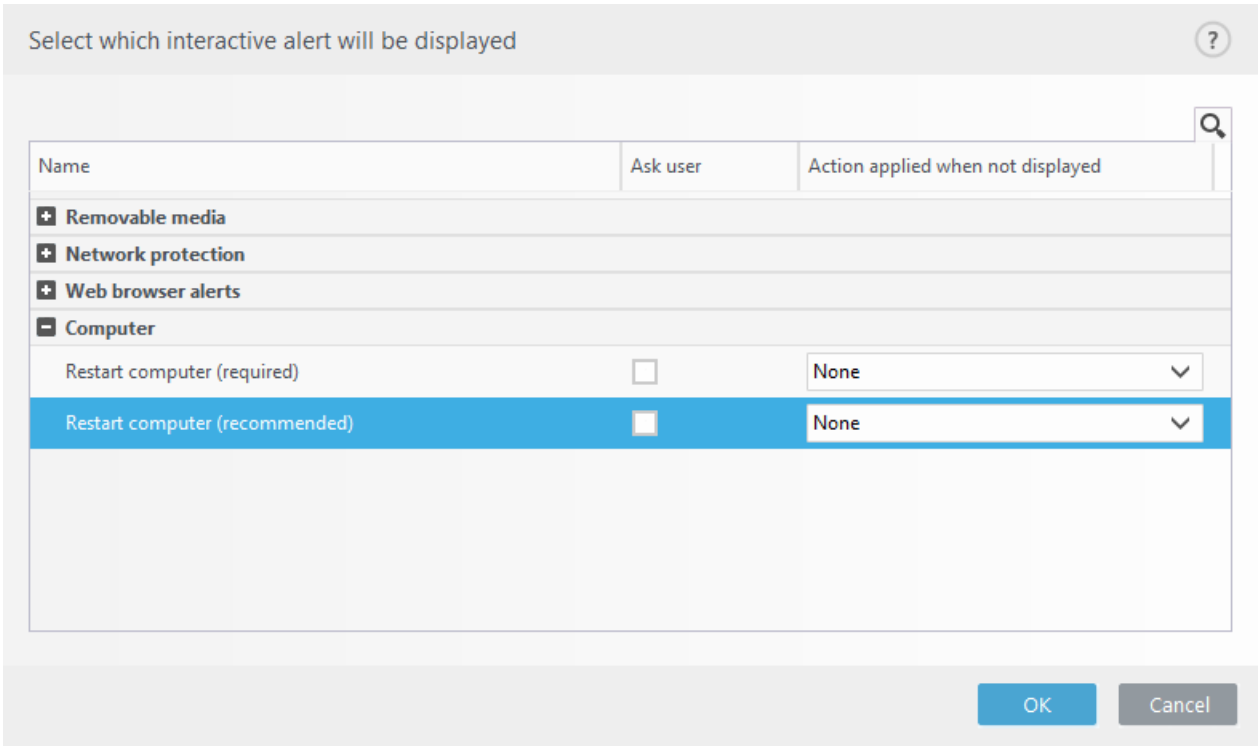


Odporúča sa reštart

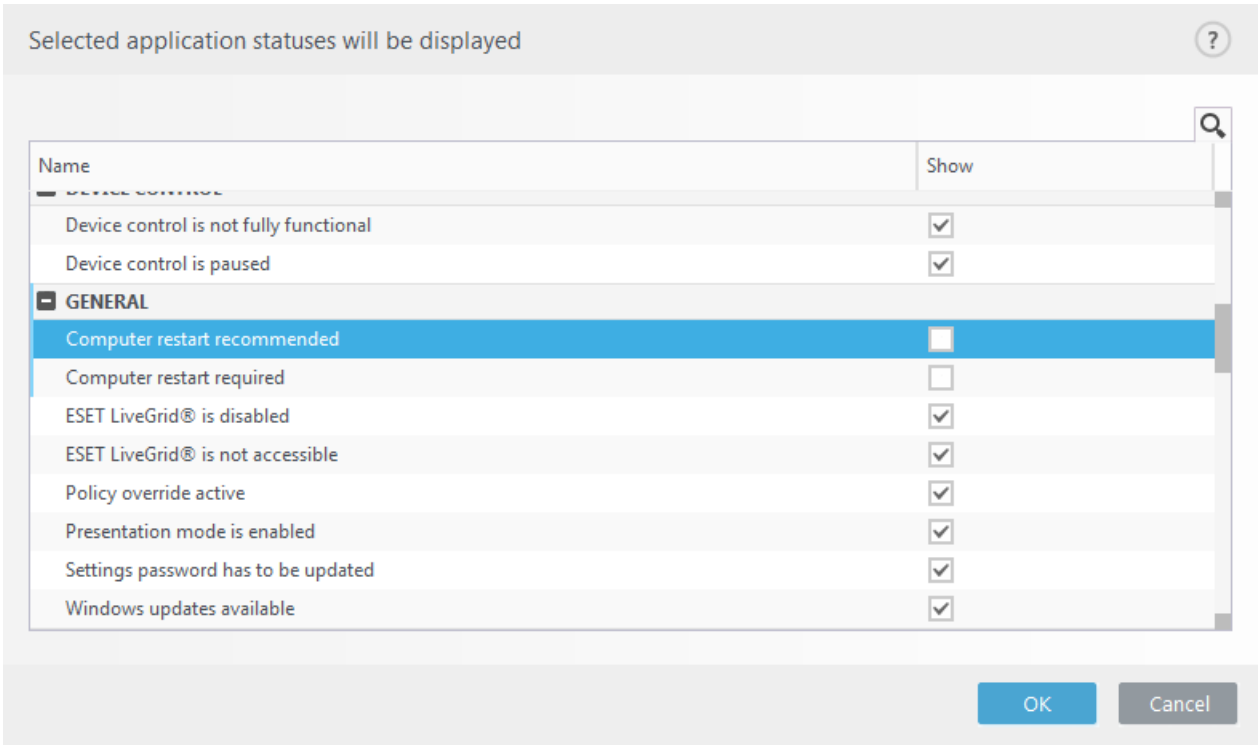
Ak sa na koncových pracovných staniciach zobrazuje žlté upozornenie „Odporúča sa reštart“, máte možnosť zobrazovanie týchto upozornení vypnúť.

Ak chcete vypnúť zobrazovanie upozornení „Vyžaduje sa reštart“ a „Odporúča sa reštart“, postupujte podľa nasledujúcich krokov:

1. Stlačte kláves **F5** pre otvorenie okna Rozšírených nastavení a rozbaľte sekciu **Upozornenia a okná správ**.
2. Kliknite na možnosť **Upraviť** vedľa položky **Zoznam interaktívnych upozornení**. V sekcii **Počítač** zrušte označenie políčok **Reštartovať počítač (povinné)** a **Reštartovať počítač (odporúčané)**.



3. V oboch otvorených oknách kliknite na tlačidlo **OK** pre uloženie zmien.
4. Príslušné upozornenia sa na koncovej pracovnej stanici už viac nebudú zobrazovať.
5. (Voliteľný krok) Ak chcete vypnúť aj zobrazovanie príslušných stavov v hlavnom okne programu ESET Endpoint Security, v okne so zoznamom stavov aplikácie zrušte označenie políčok **Vyžaduje sa reštart počítača** a **Odporúča sa reštart počítača**.

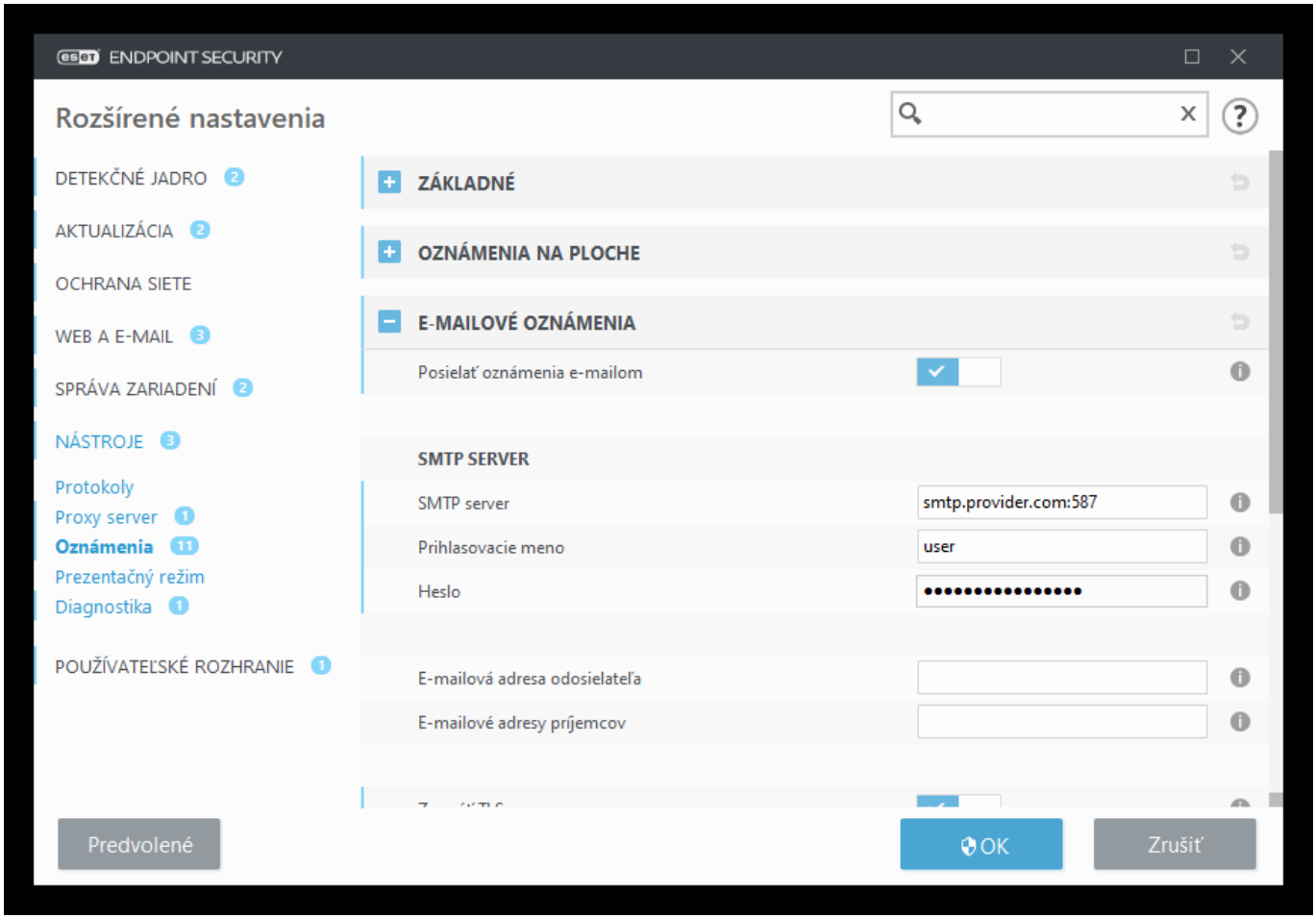


Preposielanie

ESET Endpoint Security podporuje automatické odosielanie e‑mailových oznámení pri výskyte udalostí so zvolenou úrovňou závažnosti. Ak chcete aktivovať posielanie e‑mailových oznámení, otvorte **Rozšírené**

nastavenia > **Oznámenia** > **Preposielanie** > **Preposielať na e‑mail** a zapnite možnosť **Preposielať oznámenia na e‑mail**.

Preposielané oznámenia – vyberte, ktoré oznámenia na ploche sa majú preposielať na e‑mail.



SMTP server

SMTP server – SMTP server, pomocou ktorého budú odosielané oznámenia (napr. *smtp.provider.com:587*, pričom preddefinované číslo portu je 25).

SMTP servery, ktoré využívajú šifrovanie TLS, sú produktom ESET Endpoint Security podporované.

Prihlasovacie meno a heslo – v prípade, že SMTP server vyžaduje overenie, do týchto polí je potrebné zadať platné prihlasovacie meno a heslo pre prístup k SMTP serveru.

E-mailová adresa odosielateľa – toto pole špecifikuje adresu odosielateľa, ktorá bude zobrazená v hlavičke e-mailovej správy s oznámením.

E-mailové adresy príjemcov – toto pole špecifikuje adresy príjemcov, ktoré budú zobrazené v hlavičke e-mailovej správy s oznámením. Na oddelenie viacerých e-mailových adries použite bodkočiarku (;).

Zapnúť TLS – táto možnosť zapne odosielanie upozornení a oznámení s podporou šifrovania typu TLS.

Nastavenia e-mailu

V roletovom menu **Posielať udalosti od úrovne** je možné nastaviť minimálnu úroveň závažnosti oznámení, ktoré majú byť prostredníctvom e-mailu odosielané.

- **Diagnostické** – zaznamenávané budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informatívne** – zaznamenávané budú informatívne správy, napríklad o neobvyklých sieťových aktivitách alebo o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Upozornenia** – zaznamenávané budú kritické chyby a upozornenia (Anti-Stealth nepracuje správne alebo zlyhala aktualizácia).
- **Chyby** – zaznamenávané budú chyby (ochrana dokumentov nie je spustená) a kritické chyby.
- **Kritické** – zaznamenávané budú len kritické chyby (nespustenie antivírusovej ochrany, infikovaný systém atď.).

Posielať každé oznámenie v samostatnom e-maile – každé oznámenie bude odoslané v samostatnom e-maile. Výsledkom môže byť veľký počet prijatých e-mailov za krátky čas.

Interval, po ktorom sa budú e-mailom posielať nové oznámenia (v min.) – časový interval v minútach, po ktorom budú nové oznámenia posielané na e□mail. Ak zadáte hodnotu 0, oznámenia sa budú odosielať ihneď po ich vytvorení.

Formát správy

Komunikácia medzi programom, vzdialeným používateľom alebo správcom systému je zabezpečená prostredníctvom e-mailov alebo LAN správ (pomocou služby Windows Messenger service). Prednastavený formát upozornení a oznámení je optimálny vo väčšine situácií. V niektorých prípadoch však môže byť potrebné zmeniť formát správ týkajúcich sa udalostí.

Formát správ o udalostiach – formát správ o udalostiach zobrazovaných na vzdialených počítačoch.

Formát správ o hrozbách – správy obsahujúce upozornenia o hrozbách majú preddefinovaný formát. Meniť tento formát sa neodporúča. Môžu však nastať situácie, keď budete potrebovať formát správy zmeniť (napríklad v prípade, že používate systém na automatické spracovanie e□mailov).

Znaková sada – konvertuje e-mailovú správu do ANSI kódovania, ktoré je nastavené v regionálnych nastaveniach systému Windows (napr. windows-1250, Unicode (UTF-8), ACSII 7-bit alebo japončina (ISO-2022-JP)). Výsledkom je, že napríklad znak "á" sa zmení na "a" a neznámy symbol bude označený ako "?".

Použiť Quoted-printable kódovanie – e-mailová správa bude zakódovaná do Quoted-printable ((QP)) formátu, ktorý využíva ASCII znaky, čím sa môžu prostredníctvom e-mailu bezchybne prenášať špeciálne (národné) znaky v 8-bitovom formáte (áéíóú).

Vo formáte správ sa nachádzajú kľúčové slová označené percentom („%“), ktoré sú pri vytváraní správ nahradené zodpovedajúcimi hodnotami. Sú dostupné nasledujúce kľúčové slová:

- **%TimeStamp%** – dátum a čas udalosti.
- **%Scanner%** – modul, ktorý zaznamenal udalosť.
- **%ComputerName%** – názov počítača, na ktorom došlo k udalosti.
- **%ProgramName%** – program, ktorý spôsobil udalosť.
- **%InfectedObject%** – názov škodlivého súboru, e-mailovej správy a pod.
- **%VirusName%** – názov infiltrácie.
- **%Action%** – akcia, ktorá bola vykonaná pre konkrétnu infiltráciu.
- **%ErrorDescription%** – popis chyby, ktorá nesúvisí s vírusom.

Kľúčové slová **%InfectedObject%** a **%VirusName%** sa využívajú iba v upozorneniach týkajúcich sa hrozieb, pričom kľúčové slovo **%ErrorDescription%** sa využíva iba v upozorneniach, ktoré súvisia s určitou udalosťou.

Manažér profilov

Manažér profilov sa v ESET Endpoint Security používa na dvoch miestach – v sekcii **Manuálna kontrola počítača** a v sekcii **Aktualizácia**.

Manuálna kontrola počítača

Preferované nastavenia kontroly je možné uložiť do profilov pre budúce použitie. Odporúčame vám, aby ste vždy vytvorili nový profil (s rôznymi cieľmi kontroly, metódami kontroly a ďalšími parametrami) pre každú pravidelne používanú kontrolu.

Pre vytvorenie nového profilu otvorte okno Rozšírené nastavenia (F5) a kliknite na **Antivírus** > **Manuálna kontrola počítača**, potom na **Upraviť** vedľa **Zoznamu profilov**. V roletovom menu **Manažér profilov** môžete vybrať profil pre túto sieť. Pre objasnenie ako vytvoriť profil kontroly podľa vašich predstáv si pozrite kapitolu Nastavenie parametrov skenovacieho jadra ThreatSense, ktorá obsahuje popis každého parametra kontroly.

> Predpokladajme, že chcete vytvoriť vlastný profil kontroly a čiastočne vám vyhovujú nastavenia predvoleného profilu používaného v prípade funkcie **Skontrolovať váš počítač**. Nechcete však kontrolovať runtime archívy, potenciálne nebezpečné aplikácie a chcete tiež použiť **Prísne liečenie**. Zadajte názov nového profilu do okna **Manažér profilov** a kliknite na možnosť **Pridať**. Označte svoj nový profil v roletovom menu **Aktívny profil**, upravte ostatné parametre tak, aby vám vyhovovali, a profil uložte kliknutím na **OK**.

Aktualizácia

Editor profilov nastavení aktualizácie umožňuje vytvárať nové profily pre aktualizáciu. Používanie iných profilov ako je štandardne nastavený **Môj profil** má význam v prípade, ak sa počítač pripája na aktualizačné servery viacerými spôsobmi.

Príkladom je notebook, ktorý sa pripája v domácej sieti na lokálny server – Mirror, avšak keď je mimo, na cestách, sťahuje si aktualizácie priamo zo serverov spoločnosti ESET. Vtedy je potrebné vytvoriť dva profily. Jeden sa bude pripájať na lokálny server, druhý, cestovný, na servery spoločnosti ESET. Potom už len stačí v sekcii **Nástroje** > **Plánovač** upraviť úlohu pre aktualizáciu. Označte jeden profil ako primárny a druhý ako sekundárny.

Aktualizačný profil – profil, ktorý je momentálne používaný. Je možné ho zmeniť výberom iného profilu z roletového menu.

Zoznam profilov – vytvorte nový profil alebo zmeňte už existujúce profily.

Klávesové skratky

Pre rýchlejšiu navigáciu v ESET Endpoint Security je možné použiť aj nasledujúce klávesové skratky:

Klávesové skratky	Vykonaná akcia
F1	otvorenie pomocníka
F5	otvorenie rozšírených nastavení
Up/Down	navigácia v produkte cez položky
TAB	presúvanie kurzora v rámci okna

Klávesové skratky	Vykonaná akcia
Esc	zatvorenie aktívneho dialógového okna
Ctrl+U	zobrazenie informácie o licencii ESET a vašom počítači (podrobnosti pre technickú podporu)
Ctrl+R	obnovenie prednastavenej veľkosti a umiestnenia okna programu na obrazovke

Diagnostika

Diagnostika poskytuje výpisy zlyhaní procesov ESET (napr. ekrn). Ak aplikácia prestane fungovať, vygeneruje sa výpis. Toto môže vývojárom pomôcť pri diagnostike a oprave rôznych problémov súvisiacich s ESET Endpoint Security.

Kliknite na roletové menu vedľa položky **Typ výpisu** a vyberte jednu z troch dostupných možností:

- Vyberte možnosť **Žiadny**, ak chcete vypnúť túto funkciu.
- **Skrátený** (predvolené) – zaznamená menší súbor užitočných informácií, ktoré môžu pomôcť identifikovať príčinu nečakaného zastavenia aplikácie. Tento druh výpisu môže byť užitočný, keď je obmedzený priestor na disku, avšak vzhľadom na obmedzené množstvo zahrnutých informácií nemusia byť analýzou tohto výpisu objavené chyby, ktoré neboli priamo spôsobené procesom bežiacim v čase problému.
- **Úplný** – zaznamená celý obsah systémovej pamäte, keď sa aplikácia nečakane zastaví. Kompletný výpis z pamäte môže obsahovať dáta procesov, ktoré bežali v čase, keď bol výpis zozbieraný.

Cieľový priečinok – priečinok, do ktorého sa pri zlyhaní vygeneruje výpis.

Otvoriť diagnostický priečinok – na otvorenie cieľového adresára v novom okne nástroja *Windows Prieskumník* kliknite na **Otvoriť**.

Vytvoriť diagnostický výpis – kliknite na tlačidlo **Vytvoriť** pre vytvorenie diagnostických súborov výpisu v **Cieľovom adresári**.

Vytváranie rozšírených protokolov

Zapnúť rozšírené protokoly antispamového jadra – umožňuje zaznamenávať všetky udalosti, ktoré sa vyskytnú počas antispamovej kontroly. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s Antispamovým jadrom ESET.

Zapnúť rozšírené protokoly kontroly počítača – umožňuje zaznamenávať všetky udalosti, ku ktorým dôjde počas kontroly súborov a priečinkov Kontrolou počítača alebo Rezidentnou ochranou súborového systému.

Zapnúť rozšírené protokoly správy zariadení – umožňuje zaznamenávať všetky udalosti modulu Správa zariadení. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace so Správou zariadení.

Zapnúť rozšírené protokoly Direct Cloud – umožňuje zaznamenávať všetku komunikáciu produktu so servermi Direct Cloud.

Zapnúť rozšírené protokoly ochrany dokumentov – umožňuje zaznamenávať všetky udalosti modulu Ochrana dokumentov. Toto pomôže vývojárom diagnostikovať a opraviť problémy súvisiace s touto súčasťou programu.

Zapnúť rozšírené protokoly jadra – umožňuje zaznamenávať všetky udalosti, ku ktorým dochádza v jadre produktu ESET (ekrn), čo pomôže pri diagnostike a riešení problémov (dostupné vo verzii 7.2 a novších).

Zapnúť rozšírené protokoly licencovania – umožňuje zaznamenávať všetku komunikáciu produktu s aktivačnými a ESET Business Account servermi spoločnosti ESET.

Zapnúť sledovanie pamäte – umožňuje zaznamenávať všetky udalosti, ktoré pomôžu vývojárom diagnostikovať úniky pamäte.

Zapnúť rozšírené protokoly ochrany siete – umožňuje zaznamenávať všetky sieťové dáta prechádzajúce firewallom vo formáte PCAP. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa firewallu.

Zapnúť rozšírené protokoly operačného systému – budú zozbierané dodatočné informácie o operačnom systéme, ako sú spustené procesy, aktivita procesora a operácie disku. Toto môže pomôcť pri diagnostike a oprave problémov produktov ESET spustených na vašom operačnom systéme.

Zapnúť rozšírené protokoly filtrovania protokolov – umožňuje zaznamenávať všetky dáta prechádzajúce jadrom filtrovania protokolov vo formáte PCAP. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s filtrovaním protokolov.

Zapnúť rozšírené protokoly push správ – umožňuje zaznamenávať všetky udalosti, ku ktorým dôjde pri zasielaní push správ, čo pomôže pri diagnostike a riešení problémov.

Zapnúť rozšírené protokoly rezidentnej ochrany súborového systému – umožňuje zaznamenávať všetky udalosti rezidentnej ochrany súborového systému, čo pomôže pri diagnostike a riešení problémov.

Zapnúť rozšírené protokoly zabezpečeného prehliadača – umožňuje zaznamenávať všetky udalosti, ktoré sa týkajú zabezpečeného prehliadača. Toto pomôže vývojárom diagnostikovať a opraviť problémy.

Zapnúť rozšírené protokoly aktualizačného jadra – umožňuje zaznamenávať všetky udalosti, ktoré sa vyskytnú počas procesu aktualizácie. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s aktualizačným jadrom.

Zapnúť rozšírené protokoly webovej kontroly – umožňuje zaznamenávať všetky udalosti modulu Webovej kontroly. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy súvisiace s Webovou kontrolou.

Umiestnenie protokolov

C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

Modul kontroly cez príkazový riadok

Antivírusový modul programu ESET Endpoint Security je možné spustiť cez príkazový riadok – manuálne (príkazom „ecls“) alebo pomocou súboru typu „bat“.

Spustenie kontroly ESET cez príkazový riadok:

```
ecls [MOŽNOSTI..] SÚBORY..
```

Pri spúšťaní manuálnej kontroly cez príkazový riadok môžete použiť niekoľko parametrov a prepínačov:

Možnosti

/base-dir=PRIEČINOK	načítať moduly z PRIEČINKA
/quar-dir=PRIEČINOK	umiestniť PRIEČINOK do karantény
/exclude=MASKA	vylúčiť z kontroly súbory zodpovedajúce MASKE
/subdir	kontrolovať podpriečinky (predvolené)
/no-subdir	nekontrolovať podpriečinky
/max-subdir-level=ÚROVEŇ	podpriečinky kontrolovať len do určitej úrovne
/symlink	sledovať symbolické prepojenia (predvolené)
/no-symlink	preskočiť symbolické prepojenia
/ads	kontrolovať ADS (predvolené)
/no-ads	nekontrolovať ADS
/log-file=SÚBOR	zapísať výstup do SÚBORU
/log-rewrite	prepísať výstupný súbor (predvolene sa dopíše)
/log-console	zapísať výstup do konzoly (predvolené)
/no-log-console	nezapisovať výstup do konzoly
/log-all	zapisovať do protokolu aj neinfikované súbory
/no-log-all	nezapisovať do protokolu neinfikované súbory (predvolené)
/aind	zobraziť indikátor aktivity
/auto	skontrolovať a automaticky vyliečiť všetky lokálne disky

Možnosti kontroly

/files	kontrolovať súbory (predvolené)
/no-files	nekontrolovať súbory
/memory	kontrolovať pamäť
/boots	kontrolovať zavádzacie sektory
/no-boots	nekontrolovať zavádzacie sektory (predvolené)
/arch	kontrolovať archívy (predvolené)
/no-arch	nekontrolovať archívy
/max-obj-size=VEĽKOSŤ	kontrolovať len súbory menšie ako VEĽKOSŤ megabajtov (predvolene 0 = neobmedzené)
/max-arch-level=ÚROVEŇ	podradené archívy kontrolovať len do danej úrovne hĺbky
/scan-timeout=LIMIT	archívy kontrolovať najviac po daný LIMIT sekúnd
/max-arch-size=VEĽKOSŤ	kontrolovať len súbory v archíve menšie ako daná VEĽKOSŤ (predvolene 0 = neobmedzené)
/max-sfx-size=VEĽKOSŤ	kontrolovať len súbory v samorozbaľovacích archívoch menšie ako VEĽKOSŤ megabajtov (predvolene 0 = neobmedzené)
/mail	kontrolovať e-mailové súbory (predvolené)
/no-mail	nekontrolovať e-mailové súbory
/mailbox	kontrolovať e-mailové schránky (predvolené)

/no-mailbox	nekontrolovať e-mailové schránky
/sfx	kontrolovať samorozbaľovacie archívy (predvolené)
/no-sfx	nekontrolovať samorozbaľovacie archívy
/rtp	kontrolovať runtime archívy (predvolené)
/no-rtp	nekontrolovať runtime archívy
/unsafe	kontrolovať potenciálne nebezpečné aplikácie
/no-unsafe	nekontrolovať potenciálne nebezpečné aplikácie (predvolené)
/unwanted	kontrolovať potenciálne nechcené aplikácie
/no-unwanted	nekontrolovať potenciálne nechcené aplikácie (predvolené)
/suspicious	kontrolovať podozrivé aplikácie (predvolené)
/no-suspicious	nekontrolovať podozrivé aplikácie
/pattern	používať signatúry (predvolené)
/no-pattern	nepoužívať signatúry
/heur	zapnúť heuristiku (predvolené)
/no-heur	vypnúť heuristiku
/adv-heur	zapnúť pokročilú heuristiku (predvolené)
/no-adv-heur	vypnúť pokročilú heuristiku
/ext-exclude=PRÍPONY	vylúčiť z kontroly dvojbodkou oddelené PRÍPONY súborov
/clean-mode=REŽIM	použiť REŽIM liečenia infikovaných objektov K dispozícii sú nasledujúce možnosti: • `none` (predvolené) – infikované súbory nebudú automaticky liečené. • `standard` – ecls.exe sa pokúsi infikované súbory automaticky vyliečiť alebo zmazať. • `strict` – ecls.exe sa pokúsi automaticky vyliečiť alebo zmazať infikované súbory bez zásahu používateľa (pred vymazaním súborov sa používateľovi nezobrazí výzva na potvrdenie akcie). • `rigorous` – ecls.exe vymaže infikované súbory bez predchádzajúceho pokusu o liečenie, a to bez ohľadu na druh súboru. • `delete` – ecls.exe odstráni infikované súbory bez toho, aby sa najskôr pokúsil ich vyliečiť, nevymaže však citlivé súbory ako napríklad systémové súbory Windows.
/quarantine	uložiť infikované súbory (pri liečení) do karantény (doplnková akcia pri liečení súborov)
/no-quarantine	neukladať kópie infikovaných súborov do karantény

Všeobecné možnosti

/help	zobraziť pomocníka a ukončiť
/version	zobraziť informáciu o verzii a ukončiť
/preserve-time	zachovať čas posledného prístupu

Výstupné kódy

0	nenašla sa žiadna hrozba
1	našla sa hrozba, ale bola odstránená

10	niektoré súbory nemohli byť skontrolované (a môže ísť o hrozbu)
50	našla sa hrozba
100	chyba

Výstupné kódy väčšie ako 100 znamenajú, že súbor nebol skontrolovaný, a teda môže byť infikovaný.

ESET CMD

Táto funkcia umožňuje používať pokročilé príkazy ecmd. Poskytuje vám možnosť exportovať a importovať nastavenia pomocou príkazového riadka (ecmd.exe). Doposiaľ bolo možné exportovať nastavenia len prostredníctvom grafického používateľského rozhrania. Nastavenia programu ESET Endpoint Security môžu byť exportované ako súbor *.xml*.

Po aktivovaní funkcie ESET CMD sú k dispozícii dve metódy autorizácie:

- **Žiadna** – žiadna autorizácia. Túto metódu neodporúčame, pretože umožňuje importovanie akejkoľvek nepodpísanej konfigurácie, čo môže predstavovať potenciálne riziko.
- **Heslo pre prístup k rozšíreným nastaveniam** – import konfigurácie zo súboru *.xml* bude možný, len ak je daný súbor podpísaný s použitím príslušného hesla (pozrite si sekciu týkajúcu sa podpisovania konfiguračných súborov *.xml* uvedenú nižšie). Táto metóda autorizácie overuje heslo počas importovania konfigurácie s cieľom zistiť, či je dané heslo zhodné s heslom zadaným v sekcii Nastavenia prístupu. Ak nemáte nastavenú ochranu prístupu pomocou hesla, heslá sa nezhodujú alebo konfiguračný súbor *.xml* nie je podpísaný, konfigurácia nebude importovaná.

S aktívnou funkciou ESET CMD môžete na import/export konfigurácie programu ESET Endpoint Security používať príkazový riadok. Príkazy môžete spúšťať manuálne alebo si vytvoriť skript na účely automatizácie.

Pre použitie pokročilých ecmd príkazov musíte mať oprávnenia správcu, resp. príkazový riadok systému Windows (cmd) spustiť pomocou možnosti **Spustiť ako správca**. V opačnom prípade sa zobrazí chybové hlásenie **Error executing command**. Pri exportovaní konfigurácie musí tiež existovať cieľový priečinok. Export je možný aj v prípade, že funkcia ESET CMD je v nastaveniach vypnutá.

Pokročilé ecmd príkazy možno spúšťať len lokálne. Pozastavenie ecmd príkazov je možné len prostredníctvom klientskej úlohy **Spustiť príkaz** pomocou konzoly ESET PROTECT.

Konfiguráciu z nainštalovaného produktu vyexportujete príkazom:
`ecmd /getcfg c:\config\settings.xml`

Konfiguráciu do nainštalovaného produktu naimportujete príkazom:
`ecmd /setcfg c:\config\settings.xml`

Ako podpísať konfiguračný súbor *.xml*:

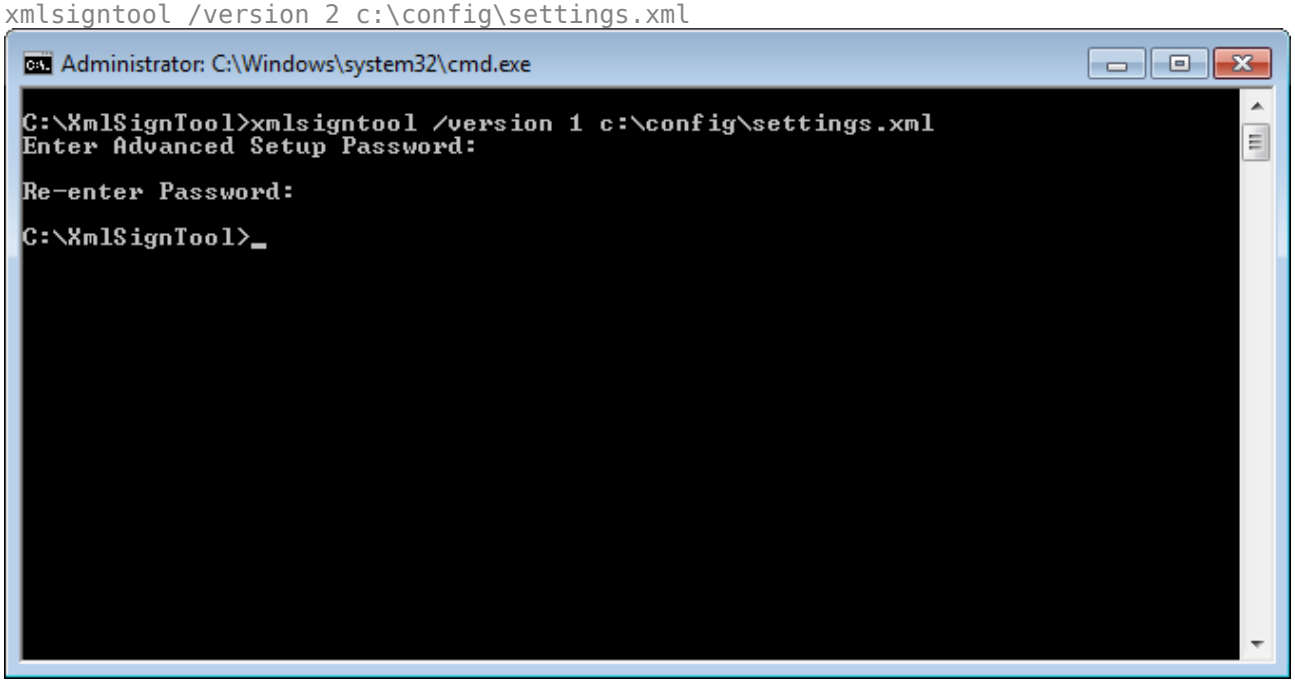
1. Stiahnite si nástroj XmlSignTool.
2. Otvorte príkazový riadok systému Windows (cmd) použitím možnosti **Spustiť ako správca**.
3. Prejdite do priečinka, do ktorého ste uložili spustiteľný súbor `xmlsigntool.exe`.
4. Konfiguračný súbor *.xml* podpíšte nasledujúcim príkazom: `xmlsigntool /version 1|2 <xml_file_path>`

Hodnota parametru `/version` závisí od verzie vášho programu ESET Endpoint Security. Pre produktové verzie 7 a novšie použite parameter s hodnotou `/version 2`.

5. Po výzve nástroja XmlSignTool zadajte heslo, ktoré máte nastavené v produkte pre ochranu prístupu do Rozšírených nastavení. Váš konfiguračný súbor *.xml* je teraz podpísaný a môžete ho prostredníctvom ESET CMD importovať v rámci ďalšej inštalácie ESET Endpoint Security s využitím autorizácie heslom.

Vyexportovaný konfiguračný súbor podpíšete týmto príkazom:

```
xmlsigntool /version 2 c:\config\settings.xml
```



Ak sa zmení heslo pre prístup k nastaveniam, ktoré ste zadali v sekcii Nastavenia prístupu, a chcete do produktu naimportovať konfiguračný súbor, ktorý bol podpísaný už skôr pomocou starého hesla, bude potrebné daný konfiguračný súbor *.xml* najskôr opätovne podpísať pomocou vášho nového hesla. Týmto spôsobom môžete použiť a importovať aj starší konfiguračný súbor bez nutnosti ho najskôr exportovať na iný počítač s programom ESET Endpoint Security.

Aktivovanie ESET CMD bez zvolenia spôsobu autorizácie sa neodporúča, nakoľko sa týmto umožní import akejkoľvek nepodpísanej konfigurácie. Aby ste predišli neoprávneným zmenám zo strany používateľov, nastavte heslo v sekcii **Rozšírené nastavenia** > **Používateľské rozhranie** > **Nastavenia prístupu**.

Zoznam ecmd príkazov

Jednotlivé bezpečnostné funkcie môžu byť zapnuté a dočasne vypnuté z ESET PROTECT pomocou klientskej úlohy Spustiť príkaz. Príkazy neprepisujú nastavenia vynútené politikou a všetky dočasne vypnuté nastavenia sa vrátia späť do pôvodného stavu po spustení príkazu alebo po reštarte zariadenia. Pre použitie ecmd príkazu zadajte pri vytváraní úlohy do príslušného poľa jeho presné znenie.

V tabuľke nižšie nájdete súhrnný prehľad dostupných príkazov podľa jednotlivých bezpečnostných funkcií:

Bezpečnostná funkcia	Príkaz na dočasné pozastavenie	Príkaz na zapnutie
Rezidentná ochrana súborového systému	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
Ochrana dokumentov	ecmd /setfeature document pause	ecmd /setfeature document enable
Správa zariadení	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
Prezentačný režim	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
Technológia Anti-Stealth	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
Firewall	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
Ochrana pred sieťovými útokmi (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
Ochrana pred botnetmi	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Webová kontrola	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Ochrana prístupu na web	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
Ochrana e□mailových klientov	ecmd /setfeature email pause	ecmd /setfeature email enable
Antispamová ochrana	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
Antiphishingová ochrana	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

Detekcia stavu nečinnosti

Nastavenia detekcie stavu nečinnosti sa nachádzajú v **Rozšírených nastaveniach** v sekcii **Detekčné jadro** > **Detekcia malvéru** > **Kontrola v nečinnosti** > **Detekcia stavu nečinnosti**. Tieto nastavenia špecifikujú spúšťač pre kontrolu v nečinnosti, keď:

- je spustený šetrič obrazovky,
- počítač je uzamknutý,
- používateľ je odhlásený.

Použite prepínacie tlačidlá pri týchto možnostiach pre zapnutie alebo vypnutie daných spúšťačov kontroly v nečinnosti.

Import a export nastavení

V rámci sekcie **Nastavenia** môžete importovať alebo exportovať nastavenia programu ESET Endpoint Security z/do súboru .xml.

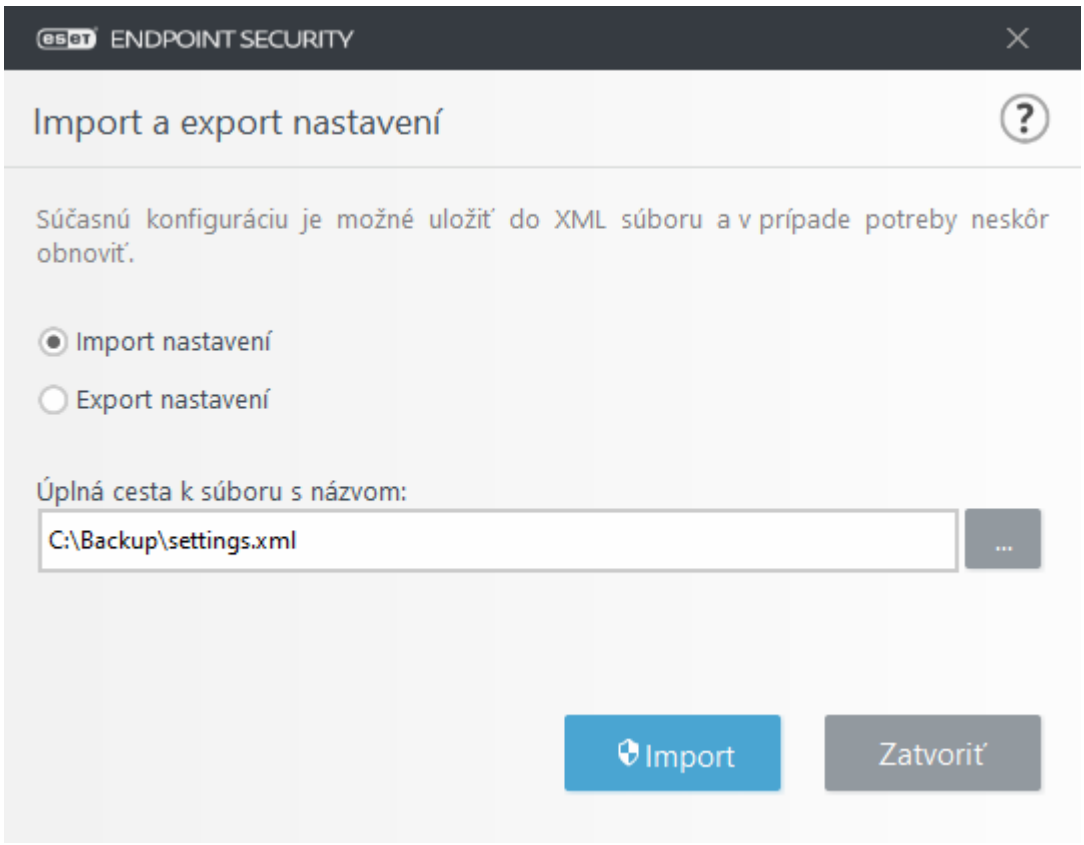
Importovanie a exportovanie konfiguračných súborov je potrebné napríklad pri zálohovaní nastavení ESET Endpoint Security, ku ktorým sa chce používateľ neskôr vrátiť. Export nastavení určite ocenia aj tí, ktorí jednotné nastavenia potrebujú použiť na viacerých počítačoch, kde do nainštalovaného programu jednoducho importujú súbor .xml s nastaveniami.

Import nastavení je veľmi jednoduchý. V hlavnom okne programu kliknite na **Nastavenia**, ďalej na **Import/export nastavení** a vyberte možnosť **Import nastavení**. Zadajte názov konfiguračného súboru alebo kliknite na tlačidlo **...** pre vyhľadanie a označenie súboru, ktorý chcete importovať.

Export nastavení má podobný postup ako import. V hlavnom okne programu kliknite na **Nastavenia** a potom na **Import/export nastavení**. Vyberte možnosť **Export nastavení** a zadajte názov konfiguračného súboru (napríklad

export.xml). Potom pomocou prieskumníka zvoľte miesto na disku, kam chcete súbor s nastaveniami uložiť.

Pri exporte nastavení sa môže objaviť chybové hlásenie, ak nemáte potrebné práva na zápis do príslušného adresára.



Všetky nastavenia zmeniť na predvolené

Kliknite na možnosť **Predvolené** v okne Rozšírených nastavení (F5) pre vrátenie všetkých nastavení programu a modulov na predvolené hodnoty. Nastavenia budú obnovené do stavu, ktorý mali po inštalácii.

Prezrite si aj kapitolu Import a export nastavení.

Vrátiť späť predvolené nastavenia v tejto sekcii

Kliknite na ikonu spätnej šípky ⍰, ak si želáte všetky nastavenia v aktuálne zobrazenej sekcii vrátiť späť na predvolené hodnoty.

Majte na pamäti, že kliknutím na **Vrátiť späť na predvolené** sa všetky vami vykonané zmeny stratia.

Vrátiť späť obsah tabuliek – po zvolení tejto možnosti sa stratia manuálne aj automaticky pridané pravidlá, úlohy a profily.

Prezrite si aj kapitolu Import a export nastavení.

Chyba pri ukladaní nastavení

Toto chybové hlásenie indikuje, že nastavenia neboli uložené správne a vyskytla sa chyba.

Zvyčajne to znamená, že používateľ, ktorý sa pokúsil zmeniť parametre programu:

- má nedostatočné prístupové práva alebo nemá potrebné oprávnenia pre operačný systém, aby mohol upravovať konfiguračné súbory a systémovú databázu Registry.
  > Pre vykonanie požadovaných zmien sa musí prihlásiť správca systému.
- nedávno povolil Učiaci sa režim v HIPS alebo firewalle a pokúsil sa vykonať zmeny v Rozšírených nastaveniach.
  > Aby sa uložili vaše nastavenia a vyhli ste sa konfliktu konfigurácie, zatvorte okno Rozšírených nastavení bez uloženia a skúste požadované zmeny vykonať znova.

Druhá najčastejšia príčina je, že program nepracuje správne, je poškodený, a preto je ho potrebné preinštalovať.

Vzdialený monitoring a správa

Remote Monitoring and Management (RMM) je proces vzdialeného monitorovania a ovládania softvérových systémov pomocou agenta inštalovaného na koncové zariadenia. Bezpečnostné produkty spoločnosti ESET určené pre firmy podporujú RMM prostredníctvom nástrojov tretích strán.

ERMM – ESET plugin pre RMM

- Súčasťou predvolenej inštalácie ESET Endpoint Security je aj súbor `ermm.exe`, ktorý sa nachádza v adresári daného produktu:
  C:\Program Files\ESET\ESET Security\ermm.exe
- `ermm.exe` je nástroj príkazového riadka vyvinutý na umožnenie správy bezpečnostných produktov pre koncové zariadenia a komunikácie s akýmkoľvek RMM pluginom.
- `ermm.exe` zabezpečuje výmenu dát s RMM pluginom, ktorý komunikuje s RMM agentom prepojeným s RMM serverom. Predvolene je nástroj ESET RMM vypnutý.

Ďalšie zdroje

- Príkazový riadok pre vzdialený monitoring a správu (ERMM)
- Zoznam ERMM JSON príkazov
- Ako aktivovať vzdialené monitorovanie a správu v ESET Endpoint Security

ESET Direct Endpoint Management pluginy pre RMM riešenia tretích strán

RMM server beží ako služba na serveri tretej strany. Ďalšie informácie nájdete v nasledujúcich online používateľských príručkách ESET Direct Endpoint Management:

- ESET Direct Endpoint Management plugin pre ConnectWise Automate
- ESET Direct Endpoint Management plugin pre DattoRMM

- ESET Direct Endpoint Management pre Solarwinds N-Central
- ESET Direct Endpoint Management pre NinjaRMM

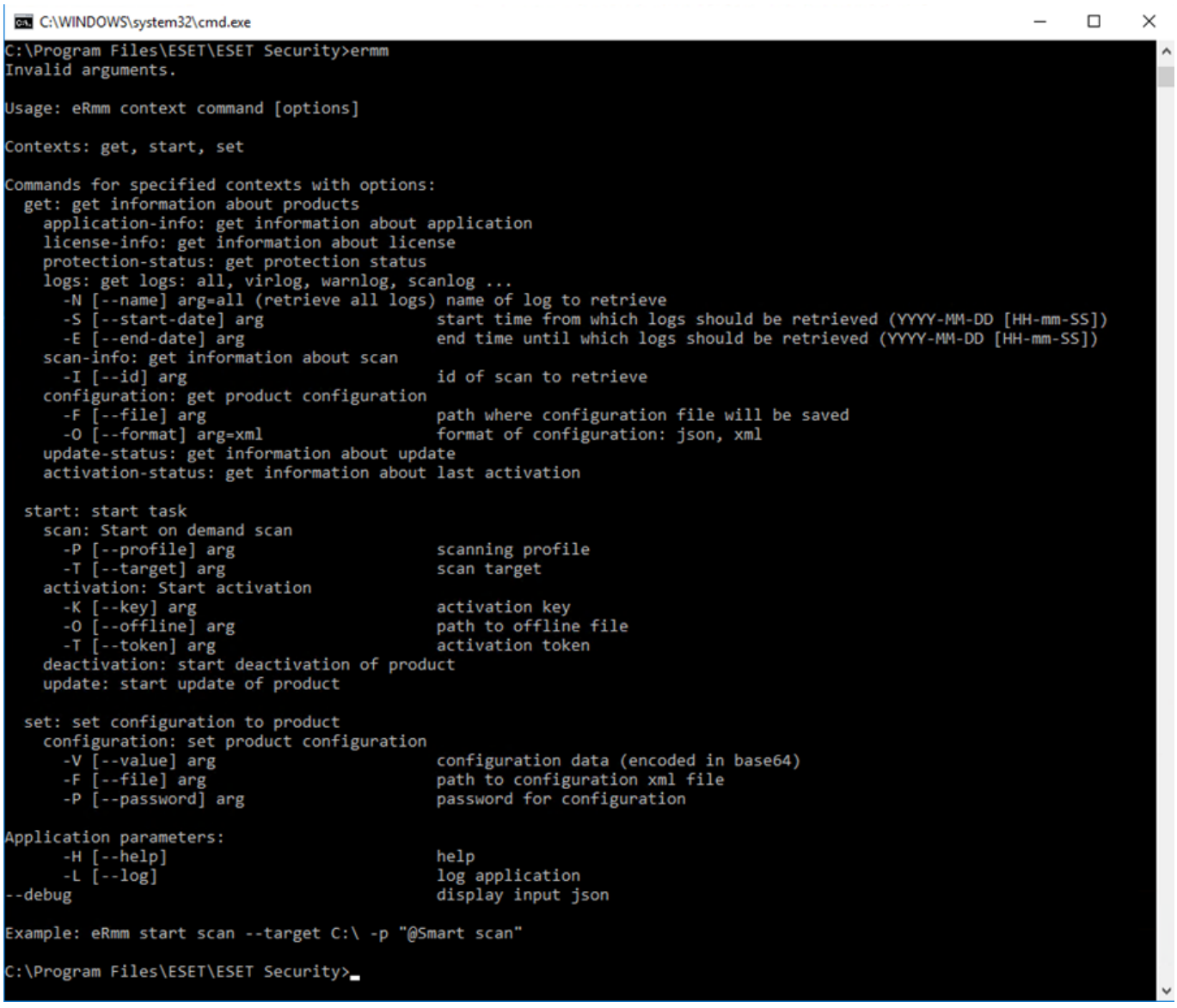
Príkazový riadok pre vzdialený monitoring a správu (ERMM)

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

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

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

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands

syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

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

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

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

Zoznam ERMM JSON príkazov

- get protection-status
- get application-info
- get license-info
- get logs
- get activation-status
- get scan-info

- get configuration
- get update-status
- start scan
- start activation
- start deactivation
- start update
- set configuration

get protection-status

Get the list of application statuses and the global application status

Command line

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

Parameters

None

Example

call

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

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```

get application-info

Get information about the installed application

Command line

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

Parameters

None

Example

call

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

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

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

Parameters

None

Example

call

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

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```

get logs

Get logs of the product

Command line

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

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call

```
{
"command":"get_logs",
"id":1,
"version":"1",
"params":{
"name":"warnlog",
"start_date":"2017-04-04 06-00-00",
"end_date":"2017-04-04 12-00-00"
}
}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```

get activation-status

Get information about the last activation. Result of status can be {

success, running, failure }

Command line

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

Parameters

None

Example

call

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

result

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

get scan-info

Get information about running scan.

Command line

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

Parameters

None

Example

call

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

result


```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```


get configuration

Get the product configuration. Result of status may be { success, error }

Command line

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

Parameters

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

Example

call

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

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```

get update-status

Get information about the update. Result of status may be { success, error }

Command line

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

Parameters

None

Example

call

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

result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```

start scan

Start scan with the product

Command line

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

Parameters

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

Example

call

```
{
"command":"start_scan",
"id":1,
"version":"1",
"params":{
"profile":"Smart scan",
"target":"c:\\"
}
}
```

result

```
{
"id":1,
"result":{
"task_id":458752
},
"error":null
}
```

start activation

Start activation of product

Command line

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

Parameters

Name	Value

key	Activation key
offline	Path to offline file

Example

call

```
{
"command":"start_activation"
"id":1,
"version":"1",
"params":{
"key":"XXXX-XXXX-XXXX-XXXX-XXXX"
}
}
```

result

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

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

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

result

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

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

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

result

```
{
"id":1,
"result":{
},
"error":{
"id":4,
"text":"Task already running."
}
}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

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

Parameters

Name	Value
file	the path where the configuration file will be saved

password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

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

result

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

Časté otázky

Táto kapitola obsahuje niektoré z najčastejšie sa vyskytujúcich otázok a problémov, s ktorými sa môžete stretnúť. Kliknutím na tému zobrazíte návod na vyriešenie problému:

- Ako aktualizovať ESET Endpoint Security
- Ako aktivovať ESET Endpoint Security
- Ako aktivovať nový produkt s pôvodnými prihlasovacími údajmi
- Ako odstrániť vírus z počítača
- Ako povoliť komunikáciu pre určitú aplikáciu
- Ako vytvoriť novú úlohu v Plánovači
- Ako naplánovať pravidelnú týždňovú kontrolu počítača
- Ako spravovať oznámenia a interaktívne upozornenia
- Ako pripojiť produkt k programu ESET PROTECT
  – Ako používať Režim prepísania
  – Ako aplikovať odporúčané politiky pre ESET Endpoint Security
- Ako nastaviť funkciu mirror
- Ako prejsť na Windows 10 s nainštalovaným produktom ESET Endpoint Security
- Ako aktivovať vzdialený monitoring a správu produktu (RMM)
- Ako blokovať stiahnutie určitých typov súborov z internetu
- Ako minimalizovať používateľské rozhranie programu ESET Endpoint Security

Ak nie je váš problém zahrnutý v tomto zozname, skúste hľadať podľa kľúčového slova alebo frázy, ktorá popisuje váš problém, v pomocníkovi programu ESET Endpoint Security.

Ak nenájdete riešenie svojho problému v pomocníkovi, môžete vyskúšať našu pravidelne aktualizovanú Databázu znalostí spoločnosti ESET, kde sa nachádzajú rôzne riešenia a návody.

- Ako ochrániť počítač pred škodlivým softvérom Filecoder (ransomvér)
- Najčastejšie otázky týkajúce sa produktov ESET Endpoint Security a ESET Endpoint Antivirus
- Ktoré porty a adresy treba povoliť, ak používam firewall od iného výrobcu?

Ak vám pomocník programu ani znalostná databáza nepomohli, môžete sa obrátiť na technickú podporu spoločnosti ESET. Kontaktný formulár možno nájsť v časti **Pomocník a podpora** v hlavnom okne programu.

Časté otázky o automatických aktualizáciách

Viac informácií o aktualizáciách produktu ESET Endpoint Security si môžete prečítať v Databáze znalostí:
- Aké rozličné typy aktualizácií a vydaní produktov ESET existujú?

Budú sa počítače aktualizovať automaticky? Stiahne sa aktualizácia pred reštartom alebo až po ňom?

Aktualizácia sa stiahne pred reštartom a v tejto fáze sa pripravia aj aktualizované súbory. Po reštarte sú aktualizované súbory stále len pripravené na použitie, pričom aktuálne nainštalovaná verzia poskytuje nepretržitú ochranu. Zmeny sa prejavia po ďalšom spustení produktu ESET určeného na ochranu koncového zariadenia.

Mám približne 3 000 počítačov. Budú všetky sťahovať aktualizácie v rovnakom čase? Môžem na automatické aktualizácie pre toľko počítačov využiť proxy?

ESET ponúka nástroj Mirror Tool a proxy riešenia pre veľké siete, z čoho vyplýva, že aktualizácie sa z internetu stiahnu len raz a potom sa distribuujú lokálne. Aktualizácie sú menšie, zvyčajne 5 až 10 MB a ESET obmedzuje aktualizácie počas prvých týždňov ich dostupnosti. Vďaka tomu nenastane hromadné, ale postupné sťahovanie aktualizácií všetkými klientmi, ktorí sú priamo pripojení na servery ESET.

Môžem rozhodnúť, koľko počítačov alebo ktoré z nich sa budú automaticky aktualizovať? Nechcem sťahovať aktualizácie na viac než desiatich počítačoch za hodinu alebo chcem teraz aktualizovať len desať počítačov a ďalšie až po niekoľkých dňoch.

V spravovaných prostrediach sa dá nastaviť politika automatickej aktualizácie, v rámci ktorej môžete určiť najnovšiu požadovanú verziu. Podporované sú aj zástupné znaky (napríklad 9.0.2032.*). Ďalšie informácie nájdete v kapitole Automatické aktualizácie na stránkach Online pomocníka pre ESET PROTECT a ESET PROTECT Cloud. Žiaľ, v súčasnosti nie sú k dispozícii iné možnosti, ako obmedziť automatické aktualizácie. K viacerým skupinám môžete priradiť viacero politík.

Sú automatické aktualizácie nakonfigurované len prostredníctvom politík? Môžem politiku jednoducho vypnúť, ak nechcem, aby sa produkt ESET aktualizoval?

Pokiaľ ide o rýchlu opravu zabezpečenia a stability, produkt sa aktualizuje aj pri vypnutých automatických aktualizáciách, ako vyplýva z príslušnej Licenčnej dohody s koncovým používateľom. Spoločnosť ESET používa Rýchle opravy zabezpečenia a stability, aby adresovala pálčivé problémy a zaistila najvyššiu mieru ochrany a stability pre váš produkt.

Politiku automatických aktualizácií môžete priradiť k ľubovoľnej skupine koncových zariadení bez ohľadu na ich aktuálnu konfiguráciu automatických aktualizácií. V nespravovanom prostredí môže používateľ lokálne

nakonfigurovať automatické aktualizácie v rozšírených nastaveniach produktu ESET pre koncové zariadenia.

Čo ak nakonfigurujem politiku tak, aby sa používala najskoršia dostupná verzia? Bude aj vtedy ESET aktualizovať moje produkty?

Rýchle opravy a kritické opravy (aktualizácie zaisťujúce bezpečnosť a stabilitu) predstavujú mierne odlišné kategórie aktualizácií. Bežné rýchle opravy sú priradené k automatickým aktualizáciám so štandardnou prioritou, pričom sa akceptujú používateľské nastavenia. Kritické opravy sú aplikované s najvyššou prioritou bez ohľadu na používateľské nastavenia.

Ako prebieha automatická aktualizácia v offline prostredí? Kedy používatelia používajú offline repozitár?

Offline repozitár tiež obsahuje súbory .dup a .fup. Časť repozitára sa musí stiahnuť pomocou nástroja Mirror Tool, nie prostredníctvom aktualizácie modulu. Ďalšie informácie nájdete v článku Databázy znalostí spoločnosti ESET.

Ako produkty ESET zistia, že je potrebná aktualizácia? Z repozitára? Odosielajú sa na servery nejaké údaje? Ak ESET plánuje aktualizáciu mesiac po vydaní verzie a pre celý svet, sú na to servery ESET pripravené?

Produkty ESET sťahujú automatické aktualizácie z repozitára. Servery sú na to pripravené, keďže kritické aktualizácie majú len niekoľko KB. Pri kritických aktualizáciách sa neuplatňuje žiadne obmedzovanie na serveroch repozitára. Obmedzovanie na serveroch však možno zapnúť, ak sú automatické aktualizácie väčšie. V nasledujúcej tabuľke sú uvedené príklady veľkosti rýchlych opráv v prípade rozdielovej automatickej aktualizácie:

Predchádzajúca verzia	Nová verzia	Veľkosť
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6,5 MB
8.0.2028.0	9.0.2032.2	11,5 MB

Ak rozdielová automatická aktualizácia z nejakého dôvodu zlyhá, produkt ESET môže spustiť úplnú aktualizáciu. Stále ide o automatickú aktualizáciu so zárukou funkčnosti produktu, ale namiesto súboru .dup sa stiahne väčší súbor .fup. V prípade verzie 9.0.2032.2 má veľkosť 27 MB. Takýto scenár je však zriedkavý.

Bude vydanie aktualizácie pre ESET Endpoint Security alebo ESET Endpoint Antivirus poskytnuté postupne? Ak áno, ako dlho sa aktualizácia po vydaní pozdrží?

ESET obmedzuje aktualizácie počas prvých týždňov ich dostupnosti po vydaní novej verzie s cieľom znížiť zaťaženie našich serverov a rovnomerne rozdistribuovať novú verziu.

Automatické aktualizácie sa stanú jednou z hlavných metód prechodu na novšie verzie. Ako presne fungujú?

Zámerom spoločnosti ESET je, aby automatické aktualizácie využívalo čo najviac našich zákazníkov. Mať v ponuke toľko starších verzií je náročné na podporu. Funkcia automatických aktualizácií funguje jednoducho. Počas prvej

kontroly dostupnosti aktualizácie modulov sa stiahnu súbory .dup. Pri aktualizácii je produkt plne funkčný a po celý čas chráni počítač. Nová verzia sa aktivuje po reštarte. V konzole ESET PROTECT (na strane servera) môžete pomocou politiky určiť najvyššiu verziu, na ktorú chcete produkt aktualizovať. Môžete použiť aj zástupné znaky. Ďalšie informácie nájdete v kapitole Automatické aktualizácie na stránkach Online pomocníka pre ESET PROTECT a ESET PROTECT Cloud.

Je pravda, že automatické aktualizácie fungujú na 10 %? Teraz používam ESET Endpoint Security 8.0.2028.1. Ak sa spustí automatická aktualizácia, na akú verziu sa produkt aktualizuje?

Automatická aktualizácia produktov môže byť oneskorená z dôvodu obmedzovania na serveroch repozitára. Ak je vydaná obmedzovaná aktualizácia produktu, pri automatickej kontrole dostupnosti aktualizácií ju nemusíte získať okamžite. Ak sa aktualizácia považuje za bezpečnú a stabilnú, obmedzovanie sa môže zmierniť alebo úplne zrušiť, aby aktualizáciu získali všetky zostávajúce klienty.

Obmedzovanie je postup, ktorý v prípade jednotlivých aktualizácií môže trvať rôzne dlho. Závisí to od toho, koľko klientov požiada o aktualizáciu, aká je aktivita na našich serveroch a od ďalších faktorov. Tento postup sa neustále vyvíja a mení. Keďže funkcia automatických aktualizácií je nová, budeme tento postup pravdepodobne zdokonaľovať, aby sme zlepšili skúsenosti zákazníkov.

Ak zapnem počítač o 8:45 a vypnem ho o 17:00, kedy sa spustia automatické aktualizácie?

Pri najbližšej naplánovanej aktualizácii modulov, najviac raz za 24 hodín.

Ak sa počítač počas automatickej aktualizácie vypne, kedy sa spustí ďalšia aktualizácia?

Aktualizácia sa spustí v najbližšom naplánovanom čase aktualizácie. Pre postup automatickej aktualizácie (predtým uPCU) existuje spoľahlivý mechanizmus zabezpečenia proti zlyhaniu. Po stiahnutí aktualizácie a reštartovaní počítača sú aktualizované súbory stále pripravené na použitie, pričom aktuálne nainštalovaná verzia poskytuje nepretržitú ochranu. Zmeny sa prejavia po ďalšom spustení produktu ESET určeného na ochranu koncového zariadenia.

Ako môžem spustiť automatické aktualizácie okamžite bez čakania na pravidelné pripojenie každých 24 hodín? Existuje nejaký iný spôsob než pomocou tlačidla Overiť dostupnosť aktualizácií?

Automatickú aktualizáciu môžete vyvolať manuálne len tak, že otvoríte hlavné okno programu a kliknete na **Aktualizácia** > **Overiť dostupnosť aktualizácií**. Všetky ostatné spôsoby vyvolania aktualizácií modulov zodpovedajú politike plánovača 24-hodinových automatických aktualizácií. V súčasnosti nie je možné spustiť sťahovanie automatických aktualizácií na diaľku. Túto funkciu plánujeme pridať v budúcnosti.

Ako aktualizovať ESET Endpoint Security

Aktualizácia produktu ESET Endpoint Security môže byť vykonaná manuálne alebo automaticky. Na spustenie aktualizácie prejdite do sekcie **Aktualizácia** v hlavnom okne programu a následne kliknite na **Overiť dostupnosť aktualizácií**.

Na základe predvolených nastavení inštalácie je vytvorená úloha v plánovači, ktorá spúšťa automatickú aktualizáciu každú hodinu. Ak chcete zmeniť tento interval, môžete tak urobiť v sekcii **Nástroje** > **Plánovač** (prečítajte si podrobnejšie informácie o Plánovači).

Ako aktivovať ESET Endpoint Security

Po ukončení inštalácie sa zobrazí dialógové okno s výzvou na aktiváciu produktu.

Existuje niekoľko spôsobov, ako aktivovať produkt. Dostupnosť konkrétnych aktivačných scenárov v okne Aktivácia sa môže líšiť v závislosti od krajiny a spôsobu distribúcie (webová stránka spoločnosti ESET, typ inštalátora .msi alebo .exe atď.).

Ak chcete aktivovať ESET Endpoint Security priamo z programu, otvorte hlavné okno programu ESET Endpoint Security a v menu kliknite na **Pomocník a podpora** > **Aktivovať produkt** alebo **Stav ochrany** > **Aktivovať produkt**.

Môžete použiť nasledujúce metódy aktivácie produktu ESET Endpoint Security:

- **Použiť zakúpený licenčný kľúč** – jedinečný reťazec znakov vo formáte XXXX-XXXX-XXXX-XXXX-XXXX, ktorý sa používa na identifikáciu vlastníka licencie a aktiváciu licencie.
- **ESET Business Account** – účet vytvorený na portáli ESET Business Account s prihlasovacími údajmi (e-mailová adresa + heslo). Táto metóda umožňuje spravovať viaceré licencie z jedného miesta.
- **Offline registrácia** – automaticky vygenerovaný súbor, ktorý bude prenesený do vášho produktu ESET s cieľom poskytnúť informácie o vašej licencii. Ak vám licencia povoľuje stiahnutie offline licenčného súboru (koncovka .lf), potom tento súbor môže byť použitý na vykonanie offline aktivácie. Počet offline licencií bude odpočítaný z celkového počtu dostupných licencií. Viac informácií o generovaní offline súboru nájdete v online používateľskej príručke pre nástroj ESET Business Account.

Kliknite na možnosť **Aktivovať neskôr**, ak sa váš počítač nachádza v spravovanej sieti a váš správca vykoná vzdialenú aktiváciu prostredníctvom nástroja ESET PROTECT. Túto možnosť môžete tiež použiť v prípade, že daného klienta chcete aktivovať neskôr.

Ak máte prihlasovacie meno a heslo, ktoré ste používali na aktiváciu starších produktov ESET, a neviete, ako aktivovať ESET Endpoint Security, skonvertujte svoje prihlasovacie údaje na licenčný kľúč.

Neúspešná aktivácia produktu?

Svoju licenciu k produktu môžete kedykoľvek zmeniť. V prípade, že chcete zmeniť licenciu, kliknite v hlavnom okne programu na **Pomocník a podpora** > **Zmeniť licenciu**. Uvidíte verejné identifikačné číslo licencie, ktoré slúži na identifikáciu licencie. Prihlasovacie meno, pod ktorým je váš počítač registrovaný v licenčnom systéme, je zaznamenané v sekcii **O programe**, ktorú otvoríte cez kontextové menu kliknutím pravým tlačidlom myši na ikonu programu v paneli oznámení.

Prostredníctvom ESET PROTECT 7.2 alebo ESET PROTECT 9 je možné produkty na pracovných staniciach aktivovať vzdialene a automaticky (aktivácia prebieha na pozadí, bez oznámení) pomocou licencií sprístupnených správcom. Bližšie inštrukcie nájdete v Online pomocníkovi pre ESET PROTECT.

Zadanie licenčného kľúča počas aktivácie

Pre úplnú funkčnosť programu sú dôležité pravidelné aktualizácie. ESET Endpoint Security bude automaticky dostávať aktualizácie len v tom prípade, že bol úspešne aktivovaný zadaním **Licenčného kľúča**.

Ak ste nezadali licenčný kľúč ihneď po inštalácii, produkt nie je aktivovaný a je teda potrebné ho dodatočne aktivovať. Licenciu je možné zadať v hlavnom okne programu. Prejdite do sekcie **Pomocník a podpora** > **Aktivovať licenciu** a do okna Aktivácia produktu zadajte licenčné údaje, ktoré ste dostali pri zakúpení programu ESET.

Je dôležité, aby ste **licenčný kľúč** zadali presne v tom tvare, v akom je napísaný:

- Licenčný kľúč je jedinečný reťazec znakov vo formáte XXXX-XXXX-XXXX-XXXX-XXXX, ktorý sa používa na identifikáciu vlastníka licencie a aktiváciu licencie.

Odporúčame vám licenčný kľúč skopírovať z registračného e□mailu a vložiť ho do programu, aby ste tak mali istotu, že kľúč je zadaný v presnom tvare.

Prihlásenie do ESET Business Account

Účet bezpečnostného správcu je účet vytvorený na portáli ESET Business Account. Na prihlásenie do účtu je potrebná **e□mailová adresa** a **heslo**. Pomocou tohto účtu vidíte všetky produkty aktivované s vašou licenciou. Účet bezpečnostného správcu tiež povoľuje spravovať viacero licencií. Na vytvorenie účtu kliknite na **Vytvoriť účet** a budete presmerovaný na portál ESET Business Account, kde sa môžete zaregistrovať pomocou svojich prihlasovacích údajov.

Ak ste zabudli svoje heslo, kliknite na možnosť **Zabudol som heslo** a budete presmerovaný na portál ESET Business Account. Zadajte svoju e-mailovú adresu a kliknite na **Prihlásiť sa** pre potvrdenie. Následne vám bude doručený e-mail s inštrukciami, ako obnoviť heslo.

Ako aktivovať nový produkt ESET určený pre koncové zariadenia pomocou starších licenčných údajov

Ak už máte svoje prihlasovacie meno a heslo a chceli by ste ich skonvertovať na licenčný kľúč, navštívte portál ESET Business Account.

Ako odstrániť vírus z počítača

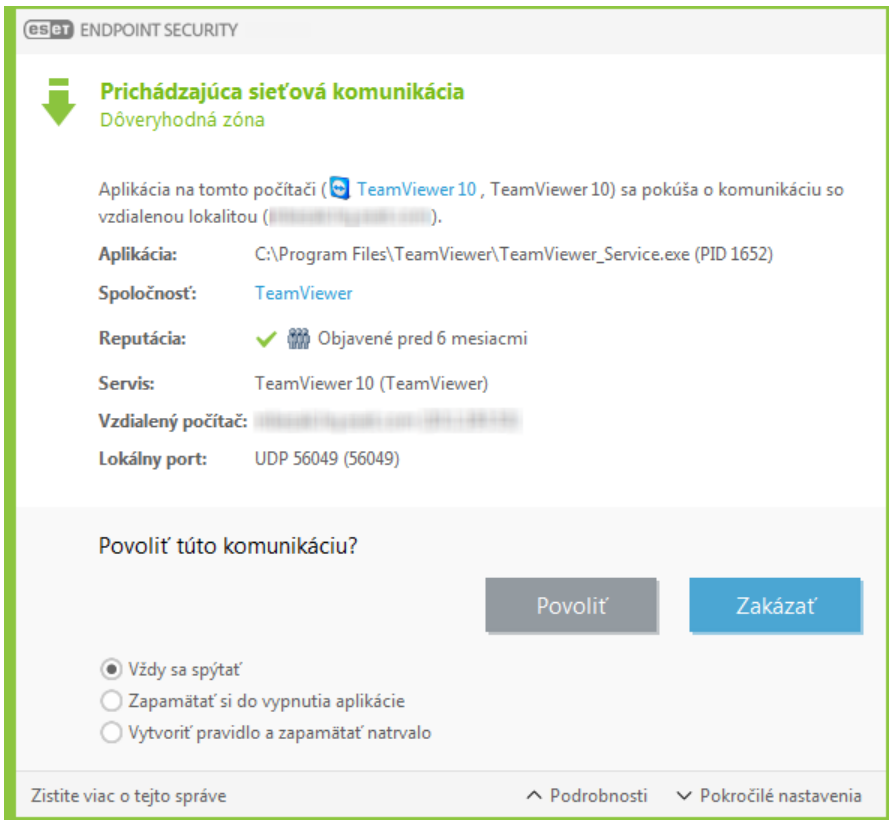
Ak má váš počítač príznaky infekcie škodlivým kódom, tzn. je pomalší, zamŕza a pod., odporúčame nasledovné kroky:

1. V hlavnom okne programu kliknite na **Kontrola počítača**.
2. Kliknutím na možnosť **Smart kontrola** sa spustí kontrola vášho počítača.
3. Po ukončení kontroly si pozrite protokol so zoznamom skontrolovaných, infikovaných a vyliečených súborov.
4. Ak chcete skontrolovať len určité časti svojho počítača, vyberte možnosť **Vlastná kontrola** a označte ciele kontroly.

Podrobnejšie a pravidelne aktualizované informácie nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Ako povoliť komunikáciu pre určitú aplikáciu

Ak pri zapnutom interaktívnom režime firewall zachytí nové sieťové spojenie, na ktoré sa neuplatňuje žiadne pravidlo, budete vyzvaný na povolenie alebo zablokovanie tohto spojenia. Ak chcete, aby váš produkt ESET Endpoint Security vykonal zvolenú akciu zakaždým, keď sa daná aplikácia pokúsi nadviazať spojenie, označte možnosť **Vytvoriť pravidlo a zapamätať natrvalo**.



V okne nastavení firewallu môžete nové pravidlá pre aplikácie vytvoriť aj pred tým, ako dôjde k detekcii ich sieťovej komunikácie. V hlavnom okne programu ESET Endpoint Security prejdite do sekcie **Nastavenia** > **Sieť** > **Firewall** > kliknite na ikonu ozubeného kolesa > **Konfigurovať** > **Pokročilé** > **Pravidlá** a kliknite na **Upraviť**.

Na pridanie nového pravidla kliknite na tlačidlo **Pridať**. Na karte **Všeobecné** zadajte názov pravidla, smer a komunikačný protokol pre nové pravidlo. V tomto okne môžete zvoliť akciu, ktorá sa má vykonať v prípade uplatnenia pravidla.

Na karte **Lokálna strana** zadajte cestu k aplikácii (*.exe) a lokálny komunikačný port. Kliknite na kartu **Vzdialená strana** na vloženie vzdialenej adresy a portu (ak je to potrebné). Novovytvorené pravidlo bude aplikované hneď, ako sa aplikácia pokúsi nadviazať sieťovú komunikáciu.

Ako vytvoriť novú úlohu v Plánovači

Novú úlohu možno vytvoriť v časti **Nástroje** > **Plánovač** kliknutím na tlačidlo **Pridať plánovanú úlohu** alebo vyvolaním kontextového menu pravým tlačidlom myši a zvolením možnosti **Pridať**. Na výber je päť typov plánovaných úloh:

- **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.
- **Údržba protokolov** – v protokoloch môžu zostávať stopy po vymazaných záznamoch. Táto úloha pravidelne

optimalizuje záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi.
- **Kontrola súborov spúšťaných pri štarte počítača** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.
- **Vytvorenie záznamu o stave počítača** – vytvára záznam o stave počítača cez nástroj ESET SysInspector, ktorý slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.
- **Manuálna kontrola počítača** – vykoná kontrolu diskov, jednotlivých priečinkov a súborov na počítači.
- **Aktualizácia** – zabezpečuje aktualizáciu programových modulov.

Keďže medzi najčastejšie používané plánované úlohy patrí **Aktualizácia**, podrobnejšie popíšeme pridanie aktualizačnej úlohy.

Z roletového menu **Plánovaná úloha** vyberte možnosť **Aktualizácia**. Zadajte názov úlohy do textového poľa **Názov úlohy** a kliknite na **Ďalej**. Vyberte interval vykonania úlohy. K dispozícii sú nasledujúce možnosti: **Raz**, **Opakovane**, **Denne**, **Týždenne** a **Pri udalosti. Možnosť Nespúšťať úlohu, ak je počítač napájaný z batérie** je dobré použiť, ak prenosný počítač nie je zapojený do elektrickej siete a chcete v tomto čase minimalizovať jeho systémové prostriedky. Zadajte čas/dátum alebo interval, v ktorom bude úloha vykonaná, do poľa **Vykonanie úlohy**. Ďalej je potrebné zadefinovať akciu, ktorá sa vykoná v prípade, že v stanovenom termíne nebude možné úlohu spustiť. Na výber sú nasledujúce možnosti, kedy môže byť úloha opätovne spustená:

- **V najbližšom naplánovanom čase**
- **Hneď ako to bude možné**
- **Okamžite, ak od posledného spustenia uplynul stanovený časový interval** (tento interval je možné nastaviť pomocou roletového menu **Čas od posledného spustenia**)

V ďalšom kroku nastavte profil, ktorý sa použije pri aktualizácii. Keď skončíte s úpravami, kliknite na **Dokončiť**.

Zobrazí sa okno umožňujúce vybrať profily, ktoré budú použité pri plánovanej úlohe. Je možné zadefinovať primárny a alternatívny profil. Alternatívny profil sa použije v prípade, že úlohu nebude možné vykonať použitím primárneho profilu. Na uloženie plánovanej úlohy kliknite na **Dokončiť**. Úloha bude následne pridaná do zoznamu úloh Plánovača.

Ako naplánovať pravidelnú týždňovú kontrolu počítača

Na naplánovanie pravidelnej kontroly otvorte hlavné okno programu a kliknite na **Nástroje** > **Plánovač**. Nižšie je popísaný stručný návod, ako vytvoriť úlohu, ktorá bude pravidelne každý týždeň kontrolovať lokálne disky. Podrobné inštrukcie nájdete v našom článku Databázy znalostí.

Na naplánovanie úlohy postupujte nasledovne:

1. Kliknite na **Pridanie plánovanej úlohy** v hlavnom okne Plánovača.
2. V roletovom menu zvoľte možnosť **Manuálna kontrola počítača**.
3. Zadajte názov úlohy a v rámci frekvencie opakovania úlohy vyberte možnosť **Týždenne.**
4. Vyberte čas a deň v týždni vykonania úlohy.
5. Označte možnosť **Vykonať úlohu hneď, ako to bude možné**, ktorá zabezpečí, že ak sa úloha nespustí v naplánovanom čase (napríklad ak je počítač vypnutý), spustí sa hneď, ako to bude opäť možné.
6. Skontrolujte prehľad nastavení naplánovanej úlohy a kliknite na **Dokončiť**.
7. V roletovom menu **Ciele kontroly** si zvoľte **Lokálne disky**.
8. Kliknite na **Dokončiť** pre pridanie úlohy.

Ako pripojiť ESET Endpoint Security k nástroju ESET PROTECT

Ak ste na počítač nainštalovali produkt ESET Endpoint Security a chcete ho spojiť s konzolou ESET PROTECT, uistite sa, že ste na danú pracovnú stanicu nainštalovali aj ESET Management Agenta. Je dôležitou súčasťou komunikácie medzi klientskou pracovnou stanicou a ESET PROTECT Serverom.

- Inštalácia alebo nasadenie ESET Management Agenta na pracovných staniciach

Prečítajte si tiež:

- Dokumentácia pre koncové zariadenia spravované vzdialene
- Ako používať Režim prepísania
- Ako aplikovať odporúčané politiky pre ESET Endpoint Security

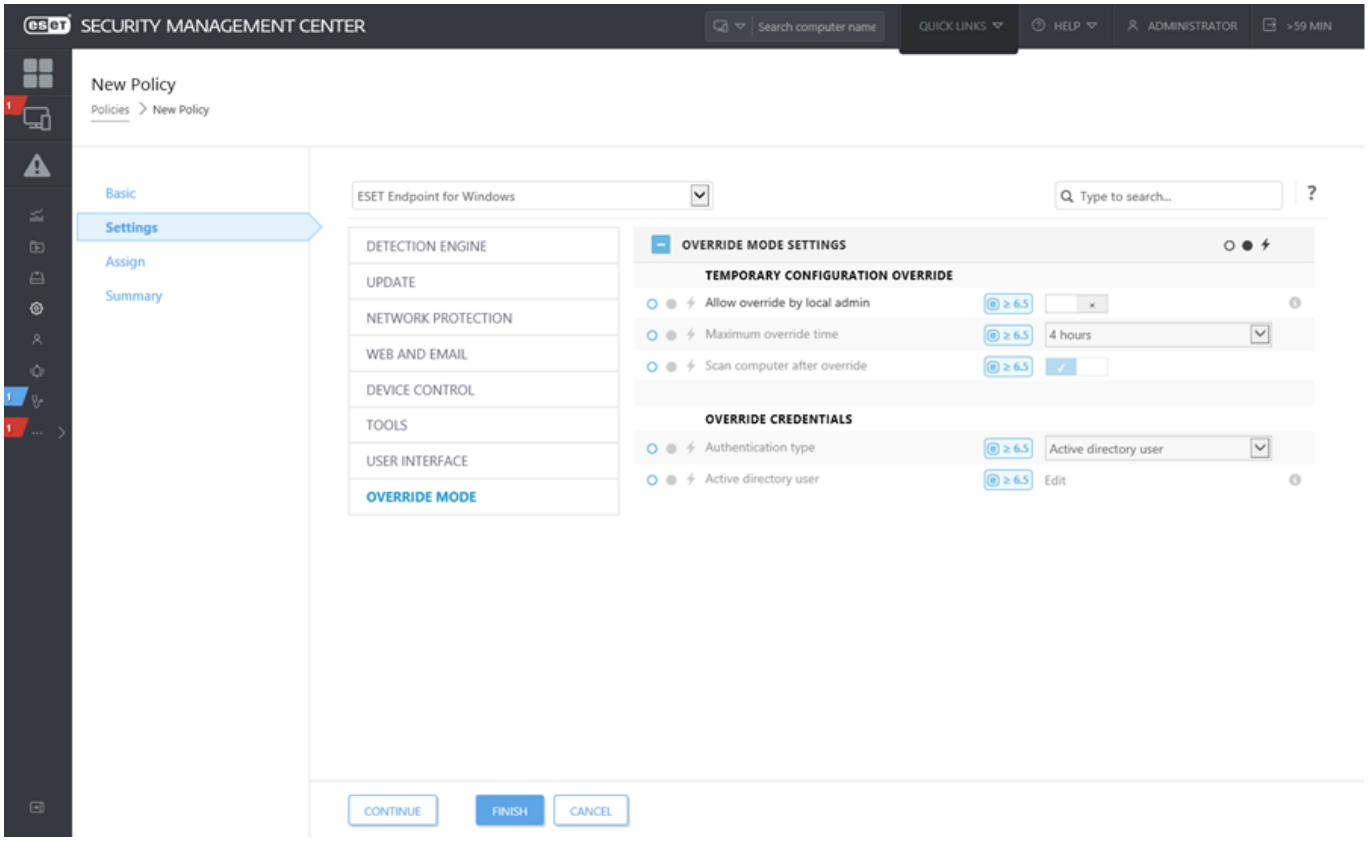
Ako používať Režim prepísania

Používatelia, ktorí majú na svojich zariadeniach nainštalované produkty ESET určené pre koncové zariadenia pre systém Windows (verzia 6.5 a vyššia), môžu využiť funkciu prepísania. Režim prepísania umožňuje používateľom na úrovni klienta meniť nastavenia v nainštalovaných produktoch ESET, a to aj v prípade, že nastavenia sú spravované politikou. Režim prepísania môže byť povolený pre určitých používateľov AD alebo môže byť chránený heslom. Táto funkcia však nemôže byť povolená naraz dlhšie ako štyri hodiny.

⚠ • Režim prepísania nemôže byť po spustení zastavený pomocou nástroja ESET PROTECT Web Console. Režim prepísania sa vypne automaticky po uplynutí stanoveného času. Možno ho tiež vypnúť na klientskom počítači.
• Používateľ, ktorý využíva režim prepísania, musí mať aj práva správcu systému Windows. V opačnom prípade nebude môcť uložiť zmeny v nastaveniach programu ESET Endpoint Security.
• Od verzie ESET Endpoint Security 7.0.2100.4 a novšej môžete oprávnenia definovať aj pre skupinu používateľov zo služby Active Directory.

Nastavenie **Režimu prepísania**:

1. Prejdite do časti **Politiky** > **Nová politika**.
2. V sekcii **Základné** zadajte **Názov** a **Popis** pre danú politiku.
3. Následne v sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows**.
4. Kliknite na **Režim prepísania** a nastavte pravidlá pre tento režim.
5. V sekcii **Priradiť** vyberte počítač alebo skupinu počítačov, na ktoré bude daná politika aplikovaná.
6. Skontrolujte nastavenia v sekcii **Súhrn** a kliknite na **Dokončiť** pre aplikovanie politiky.



Povedzme, že *John* má problém s nastaveniami koncového bezpečnostného produktu, ktoré blokujú na jeho počítači niektorú dôležitú funkcionalitu alebo prístup na internet. V takomto prípade môže správca *Johnovi* povoliť na jeho počítači prepísanie politiky aplikovanej na jeho koncovom bezpečnostnom produkte a umožniť manuálne doladenie nastavení. Tieto nové nastavenia môžu byť následne vyžiadané nástrojom ESET PROTECT, aby mohol na základne nich správca vytvoriť novú politiku.
Postupujte podľa nasledujúcich krokov:
1. Prejdite do časti **Politiky** > **Nová politika**.
2. Vyplňte polia **Názov** a **Popis**. Následne v sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows**.
3. Kliknite na **Režim prepísania**, povoľte tento režim na jednu hodinu a vyberte *Johna* ako používateľa AD.
4. Priraďte politiku na *Johnov počítač* a kliknite na **Dokončiť** pre uloženie politiky.
5. *John* musí povoliť **Režim prepísania** na svojom produkte ESET určenom pre koncové zariadenia a manuálne zmeniť nastavenia na svojom počítači.
6. V nástroji ESET PROTECT Web Console prejdite do časti **Počítače**, vyberte *Johnov počítač* a kliknite na možnosť **Zobraziť podrobnosti**.
7. V sekcii **Konfigurácia** kliknite na tlačidlo **Požiadať o konfiguráciu** pre naplánovanie úlohy pre klienta, aby ste z klienta čo najskôr získali konfiguráciu.
8. Po krátkom čase sa zobrazí nová konfigurácia. Kliknite na produkt, ktorého konfiguráciu chcete uložiť, a následne kliknite na **Otvoriť konfiguráciu**.
9. Môžete skontrolovať nastavenia a potom kliknúť na **Konvertovať na politiku**.
10. Vyplňte polia **Názov** a **Popis**.
11. V sekcii **Nastavenia** môžete v prípade potreby upraviť konfiguráciu.
12. V sekcii **Priradiť** môžete priradiť politiku k *Johnovmu počítaču* (alebo k iným počítačom).
13. Kliknite na **Dokončiť** pre uloženie nastavení.
14. Nezabudnite zrušiť prepisovanie politiky, ak už nie je potrebné.

Ako aplikovať odporúčané politiky pre ESET Endpoint Security

Po pripojení ESET Endpoint Security k ESET PROTECT odporúčame aplikovať politiku, či už odporučenú, alebo vlastnú.

Existuje niekoľko vstavaných politík pre ESET Endpoint Security:

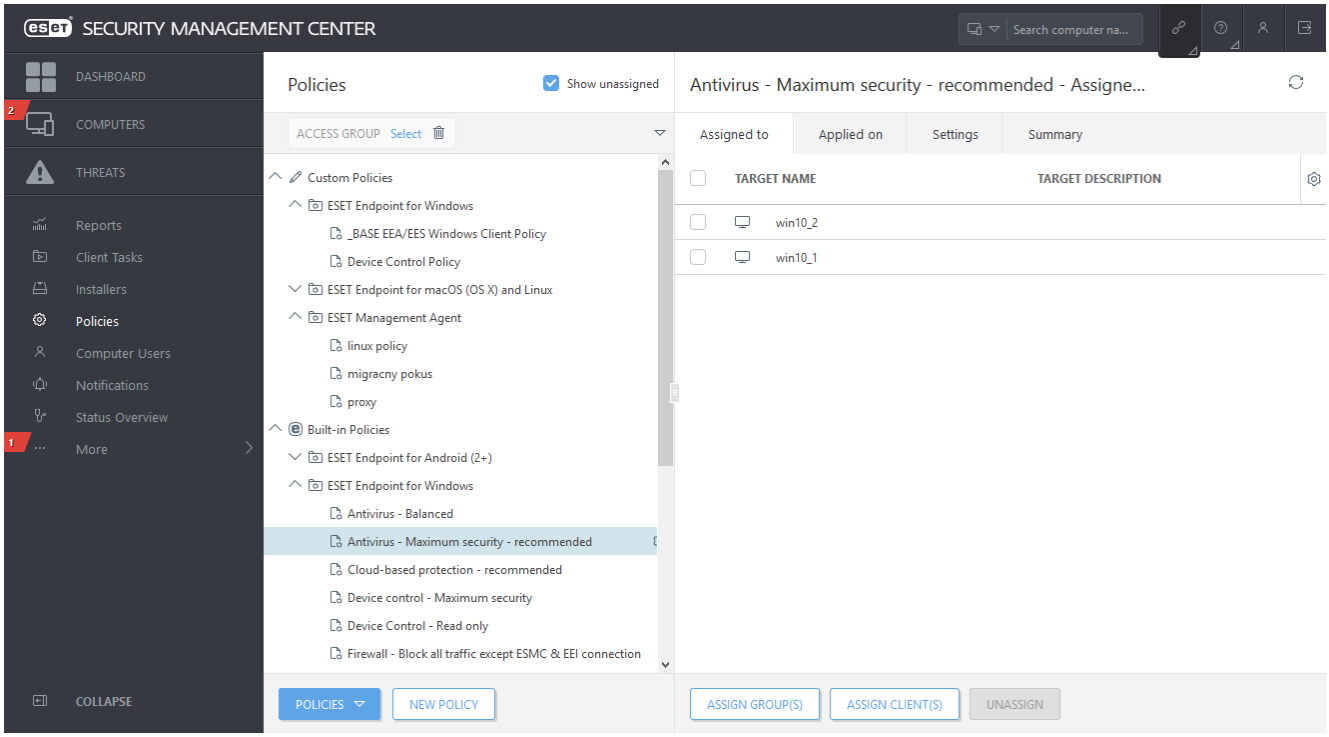
Politika	Popis
Antivírus – Vyvážená	Bezpečnostná konfigurácia odporúčaná pre väčšinu situácií.
Antivírus – Maximálna bezpečnosť	Aktivuje sa strojové učenie, hĺbková kontrola správania a SSL filtrovanie. Tieto funkcie majú vplyv na detekciu potenciálne nebezpečných, nechcených a podozrivých aplikácií.
Cloudový systém reputácie a spätnej väzby	Umožňuje využívať ESET LiveGrid®, cloudový systém reputácie a spätnej väzby, ktorý zlepšuje detekciu najnovších hrozieb a pomáha zdieľať škodlivé alebo neznáme potenciálne hrozby pre ďalšiu analýzu.
Správa zariadení – Maximálna bezpečnosť	Všetky zariadenia sú blokované. Ak sa bude chcieť zariadenie pripojiť, bude musieť byť povolené správcom.
Správa zariadení – Iba na čítanie	Všetky zariadenia je možné iba čítať. Zápis nie je povolený.
Firewall – Blokovať všetku komunikáciu okrem pripojení k ESET PROTECT a ESET Inspect	Zablokuje všetku komunikáciu okrem pripojení k ESET PROTECT a ESET Inspect Serveru (len pre ESET Endpoint Security).
Protokolovanie – Vykonávať úplný diagnostický zápis do protokolu	Táto šablóna zabezpečí, že správca bude mať v prípade potreby k dispozícii všetky protokoly. Zaznamenané budú všetky udalosti od najnižšej úrovne, vrátane HIPS a parametrov ThreatSense, ako aj firewallu. Protokoly sa automaticky odstránia po 90 dňoch.
Protokolovanie – Zapisovať len dôležité udalosti	Politika zabezpečí, aby boli do protokolu uložené upozornenia, chyby a kritické udalosti. Protokoly sa automaticky odstránia po 90 dňoch.
Viditeľnosť – Vyvážená	Predvolené nastavenia viditeľnosti. Stavy a oznámenia sú povolené.
Viditeľnosť – Neviditeľný režim	Vypne sa zobrazovanie oznámení, grafické používateľské rozhranie a integrácia do kontextového menu. Nespustí sa egui.exe. Vhodné pre úplnú správu prostredníctvom ESET PROTECT Cloud.
Viditeľnosť – Obmedzená interakcia s používateľom	Vypne sa zobrazovanie oznámení a stavov aplikácie, ale grafické používateľské rozhranie sa spustí.

Ak chcete nastaviť politiku nazvanú **Antivírus – Maximálna bezpečnosť**, v rámci ktorej sa v produkte ESET Endpoint Security nainštalovanom na vašich pracovných staniciach uplatní viac ako 50 odporúčaných nastavení, postupujte podľa nasledujúcich krokov:

> Nasledujúce články Databázy znalostí spoločnosti ESET môžu byť dostupné len v anglickom jazyku:
> • Použitie odporúčanej alebo preddefinovanej politiky pre ESET Endpoint Security prostredníctvom ESET PROTECT

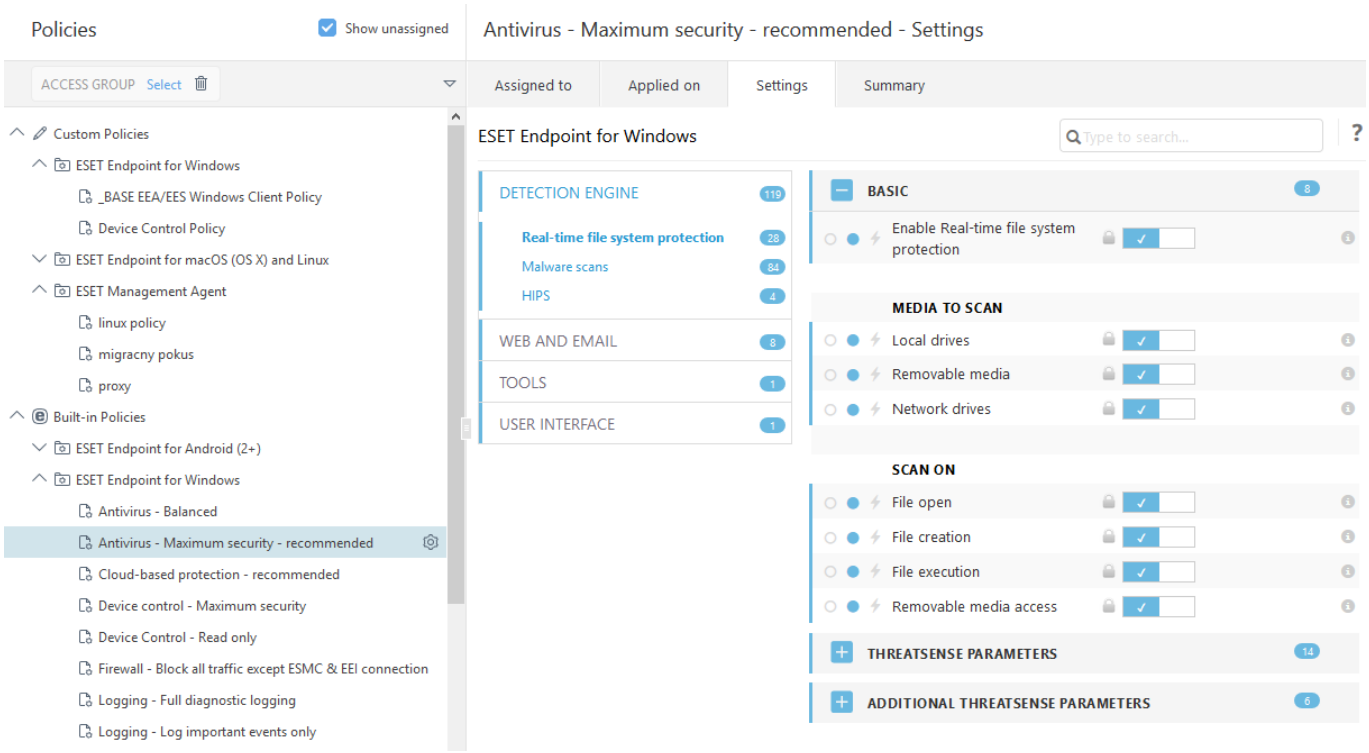
1. Otvorte ESET PROTECT Web Console.
2. Prejdite na **Politiky** a rozbaľte sekciu **Vstavané politiky** > **ESET Endpoint pre Windows**.
3. Kliknite na **Antivírus – Maximálna bezpečnosť – odporúča sa**.

4. Na karte **Priradené** kliknite na **Priradiť klientu** alebo **Priradiť skupine** a vyberte počítače, pre ktoré chcete použiť politiku.



Ak chcete zistiť, ktoré nastavenia budú prostredníctvom danej politiky použité, kliknite na kartu **Nastavenia** a rozbaľte stromovú štruktúru Rozšírené nastavenia.

- Modrá bodka predstavuje nastavenie definované v tejto politike.
- Číslo v modrom ráme predstavuje množstvo nastavení zmenených touto politikou.
- Viac informácií o politikách v konzole ESET PROTECT



Ako nastaviť funkciu mirror

ESET Endpoint Security môže byť nastavený tak, aby ukladal kópie aktualizačných súborov detekčného jadra a tieto aktualizácie distribuoval na ostatné pracovné stanice, ktoré používajú ESET Endpoint Security alebo ESET Endpoint Antivirus.

Nastavenie programu ESET Endpoint Security ako mirror servera pre poskytovanie aktualizácií prostredníctvom interného HTTP servera

1. Otvorte Rozšírené nastavenia stlačením klávesu **F5** a rozbaľte sekciu **Aktualizácia** > **Profily** > **Aktualizačný mirror**.
2. Rozbaľte sekciu **Aktualizácie** a uistite sa, že je zapnutá možnosť **Automatický výber servera** v časti **Aktualizácie modulov**.
3. Rozbaľte sekciu **Aktualizačný mirror** a zapnite možnosti **Vytvárať kópie aktualizácií** a **Povoliť HTTP Server**.

Pre viac informácií si prečítajte:
- Aktualizačný mirror
- Aktualizácia z mirrora

Sprístupnenie mirrora prostredníctvom zdieľaného sieťového priečinku

1. Vytvorte zdieľaný priečinok na lokálnom alebo sieťovom disku. K priečinku musia mať prístupové práva na čítanie všetci používatelia, ktorých produkty ESET si z daného priečinka budú sťahovať aktualizácie, a lokálny systémový účet musí mať pridelené práva na zápis do priečinka, aby doň bolo možné ukladať kópie aktualizácií.
2. Zapnite možnosť **Vytvárať kópie aktualizácií** v sekcii **Rozšírené nastavenia** > **Aktualizácia** > **Profily** > **Aktualizačný mirror**.
3. Vyberte vhodný **Úložný priečinok** kliknutím na **Vyčistiť** a následne na **Upraviť**. Vyhľadajte a vyberte vytvorený zdieľaný priečinok.

Ak nechcete poskytovať aktualizácie modulov prostredníctvom interného HTTP servera, vypnite možnosť **Vytvárať kópie aktualizácií**.

Ako prejsť na Windows 10 s nainštalovaným produktom ESET Endpoint Security

Predtým ako vykonáte aktualizáciu (upgrade) na Windows 10, dôrazne vám odporúčame aktualizovať váš produkt ESET na najnovšiu verziu a aktualizovať detekčné jadro. Týmto bude zaistená maximálna ochrana a vaše nastavenia programu vrátane licenčných informácií budú počas aktualizácie na Windows 10 zachované.

Verzia 7.x:

Kliknite na príslušný odkaz nižšie pre stiahnutie a inštaláciu najnovšej verzie v rámci prípravy na aktualizáciu na Windows 10:

Stiahnuť ESET Endpoint Security 7 (32-bitová verzia) Stiahnuť ESET Endpoint Antivirus 7 (32-bitová verzia)

Stiahnuť ESET Endpoint Security 7 (64-bitová verzia) Stiahnuť ESET Endpoint Antivirus 7 (64-bitová verzia)

Verzia 5.x:

Produktom ESET pre koncové zariadenia vo verzii 5 sa končí životný cyklus. Znamená to, že vydané podverzie už nie sú verejne dostupné na stiahnutie. Dôrazne vám odporúčame prejsť na najnovšiu verziu produktov ESET pre koncové zariadenia.

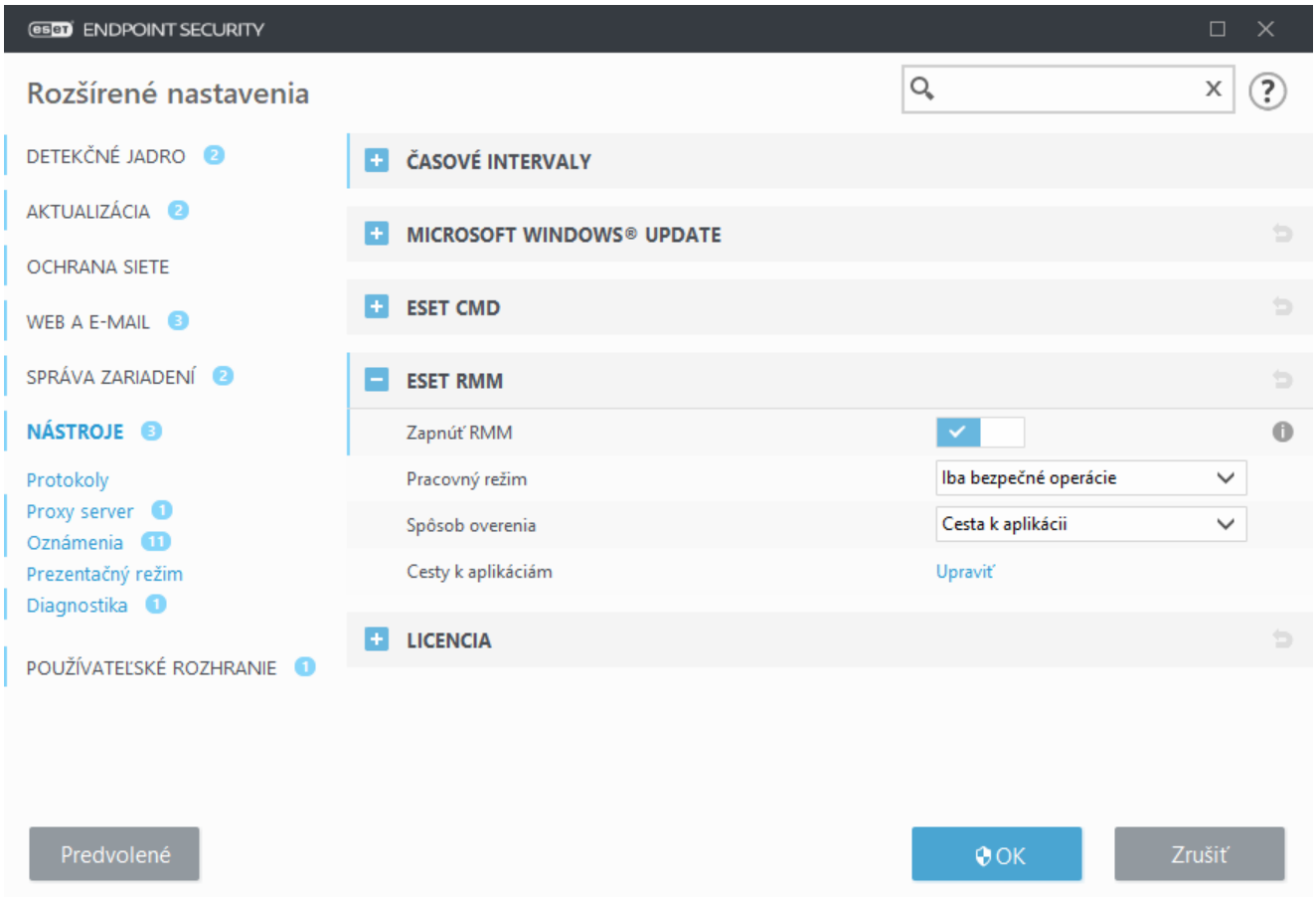
Verzie pre ostatné jazyky:

Ak hľadáte inú jazykovú verziu produktu ESET pre koncové zariadenia, navštívte našu webovú stránku.

Dodatočné informácie o kompatibilite firemných produktov ESET s operačným systémom Windows 10.

Ako aktivovať vzdialený monitoring a správu produktu (RMM)

Remote Monitoring and Management (RMM) je proces vzdialeného monitorovania a ovládania softvérových systémov (napr. na stolových počítačoch, serveroch a mobilných zariadeniach) pomocou lokálne nainštalovaného agenta, ku ktorému sa dokáže poskytovateľ služieb spravovania pripojiť. ESET Endpoint Security môže byť spravovaný prostredníctvom RMM počnúc verziou 6.6.2028.0.



V predvolených nastaveniach je funkcia ESET RMM vypnutá. Na povolenie ESET RMM stlačte **F5**, čím otvoríte rozšírené nastavenia. Následne kliknite na **Nástroje**, rozbaľte sekciu **ESET RMM** a použite možnosť **Zapnúť RMM**.

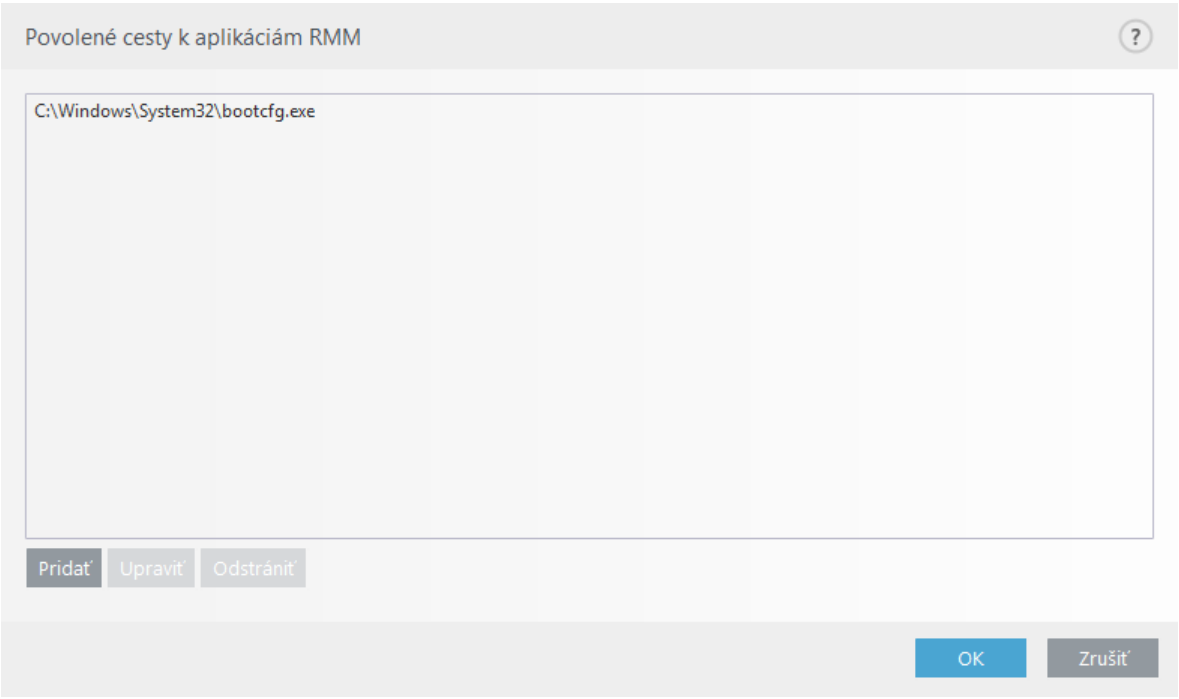
Pracovný režim – zvoľte možnosť **Iba bezpečné operácie**, ak chcete povoliť RMM rozhranie len pre operácie, ktoré sú bezpečné alebo dostupné len na čítanie. Ak chcete povoliť RMM rozhranie pre všetky operácie, zvoľte možnosť **Všetky operácie**.

Operácia	Režim „Iba bezpečné operácie“	Režim „Všetky operácie“
Získať informácie o aplikácii	✔	✔
Získať konfiguráciu	✔	✔
Získať licenčné informácie	✔	✔
Získať protokoly	✔	✔
Získať stav ochrany	✔	✔
Získať stav aktualizácie	✔	✔
Nastaviť konfiguráciu		✔
Spustiť aktiváciu		✔
Spustiť kontrolu	✔	✔
Spustiť aktualizáciu	✔	✔

Spôsob oprávnenia – nastavte autorizačnú metódu pre RMM. Ak chcete používať autorizáciu, zvoľte v roletovom menu možnosť **Cesta k aplikácii**, v opačnom prípade zvoľte možnosť **Žiadne**.

V rámci RMM by mala byť vždy používaná autorizácia, aby sa zabránilo škodlivému softvéru vypnúť alebo obísť ochranu ESET Endpoint produktu.

Cesty k aplikáciám – konkrétna aplikácia, ktorá má povolené spúšťať RMM. Ak ste zvolili možnosť **Cesta k aplikácii** ako autorizačnú metódu, kliknite na **Upraviť** pre otvorenie konfiguračného okna **Povolené cesty k aplikáciám RMM**.



Pridať – pridanie novej povolenej cesty k RMM aplikácii. Zadajte cestu alebo kliknite na tlačidlo **...** na vyhľadanie

spustiteľného súboru.

Upraviť – pomocou tejto možnosti môžete upraviť už existujúcu povolenú cestu. Možnosť **Upraviť** použite v prípade, že sa zmenilo umiestnenie spustiteľného súboru.

Odstrániť – pomocou tejto možnosti môžete odobrať už existujúcu povolenú cestu.

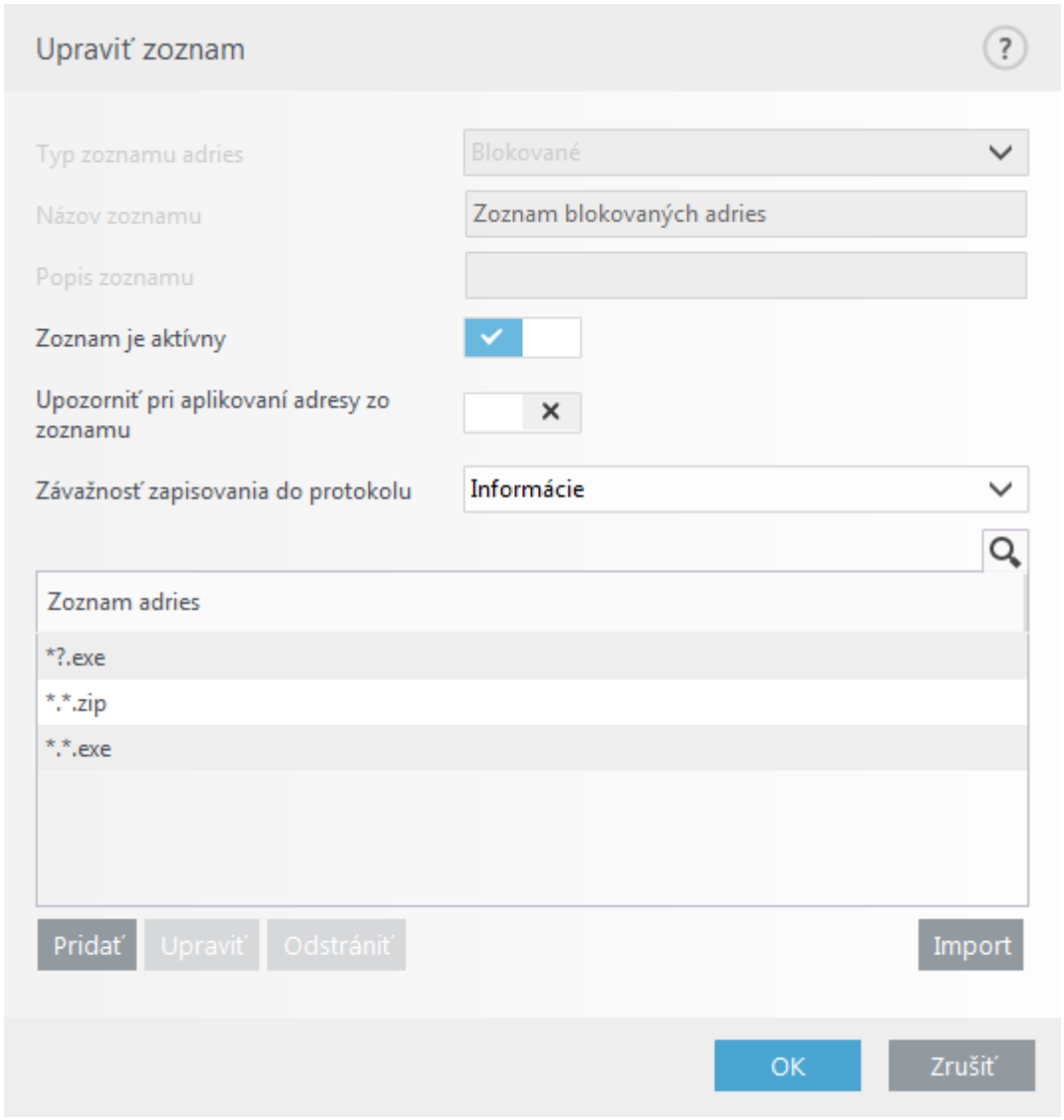
Súčasťou predvolenej inštalácie ESET Endpoint Security je aj súbor ermm.exe, ktorý sa nachádza v adresári ESET Endpoint produktu (predvolená cesta je C*:\Program Files\ESET\ESET Security*). Súbor ermm.exe zabezpečuje výmenu dát s doplnkom RMM Plugin, ktorý komunikuje s RMM Agentom prepojeným s RMM Serverom.

- ermm.exe – nástroj príkazového riadka vyvinutý spoločnosťou ESET, ktorý umožňuje správu firemných bezpečnostných produktov a komunikáciu s akýmkoľvek RMM doplnkom.
- RMM Plugin je aplikácia tretej strany, ktorá beží lokálne na počítači so systémom Windows, chráneným produktom ESET Endpoint. Tento doplnok komunikuje s konkrétnym RMM Agentom (napr. Kaseya) a so súborom ermm.exe.
- RMM Agent je aplikácia tretej strany (napr. Kaseya), ktorá beží lokálne na počítači so systémom Windows, chráneným produktom ESET Endpoint. Agent komunikuje s RMM doplnkom a RMM Serverom.

Ako blokovať stiahnutie určitých typov súborov z internetu

Ak chcete blokovať sťahovanie určitých typov súborov z internetu (napríklad exe, pdf alebo zip), využite Manažment URL adries v kombinácii so zástupnými znakmi. Stlačením klávesu F5 otvorte **Rozšírené nastavenia**. Kliknite na **Web a e□mail** > **Ochrana prístupu na web** a rozbaľte časť **Manažment URL adries**. Kliknite na možnosť **Upraviť** vedľa **Zoznamu adries**.

V okne **Zoznam adries** vyberte **Zoznam blokovaných adries** a kliknite na **Upraviť**, prípadne na možnosť **Pridať** na vytvorenie nového zoznamu. Zobrazí sa nové okno. Ak vytvárate nový zoznam, vyberte z roletového menu **Typ zoznamu adries** možnosť **Blokované** a zadajte názov zoznamu. Ak si želáte dostávať upozornenia v prípade prístupu k typu súboru zadefinovanému v aktuálnom zozname, povoľte možnosť **Upozorniť pri aplikovaní adresy zo zoznamu**. Z roletového menu **Závažnosť zapisovania do protokolu** vyberte niektorú z dostupných možností. Remote Administrator môže zozbierať záznamy so závažnosťou na úrovni **Upozornení**.



Kliknutím na **Pridať** môžete zadať masku, ktorá zadefinuje typy súborov, ktorých sťahovanie chcete blokovať. Zadajte úplnú URL adresu, ak chcete blokovať sťahovanie konkrétneho súboru z určitej webovej stránky (napr. *http://example.com/file.exe*). Ak chcete pokryť celú skupinu súborov, môžete použiť zástupné znaky. Otáznik (?) nahrádza jeden ľubovoľný znak a hviezdička (*) nahrádza ľubovoľný reťazec v dĺžke 0 až niekoľko znakov. Napríklad maska **/*.zip* bude blokovať sťahovanie všetkých skomprimovaných súborov vo formáte zip.

Túto metódu môžete použiť na blokovanie sťahovania konkrétnych typov súborov len v prípade, ak je prípona súboru súčasťou URL. Ak webová stránka používa odkaz na stiahnutie súboru napríklad v tvare *www.example.com/download.php?fileid=42*, akýkoľvek súbor nachádzajúci sa na tomto odkaze by bol stiahnutý aj v prípade, že má príponu, ktorú ste zablokovali.

Ako minimalizovať používateľské rozhranie programu ESET Endpoint Security

Ak je program spravovaný vzdialene, môžete použiť prednastavenú politiku súvisiacu s „viditeľnosťou“ produktu pre koncového používateľa.

V opačnom prípade môžete manuálne priamo v lokálne nainštalovanom programe vykonať nasledujúce kroky:

1. Stlačte kláves **F5** pre otvorenie okna Rozšírených nastavení a rozbaľte sekciu **Používateľské rozhranie** >

Prvky používateľského rozhrania.

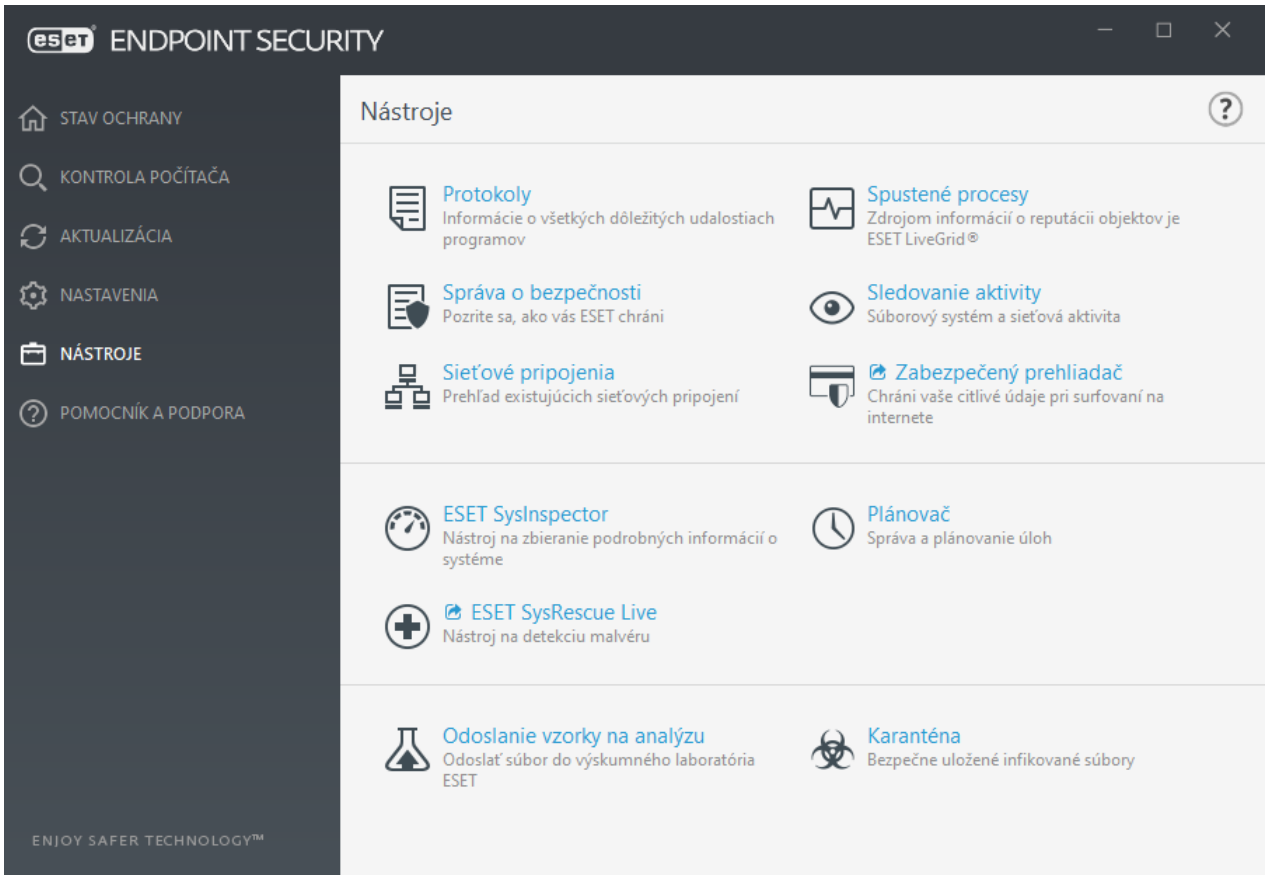
2. Nastavte **Režim spustenia** na požadovanú hodnotu. Viac informácií o režimoch spustenia programu.
3. Deaktivujte možnosti **Zobrazovať úvodný obrázok pri štarte** a **Používať zvukové upozornenia**.
4. Nastavte Oznámenia.
5. Nastavte Stavy aplikácie.
6. Nastavte Potvrdzovacie správy.
7. Nastavte Upozornenia a okná správ.

Ako vyriešiť chybové hlásenie „Zabezpečený prehliadač nemohol byť presmerovaný na požadovanú webovú stránku“

Pre vyriešenie tohto problému postupujte podľa pokynov nižšie:

Po dokončení každého kroku skontrolujte, či zabezpečený prehliadač už pracuje správne. Ak okno prehliadača stále nefunguje, postupujte ďalšími krokmi, až kým sa okno nezačne opäť zobrazovať.

1. Reštartujte počítač.
2. Uistite sa, že používate najnovšiu verziu operačného systému Windows a firemného produktu ESET pre Windows: Akú verziu produktu ESET pre firmy mám nainštalovanú a je to najnovšia verzia?



3. Mohlo dôjsť ku konfliktu s vaším bezpečnostným softvérom tretej strany alebo firewallom. Skontrolujte preto tento softvér, prípadne zvážte jeho odinštalovanie v okne Pridať alebo odstrániť programy. Kliknite na **Nástroje** > **Zabezpečený prehliadač**. Po otvorení zabezpečeného prehliadača pokračujte na ďalší krok.
4. Vypnite všetky rozšírenia prehliadača tretích strán.

5. Vymažte vyrovnávaciu pamäť webového prehliadača. Ako vymažem vyrovnávaciu pamäť prehliadača Firefox alebo prehliadača Google Chrome?
6. Uistite sa, že váš predvolený prehliadač sa nenachádza v zozname vylúčených aplikácií v časti **Rozšírené nastavenia** > **Web a e-mail** > **Filtrovanie protokolov** > **Vylúčené aplikácie**.
7. Ak ste neaktualizovali svoj produkt ESET na novšiu verziu v predchádzajúcich krokoch, odinštalujte a opätovne ho nainštalujte. Po reštarte počítača vypnite zabezpečený prehliadač a znova reštartujte počítač. Následne funkciu zabezpečeného prehliadača znovu zapnite a pokúste sa spustiť okno zabezpečeného prehliadača.

Zabezpečený prehliadač predstavuje dodatočnú vrstvu ochrany, ktorej cieľom je chrániť vaše online transakcie a finančné údaje pred zneužitím.

Zabezpečený prehliadač sa spustí vo vašom predvolenom prehliadači, ak navštívite známu stránku internetového bankovníctva. Ak si chcete priamo otvoriť zabezpečený prehliadač, prejdite v programe ESET Endpoint Security do sekcie **Nástroje** a následne kliknite na  **Zabezpečený prehliadač**.

Pre podrobnejšie informácie o fungovaní Zabezpečeného prehliadača si prečítajte nasledujúce články Databázy znalostí spoločnosti ESET, ktoré sú dostupné v angličtine a niekoľkých ďalších jazykoch:

- Ako používať Zabezpečený prehliadač?
- Ako zapnem alebo vypnem ESET Ochranu online platieb pre konkrétnu webovú stránku?
- Ako pozastavím alebo vypnem ochranu online platieb v ESET Windows produkte pre domácnosti?
- Ochrana online platieb – bežné chyby
- Slovník pojmov ESET | Ochrana online platieb

Ak sa vám stále nedarí vyriešiť váš problém, kontaktujte technickú podporu spoločnosti ESET.

Licenčná dohoda s koncovým používateľom

S účinnosťou od 19. októbra 2021.

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.**

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532 („ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou („Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva

vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody a prijímate Zásady ochrany osobných údajov. Ak s niektorými podmienkami a požiadavkami tejto Dohody a/alebo Zásad ochrany osobných údajov nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru („Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto zmluvy a dodržiavate všetky jej zmluvné podmienky, poskytovateľ vám udeľuje nasledujúce práva („licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií.** Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent („MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač. Jednu

licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má Koncový používateľ právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Home/Business Edition.** Verzia Softvéru Home Edition je určená výlučne na domáce a rodinné používanie v súkromných alebo nekomerčných prostrediach. Na použitie v komerčnom prostredí, ako aj na použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie.** Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér.** Softvér klasifikovaný ako OEM je obmedzený len na počítač, s ktorým bol získaný. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér.** Softvér označený ako „Nepredajný“, „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie.** Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zrušenia licencie musíte softvér a všetky záložné kópie okamžite odstrániť, zničiť alebo na svoje náklady vrátiť spoločnosti ESET alebo na miesto, kde ste softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4. **Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a zhromažďovanie údajov je nevyhnutné na tieto funkcie Softvéru:

a) **Aktualizácia Softvéru.** Poskytovateľ môže príležitostne vydávať aktualizácie alebo inovácie Softvéru („Update“), nie je však povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Pre poskytovanie aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

Na poskytovanie akýchkoľvek aktualizácií sa môžu vzťahovať Zásady Ukončenia životného cyklu („Zásady Ukončenia životného cyklu“), ktoré sú k dispozícii na adrese https://go.eset.com/eol_business. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebudú sa poskytovať žiadne aktualizácie.

b) **Preposielanie infiltrácií a informácií Poskytovateľovi.** Softvér obsahuje funkcie, ktoré zhromažďujú vzorky počítačových vírusov a iných škodlivých počítačových programov, ako aj podozrivých, problémových, potenciálne nechcených alebo potenciálne nebezpečných objektov, ako sú napríklad súbory, URL adresy, IP pakety a ethernetové rámce („Infiltrácie“), a potom ich odosiela Poskytovateľovi vrátane, nie však výhradne, informácií o procese inštalácie, počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, a/alebo informácií o prevádzke a fungovaní Softvéru („Informácie“.) Informácie a Infiltrácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov) o Koncovom používateľovi alebo iných používateľoch počítača, v ktorom je Softvér nainštalovaný, a súboroch postihnutých Infiltráciami spolu so súvisiacimi metaúdajmi.

Informácie a Infiltrácie sa môžu zhromažďovať prostredníctvom nasledujúcich funkcií Softvéru:

i. Súčasťou funkcie LiveGrid Reputation System je zhromažďovanie a odosielanie jednosmerných hodnôt hash súvisiacich s infiltráciami Poskytovateľovi. Táto funkcia sa zapína v štandardných nastaveniach Softvéru.

ii. Súčasťou funkcie LiveGrid Feedback System je zhromažďovanie a odosielanie Infiltrácií spolu so súvisiacimi metaúdajmi a Informáciami Poskytovateľovi. Túto funkciu môže aktivovať Koncový používateľ počas inštalácie Softvéru.

Poskytovateľ použije získané Informácie a Infiltrácie iba na účely analýzy a preskúmania Infiltrácií, vylepšenia Softvéru a overenia pravosti Licencie, pričom vykoná primerané opatrenia na zachovanie zabezpečenia získaných Infiltrácií a Informácií. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Infiltrácie a Informácie v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Tieto funkcie môžete kedykoľvek deaktivovať.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi

predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Dohody budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, tým nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Dohody.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Na vaše právo používať Softvér a ktorúkoľvek z jeho funkcií sa môžu vzťahovať Zásady Ukončenia životného cyklu. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, vaše právo používať Softvér zanikne. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY,

ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ INŠTALÁCIOU, POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebude sa poskytovať žiadna technická podpora. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti Softvéru.** Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo). Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**.

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje.

(právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez toho, aby bolo dotknuté právo spoločnosti ESET oznámiť vám akékoľvek zmeny tejto Dohody, Zásad ochrany osobných údajov, Zásad Ukončenia životného cyklu a Dokumentácie v súlade s článkom 22 Dohody. Spoločnosť ESET vám môže posielať e-maily, oznámenia v aplikácii prostredníctvom Softvéru alebo uverejniť komunikáciu na svojej webovej lokalite. Súhlasíte s tým, že budete od spoločnosti ESET dostávať právnu komunikáciu v elektronickej forme vrátane akejkoľvek komunikácie o zmene podmienok, osobitných podmienok alebo zásad ochrany osobných údajov, akýchkoľvek návrhov/prijatí zmluvy alebo pozvánok, upozornení alebo inej právnej komunikácie. Takáto elektronická komunikácia sa bude považovať za prijatú v písomnej forme, pokiaľ príslušné právne predpisy osobitne nevyžadujú inú formu komunikácie.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky.

Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. Táto Dohoda bola vyhotovená v angličtine. V prípade, že je z praktických dôvodov alebo na akýkoľvek iný účel vypracovaný akýkoľvek preklad Dohody, alebo v prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí verzia v angličtine.

Spoločnosť ESET si vyhradzuje právo kedykoľvek vykonať zmeny v Softvéri, ako aj kedykoľvek upraviť podmienky tejto Dohody, jej prílohy, dodatky, Zásady ochrany osobných údajov, Zásady Ukončenia životného cyklu a dokumentáciu, prípadne ich ľubovoľnú časť tak, že aktualizuje príslušný dokument: (i) aby zohľadňoval zmeny v Softvéri alebo v tom, ako spoločnosť ESET vykonáva podnikateľskú činnosť, (ii) z právnych, regulačných alebo bezpečnostných dôvodov alebo (iii) na zabránenie zneužitiu alebo ublíženiu. O každej úprave Dohody vás informujeme prostredníctvom e-mailu, oznámenia v aplikácii alebo iným spôsobom elektronickej komunikácie. Ak s navrhovanými zmenami Dohody nebudete súhlasiť, môžete ju v súlade s článkom 10 ukončiť do 30 dní od prijatia oznámenia o zmene. Ak Dohodu v tejto časovej lehote neukončíte, navrhované zmeny sa budú považovať za prijaté a nadobudnú voči vám účinnosť k dátumu prijatia oznámenia o zmene.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

EULAID: EULA-PRODUCT-LG; 3537.0

Zásady ochrany osobných údajov

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, chce byť ako kontrolór údajov (ďalej len „ESET“ alebo „my“ alebo formulácie vyjadrené v prvej osobe množného čísla) pri spracovaní osobných údajov a ochrane osobných údajov svojich zákazníkov transparentná. S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať našich zákazníkov (ďalej len „koncový používateľ“ alebo „vy“ alebo formulácie vyjadrené v druhej osobe množného čísla) o nasledujúcich témach:

- Spracovávanie osobných údajov,
- Dôvernosť údajov,
- práva dotknutej osoby.

Spracovávanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho produktu sa poskytujú za podmienok Licenčnej zmluvy koncového používateľa (ďalej len "EULA"), niektoré z nich však môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o zhromažďovaní údajov, ktoré súvisí s poskytovaním našich služieb. Poskytujeme rôzne služby, ktoré sú opísané v zmluve EULA, ako aj v produktovej dokumentácii. Patria k nim napríklad služby aktualizácie/inovácie, ESET LiveGrid®, ochrana pred zneužitím údajov, podpora atď. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

• Informácie o aktualizáciách a ďalšie štatistické informácie týkajúce sa procesu inštalácie a počítača vrátane informácií o platforme, na ktorej je produkt nainštalovaný, a informácií o operáciách a funkčnosti našich produktov, napríklad informácie o operačnom systéme, hardvéri, identifikátoroch inštalácie, identifikácii licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu.

• Jednosmerné haše súvisiace s infiltráciami, ktoré sú zhromažďované v rámci reputačného systému ESET LiveGrid® a ktorými sa zlepšuje účinnosť našich antimalvérových riešení na základe porovnávania naskenovaných súborov s databázou položiek zaradených na whitelist a blacklist v cloude.

• Prijaté podozrivé vzorky a metadáta zhromažďované v rámci systému spätnej väzby ESET LiveGrid®, ktoré umožňujú spoločnosti ESET okamžite reagovať na potreby svojich koncových používateľov, ako aj na najnovšie hrozby. Spoliehame sa na to, že nám zašlete

  o infiltrácie, ako napríklad vzorky potenciálnych vírusov a iných škodlivých a podozrivých programov; problematické, potenciálne neželané alebo potenciálne nebezpečné objekty, ako napríklad spustiteľné súbory, e-mailové správy, ktoré ste nahlásili ako spam alebo ktoré takto označil váš produkt;

  o informácie o zariadeniach v lokálnej sieti, ako napríklad typ, dodávateľ, model a/alebo názov zariadenia;

  o informácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;

  o súbory výpisov pri zlyhaní a informácie, ktoré obsahujú.

Nemáme v úmysle zhromažďovať vaše údaje mimo tohto rozsahu, niekedy sa tomu však nedá zabrániť. Náhodne zhromaždené údaje môžu byť obsiahnuté v samotnom malvéri (zhromaždené bez vášho vedomia alebo súhlasu) alebo môžu byť súčasťou názvov súborov či URL adries a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

• Licenčné informácie, ako napríklad identifikácia licencie, a osobné údaje, ako napríklad meno, priezvisko, adresa a e-mailová adresa, sa vyžadujú na fakturačné účely, overenie pravosti licencie a poskytovanie našich služieb.

• Kontaktné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa vyžadujú na poskytnutie technickej alebo inej podpory spoločnosťou ESET. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a popis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia podpory vás môžeme požiadať o poskytnutie ďalších informácií.

Dôvernosť údajov

ESET je spoločnosť s celosvetovou pôsobnosťou prostredníctvom pridružených subjektov alebo partnerov, ktorí sú súčasťou našej distribučnej, servisnej či podpornej siete. Informácie spracúvané spoločnosťou ESET sa môžu na účely výkonu zmluvy EULA, napríklad na poskytovanie služieb či podpory alebo fakturácie, prenášať medzi jednotlivými pridruženými subjektmi alebo partnermi. V závislosti od vašej polohy a služby, ktorú si vyberiete, sa od nás môže žiadať prenos vašich údajov do krajiny, v ktorej neplatí príslušné rozhodnutie Európskej komisie. Aj v takom prípade podlieha každý prenos informácií úprave vychádzajúcej z právnych predpisov o ochrane údajov a uskutočňuje sa iba v prípade potreby. Bez výnimky musia byť zavedené štandardné zmluvné doložky, záväzné vnútropodnikové pravidlá alebo iné vhodné záruky.

Čo najviac sa snažíme zabrániť tomu, aby sa pri poskytovaní služieb podľa zmluvy EULA údaje uchovávali dlhšie, než je naozaj potrebné. Obdobie uchovávania môže prekračovať platnosť vašej licencie, aby ste mali čas na jej jednoduché a pohodlné obnovenie. Minimalizované a pseudonymizované štatistické a iné údaje zo systému ESET LiveGrid® sa môžu ďalej spracúvať na štatistické účely.

Spoločnosť ESET realizuje vhodné technické a organizačné opatrenia na zabezpečenie úrovne bezpečnosti, ktorá zodpovedá potenciálnym rizikám. Čo najlepšie sa snažíme zabezpečiť neustálu dôvernosť, integritu, dostupnosť a odolnosť systémov a služieb spracovania údajov. V prípade úniku údajov, ktorý má za následok ohrozenie vašich práv a slobôd, sme však pripravení informovať dozorný orgán, ako aj dotknuté osoby. Ako dotknutá osoba máte právo podať sťažnosť dozornému orgánu.

Práva dotknutej osoby

Spoločnosť ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. V súlade s podmienkami určenými príslušnými zákonmi na ochranu údajov máte ako dotknutá osoba tieto práva:

- právo požiadať spoločnosť ESET o prístup k svojim osobným údajom;
- právo na opravu svojich osobných údajov, ak sú nepresné (máte tiež právo doplniť neúplné osobné údaje);
- právo požiadať o vymazanie svojich osobných údajov;
- právo požiadať o zákaz spracovania svojich osobných údajov;
- právo namietať voči spracovaniu
- právo podať sťažnosť, ako aj
- právo na prenosnosť údajov.

Veríme, že všetky informácie, ktoré spracúvame, sú cenné a potrebné z hľadiska nášho legitímneho záujmu, ktorým je poskytovanie služieb a produktov zákazníkom.

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk