ESET Security for Microsoft SharePoint

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

Copyright ©2023 ESET, spol. s r. o.

ESET Security for Microsoft SharePoint 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. 19.3.2023

1 Úvod ... 1
2 Prehľad ... 2
2.1 Hlavné funkcie ... 2
2.2 Čo je nové ... 4
2.3 Nasadenie ... 4
2.3 Nasadenie vo farme SharePoint ... 4
2.3 Inštalácia v klastrovom prostredí ... 5
2.4 Typy ochrany SharePoint ... 5
2.4 Integrácia so SharePointom ... 6
2.4 Filtrovanie pri prístupe ... 6
2.4 Manuálna kontrola databáz ... 7
3 Príprava na inštaláciu ... 8
3.1 Systémové požiadavky ... 10
3.2 Potrebná kompatibilita s SHA-2 ... 11
3.3 Inštalácia ESET Security for Microsoft SharePoint ... 12
3.3 Úprava existujúcej inštalácie ... 15
3.4 Tichá inštalácia/inštalácia bez obsluhy ... 17
3.4 Inštalácia cez príkazový riadok ... 17
3.5 Aktivácia produktu ... 20
3.5 ESET Business Account ... 22
3.5 Úspešná aktivácia ... 22
3.5 Chyba aktivácie ... 22
3.5 Licencia ... 22
3.6 Aktualizácia na novú verziu ... 23
3.6 Aktualizácia pomocou nástroja ESET PROTECT ... 24
3.6 Aktualizácia prostredníctvom klastra ESET ... 26
3.7 Terminálový server ... 29
4 Ako začať ... 29
4.1 Spravovanie pomocou nástroja ESET PROTECT ... 30
4.2 Monitorovanie ... 30
4.2 Stav ochrany ... 32
4.2 K dispozícii sú aktualizácie Windows ... 34
4.2 Izolácia siete ... 34
5 Používanie programu ESET Security for Microsoft SharePoint ... 35
5.1 Kontrola ... 36
5.1 Okno kontroly a protokol o kontrole ... 38
5.2 Protokoly ... 39
5.2 Filtrovanie protokolov ... 43
5.3 Aktualizácia ... 44
5.4 Nastavenia ... 46
5.4 Server ... 47
5.4 Počítač ... 48
5.4 Sieť ... 49
5.4 Sprievodca riešením problémov so sieťou ... 50
5.4 Web a e-mail ... 50
5.4 Nástroje – Diagnostické zapisovanie do protokolu ... 51
5.4 Import a export nastavení ... 52
5.5 Nástroje ... 53
5.5 Spustené procesy ... 54
5.5 Sledovanie aktivity ... 56

5.5 Štatistiky ochrany ... 57
5.5 Klaster ... 59
5.5 Sprievodca konfiguráciou klastra – výber uzlov ... 61
5.5 Sprievodca konfiguráciou klastra – nastavenie klastra ... 62
5.5 Sprievodca konfiguráciou klastra – nastavenia inštalácie klastra ... 62
5.5 Sprievodca konfiguráciou klastra – kontrola uzlov ... 63
5.5 Sprievodca konfiguráciou klastra – inštalácia uzlov ... 64
5.5 ESET Shell ... 67
5.5 Použitie ... 69
5.5 Príkazy ... 74
5.5 Batch súbory/skriptovanie ... 77
5.5 ESET SysInspector ... 78
5.5 ESET SysRescue Live ... 79
5.5 Plánovač ... 79
5.5 Plánovač – pridanie úlohy ... 80
5.5 Typ úlohy ... 83
5.5 Načasovanie úlohy ... 83
5.5 Pri udalosti ... 84
5.5 Spustenie aplikácie ... 84
5.5 Vynechaná úloha ... 84
5.5 Informácie o naplánovanej úlohe ... 85
5.5 Odoslanie vzorky na analýzu ... 85
5.5 Podozrivý súbor ... 86
5.5 Podozrivá stránka ... 86
5.5 Nesprávne detegovaný súbor ... 87
5.5 Nesprávne detegovaná stránka ... 87
5.5 Iné ... 87
5.5 Karanténa ... 88
6 Nastavenia ochrany servera ... 89
6.1 Počítadlá výkonu ... 91
6.2 Filtrovanie pri prístupe ... 92
6.2 Antivírus a antispyware ... 93
6.3 Manuálna kontrola databáz ... 95
6.3 Ciele manuálnej kontroly databáz ... 95
6.3 Antivírus a antispyware ... 96
6.4 Pravidlá ... 97
6.4 Zoznam pravidiel ... 97
6.4 Sprievodca pravidlami ... 98
6.4 Podmienka pravidla ... 100
6.4 Akcia pravidla ... 101
7 Všeobecné nastavenia ... 102
7.1 Počítač ... 103
7.1 Ochrana využívajúca strojové učenie ... 105
7.1 Vylúčenia ... 108
7.1 Výkonnostné vylúčenia ... 108
7.1 Vylúčenia detekcií ... 109
7.1 Sprievodca vytvorením vylúčenia ... 111
7.1 Pokročilé možnosti ... 111
7.1 Automatické vylúčenia ... 112
7.1 Zdieľaná lokálna vyrovnávacia pamäť ... 112
7.1 Našla sa infiltrácia ... 112

7.1 Rezidentná ochrana súborového systému ... 113
7.1 Parametre ThreatSense ... 115
7.1 Doplňujúce parametre ThreatSense ... 119
7.1 Prípony súborov vylúčené z kontroly ... 119
7.1 Vylúčenia procesov ... 119
7.1 Ochrana s podporou cloudu ... 121
7.1 Filter vylúčení ... 122
7.1 Detekcia malvéru ... 123
7.1 Manažér profilov ... 124
7.1 Ciele profilu ... 125
7.1 Ciele kontroly ... 127
7.1 Kontrola v nečinnosti ... 128
7.1 Kontrola pri štarte ... 129
7.1 Kontrola súborov spúšťaných pri štarte počítača ... 129
7.1 Vymeniteľné médiá ... 130
7.1 Ochrana dokumentov ... 130
7.1 Kontrola Hyper-V ... 131
7.1 HIPS ... 133
7.1 Nastavenie pravidla HIPS ... 135
7.1 Rozšírené nastavenia HIPS ... 138
7.2 Nastavenia aktualizácie ... 138
7.2 Vrátenie zmien aktualizácií ... 142
7.2 Naplánovaná úloha – Aktualizácia ... 143
7.2 Aktualizačný mirror server ... 143
7.3 Ochrana siete ... 145
7.3 IDS výnimky ... 146
7.3 Dočasný blacklist IP adries ... 147
7.4 Web a e-mail ... 147
7.4 Filtrovanie protokolov ... 148
7.4 Webové a e-mailové klienty ... 149
7.4 SSL/TLS ... 149
7.4 Zoznam známych certifikátov ... 150
7.4 Šifrovaná SSL komunikácia ... 151
7.4 Ochrana e-mailových klientov ... 152
7.4 E-mailové protokoly ... 153
7.4 Upozornenia a udalosti ... 154
7.4 Panel nástrojov MS Outlook ... 154
7.4 Panel nástrojov v Outlook Express a Windows Mail ... 155
7.4 Potvrdzovacie dialógové okno ... 155
7.4 Opätovná kontrola správ ... 156
7.4 Ochrana prístupu na web ... 156
7.4 Manažment URL adries ... 157
7.4 Vytvorenie nového zoznamu ... 158
7.4 Antiphishingová ochrana ... 160
7.5 Správa zariadení ... 161
7.5 Pravidlá zariadení ... 162
7.5 Skupiny zariadení ... 164
7.6 Konfigurácia nástrojov ... 165
7.6 Časové intervaly ... 165
7.6 Microsoft Windows® Update ... 166
7.6 Modul kontroly cez príkazový riadok ... 166

7.6 ESET CMD ... 168
7.6 ESET RMM ... 170
7.6 Licencia ... 171
7.6 Poskytovateľ WMI ... 171
7.6 Poskytnuté údaje ... 172
7.6 Prístup k poskytnutým údajom ... 179
7.6 Ciele kontroly v ESET PROTECT ... 180
7.6 Režim prepísania ... 180
7.6 Protokoly ... 184
7.6 Proxy server ... 185
7.6 Oznámenia ... 186
7.6 Oznámenia aplikácie ... 187
7.6 Oznámenia na ploche ... 187
7.6 E-mailové oznámenia ... 188
7.6 Prispôsobenie ... 189
7.6 Prezentačný režim ... 190
7.6 Diagnostika ... 190
7.6 Technická podpora ... 192
7.6 Klaster ... 192
7.7 Používateľské rozhranie ... 193
7.7 Upozornenia a okná správ ... 194
7.7 Nastavenia prístupu ... 195
7.7 ESET Shell ... 196
7.7 Vypnutie grafického používateľského rozhrania (GUI) na terminálovom serveri ... 196
7.7 Vypnuté správy a stavy ... 197
7.7 Nastavenia stavov aplikácie ... 197
7.7 Ikona na paneli úloh ... 198
7.8 Vrátiť späť na predvolené nastavenia ... 199
7.9 Pomocník a podpora ... 200
7.9 Odoslať žiadosť na technickú podporu ... 201
7.9 O programe ESET Security for Microsoft SharePoint ... 202
7.10 Slovník pojmov ... 202
8 Licenčná dohoda s koncovým používateľom ... 202
9 Zásady ochrany osobných údajov ... 208

Úvod

Pripravili sme pre vás používateľskú príručku, ktorá vám pomôže pri používaní programu ESET Security for Microsoft SharePoint. Pre spustenie pomocníka k časti programu, v ktorej sa nachádzate, stlačte kláves **F1**. Zobrazí sa Pomocník programu pre sekciu programu, ktorú máte otvorenú.

Pre zachovanie konzistencie, a aby sa zabránilo zámene, je terminológia použitá v tejto príručke založená na názvoch parametrov nástroja ESET Security for Microsoft SharePoint. Používame tiež jednotnú sadu symbolov na zvýraznenie kapitol, ktoré sú zvlášť dôležité alebo sú iným spôsobom markantné.

Poznámka:
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.

Dôležité:
Takéto označenie vyžaduje vašu pozornosť a neodporúča sa ho ignorovať. Väčšinou ide o dôležité, avšak nie kritické informácie.

Upozornenie:
Toto označenie obsahuje mimoriadne dôležité informácie, pri ktorých by ste mali spozornieť. Varovania sú umiestnené tak, aby vás varovali včas 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.

Príklad:
Ide o prípad použitia alebo praktické znázornenie, ktorého cieľom je pomôcť vám porozumieť, ako je možné využiť konkrétnu funkciu.

Ak je v pravom hornom rohu stránky pomocníka zobrazený nasledujúci prvok, znázorňuje navigáciu v používateľskom rozhraní ESET Security for Microsoft SharePoint. Pomocou týchto inštrukcií sa dostanete do sekcie programu, ktorej je venovaná príslušná kapitola.

Otvorte ESET Security for Microsoft SharePoint
Kliknite na Nastavenia > Server > Nastavenia kontroly OneDrive > Registrovať 

Formátovanie:

Konvencia	Význam
Tučné písmo	Nadpisy sekcií, názvy funkcií alebo položky používateľského rozhrania, ako napr. tlačidlá.

Konvencia	Význam
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 systému Windows a ďalšie programy.

Príručka pre ESET Security for Microsoft SharePoint je rozdelená na niekoľko kapitol a podkapitol. Vďaka tomu môžete nájsť relevantné informácie jednoduchým prechádzaním Obsahu. Môžete tiež prípadne použiť textové vyhľadávanie podľa konkrétnych slov a fráz.

Prehľad

ESET Security for Microsoft SharePoint je integrované riešenie špeciálne vyvinuté pre rodinu produktov Microsoft SharePoint bežiacich na operačných systémoch Microsoft Windows Server, či už na samostatnom serveri (Standalone) alebo v prostredí serverovej farmy (Server Farm). Prináša efektívnu a stabilnú ochranu proti rôznym druhom malvéru, vírusov a iných infiltrácií. ESET Security for Microsoft SharePoint chráni súbory uložené v obsahovej databáze SharePointu. Chránené sú nielen súbory od používateľov uložené v knižniciach dokumentov, knižniciach materiálov, stránkach wiki a podobne, ale rovnako aj stránky ASP, (JavaScript) skripty, obrázky a pod., ktoré tvoria samotnú lokalitu SharePoint.

ESET Security for Microsoft SharePoint chráni obsah:

- filtrovaním počas prístupu k súborom (Filtrovanie pri prístupe),
- manuálnou kontrolou databáz na základe podnetu od používateľa (Manuálna kontrola).

Filtrovanie pri prístupe je spúšťané samotným serverom SharePoint a jeho správanie sa mierne líši v závislosti od použitej generácie produktu SharePoint (2010 v. 2007). Obvykle je filtrovanie spustené pri prvom prístupe k súboru a výsledok kontroly je uložený vo vyrovnávacej pamäti, až pokým sa nezmení verzia vírusovej databázy alebo neubehne určitý čas.

Mnauálna kontrola databáz hierarchicky prehľadáva všetky súbory a priečinky webových stránok, ktoré sú označené správcom systému. Prístup k súborom je zabezpečený objektovým modelom SharePoint (založeným na technológii .NET), ktorý poskytuje ucelený pohľad do celého obsahu serverovej farmy SharePoint a abstrahuje ho od použitej technológie databázového servera.

Filtrovanie pri prístupe aj manuálna kontrola databáz používajú nasledujúce druhy kontroly:

- antivírusová a antispywarová ochrana,
- pravidlá definované používateľom s rôznymi druhmi podmienok.

Hlavné funkcie

V nasledujúcej tabuľke nájdete zoznam funkcií, ktoré sú dostupné v ESET Security for Microsoft SharePoint. ESET Security for Microsoft SharePoint podporuje takmer všetky verzie Microsoft Windows Server 2008 R2 SP1, 2012, 2016 a 2019 v samostatných alebo klastrových prostrediach. Vzdialenú správu produktu ESET Security for Microsoft SharePoint vo väčších sieťach umožňuje nástroj ESET PROTECT.

64-bitové jadro	Prispieva k vyššej výkonnosti a stabilite súčastí tvoriacich jadro produktu.
Počítadlá výkonu	Počítadlá výkonu vám umožňujú monitorovať celkový výkon programu ESET Security for Microsoft SharePoint.
Filtrovanie pri prístupe	Ochrana súborov, ktorá funguje na princípe filtrovania počas prístupu k súborom.
Manuálna kontrola	Ochrana súborov prostredníctvom kontroly databáz, ktorej spustenie je iniciované používateľom alebo naplánované na konkrétny čas
Pravidlá definované používateľom	Umožňujú správcovi vytvárať a spravovať vlastné pravidlá filtrovania súborov zadefinovaním podmienok a akcií, ktoré sa majú vykonať s filtrovanými súbormi.
Automatické vylúčenia	Automatická detekcia a vylúčenie kritických aplikácií a serverových súborov pre bezproblémové fungovanie a výkon.
Self-Defense	Sebaobrana bezpečnostných produktov spoločnosti ESET, ktorá chráni súčasti programu pred zmenou alebo pred vypnutím ochrany.
Efektívne riešenie problémov	Zabudované nástroje na riešenie rôznych problémov: ESET SysInspector na diagnostiku systému a ESET SysRescue Live na vytvorenie spúšťacieho obnovovacieho CD alebo USB.
Klaster ESET	Produktom spoločnosti ESET určeným pre servery umožňuje navzájom komunikovať, vymieňať si dáta, ako napr. nastavenia a oznámenia, a taktiež vykonávať synchronizáciu dát potrebných pre správne fungovanie skupiny produktov. Vďaka tomu je zaistená konzistentná konfigurácia produktu naprieč celým klastrom. ESET Security for Microsoft SharePoint podporuje klastre typu Windows Failover Cluster a Network Load Balancing (NLB) Cluster. Členov klastra ESET môžete pridať aj manuálne bez klastra Windows. Klastre ESET pracujú v doméne aj v pracovnej skupine.
Inštalácia súčastí	Vyberte súčasti, ktoré chcete pridať alebo odstrániť.
Kontrola úložiska	Kontroluje súbory zdieľané na lokálnom serveri. Vďaka tomu je možné jednoduchým spôsobom selektívne skontrolovať len dáta používateľov, ktoré sú uložené na serveri.
Vylúčenia procesov	Vylučuje z antivírusovej kontroly konkrétne procesy. Vzhľadom na mimoriadne dôležitú úlohu jednoúčelových serverov (application server, storage server atď.) sú nevyhnutnosťou pravidelné zálohy pre zabezpečenie včasnej obnovy pri fatálnych incidentoch každého druhu. Pre zlepšenie rýchlosti zálohy, integrity a dostupnosti služieb, sa pri zálohovaní používajú niektoré techniky, ktoré sa dostávajú do konfliktu s antivírusovou kontrolou súborov. Podobné konflikty môžu nastať aj pri živej migrácii virtuálnych počítačov. Jediným efektívnym riešením je v tomto prípade vypnutie antivírusu. Vylúčením konkrétneho procesu (napr. procesu používaného pri zálohovaní) budú všetky operácie so súbormi pre daný vylúčený proces ignorované a považované za bezpečné, čím sa zároveň minimalizuje možné riziko prerušenia zálohovania dát. Pri výbere vylúčení odporúčame byť maximálne opatrný – zálohovacie nástroje vylúčené z kontroly totiž môžu pristupovať k infikovaným súborom bez toho, aby sa spustilo upozornenie, čo je vlastne dôvod, prečo sú rozšírené oprávnenia dostupné len pre modul rezidentnej ochrany.
eShell (ESET Shell)	eShell 2.0 je teraz dostupný pre ESET Security for Microsoft SharePoint. eShell je nástroj s príkazovým riadkom pre pokročilých používateľov, ktorým ponúka komplexnú správu produktov ESET určených pre server.
ESET PROTECT	Lepšia integrácia s ESET PROTECT vrátane možnosti naplánovať Manuálnu kontrolu. Viac informácií o ESET PROTECT sa nachádza v Online pomocníkovi pre nástroj ESET PROTECT.
Kontrola Hyper-V	Kontrola Hyper-V je nová technológia, ktorá umožňuje kontrolu diskov virtuálnych počítačov (VP) na serveri Microsoft Hyper-V bez potreby nasadeného „Agenta“ na danom virtuálnom počítači.

Čo je nové

ESET Security for Microsoft SharePoint predstavuje nasledujúce nové funkcie:

- 64-bitové jadro
- Priamy prístup k SQL databáze
- Počítadlá výkonu
- Podpora pre ESET Enterprise Inspector
- ESET RMM
- Izolácia siete
- Ochrana využívajúca strojové učenie
- Protokoly auditu
- mikroaktualizácie programových súčastí (µPCU)

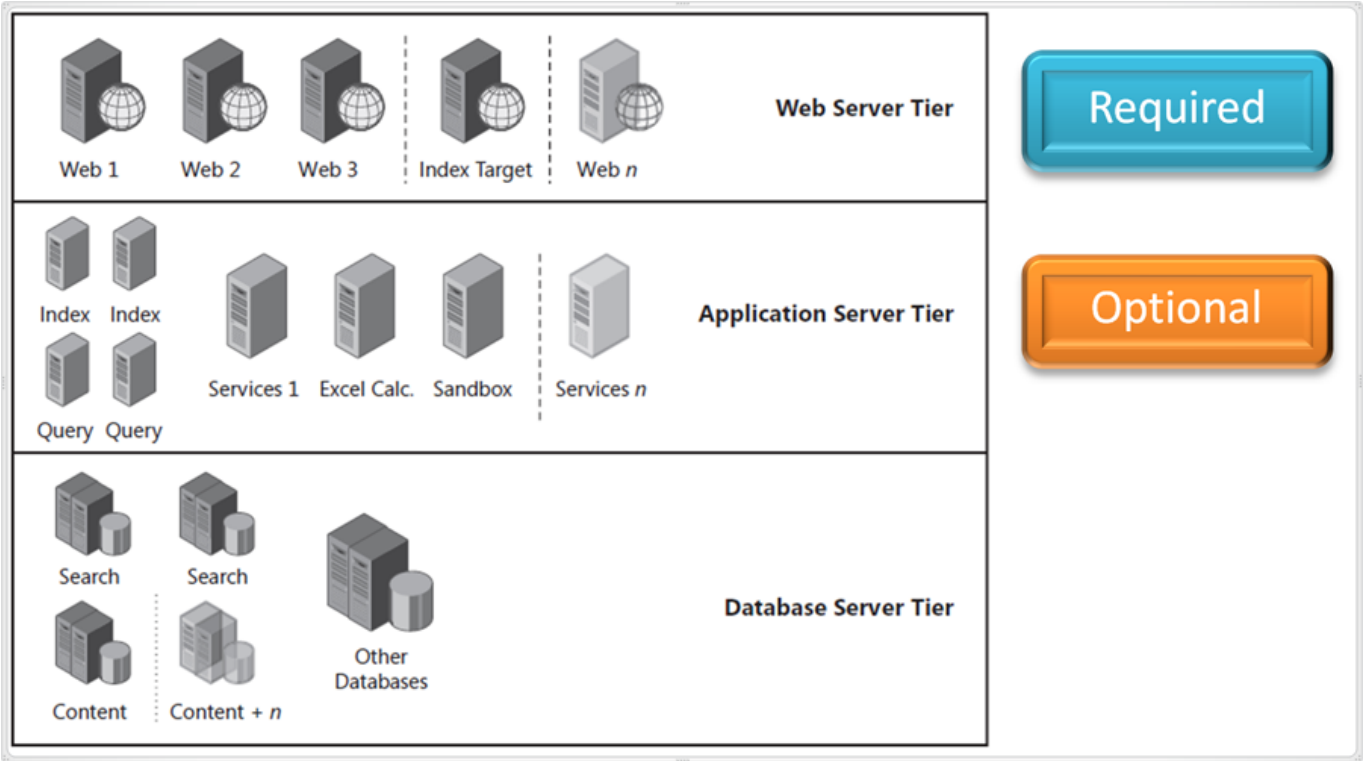
Nasadenie

Nasledujúce kapitoly vám pomôžu zvoliť si to najvhodnejšie nasadenie produktu ESET Security for Microsoft SharePoint vo vašej infraštruktúre SharePoint, predovšetkým ak používate serverovú farmu SharePoint alebo serverové klastre.

Nasadenie vo farme SharePoint

ESET Security for Microsoft SharePoint musí byť nainštalovaný na všetkých serveroch SharePoint s rolou Webového servera, aby bola zabezpečená ochrana používateľov pomocou kontroly pri prístupe k súborom. Každý z týchto serverov môže byť použitý na spustenie kontroly databáz. ESET Security for Microsoft SharePoint je možné nainštalovať aj na server(y) SharePoint s rolou Aplikačného servera, z ktorého sa taktiež dá vykonať manuálna kontrola obsahovej databázy SharePointu. Filtrovanie pri prístupe k súborom však na aplikačnom serveri možné nie je.

Nižšie uvedená schéma zobrazuje časti serverového prostredia, na ktorých je inštalácia bezpečnostného riešenia ESET nevyhnutná a na ktorých je naopak voliteľná.



Poznámka:
Manuálnu kontrolu databáz stačí spúšťať z jedného servera farmy SharePoint. Skontrolovaná bude databáza celej serverovej farmy SharePoint.

Keďže manuálna kontrola databáz je operácia náročná na systémové zdroje, odporúčame spúšťať ju na serveri, pre ktorý zvýšená záťaž nebude problémom. Z hľadiska funkčnosti je však Manuálnu kontrolu databáz možné spúšťať z ktoréhokoľvek servera farmy SharePoint, ktorý má prístup k obsahovej databáze, bez ohľadu na jeho rolu.

Rýchlosť Manuálnej kontroly databáz závisí najmä od priepustnosti a výkonovej kapacity databázového servera a od siete, v ktorej sa SharePoint farma nachádza. Zvýšiť rýchlosť Manuálnej kontroly databáz vo veľkých farmách SharePoint môžete tak, že kontrolu databáz spustíte na viac ako jednom serveri a tieto servery následne nastavíte tak, aby každý kontroloval inú (neprekrývajúcu sa) časť obsahovej databázy. Takáto paralelná kontrola by však spôsobila zvýšenie záťaže samotného databázového servera, a preto by výhody takejto kontroly mal zhodnotiť správca farmy SharePoint.

Inštalácia v klastrovom prostredí

Produkt ESET Security for Microsoft SharePoint môžete nasadiť v klastrovom prostredí (napríklad vo failover klastri). Odporúčame nainštalovať ESET Security for Microsoft SharePoint na aktívny uzol a potom umiestniť inštaláciu na pasívny uzol/uzly za použitia funkcie klaster ESET produktu ESET Security for Microsoft SharePoint. Odhliadnuc od inštalácie bude klaster ESET slúžiť ako replikácia konfigurácie ESET Security for Microsoft SharePoint na zabezpečenie konzistencie medzi uzlami klastra potrebnými pre správne fungovanie.

Typy ochrany SharePoint

ESET Security for Microsoft SharePoint poskytuje dva druhy ochrany SharePoint:

- antivírusovú ochranu,

- antispywarovú ochranu.

Ochrana SharePoint je zabezpečovaná pomocou:

- filtrovania počas prístupu k súborom (Filtrovanie pri prístupe),
- manuálnej kontroly databáz na základe podnetu od používateľa (Manuálna kontrola).

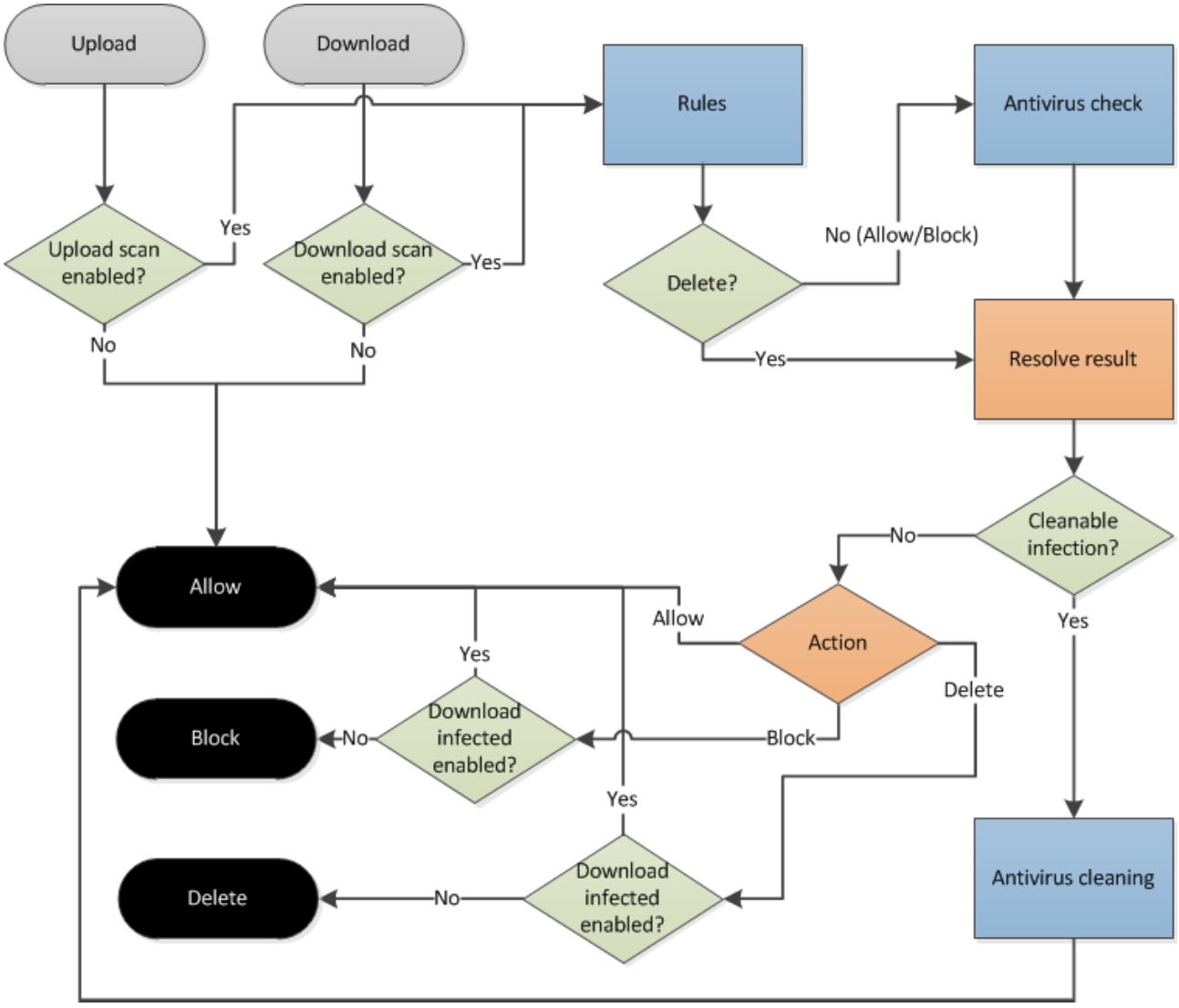
Integrácia so SharePointom

Táto časť popisuje vlastnosti a fungovanie Filtrovania pri prístupe a Manuálnej kontroly databáz a taktiež to, ako sú tieto funkcie integrované do SharePointu.

Filtrovanie pri prístupe

Filtrovanie pri prístupe kontroluje všetky súbory v súlade s nastaveniami ochrany SharePoint. Napríklad pri kontrole dokumentu balíka MS Office uloženého v SharePointe sa skontrolujú aj obrázky, `aspx` súbory (ktoré tvoria samotné stránky SharePoint), css štýly a ikony súvisiace s daným dokumentom MS Office. Rozsah súborov posielaných na kontrolu prostredníctvom VSAPI závisí od nastavení SharePointu. ESET Security for Microsoft SharePoint nemôže aktívne rozhodovať o tom, ktoré súbory budú kontrolované. Keď je súbor zaslaný na kontrolu/liečenie, ESET Security for Microsoft SharePoint rozpoznáva len názov a veľkosť tohto súboru. ESET Security for Microsoft SharePoint však nemá dosah na iné podrobnosti o súbore, napríklad kto je jeho vlastník, aké je jeho umiestnenie v SharePoint a to, či bude súbor skontrolovaný pri sťahovaní alebo nahrávaní. Pri zapnutej funkcii **Kontrolovať verzie dokumentov** sa názov súboru zobrazuje len pre aktuálnu verziu súboru, pre staršie verzie daného súboru sa použije zástupný text.

Proces kontroly súborov Filtrovaním pri prístupe je zobrazený v schéme nižšie. Táto schéma znázorňuje možné akcie vykonávané pri kontrole pomocou Filtrovania pri prístupe:



Manuálna kontrola databáz

Manuálna kontrola databáz je funkcia umožňujúca kontrolovať obsahovú databázu SharePoint, ktorá obsahuje súbory a webové stránky SharePoint. Pre každú webovú stránku určenú na kontrolu ESET Security for Microsoft SharePoint skontroluje aj príslušnú štruktúru priečinkov a súborov.

V prípade nájdenia infiltrácie sa vykoná jedna z troch dostupných akcií (ponechať, liečiť a zmazať). Pokiaľ je súbor z akéhokoľvek dôvodu zmazaný, napríklad aj počas liečenia, znamená to, že je presunutý do Koša. Ak je kôš vypnutý, súbor bude nenávratne odstránený.

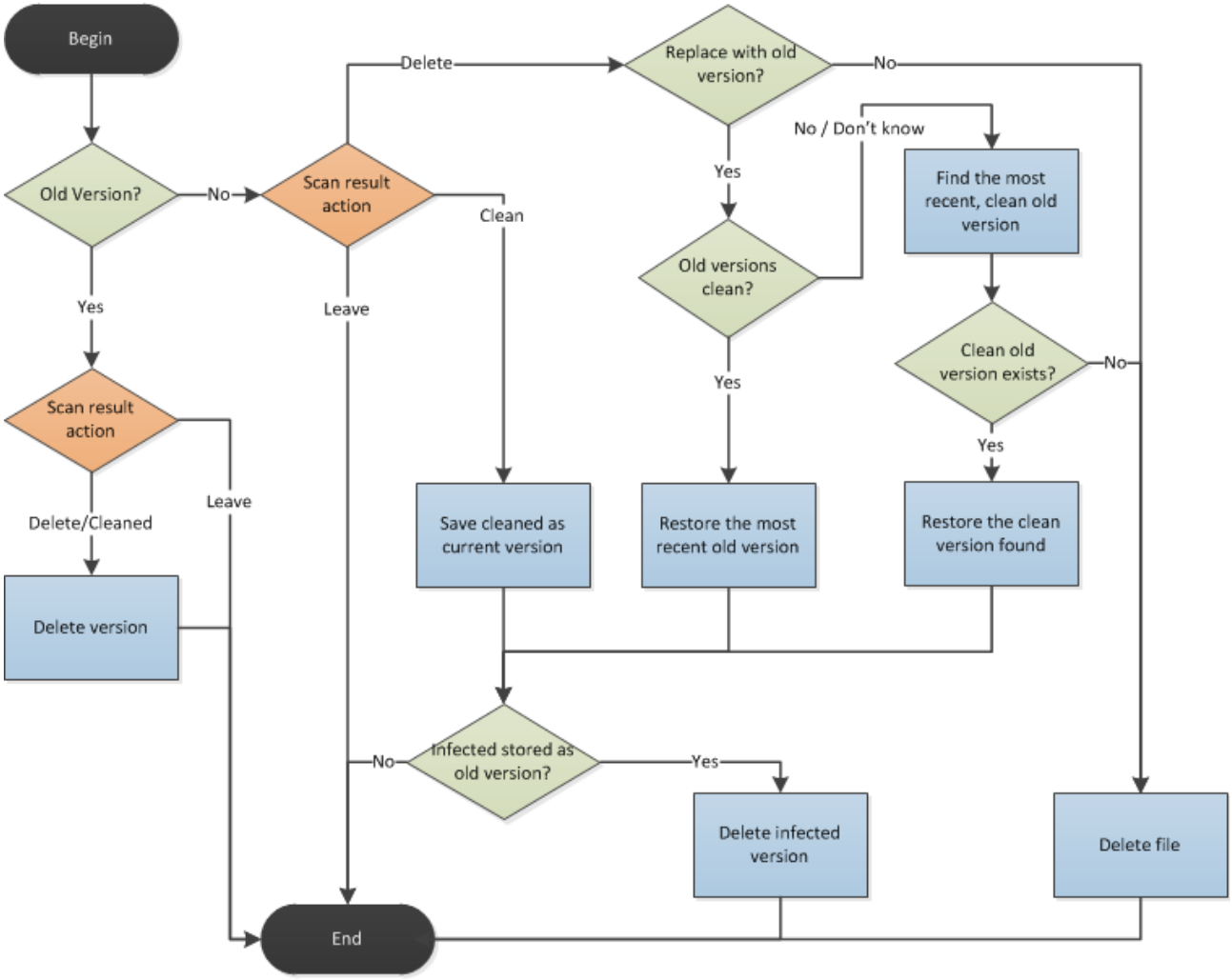
Ak existujú aj staršie verzie konkrétneho súboru a je zapnutá funkcia **Kontrolovať verzie dokumentov**, budú tieto staršie verzie skontrolované ako prvé.

Poznámky ku kontrole verzií dokumentov:

- Kontrola starších verzií dokumentov sa dá aktivovať v nastaveniach programu ESET Security for Microsoft SharePoint (funkcia Kontrolovať verzie dokumentov).
- Pri liečení infikovaného dokumentu sa vytvorí jeho nová verzia. Pôvodná infikovaná verzia bude presunutá do koša.
- Staršie verzie dokumentov nie je možné liečiť, dajú sa iba vymazať.
- V prípade vymazania aktuálnej verzie dokumentu sú staršie verzie zachované. Najnovšia neinfikovaná

verzia je použitá ako náhrada za vymazaný dokument. Túto funkciu je možné aktivovať v nastaveniach programu ESET Security for Microsoft SharePoint (funkcia Pri odstránení dokumentu obnoviť poslednú neinfikovanú verziu) a je funkčná aj vtedy, keď je vypnutá možnosť Kontrolovať verzie dokumentov.

Nasledujúca schéma znázorňuje postup vyhodnocovania výsledku kontroly súboru a následnú akciu (resp. akcie) vykonanú v rámci Manuálnej kontroly databáz:



Príprava na inštaláciu

Existuje niekoľko krokov, ktoré odporúčame vykonať v rámci prípravy na inštaláciu produktu:

- Po zakúpení produktu ESET Security for Microsoft SharePoint si stiahnite inštalačný balík `.msi` z webovej stránky ESET.
- Uistite sa, že server, na ktorý chcete inštalovať ESET Security for Microsoft SharePoint, spĺňa systémové požiadavky.
- Prihláste sa na server pomocou účtu správcu.

Poznámka:
Inštalátor je potrebné spustiť pod vstavaným účtom správcu alebo doménovým účtom správcu (v prípade, že lokálny vstavaný účet správcu nie je povolený). Iní používatelia nebudú mať dostatočné práva na dokončenie inštalácie, a to ani v prípade, že sú v skupine správcov. Je preto nutné použiť vstavaný účet správcu. Inštaláciu nie je možné úspešne dokončiť pod iným používateľským účtom ako lokálnym alebo doménovým účtom správcu.

- Ak chcete vykonať aktualizáciu už nainštalovaného produktu ESET Security for Microsoft SharePoint, odporúčame vám vytvoriť si zálohu aktuálnych nastavení produktu pomocou funkcie Export nastavení.

- V prípade potreby zo svojho systému odinštalujte akýkoľvek antivírusový softvér tretích strán. Na odstránenie/odinštalovanie antivírusového softvéru tretích strán odporúčame použiť nástroj ESET AV Remover. Zoznam antivírusových programov tretích strán, ktoré možno odstrániť pomocou nástroja ESET AV Remover, nájdete v nasledujúcom článku databázy znalostí spoločnosti ESET.

- Pri inštalácii ESET Security for Microsoft SharePoint na Windows Server 2016 spoločnosť Microsoft odporúča zo systému odinštalovať Windows Defender a pre daný systém zrušiť využívanie služby Windows Defender ATP, aby ste predišli problémom zapríčineným súčasným používaním viacerých antivírusových riešení.

Inštalátor programu ESET Security for Microsoft SharePoint môžete spustiť v dvoch režimoch:

- Grafické používateľské rozhranie (GUI)
  Ide o odporúčaný typ inštalácie v podobe sprievodcu inštaláciou.

- Tichá inštalácia/inštalácia bez obsluhy
  Okrem sprievodcu inštaláciou je k dispozícii aj možnosť tichej inštalácie ESET Security for Microsoft SharePoint pomocou príkazového riadka.

Dôležité:
Odporúčame inštalovať ESET Security for Microsoft SharePoint na čistú inštaláciu nakonfigurovaného operačného systému. Ak však potrebujete nainštalovať ESET Security for Microsoft SharePoint na zabehnutý systém, najprv odinštalujte staršie verzie programu, reštartujte server, a až tak nainštalujte novú verziu ESET Security for Microsoft SharePoint.

- Aktualizácia na novú verziu
  Ak používate staršiu verziu ESET Security for Microsoft SharePoint, môžete si vybrať vhodnú metódu aktualizácie.

Po úspešnej inštalácii alebo aktualizácii svojho produktu ESET Security for Microsoft SharePoint ešte môžete vykonať nasledovné:

- Aktivácia produktu
  Dostupnosť konkrétnych možností aktivácie sa môže líšiť v závislosti od spôsobu distribúcie inštalačného súboru.

- Konfigurácia ochrany servera
  Svoj produkt ESET Security for Microsoft SharePoint si môžete prispôsobiť podľa potreby úpravou pokročilých nastavení každej funkcie.

Dôležité:
Odporúčame inštalovať ESET Security for Microsoft SharePoint na čistú inštaláciu nakonfigurovaného operačného systému. Ak však potrebujete nainštalovať ESET Security for Microsoft SharePoint na zabehnutý systém, najprv odinštalujte staršie verzie programu, reštartujte server, a až tak nainštalujte novú verziu ESET Security for Microsoft SharePoint.

- Aktualizácia na novú verziu – ak používate staršiu verziu ESET Security for Microsoft SharePoint, môžete si vybrať vhodnú metódu aktualizácie.
- Aktivácia produktu - Dostupnosť konkrétnych možností aktivácie sa môže líšiť v závislosti od spôsobu distribúcie inštalačného súboru.
- Spravovanie a konfigurácia

Systémové požiadavky

Podporované operačné systémy:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 s nainštalovanou aktualizáciou KB4474419 a KB4490628

Poznámka:
Ak používate Microsoft Windows Server 2008 R2 SP1, prečítajte si kapitolu Potrebná kompatibilita s SHA-2 a uistite sa, že váš operačný systém obsahuje všetky potrebné aktualizácie.

Podporované servery určené pre menšie firmy:

- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Small Business Server 2011 SP1 (64-bitová verzia) s nainštalovanou aktualizáciou KB4474419 a KB4490628

a ktorékoľvek z nasledujúcich aplikačných serverov:

- Microsoft SharePoint Server Subscription Edition
- Microsoft SharePoint Server 2019 (x64) – všetky edície
- Microsoft SharePoint Server 2016 (x64) – všetky edície
- Microsoft SharePoint Server 2013 (x64) – všetky edície
- Microsoft SharePoint Server 2010 (x64) – všetky edície
- Microsoft SharePoint Server 2007 (x86 a x64) – všetky edície

Podporované hostiteľské operačné systémy s rolou Hyper-V:

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 – virtuálne počítače s týmto operačným systémom môžu byť kontrolované, len ak sú v režime offline (vypnuté).

Hardvérové požiadavky závisia od používanej verzie operačného systému. Viac informácií o hardvérových požiadavkách nájdete v produktovej dokumentácii pre Microsoft Windows Server a Microsoft SharePoint Server.

> Poznámka:
> Dôrazne odporúčame, aby ste si ešte pred samotnou inštaláciou bezpečnostného produktu od spoločnosti ESET nainštalovali najnovší Service Pack pre váš operačný systém a serverovú aplikáciu od firmy Microsoft. Tiež odporúčame, aby ste najnovšie aktualizácie a opravy hotfix inštalovali vždy, keď sú dostupné.

Potrebná kompatibilita s SHA-2

Spoločnosť Microsoft oznámila ukončenie používania algoritmu SHA-1 a začiatkom roka 2019 začala migračný proces na SHA-2. To znamená, že certifikáty podpísané algoritmom SHA-1 už nebudú rozpoznané a budú spôsobovať bezpečnostné upozornenia. Bezpečnosť algoritmu SHA-1 v priebehu času utrpela kvôli nedostatkom, ktoré sa našli v algoritme, zvýšenému zaťaženiu procesora a príchodu cloudovej architektúry.

Algoritmus SHA-2 (ako nástupca SHA-1) je teraz preferovanou metódou na zaručenie spoľahlivosti SSL zabezpečenia. Podrobnejšie informácie nájdete v nasledujúcom dokumente.

> Poznámka:
> Táto zmena znamená, že na operačnom systéme bez podpory SHA-2 nebude vaše bezpečnostné riešenie ESET schopné aktualizovať svoje moduly vrátane detekčného jadra, v dôsledku čoho program ESET Security for Microsoft SharePoint nebude plne funkčný a schopný poskytnúť dostatočnú ochranu.

Ak používate **Microsoft Windows Server 2008 R2 SP1**, **Microsoft Windows Small Business Server 2011 SP1** uistite sa, že váš systém je kompatibilný s SHA-2. Nainštalujte potrebné aktualizácie podľa verzie svojho operačného systému:

- **Microsoft Windows Server 2008 R2 SP1** – nainštalujte aktualizáciu KB4474419 a KB4490628 (môže byť potrebný reštart systému).
- **Microsoft Windows Small Business Server 2011 SP1 (x64)** – nainštalujte aktualizáciu KB4474419 a KB4490628 (môže byť potrebný reštart systému).

> Dôležité:
> Po nainštalovaní aktualizácií a reštartovaní systému otvorte grafické používateľské rozhranie programu ESET Security for Microsoft SharePoint a skontrolujte jeho stav. V prípade, že stav je oranžový, vykonajte ďalší reštart systému. Stav by potom mal byť zelený, čo predstavuje maximálne zabezpečenie.

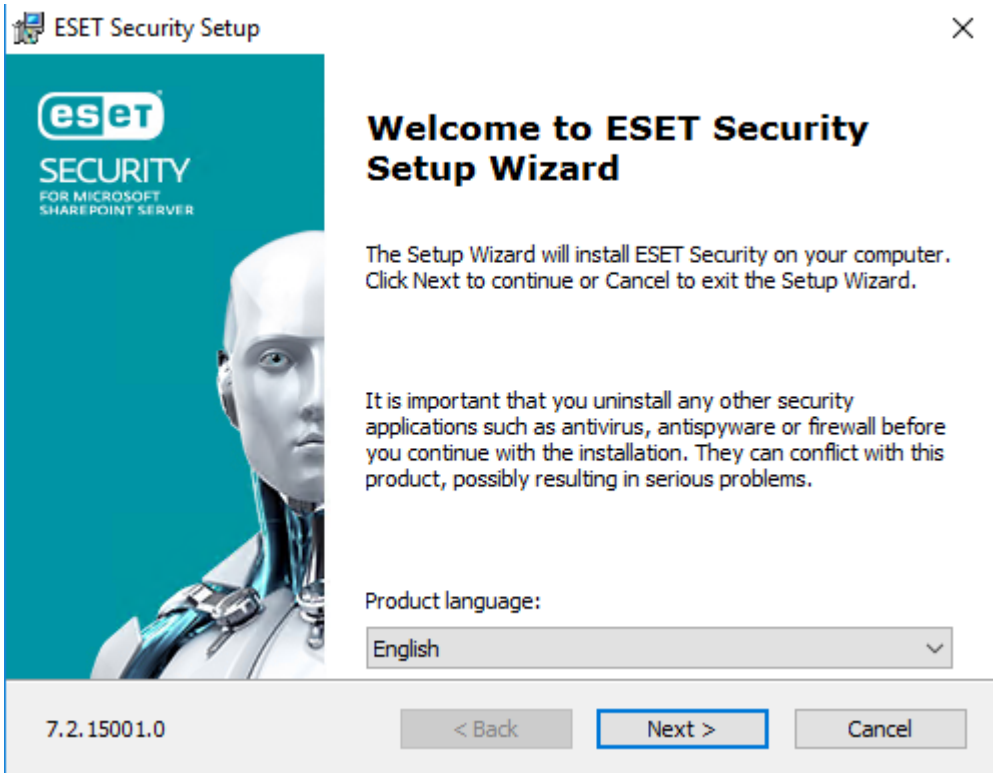
> Poznámka:
> Dôrazne odporúčame, aby ste si nainštalovali najnovší Service Pack pre svoj operačný systém a serverovú aplikáciu od spoločnosti Microsoft. Tiež odporúčame, aby ste najnovšie aktualizácie a opravy inštalovali vždy, keď sú dostupné.

Inštalácia ESET Security for Microsoft SharePoint

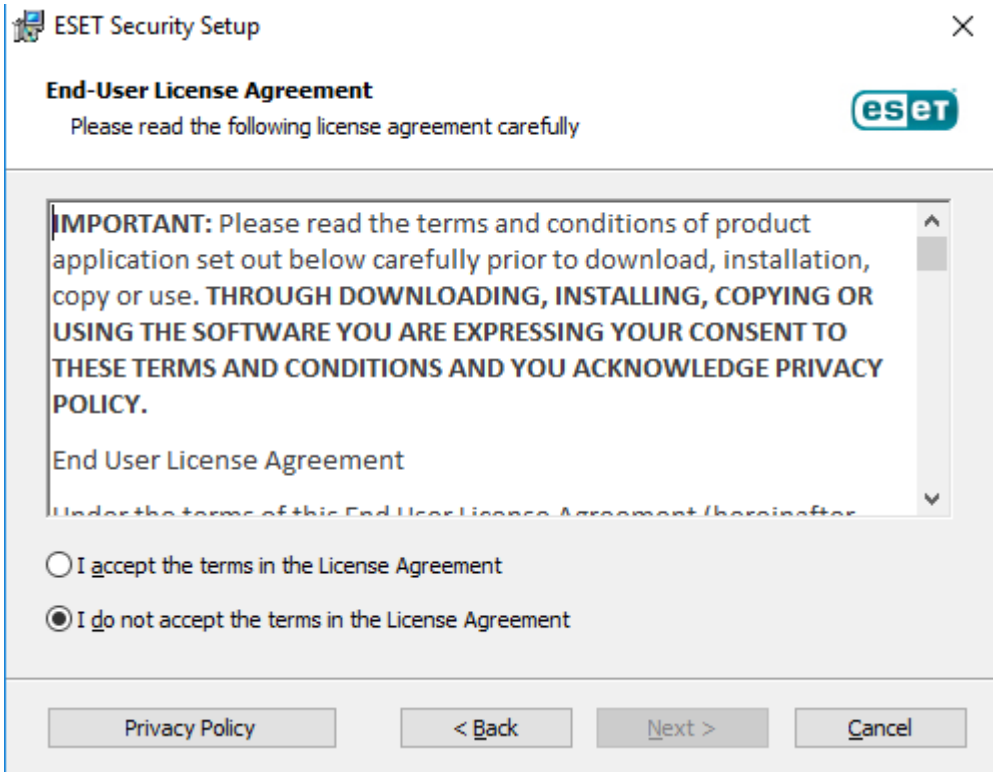
Ide o typického sprievodcu inštaláciou prostredníctvom grafického požívateľského rozhrania. Dvakrát kliknite na inštalačný balík `.msi` a postupujte podľa nasledujúcich krokov pre inštaláciu ESET Security for Microsoft SharePoint:

1. Kliknite na **Ďalej** pre pokračovanie alebo kliknite na **Zrušiť**, ak chcete ukončiť inštaláciu.

2. Sprievodca inštaláciou je v jazyku, ktorý je určený v rámci **Home location** v nastavení **Region** > **Location** na vašom operačnom systéme (alebo v rámci **Current location** v nastavení **Region and Language** > **Location** na starších systémoch). Pomocou roletového menu vyberte **Jazyk produktu**, v ktorom bude produkt ESET Security for Microsoft SharePoint nainštalovaný. Jazyk zvolený pre ESET Security for Microsoft SharePoint nie je závislý od jazyka, v ktorom je sprievodca inštaláciou.



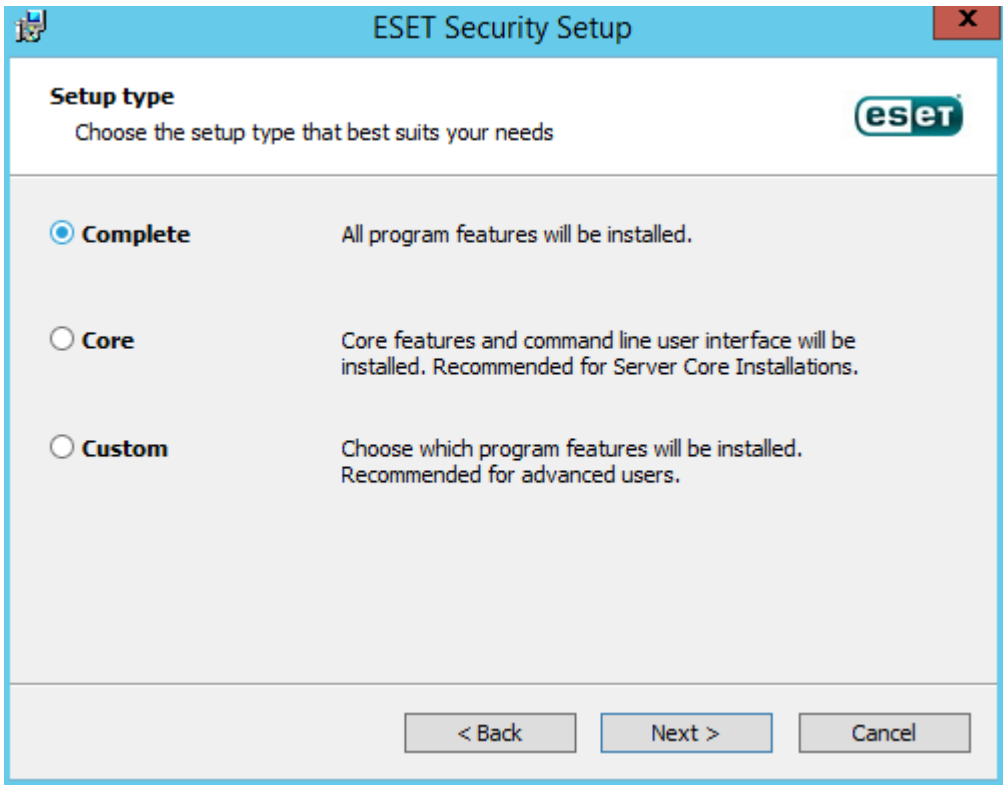
3. Po kliknutí na **Ďalej** sa zobrazí Licenčná dohoda s koncovým používateľom. Po potvrdení vášho súhlasu s podmienkami Licenčnej dohody s koncovým používateľom a Zásadami ochrany osobných údajov kliknite na **Ďalej**.



4. Vyberte si jeden z dostupných typov inštalácie (dostupnosť závisí od vášho operačného systému).

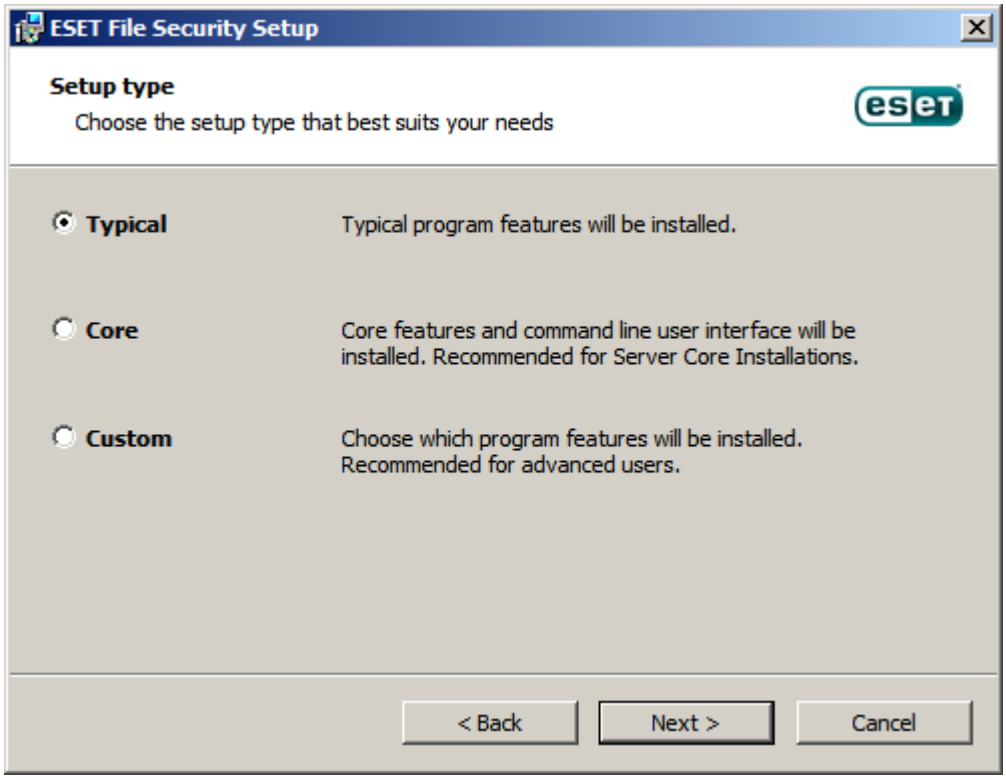
Úplná

Budú nainštalované všetky funkcie produktu ESET Security for Microsoft SharePoint. Táto inštalácia sa tiež nazýva kompletná inštalácia. Ide o odporúčaný typ inštalácie, ktorá je dostupná pre **Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials a 2019 Essentials**.



Typická

Nainštaluje odporúčané funkcie produktu ESET Security for Microsoft SharePoint. Táto inštalácia je dostupná pre Windows Server 2008 R2 SP1, Windows Small Business Server 2011 SP1.



Základná

Tento typ inštalácie je určený pre server typu Windows Server Core. Postup inštalácie je rovnaký ako pri Kompletnej inštalácii, avšak inštalátor vyberie len základné funkcie a ovládanie cez príkazový riadok. Hoci je základná inštalácia určená hlavne pre Windows Server Core, môžete ju v prípade potreby použiť aj na štandardných Windows serveroch. Bezpečnostné produkty ESET nainštalované v rámci základnej inštalácie nebudú mať grafické používateľské rozhranie. To znamená, že ESET Security for Microsoft SharePoint budete ovládať len cez príkazový riadok. Podrobnejšie informácie a parametre nájdete v kapitole Inštalácia cez príkazový riadok.

Príklad:
Pre spustenie základnej inštalácie pomocou príkazového riadka použite nasledujúci vzorový príkaz:

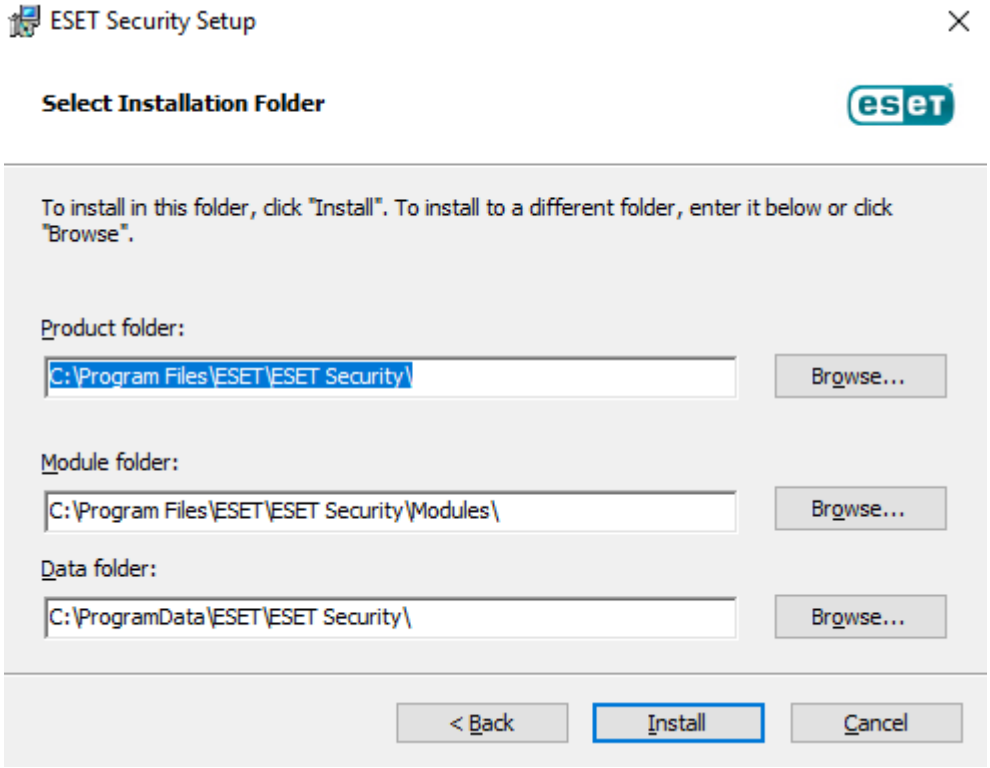
```
msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base
```

Vlastná

Vlastná inštalácia vám umožňuje vybrať, ktoré funkcie ESET Security for Microsoft SharePoint budú na systém nainštalované. Pred začatím inštalácie sa zobrazí zoznam modulov a funkcií produktu. Je to užitočné v prípade, ak si chcete prispôsobiť vašu inštaláciu a nainštalovať len súčasti produktu ESET Security for Microsoft SharePoint, ktoré potrebujete.

Poznámka:
Na operačných systémoch Windows Server 2008 R2 SP1 je inštalácia komponentu **Ochrana siete** štandardne zakázaná (**Typická** inštalácia). Ak chcete mať tento komponent nainštalovaný, zvoľte **Vlastný** typ inštalácie.

5. Budete vyzvaný na nastavenie cesty k adresáru, kam bude ESET Security for Microsoft SharePoint nainštalovaný. Štandardne sa program inštaluje do adresára *C:\Program Files\ESET\ESET Security for Microsoft SharePoint*. Kliknite na možnosť **Prechádzať** pre zmenu umiestnenia (neodporúča sa).

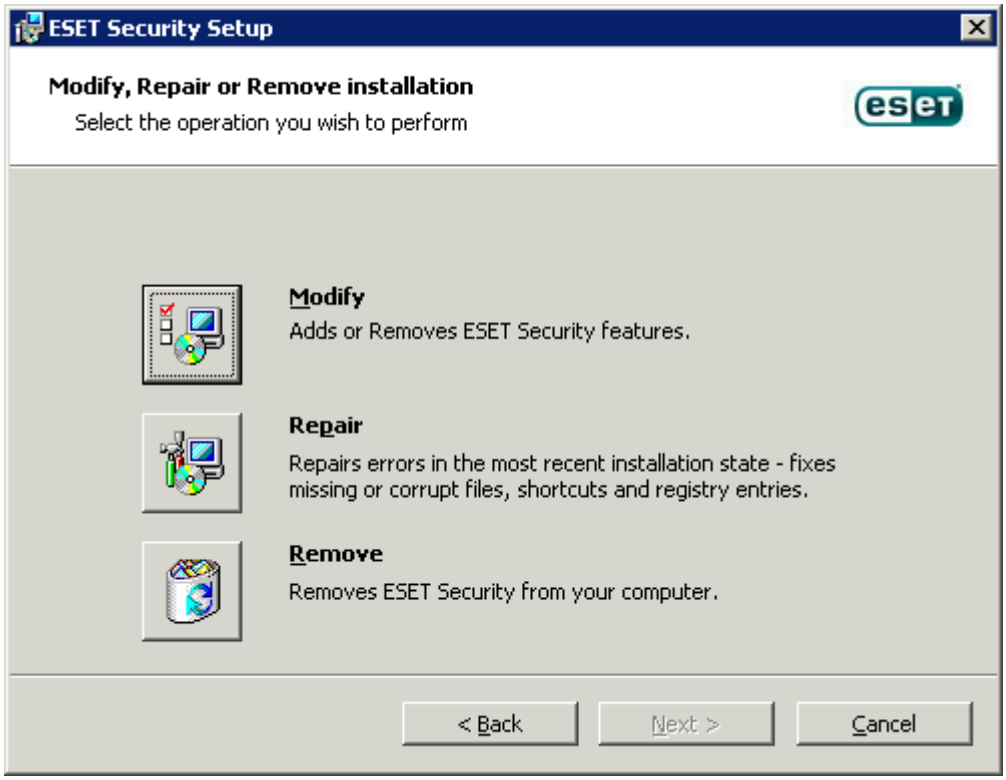


6.Kliknite na tlačidlo **Inštalovať** pre spustenie inštalačného procesu. Po dokončení inštalácie sa spustí grafické používateľské rozhranie ESET a na paneli úloh (v oblasti oznámení systému) sa zobrazí ikona.

Úprava existujúcej inštalácie

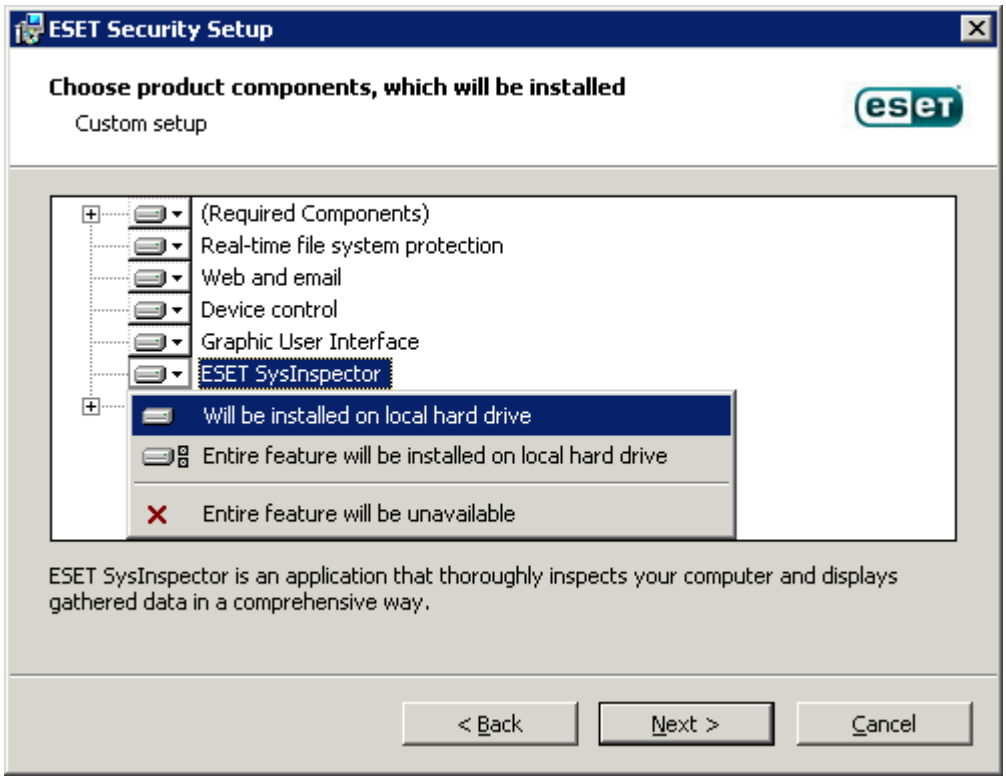
Môžete pridať/odobrať súčasti do/z existujúcej inštalácie. Stačí znova spustiť inštalačný balík s koncovkou `.msi`, z ktorého ste program nainštalovali, alebo cez Ovládací panel v systéme Windows spustite **Programy a súčasti**. V tomto okne kliknite pravým tlačidlom na ESET Security for Microsoft SharePoint a vyberte možnosť **Zmeniť**. Postupujte podľa návodu nižšie pre odstránenie alebo pridanie súčastí.

Sú dostupné tri možnosti. Môžete **Zmeniť** nainštalované súčasti, **Opraviť** inštaláciu programu ESET Security for Microsoft SharePoint alebo **Odstrániť**, teda odinštalovať program.



Ak vyberiete možnosť **Zmeniť**, zobrazí sa zoznam dostupných programových súčastí.

Vyberte súčasti, ktoré chcete pridať alebo odstrániť. Môžete označiť viacero súčastí súčasne. Kliknite na danú súčasť programu a vyberte možnosť z roletového menu:



Po vybratí možnosti kliknite na **Zmeniť** pre potvrdenie zmien.

Poznámka:
Zmeniť nainštalované súčasti môžete kedykoľvek spustením inštalátora. Pri zmene väčšiny súčastí nie je nutné vykonať reštart servera. Grafické používateľské rozhranie sa reštartuje a po jeho zapnutí sa zobrazia len súčasti, ktoré ste zvolili pri inštalácii. Pri súčastiach, ktoré vyžadujú reštart servera, vás Windows Installer automaticky vyzve na reštart systému, pričom nové súčasti budú dostupné hneď po zapnutí servera.

Tichá inštalácia/inštalácia bez obsluhy

Pre nainštalovanie produktu spustite cez príkazový riadok nasledujúci príkaz: `msiexec /i <packagename> /qn /l*xv msi.log`

Poznámka:
Na systémoch Windows Server 2008 R2 SP1 nebude nainštalovaná funkcia **Ochrana siete**.

Ak sa chcete uistiť, že inštalácia prebehla úspešne, prípadne ak pri inštalácii nastali problémy, použite Zobrazovač udalostí systému Windows a skontrolujte **Denník aplikácie** (hľadajte záznamy pre Zdroj: MsiInstaller).

Príklad:
Úplná inštalácia na 64-bitovom systéme:
```
msiexec /i eshp_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Po dokončení inštalácie sa spustí grafické používateľské rozhranie ESET a na paneli úloh (v oblasti oznámení systému) sa zobrazí ikona.

Príklad:
Inštalácia produktu v **konkrétnom jazyku** (nemčina):
```
msiexec /i eshp_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Podrobnejšie informácie a zoznam jazykových kódov nájdete v sekcii **Jazykové parametre** v kapitole Inštalácia cez príkazový riadok.

Dôležité:
Pri definovaní parametra `REINSTALL` musíte uviesť všetky zostávajúce funkcie, ktoré ste nezadefinovali v parametri `ADDLOCAL` alebo `REMOVE`. Aby inštalácia cez príkazový riadok prebehla úspešne, je nevyhnutné, aby ste pri definovaní parametrov REINSTALL, `ADDLOCAL` a `REMOVE` uviedli všetky funkcie. Pridanie alebo odobranie funkcie sa nemusí podariť, ak nepoužijete parameter `REINSTALL`.
Úplný zoznam funkcií produktu nájdete v kapitole Inštalácia cez príkazový riadok.

Príklad:
Kompletné odstránenie (odinštalovanie) z 64-bitového systému:
```
msiexec /x eshp_nt64.msi /qn /l*xv msi.log
```
Po úspešnom odinštalovaní sa server automaticky reštartuje.

Inštalácia cez príkazový riadok

Nasledujúce nastavenia sú určené na použitie **len pri obmedzenom**, **základnom** alebo **žiadnom** používateľskom grafickom rozhraní. Podrobnejšie informácie o príkazoch v príkazovom riadku nájdete v dokumentácii nástroja

msiexec.

Podporované parametre:

APPDIR=<path>

- path – platná cesta k adresáru
- Adresár, do ktorého bude aplikácia nainštalovaná.
- Napríklad: `eshp_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- path – platná cesta k adresáru
- Adresár, do ktorého budú nainštalované dátové súbory 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`: `eshp_nt64.msi /qn ADDLOCAL=<list>`
- Viac informácii o parametri `ADDLOCAL` nájdete na webovej stránke https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal.
- Zoznam `ADDLOCAL` je zoznam čiarkou oddelených funkcií, ktoré budú nainštalované.
- Pri výbere funkcie na inštaláciu musí byť v zozname uvedená úplná cesta (vrátane všetkých nadradených funkcií).

REMOVE=<list>

- Inštalácia súčastí – nadradená funkcia , ktorú nechcete mať nainštalovanú lokálne.
- Použitie s ESET inštalačnými balíkmi `.msi`: `eshp_nt64.msi /qn REMOVE=<list>`
- Viac informácii o parametri `REMOVE` nájdete na webovej stránke https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove.
- Zoznam `REMOVE` je zoznam čiarkou oddelených nadradených funkcií, ktoré nebudú nainštalované (alebo budú odstránené v prípade existujúcej inštalácie).
- Stačí, ak uvediete iba nadradenú funkciu. Nie je potrebné zadávať do zoznamu každú podradenú funkciu.

ADDEXCLUDE=<list>

- Zoznam `ADDEXCLUDE` je zoznam čiarkou oddelených funkcií, ktoré nebudú nainštalované.
- Pri výbere funkcie, ktorá nemá byť nainštalovaná, musí byť v zozname zadaná jej úplná cesta (t. j. vrátane všetkých podfunkcií) a všetky súvisiace neviditeľné funkcie.
- Napríklad: `eshp_nt64.msi /qn ADDEXCLUDE=<list>`

> Poznámka:
> `ADDEXCLUDE` nemôže byť používaný spolu s parametrom `ADDLOCAL`.

Prítomnosť funkcie

- **Povinné** – táto funkcia bude nainštalovaná vždy.
- **Voliteľné** – výber tejto funkcie môžete zrušiť.
- **Neviditeľné** – funkcia je potrebná pre správne fungovanie inej funkcie.

Zoznam funkcií programu ESET Security for Microsoft SharePoint:

> Dôležité:
> V názvoch funkcií sa rozlišujú veľké a malé písmená. Napríklad, `RealtimeProtection` nie je to isté ako `REALTIMEPROTECTION`.

Názov funkcie	Prítomnosť funkcie
SERVER	Povinné
RealtimeProtection	Voliteľné
WMIProvider	Povinné
HIPS	Povinné
Updater	Povinné
eShell	Povinné
UpdateMirror	Povinné
DeviceControl	Voliteľné
DocumentProtection	Voliteľné
WebAndEmail	Voliteľné
ProtocolFiltering	Neviditeľné
NetworkProtection	Voliteľné
IdsAndBotnetProtection	Voliteľné
Rmm	Voliteľné
WebAccessProtection	Voliteľné
EmailClientProtection	Voliteľné
MailPlugins	Neviditeľné
Klaster	Voliteľné
_Base	Povinné
eula	Povinné
ShellExt	Voliteľné
_FeaturesCore	Povinné
GraphicUserInterface	Voliteľné
SysInspector	Voliteľné
SysRescue	Voliteľné
EnterpriseInspector	Voliteľné

Ak chcete odstrániť niektorú z nasledujúcich funkcií, musíte odstrániť celú skupinu zadaním každej funkcie, ktorá patrí do danej skupiny. V opačnom prípade sa funkcia neodstráni. Nižšie sú dve skupiny (každý riadok predstavuje jednu skupinu):

```
GraphicUserInterface,ShellExt

NetworkProtection,WebAccessProtection,IdsAndBotnetProtection^
```

```
ProtocolFiltering,MailPlugins,EmailClientProtection
```

Príklad:
Vylúčenie sekcie **NetworkProtection** vrátane podradených funkcií z inštalácie zadaním len nadradenej funkcie a použitím parametra `REMOVE`:

```
msiexec /i eshp_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection
```

Môžete prípadne použiť parameter `ADDEXCLUDE`, musíte však zadať aj všetky podradené funkcie:

```
msiexec /i eshp_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection^
IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

Príklad:
Príklady príkazov pri **Základnej inštalácii**:

```
msiexec /qn /i eshp_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm
```

Ak chcete, aby bol program ESET Security for Microsoft SharePoint po nainštalovaní automaticky nakonfigurovaný, môžete v rámci inštalácie cez príkazový riadok použiť základné konfiguračné parametre.

Príklad:
Inštalácia ESET Security for Microsoft SharePoint s vypnutou technológiou ESET LiveGrid®:

```
msiexec /qn /i eshp_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0
```

Zoznam konfiguračných parametrov:

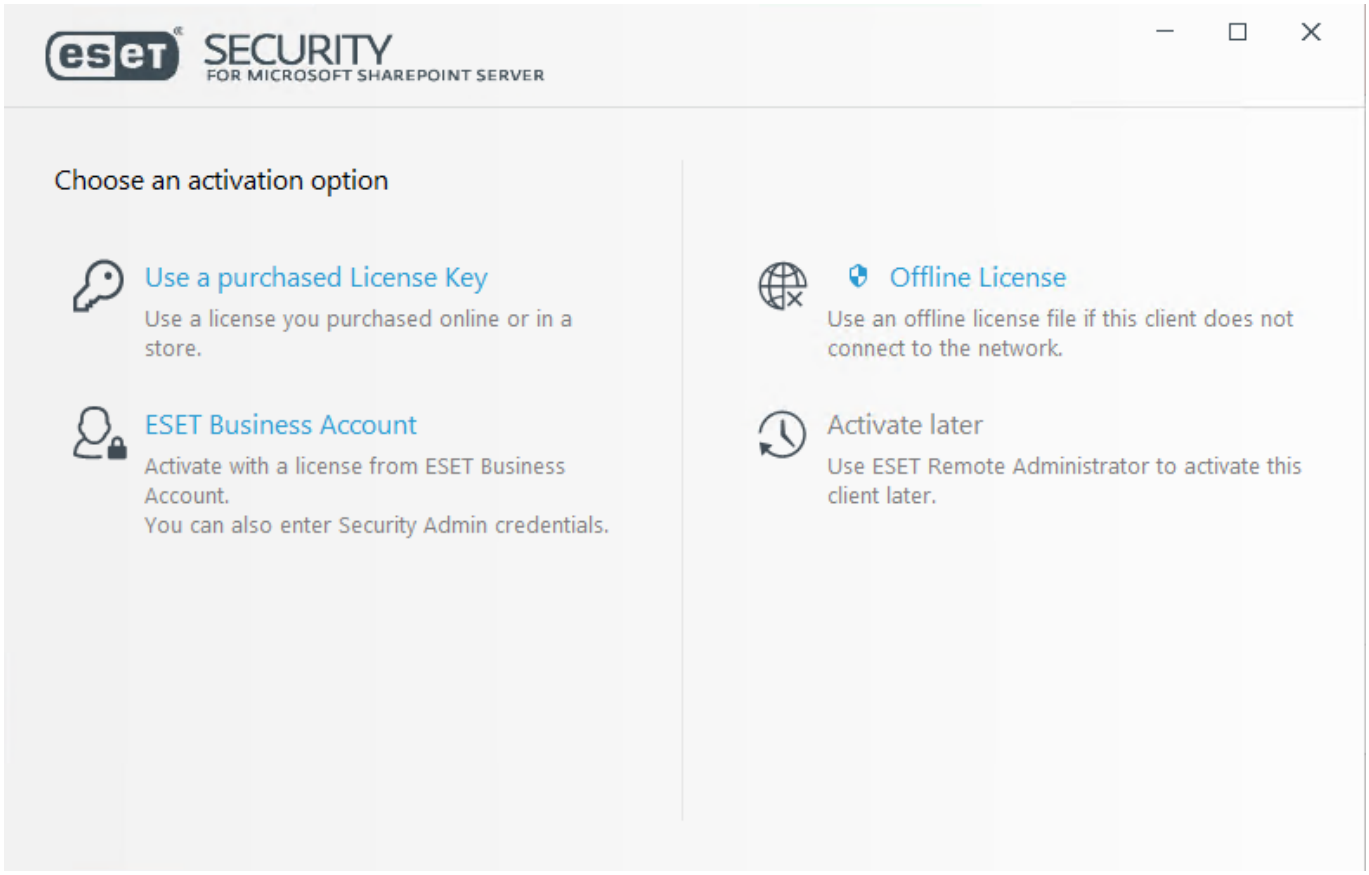
Prepínač	Hodnota
`CFG_POTENTIALLYUNWANTED_ENABLED=1/0`	0 – vypnuté, 1 – zapnuté
`CFG_LIVEGRID_ENABLED=1/0`	0 – vypnuté, 1 – zapnuté
`FIRSTSCAN_ENABLE=1/0`	0 – vypnuté, 1 – zapnuté
`CFG_PROXY_ENABLED=0/1`	0 – vypnuté, 1 – zapnuté
`CFG_PROXY_ADDRESS=<ip>`	IP adresa proxy.
`CFG_PROXY_PORT=<port>`	Číslo portu proxy.
`CFG_PROXY_USERNAME=<user>`	Používateľské meno pre overenie.
`CFG_PROXY_PASSWORD=<pass>`	Heslo pre overenie.

Jazykové parametre: Jazyk produktu (musíte zadať oba parametre)

Prepínač	Hodnota
`PRODUCT_LANG=`	Kód LCID uvedený v desiatkovej sústave (identifikácia miestneho nastavenia – Locale ID), napríklad `1033` pre *English - United States*. Zoznam jazykových kódov nájdete tu.
`PRODUCT_LANG_CODE=`	Reťazec LCID (Language Culture Name) uvedený malými písmenami, napríklad `en-us` pre *English - United States*. Zoznam jazykových kódov nájdete tu.

Aktivácia produktu

Po ukončení inštalácie budete vyzvaný, aby ste si aktivovali svoj produkt.



ESET Security for Microsoft SharePoint môžete aktivovať nasledujúcimi spôsobmi:

Zadať licenčný kľúč

Ide o jedinečný reťazec znakov XXXX-XXXX-XXXX-XXXX-XXXX, ktorý je použitý na identifikáciu vlastníka licencie a aktiváciu licencie.

ESET Business Account

Túto možnosť použite v prípade, že ste zaregistrovaný a máte svoj ESET Business Account, do ktorého bola importovaná vaša ESET Security for Microsoft SharePoint licencia. Zadať môžete aj prihlasovacie údaje **bezpečnostného správcu**, ktoré používate v rámci portálu License Administrator.

Offline licenčný súbor

Automaticky vygenerovaný offline licenčný súbor s informáciami o vašej licencii. Offline licenčný súbor je generovaný pomocou licenčného portálu spoločnosti ESET a používa sa v sieťach, odkiaľ sa aplikácia nemôže pripojiť na licenčné servery.

Kliknite na možnosť **Aktivovať neskôr** pomocou nástroja ESET PROTECT, 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.

Kliknite na **Pomocník a podpora** > **Spravovať licenciu** v hlavnom okne programu a zadajte nový licenčný kľúč. Uvidíte verejné identifikačné číslo licencie, ktoré slúži na identifikáciu produktu a licencie. Vaše používateľské meno, pod ktorým je počítač registrovaný v licenčnom systéme, je zobrazené v sekcii O programe, ktorú spustíte cez kontextové menu kliknutím pravým tlačidlom myši na ikonu programu v paneli úloh.

Po úspešnej aktivácii ESET Security for Microsoft SharePoint sa otvorí hlavné okno programu s aktuálnym stavom

ochrany zobrazeným v okne Monitorovanie. Je možné, že bude potrebné nakonfigurovať počiatočné nastavenia, napríklad pre ESET LiveGrid®.

Hlavné okno programu zobrazí oznámenia aj o ostatných záležitostiach, ako sú napríklad aktualizácie systému (Windows Updates) alebo aktualizácie detekčného jadra. Keď sú všetky položky, ktoré vyžadujú pozornosť, vyriešené, stav monitorovania bude zobrazený zelenou farbou a zároveň bude zobrazený text **Ste chránený**.

Prípadne v hlavnom okne programu kliknite na **Pomocník a podpora** > **Aktivovať produkt** alebo **Monitorovanie** > **Produkt nie je aktivovaný**.

> Poznámka:
> ESET PROTECT dokáže automaticky aktivovať pracovné stanice (aktivácia prebieha na pozadí, bez oznámení) pomocou licencie sprístupnenej správcom.

ESET Business Account

ESET Business Account vám umožňuje spravovať viacero licencií. Ak ešte nemáte účet ESET Business Account, kliknite na **Vytvoriť účet**. Budete presmerovaný na portál ESET Business Account, kde sa môžete zaregistrovať.

> Poznámka:
> Viac informácií nájdete v používateľskej príručke k ESET Business Account (EBA).

Ak sa prihlasujete pod účtom bezpečnostného správcu a zabudli ste heslo, kliknite na možnosť **Nepamätám si svoje heslo** a budete presmerovaný na portál ESET License Administrator. Zadajte e-mailovú adresu a kliknite na **Odoslať**. Následne vám budú na e-mailovú adresu doručené inštrukcie týkajúce sa obnovenia vášho hesla.

Úspešná aktivácia

Aktivácia ESET Security for Microsoft SharePoint bola úspešná, produkt je aktivovaný. Odteraz bude váš produkt ESET Security for Microsoft SharePoint dostávať pravidelné aktualizácie na zachytávanie najnovších hrozieb a bude môcť udržiavať váš počítač v bezpečí. Kliknite na **Hotovo** pre dokončenie aktivácie produktu.

Chyba aktivácie

Aktivácia ESET Security for Microsoft SharePoint nebola úspešná. Uistite sa, že ste zadali správny **Licenčný kľúč** alebo vložili správnu **Offline licenciu**. Ak máte rozdielnu **Offline licenciu**, skúste ju zadať znova. Pre skontrolovanie zadaného licenčného kľúča kliknite na **Skontrolovať licenčný kľúč**, prípadne **zadajte inú licenciu**.

Licencia

Budete vyzvaný, aby ste vybrali licenciu pridruženú k vášmu účtu, ktorá bude použitá pre ESET Security for Microsoft SharePoint. Pokračujte v aktivácii kliknutím na **Pokračovať**.

Aktualizácia na novú verziu

Nové verzie ESET Security for Microsoft SharePoint sú vydávané na účely zdokonalenia produktu a opravy chýb, ktoré nie je možné opraviť v rámci automatickej aktualizácie programových súčastí.

Metódy aktualizácie:

- **Odinštalovanie/inštalácia** – odstránenie starej verzie pred nainštalovaním novej verzie. Stiahnite si najnovšiu verziu ESET Security for Microsoft SharePoint. Ak chcete zachovať aktuálnu konfiguráciu produktu, exportujte nastavenia zo svojej súčasnej verzie produktu ESET Security for Microsoft SharePoint. Odinštalujte ESET Security for Microsoft SharePoint a reštartujte server. Vykonajte novú inštaláciu pomocou inštalátora, ktorý ste stiahli. Importujte nastavenia pre načítanie vašej predošlej konfigurácie. Tento postup odporúčame použiť v prípade, že používate ESET Security for Microsoft SharePoint na jednom serveri.

- **In-place** – metóda aktualizácie, kde je nová verzia ESET Security for Microsoft SharePoint nainštalovaná cez existujúcu inštaláciu.

Dôležité:
Je nevyhnutné, aby na vašom serveri neboli žiadne **čakajúce aktualizácie operačného systému Windows** ani **nebol vyžadovaný reštart** systému kvôli aktualizáciám či z akýchkoľvek iných dôvodov. Ak sa pokúsite vykonať aktualizáciu produktu pomocou metódy in-place na systéme, kde sú čakajúce aktualizácie operačného systému Windows alebo sa vyžaduje reštart systému, môže sa stať, že existujúca verzia ESET Security for Microsoft SharePoint nebude odstránená správne. Môže taktiež dôjsť k problémom pri následnom pokuse o manuálne odinštalovanie starej verzie ESET Security for Microsoft SharePoint.

Poznámka:
Počas aktualizácie ESET Security for Microsoft SharePoint bude vyžadovaný reštart servera.

- Vzdialená – táto metóda ja vhodná vo väčších sieťových prostrediach spravovaných nástrojom ESET PROTECT. Ide v podstate o čistú aktualizáciu, ktorá je vykonávaná vzdialene. Táto metóda je užitočná v prípade, že používate ESET Security for Microsoft SharePoint na viacerých serveroch.

- Sprievodca konfiguráciou klastra ESET – môže byť použitý aj ako metóda aktualizácie. Túto metódu odporúčame použiť pri 2 alebo viacerých serveroch využívajúcich ESET Security for Microsoft SharePoint. Ide v podstate o aktualizáciu metódou in-place, ktorá je vykonávaná pomocou klastra ESET. Klaster ESET vrátane jeho funkcií však môžete využívať aj po vykonaní aktualizácie.

Dôležité:
Pri aktualizácii z verzie 4.x nie je z technických dôvodov možné premigrovať určité nastavenia, predovšetkým pravidlá. Je to z dôvodu zmien týkajúcich sa funkcie pravidiel, ktoré boli predstavené v neskorších verziách produktu. Odporúčame, aby ste si pred vykonaním aktualizácie z verzie 4.x poznačili svoje nastavenia pravidiel. Pravidlá môžete nastaviť po dokončení aktualizácie. Nové pravidlá vám poskytnú väčšiu flexibilitu a ešte väčší počet možností v porovnaní s pravidlami v predchádzajúcich verziách produktu ESET Security for Microsoft SharePoint.

Poznámka:
Po aktualizácii produktu ESET Security for Microsoft SharePoint odporúčame prejsť si všetky nastavenia a uistiť sa, že všetko je nastavené správne a podľa vašich požiadaviek.

Aktualizácia pomocou nástroja ESET PROTECT

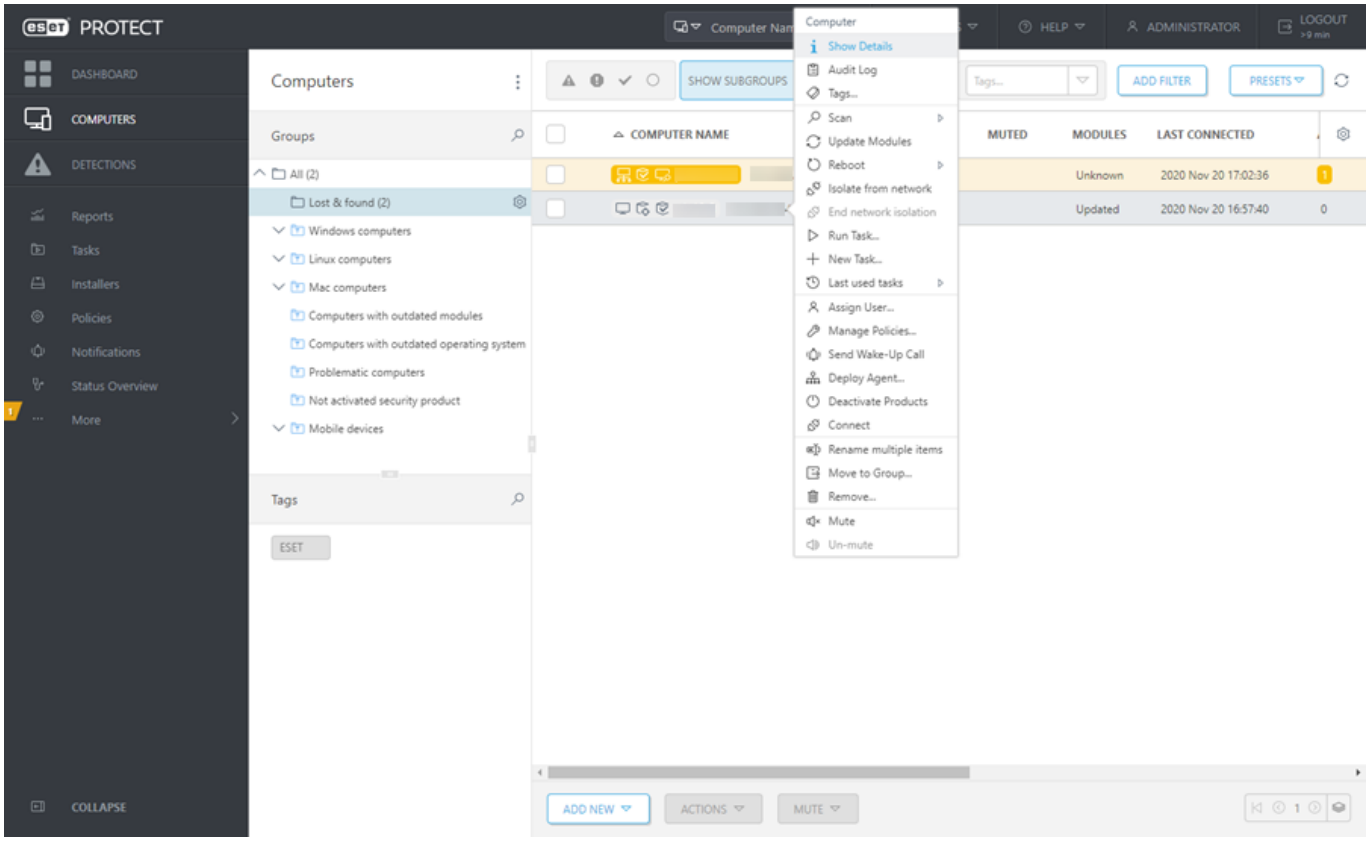
ESET PROTECT vám umožňuje aktualizovať viacero serverov, na ktorých je používaná staršia verzia produktu ESET Security for Microsoft SharePoint. Výhodou tejto metódy je aktualizácia veľkého množstva serverov súčasne, pričom každý produkt ESET Security for Microsoft SharePoint má identickú konfiguráciu (v prípade potreby).

Samotná procedúra pozostáva z nasledujúcich fáz:

- Najprv manuálne **aktualizujte prvý server** nainštalovaním najnovšej verzie produktu ESET Security for Microsoft SharePoint na svoju existujúcu inštaláciu, aby bola zachovaná celková konfigurácia vrátane pravidiel, whitelistov a blacklistov atď. Táto fáza sa vykonáva lokálne na serveri, na ktorom je spustený produkt ESET Security for Microsoft SharePoint.
- V nástroji ESET PROTECT si **vyžiadajte konfiguráciu** novej verzie ESET Security for Microsoft SharePoint a **konvertujte ju na politiku**. Politika bude neskôr aplikovaná na všetky aktualizované servery. Táto fáza, ako aj ďalšie fázy, sa vykonávajú vzdialene prostredníctvom nástroja ESET PROTECT.
- Spustite úlohu **Odinštalovanie softvéru** na všetkých serveroch so staršou verziou ESET Security for Microsoft SharePoint.
- Spustite úlohu **Inštalácia softvéru** na všetkých serveroch, na ktorých chcete pracovať s najnovšou verziou produktu ESET Security for Microsoft SharePoint.
- **Priraďte konfiguračnú politiku** k všetkých serverom s najnovšou verziou produktu ESET Security for Microsoft SharePoint.
- **Zadajte účet správcu farmy SharePoint** manuálne na každom serveri. Táto fáza sa vykonáva lokálne.

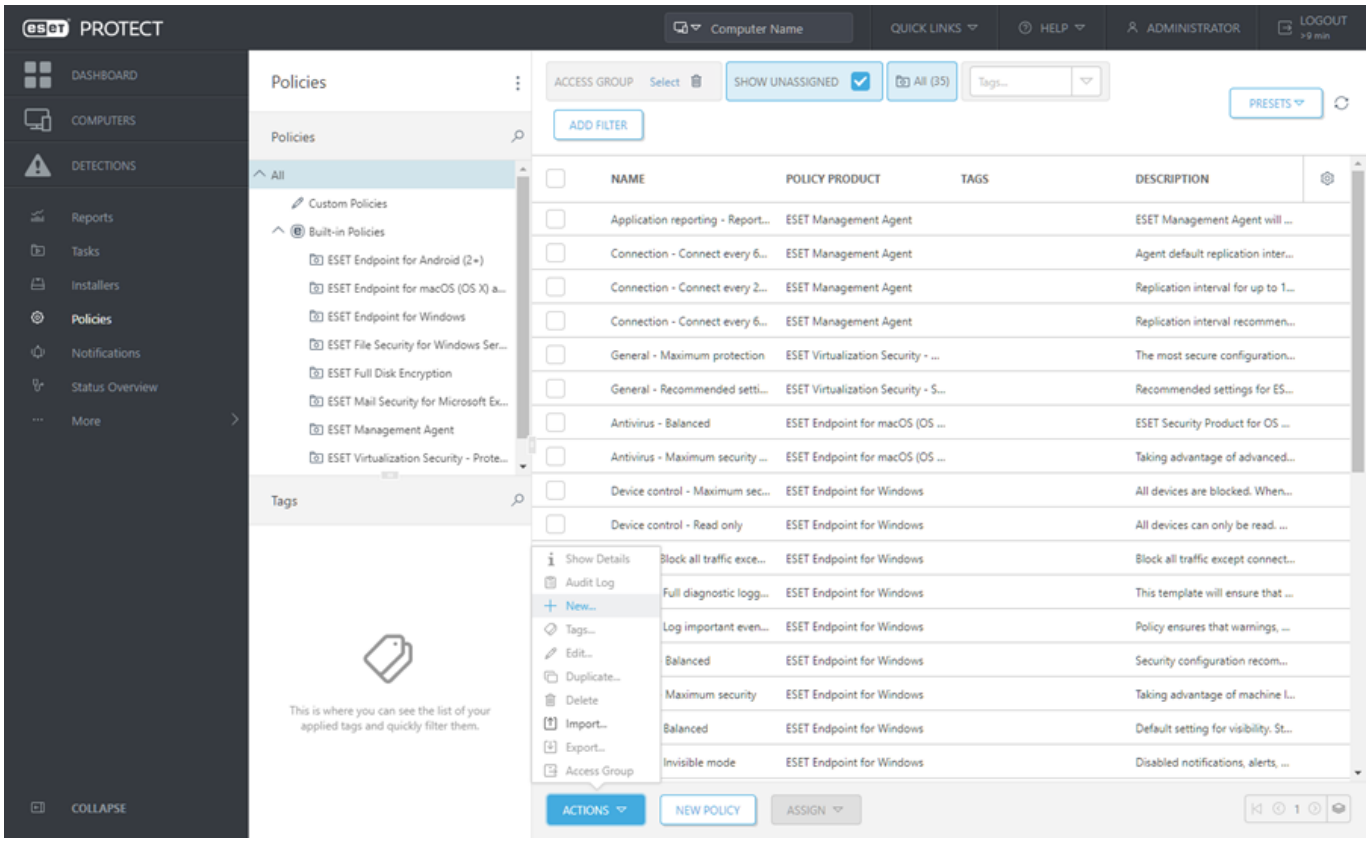
Postup krok za krokom:

1. Prihláste sa na jeden zo serverov, na ktorých sa nachádza ESET Security for Microsoft SharePoint, a aktualizujte ho stiahnutím a inštaláciou najnovšej verzie na vašu existujúcu verziu. Postupujte podľa krokov pre štandardnú inštaláciu. Počas inštalácie bude zachovaná celá pôvodná konfigurácia vašej staršej verzie produktu ESET Security for Microsoft SharePoint.
2. Otvorte **ESET Security Management Center Web Console**, vyberte klientsky počítač zo statickej alebo dynamickej skupiny a kliknite na možnosť **Zobraziť podrobnosti**.



3.Prejdite na kartu Konfigurácia a kliknite na tlačidlo **Požiadať o konfiguráciu**. Bude získaná celková konfigurácia príslušného spravovaného produktu. Získanie konfigurácie môže chvíľu trvať. Keď sa najnovšia konfigurácia objaví v zozname, kliknite na **Bezpečnostný produkt** a vyberte možnosť **Otvoriť konfiguráciu**.

4.Následne vytvorte konfiguračnú politiku kliknutím na tlačidlo Konvertovať na politiku. Zadajte **Názov** novej politiky a kliknite na **Dokončiť**.



5.Prejdite do sekcie **Úlohy pre klienta** a vyberte úlohu Odinštalovanie softvéru. Po odinštalovaní softvéru odporúčame reštartovať server. Reštart servera je možné vykonať automaticky pomocou označenia možnosti **V prípade potreby automaticky reštartovať**. Po vytvorení úlohy pridajte všetky požadované cieľové počítače, na ktorých bude vykonané odinštalovanie softvéru.

6.Uistite sa, že produkt ESET Security for Microsoft SharePoint bol odinštalovaný zo všetkých cieľových počítačov.

7.Vytvorte úlohu Inštalácia softvéru pre inštaláciu najnovšej verzie ESET Security for Microsoft SharePoint na všetky požadované ciele.

8.**Priraďte konfiguračnú politiku** k všetkých serverom (ideálne ku skupine) s najnovšou verziou produktu ESET Security for Microsoft SharePoint.

9.Prihláste sa na každý server lokálne a otvorte ESET Security for Microsoft SharePoint. Zobrazí sa červená varovná správa o stave s textom: *ESET SharePoint Helper Service is not running*. V rozšírených nastaveniach zadajte **účet správcu farmy SharePoint**.

> Dôležité:
> Tento krok je potrebné vykonať pre každý server, na ktorom je spustený produkt ESET Security for Microsoft SharePoint. Je to z bezpečnostných dôvodov. Produkty spoločnosti ESET si do databázy neukladajú prihlasovacie údaje správcu SharePointu, čo znamená, že prihlasovacie údaje nie sú súčasťou konfiguračnej politiky a teda nie sú synchronizované naprieč ostatnými servermi.

Aktualizácia prostredníctvom klastra ESET

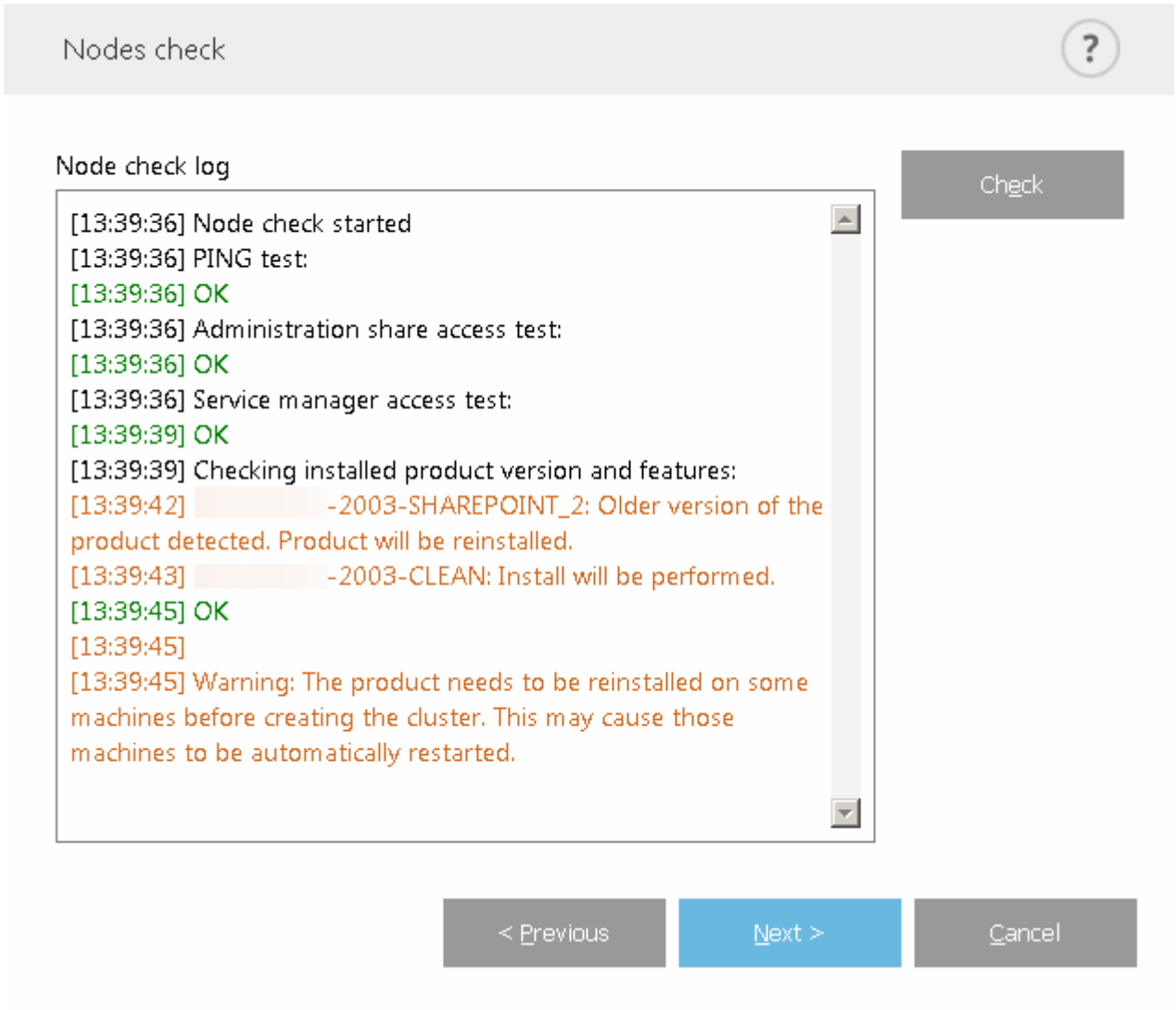
Vytvorenie klastra ESET vám umožňuje aktualizovať viacero serverov, ktoré používajú staršiu verziu produktu ESET Security for Microsoft SharePoint. Je to alternatíva k aktualizácii pomocou nástroja ESET PROTECT. Metódu aktualizácie pomocou klastra ESET odporúčame použiť v prípade, ak máte vo vašom prostredí 2 alebo viac serverov s nainštalovaným produktom ESET Security for Microsoft SharePoint. Ďalšou z výhod tejto metódy aktualizácie je, že môžete pokračovať v používaní klastra ESET, aby mal produkt ESET Security for Microsoft SharePoint synchronizovanú konfiguráciu na všetkých uzloch.

Postupujte podľa krokov uvedených nižšie pre vykonanie aktualizácie pomocou tejto metódy:

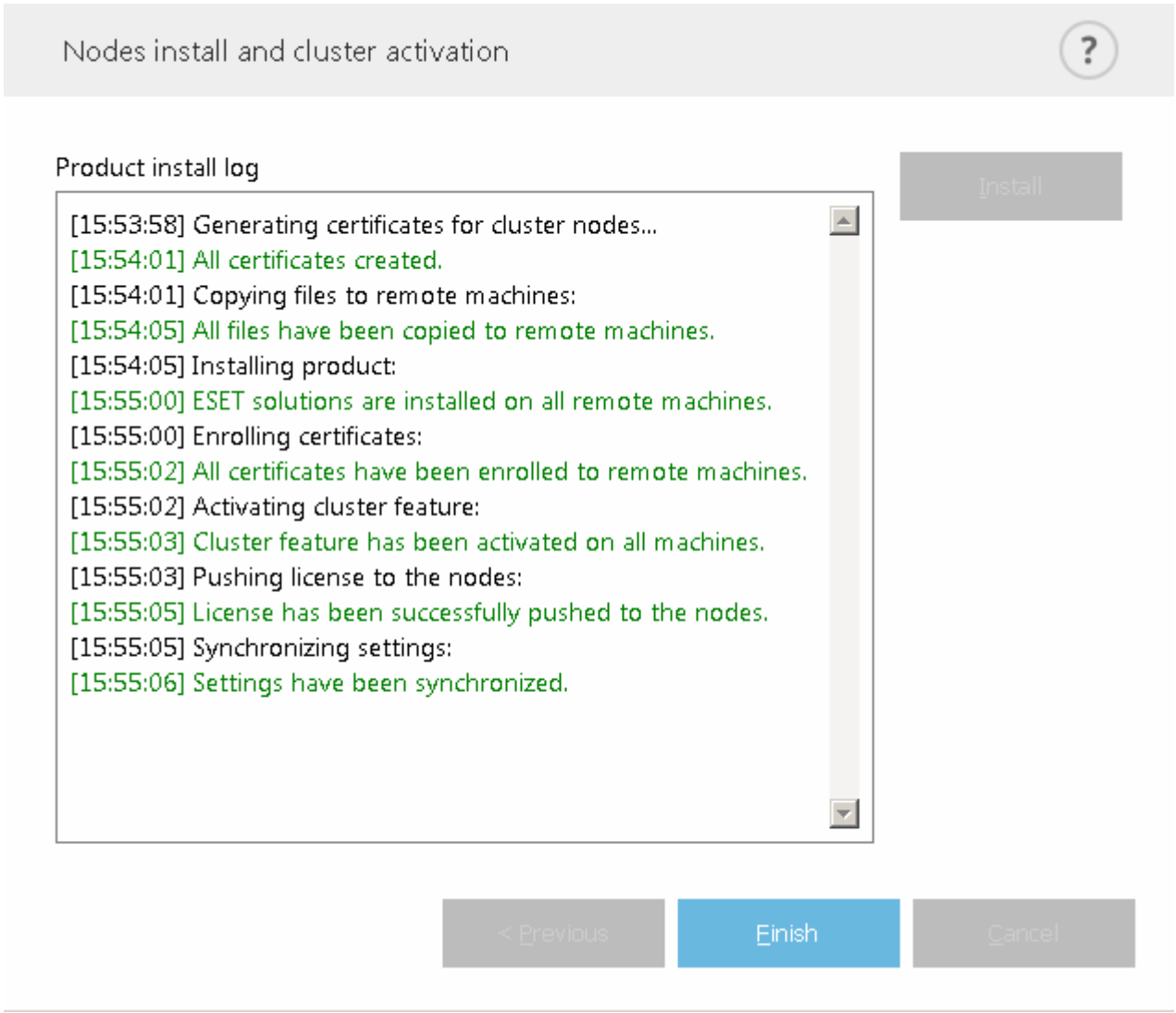
1.Prihláste sa na jeden zo serverov, na ktorých sa nachádza ESET Security for Microsoft SharePoint, a aktualizujte ho stiahnutím a inštaláciou najnovšej verzie na vašu existujúcu verziu. Postupujte podľa krokov pre štandardnú inštaláciu. Počas inštalácie bude zachovaná celá pôvodná konfigurácia vašej staršej verzie produktu ESET Security for Microsoft SharePoint.

2.Spustite Sprievodcu klastrom ESET a pridajte uzly klastra (servery, na ktorých chcete aktualizovať produkt ESET Security for Microsoft SharePoint). V prípade potreby môžete pridať ďalšie servery, na ktorých sa zatiaľ nenachádza produkt ESET Security for Microsoft SharePoint (bude vykonaná inštalácia). Pri výbere názvu klastra a typu inštalácie odporúčame ponechať predvolené nastavenia (uistite sa, že je zvolená možnosť **Doručiť licenciu k uzlom bez aktivovaného produktu**).

3.Skontrolujte **Záznam kontroly uzlov**. V danom zázname budú zobrazené severy so staršími verziami produktu a na ktorých bude produkt preinštalovaný. ESET Security for Microsoft SharePoint bude taktiež nainštalovaný na všetky pridané servery, kde nainštalovaný nie je.



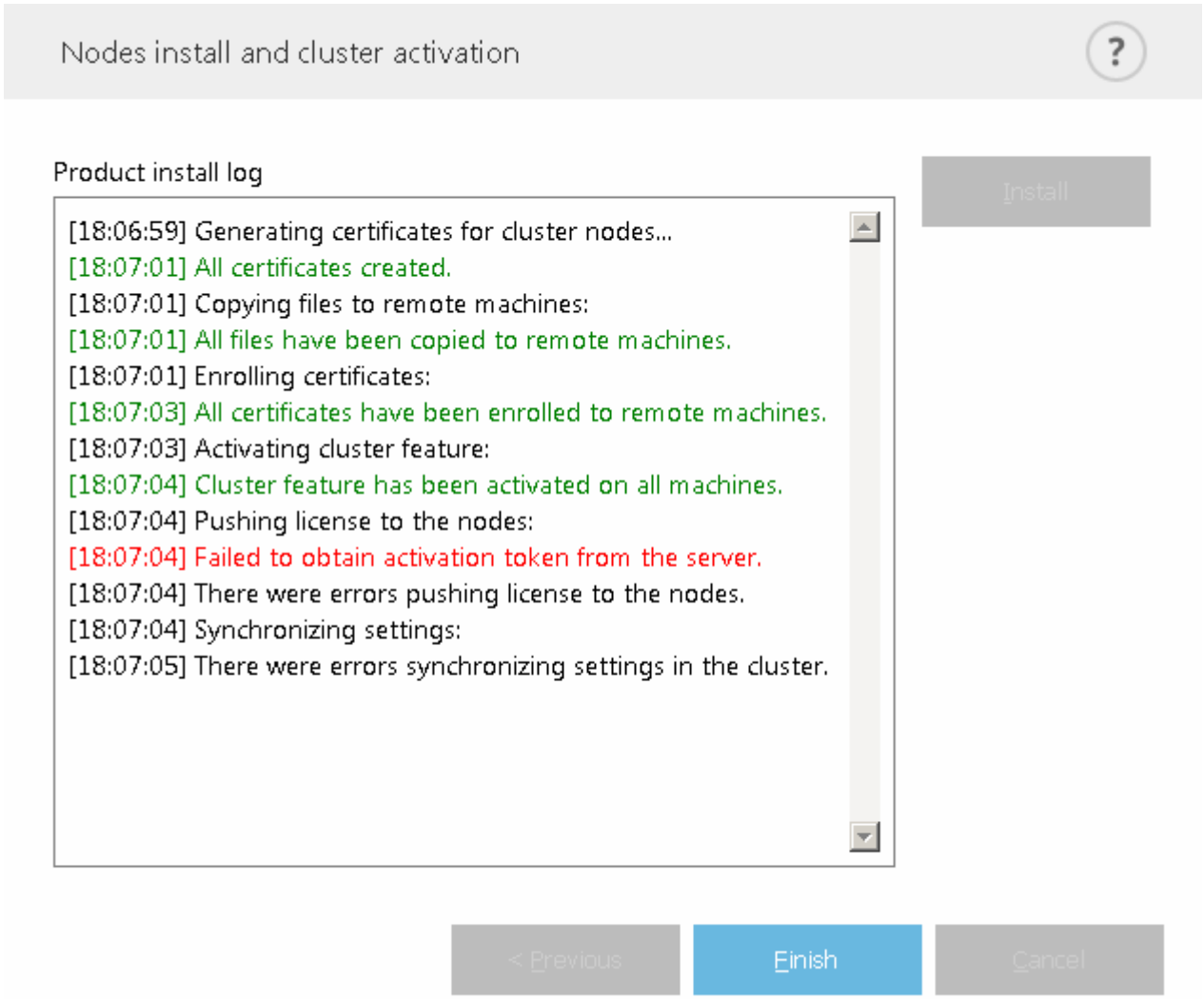
4.Priebeh inštalácie bude zobrazený v okne **Inštalácia uzlov a aktivácia klastra**. Po úspešnom dokončení inštalácie by výsledky mali byť podobné výsledkom uvedeným nižšie:



5.Prihláste sa na každý server lokálne a otvorte ESET Security for Microsoft SharePoint. Zobrazí sa nasledujúce hlásenie: *Služba ESET SharePoint Helper nie je spustená*. V rozšírených nastaveniach zadajte svoj **účet správcu farmy SharePoint**.

Dôležité:
Tento krok je potrebné vykonať pre každý server, na ktorom je spustený produkt ESET Security for Microsoft SharePoint. Je to z bezpečnostných dôvodov. Produkty spoločnosti ESET si do databázy neukladajú prihlasovacie údaje správcu SharePointu, čo znamená, že tieto údaje nie sú synchronizované naprieč ostatnými servermi.

Ak vaša sieť alebo DNS nie sú správne nakonfigurované, môže sa zobraziť chybové hlásenie **Nepodarilo sa získať aktivačný token zo servera**. Pokúste sa spustiť Sprievodcu klastrom ESET znova. Existujúci klaster bude zničený a bude vytvorený nový (bez potreby preinštalovania produktu), pričom aktivácia by mala byť tentokrát úspešne dokončená. Ak daný problém pretrváva aj naďalej, skontrolujte vaše nastavenia siete ad DNS.



Terminálový server

Ak inštalujete produkt ESET Security for Microsoft SharePoint na Windows Server, ktorý je nastavený ako terminálový server, môžete vypnúť grafické rozhranie ESET Security for Microsoft SharePoint a zamedziť tak jeho zapínaniu vždy, keď sa používateľ prihlási do systému. Bližšie inštrukcie nájdete v kapitole Vypnutie grafického rozhrania (GUI) na terminálovom serveri.

Ako začať

Nasledujúca časť by vám mala pomôcť začať s používaním programu ESET Security for Microsoft SharePoint.

Monitorovanie

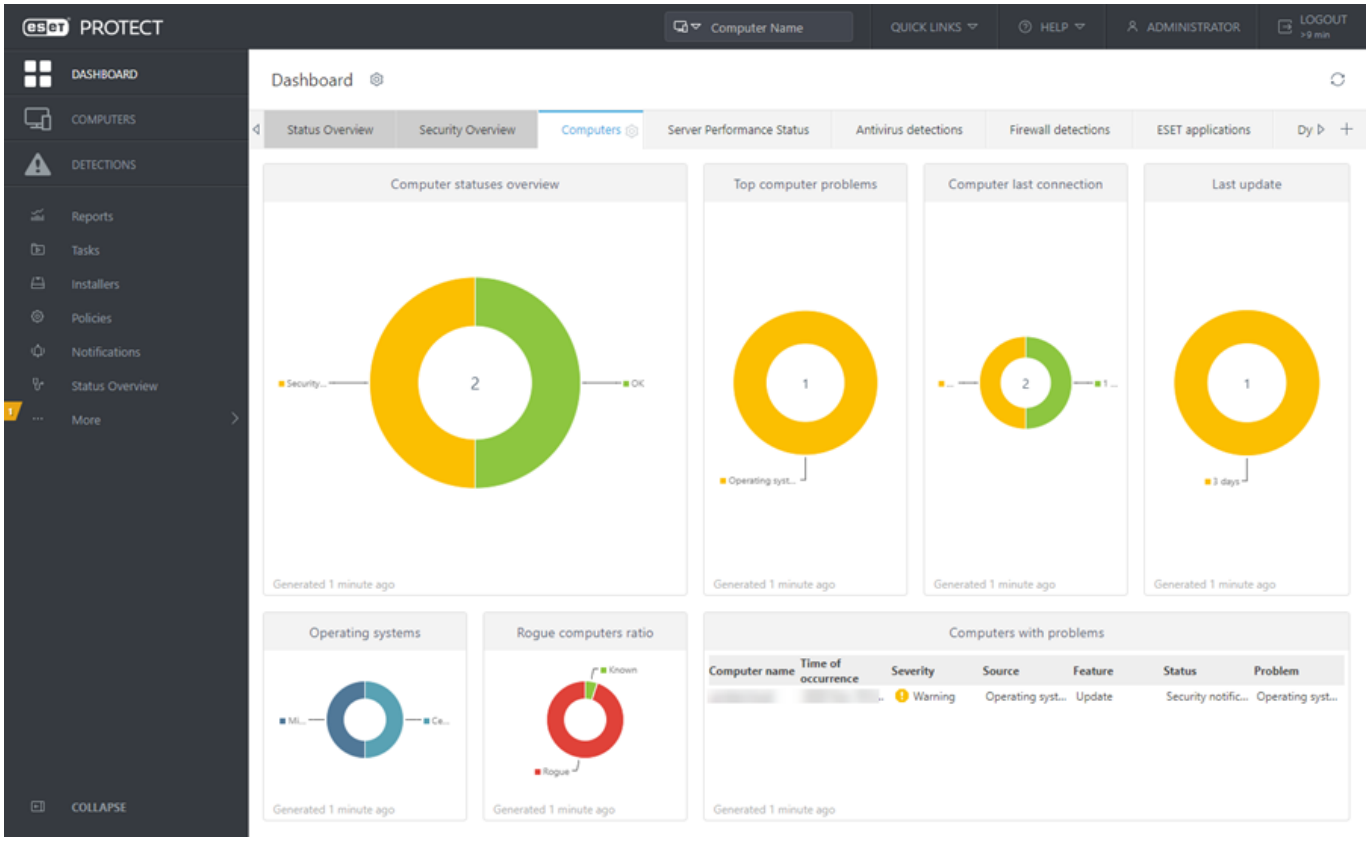
V tejto sekcii nájdete okamžitý prehľad aktuálneho stavu programu ESET Security for Microsoft SharePoint. Už na prvý pohľad môžete vidieť, či sa vyskytli problémy s programom, ktoré si vyžadujú vašu pozornosť.

Spravovanie pomocou nástroja ESET PROTECT

Na vzdialenú správu programu ESET Security for Microsoft SharePoint môžete použiť nástroj ESET PROTECT.

Spravovanie pomocou nástroja ESET PROTECT

ESET PROTECT je nástroj, ktorý vám umožňuje spravovať produkty spoločnosti ESET v sieťovom prostredí z jednej centrálnej lokality. Pomocou spravovania úloh vám umožňuje inštalovať bezpečnostné riešenia spoločnosti ESET na vzdialené počítače v sieti a okamžite reagovať na problémy a hrozby, ktoré sa môžu na zariadeniach vyskytnúť. ESET PROTECT neposkytuje ochranu proti škodlivému kódu, spolieha sa na bezpečnostné riešenia spoločnosti ESET nainštalované na pripojených klientskych počítačoch. Bezpečnostné riešenia spoločnosti ESET podporujú siete, ktoré zahŕňajú rôzne typy platforiem. Vaša sieť môže obsahovať kombináciu aktuálnych operačných systémov Microsoft, Linux a Mac OS.



Viac informácií o ESET PROTECT sa nachádza v Online pomocníkovi pre nástroj ESET PROTECT.

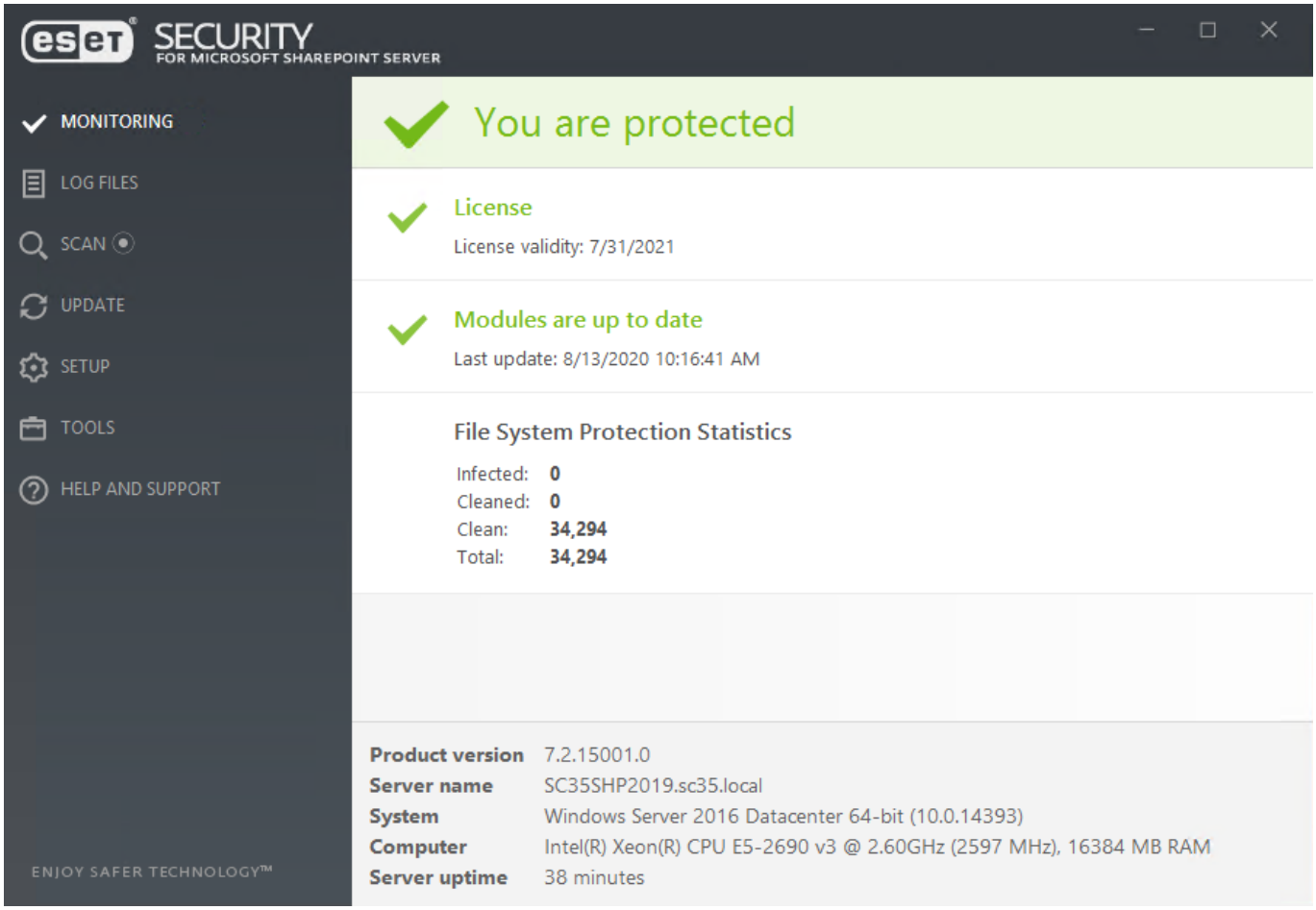
Monitorovanie

Stav ochrany zobrazený v časti **Monitorovanie** zobrazuje informácie o aktuálnej úrovni ochrany vášho systému. Súhrnné informácie o stave prevádzky programu ESET Security for Microsoft SharePoint budú zobrazené v hlavnom okne.

Zelená ikona a zelený nápis **Ste chránený** znamená, že je zaistená maximálna úroveň ochrany.

Červený výkričník oznamuje kritické problémy – ochrana vášho systému nie je zaručená v plnej miere. Zoznam všetkých stavov ochrany nájdete v kapitole Stavy.

Oranžová ikona oznamuje, že produkt si vyžaduje pozornosť, pretože sa vyskytol problém, ktorý však nie je kritický.



Moduly, ktoré pracujú správne, majú pridelené zelené symboly. Moduly, ktoré nie sú plne funkčné sa zobrazujú buď s červeným výkričníkom, alebo s oranžovou notifikáciou. 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.

Sekcia Monitorovanie tiež obsahuje informácie o vašom systéme:

- **Verzia produktu** – číslo verzie produktu ESET Security for Microsoft SharePoint.
- **Názov servera** – hostiteľský názov počítača alebo FQDN.
- **Systém** – podrobnosti o operačnom systéme.
- **Počítač** – podrobnosti o používanom hardvéri.
- **Doba prevádzky** – zobrazuje, ako dlho je systém spustený.

Počet používateľov

ESET Security for Microsoft SharePoint zobrazuje počet používateľov, ktorí používajú SharePoint. Tento výpočet bude použitý na účely licencovania. Existujú dva typy používateľov:

- **Používatelia domény** – počet používateľov nachádzajúcich sa v databáze SharePointu, ktorí na prihlásenie do systému používajú overovanie pomocou systému Windows. Ich prítomnosť je taktiež overovaná priamo v Active Directory. Ak sa zhoduje, používatelia sú započítaní. Takéto overenie slúži na zabránenie započítania používateľov, ktorí sa už nenachádzajú v Active Directory, ale ešte sú v zozname služby SharePoint. Takíto používatelia sa nezapočítavajú.
- **Iné** – počet používateľov, ktorí používajú iné formy overovania (bez ohľadu na to, či sú v Active Directory), napríklad overovanie na základe formulárov alebo overovanie založené na deklarácii identity. Počet je taktiež vyhodnotený na základe zoznamu používateľov v databáze SharePointu.

Poznámka:
Počet používateľov je prepočítaný 5 minút po reštarte systému alebo každých 6 hodín. Ak chcete zobraziť počet používateľov, musíte zadať správne prihlasovacie údaje pre účet správcu SharePointu.

V prípade, že problém nie je možné 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 otázky rýchlo a efektívne vám pomôžu s vyriešením vášho problému.

Stav ochrany

Súhrnné informácie o stave programu ESET Security for Microsoft SharePoint budú zobrazené v hlavnom okne spolu s podrobnými informáciami o vašom systéme. Za normálnych okolností, keď všetko funguje správne, má stav ochrany zelenú farbu. Stav ochrany sa však za určitých podmienok môže zmeniť. Ak dôjde k niektorej z udalostí spomenutých v tabuľke nižšie, stav ochrany zmení farbu na oranžovú alebo červenú a zobrazí sa príslušné upozornenie.

Poznámka:
V tabuľke sa nachádza zoznam správ doplnku SharePoint. V stavovom okne sa však môžu zobraziť aj iné správy súvisiace s ochranou súborových serverov (nie sú uvedené v tabuľke).

Upozornenie	Popis
SharePoint nie je nainštalovaný	Microsoft SharePoint Server nebol nájdený alebo je nainštalovaná jeho nepodporovaná verzia. Nainštalujte si, prosím, jednu z podporovaných verzií.
SharePoint Server nie je podporovaný	Nainštalovaná verzia nie je podporovaná programom ESET Security for Microsoft SharePoint, nainštalujte si jednu z podporovaných verzií.
Filtrovanie pri prístupe k SharePointu je dočasne vypnuté	Microsoft SharePoint Server nie je chránený pred hrozbami a nebudú sa uplatňovať žiadne pravidlá.
Filtrovanie pri prístupe k SharePointu sa nepoužíva	Filtrovanie pri prístupe k Microsoft SharePoint Serveru nekontroluje sťahované ani nahrávané dokumenty.
Filtrovanie pri prístupe k SharePointu je vypnuté	Microsoft SharePoint Server nie je chránený pred hrozbami a nebudú sa uplatňovať žiadne pravidlá.
Nie je možný prístup ku konfigurácii SharePointu	Účet správcu SharePointu nemá prístup k objektom konfigurácie. Skontrolujte, či je správne nastavený účet správcu SharePointu.
Nie je možné získať prístup k objektom webovej stránky SharePoint	Účet správcu SharePointu nemá prístup k objektom webovej stránky SharePoint. Nebude možné vykonať manuálnu kontrolu databáz. Skontrolujte, či je správne nastavený účet správcu SharePointu.
Nie je možné získať prístup k niektorým objektom webovej stránky SharePoint	Účet správcu SharePointu nemá prístup k niektorým objektom webovej stránky SharePoint. Nebude možné vykonať manuálnu kontrolu databáz týchto webových stránok.
Čaká sa na Microsoft SharePoint	ESET Security for Microsoft SharePoint čaká na dostupnosť služieb Microsoft SharePoint. Niektoré chyby týkajúce sa SharePointu sa nemusia zobraziť.
Požadované služby SharePoint nie sú spustené	Služba SharePoint Administration alebo SharePoint Timer nie je spustená. Tieto služby sú potrebné pre fungovanie aktualizačných upozornení.
Neplatný účet správcu SharePointu	Zadaný názov účtu správcu SharePointu neexistuje. Je potrebné zmeniť účet správcu.
Účet správcu SharePointu nie je nakonfigurovaný	Je potrebné zapnúť filtrovanie pri prístupe.

Upozornenie	Popis
Služba SharePoint Helper nie je spustená	Služba ESET SharePoint Helper prestala fungovať alebo ju nie je možné spustiť. Spustenie služby ESET SharePoint Helper vyžaduje účet správcu SharePointu. Skontrolujte, či sú zadané prihlasovacie údaje platné a či má účet oprávnenia „Prihlásiť sa ako služba“.
Operačný systém nie je aktualizovaný	Okno aktualizácií operačného systému zobrazuje zoznam dostupných aktualizácií pripravených na inštaláciu.
Vaše zariadenie čoskoro stratí ochranu	Kliknutím na Zobraziť možnosti riešenia zobrazíte podrobné informácie o tom, ako aktualizovať váš systém Microsoft Windows. Ak používate **Microsoft Windows Server 2008 R2 SP1**, uistite sa, že váš systém je kompatibilný s SHA-2. Nainštalujte potrebné aktualizácie podľa verzie svojho operačného systému.
Vyžaduje sa reštart počítača	Kliknite na **Reštartovať počítač** pre okamžitý reštart, prípadne kliknite na **Zatvoriť**, ak chcete reštartovať počítač neskôr.
Detekcia potenciálne nechcených aplikácií nie je nakonfigurovaná	Potenciálne nechcená aplikácia (PUA) je program, ktorý obsahuje adware, inštaluje panely s nástrojmi (toolbar), prípadne má iný nejasný účel. Vyskytujú sa situácie, keď sa používateľ rozhodne, že výhody, ktoré mu potenciálne nechcená aplikácia poskytuje, prevyšujú riziko spojené s jej používaním.
Rezidentná ochrana súborového systému je pozastavená	Kliknite na možnosť Zapnúť rezidentnú ochranu v sekcii **Monitorovanie** alebo opätovne povoľte **Rezidentnú ochranu súborového systému** na karte Nastavenia v hlavnom okne programu.
Produkt nie je aktivovaný alebo Platnosť licencie uplynula	V takomto prípade ikona stavu ochrany zmení farbu na červenú. Po uplynutí platnosti licencie nebude možné program aktualizovať. Pre obnovenie licencie postupujte podľa inštrukcií uvedených vo výstražnom okne.
Prepísanie politiky je aktívne	Konfigurácia stanovená politikou je dočasne prepísaná, pravdepodobne dovtedy, kým nebudú vyriešené prípadné problémy. Ak spravujete ESET Security for Microsoft SharePoint pomocou nástroja ESET PROTECT a máte k nemu priradenú politiku, odkaz na stav bude uzamknutý (v sivom poli) v závislosti od toho, ktoré funkcie patria danej politike.
Ochrana pred sieťovými útokmi (IDS) je pozastavená	Kliknite na Zapnúť ochranu pred sieťovými útokmi (IDS) pre opätovné zapnutie tejto funkcie.
Ochrana pred botnetmi je pozastavená	Kliknite na Zapnúť ochranu pred botnetmi pre opätovné zapnutie tejto funkcie.
Ochrana prístupu na web je pozastavená	Kliknite na možnosť Zapnúť ochranu prístupu na web v sekcii **Monitorovanie** alebo opätovne povoľte **Ochranu prístupu na web** na karte Nastavenia v hlavnom okne programu.
Prepísanie politiky je aktívne	Konfigurácia stanovená politikou je dočasne prepísaná, pravdepodobne dovtedy, kým nebudú vyriešené prípadné problémy. Ak spravujete ESET Security for Microsoft SharePoint pomocou nástroja ESET PROTECT a máte k nemu priradenú politiku, odkaz na stav bude uzamknutý (v sivom poli) v závislosti od toho, ktoré funkcie patria danej politike.

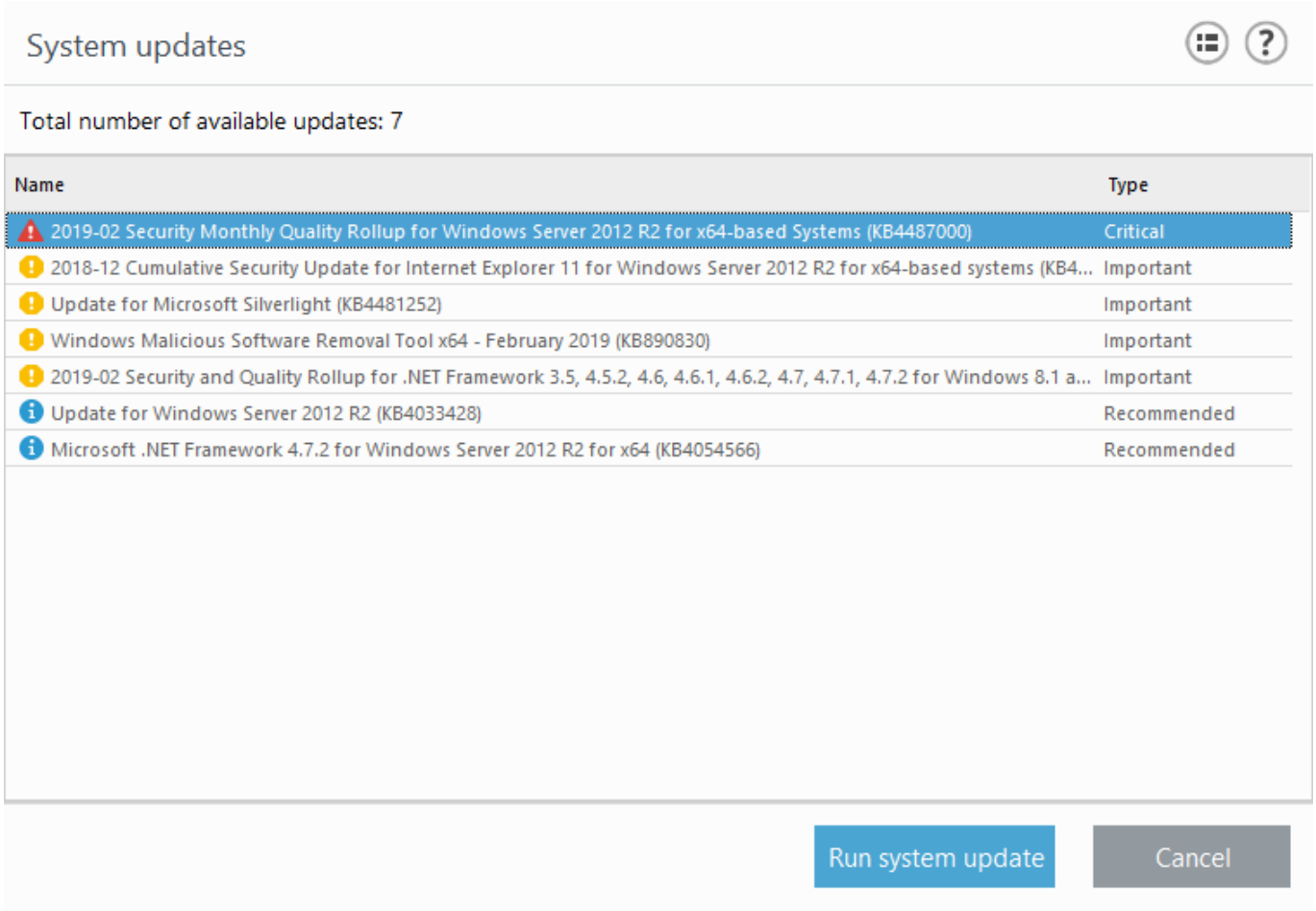
Poznámka:
Posledné dve správy sú na 5 minút po spustení servera pozdržané. Počas tohto času prebieha spúšťanie služby ESET SharePoint helper a čaká sa na dostupnosť SharePointu. Tento proces zvyčajne trvá len pár sekúnd, no pri vysokom zaťažení systému môže dosiahnuť trvanie 5 minút. Skončenie tohto procesu je v protokole udalostí zapísané formou nasledujúceho záznamu: Initial wait for SharePoint services has finished (čakanie na dostupnosť služieb SharePoint sa skončilo).

V prípade, že problém neviete vyriešiť, vyhľadajte 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 otázky rýchlo a efektívne vám pomôžu s vyriešením

vášho problému.

K dispozícii sú aktualizácie Windows

Okno aktualizácií operačného systému zobrazuje zoznam dostupných aktualizácií pripravených na inštaláciu. Vedľa názvu aktualizácie je zobrazená jej priorita. Pravým kliknutím na riadok v zozname a výberom možnosti **Viac informácií** z kontextového menu sa zobrazí okno s doplnkovými informáciami o aktualizácii:



Kliknite na **Spustiť aktualizáciu systému** pre otvorenie okna **aktualizácie systému Windows**.

Izolácia siete

ESET Security for Microsoft SharePoint poskytuje možnosť blokovať sieťové pripojenie vášho servera. Táto funkcia sa nazýva izolácia siete. V niektorých kritických situáciách môže byť potrebné izolovať server od siete ako preventívne opatrenie. Napríklad, ak ste zistili, že váš server bol napadnutý malvérom alebo bol počítač ohrozený iným spôsobom.

Aktivovaním izolácie siete sa zablokujú všetky sieťové prenosy okrem nasledujúcich výnimiek:

- Pripojenie k doménovému radiču.
- ESET Security for Microsoft SharePoint stále dokáže komunikovať.
- ESET Management Agent a ESET Enterprise Inspector Agent môžu aj naďalej komunikovať cez sieť.

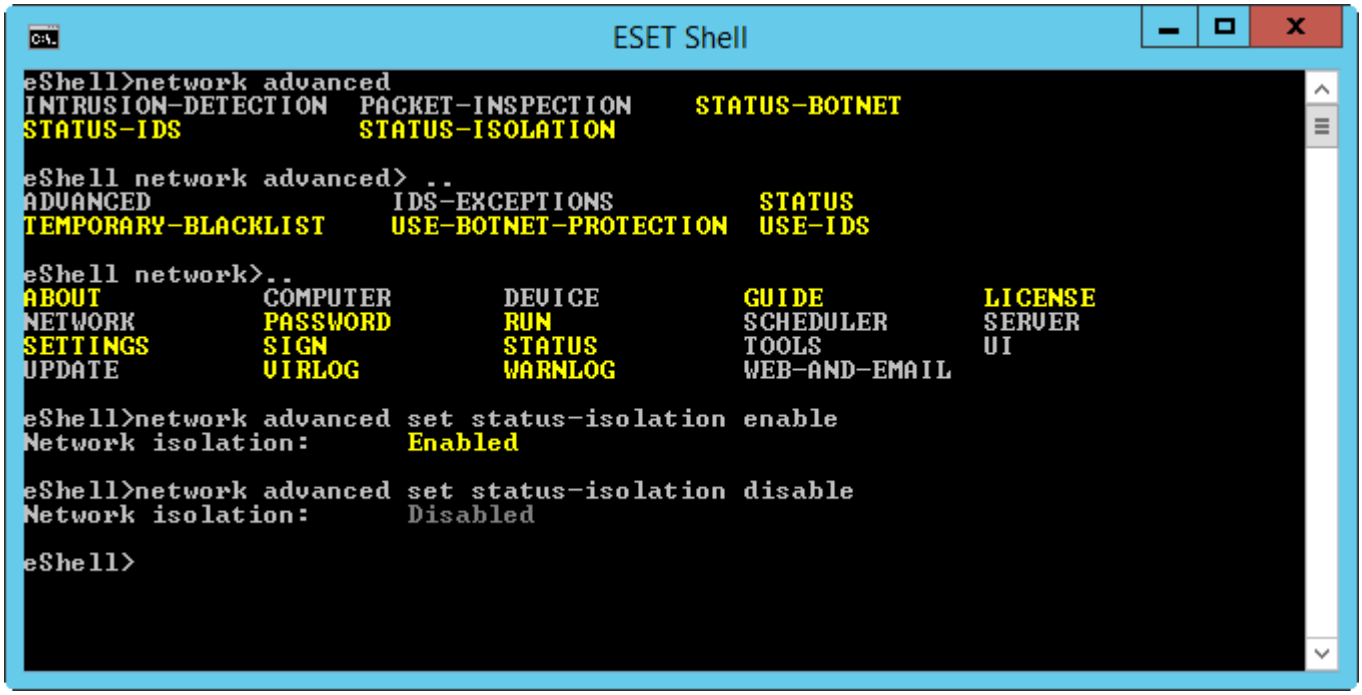
Aktivovať a deaktivovať izoláciu siete môžete pomocou eShell príkazu alebo prostredníctvom klientskej úlohy v

ESET PROTECT.

eShell

V interaktívnom režime:

- Aktivácia izolácie siete: `network advanced set status-isolation enable`
- Deaktivácia izolácie siete: `network advanced set status-isolation disable`



Môžete tiež vytvoriť a spustiť batch súbor použitím režimu Batch/skript.

ESET PROTECT

- Aktivácia izolácie siete prostredníctvom klientskej úlohy.
- Deaktivácia izolácie siete prostredníctvom klientskej úlohy.

Ak je aktivovaná izolácia siete, stav programu ESET Security for Microsoft SharePoint sa zmení na červenú a zobrazí sa oznámenie **Prístup na sieť bol zablokovaný**.

Používanie programu ESET Security for Microsoft SharePoint

Táto časť obsahuje podrobný popis používateľského rozhrania programu a vysvetľuje, ako používať ESET Security for Microsoft SharePoint.

Používateľské rozhranie umožňuje rýchly prístup k najčastejšie používaným funkciám produktu:

- Monitorovanie
- Protokoly
- Kontrola

- Aktualizácia
- Nastavenia
- Nástroje

Kontrola

Manuálna kontrola je dôležitou súčasťou ESET Security for Microsoft SharePoint. Umožňuje kontrolu diskov, jednotlivých priečinkov a súborov na počítači. Pre zaistenie zabezpečenia vašej siete je kľúčové, 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. Toto sa môže stať v prípade výskytu hrozby v čase, keď je rezidentná ochrana deaktivovaná, detekčné jadro nie je aktualizované alebo súbor nebol detegovaný, keď bol prvýkrát uložený na disk.

Vyberte si v rámci ESET Security for Microsoft SharePoint niektorú z dostupných manuálnych kontrol:

Kontrola databáz SharePointu

Umožňuje vám vybrať webové stránky SharePoint, ktoré chcete skontrolovať, a spustiť proces kontroly.

Kontrola úložiska

Kontroluje všetky zdieľané priečinky na lokálnom serveri. Ak Kontrola úložiska nie je dostupná, znamená to, že na vašom serveri nie sú žiadne zdieľané priečinky.

Skontrolovať váš počítač

Umožňuje rýchlo spustiť kontrolu počítača a vyliečiť infikované súbory bez potreby zásahu používateľa. Výhodou tohto typu kontroly je rýchle spustenie kontroly bez nutnosti nastavovania. Kontrolujú sa všetky súbory na lokálnych diskoch. Detegované infiltrácie budú automaticky vyliečené alebo zmazané. Úroveň liečenia je automaticky nastavená na predvolenú hodnotu. Podrobnejšie informácie o type liečenia sa nachádzajú v kapitole Liečenie.

> Poznámka:
> Odporúča sa, aby kontrola prebehla raz za 1 – 2 mesiace. Kontrolu je možné nastaviť aj ako plánovanú úlohu.

Vlastná kontrola

Vlastná kontrola je užitočná v prípade, že chcete vybrať konkrétne ciele a metódy kontroly. Výhodou je možnosť vlastného nastavenia všetkých podrobností kontroly. Tieto nastavenia sa dajú uložiť do tzv. profilov. To je užitočné najmä v prípadoch, keď chcete vykonávať pravidelnú prispôsobenú kontrolu počítača pomocou vašich preferovaných nastavení.

Kontrola vymeniteľných médií

Funguje podobne ako Kontrola lokálnych diskov – spustí rýchlu kontrolu vymeniteľných médií pripojených do počítača (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 vírusov alebo iných potenciálnych hrozieb. Tento typ kontroly počítača je možné spustiť aj kliknutím na možnosť **Vlastná kontrola** > **Ciele kontroly** a následným kliknutím na **Vymeniteľné médiá** > **Kontrolovať**.

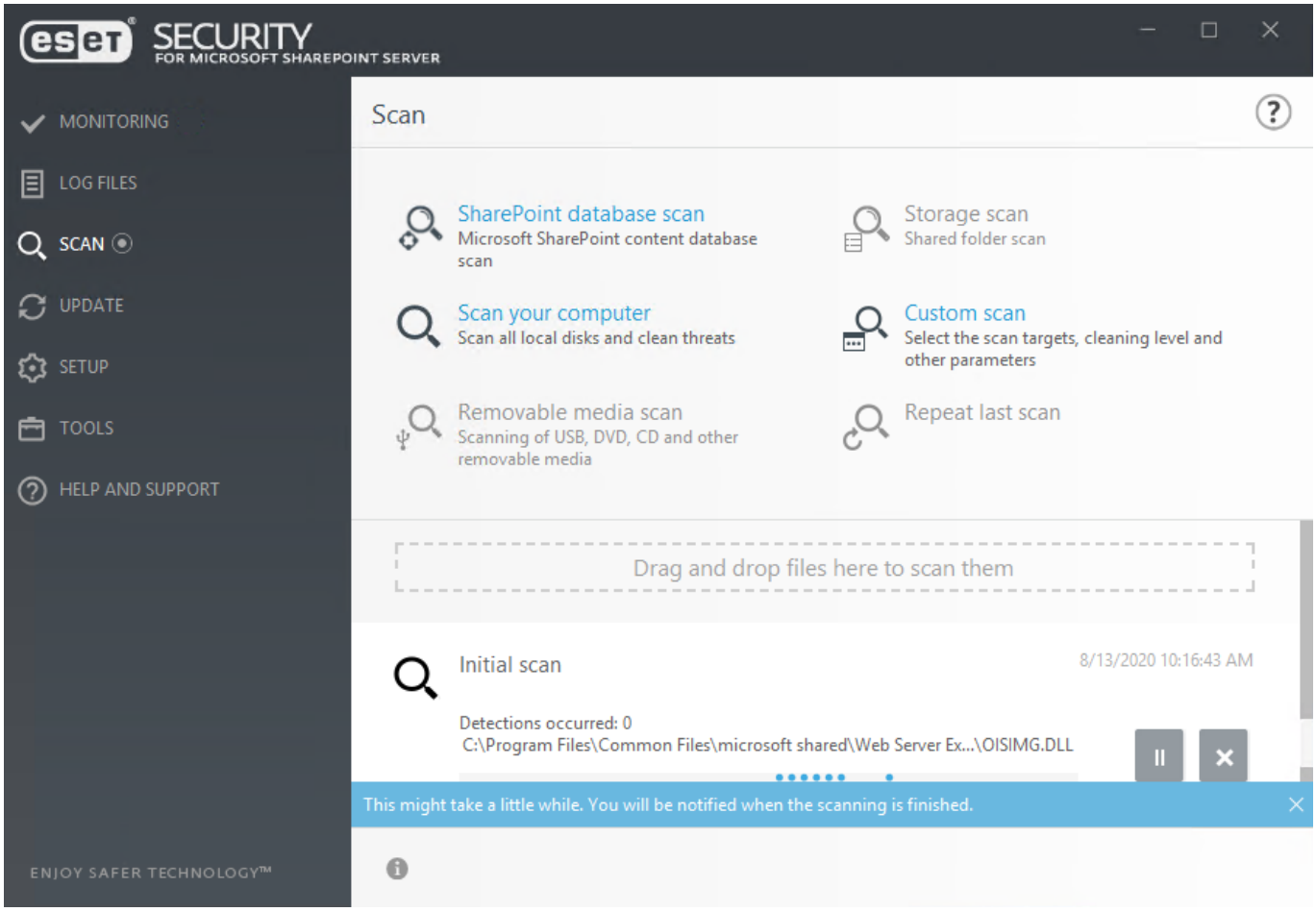
Kontrola Hyper-V

Tento typ kontroly je dostupný len v prípade, že je na serveri nainštalovaný nástroj Hyper-V Manager spolu s produktom ESET Security for Microsoft SharePoint. Kontrola Hyper-V umožňuje kontrolu diskov virtuálnych počítačov na serveri Microsoft Hyper-V bez potreby nasadeného „Agenta“ na danom virtuálnom počítači.

Opakovať poslednú kontrolu

Zopakuje poslednú kontrolu s rovnakými nastaveniami.

> Poznámka:
> Zopakovanie poslednej kontroly nie je dostupné pri manuálnej kontrole databáz.



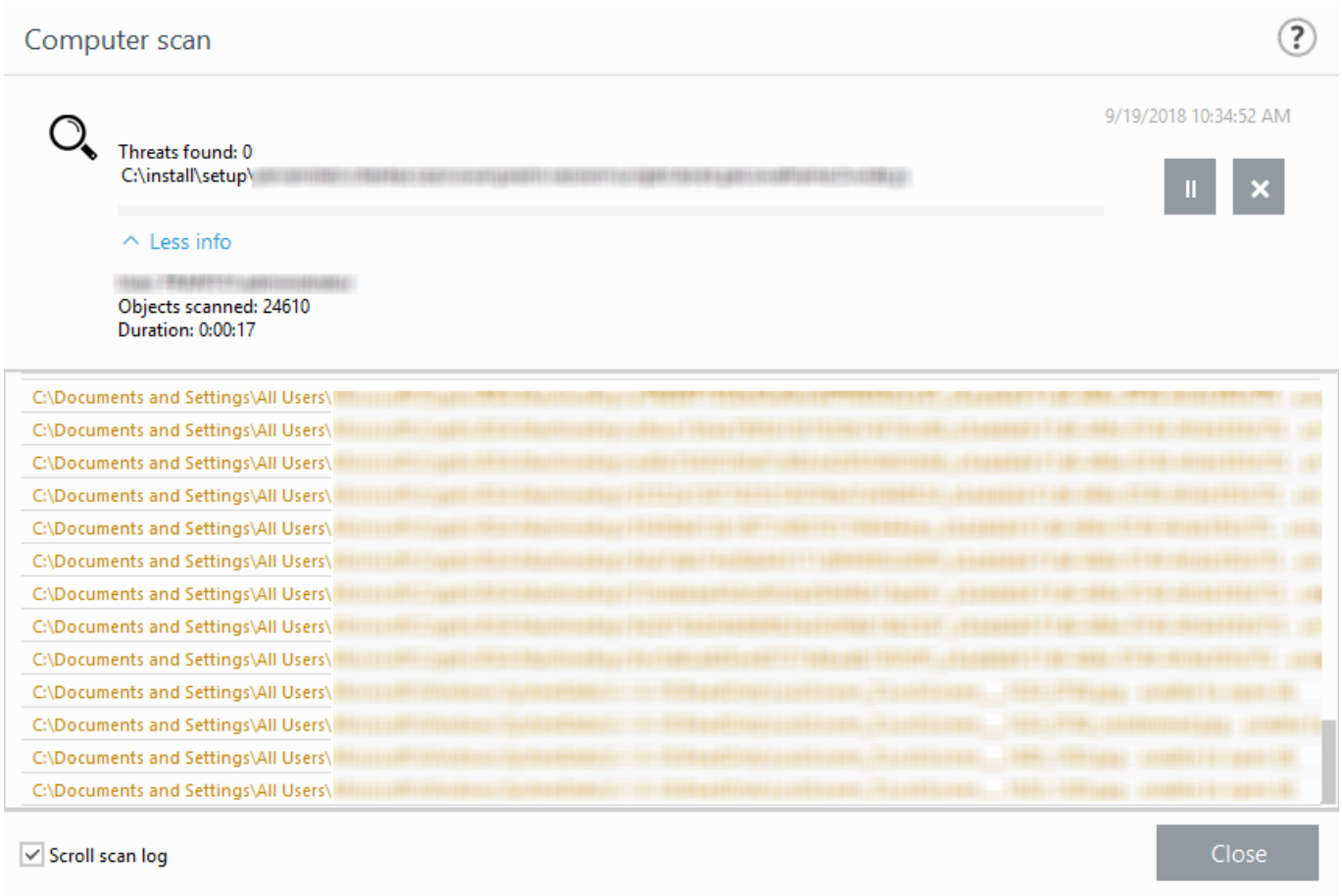
Pomocou nižšie spomenutých možností môžete získať podrobnejšie informácie o prebiehajúcich kontrolách:

Drag and drop	**Súbory môžete skontrolovať aj tak, že ich presuniete myšou do okna kontroly v ESET Security for Microsoft SharePoint. Tieto súbory budú následne okamžite skontrolované.**
Zatvoriť/Zatvoriť všetko	Kliknutím na tieto možnosti zatvoríte konkrétne správy.
Stav kontroly	Zobrazí stav počiatočnej kontroly, konkrétne, či bola kontrola dokončená, alebo bola prerušená používateľom.
Zobraziť protokol	Kliknutím zobrazíte podrobnejšie informácie.
Viac informácií	Počas kontroly môžete kliknúť na túto možnosť pre zobrazenie podrobností, ako napr. **Používateľ**, ktorý spustil kontrolu z grafického používateľského rozhrania, počet **Skontrolovaných objektov** a **Trvanie** kontroly.
Otvoriť okno kontroly	Okno priebehu kontroly ukazuje aktuálny stav kontroly a počet nájdených súborov, ktoré obsahujú škodlivý kód.

Okno kontroly a protokol o kontrole

Okno kontroly zobrazuje práve kontrolované objekty vrátane ich umiestnenia, počet nájdených hrozieb, počet kontrolovaných objektov a čas trvania kontroly. Spodnú časť okna tvorí protokol o kontrole, ktorý zobrazuje verziu detekčného jadra, dátum a čas začatia kontroly a ciele kontroly.

Ak práve prebieha kontrola a chcete ju dočasne prerušiť, môžete kliknúť na **Pozastaviť**. Ak je kontrola pozastavená, môžete ju znova spustiť kliknutím na **Pokračovať**.

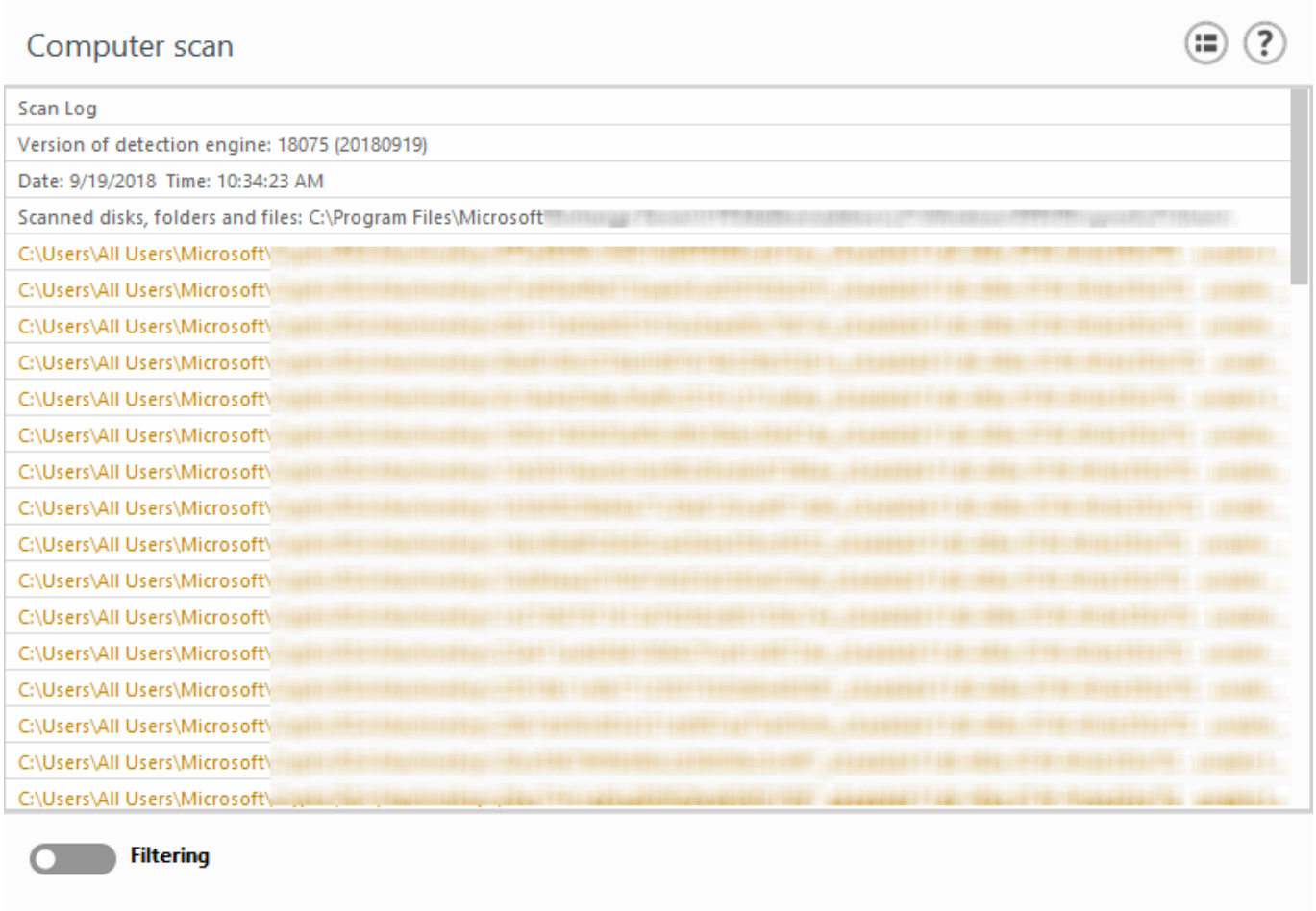


Rolovanie výpisu protokolu kontroly

Ponechajte túto možnosť zapnutú, ak chcete, aby sa okno Protokoly posúvalo súčasne s pribúdajúcimi protokolmi.

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

Po ukončení kontroly sa zobrazí protokol o kontrole, ktorý bude obsahovať všetky relevantné informácie súvisiace s danou kontrolou.



Kliknutím na ikonu **Filtrovanie** otvoríte okno Filtrovanie protokolov, kde môžete nastaviť podmienky filtrovania alebo vyhľadávania. Kliknutím na konkrétny záznam protokolu pravým tlačidlom myši zobrazíte kontextové menu:

Akcia	Použitie	Skratka	Pozrite si tiež
Filtrovať rovnaké záznamy	Po aktivácii tohto filtra sa zobrazia protokoly rovnakého typu.	Ctrl + Shift + F	
Filtrovať...	Po kliknutí na túto možnosť vám okno Filtrovanie protokolov umožní definovať kritériá filtrovania pre konkrétne položky protokolu.		Filtrovanie protokolov
Zapnúť filter	Zapne filter, ktorý ste nastavili v okne Filtrovanie protokolov. Pri prvej aktivácii filtrovania musíte upresniť nastavenia.		
Zrušiť filter	Vypne aktivovaný filter.		
Kopírovať	Kopíruje len označené protokoly z okna.	Ctrl + C	
Kopírovať všetko	Kopíruje informácie zo všetkých záznamov v okne.		
Exportovať...	Exportuje informácie o označených/vybraných protokoloch vo formáte XML.		
Exportovať všetko...	Exportuje všetky informácie zo všetkých protokolov vo formáte XML.		

Protokoly

Protokoly obsahujú informácie o dôležitých systémových udalostiach a poskytujú prehľad o výsledkoch kontroly, odhalených hrozbách atď. 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. Zaznamenávajú sa informácie podľa aktuálnych nastavení detailnosti protokolov. Prezeranie alebo exportovanie protokolov je umožnené priamo z prostredia ESET Security for Microsoft SharePoint.

Vyberte typ protokolu z roletového menu. Sú dostupné tieto typy protokolov:

Detekcie

Protokol Detekcie ponúka podrobné informácie o infiltráciách zachytených modulmi ESET Security for Microsoft SharePoint. Informácie zahŕňajú čas detekcie, názov infiltrácie, umiestnenie, vykonanú akciu a používateľa prihláseného v čase detekcie. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte jej podrobnosti v novom okne. V prípade potreby môžete vytvoriť vylúčenie detekcie – pravým tlačidlom myši kliknite na záznam protokolu (detekciu) a potom na **Vytvoriť vylúčenie**. Otvorí sa sprievodca vylúčeniami s preddefinovanými kritériami. Ak je pri vylúčenom súbore uvedený aj názov detekcie, znamená to, že v rámci súboru je vylúčená iba daná detekcia, nie je vylúčený súbor ako celok. Ak by teda došlo k infikovaniu tohto súboru iným typom malvéru, takáto hrozba bude detegovaná.

Udalosti

V tomto protokole sú zaznamenané všetky dôležité operácie vykonané produktom ESET Security for Microsoft SharePoint. 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

Všetky výsledky kontroly sú zobrazené v tomto okne. Každý riadok prináleží samostatnej kontrole. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte podrobnosti príslušnej kontroly.

Blokované súbory

Tento protokol obsahuje záznamy o súboroch, ktoré boli zablokované alebo neboli prístupné. Zobrazený je tiež dôvod blokovania, modul, ktorý prístup zablokoval, ako aj informácie o aplikácii, ktorá sa pokúšala získať prístup k súboru a pod akým používateľom bola spustená.

Odoslané súbory

Protokol obsahuje prehľad súborov zachytených cloudovou ochranou (ESET Dynamic Threat Defense a ESET LiveGrid®).

Protokoly auditu

Obsahujú záznamy o zmenách v konfigurácii alebo stave ochrany a vytvárajú snímky (snapshot) pre neskoršie použitie. Kliknutím pravým tlačidlom myši na ktorýkoľvek záznam zmeny nastavení a zvolením možnosti **Zobraziť** z kontextového menu sa zobrazia podrobné informácie o vykonanej zmene. Ak sa chcete vrátiť k pôvodným nastaveniam, použite možnosť **Obnoviť**. Môžete tiež použiť možnosť **Odstrániť všetko** a odstrániť záznamy protokolu. Ak chcete deaktivovať zapisovanie do protokolov auditu, prejdite do sekcie **Rozšírené nastavenia** > **Nástroje** > **Protokoly** > Protokol auditu.

HIPS

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 obsahuje záznamy o súboroch, ktoré boli zablokované Ochranou pred botnetmi a IDS (Ochrana pred sieťovými útokmi).

Filtrované webové stránky

Zoznam webových stránok, ktoré boli zablokované Ochranou prístupu na web . V týchto protokol nájdete čas, adresu URL, používateľa a aplikáciu, ktorá vytvorila spojenie s príslušnou webovou stránkou.

Správa zariadení

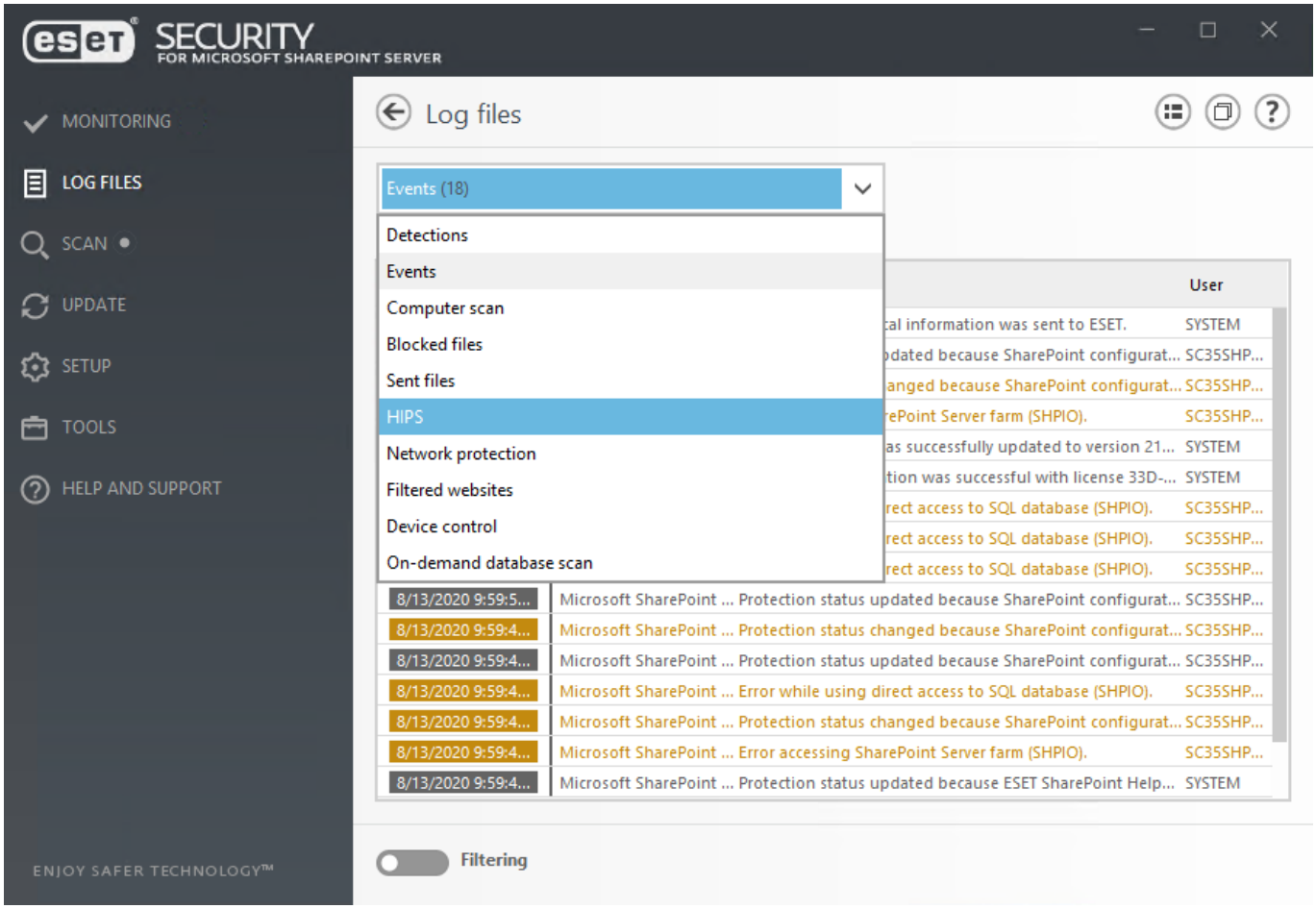
Zoznam vymeniteľných médií a zariadení, ktoré boli pripojené k vášmu počítaču. V protokole sú zaznamenané len zariadenia s vytvoreným pravidlom. Ak na pripojené zariadenie nie je uplatnené žiadne pravidlo, protokol sa nevytvorí. Môžete tu tiež vidieť podrobnosti o zariadeniach, ako napríklad typ zariadenia, sériové číslo, výrobca, model, veľkosť pamäte (v prípade médií).

Manuálna kontrola databáz

Obsahuje zoznam kontrol databáz obsahu SharePointu. Pre každú kontrolu budú zobrazené nasledujúce informácie: verzia detekčného jadra, dátum, lokalita kontroly, počet kontrolovaných objektov, počet zistených hrozieb, počet uplatnených pravidiel a čas ukončenia kontroly.

Kontrola Hyper-V

Obsahuje zoznam výsledkov kontroly Hyper-V. Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte podrobnosti príslušnej kontroly.



Kontextové menu (pravé tlačidlo myši) vám umožňuje vybrať akciu, ktorá bude vykonaná pre zvolený záznam v protokole:

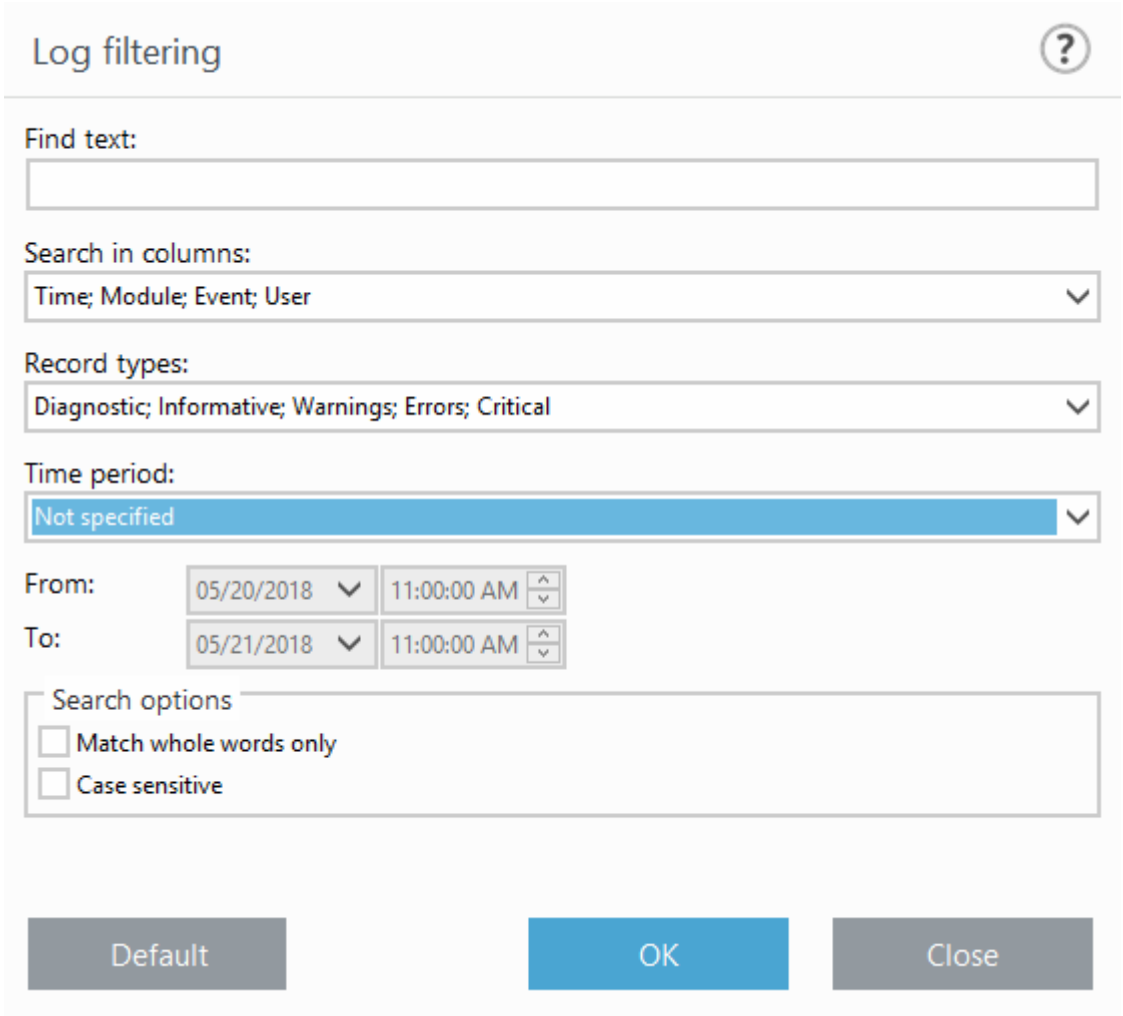
Akcia	Použitie	Skratka	Pozrite si tiež
Zobraziť	Zobrazí podrobnejšie informácie o označenom protokole v novom okne (rovnako ako pri dvojitom kliknutí).		
Filtrovať rovnaké záznamy	Po aktivácii tohto filtra sa zobrazia protokoly rovnakého typu.	Ctrl + Shift + F	
Filtrovať...	Po kliknutí na túto možnosť vám okno Filtrovanie protokolov umožní definovať kritériá filtrovania pre konkrétne položky protokolu.		Filtrovanie protokolov
Zapnúť filter	Zapne filter, ktorý ste nastavili v okne Filtrovanie protokolov. Pri prvej aktivácii filtrovania musíte upresniť nastavenia.		
Zrušiť filter	Vypne aktivovaný filter.		
Kopírovať	Kopíruje len označené protokoly z okna.	Ctrl + C	
Kopírovať všetko	Kopíruje informácie zo všetkých záznamov v okne.		
Odstrániť	Odstráni označené záznamy – táto akcia si vyžaduje oprávnenia správcu.	Del	
Odstrániť všetko	Odstráni všetky záznamy v okne – táto akcia si vyžaduje oprávnenia správcu.		
Exportovať...	Exportuje informácie o označených/vybraných protokoloch vo formáte XML.		
Exportovať všetko...	Exportuje všetky informácie zo všetkých protokolov vo formáte XML.		

Akcia	Použitie	Skratka	Pozrite si tiež
Hľadať...	Otvorí okno Vyhľadávanie v protokole a umožní vám definovať kritériá vyhľadávania. Funkciu „hľadať“ môžete použiť na vyhľadanie konkrétneho záznamu aj v prípade, že je filtrovanie zapnuté.	Ctrl + F	Vyhľadávanie v protokole
Hľadať ďalší	Nájde ďalší výskyt podľa kritérií vyhľadávania.	F3	
Hľadať predošlý	Nájde predchádzajúci výskyt.	Shift + F3	
Vytvoriť vylúčenie	Vylúči objekty z liečenia, a to pomocou názvu detekcie, cesty alebo hodnoty hash.		Vytvoriť vylúčenie

Filtrovanie protokolov

Filtrovanie protokolov vám umožňuje nájsť konkrétnu informáciu v protokoloch. Vďaka tejto funkcii môžete zobraziť záznamy protokolu, ktoré spĺňajú určité kritériá; napr. môžete filtrovať konkrétny typ udalosti, stav alebo časové obdobie. Vyberte Typy záznamov a nastavte Časové obdobie pre vyhľadávanie v určitom časovom období. Upresnením nastavení vyhľadávania docielite zobrazenie len tých výsledkov, ktoré sú pre vás dôležité.

Do poľa **Hľadať text** zadajte kľúčové slovo, ktoré chcete vyhľadať. Pomocou roletového menu **Hľadať v stĺpcoch** môžete bližšie upresniť svoje vyhľadávanie. Z roletového menu **Typy záznamov** vyberte jeden alebo viacero typov záznamov. Môžete taktiež vybrať **Časové obdobie**, v ktorom chcete zobraziť výsledky. Zobrazené výsledky môžete ešte viac upresniť pomocou ďalších možností vyhľadávania, akými sú napr. **Hľadať iba celé slová** alebo **Rozlišovať veľké a malé písmená**.



Hľadať text

Zadajte textový reťazec (slovo alebo časť slova). Budú zobrazené len záznamy, ktoré obsahujú zadané slovo. Ostatné záznamy nebudú brané do úvahy.

Hľadať v stĺpcoch

Vyberte stĺpce, ktoré budú zohľadnené pri vyhľadávaní. Môžete označiť jeden alebo viac stĺpcov.

Typy záznamov

Z roletového menu vyberte jeden alebo viacero typov záznamov:

- **Diagnostické** – informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informačné** – informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Varovania** – varovné správy a kritické chyby.
- **Chyby** – chyby typu „Chyba pri sťahovaní súboru“ a kritické chyby.
- **Kritické** – len kritické chyby.

Časové obdobie

Túto možnosť použite v prípade, ak chcete, aby boli vyhľadávané iba záznamy, ktoré spadajú do určeného časového obdobia:

- **Nešpecifikované** (predvolené) – vyhľadáva v celom protokole.
- **Posledný deň**
- **Posledný týždeň**
- **Posledný mesiac**
- **Časové obdobie** – pomocou tejto možnosti môžete určiť časový interval (dátum a čas) pre zobrazenie protokolov zaznamenaných v danom časovom období.

Hľadať iba celé slová

Túto možnosť použite v prípade, ak chcete vyhľadávať len pre zadaný tvar kľúčového slova.

Rozlišovať veľké a malé písmená

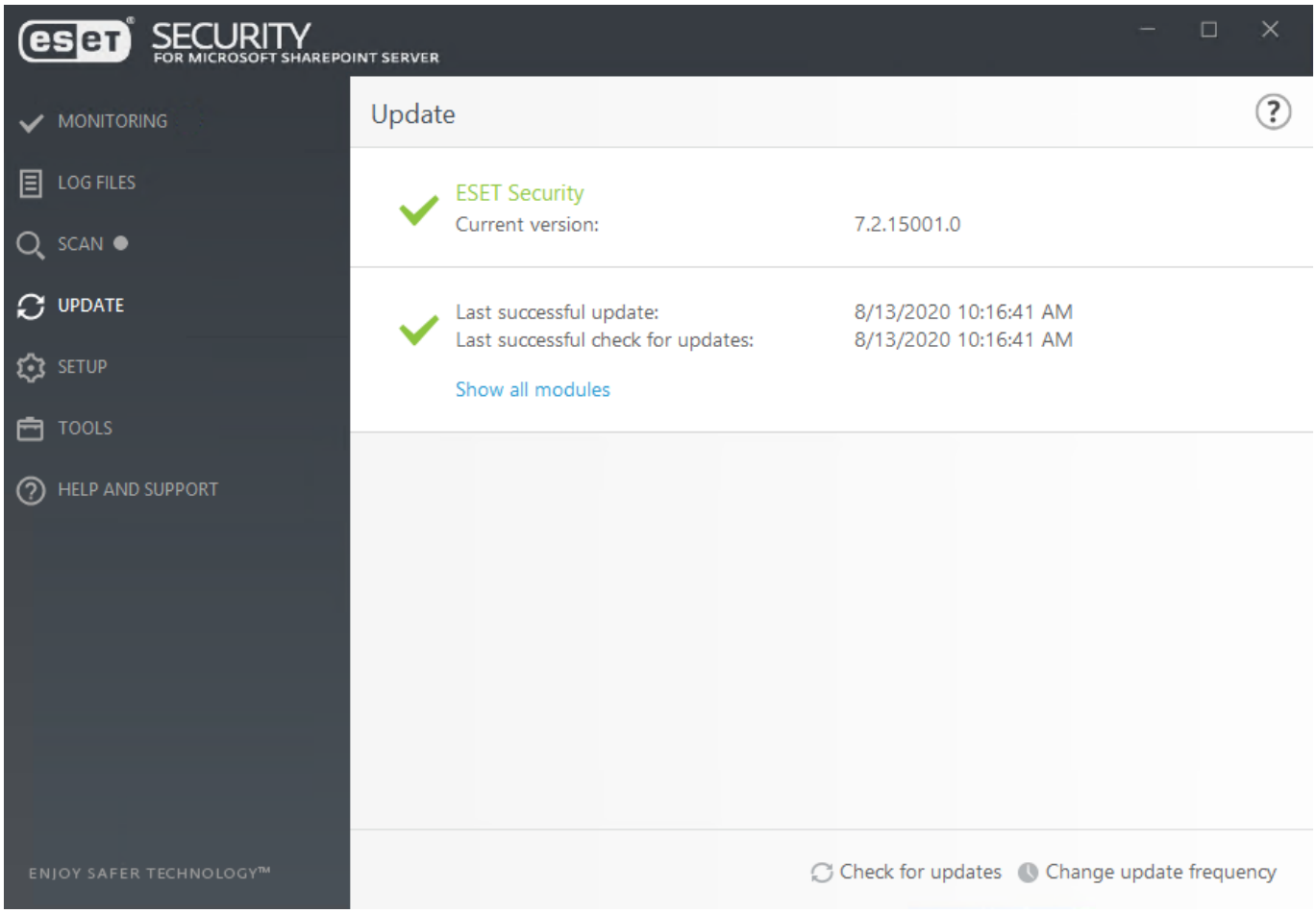
Túto možnosť použite v prípade, ak je dôležité vo vyhľadávaní rozlišovať malé a veľké písmená. Po nastavení možností vyhľadávania kliknite na **OK** pre zobrazenie filtrovaných záznamov, prípadne kliknite na **Hľadať** pre spustenie vyhľadávania. Protokoly sú prehľadávané smerom zhora nadol, začínajúc z danej pozície (záznam, ktorý je momentálne označený). Vyhľadávanie sa zastaví pri prvom nájdenom zázname. Stlačením klávesu **F3** budete pokračovať vo vyhľadávaní ďalšieho záznamu, prípadne môžete kliknúť pravým tlačidlom myši, vybrať možnosť **Hľadať** a upresniť možnosti vyhľadávania.

Aktualizácia

V sekcii Aktualizácia je zobrazený stav aktualizácie vášho produktu ESET Security for Microsoft SharePoint vrátane dátumu a času poslednej úspešnej aktualizácie. Pravidelná aktualizácia produktu ESET Security for Microsoft SharePoint a programových modulov je tou najlepšou metódou, ako zabezpečiť maximálnu úroveň ochrany vášho servera. Modul Aktualizácia zabezpečuje, aby bol program stále aktuálny, čo zahŕňa aktualizáciu detekčného

jadra, ako aj aktualizáciu všetkých komponentov systému. Aktualizácia detekčného jadra a programových súčastí je dôležitá na zabezpečenie komplexnej ochrany pred škodlivým kódom.

Poznámka:
Ak ste ešte nezadali licenčný kľúč, aktualizáciu nebude možné vykonať a budete vyzvaný, aby ste si aktivovali svoj produkt. Pre aktiváciu produktu prejdite do sekcie **Pomocník a podpora** > **Aktivovať produkt**.



Aktuálna verzia

Aktuálna verzia produktu ESET Security for Microsoft SharePoint.

Posledná úspešná aktualizácia

Dátum, kedy sa program naposledy aktualizoval. Ak nie je zobrazený dnešný dátum, je možné, že moduly nie sú aktuálne.

Posledné úspešné overenie dostupnosti aktualizácií

Dátum, kedy sa program naposledy pokúšal overiť dostupnosť aktualizácií modulov.

Zobraziť všetky moduly

Otvorí sa zoznam nainštalovaných modulov.

Overiť dostupnosť aktualizácií

Aktualizácia modulov je dôležitá súčasť na zabezpečenie komplexnej ochrany pred škodlivým kódom.

Zmeniť frekvenciu aktualizácií

Kliknutím na túto možnosť môžete zmeniť interval spúšťania úlohy určenej na pravidelnú automatickú aktualizáciu.

Ak nedôjde k aktualizácii dlhší čas, môžu sa zobraziť nasledujúce chybové hlásenia:

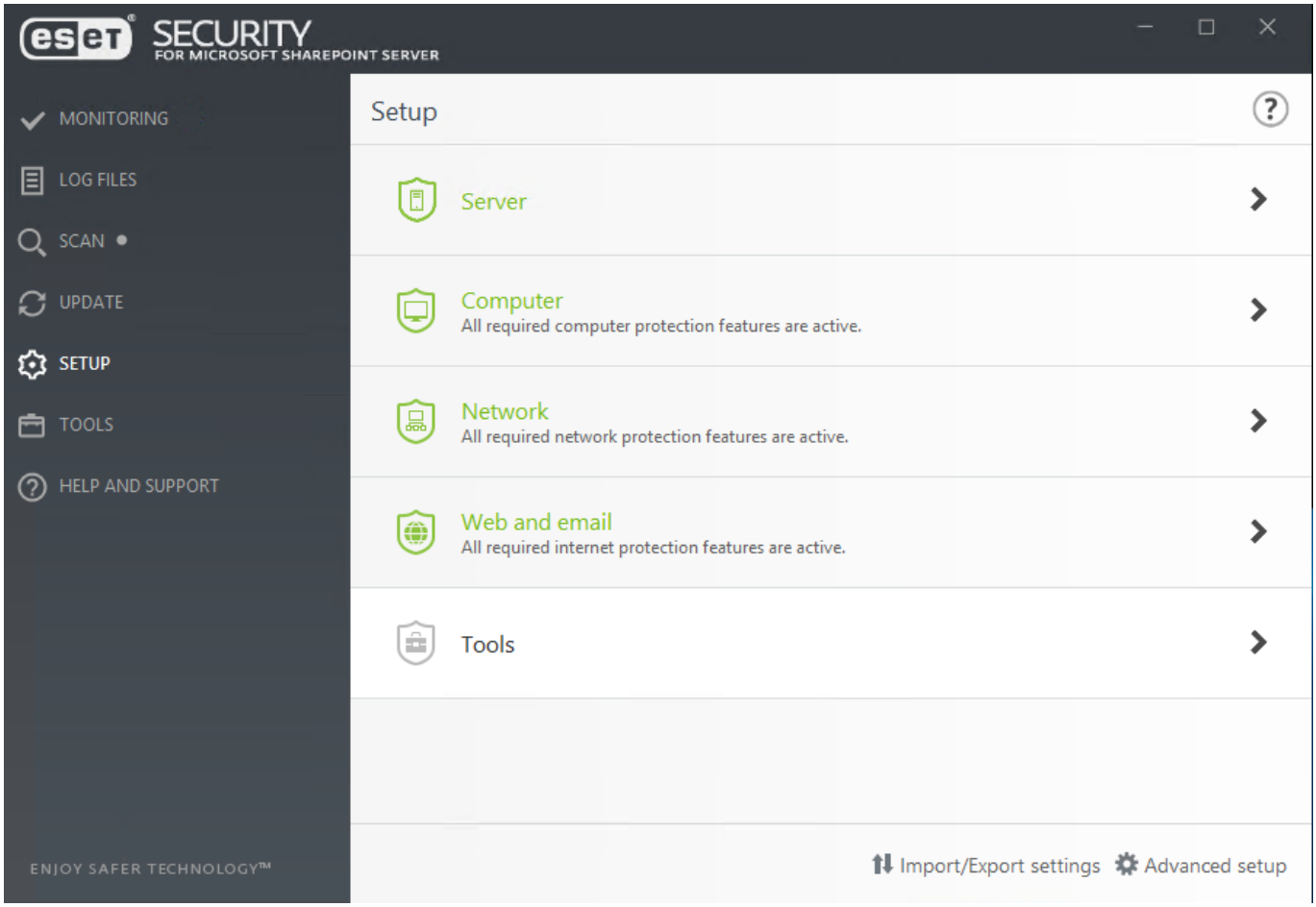
Chybové hlásenie	Popis
Moduly programu sú neaktuálne.	Toto hlásenie sa zobrazí po niekoľkých neúspešných pokusoch o aktualizáciu. Odporúčame, aby ste skontrolovali nastavenia aktualizácie. Najčastejším problémom sú nesprávne zadané overovacie údaje alebo nesprávne nakonfigurované nastavenia pripojenia.
Aktualizácia modulov nebola úspešná – produkt nie je aktivovaný	Licenčný kľúč bol zadaný nesprávne. Odporúčame, aby ste skontrolovali overovacie údaje. **Rozšírené nastavenia** (**F5**) obsahujú dodatočné nastavenia aktualizácií. Kliknite na **Pomocník a podpora** > Spravovať licenciu a zadajte nový licenčný kľúč.
Pri sťahovaní aktualizačných súborov nastala chyba	Táto chyba môže byť spôsobená nesprávnym nastavením internetového pripojenia. Odporúčame, aby ste skontrolovali vaše internetové pripojenie (otvorením akejkoľvek webovej stránky vo webovom prehliadači). Ak sa webová stránka nenačíta, pravdepodobne nie je nastavené internetové pripojenie alebo má váš počítač problémy s pripojením. Uistite sa tiež, že váš poskytovateľ internetu nemá výpadok pripojenia.
Aktualizácia modulov nebola úspešná Chyba 0073	Kliknite na **Aktualizácia** > **Overiť dostupnosť aktualizácií**. Viac informácií nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Poznámka:
Nastavenia proxy servera sa môžu líšiť pre rôzne aktualizačné profily. Ak ide o takýto prípad, nakonfigurujte jednotlivé aktualizačné profily v okne **Rozšírené nastavenia** (**F5**) kliknutím na **Aktualizácia** > Profily.

Nastavenia

Sekcia Nastavenia obsahuje nasledujúce časti:

- Server
- Počítač
- Sieť
- Web a e-mail
- Nástroje – Diagnostické zapisovanie do protokolu



Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo. Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso.

Import/export nastavení

Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Server

Zobrazí sa okno so zoznamom komponentov, ktoré môžete zapnúť/vypnúť pomocou ikony. Pre zobrazenie nastavení pre konkrétnu položku kliknite na ozubené koleso.

Rezidentná ochrana SharePoint Servera

Ide o filtrovanie pri prístupe, ktoré je možné v prípade potreby konfigurovať. Kliknite na ikonu ⚙, čím sa otvorí okno Nastavenia ochrany SharePoint.

Automatické vylúčenia

Automaticky dôjde k identifikácii kritických aplikácií a súborov operačného systému servera a ich následnému pridaniu do zoznamu vylúčení. Tým sa znižuje riziko konfliktov a zvyšuje celkový výkon servera pri spustenej detekcii hrozieb.

Klaster

V tejto sekcii môžete nakonfigurovať a aktivovať klaster ESET.

Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo. Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso ⚙.

Import/export nastavení

Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Počítač

ESET Security for Microsoft SharePoint obsahuje všetky potrebné moduly na poskytovanie ochrany pre server a počítače v sieti. Tento modul vám umožňuje zapnúť/vypnúť alebo nastaviť nasledujúce komponenty:

Rezidentná ochrana súborového systému

Všetky súbory, ktoré sa v počítači otvárajú, vytvárajú alebo spúšťajú sú kontrolované na prítomnosť infiltrácie. Pre Rezidentnú ochranu existuje aj možnosť **Nastaviť** alebo **Upraviť vylúčenia**, ktorá otvorí okno nastavení pre vylúčenia, kde môžete definovať súbory a priečinky, ktoré majú byť vylúčené z kontroly.

Správa zariadení

Tento modul umožňuje kontrolovať (skenovať), blokovať a nastavovať rozšírené prístupové práva a pravidlá filtrovania, ako aj nastavovať prístup konkrétneho používateľa k zariadeniu.

Host Intrusion Prevention System (HIPS)

Systém HIPS monitoruje udalosti vo vnútri operačného systému a reaguje na ne podľa pravidiel, ktoré sú štruktúrou podobné pravidlám firewallu.

- Pokročilá kontrola pamäte
- Exploit Blocker
- Ransomware Shield

Prezentačný režim

Táto funkcia je určená pre používateľov, ktorí chcú neprerušovane používať svoj softvér a neželajú si byť vyrušovaní oznámeniami a dialógovými oknami, pričom taktiež požadujú minimálnu záťaž systému. Po zapnutí prezentačného režimu sa zobrazí upozornenie (potenciálne bezpečnostné riziko) a hlavné okno programu zmení farbu na oranžovú.

Pozastaviť antivírusovú a antispyvérovú ochranu

Ak chcete dočasne pozastaviť antivírusovú a antispyvérovú ochranu, z roletového menu vyberte časové obdobie, na ktoré chcete pozastaviť ochranu, a následne kliknite na **Použiť**. Pre opätovné zapnutie pozastavenej ochrany kliknite na možnosť **Zapnúť antivírusovú a antispyvérovú ochranu**.

Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo. Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso.

Import/export nastavení

Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Sieť

V tejto časti nájdete komponenty, pomocou ktorých môžete vytvárať pravidlá, ktoré slúžia na povolenie alebo blokovanie sieťovej komunikácie. Tieto komponenty poskytujú ochranu pred útokmi zo vzdialených počítačov a blokujú niektoré potenciálne nebezpečné služby.

Modul Sieť vám umožňuje zapnúť/vypnúť alebo nakonfigurovať nasledujúce komponenty:

Ochrana pred sieťovými útokmi (IDS)

Analyzuje obsah sieťovej komunikácie a poskytuje ochranu pred sieťovými útokmi. Sieťová komunikácia, ktorá je vyhodnotená ako škodlivá, bude blokovaná.

Ochrana pred botnetmi

Detekcia a blokovanie komunikácie siete botnet. Slúži na rýchle a presné odhalenie malvéru v systéme.

Dočasný blacklist IP adries (blokované adresy)

Kliknutím zobrazíte zoznam IP adries, ktoré boli zachytené ako zdroj útokov a pridané na blacklist s cieľom na istý čas zablokovať spojenie.

Sprievodca riešením problémov (nedávno blokované aplikácie alebo zariadenia)

Tento sprievodca vám pomôže pri riešení problémov s pripojením, ktoré boli spôsobené ochranou pred sieťovými útokmi.

Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo. Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso.

Import/export nastavení

Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Sprievodca riešením problémov so sieťou

Sprievodca riešením problémov monitoruje blokovanú sieťovú komunikáciu a prevedie vás procesom riešenia problémov s ochranou pred sieťovými útokmi, ktoré sa týkajú konkrétnych aplikácií alebo zariadení. Sprievodca tiež navrhne novú sadu pravidiel, ktoré môžete schváliť a aplikovať.

Web a e-mail

V sekcii Web a e-mail môžete zapnúť, vypnúť a nastaviť nasledujúce komponenty:

Ochrana prístupu na web

Ak je zapnutá, všetka HTTP alebo HTTPS komunikácia je kontrolovaná na prítomnosť škodlivého kódu.

Ochrana e-mailových klientov

Zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3 a IMAP.

Antiphishingová ochrana

Filtruje obsah webových stránok podozrivých z distribúcie obsahu určeného na manipuláciu používateľov, aby poskytli svoje osobné údaje (napr. heslá, bankové údaje atď.).

Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo  vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo . Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso .

Import/export nastavení

Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

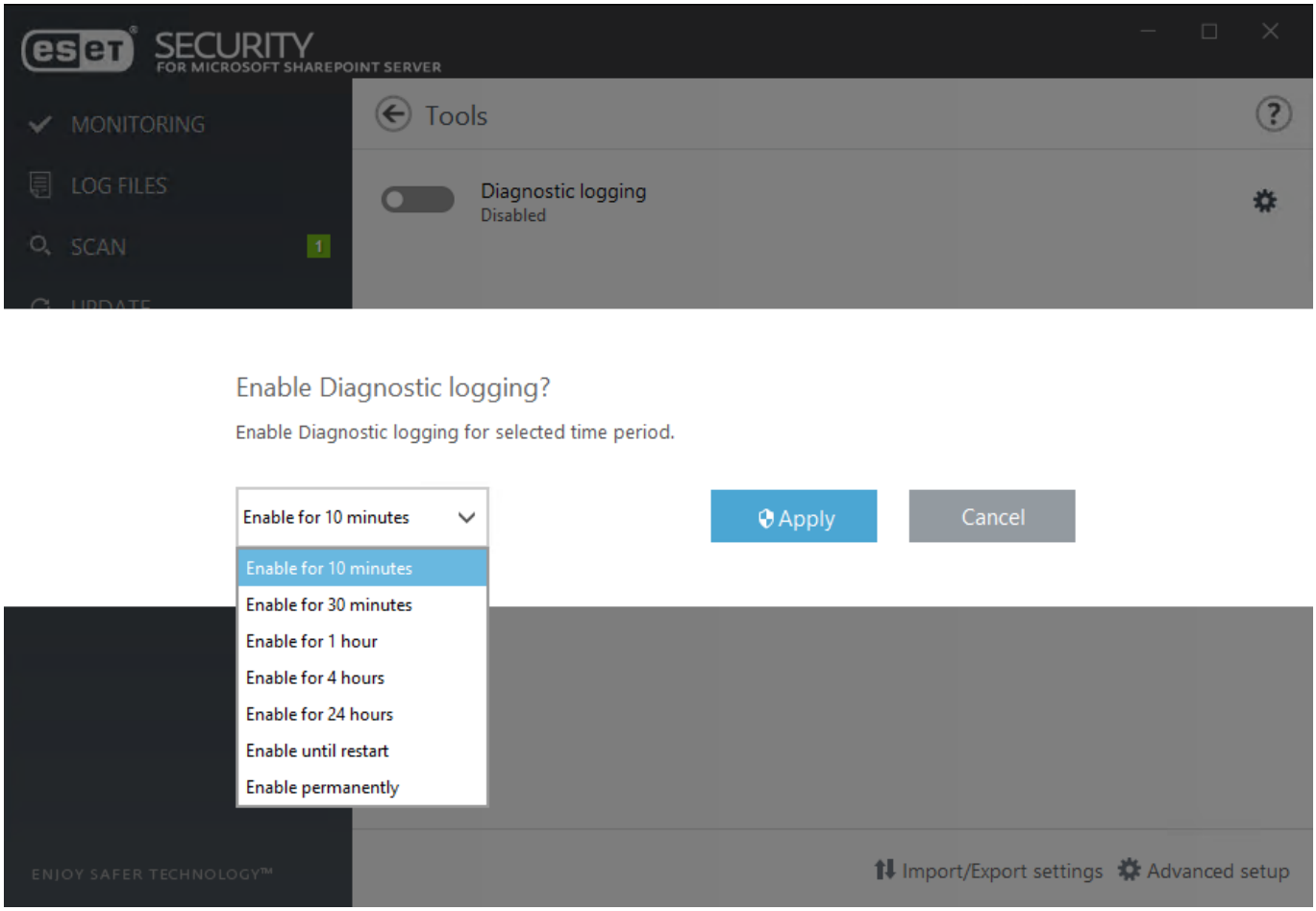
Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Nástroje – Diagnostické zapisovanie do protokolu

Diagnostické zapisovanie do protokolov môžete použiť v prípade, keď potrebujete získať podrobné informácie o aktivite konkrétnej funkcie programu ESET Security for Microsoft SharePoint (napríklad na účely riešenia problémov). Kliknutím na ikonu  môžete určiť, pre ktoré funkcie programu budú vytvárané diagnostické protokoly.

Môžete tiež vybrať časové obdobie, počas ktorého bude táto funkcia povolená (10 minút, 30 minút, 1 hodina, 4 hodiny, 24 hodín, do ďalšieho reštartu servera, natrvalo). Po povolení diagnostického zapisovania do protokolov bude ESET Security for Microsoft SharePoint vytvárať podrobné protokoly v závislosti od funkcií povolených v tejto sekcii.



Pre dočasné pozastavenie jednotlivých modulov kliknite na zelené tlačidlo vedľa príslušného modulu. Berte na vedomie, že pozastavením jednotlivých modulov vystavujete váš systém bezpečnostnému riziku.

Pre opätovné zapnutie vypnutého bezpečnostného modulu kliknite na červené tlačidlo. Modul bude opäť aktívny.

Pre zobrazenie podrobných nastavení konkrétneho bezpečnostného modulu kliknite na ozubené koleso.

Import/export nastavení

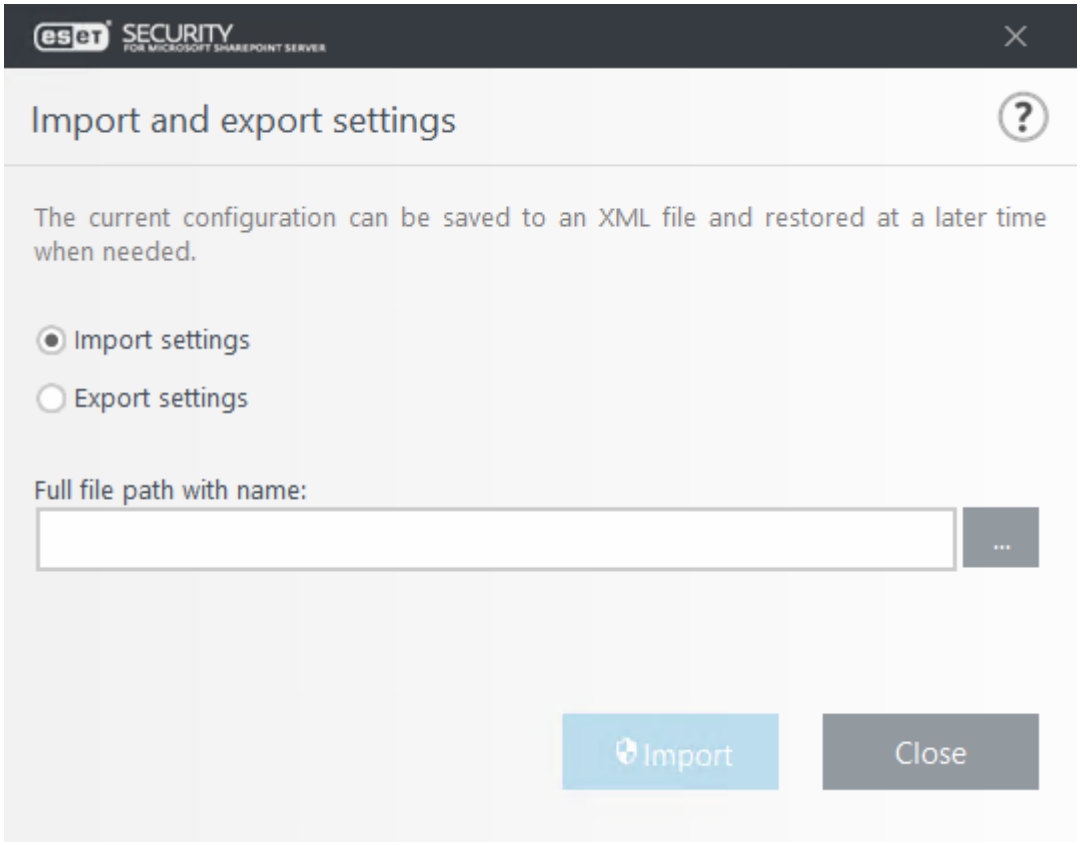
Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

V tejto časti nájdete podrobné nastavenia programu, ktoré si môžete upraviť podľa potreby. Do **Rozšírených nastavení** sa dostanete z ktorejkoľvek časti programu pomocou klávesu **F5**.

Import a export nastavení

Import a export sú užitočné funkcie, ak potrebujete zálohovať nastavenia produktu ESET Security for Microsoft SharePoint. Export môžete využiť pri odosielaní/aplikovaní rovnakých nastavení na iné servery, kde je nainštalovaný produkt ESET Security for Microsoft SharePoint. Nastavenia sú exportované v podobe súboru *.xml*.

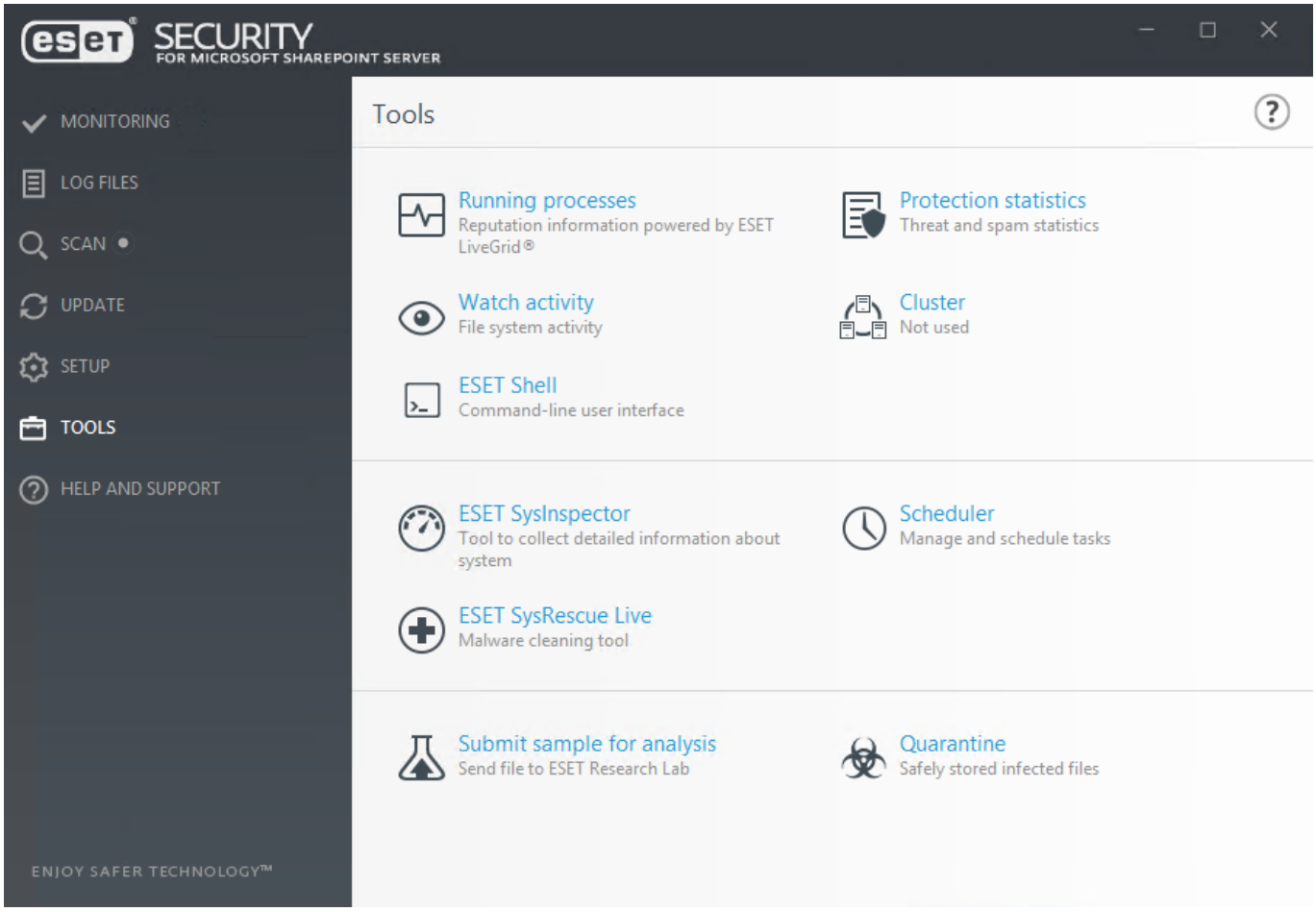


Poznámka:
Ak nemáte dostatočné oprávnenia na zapisovanie exportovaného súboru do určeného adresára, môže sa pri exportovaní zobraziť chybové hlásenie.

Nástroje

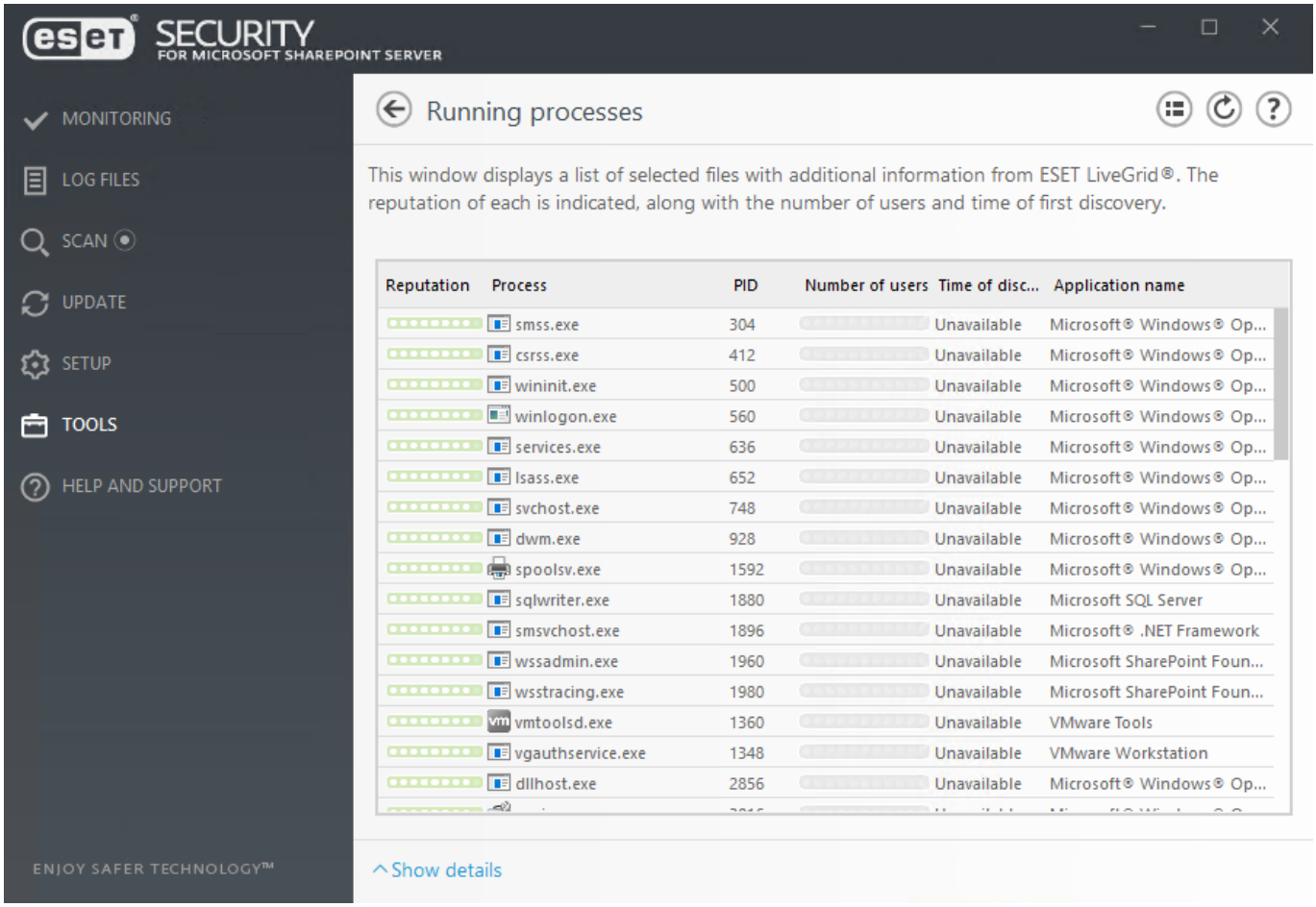
Na správu programu ESET Security for Microsoft SharePoint sú dostupné nasledujúce funkcie:

- Spustené procesy
- Sledovanie aktivity
- Štatistiky ochrany
- Klaster
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Plánovač
- Odoslanie vzorky na analýzu
- Karanténa



Spustené procesy

Okno spustené procesy zobrazuje programy a procesy, ktoré sú spustené vo vašom počítači, a zabezpečuje pohotovú a neustálu informovanosť spoločnosti ESET o nových infiltráciách. ESET Security for Microsoft SharePoint poskytuje podrobné informácie o spustených procesoch s cieľom chrániť používateľov vďaka technológii ESET LiveGrid®.



Poznámka:
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.

Úroveň rizika	**Vo väčšine prípadov ESET Security for Microsoft SharePoint 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 aj pravým kliknutím kdekoľvek na hlavný panel a zvolením možnosti Spustiť správcu úloh, prípadne pomocou klávesovej skratky Ctrl + Shift + Esc.
PID	Identifikačné číslo procesu spusteného na operačnom systéme Windows.
Počet používateľov	Počet používateľov, ktorí používajú danú aplikáciu. Tieto informácie sú zhromažďované pomocou technológie ESET LiveGrid®.
Čas objavenia	Doba, odkedy bol proces objavený technológiou ESET LiveGrid®.
Názov aplikácie	Názov vydavateľa aplikácie alebo procesu.

Poznámka:
Aj v prípade, že je aplikácia označená ako Neznáma (oranžová), nemusí to znamenať, že obsahuje škodlivý kód. Zvyčajne ide o novú aplikáciu. Ak si nie je používateľ istý, či je tomu skutočne tak, má možnosť poslať vzorku na analýzu do vírusového laboratória spoločnosti ESET. Ak sa ukáže, že ide o nebezpečnú aplikáciu, jej detekcia bude pridaná v najbližšej aktualizácii detekčného jadra.

Zobraziť podrobnosti

Po kliknutí na jednotlivé procesy sa v dolnej časti okna zobrazia nasledujúce informácie:

- **Cesta –** umiestnenie aplikácie vo vašom počítači.
- **Veľkosť** – veľkosť súboru 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, kedy bola aplikácia vytvorená.
- **Upravené** – dátum a čas, kedy bola aplikácia naposledy upravená.

Pridať vylúčenia procesov

Kliknutím pravého tlačidla na konkrétny proces v okne Spustené procesy ho môžete vylúčiť z kontroly. Cesta k danému procesu bude pridaná do zoznamu vylúčení.

Sledovanie aktivity

V okne Sledovanie aktivity môžete prostredníctvom grafov sledovať aktivitu:

Aktivita súborového systému

Zobrazuje objem prečítaných a zapisovaných dát. Zvislá os grafu zobrazuje množstvo prečítaných dát (modrou farbou) a množstvo zapisovaných dát (zelenou farbou).

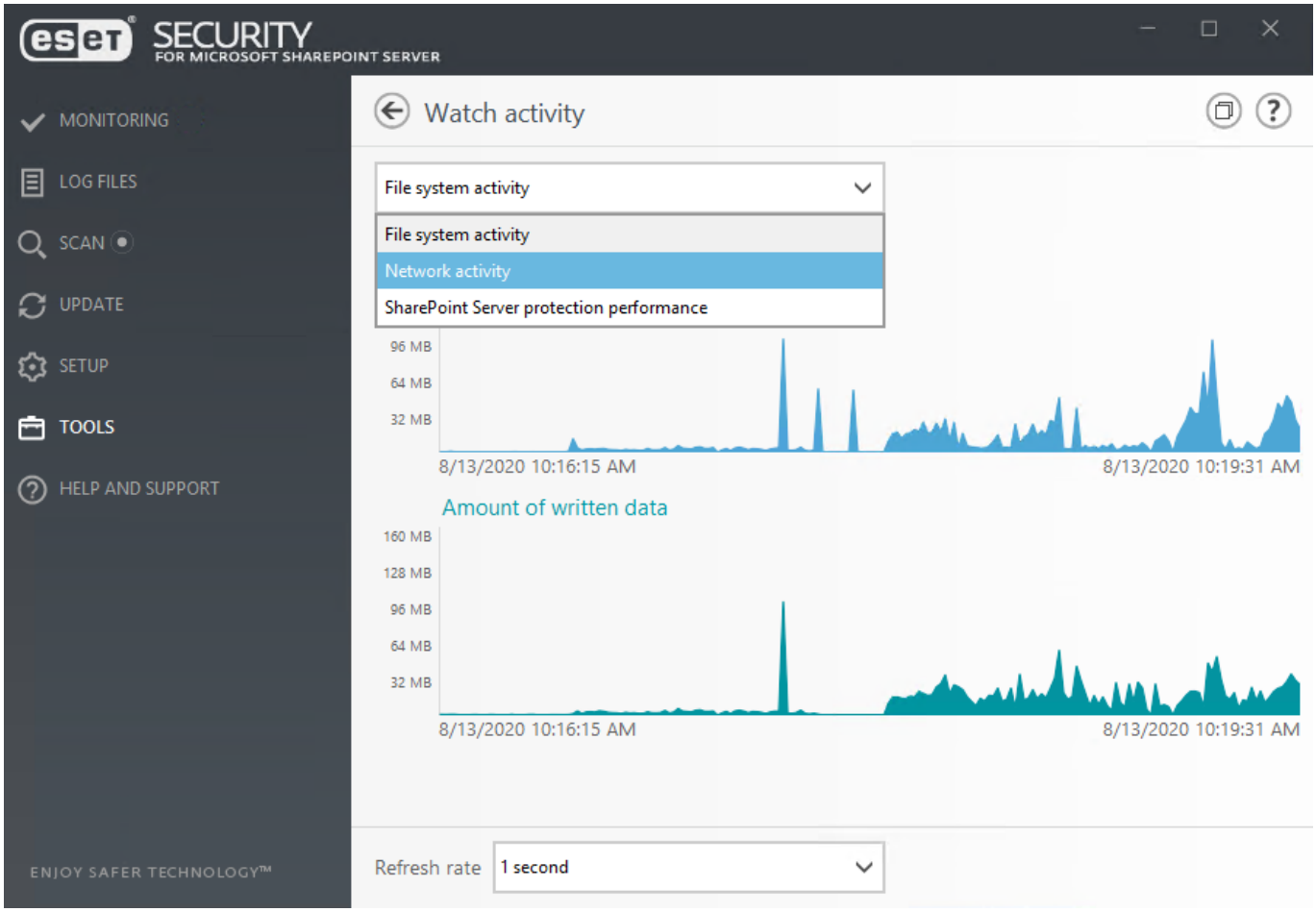
Sieťová aktivita

Zobrazuje objem prijatých a odoslaných dát. Zvislá os grafu zobrazuje množstvo prijatých dát (modrou farbou) a množstvo odoslaných dát (zelenou farbou).

Výkon ochrany SharePoint Servera

Zobrazuje aktuálny (v B/s) (modrou farbou) a priemerný (v B/s) (zelenou farbou) výkon servera.

V spodnej časti grafu je časová os zobrazujúca systémovú aktivitu v reálnom čase, obnovuje sa v nastavených intervaloch. V roletovom menu **Frekvencia obnovovania** môžete zmeniť frekvenciu aktualizácií.

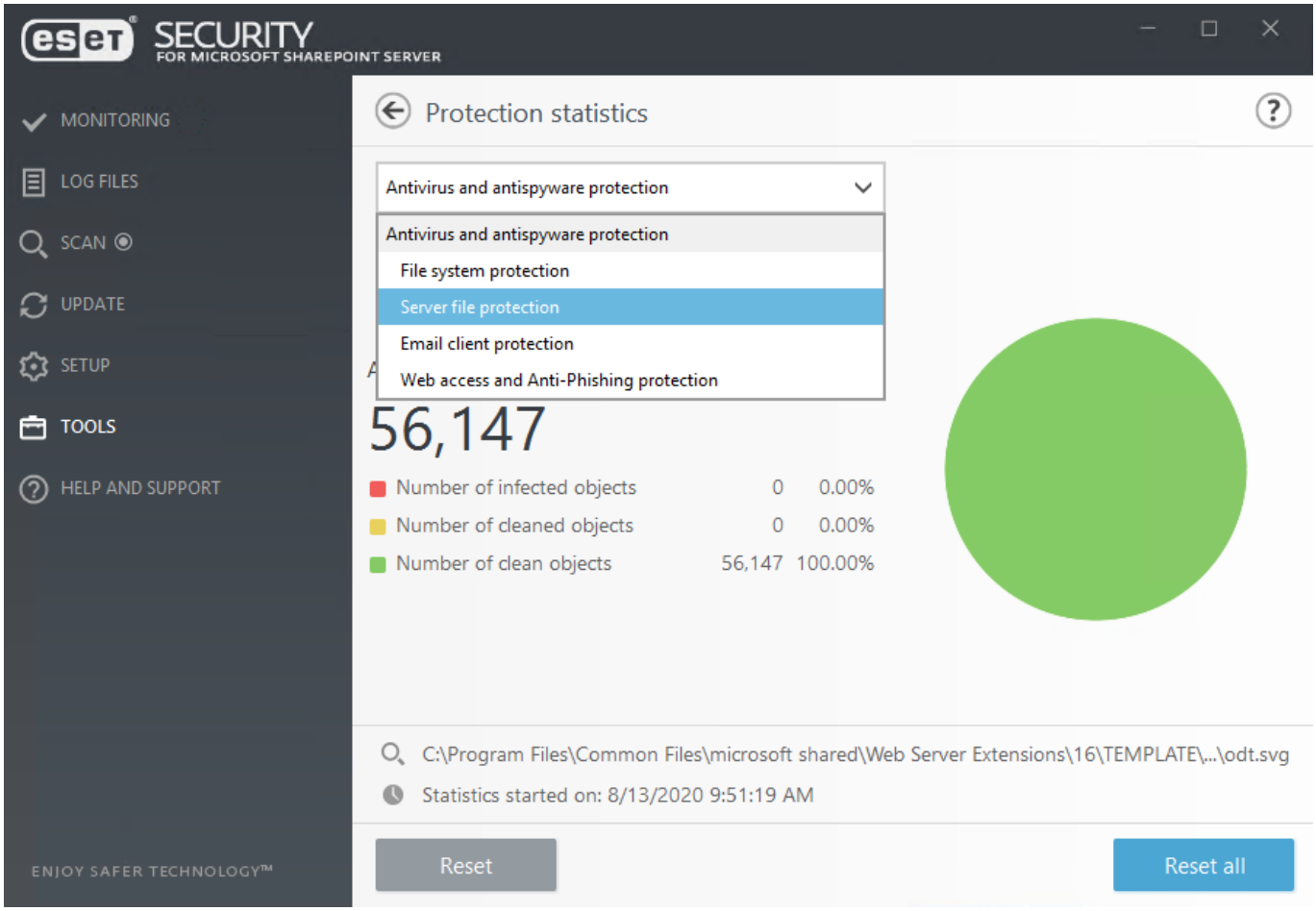


Na výber sú tieto možnosti:

1 sekunda	Graf sa obnovuje každú sekundu, časová os zobrazuje posledných 10 minút.
1 minúta (posledných 24 hodín)	Graf sa obnovuje každú minútu, časová os zobrazuje posledných 24 hodín.
1 hodina (posledný mesiac)	Graf sa obnovuje každú hodinu, časová os zobrazuje posledný mesiac.
1 hodina (vybraný mesiac)	Graf sa obnovuje každú hodinu, časová os zobrazuje zvolený mesiac. Ak chcete zobraziť aktivitu, z roletového menu vyberte mesiac (a rok). Kliknite na **Zmeniť**.

Štatistiky ochrany

Ak chcete zobraziť štatistické údaje týkajúce sa modulov ochrany produktu ESET Security for Microsoft SharePoint, vyberte príslušný modul z roletového menu. Štatistiky obsahujú informácie, ako napr. počet všetkých skontrolovaných objektov, počet infikovaných objektov, počet vyliečených objektov a počet neinfikovaných objektov. Po ponechaní kurzora na zvolenej položke umiestnenej vedľa grafu sa v danom grafe zobrazia len údaje pre konkrétnu položku. Ak chcete vynulovať štatistické údaje pre príslušný modul ochrany, kliknite na **Vynulovať**. Ak chcete vynulovať údaje pre všetky moduly, kliknite na **Vynulovať všetko**.



V ESET Security for Microsoft SharePoint sú dostupné tieto grafy:

Antivírusová a antispyvérová ochrana

Zobrazuje celkový počet infikovaných a vyliečených objektov.

Ochrana súborového systému

Zobrazuje len tie objekty, ktoré boli čítané alebo zapisované v rámci súborového systému.

Ochrana Hyper-V

Zobrazuje celkový počet infikovaných, vyliečených a neinfikovaných objektov (len na systémoch Hyper-V).

Ochrana e-mailových klientov

Zobrazuje len tie objekty, ktoré boli prijaté alebo odoslané pomocou e-mailových klientov.

Ochrana prístupu na web a antiphishingová ochrana

Zobrazuje len tie objekty, ktoré boli stiahnuté pomocou webových prehliadačov.

Serverová ochrana súborov

Zobrazuje objekty SharePoint, ktoré boli odovzdané alebo stiahnuté.

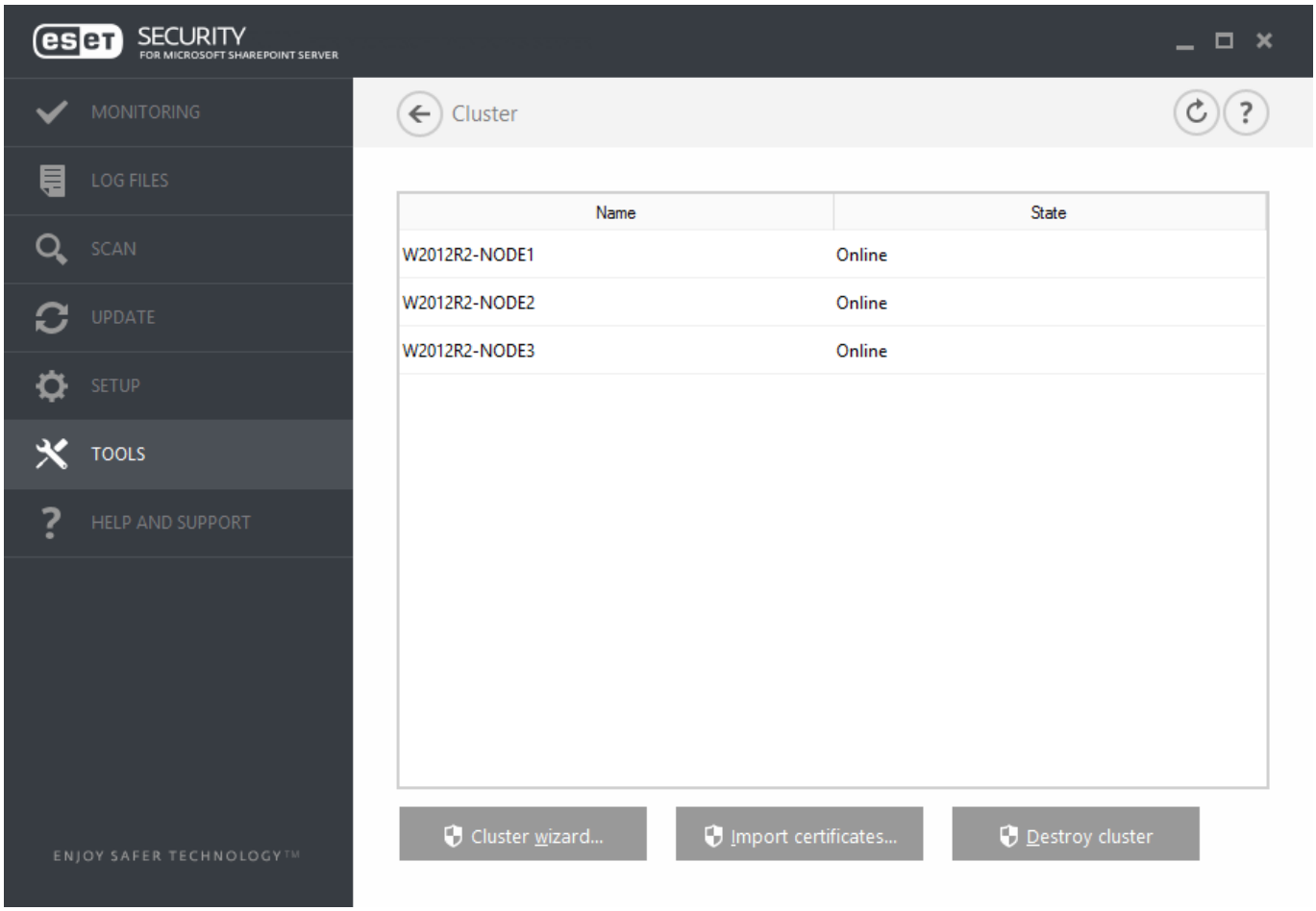
Klaster

Klaster ESET je komunikačná infraštruktúra založená na technológii Peer-to-Peer, určená pre produkty spoločnosti ESET pre servery typu Microsoft Windows Server.

Umožňuje produktom spoločnosti ESET určeným pre servery komunikovať medzi sebou a umožňuje vzájomnú výmenu synchronizačných dát, nastavení a oznámení. Okrem toho poskytuje synchronizáciu dát potrebných pre správne fungovanie skupiny inštancií produktov. Príkladom takejto skupiny je skupina uzlov v klastri Windows Failover alebo klastri Network Load Balancing (NLB) s nainštalovanými produktmi ESET, kde je potrebné používať rovnakú konfiguráciu produktu v rámci celého klastra. Klaster ESET zabezpečuje konzistenciu medzi inštanciami.

> Poznámka:
> Nastavenia používateľského rozhrania a naplánovaných úloh sa medzi uzlami klastra ESET nesynchronizujú. Toto správanie je zámerné.

Stránka stavu klastra ESET je prístupná z hlavného menu programu cez **Nástroje** > **Klaster**.



> Poznámka:
> Vytváranie klastra ESET medzi ESET Security for Microsoft SharePoint a ESET File Security pre Linux nie je podporované.

Pri nastavovaní klastra sú dostupné dva spôsoby pridania uzlov:

Autodetekcia

Ak už máte klaster Windows Failover/NLB, autodetekcia automaticky pridá jeho uzly do klastra ESET.

Vybrať

Uzly môžete pridať aj manuálne zadaním názvov serverov (z rovnakej pracovnej skupiny alebo domény).

> Poznámka:
> **Servery sa nemusia nachádzať v** klastri Windows Failover/NLB nato, aby mohli používať klaster ESET. Klastre Windows Failover a NLB nie sú vyžadované na použitie klastra ESET.

Po pridaní uzlov do klastra ESET nasleduje inštalácia produktu ESET Security for Microsoft SharePoint na každý uzol. Inštalácia prebieha automaticky počas nastavovania klastra ESET. Prihlasovacie údaje potrebné na vzdialenú inštaláciu ESET Security for Microsoft SharePoint na iné uzly:

Doména

V prípade domény zadajte údaje doménového správcu.

Pracovná skupina

V prípade pracovnej skupiny zadajte údaje lokálneho správcu a uistite sa, že daný účet existuje na všetkých uzloch.

Pri nastavovaní klastra ESET môžete použiť kombináciu oboch spôsobov pridania uzlov – automaticky pomocou klastra Windows Failover/NLB a manuálne pre počítače, ktoré sú v pracovnej skupine alebo doméne.

> Dôležité:
> Nie je možné kombinovať uzly na doméne s uzlami v pracovnej skupine.

Ďalšou požiadavkou klastra ESET je povolenie **zdieľania súborov a tlačiarní** v bráne Windows Firewall pred spustením vzdialenej inštalácie ESET Security for Microsoft SharePoint na uzloch klastra ESET.

Pridávanie nových uzlov do existujúceho klastra ESET je možné kedykoľvek pomocou Sprievodcu konfiguráciou klastra.

Import certifikátov

Ak sa používa HTTPS, certifikáty sa slúžia na overovanie komunikácie medzi jednotlivými zariadeniami. Pre každý klaster ESET existuje nezávislá hierarchia certifikátov. V rámci hierarchie existuje jeden koreňový certifikát a sada certifikátov pre jednotlivé uzly, ktoré sú podpísané koreňovým certifikátom. Súkromný kľúč koreňového certifikátu je po vytvorení certifikátov pre všetky uzly zmazaný. Ak pridáte nový uzol do klastra, vytvorí sa nová hierarchia certifikátov. Prejdite do priečinka, ktorý obsahuje certifikáty (tie, ktoré boli vygenerované počas konfigurácie klastra). Vyberte súbor certifikátu a kliknite na **OK**.

Zrušenie klastra

Klaster ESET je možné jednoducho zrušiť. Každý uzol si vytvorí záznam o zrušení klastra ESET v protokole. Taktiež sú vymazané všetky pravidlá firewallu ESET z brány Windows Firewall. Uzly budú obnovené do pôvodného stavu a môžu byť znovu použité pre iný klaster.

Sprievodca konfiguráciou klastra – výber uzlov

Prvým krokom nastavenia klastra ESET je pridanie uzlov. Môžete zvoliť možnosť **Autodetekcia** alebo manuálne vybrať uzly pomocou tlačidla **Vybrať...** Taktiež môžete zadať meno servera pomocou tlačidla **Pridať**.

Autodetekcia

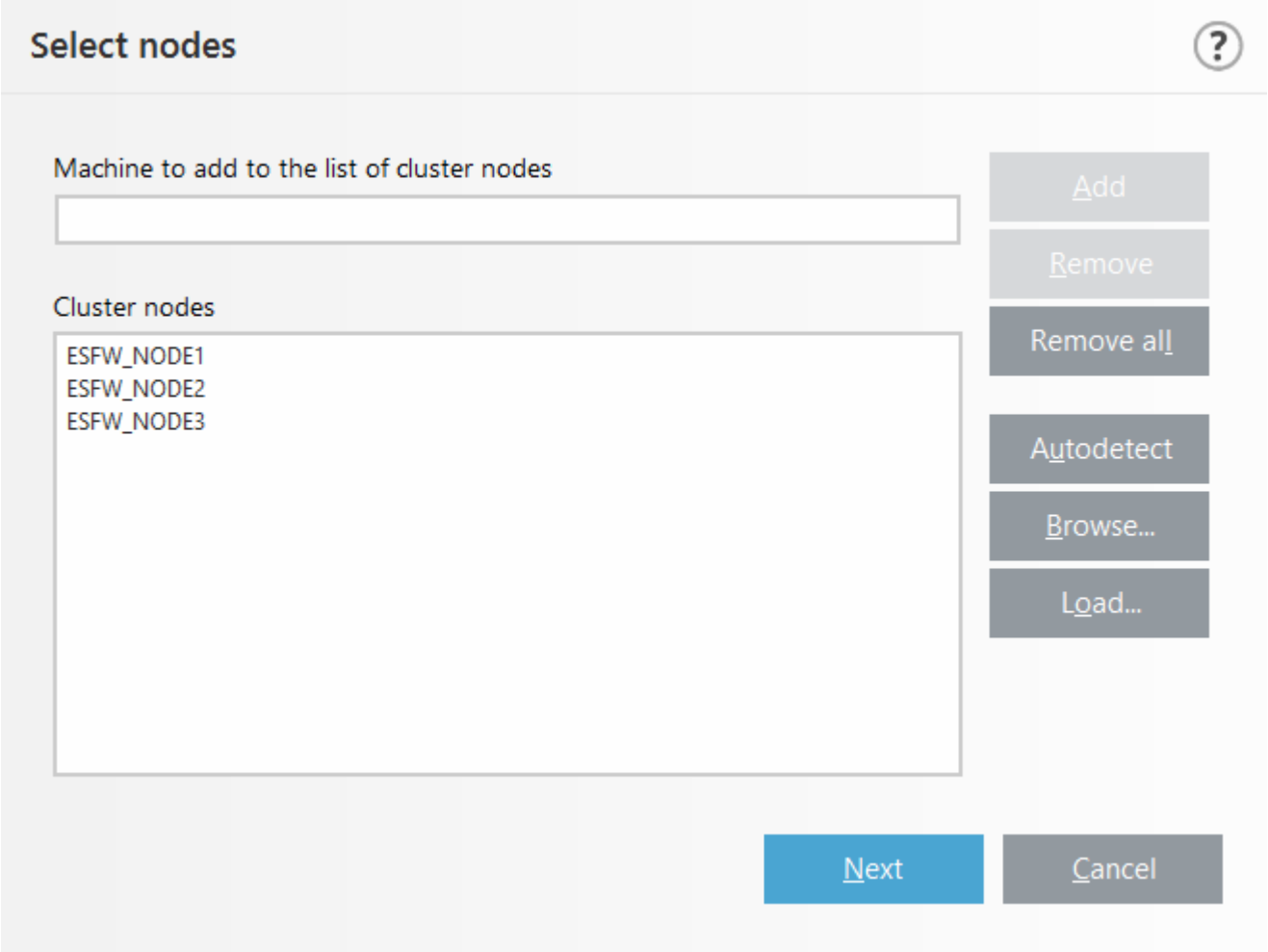
Autodetekcia automatický pridá uzly z existujúceho klastra Windows Failover Cluster/Network Load Balancing (NLB) Cluster. Server, ktorý používate na vytvorenie klastra ESET, musí byť členom daného klastra Windows Failover Cluster/NLB Cluster, aby bolo možné automatické pridanie uzlov. Pre správnu detekciu uzlov zo strany ESET Cluster musí mať NLB Cluster povolenú funkciu **Povoliť vzdialenú kontrolu**. Keď už máte zoznam novovytvorených uzlov, môžete odstrániť tie, ktoré nechcete.

Vybrať

Pomocou tejto možnosti môžete vyhľadať a pridať uzly v rámci domény (Domain) alebo pracovnej skupiny (Workgroup). Táto metóda vám umožňuje manuálne pridanie uzlov do klastra ESET. Ďalším spôsobom pridania uzlov je zadanie mena servera a kliknutie na **Pridať...**

Načítať

Táto možnosť slúži na import zoznamu uzlov zo súboru.



Pre zmenu **uzlov klastra** v zozname označte daný uzol a kliknite na **Odstrániť** alebo **Odstrániť všetko**.

Ak už máte existujúci klaster ESET, nové uzly môžete pridať kedykoľvek. Postup je rovnaký.

> Poznámka:
> Všetky uzly, ktoré ostanú v zozname, musia byť pripojené na sieť a prístupné. Localhost je predvolene pridaný do zoznamu uzlov.

Sprievodca konfiguráciou klastra – nastavenie klastra

Zadajte názov klastra a v prípade potreby podrobnosti o sieti.

Názov klastra

Zadajte názov klastra a kliknite na **Ďalej**.

Načúvací port (predvolene 9777)

Ak už vo svojom sieťovom prostredí používate port 9777, zadajte iné číslo portu.

Otvoriť port vo firewalle systému Windows

Ak povolíte túto možnosť, pre komunikáciu na definovanom porte sa vytvorí pravidlo vo firewalle systému Windows.

Sprievodca konfiguráciou klastra – nastavenia inštalácie klastra

Definujte distribúciu certifikátov a inštaláciu produktov na uzly.

Distribúcia certifikátov

- **Automatická vzdialená** – certifikáty budú inštalované automaticky.
- **Manuálna** – kliknite na **Generovať** a vyberte priečinok, kde budú uložené certifikáty. Bude vytvorený koreňový certifikát spolu s certifikátmi pre každý uzol vrátane lokálneho počítača, z ktorého konfigurujete klaster ESET. Následne môžete certifikát registrovať na lokálne zariadenie kliknutím na **Áno**.

Inštalácia produktu na ostatné uzly

- **Automatická vzdialená** – ESET Security for Microsoft SharePoint bude automaticky nainštalovaný na každý uzol (ak má ich operačný systém rovnakú architektúru).
- **Manuálna** – tento typ inštalácie slúži na manuálnu inštaláciu ESET Security for Microsoft SharePoint (napríklad pri rozdielnej architektúre operačného systému uzlov).

Doručiť licenciu k uzlom bez aktivovaného produktu

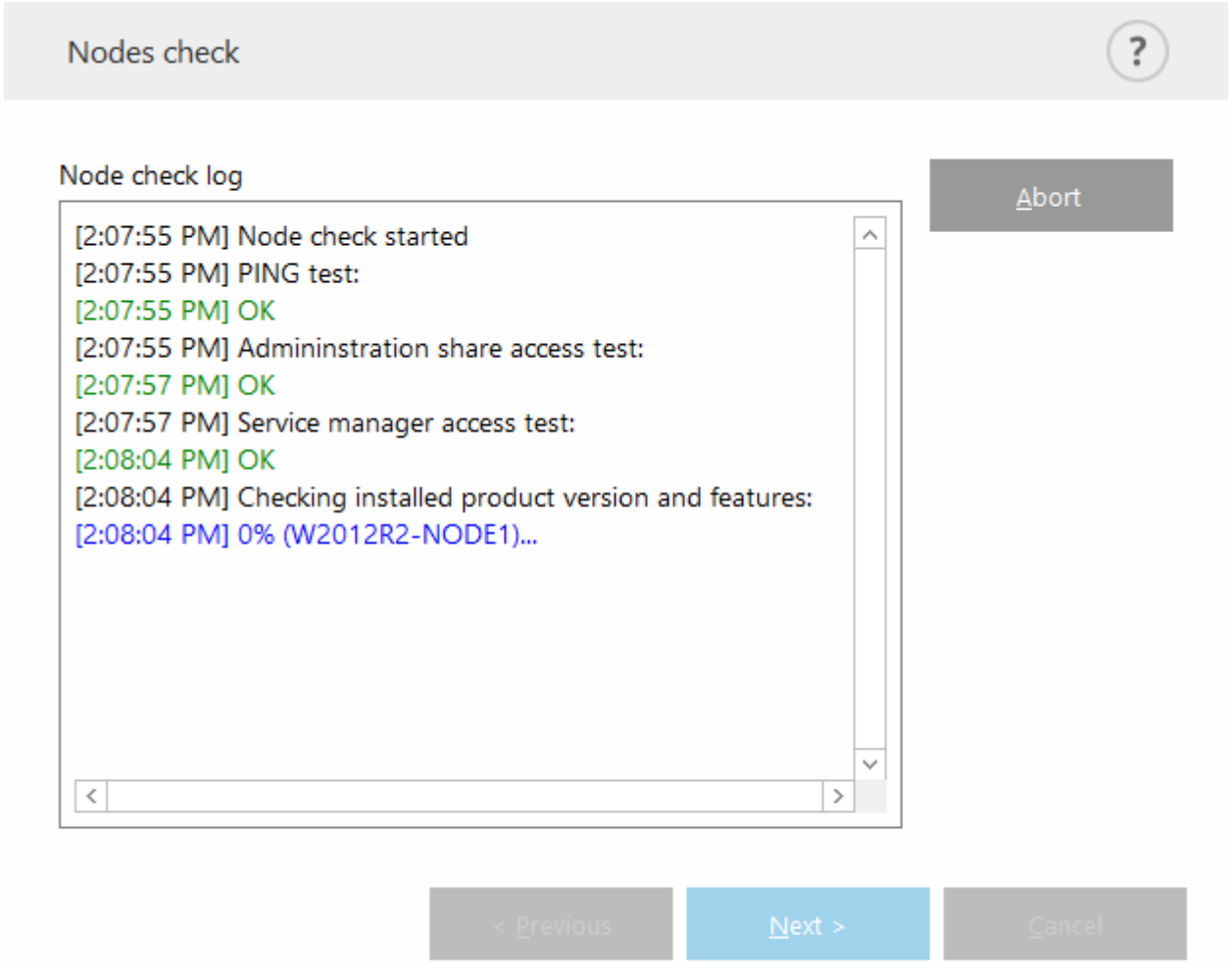
Túto možnosť je vhodné použiť v prípade, ak chcete, aby bol bezpečnostný produkt spoločnosti ESET inštalovaný na uzly klastra automaticky aktualizovaný.

Poznámka:
Ak chcete vytvoriť klaster ESET s uzlami s rozdielnou systémovou architektúrou (32 aj 64-bitový operačný systém), budete musieť nainštalovať ESET Security for Microsoft SharePoint manuálne. Architektúra operačných systémov na uzloch bude detegovaná v ďalšom kroku a vy uvidíte tieto informácie v okne protokolov.

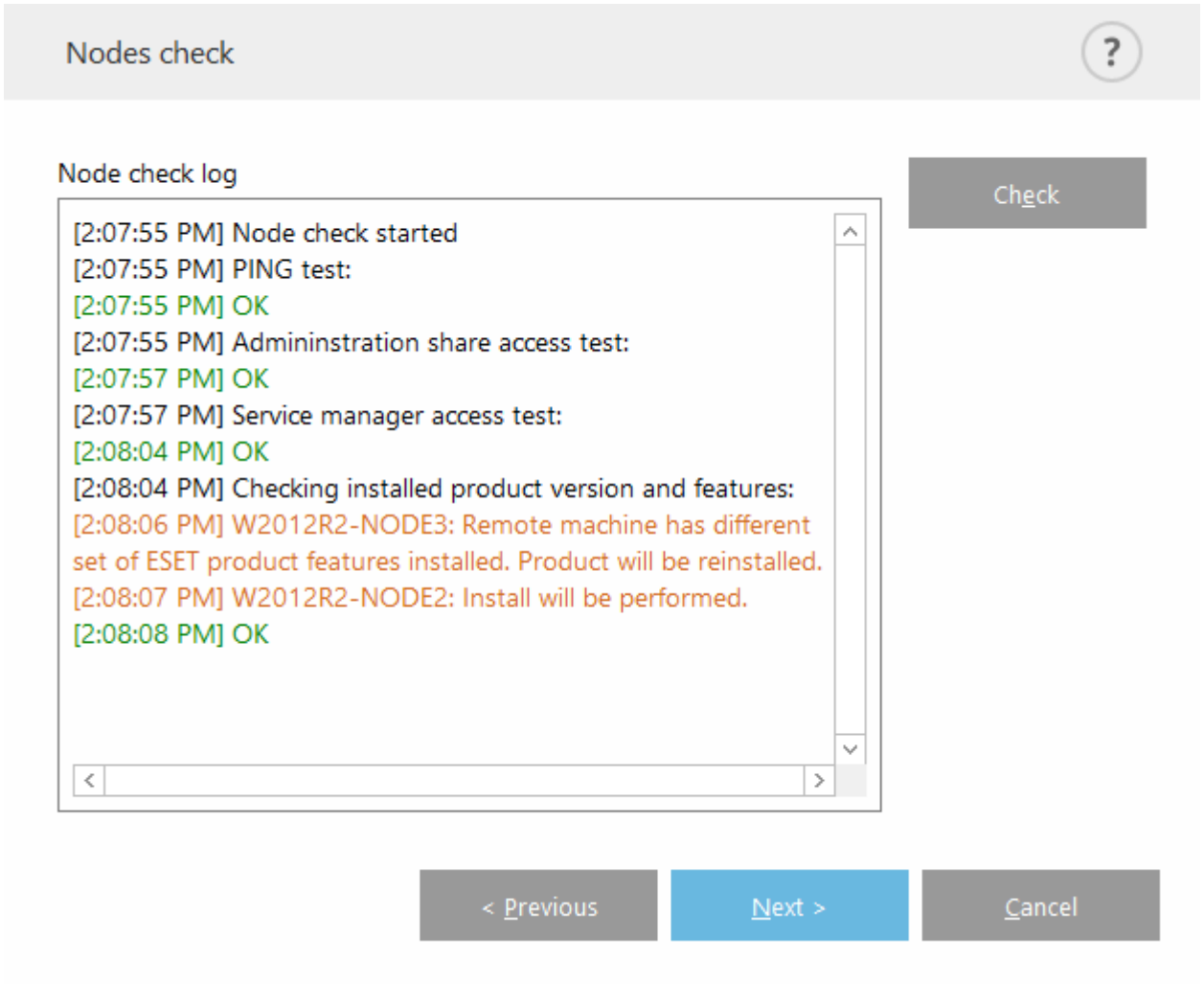
Sprievodca konfiguráciou klastra – kontrola uzlov

Po zadaní podrobností inštalácie prebehne kontrola uzlov. V **Zázname kontroly uzlov** budú zobrazené nasledujúce informácie:

- všetky existujúce uzly, ktoré sú v stave online,
- nové uzly, ktoré sú prístupné,
- uzol, ktorý je v stave online,
- správcovské zdieľané umiestnenie je prístupné,
- je možné vzdialené spustenie,
- sú nainštalované správne verzie produktu (alebo žiadny produkt),
- skontrolujte prítomnosť nových certifikátov.

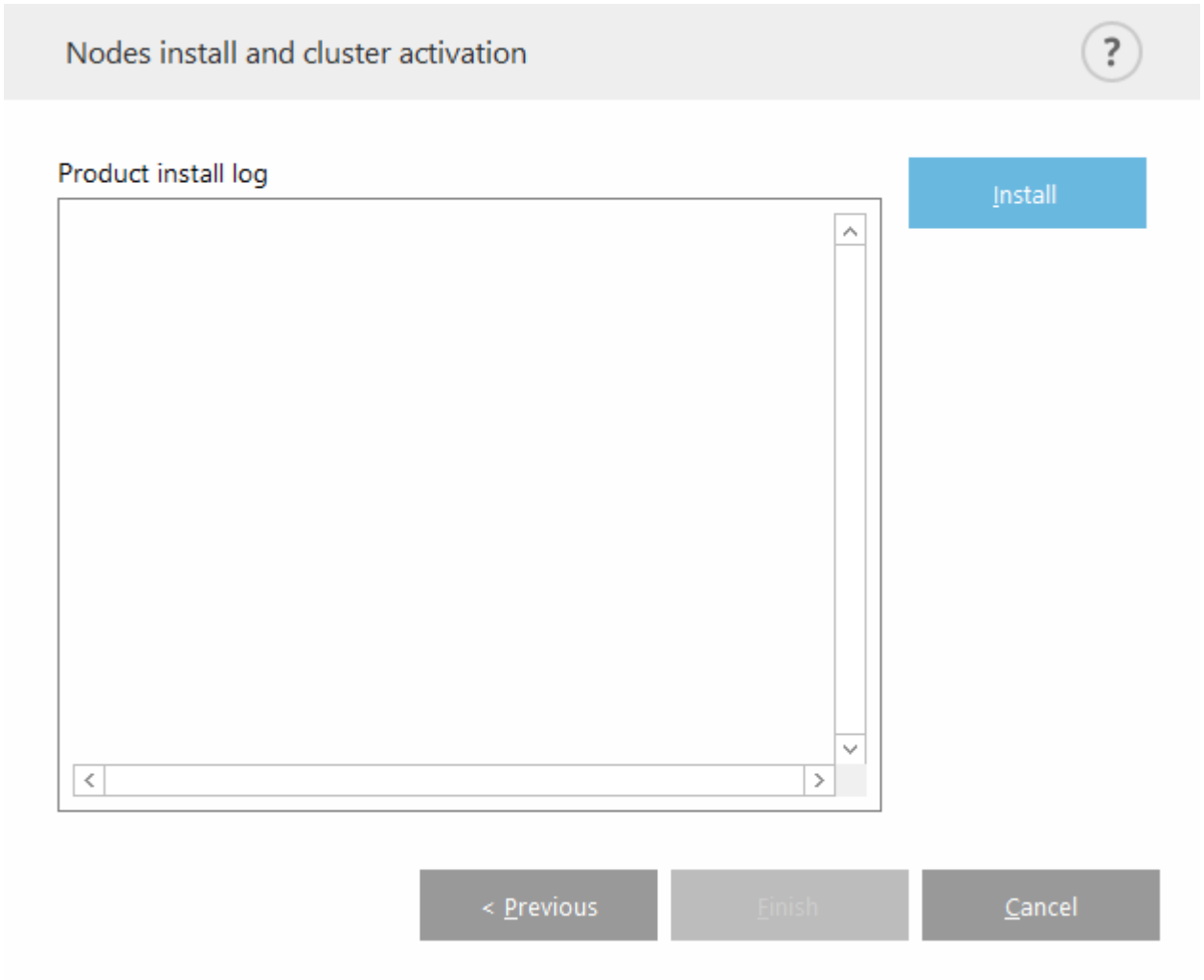


Po ukončení kontroly bude zobrazené hlásenie:

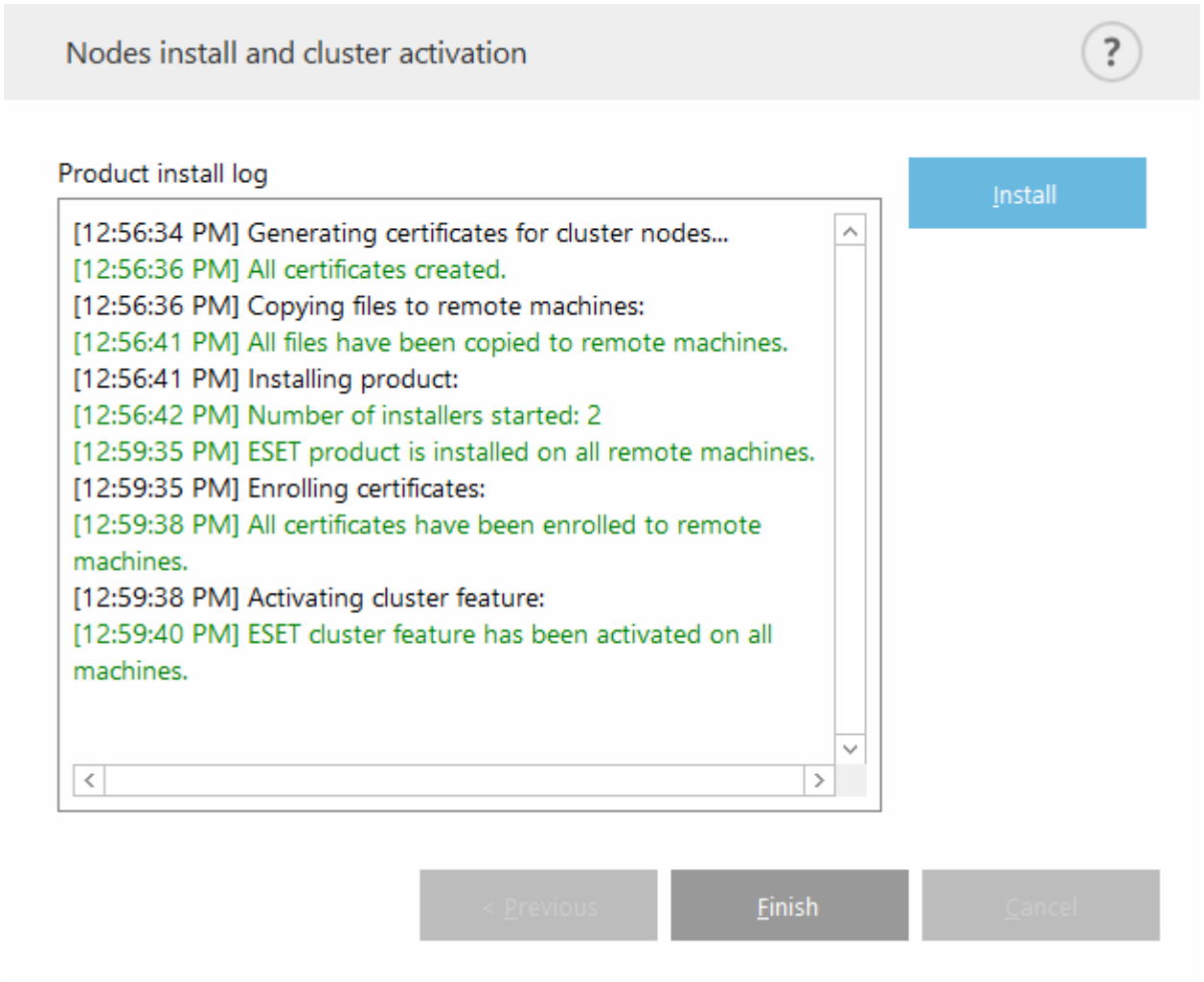


Sprievodca konfiguráciou klastra – inštalácia uzlov

Pri inštalácii produktu na vzdialené zariadenie bude v priebehu inicializácie klastra ESET inštalačný balík vyhľadávaný v adresári *%ProgramData%\ESET\ESET Security\Installer*. Ak sa inštalačný balík v danom adresári nenachádza, bude potrebné vyhľadať ho manuálne.

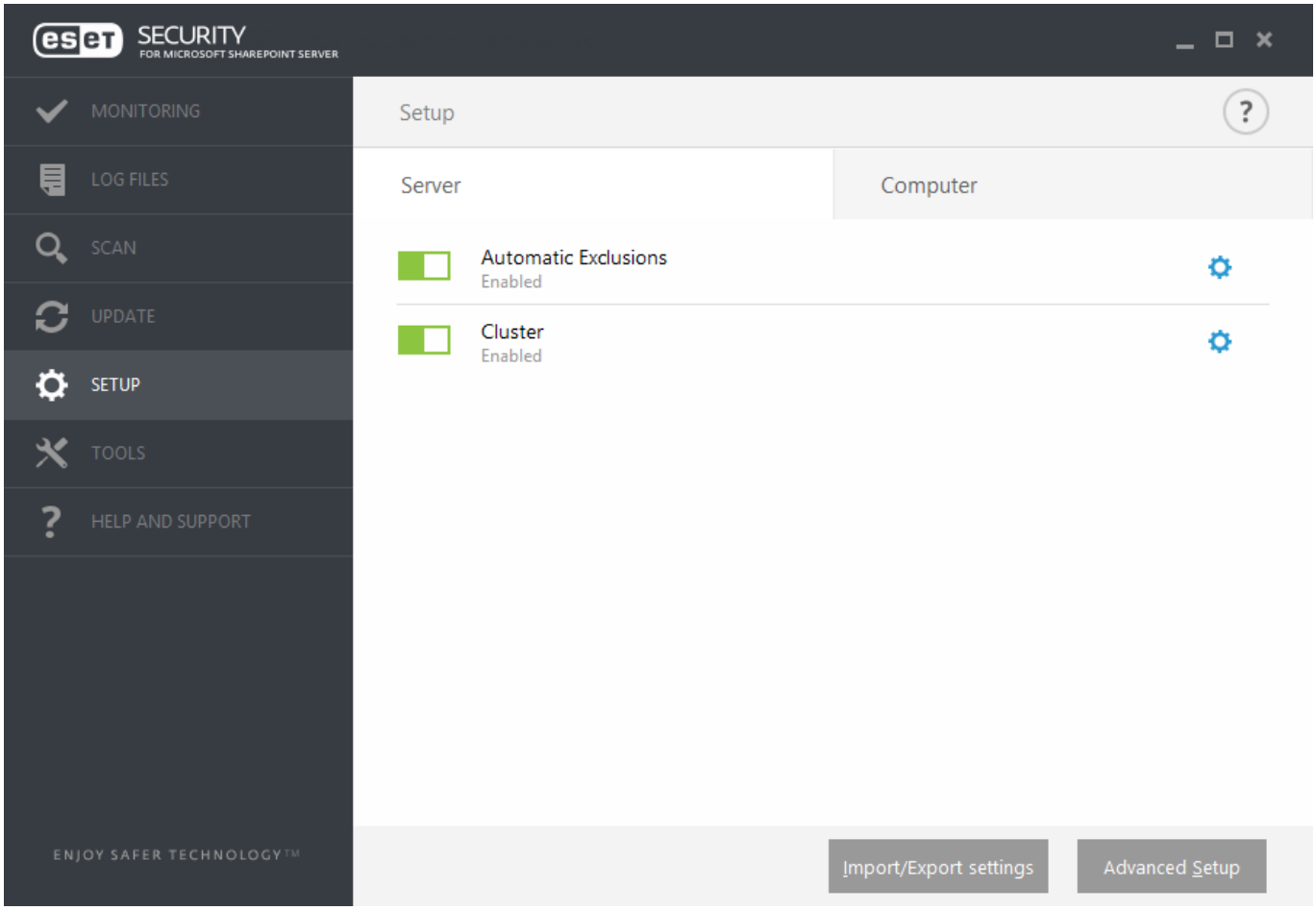


Poznámka:
Pri vzdialenej automatickej inštalácii na uzol s rozdielnou architektúrou (32-bitovým alebo 64-bitovým operačným systémom) sa zobrazí výzva na vykonanie manuálnej inštalácie.



Po správnom nastavení sa klaster ESET zobrazí v okne **Nastavenia** > **Server**.

Poznámka:
Ak je už na niektorých uzloch nainštalovaná staršia verzia ESET Security for Microsoft SharePoint, zobrazí sa oznámenie, že je na daných zariadeniach vyžadovaná najnovšia verzia. Aktualizácia produktu ESET Security for Microsoft SharePoint môže spôsobiť automatický reštart.



Aktuálny stav klastra ESET môžete zistiť pomocou hlavného menu v časti **Nástroje** > **Klaster**.

ESET Shell

eShell (skrátený tvar pre ESET Shell) je prostredie príkazového riadka pre ESET Security for Microsoft SharePoint. Je to alternatíva k grafickému používateľskému rozhraniu (GUI). eShell má všetky funkcie a možnosti, ktoré vám poskytuje GUI. eShell umožňuje konfigurovať a spravovať celý program bez použitia GUI.

Okrem všetkých funkcií a vlastností, ktoré sú dostupné cez GUI, vám taktiež poskytuje možnosť automatizácie použitím skriptov (napr. nakonfigurovanie, modifikovanie konfigurácie alebo vykonanie akcie). Taktiež, eShell môže byť užitočný pre tých, ktorí uprednostňujú príkazový riadok.

> Poznámka:
> Pre úplnú funkčnosť odporúčame spustiť nástroj eShell s možnosťou Spustiť ako správca. To isté platí pre spúšťanie jednotlivých príkazov v príkazovom riadku Windows (cmd). Spustite príkazový riadok použitím možnosti Spustiť ako správca. Ak nespustíte príkazový riadok ako správca, nebudete môcť spúšťať príkazy z dôvodu nedostatočných oprávnení.

Existujú dva režimy, v ktorých je možné eShell spustiť:

1. **Interaktívny režim** – tento režim je užitočný v prípade, keď chcete pracovať s nástrojom eShell (nie iba spustiť jeden príkaz) napríklad pri nastavovaní konfigurácie, prezeraní protokolov atď. Interaktívny režim môžete tiež použiť, ak ešte nepoznáte všetky príkazy. Interaktívny režim vám uľahčí orientáciu v nástroji eShell. Takisto vám zobrazí dostupné príkazy, ktoré môžete použiť v rámci daného kontextu.

2. **Spustenie jednotlivého príkazu/Batch režim** – môžete ho použiť, ak potrebujete len spustiť príkaz bez

vstupovania do interaktívneho režimu nástroja eShell. Stačí v príkazovom riadku Windows napísať eshell s potrebnými parametrami.

Príklad:
`eshell get status` alebo `eshell computer set real-time status disabled 1h`

Pre spustenie niektorých príkazov (napr. horeuvedené príklady) v batch/skript režime je potrebné najprv nakonfigurovať určité nastavenia. V opačnom prípade sa zobrazí hlásenie **Prístup odmietnutý**. Toto hlásenie sa zobrazí z bezpečnostných dôvodov.

Poznámka:
Pre povolenie eShell príkazov v príkazovom riadku systému Windows je potrebné vykonať zmeny v nastaveniach. Viac informácií o spúšťaní batch súborov nájdete tu.

Existujú dva spôsoby vstúpenia do interaktívneho režimu v nástroji eShell:

1. Windows **Štart menu**: Štart > Všetky programy > ESET > ESET Security pre Microsoft SharePoint Server > ESET Shell

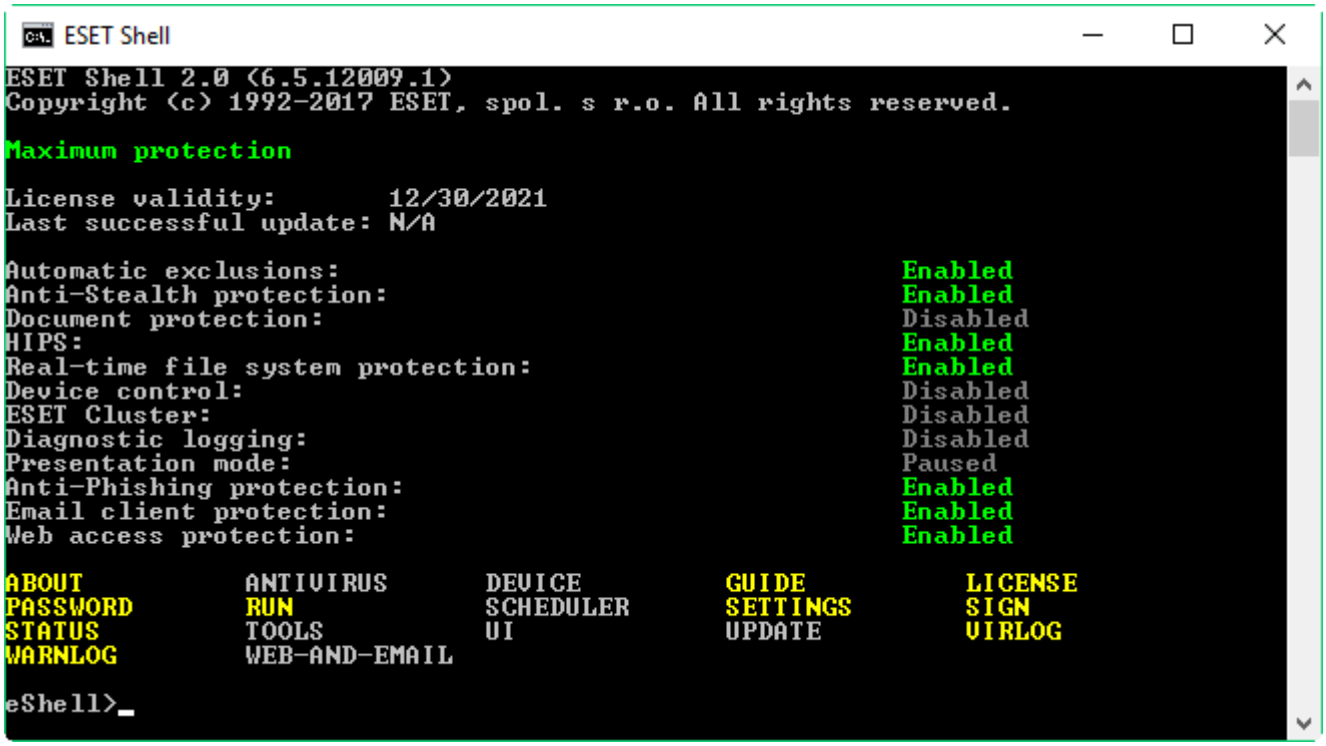
2. Pomocou **príkazového riadka Windows** napísaním `eshell` a stlačením klávesu Enter.

Dôležité:
V prípade, že sa zobrazí chybové hlásenie `'eshell' is not recognized as an internal or external command`, je to spôsobené tým, že nové premenné prostredia neboli načítané vaším systémom po inštalácii produktu ESET Security for Microsoft SharePoint. Skúste otvoriť nový príkazový riadok a spustiť eShell znova. Ak sa aj naďalej zobrazuje chybové hlásenie alebo ste pri inštalácii produktu ESET Security for Microsoft SharePoint zvolili Základnú inštaláciu, spustite nástroj eShell použitím absolútnej cesty, napr. `"%PROGRAMFILES%\ESET\ESET Security\eShell.exe"` (aby príkaz fungoval, musíte použiť úvodzovky "").

Keď spustíte eShell v interaktívnom režime po prvýkrát, zobrazí sa obrazovka (pomocníka) prvého spustenia.

Poznámka:
Ak chcete zobraziť obrazovku prvého spustenia v budúcnosti, zadajte príkaz `guide`. Ukáže vám základné príklady, ako používať eShell so syntaxou, operáciou, príkazovou cestou, skrátenými podobami, aliasmi atď.

Po začatí novej relácie eShell sa zobrazí nasledujúca obrazovka:



> Poznámka:
> Príkazy nerozlišujú veľké a malé písmená. Môžete používať veľké alebo malé písmená, nemá to vplyv na spustenie príkazu.

Prispôsobenie eShell

Nastavenie rozhrania eShell je možné z kontextu `ui eshell`. Môžete nastaviť aliasy, farby, jazyk, politiku spustenia pre skripty, zobrazovanie skrytých príkazov atď.

Použitie

Syntax

Aby príkazy mohli správne fungovať, musia mať správnu syntax a môžu sa skladať z operácie (prefix), kontextu, argumentov, možností atď. Toto je všeobecná syntax používaná v rámci celého nástroja eShell:

[<prefix>] [<command path>] <command> [<arguments>]

Príklad (tento príkaz aktivuje ochranu dokumentov):

```
SET COMPUTER SCANS DOCUMENT REGISTER ENABLED
```

`SET` – operácia (prefix)
`COMPUTER SCANS DOCUMENT` – cesta k danému príkazu, kontext v ktorom sa príkaz nachádza
`REGISTER` – samotný príkaz
`ENABLED` – argument pre daný príkaz

Použitím argumentu `?` sa zobrazí syntax pre daný príkaz. Napríklad, `STATUS ?` zobrazí syntax pre príkaz `STATUS`:

SYNTAX:

```
[get] status
```

OPERÁCIE:

`get` – zobraziť stav všetkých modulov ochrany

Môžete si všimnúť, že `[get]` je v zátvorkách. To znamená, že `get` je predvolená operácia pre príkaz `status`. Ďalej to znamená, že ak spustíte príkaz `status` bez zadania operácie, použije sa predvolená operácia (v tomto prípade `get status`). Použitím príkazov bez operácie dokážete ušetriť čas pri písaní. Zvyčajne je `get` predvolenou operáciou pre väčšinu príkazov, avšak je lepšie sa uistiť, aká je predvolená operácia pre konkrétny príkaz, aby ste mali istotu, aký úkon sa vykoná.

> Poznámka:
> Príkazy nerozlišujú veľké a malé písmená. Môžete používať veľké alebo malé písmená, nemá to vplyv na spustenie príkazu.

Operácia/prefix

Operácia alebo tzv. predpona (prefix) určuje, akú operáciu ma príkaz vykonať. Operácia `GET` vám poskytne informácie o tom, ako je určitá funkcia programu ESET Security for Microsoft SharePoint nakonfigurovaná, prípadne ukáže stav (napr. `GET COMPUTER REAL-TIME STATUS` vám ukáže momentálny stav Rezidentnej ochrany). Operácia `SET` nakonfiguruje funkciu alebo zmení jej stav (`SET COMPUTER REAL-TIME STATUS ENABLED` aktivuje Rezidentnú ochranu).

Toto sú operácie, ktoré môžete v nástroji eShell použiť. Príkaz môže alebo nemusí podporovať niektoré z týchto operácií:

GET	vráti aktuálne nastavenie/stav
SET	nastaví hodnotu/stav
SELECT	zvolí položku
ADD	pridá položku
REMOVE	odstráni položku
CLEAR	odstráni všetky položky/súbory
START	spustí akciu
STOP	úplne zastaví akciu
PAUSE	pozastaví akciu
RESUME	obnoví priebeh pozastavenej akcie
RESTORE	obnoví pôvodné nastavenia/objekt/súbor
SEND	odošle objekt/súbor
IMPORT	importuje zo súboru
EXPORT	exportuje do súboru

> Poznámka:
> Operácie ako `GET` a `SET` sa používajú s veľkým množstvom príkazov, avšak niektoré príkazy (napr. `EXIT`) nepoužívajú operáciu.

Cesta príkazu/kontext

Príkazy sú umiestnené do kontextov, ktoré tvoria stromovú štruktúru. Vrchná úroveň stromu je koreň (root). Po spustení eShell budete na úrovni koreňa (root):

```
eShell>
```

Príkaz môžete vykonať priamo odtiaľto alebo môžete vstúpiť do potrebného kontextu zadaním názvu kontextu. Týmto spôsobom sa pohybujete v rámci stromovej štruktúry. Napríklad pri použití kontextu `TOOLS` sa zobrazia všetky príkazy a podkontexty, ktoré sú k dispozícii z daného miesta.



Žlté položky sú príkazy, ktoré môžete vykonať a sivé položky sú podkontexty, do ktorých môžete vojsť. Podkontext obsahuje ďalšie príkazy.

Ak sa potrebujete vrátiť späť na vyššiu úroveň, použite `..` (dve bodky).

> Príklad:
> Napríklad, ak sa nachádzate tu:
> `eShell computer real-time>`
> napíšte `..` pre presunutie o úroveň vyššie na:
> `eShell computer>`

Ak sa chcete vrátiť späť na úroveň koreňa (root) z `eShell computer real-time>` (podkontext, ktorý je o dve úrovne nižšie ako koreň), jednoducho napíšte `.. ..` (dve bodky a dve bodky oddelené medzerou). Keď to urobíte, dostanete sa o dve úrovne vyššie, v tomto prípade na úroveň koreňa. Použitím spätnej lomky `\` sa vrátite priamo na úroveň koreňa (root) bez ohľadu na to, ako hlboko v kontextovom strome sa nachádzate. Ak sa chcete dostať do konkrétneho kontextu na vyššej úrovni, použite zodpovedajúci počet `..` v príkaze, aby ste sa dostali na želanú úroveň, pričom použite medzeru ako oddeľovač. Napríklad, ak sa chcete dostať o tri úrovne vyššie, použite `.. .. ..`

Cesta je relatívna k momentálnemu kontextu. Ak je príkaz obsiahnutý v momentálnom kontexte, cestu nevkladajte. Napríklad, pre spustenie `GET COMPUTER REAL-TIME STATUS` zadajte:

`GET COMPUTER STATUS` – ak sa nachádzate v koreňovom kontexte (príkazový riadok zobrazuje `eShell>`)
`GET STATUS` – ak ste v kontexte `COMPUTER` (príkazový riadok zobrazuje `eShell computer>`)

`.. GET STATUS` – ak ste v kontexte `COMPUTER REAL-TIME` (príkazový riadok zobrazuje `eShell computer real-time>`)

Môžete použiť jednu bodku `.` miesto dvoch bodiek `..`, pretože jedna bodka je skratka dvoch bodiek.

Príklad:
`. GET STATUS` – ak ste v kontexte `COMPUTER REAL-TIME` (príkazový riadok zobrazuje `eShell computer real-time>`)

Argument

Argument je akcia, ktorá je vykonaná pre určitý príkaz. Napríklad, príkaz `CLEAN-LEVEL` (umiestnený v `COMPUTER REAL-TIME ENGINE`) môže byť použitý s nasledujúcimi argumentmi:

`rigorous` – vždy vyriešiť detekciu
`safe` – vyriešiť detekciu a ak to nie je možné, ponechať ju
`normal` – vyriešiť detekciu a ak to nie je možné, spýtať sa
`none` – vždy sa spýtať koncového používateľa

Ďalším príkladom sú argumenty `ENABLED` alebo `DISABLED`, ktoré sa používajú na povolenie alebo zakázanie určitej funkcie.

Skrátená forma príkazov

eShell vám umožňuje skracovať kontexty, príkazy a argumenty (za predpokladu, že argument je prepínač alebo alternatívna možnosť). Nie je možné skrátiť operáciu (prefix) alebo argument, ktorý je konkrétnou hodnotou, ako napr. číslo, názov alebo cesta. Môžete použiť čísla `1` a `0` namiesto argumentov enabled a disabled.

Príklad:
```
computer set real-time status enabled    =>   com set real stat 1
computer set real-time status disabled    =>   com set real stat 0
```

Príklady skrátenej formy:

Príklad:
```
computer set real-time status enabled    =>   com set real stat en
computer exclusions add detection-excludes object C:\path\file.ext    =>   com
excl add det obj C:\path\file.ext
computer exclusions remove detection-excludes 1    =>   com excl rem det 1
```

V prípade, že dva príkazy alebo kontexty začínajú rovnakým písmenom, napríklad `ADVANCED` a `AUTO-EXCLUSIONS`, a vy zadáte `A` ako skrátenú podobu kontextu, eShell nebude schopný rozhodnúť, do ktorého z dvoch kontextov chcete prejsť. Preto zobrazí chybovú správu a zoznam príkazov začínajúcich na „A“, z ktorých si môžete vybrať:

```
eShell>a

The following command is not unique: a
```

V kontexte `COMPUTER` sú dostupné nasledujúce podkontexty:

```
ADVANCED

AUTO-EXCLUSIONS
```

Po pridaní jedného alebo viacerých písmen (napr. `AD` namiesto `A`) eShell prejde do podkontextu `ADVANCED`, ktorý je už pri tomto zadaní jedinečný. To isté platí pre skrátené príkazy.

> Poznámka:
> Keď si chcete byť istý, že sa príkaz vykoná ako potrebujete, potom neodporúčame skracovať príkazy, argumenty atď., ale používať úplnú formu. Týmto spôsobom eShell vykoná presne to, čo potrebujete, a predídete tak nežiaducim chybám. Toto obzvlášť platí pre dávkové súbory (batch files)/skripty.

Automatické dopĺňanie

Táto nová funkcia bola predstavená v nástroji eShell 2.0 a je do veľkej miery podobná automatickému dopĺňaniu v príkazovom riadku systému Windows. Príkazový riadok systému Windows dopĺňa len cesty k súborom, eShell dopĺňa aj príkaz, kontext a názov operácie. Dokončovanie argumentov nie je podporované. Pri zadávaní príkazu stláčajte kláves TAB pre zobrazenie dostupných príkazov. Môžete tiež stlačiť klávesy SHIFT a TAB pre vrátenie predošlého zobrazenia. Miešanie zjednodušených podôb a automatického dopĺňania nie je podporované. Použite buď jedno, alebo druhé. Napríklad, ak zadáte reťazec `computer real-time additional` a stlačíte kláves TAB, nič sa nestane. Ak však zadáte len `com` a stlačíte kláves TAB, zadaný príkaz sa doplní na tvar `computer`. Potom môžete pokračovať napísaním `real`, stlačiť kláves TAB, napísať `add`, znova stlačiť TAB a napokon stlačiť Enter. Zadajte `on`, stlačte Tab a každým ďalším stlačením klávesu Tab prejdite všetkými dostupnými variáciami: `on-execute-ah`, `on-execute-ah-removable`, `on-write-ah`, `on-write-archive-default` atď.

Aliasy

Alias je alternatívny názov, ktorý môže byť použitý na vykonanie príkazu (za predpokladu, že príkaz má priradený alias). Je dostupných niekoľko predvolených aliasov:

`(global) close` – koniec
`(global) quit` – koniec
`(global) bye` – koniec
`warnlog` – protokol udalostí
`virlog` – protokol detekcií

„(global)“ znamená, že príkaz môže byť použitý kdekoľvek, bez ohľadu na kontext. Jeden príkaz môže mať pridelené viaceré aliasy, napríklad príkaz `EXIT` má aliasy `CLOSE`, `QUIT` a `BYE`. Ak chcete zatvoriť eShell, môžete použiť samotný príkaz `EXIT` alebo ktorýkoľvek jeho alias. Alias `VIRLOG` je alias pre príkaz `DETECTIONS`, ktorý sa nachádza v `TOOLS LOG` kontexte. Týmto spôsobom je príkaz dostupný z kontextu `ROOT` a tým pádom je ľahšie prístupný (nemusíte prejsť do kontextu `TOOLS` a následne do podkontextu `LOG`, ale spustíte ho priamo z kontextu `ROOT`).

eShell vám umožňuje definovať vaše vlastné aliasy. Príkaz `ALIAS` je možné nájsť v `UI ESHELL` kontexte.

Ochrana nastavení heslom

ESET Security for Microsoft SharePoint nastavenia môžu byť ochránené heslom. Heslo môžete nastaviť pomocou grafického rozhrania (GUI) alebo použitím nástroja eShell pomocou príkazu `set ui access lock-password`. Toto heslo budete musieť zadať pre niektoré príkazy (napríklad pri zmene nastavení alebo zmene údajov). Ak plánujete pracovať s nástrojom eShell dlhší čas a nechcete opakovane zadávať heslo, môžete eShell nastaviť tak, aby si heslo zapamätal. Využijete na to príkaz `set password` (spustením z `root`). Heslo bude potom automaticky vyplnené pre všetky ďalšie príkazy, ktoré vyžadujú heslo. eShell si heslo zapamätá do chvíle, keď ho

ukončíte. To znamená, že pri začatí novej relácie eShell bude nutné znova použiť príkaz `set password` na zapamätanie hesla.

Sprievodca/pomocník

Po spustení príkazu `GUIDE` alebo `HELP` sa zobrazí obrazovka prvého spustenia s vysvetlením, ako používať nástroj eShell. Tento príkaz je dostupný iba z kontextu `ROOT` (`eShell>`).

História príkazov

eShell uchováva históriu predchádzajúcich vykonaných príkazov. Toto platí len pre momentálnu interaktívnu reláciu eShell. Po ukončení nástroja eShell sa história príkazov zruší. Použite klávesy na klávesnici so šípkami hore a dole pre navigáciu v histórii. Keď nájdete hľadaný príkaz, môžete ho opäť spustiť, prípadne upraviť bez toho, aby ste museli celý príkaz písať odznova.

CLS/vymazať obrazovku

Príkaz `CLS` môže byť použitý na vymazanie obrazovky. Funguje rovnako ako v príkazovom riadku Windows alebo v podobných rozhraniach príkazového riadka.

EXIT/CLOSE/QUIT/BYE

Na zatvorenie alebo ukončenie nástroja eShell môžete použiť ktorýkoľvek z nasledujúcich príkazov: `EXITCLOSE`, `QUIT` alebo`BYE`.

Príkazy

Táto sekcia obsahuje zoznam niektorých základných príkazov nástroja eShell s popismi.

> Poznámka:
> Príkazy nerozlišujú veľké a malé písmená. Môžete používať veľké alebo malé písmená, nemá to vplyv na spustenie príkazu.

Príklady príkazov (nachádzajú sa v koreňovom kontexte ROOT):

ABOUT

Zobrazí informáciu o programe. Zobrazené sú napr. nasledujúce informácie:

- Názov vášho nainštalovaného bezpečnostného produktu ESET a jeho verzia.
- Operačný systém a základné podrobnosti o hardvéri.
- Prihlasovacie meno (vrátane domény), úplný názov počítača (FQDN, ak sa váš server nachádza v doméne) a názov jednotky.
- Nainštalované súčasti vášho bezpečnostného produktu ESET vrátane verzie každej súčasti.

KONTEXT:

```
root
```

PASSWORD

Na spustenie príkazov chránených heslom by ste za normálnych okolností potrebovali zadať toto heslo. Týka sa to napríklad príkazov na vypnutie ochrany a príkazov, ktoré môžu ovplyvniť chod alebo funkcie produktu ESET Security for Microsoft SharePoint. Pri každom spustení takéhoto príkazu budete vyzvaný na zadanie hesla. Toto heslo môžete definovať, aby ste ho nemuseli vždy zadávať. eShell si heslo zapamätá a v prípade potreby bude automaticky zadané na príslušné miesto.

> Poznámka:
> Heslo platí vždy len pre aktuálnu reláciu nástroja eShell. Po ukončení relácie eShell je heslo zabudnuté. Po začatí novej relácie eShell je potrebné heslo znova definovať.

Definované heslo môže byť tiež použité pri spúšťaní nepodpísaných batch súborov alebo skriptov. Uistite sa, že pri spúšťaní nepodpísaných batch súborov je politika spustenia ESET Shell nastavená na Úplný prístup. Príklad takéhoto batch súboru:

```
eshell set password plain <yourpassword> "&" computer set real-time status disabled
```

Takýto zreťazený príkaz definuje heslo a vypína ochranu.

> Dôležité:
> Odporúčame vám používať podpísane batch súbory vždy, keď je to možné. Týmto sa vyhnete tomu, že budete mať heslá v podobe obyčajného textu v batch súbore (pri použití metódy popísanej vyššie). Viac informácií nájdete v časti Batch súbory/skriptovanie (sekcia Podpísané batch súbory).

KONTEXT:

```
root
```

SYNTAX:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERÁCIE:

- `get` – zobrazí heslo
- `set` – nastaví alebo zmaže heslo
- `restore` – zruší heslo

ARGUMENTY:

- `plain` – zadanie hesla ako parametra
- `password` – heslo

PRÍKLADY:

- `set password plain <yourpassword>` – nastaví heslo, ktoré sa automaticky použije pri spúšťaní príkazov chránených heslom
- `restore password` – zruší heslo

PRÍKLADY:

`get password` – tento príkaz použite na zistenie, či je nastavené heslo (tento príkaz zobrazí heslo ako ******, nezobrazí vám samotné heslo). Ak sa nezobrazia hviezdičky, nie je nastavené žiadne heslo.

`set password plain <vaseheslo>` – tento príkaz použite na definovanie hesla

`restore password` – tento príkaz použite na zrušenie definovaného hesla

STATUS

Zobrazuje informácie o aktuálnom stave rezidentnej ochrany ESET Security for Microsoft SharePoint a taktiež vám umožňuje pozastaviť/obnoviť ochranu (podobne ako cez používateľské rozhranie).

KONTEXT:

```
computer real-time
```

SYNTAX:

```
[get] status

set status enabled | disabled  [ 10m | 30m | 1h | 4h | temporary ]

restore status
```

OPERÁCIE:

`get` – vráti aktuálne nastavenie/stav

`set` – nastaví hodnotu/stav

`restore` – obnoví pôvodné nastavenia/objekt/súbor

ARGUMENTY:

`enabled` – zapne ochranu/funkciu

`disabled` – vypne ochranu/funkciu

`10m` – vypne na 10 minút

`30m` – vypne na 30 minút

`1h` – vypne na 1 hodinu

`4h` – vypne na 4 hodiny

`temporary` – vypne do reštartu

> Poznámka:
> Nie je možné vypnúť všetky funkcie ochrany jediným príkazom. Funkcie a moduly ochrany môžete spravovať po jednom pomocou príkazu `status`. Každá funkcia alebo modul ochrany má vlastný príkaz `status`.

Zoznam funkcií s príkazom `status`:

Funkcia	Kontext a príkaz
Automatické vylúčenia	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Rezidentná ochrana súborového systému	`COMPUTER REAL-TIME STATUS`
Správa zariadení	`DEVICE STATUS`
Ochrana pred botnetmi	`NETWORK ADVANCED STATUS-BOTNET`
Ochrana pred sieťovými útokmi (IDS)	`NETWORK ADVANCED STATUS-IDS`
Izolácia od siete	`NETWORK ADVANCED STATUS-ISOLATION`
Klaster ESET	`TOOLS CLUSTER STATUS`
Diagnostické zapisovanie do protokolu	`TOOLS DIAGNOSTICS STATUS`
Prezentačný režim	`TOOLS PRESENTATION STATUS`
Antiphishingová ochrana	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Ochrana e-mailových klientov	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Ochrana prístupu na web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Ide o alias k príkazu `DETECTIONS`. Je užitočný v prípade, že si želáte zobraziť informácie o nájdených infiltráciách.

WARNLOG

Ide o alias k príkazu `EVENTS`. Je užitočný v prípade, že si želáte zobraziť informácie o rôznych udalostiach.

Batch súbory/skriptovanie

eShell je efektívny nástroj na vytváranie skriptov a automatizácie. Ak chcete použiť batch súbor v nástroji eShell, vytvorte takýto súbor pomocou nástroja eShell a zadávajte v ňom príkazy.

> Príklad:
> `eshell get computer real-time status`

Niekedy je potrebné príkazy používať reťazovo. Napríklad, ak chcete zistiť typ naplánovanej úlohy, zadajte príkaz:

```
eshell select scheduler task 4 "&" get scheduler action
```

Výber položky (v tomto prípade úloha č. 4) sa aplikuje len na práve spustenú inštanciu nástroja eShell. Ak by ste chceli tieto dva príkazy spustiť jeden po druhom, druhý príkaz by zlyhal so správou „Nebola zvolená žiadna úloha alebo zvolená úloha už neexistuje“.

Z bezpečnostných dôvodov je pri spúšťaní súborov nastavená politika **Obmedzené skriptovanie**. To vám umožňuje používať eShell ako nástroj na monitorovanie, pričom nebudú umožnené zmeny nastavení ESET Security for Microsoft SharePoint pomocou skriptu. Príkazy, ktoré ovplyvňujú bezpečnosť, ako napr. vypnutie ochrany, budú zamietnuté so správou **Prístup odmietnutý**. Odporúčame, aby ste používali podpísané batch súbory na spúšťanie príkazov, ktoré vykonávajú zmeny v nastaveniach.

Ak chcete vykonávať zmeny v konfigurácii manuálnym zadaním jediného príkazu v príkazovom riadku systému Windows, musíte umožniť nástroju eShell úplný prístup (neodporúča sa). Pre umožnenie úplného prístupu použite príkaz `ui eshell shell-execution-policy` v interaktívnom režime samotného nástroja eShell alebo použite grafické používateľské rozhranie a prejdite do časti **Rozšírené nastavenia** (**F5**) > **Používateľské rozhranie** >

ESET Shell.

Podpísané batch súbory

eShell umožňuje zabezpečenie bežných batch (*.bat) súborov podpisom. Skripty sú podpísané rovnakým heslom aké je použité na ochranu nastavení. Aby bolo možné podpísať skript, je potrebné najprv povoliť ochranu nastavení heslom. Môžete to vykonať pomocou grafického používateľského rozhrania alebo v rámci nástroja eShell pomocou príkazu `set ui access lock-password`. Po vytvorení hesla môžete začať podpisovať batch súbory.

> Poznámka:
> Ak zmeníte heslo pre ochranu prístupu k nastaveniam, budete musieť podpísať všetky skripty znova. V opačnom prípade sa po zmene hesla skripty nebudú môcť spustiť správne. Heslo zadané pri podpisovaní skriptu musí byť zhodné s heslom ochrany prístupu k nastaveniam.

Ak chcete podpísať batch súbor, spustite príkaz `sign <script.bat>` z koreňového kontextu eShell, kde *script.bat* je cesta k skriptu, ktorý chcete podpísať. Zadajte a potvrďte heslo, ktoré bude použité na podpisovanie. Toto heslo musí byť rovnaké ako heslo použité na ochranu nastavení. Podpis sa nachádza na konci batch súboru vo forme komentára. V prípade, že už bol v minulosti súbor podpísaný, starý podpis bude nahradený novým podpisom.

> Poznámka:
> Ak zmeníte podpísaný batch súbor, musíte súbor znova podpísať.

Na spustenie podpísaného batch súboru z príkazového riadka systému Windows alebo pomocou plánovanej úlohy použite nasledujúci príkaz:

```
eshell run <script.bat>
```

Script.bat je cesta k batch súboru.

> Príklad:
> `eshell run d:\myeshellscript.bat`

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 záznamoch v systémovej databáze Registry a zobraziť ich v jednoduchej čitateľnej forme. Tieto informácie vám môžu pomôcť zistiť príčiny podozrivého správania systému, či už vplyvom nekompatibility, alebo infekcie škodlivého kódu.

Kliknite na **Vytvoriť** a napíšte stručný **Komentár** popisujúci vytváraný protokol. Počkajte, kým ESET SysInspector vytvorí protokol (kým jeho stav nebude zobrazený ako „Vytvorený“). Vytváranie protokolu môže byť spomalené nastavením hardvéru alebo systému a môže trvať niekoľko minút.

V okne ESET SysInspector sa nachádzajú informácie o vytvorených protokoloch:

- **Čas** – čas vytvorenia.
- **Komentár** – stručný komentár.

- **Používateľ** – meno používateľa, ktorý vytvoril protokol.
- **Stav** – stav vytvorenia protokolu.

Sú dostupné tieto akcie:

- **Zobraziť** – otvorenie vytvoreného protokolu. Taktiež môžete kliknúť pravým tlačidlom myši na protokol a z kontextového menu vybrať možnosť Zobraziť.
- **Porovnať** – porovnanie dvoch existujúcich protokolov.
- **Vytvoriť** – vytvorenie nového protokolu. Napíšte stručný komentár popisujúci vytváraný protokol a kliknite na Vytvoriť. Počkajte, kým ESET SysInspector vytvorí protokol (kým jeho stav nebude zobrazený ako „Vytvorený“).
- **Odstrániť** – odstránenie vybraných protokolov zo zoznamu.

Po kliknutí pravým tlačidlom myši na jeden alebo viacero vybraných protokolov sú v kontextovom menu dostupné nasledujúce možnosti:

- **Zobraziť** – otvorenie zvoleného protokolu v nástroji ESET SysInspector (rovnako ako pri dvojitom kliknutí na protokol).
- **Porovnať** – porovnanie dvoch existujúcich protokolov.
- **Vytvoriť** – vytvorenie nového protokolu. Napíšte stručný komentár popisujúci vytváraný protokol a kliknite na **Vytvoriť**. Počkajte, kým ESET SysInspector vytvorí protokol (kým jeho **Stav** nebude zobrazený ako „Vytvorený“).
- **Odstrániť** – odstránenie vybraných protokolov zo zoznamu.
- **Odstrániť všetko** – vymazanie všetkých protokolov.
- **Exportovať** – uloženie protokolu do súboru .xml alebo do skomprimovaného súboru .zip.

ESET SysRescue Live

ESET SysRescue Live je bezplatný nástroj, ktorý umožňuje vytvoriť spúšťací 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 nástroja ESET SysRescue Live je, že bezpečnostný produkt ESET pracuje nezávisle od aktuálne nainštalovaného operačného systému, pričom má priamy prístup k disku a celému súborovému systému. Takto je možné napríklad odstrániť z disku hrozby, ktoré by nebolo možné zmazať štandardným spôsobom pri spustenom operačnom systéme a pod.

Plánovač

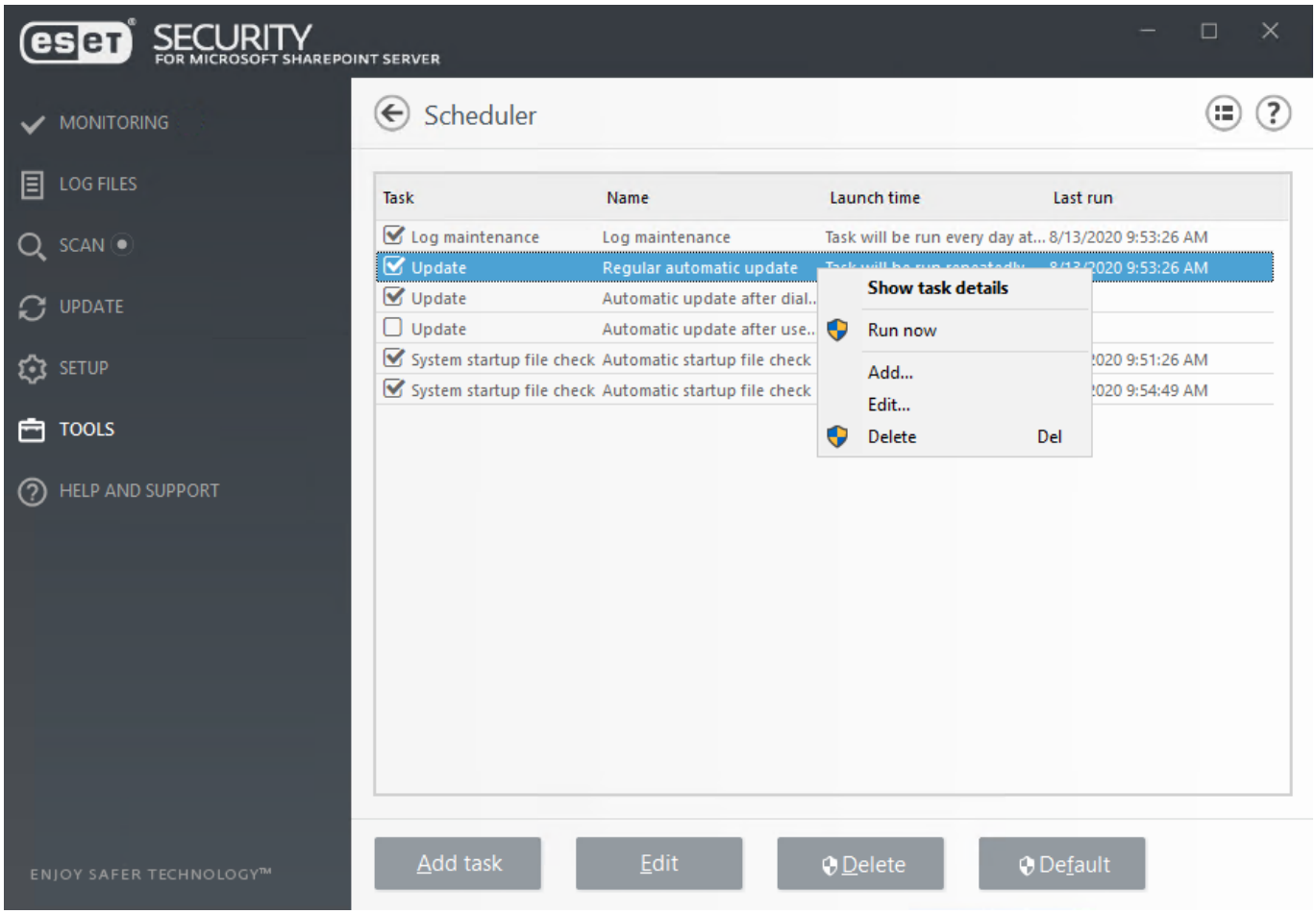
Plánovač spravuje a spúšťa naplánované úlohy podľa definovaných parametrov. Obsahuje zoznam všetkých naplánovaných úloh v podobe tabuľky, ktorá zobrazuje ich parametre, ako napr. Typ úlohy, Názov úlohy, Čas spustenia a Naposledy spustené. Môžete vytvoriť aj nové naplánované úlohy, a to tak, že kliknete na možnosť Pridať plánovanú úlohu. Upraviť konfiguráciu existujúcej naplánovanej úlohy môžete pomocou tlačidla **Upraviť**. Kliknutím na **Predvolené** a následne na **Vrátiť späť na predvolené** dôjde k obnoveniu všetkých preddefinovaných úloh a zmeny, ktoré ste vykonali, budú stratené.

Zároveň sa v ňom nachádza aj sada preddefinovaných úloh:

- Údržba protokolov

- Pravidelná automatická aktualizácia (túto úlohu môžete použiť na zmenu intervalu aktualizácie)
- 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)

> Poznámka:
> Aktivovať alebo deaktivovať úlohy môžete pomocou začiarkavacích políčok.



Kliknutím pravého tlačidla na konkrétnu úlohu je možné vykonať nasledujúce akcie:

Zobraziť podrobnosti	**Dvojitým kliknutím alebo kliknutím pravého tlačidla na konkrétnu úlohu sa zobrazia podrobné informácie o naplánovanej úlohe.**
Spustiť teraz	Spustenie a okamžité vykonanie zvolenej naplánovanej úlohy.
Pridať...	Otvorí sa sprievodca, ktorý vám pomôže vytvoriť naplánovanú úlohu.
Upraviť...	Nastavenie už existujúcich/vytvorených naplánovaných úloh (aj predvolených, aj tých, ktoré sú definované používateľom).
Odstrániť	Odstránenie existujúcej úlohy.

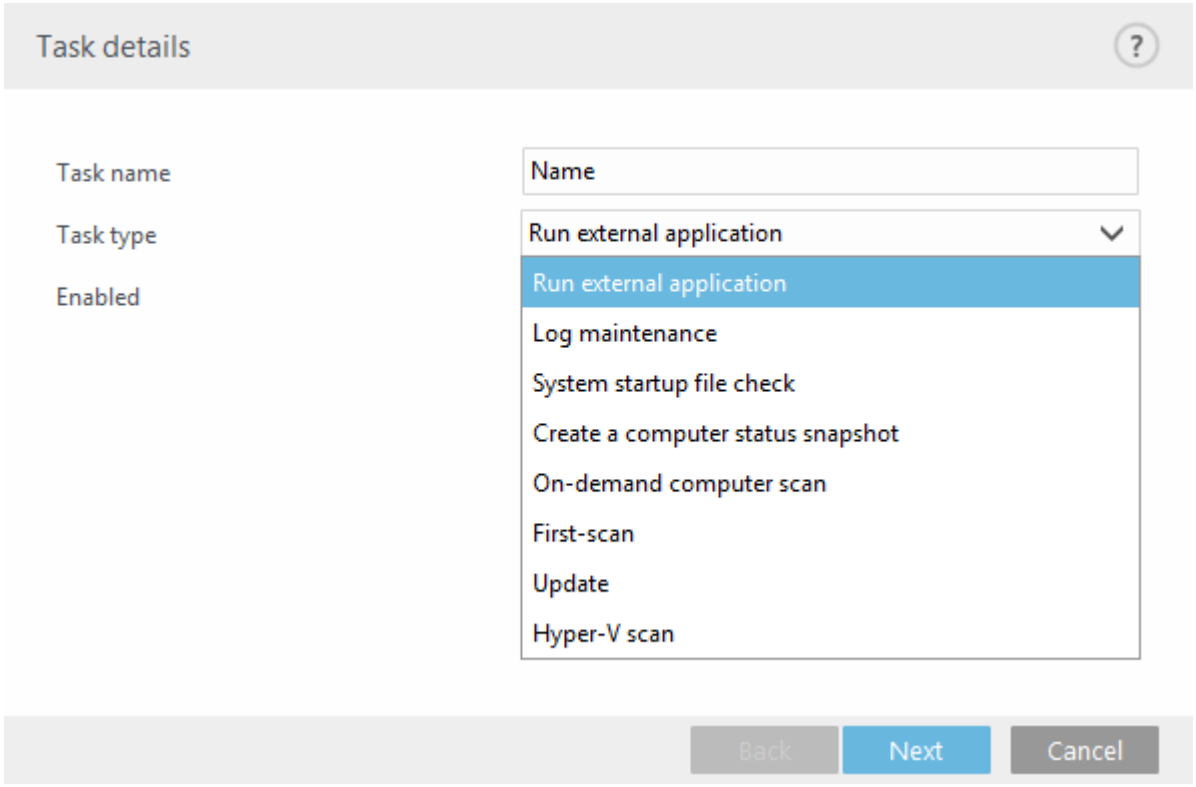
Plánovač – pridanie úlohy

Konfigurácia novej úlohy:

1. Kliknite na **Pridať plánovanú úlohu**.

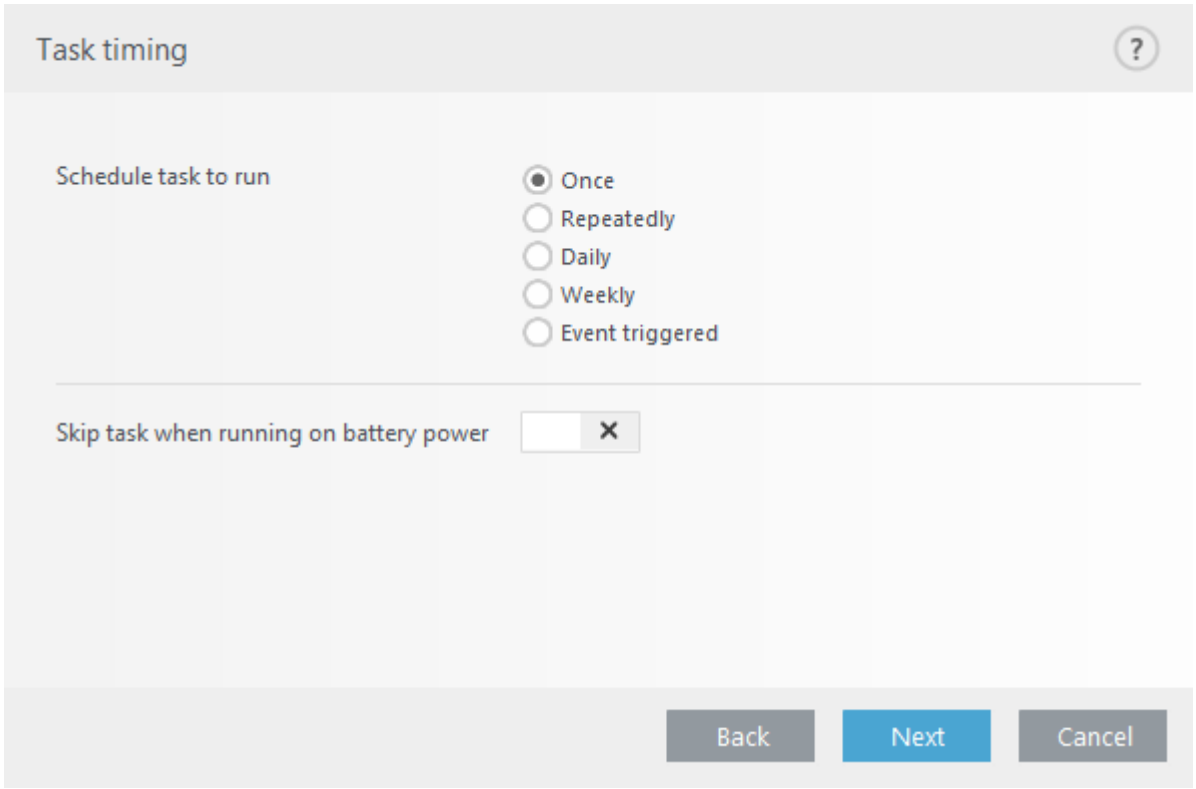
2.Zadajte **Názov úlohy** a nakonfigurujte si svoju vlastnú plánovanú úlohu.

3. Typ úlohy – pomocou roletového menu vyberte vhodný **Typ úlohy**.

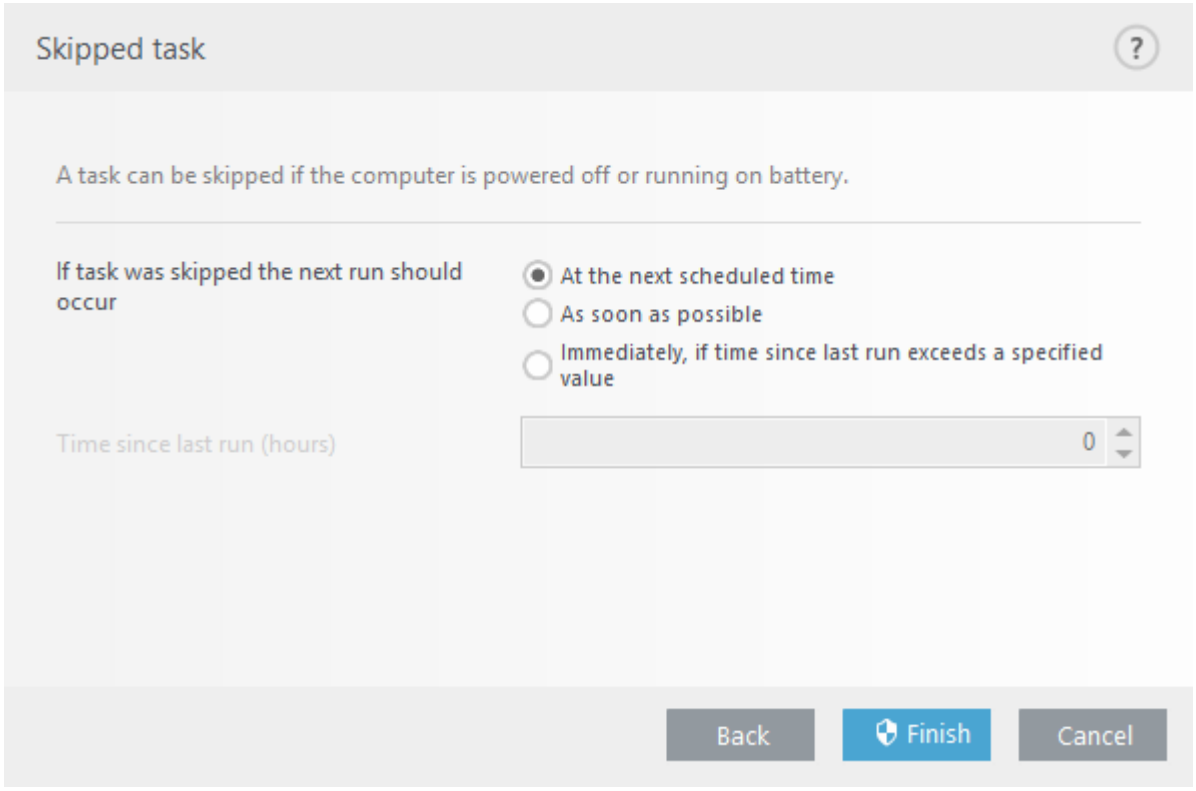


Poznámka:
Ak chcete úlohu deaktivovať, kliknite na tlačidlo vedľa možnosti **Zapnuté**. Úlohu môžete aktivovať neskôr pomocou začiarkavacieho políčka v okne Plánovača.

4. Načasovanie úlohy – vyberte jednu z možností načasovania podľa toho, kedy chcete úlohu spustiť. V závislosti od vášho výberu budete vyzvaný, aby ste si vybrali konkrétny čas, deň, interval alebo udalosť.



5. Vynechaná úloha – v prípade, že sa naplánovanú úlohu nepodarí spustiť v stanovenom čase, môžete určiť, kedy bude úloha najbližšie spustená.



6. Spustenie aplikácie – ak ste ako typ úlohy vybrali úlohu, ktorá spúšťa externú aplikáciu, vyberte spustiteľný súbor zo stromovej štruktúry adresárov.

7.Ak potrebujete urobiť zmeny, kliknite na **Späť**, čím sa vrátite k predchádzajúcim krokom, a následne zmeňte požadované parametre.

8.Kliknite na **Dokončiť** pre vytvorenie úlohy alebo aplikovanie zmien.

Nová naplánovaná úloha sa zobrazí v okne Plánovača.

Typ úlohy

Sprievodca konfiguráciou je odlišný pre každý **typ naplánovanej úlohy**. Zadajte **Názov úlohy** a vyberte požadovaný **Typ úlohy** z roletového menu:

- **Spustenie externej aplikácie** – výber aplikácie, ktorá má byť spustená plánovačom.
- **Údržba protokolov** – defragmentácia odstraňuje prázdne záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi. Viditeľné zlepšenie práce s protokolmi po optimalizácii je pozorovateľné hlavne pri väčších množstvách záznamov v protokoloch.
- **Kontrola súborov spúšťaných po štarte** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.
- **Vytvorenie záznamu o stave počítača** – je to ESET SysInspector snímka stavu počítača, ktorá slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.
- **Manuálna kontrola počítača** – vykoná manuálnu kontrolu diskov, jednotlivých priečinkov a súborov na počítači.
- **Aktualizácia** – zabezpečuje aktualizáciu detekčného jadra, ako aj aktualizáciu všetkých programových súčastí.
- **Pravidelná kontrola databázy** – umožňuje vám nastaviť kontrolu databázy a vybrať položky, ktoré budú kontrolované. Ide v podstate o Manuálnu kontrolu databáz.
- **Kontrola Hyper-V** – umožňuje vám nastaviť kontrolu virtuálnych diskov v rámci Hyper-V.

Ak chcete úlohu po vytvorení deaktivovať, kliknite na tlačidlo vedľa možnosti **Zapnuté**. Úlohu môžete aktivovať neskôr pomocou začiarkavacieho políčka v okne Plánovača. Kliknite na **Ďalej** pre pokračovanie k ďalšiemu kroku.

Načasovanie úlohy

Vyberte si jednu z nasledujúcich možností načasovania úlohy:

- **Raz** – úloha sa vykoná iba raz v presne určený dátum a čas. Umožní vykonať úlohu iba raz v stanovenom čase. V okne **Vykonanie úlohy** zadajte dátum a čas vykonania úlohy.
- **Opakovane** – úloha bude vykonávaná opakovane v určenom časovom intervale (v minútach). V okne **Vykonanie úlohy** zadajte čas, kedy bude úloha vykonaná každý deň.
- **Denne** – úloha bude vykonávaná opakovane každý deň v určenom čase.
- **Týždenne** – úloha bude vykonávaná raz alebo viackrát týždenne v určené dni a v určený čas. Umožní vykonávať úlohu opakovane v konkrétnych dňoch týždňa počnúc stanoveným dňom a časom. Do poľa Čas vykonania úlohy zadajte čas spustenia. Zvoľte deň alebo dni v týždni, kedy má byť úloha spustená.
- Pri udalosti – úloha sa vykoná po určenej udalosti.

Ak povolíte možnosť **Nespúšťať úlohu, ak je počítač napájaný z batérie**, úloha sa nespustí, ak je prenosný počítač napájaný z batérie v čase, keď by mala byť úloha spustená. Táto možnosť sa vzťahuje aj na počítače napájané pomocou UPS.

Pri udalosti

Ak plánujete úlohu, ktorá bude vykonaná pri určitej udalosti, môžete nastaviť minimálny interval medzi dvoma vykonaniami úlohy.

Úloha bude vykonaná pri jednej z nasledujúcich udalostí:

- **Každé spustenie počítača**
- **Prvé spustenie počítača počas dňa**
- **Modemové pripojenie k internetu/VPN**
- **Úspešná aktualizácia modulu**
- **Úspešná aktualizácia produktu**
- **Prihlásenie používateľa** – úloha bude vykonaná, keď sa používateľ prihlási do systému. Napríklad, ak sa prihlasujete na počítač viackrát za deň, nastavením intervalu na 24 hodín sa táto úloha vykoná len pri prvom prihlásení a následne až v nasledujúci deň.
- **Detekcia hrozieb**

Spustenie aplikácie

Táto úloha naplánuje spustenie externej aplikácie.

- **Spustiteľný súbor** – vyberte spustiteľný súbor zo stromovej štruktúry adresárov kliknutím na **...** alebo zadajte cestu k súboru manuálne.
- **Pracovný priečinok** – zadajte pracovný adresár externej aplikácie. Všetky dočasné súbory zvoleného **spustiteľného súboru** budú vytvorené v tomto adresári.
- **Parametre** – parametre, s ktorými bude aplikácia spustená (voliteľné).

Vynechaná úloha

V prípade, že sa naplánovanú úlohu nepodarí spustiť v určenom čase, môžete nastaviť spôsob, ako bude program postupovať:

- **Vykonať úlohu v najbližšom naplánovanom čase** – úloha sa vykoná v konkrétny čas po uplynutí určitej doby (napr. 24 hodín).
- **Vykonať úlohu hneď, ako to bude možné** – úloha sa vykoná okamžite alebo hneď po odstránení problémov, ktoré bránili spusteniu danej úlohy.
- **Vykonať úlohu okamžite, ak od posledného spustenia uplynul stanovený časový interval – Čas od**

posledného spustenia (v hodinách) – po zvolení tejto možnosti sa bude daná úloha vždy opakovať po uplynutí určitej doby (v hodinách).

Informácie o naplánovanej úlohe

Toto dialógové okno zobrazuje podrobné informácie o označenej naplánovanej úlohe. Zobrazuje sa po dvojitom kliknutí na úlohu v okne **Plánovača** alebo po kliknutí pravého tlačidla myši a vybratí možnosti **Zobraziť podrobnosti** z kontextového menu.

Odoslanie vzorky na analýzu

Prostredníctvom okna Poslať vzorku na analýzu môžete odoslať podozrivý súbor alebo stránku do spoločnosti ESET na analýzu. V prípade, že ste našli na svojom počítači súbor s podozrivým správaním alebo podozrivú stránku na internete, pošlite ich na analýzu do vírusového laboratória spoločnosti ESET. Ak sa ukáže, že ide o nebezpečnú aplikáciu alebo stránku, jej detekcia bude pridaná v niektorej najbližšej aktualizácii.

Súbor skomprimujte do archívu pomocou programu WinRAR/WinZip a zabezpečte ho heslom „*infected*“. Následne súbor odošlite na adresu samples@eset.com. Nezabudnite uviesť výstižný predmet správy a čo najviac informácií o danom súbore (napr. URL adresa, z ktorej ste súbor stiahli a pod.).

Predtým, ako odošlete vzorku do spoločnosti ESET na analýzu, sa uistite, že daná vzorka spĺňa niektorú z nasledujúcich podmienok:

- súbor alebo webová stránka nie je zachytená programom,
- súbor alebo webová stránka je nesprávne vyhodnotená ako hrozba.

Ak nebude splnená aspoň jedna z týchto podmienok, nebude vám doručená odpoveď, kým neposkytnete dodatočné informácie.

Z roletového menu **Dôvod odoslania vzorky** zvoľte popis, ktorý najlepšie zodpovedá podozreniu:

- Podozrivý súbor
- Podozrivá stránka (stránka infikovaná malvérom)
- Nesprávne detegovaný súbor (súbor, ktorý je detegovaný ako infikovaný, v skutočnosti však nie je)
- Nesprávne detegovaná stránka
- Iné

Súbor/Stránka

Cesta k súboru alebo webovej stránke, ktorú chcete odoslať.

Kontaktný e-mail

Kontaktný e-mail môže byť v prípade potreby použitý na získanie dodatočných informácií nevyhnutných na analýzu. Zadanie e-mailu nie je povinné. Nebude vám zaslaná žiadna odpoveď, pokiaľ nebudú pracovníci vírusového laboratória potrebovať viac informácií. Každý deň do spoločnosti ESET odošlú používatelia tisícky súborov, preto nie je možné na každý z nich odpovedať.

Odoslať anonymne

Označením možnosti **Odoslať anonymne** môžete odoslať podozrivý súbor alebo webovú stránku bez zadania e-mailovej adresy.

Podozrivý súbor

Spozorované príznaky a správanie malvéru

Uveďte čo najpodrobnejší popis správania súboru v systéme pre presnejšiu analýzu súboru.

Pôvod súboru (URL adresa alebo výrobca aplikácie)

Uveďte URL adresu, prípadne jeho výrobcu (ak je známy) pre lepšiu identifikáciu.

Poznámky a dodatočné informácie

Sem môžete zadať všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní súboru.

> Poznámka:
> Povinné je len pole **Spozorované príznaky a správanie malvéru**, avšak poskytnutím doplňujúcich informácií významnou mierou pomôžete našim laboratóriám pri identifikácii a spracovaní vzoriek.

Podozrivá stránka

V roletovom menu **Aký je problém so stránkou** označte jednu z nasledujúcich možností:

Infikovaná stránka

Webová stránka, ktorá obsahuje vírus alebo rôznymi spôsobmi distribuuje iné typy malvéru.

Phishing

Cieľom je získať citlivé údaje, ako napríklad heslá k bankovým účtom, PIN kódy a pod. Viac o tomto type útoku sa môžete dočítať v slovníku pojmov.

Podvodná stránka

Podvodná, zavádzajúca webová stránka.

Iné

Túto možnosť môžete použiť v prípade, že sa na danú stránku nevzťahuje žiadna z ostatných možností.

Poznámky a dodatočné informácie

Môžete zadať všetky doplňujúce informácie, ktoré by mohli pomôcť pri analýze podozrivej stránky.

Nesprávne detegovaný súbor

Prosíme vás, aby ste nám posielali súbory, ktoré boli programom vyhodnotené ako infikované, hoci v skutočnosti infikované nie sú, aby sme mohli vylepšiť naše detekčné jadro a zvýšiť tak účinnosť ochrany pre všetkých používateľov. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétneho súboru zhoduje so vzorom obsiahnutým v detekčnom jadre.

> Poznámka:
> **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.

Názov a verzia aplikácie

Názov a verzia aplikácie (napr. číslo, alias alebo názov kódu).

Pôvod súboru (URL adresa alebo výrobca aplikácie)

Uveďte pôvod súboru (zdroj) a popíšte, ako ste k danému súboru prišli.

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.

Nesprávne detegovaná stránka

Prosíme vás, aby ste nám posielali webové stránky, ktoré boli programom vyhodnotené ako infikované, ako scam alebo ako phishing, hoci v skutočnosti z bezpečnostného pohľadu problematické nie sú. Falošný poplach (False positive – FP) môže nastať vtedy, keď sa štruktúra alebo charakteristika konkrétnej stránky zhoduje so vzorom obsiahnutým v detekčnom jadre. Zaslaním nesprávne detegovanej stránky nám pomôžete zlepšiť naše detekčné jadro a zvýšiť tak účinnosť ochrany pre všetkých používateľov.

Poznámky a dodatočné informácie

Všetky ďalšie informácie, ktoré by mohli pomôcť pri identifikácii a spracovaní podozrivého súboru.

Iné

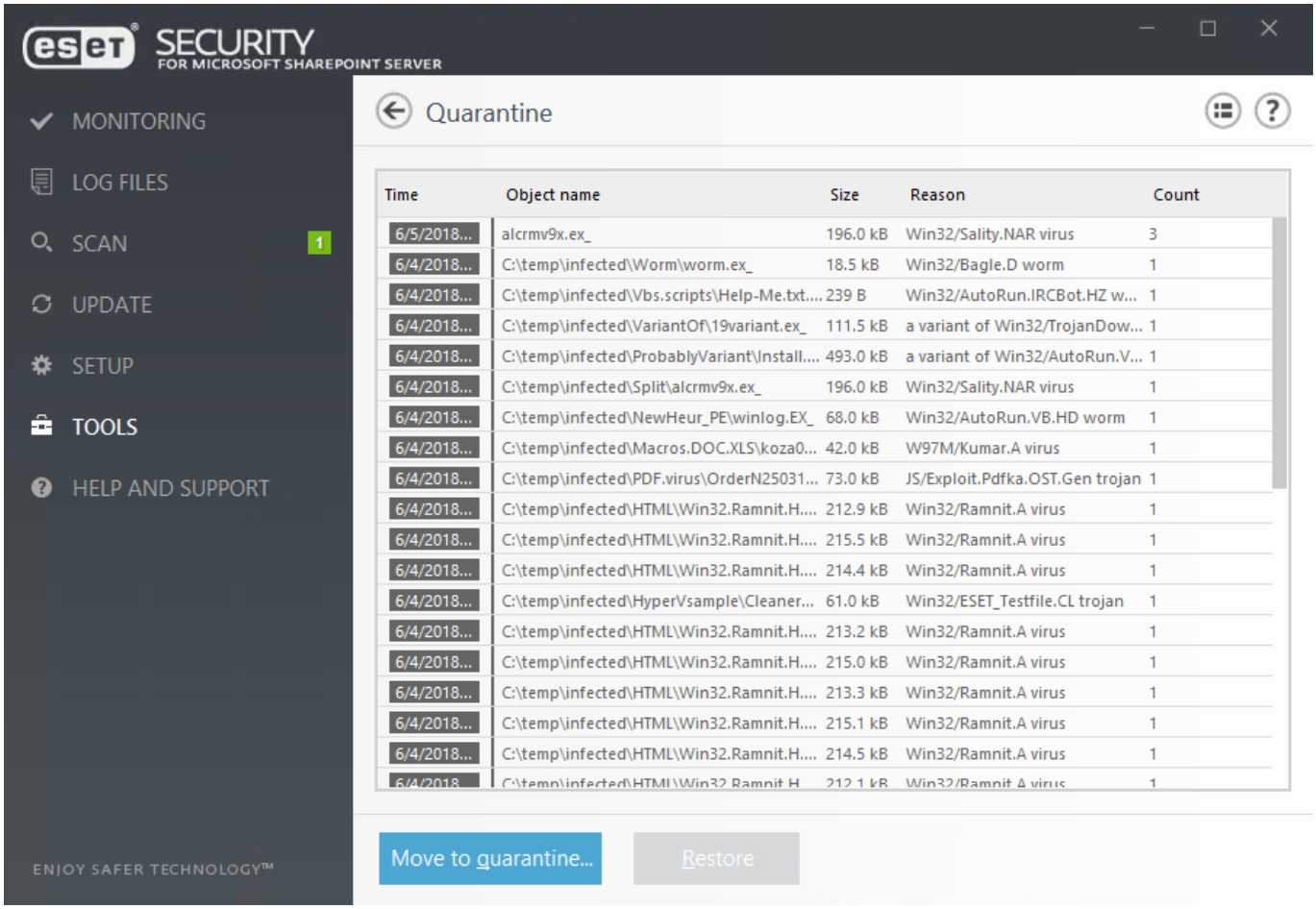
Tento formulár sa používa v prípade, že súbor nie je možné kategorizovať ako **Podozrivý súbor** ani ako **Falošný poplach**.

Dôvod odoslania súboru

Uveďte dôvod odoslania súboru a čo najpresnejší popis súboru.

Karanténa

Hlavnou úlohou karantény je bezpečné uchovanie infikovaných súborov. Vo väčšine prípadov môže ísť o súbory, pre ktoré neexistuje liečenie, nie je isté či je bezpečné ich zmazať, prípadne ide o nesprávnu detekciu antivírusovej ochrany produktu ESET Security for Microsoft SharePoint. Súbory do karantény môžu byť pridané aj samotným používateľom. Túto možnosť je vhodné použiť v prípade, že súbor má podozrivé správanie, no nie je detegovaný antimalvérovým skenerom. Súbory z karantény môžu byť zaslané na analýzu do vírusového laboratória spoločnosti ESET.



Súbory uložené v karanténe môžete vidieť v prehľadnej tabuľke, kde sú informácie o dátume a čase pridania súboru do karantény, cesta k pôvodnému umiestneniu súboru, jeho dĺžka v bytoch, dôvod (napr. objekt pridaný používateľom), počet infiltrácii (napr. ak archív obsahoval viac infikovaných súborov).

V prípade umiestnenia e-mailových správ do karantény bude zobrazená cesta k e-mailovej schránke/priečinku/názvu súboru.

Pridávanie súborov do karantény

ESET Security for Microsoft SharePoint pridáva súbory do karantény automaticky pri ich mazaní (pokiaľ používateľ vo varovnom okne nezruší túto možnosť). Ak chcete manuálne umiestniť podozrivý súbor do karantény, kliknite na možnosť **Karanténa**. Súbory uložené v karanténe budú odstránené z ich pôvodného umiestnenia. Na tento účel môže byť použité aj kontextové menu. Kliknite pravým tlačidlom myši v okne **Karanténa** a z kontextového menu vyberte možnosť **Presunúť...**

Obnovenie z karantény

Súbory uložené v karanténe je možné obnoviť a vrátiť do pôvodného umiestnenia. Slúži na to funkcia **Obnoviť**, ktorá je takisto dostupná aj pomocou kontextového menu po kliknutí pravým tlačidlom na daný súbor v karanténe. Ak je súbor označený ako Potenciálne nechcená aplikácia, bude dostupná možnosť **Obnoviť a vylúčiť z kontroly**. V kontextovom menu sa tiež nachádza možnosť **Obnoviť do...** Táto funkcia umožňuje súbor obnoviť na iné miesto, než to, z ktorého bol pôvodne zmazaný.

Poznámka:
Ak program omylom uložil do karantény neškodný súbor, po obnovení vylúčte daný súbor z kontroly a odošlite ho Technickej podpore spoločnosti ESET.

Poslanie na analýzu

Ak máte v karanténe uložený súbor s podozrivým správaním, ktorý nebol detegovaný programom, prípadne bol nesprávne vyhodnotený ako škodlivý, môžete ho poslať do spoločnosti ESET na analýzu. Pre odoslanie súboru z karantény kliknite pravým tlačidlom na príslušný súbor a z kontextového menu vyberte možnosť Poslať na analýzu.

Odstránenie objektu z karantény

Kliknite pravým tlačidlom na súbor v umiestnený v karanténe a z roletového menu vyberte možnosť **Odstrániť** alebo stlačte kláves **Delete**.

Nastavenia ochrany servera

ESET Security for Microsoft SharePoint zabezpečuje ochranu pre váš Microsoft SharePoint Server pomocou nasledujúcich funkcií:

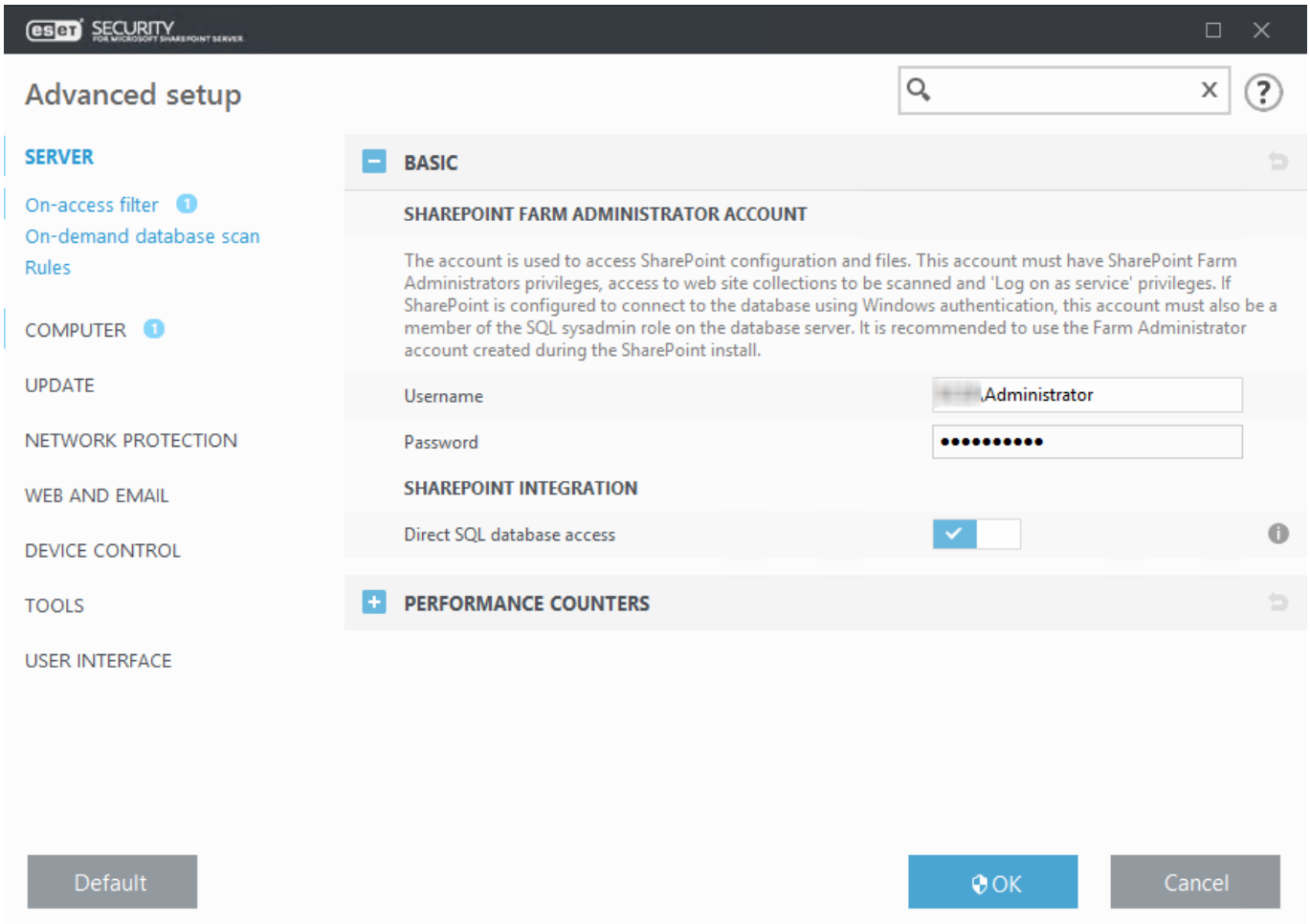
- Filtrovanie pri prístupe
- Manuálna kontrola databáz
- Pravidlá

Dôležité:
Účet správcu SharePointu musí mať pridelené práva správcu farmy SharePoint pre prístup ku kolekciám webových stránok určených na kontrolu. Tento účet zároveň musí mať oprávnenie „prihlásiť sa ako služba“. Ak je SharePoint nakonfigurovaný tak, aby na prístup k databáze používal overovanie systému Windows, účet správcu SharePointu musí byť členom roly SQL Sysadmin na databázovom serveri. Odporúčame používať účet správcu farmy SharePoint vytvorený počas inštalácie SharePointu. Bez zadania platných prihlasovacích údajov nebude ESET Security for Microsoft SharePoint po inštalácii fungovať. Ak bola inštalácia vykonaná bez použitia grafického používateľského rozhrania (GUI), bude potrebné zadať účet správcu SharePointu buď v GUI, alebo cez eShell. V opačnom prípade bude produkt nefunkčný.
V prostredí spravovanom pomocou ESET PROTECT môžete na vykonanie príkazov eShell použiť klientsku úlohu Spustiť príkaz. Je to užitočné najmä v prípade veľkých fariem s mnohými inštanciami SharePoint, alebo ak chcete na diaľku prideľovať prihlasovacie údaje. Pri vytváraní novej klientskej úlohy ESET PROTECT špecifikujte **Príkazový riadok na spustenie**:

```
powershell eshell server set farm-username <domain\user> && eshell server set farm-password plain <password>
```

Uistite sa, že politika spustenia ESET Shell je nastavená na **Úplný prístup**, aby príkaz fungoval.

Poznámka:
Na zaistenie nepretržitej ochrany musia byť prihlasovacie údaje k účtu správcu SharePointu znova zadané (aktualizované) vždy, keď sa zmenia. V prípade, že tu zadané prihlasovacie údaje sa nezhodujú s tými, ktoré sú používané pre účet správcu SharePointu, ESET Security for Microsoft SharePoint nebude správne fungovať, a teda nebude poskytovať maximálnu ochranu.



Priamy prístup k SQL databáze

Táto funkcia slúži na povolenie prístupu na čítanie k databázam SharePointu. Umožňuje programu ESET Security for Microsoft SharePoint čítať dáta priamo z SQL Servera (obsahové databázy SharePointu). Priamy prístup k databáze má oproti objektovému modelu SharePoint viacero výhod. Priamy prístup k databáze je rýchlejší, má vyššiu celkovú výkonnosť a využíva menej systémových prostriedkov. Ide o atribúty, ktoré sú užitočné pri kontrole. Priamy prístup k databáze sa používa pri všetkých operáciách, kde dochádza k čítaniu, pričom všetky operácie súvisiace so zápisom (liečenie, odstránenie atď.) sú spúšťané prostredníctvom objektového modelu SharePoint. Ak zakážete priamy prístup k SQL databáze, objektový model SharePoint bude použitý pre všetky operácie (čítanie aj zápis). Priamy prístup k SQL databáze aj objektový model SharePoint podporujú paralelné sťahovanie. Paralelné sťahovanie môžete nastaviť zadaním **Počtu súbežných sťahovaní** v časti Manuálna kontrola databáz.

Počítadlá výkonu

Počítadlá výkonu môžete použiť na monitorovanie výkonu programu ESET Security for Microsoft SharePoint. Táto funkcia je dostupná na systéme Microsoft Windows Server 2008 R2 SP1 a novších systémoch.

Počítadlá výkonu

Počítadlá výkonu ESET Security for Microsoft SharePoint vám umožňujú monitorovať výkonnosť procesu kontroly. Poskytujú informácie, ako napríklad počet spracovaných a skontrolovaných súborov, objem dát stiahnutých z lokality Microsoft SharePoint, priemerný čas kontroly atď. Zoznam dostupných počítadiel nájdete v tabuľke nižšie. Počítadlá výkonu ESET Security for Microsoft SharePoint sa delia na dve skupiny podľa typu ochrany (manuálna a pri prístupe). Obe skupiny majú rovnakú sadu počítadiel výkonu.

Počítadlá výkonu ESET Security for Microsoft SharePoint sú registrované do operačného systému automaticky počas inštalácie programu. Po aktivovaní počítadiel výkonu začne program ESET Security for Microsoft SharePoint poskytovať údaje o výkonnosti. Ak počítadlá výkonu vypnete, ostanú aj naďalej registrované v systéme, avšak ESET Security for Microsoft SharePoint prestane poskytovať údaje o výkonnosti. Ak odinštalujete ESET Security for Microsoft SharePoint, registrácia počítadiel v systéme bude automaticky zrušená.

ESET Security for Microsoft SharePoint využíva pri poskytovaní údajov o výkonnosti novú architektúru (verzia 2.0). Tieto údaje o výkone ESET Security for Microsoft SharePoint môžu byť spracované a zobrazené priamo pomocou nástroja Windows Server Performance Monitor. Pracovať s nimi dokáže taktiež rozhranie Performance Data Helper (PDH).

> Poznámka:
> Počítadlá výkonu ESET Security for Microsoft SharePoint sú dostupné pre Microsoft Windows Server 2008 R2 SP1 a novšie systémy.

Po aktivovaní počítadiel výkonu ESET Security for Microsoft SharePoint otvorte nástroj Performance Monitor a pridajte počítadlá, z ktorých chcete prijímať údaje. Počítadlá si môžete vybrať z dvoch skupín: **ESET Security for Microsoft SharePoint - On-access Scan** a **ESET Security for Microsoft SharePoint - On-access Scan - On-demand Scan**. Bližšie informácie o nástroji Performance Monitor nájdete v článku Windows Performance Monitor Overview od spoločnosti Microsoft.

Zoznam dostupných počítadiel:

Počítadlá výkonu pre kontrolu pri prístupe (názov skupiny: ESET Security for Microsoft SharePoint - On-access Scan)

Názov počítadla	Popis
OA - Processed Files	Celkový počet spracovaných súborov od spustenia ESET Security for Microsoft SharePoint.
OA - Processed Files/sec	Počet súborov spracovaných za 1 sekundu.
OA - Processed Files/sec (Average)	Pohyblivý priemer počtu spracovaných súborov.
OA - Scanned Files	Celkový počet skontrolovaných súborov od spustenia ESET Security for Microsoft SharePoint.
OA - Scanned Files/sec	Počet súborov skontrolovaných za 1 sekundu.
OA - Scanned Files/sec (Average)	Pohyblivý priemer počtu skontrolovaných súborov.
OA - File Processing Time (ms) (Average)	Priemerný čas v milisekundách potrebný na spracovanie súboru (spracovanie súborov zahŕňa sťahovanie, vyhodnocovanie pravidiel a kontrolu).
OA - File Downloading Time (ms) (Average)	Priemerný čas v milisekundách potrebný na stiahnutie súboru z lokality Microsoft SharePoint.
OA - File Scanning Time (ms) (Average)	Priemerný čas v milisekundách potrebný na kontrolu súboru na prítomnosť hrozieb.

Názov počítadla	Popis
OA - File Rule Checking Time (ms) (Average)	Priemerný čas v milisekundách potrebný na vyhodnotenie pravidiel pre konkrétny súbor.
OA - Downloaded MB	Celkový objem dát v MB stiahnutých z lokality Microsoft SharePoint od spustenia ESET Security for Microsoft SharePoint.
OA - Download Speed KB/sec (Average)	Priemerná rýchlosť sťahovania z lokality Microsoft SharePoint v KB/s.

Počítadlá výkonu pre manuálnu kontrolu (názov skupiny: ESET Security for Microsoft SharePoint - On-demand Scan)

Názov počítadla	Popis
OD - Processed Files	Celkový počet spracovaných súborov od spustenia ESET Security for Microsoft SharePoint.
OD - Processed Files/sec	Počet súborov spracovaných za 1 sekundu.
OD - Processed Files/sec (Average)	Pohyblivý priemer počtu spracovaných súborov.
OD - Scanned Files	Celkový počet skontrolovaných súborov od spustenia ESET Security for Microsoft SharePoint.
OD - Scanned Files/sec	Počet súborov skontrolovaných za 1 sekundu.
OD - Scanned Files/sec (Average)	Pohyblivý priemer počtu skontrolovaných súborov.
OD - File Processing Time (ms) (Average)	Priemerný čas v milisekundách potrebný na spracovanie súboru (spracovanie súborov zahŕňa sťahovanie, vyhodnocovanie pravidiel a kontrolu).
OD - File Downloading Time (ms) (Average)	Priemerný čas v milisekundách potrebný na stiahnutie súboru z lokality Microsoft SharePoint.
OD - File Scanning Time (ms) (Average)	Priemerný čas v milisekundách potrebný na kontrolu súboru na prítomnosť hrozieb.
OD - File Rule Checking Time (ms) (Average)	Priemerný čas v milisekundách potrebný na vyhodnotenie pravidiel pre konkrétny súbor.
OD - Downloaded MB	Celkový objem dát v MB stiahnutých z lokality Microsoft SharePoint od spustenia ESET Security for Microsoft SharePoint.
OD - Download Speed KB/sec (Average)	Priemerná rýchlosť sťahovania z lokality Microsoft SharePoint v KB/s.

Filtrovanie pri prístupe

V tomto okne môžete meniť nastavenia parametrov Filtrovania pri prístupe podľa vlastných potrieb. Môžete sa rozhodnúť, či chcete možnosť Zapnúť filtrovanie pri prístupe zapnúť (predvolené nastavenie) alebo vypnúť. Pokiaľ Filtrovanie pri prístupe vypnete, nižšie uvedené funkcie sa deaktivujú.

Pri vypnutom Filtrovaní pri prístupe program ESET Security for Microsoft SharePoint nekontroluje dokumenty pri nahrávaní (upload) ani sťahovaní (download), neuplatnia sa žiadne pravidlá filtrovania a v sekcii Monitorovanie sa zobrazí varovná správa.

> Poznámka:
> Pre zaistenie maximálnej ochrany vám odporúčame ponechať možnosť **Zapnúť filtrovanie pri prístupe** zapnutú.

Nastavenia ochrany SharePoint (tieto nastavenia môžu byť spravované aj cez Centrálnu správu lokality

SharePoint):

Prepojiť s Centrálnou správou lokality SharePoint

Kliknite na URL adresu, ak chcete otvoriť Centrálnu správu lokality SharePoint – Nastavenia antivírusu. Pokiaľ budete nastavenia meniť cez Centrálnu správu lokality SharePoint, zobrazenie daných zmien v samotnom produkte ESET Security for Microsoft SharePoint môže chvíľu trvať.

Kontrolovať dokumenty pri nahrávaní

Dokumenty nahrávané do lokality SharePoint budú kontrolované cez webové rozhranie pri každom uložení v programoch MS Office a počas synchronizácie cez SharePoint workspace.

Kontrolovať dokumenty pri sťahovaní

Dokumenty preberané z lokality SharePoint cez webové rozhranie budú kontrolované počas sťahovania. Kontrola zahŕňa aj obrázky a dokumenty otvárané v programoch MS Office počas synchronizácie cez SharePoint workspace.

Povoliť používateľovi sťahovať infikované dokumenty

Ak je táto možnosť povolená, SharePoint zobrazí upozornenie o infikovaných súboroch, no používateľ bude aj napriek tomu môcť tieto súbory otvoriť, pričom infikované súbory nebudú vymazané, ale iba zablokované. Ak je táto možnosť vypnutá, zobrazí sa správa, ktorá upozorní používateľa na to, že dokument je infikovaný a jeho stiahnutie nie je možné. Správca SharePointu však môže infikované súbory preberať vždy, a to bez ohľadu na to, či je táto možnosť vypnutá alebo zapnutá.

Pokúsiť sa vyliečiť infikované dokumenty

Ak je táto možnosť povolená, infikované dokumenty, ktoré je možné vyliečiť, budú vyliečené.

Dĺžka časového limitu (v sekundách)

Maximálny čas, ktorý bude SharePoint čakať na odpoveď od ESET Security for Microsoft SharePoint. Ak nie je prijatá žiadna odpoveď, SharePoint vyhlási, že pri antivírusovej kontrole došlo k chybe (AV scanner error). Predvolená hodnota je 300 sekúnd.

Počet vlákien kontroly

Počet inštancií pre každý w3wp proces. SharePoint zvyčajne používa tri w3wp procesy. K dispozícii je celkovo 15 (3x5) kontrolujúcich vlákien. Toto nastavenie vám umožňuje určiť maximálny počet súborov, ktoré môžu byť sťahované/nahrávané naraz v tom istom čase. Počet kontrolujúcich vlákien však nie je to isté ako počet skenovacích jadier ThreatSense.

Antivírus a antispyware

Vykonať akciu, ak nie je možné liečenie

Umožňuje vybrať akciu, ktorá sa má vykonať v prípade, že je nájdený infikovaný súbor, avšak liečenie nie je možné:

- **Žiadna akcia** – nebudú vykonané žiadne zmeny. V prípade, že bude na SharePoint nahraný infikovaný

súbor, zostane uložený v systéme a používatelia k nemu budú mať prístup.

• **Blokovať** – infikovaný súbor bude zablokovaný a nebude nahraný/prevzatý. Ak to bude možné, zobrazí sa správa, ktorá používateľovi oznámi, prečo súbor nebol nahraný/prevzatý.

• **Označiť na odstránenie** – súbor je navrhnutý na odstránenie a SharePoint sám rozhodne o jeho odstránení. Zvyčajne nie je možné odstrániť súbor, keď k nemu pristupuje používateľ (počas preberania), pretože používateľ nemá práva na zápis/odstránenie. Táto možnosť nie je dostupná, ak je v rámci nastavení skenovacieho jadra ThreatSense úroveň liečenia nastavená na možnosti Neliečiť. Ak však používateľ, ktorý preberá súbor, má príslušné práva, súbor bude odstránený. Typ správy, ktorá sa používateľovi zobrazí, spravuje SharePoint. V prípade SharePoint 2010, 2013 a 2016 sa zobrazuje správna správa. Ale v prípade SharePoint 2007 bude informácia v správe hovoriť o tom, že súbor bol odstránený, a to aj napriek tomu, že používateľ nemá dostatočné práva a súbor v skutočnosti odstránený nebol.

Poznámka:
Ak je dokument odstránený, odstránia sa aj jeho staršie verzie. Odporúčame preto používať akciu Blokovať. Na odstránenie infikovaného dokumentu z databázy SharePointu odporúčame použiť manuálnu kontrolu databáz.

Presunúť infikované súbory do karantény

Ak je táto možnosť povolená, súbory, ktoré boli označené na odstránenie, budú presunuté do karantény. Túto možnosť odporúčame vypnúť v prípade, ak nechcete, aby sa súbory hromadili v karanténe. Takéto nastavenie je možné použiť, ak je napríklad oblasť disku, na ktorej sa karanténa nachádza, príliš malá a mohla by sa veľmi rýchlo zaplniť. Karanténa by však za normálnych okolností nemala byť vypnutá. Toto nastavenie má vplyv na politiku karantény pre liečiteľné aj neliečiteľné súbory. Na druhej strane na pravidlá nemá použitie karantény žiaden vplyv.

Šablóna správy, ktorá sa zobrazí pri nájdení hrozby

Môžete upraviť správu, ktorá sa používateľovi zobrazuje vo webovom prehliadači vždy, keď bola zachytená infiltrácia, ktorá bola následne vyliečená, zablokovaná alebo odstránená. Zadajte želaný text do poľa Šablóna správy zobrazenej pri nájdení hrozby. Správa sa zobrazí iba v rámci webového rozhrania. Verzie SharePoint 2007 a SharePoint 2010, 2013 a 2016 používajú odlišnú predvolenú správu. V správe môžete použiť nasledujúce premenné:

%VIRUSNAME% – názov infiltrácie zo skenovacieho jadra.
%FILENAME% – názov súboru.
%FILESIZE% – veľkosť súboru.
%PRODUCTNAME% – názov produktu, v tomto prípade: ESET Security for Microsoft SharePoint.

Parametre ThreatSense

Táto možnosť slúži na zmenu parametrov kontroly pre Filtrovanie pri prístupe.

Ochrana filtra prístupu s využitím strojového učenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia.

Manuálna kontrola databáz

Pre každú zvolenú webovú stránku bude v rámci kontroly skontrolovaná aj príslušná štruktúra priečinkov a súborov. Každý jeden súbor, či už dokument používateľa, alebo iný interný súbor SharePointu, je uložený do dočasného súboru, ktorý je následne odoslaný skenovaciemu jadru na kontrolu. Ak existujú aj staršie verzie konkrétneho súboru a je zapnutá funkcia **Kontrolovať verzie dokumentov**, budú tieto staršie verzie skontrolované ako prvé.

Kontrolovať v režime len na čítanie

Infikované dokumenty nebudú vyliečené ani vymazané. Akcia Zmazať nebude vykonaná.

Kontrolovať verzie dokumentov

Ak v databáze SharePointu existujú rôzne verzie toho istého dokumentu, budú všetky skontrolované (nebude teda skontrolovaná len aktuálna verzia dokumentu).

Pri odstránení dokumentu obnoviť poslednú neinfikovanú verziu

V prípade vymazania infikovaného dokumentu sa skontrolujú jeho staršie neinfikované verzie. Ak existujú staršie neinfikované verzie, najnovšia z nich sa obnoví a nahradí vymazaný dokument. Táto možnosť nie je dostupná, pokiaľ je zapnutá funkcia Kontrolovať v režime len na čítanie.

Ciele kontroly

Zobrazí sa okno, v ktorom si môžete zvoliť, či chcete kontrolovať všetky alebo len vami vybrané ciele. Viac informácií nájdete v kapitole Ciele manuálnej kontroly databáz.

Počet súbežných sťahovaní

Tento parameter umožňuje súbežnú kontrolu súborov pomocou viacerých vlákien. Ak je hodnota v tomto poli nastavená na 0, súbory sa budú kontrolovať sekvenčne a nie paralelne.

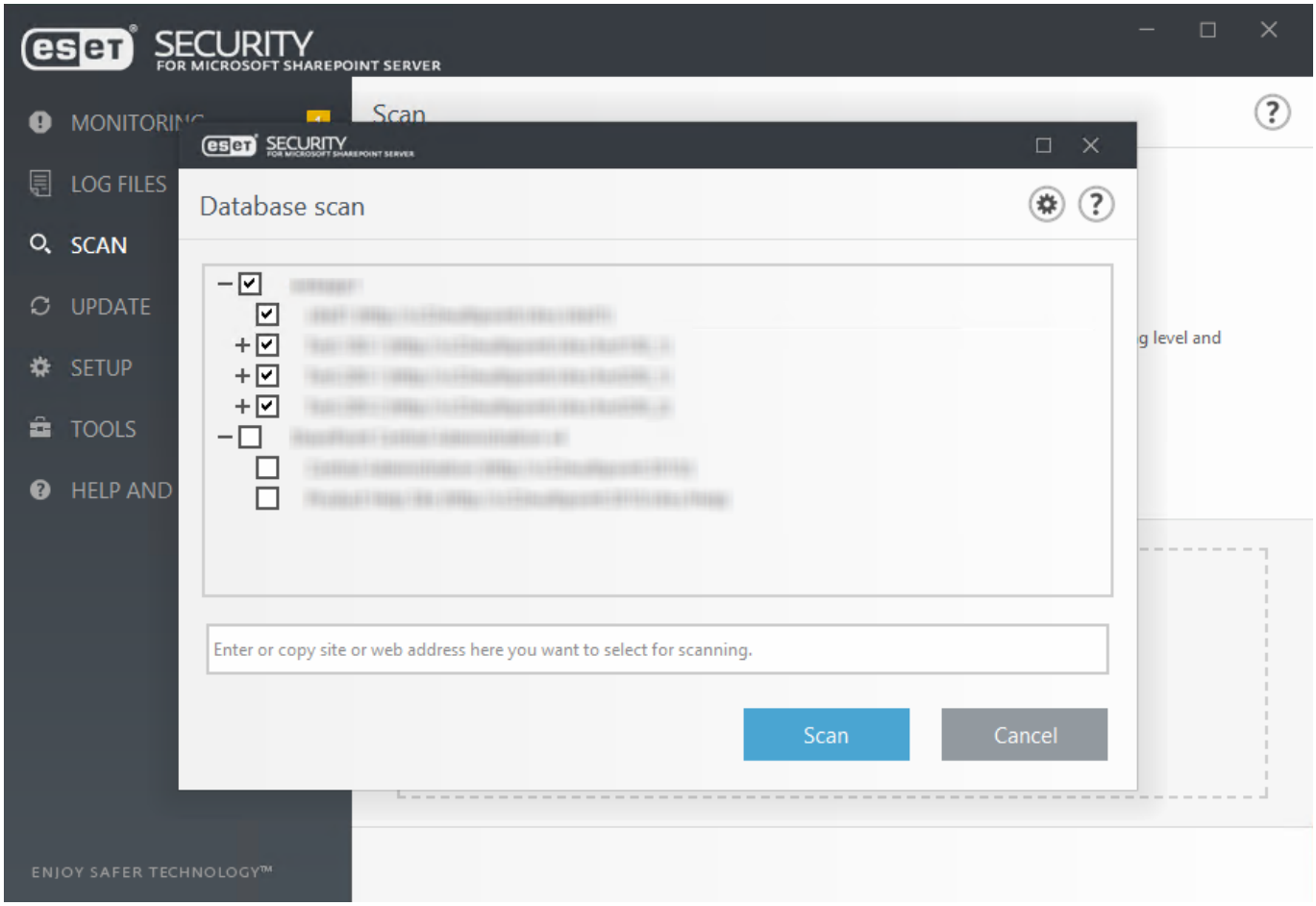
Ciele manuálnej kontroly databáz

V tomto dialógovom okne si môžete vybrať webové stránky SharePoint, ktoré chcete kontrolovať, a spustiť samotný proces kontroly. Zobrazí sa zoznam webových stránok. V roletovom menu **Ciele kontroly** si zvoľte možnosť **Všetky ciele** alebo **Vlastné ciele**.

Pri vlastnom výbere cieľov označte zaškrtávacie políčko vedľa tej webovej stránky, ktorú chcete pridať do kontroly.

Ak chcete do zoznamu pridať ďalšiu webovú stránku, zadajte jej URL adresu do textového poľa v spodnej časti dialógového okna. Načítanie zoznamu a celej štruktúry webových stránok môže chvíľu trvať. Čas zobrazenia závisí od počtu stránok a ich komplexnosti. Ak nastanú akékoľvek zmeny, zoznam môžete aktualizovať stlačením klávesu **F5**. Keď je celý zoznam zobrazený, prostredníctvom zaškrtávacích políčok môžete vybrať webové stránky, ktoré chcete skontrolovať.

Na vrchu zobrazenej štruktúry sa nachádza webová aplikácia SharePoint zahŕňajúca jednu alebo viacero kolekcií webových stránok SharePoint, ktoré obsahujú samotné webové stránky SharePoint. Webové stránky sú usporiadané hierarchicky, jedna zo stránok je teda vždy koreňom (root).



- **Kontrolovať v režime len na čítanie** – infikované dokumenty nebudú vyliečené ani vymazané. Akcia Zmazať nebude vykonaná.
- **Kontrolovať verzie dokumentov** – ak v databáze SharePointu existujú rôzne verzie toho istého dokumentu, budú všetky skontrolované (nebude teda skontrolovaná len aktuálna verzia dokumentu).
- **Pri vymazaní dokumentu obnoviť poslednú neinfikovanú verziu** – v prípade vymazania infikovaného dokumentu sa skontrolujú jeho staršie neinfikované verzie. Ak existujú staršie neinfikované verzie, najnovšia z nich sa obnoví a nahradí vymazaný dokument. Táto možnosť nie je dostupná, pokiaľ je zapnutá funkcia Kontrolovať v režime len na čítanie.

Po nastavení želaných cieľov a parametrov kliknite na **Kontrolovať**, čím spustíte proces kontroly.

Keď je celá štruktúra webových stránok načítaná a zobrazená po prvý krát, uloží sa do vyrovnávacej pamäte služby ESET SharePoint Helper pre rýchlejší prístup. Štruktúra webových stránok sa po uplynutí určitej doby aktualizuje automaticky, no môžete ju obnoviť aj manuálne stlačením klávesu **F5**.

Antivírus a antispyware

Vykonať akciu, ak nie je možné liečenie

Umožňuje vybrať akciu, ktorá sa má vykonať v prípade, že je nájdený infikovaný súbor, avšak liečenie nie je možné (odstránenie súboru nie je považované za spôsob liečenia):

- **Žiadna akcia** – nebudú vykonané žiadne zmeny a súbory budú stiahnuté/nahrané.
- **Odstrániť** – súbor bude odstránený z databázy. Ak sa počas odstraňovania súboru vyskytne chyba, informácia o nej bude zaznamenaná v protokole o kontrole databázy. Táto možnosť nie je dostupná, ak je

v rámci nastavení skenovacieho jadra ThreatSense úroveň liečenia nastavená na možnosti Neliečiť.

Presunúť infikované súbory do karantény

Ak je táto možnosť povolená, súbory, ktoré boli označené na odstránenie, budú presunuté do karantény. Vypnutím tejto funkcie deaktivujete karanténu, čím sa zamedzí hromadeniu súborov v karanténe. Takéto nastavenie je možné použiť, ak je napríklad oblasť disku, na ktorej sa karanténa nachádza, príliš malá a mohla by sa veľmi rýchlo zaplniť. Karanténa by však za normálnych okolností nemala byť vypnutá. Toto nastavenie má vplyv na politiku karantény pre liečiteľné aj neliečiteľné súbory. Na druhej strane na pravidlá nemá použitie karantény žiaden vplyv.

Parametre ThreatSense

Na túto možnosť kliknite v prípade, ak chcete zmeniť parametre Manuálnej kontroly databáz.

Manuálna kontrola databáz s využitím strojového učenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia.

Pravidlá

Pravidlá umožňujú manuálne zadefinovať a spravovať podmienky filtrovania súborov, ako aj akcie, ktoré budú vykonané s filtrovanými súbormi. Pravidlá sa uplatňujú na základe kombinácie podmienok. Pre pravidlá Filtrovania pri prístupe a Manuálnej kontroly databáz sú k dispozícii rôzne podmienky a akcie. Sú dostupné dve rozdielne skupiny pravidiel:

- Filtrovanie pri prístupe
- Manuálna kontrola databáz

Ak chcete vytvoriť nové pravidlo, kliknite na **Upraviť**, čím otvoríte zoznam pravidiel, potom kliknite na **Pridať** a postupujte podľa Sprievodcu pravidlami.

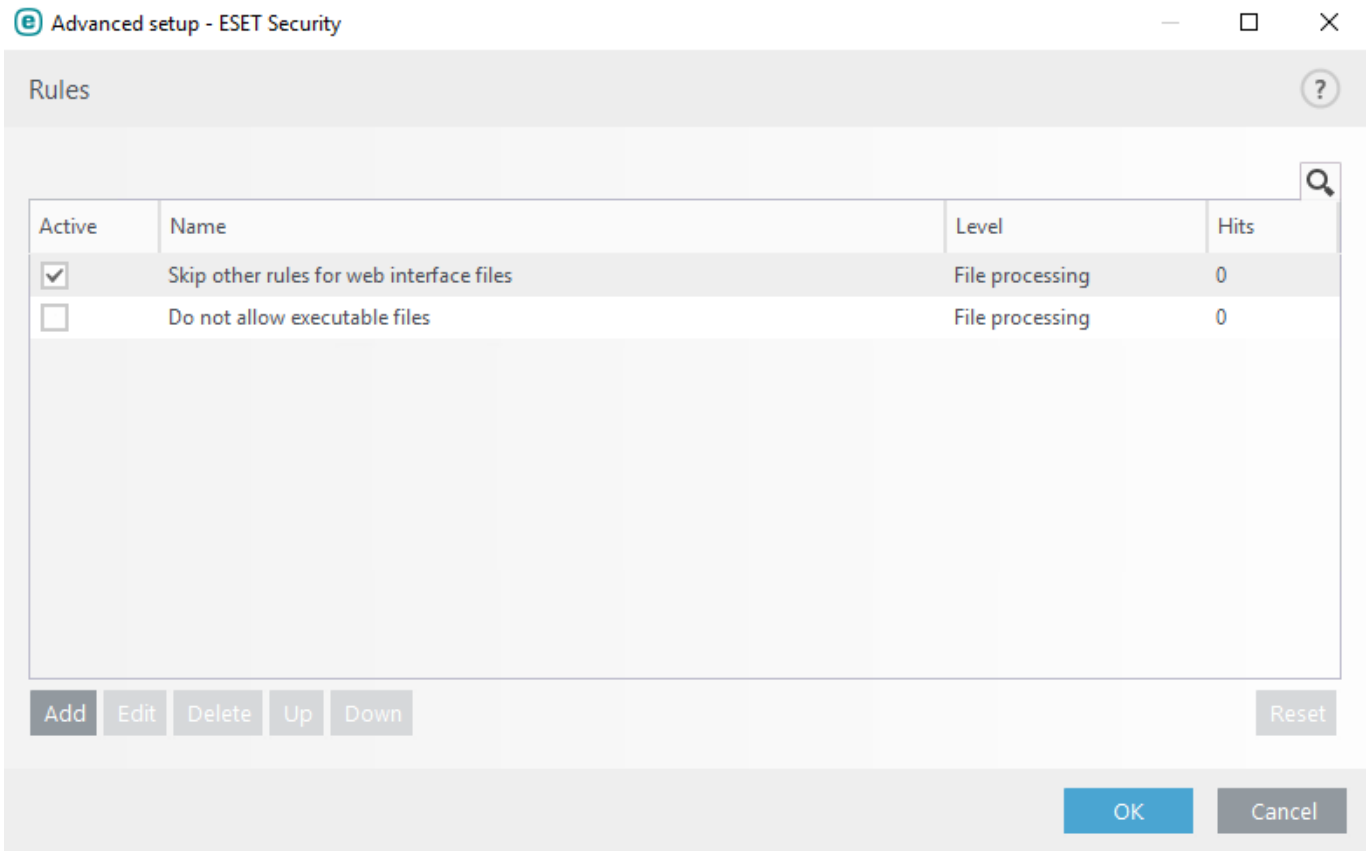
Zoznam pravidiel

Pravidlá sú rozdelené do troch úrovní a sú vyhodnocované v nasledujúcom poradí:

- **Pravidlá filtrovania (1)** – pravidlo je vyhodnocované pred antivírusovou kontrolou.
- **Pravidlá spracovania prílohy (2)** – pravidlo je vyhodnocované počas antivírusovej kontroly.
- **Pravidlá spracovania výsledku (3)** – pravidlo je vyhodnocované po antivírusovej kontrole.

Pravidlá na rovnakej úrovni sú vyhodnocované v rovnakom poradí, v akom sú zobrazené v zozname pravidiel. Poradie pravidiel je možné zmeniť len pre pravidlá na rovnakej úrovni. Pri viacerých filtrovacích pravidlách môžete zmeniť poradie, v akom budú aplikované. Nemôžete však zmeniť poradie takým spôsobom, že presuniete pravidlá pre **spracovanie prílohy** pred **filtrovacie pravidlá**. Tlačidlá **Hore**/**Dole** nebudú dostupné. Inými slovami nemôžete miešať pravidlá rôznych **úrovní**.

Stĺpec **Počet uplatnení** zobrazuje počet úspešných uplatnení daného pravidla. Zrušením možnosti v stĺpci Aktívny deaktivujete dané pravidlo.



Kliknutím na **Vynulovať** môžete vynulovať počítadlo zásahov pre dané pravidlo (stĺpec **Počet uplatnení**). Kliknutím na **Zobraziť** môžete zobraziť konfiguráciu priradenú z ESET PROTECT politiky.

Dôležité:
Ak sú podmienky pravidla za normálnych okolností splnené, pravidlá s nižšou prioritou nie sú ďalej vyhodnocované. Avšak, ak je to potrebné, môžete použiť špeciálnu akciu pravidla nazvanú **Vyhodnotiť ďalšie pravidlá**, čo umožní pokračovanie vyhodnocovania.

- **Pridať** – pridanie nového pravidla.
- **Upraviť** – úprava existujúceho pravidla.
- **Zobraziť** – zobrazenie konfigurácie priradenej z ESET PROTECT politiky.
- **Odstrániť** – odstránenie zvoleného pravidla.
- **Hore** – posunutie zvoleného pravidla v zozname hore.
- **Dole** – posunutie zvoleného pravidla v zozname nadol.
- **Vynulovať** – vynulovanie počítadla zásahov pre dané pravidlo (stĺpec Počet uplatnení).

Poznámka:
Po pridaní nového pravidla alebo upravení existujúceho pravidla sa začne kontrola správ za pomoci nových/upravených pravidiel.

Sprievodca pravidlami

Podmienky a akcie môžete definovať pomocou Sprievodcu pravidlami. Najskôr nastavte podmienky, až potom akcie. Niektoré podmienky a akcie sú rozdielne pre pravidlá Filtrovania pri prístupe a pravidlá Manuálnej kontroly databáz. Je to z dôvodu, že každý typ ochrany používa trocha odlišný prístup, čo sa týka spracovávania pošty.

1. Kliknite na **Pridať** a zobrazí sa okno Podmienka pravidla umožňujúce vybrať podmienku pravidla,

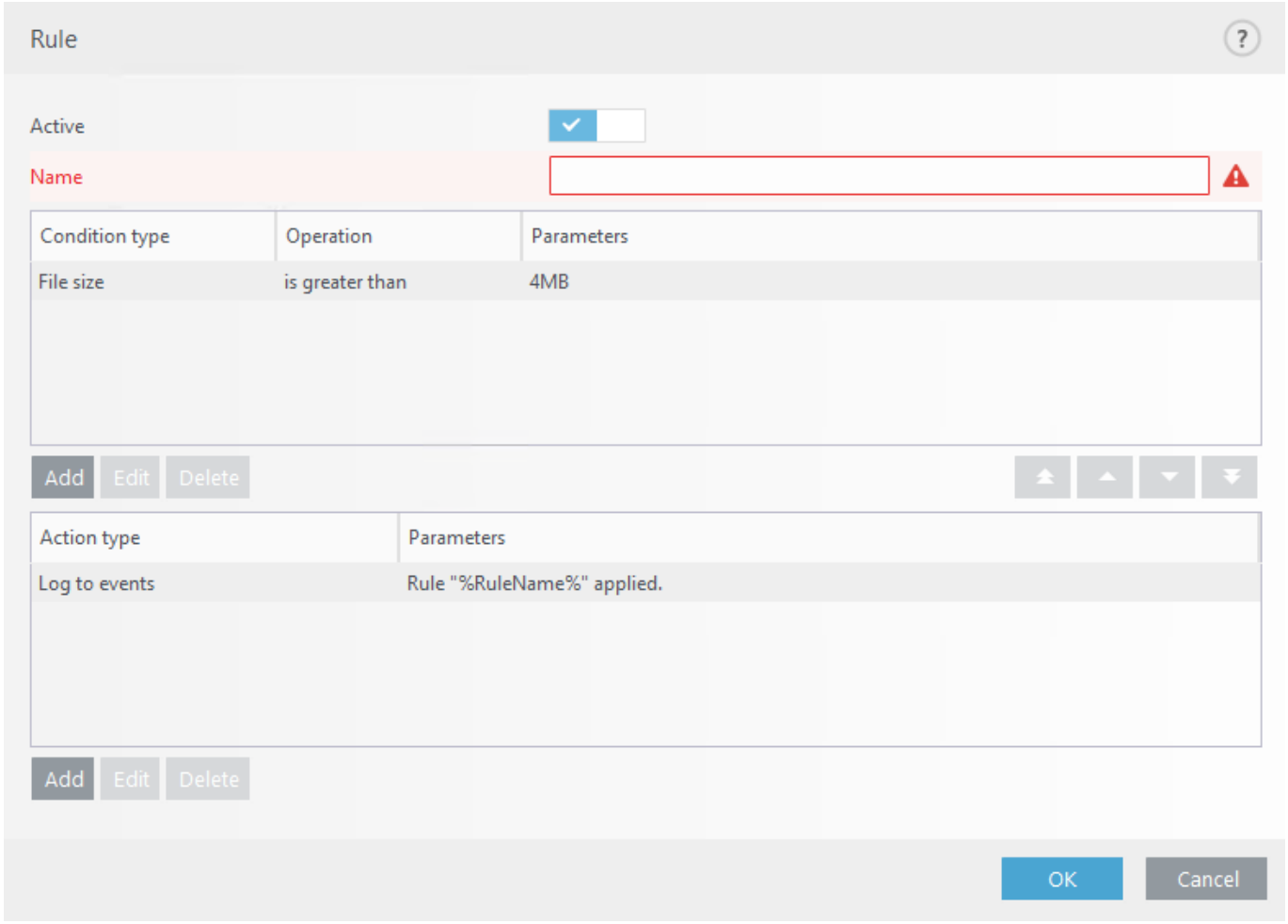
operáciu a hodnotu.

> Dôležité:
> Môžete zadefinovať viacero podmienok. Ak tak urobíte, všetky tieto podmienky musia byť splnené, aby bolo pravidlo aplikované. Všetky podmienky sú spojené pomocou logického operátora **AND**. Aj v prípade, že je väčšina podmienok splnená a hoci len jedna podmienka splnená nie je, výsledkom vyhodnotenia podmienok bude *not met*, čo znamená, že akcia pravidla nemôže byť vykonaná.

2.Kliknutím na tlačidlo **Pridať** (dole) pridajte Akciu pravidla.

> Poznámka:
> Pre jedno pravidlo je možné pridať viacero akcií.

3.Po zadefinovaní podmienok a akcií zadajte pre pravidlo **Názov** (názov podľa ktorého dané pravidlo ľahko rozpoznáte). Tento názov bude zobrazený v zozname pravidiel. Pole **Názov** musí byť vyplnené. Pokiaľ je pole zvýraznené červenou farbou, vpíšte doň názov pre pravidlo a následne kliknite na tlačidlo **OK** pre vytvorenie pravidla. Pole zostane označené červenou farbou aj po zadaní názvu pre pravidlo, až pokým nekliknete na tlačidlo **OK**.



4.Ak chcete pripraviť pravidlá, ktoré budete používať neskôr, môžete kliknúť na tlačidlo prepínača vedľa popisu **Aktívne**, čím pravidlo deaktivujete. Pre aktiváciu pravidla kliknite na začiarkavacie políčko v riadku daného pravidla v Zozname pravidiel.

Poznámka:
Po pridaní nového pravidla alebo upravení existujúceho pravidla sa začne kontrola správ za pomoci nových/upravených pravidiel.

Podmienka pravidla

Tento sprievodca vám umožňuje pridať podmienky pre pravidlá. Najskôr vyberte **Typ** podmienky a **Operáciu**. Zoznam operácií sa mení v závislosti od zvoleného typu podmienky. Následne vyberte **Parameter**. Pole parametra sa mení v závislosti od zvoleného typu a operácie. Vyberte **Veľkosť súboru** > **je viac ako** a do poľa **Parameter** zadajte 10 MB. Podľa týchto nastavení každý súbor väčší ako 10 MB spustí akciu, ktorú ste pre dané pravidlo nastavili. Z tohto dôvodu by ste mali určiť akciu, ktorá bude vykonaná, keď sa pravidlo aktivuje, ak ste tak ešte neurobili pri nastavovaní parametrov pre dané pravidlo.

Môžete tiež zadať **Regulárny výraz**; v tomto prípade ako **Operáciu** vyberte **sa zhoduje s regulárnym výrazom** alebo **sa nezhoduje s regulárnym výrazom**. ESET Security for Microsoft SharePoint používa std::regex. Pre tvorbu regulárnych výrazov si prezrite ECMAScript syntax.

Dôležité:
Môžete zadefinovať viacero podmienok. Ak tak urobíte, všetky tieto podmienky musia byť splnené, aby bolo pravidlo aplikované. Všetky podmienky sú spojené pomocou logického operátora **AND**. Aj v prípade, že je väčšina podmienok splnená a hoci len jedna podmienka splnená nie je, výsledkom vyhodnotenia podmienok bude *not met*, čo znamená, že akcia pravidla nemôže byť vykonaná.

Pre pravidlá Filtrovania pri prístupe alebo Manuálnej kontroly databáz sú dostupné nasledujúce typy podmienok (niektoré z uvedených možností sa z dôvodu skôr zvolených podmienok nemusia zobraziť):

Názov podmienky	Filtrovanie pri prístupe	Manuálna kontrola databáz	Popis
Názov súboru	☑	☑	Vzťahuje sa na súbory so zadaným názvom. Ak vyberiete túto podmienku, môžete určiť masku pre zadaný názov súboru. Pri zadávaní masky môžete použiť aj zástupné znaky (wildcards) *? atď. Táto podmienka sa vzťahuje len na názov súboru, bez ohľadu na cestu k súboru (cesta sa neberie do úvahy).
Veľkosť súboru	☑	☑	Vzťahuje sa na súbory, ktorých veľkosť prekračuje zadanú hodnotu. Ak vyberiete túto podmienku, môžete určiť maximálnu povolenú veľkosť súboru – v prípade, že veľkosť konkrétneho súboru presiahne stanovený limit, dôjde k uplatneniu pravidla.
URL súboru	☑	☑	Vzťahuje sa na súbory so zadanou URL adresou. Ak vyberiete túto podmienku, môžete určiť URL a masku pre zadaný názov súboru. Pri zadávaní masky môžete použiť aj zástupné znaky (wildcards) *? atď.
Typ súboru	☑	☑	Vzťahuje sa na súbory zadaného typu (typ súboru sa zisťuje na základe obsahu súboru, bez ohľadu na príponu či názov). Ak vyberiete túto podmienku, môžete označiť jeden alebo viacero typov súborov, pre ktoré bude uplatnené pravidlo. Kompletný zoznam rozpoznávaných typov súborov nájdete v tomto článku databázy znalostí.

Názov podmienky	Filtrovanie pri prístupe	Manuálna kontrola databáz	Popis
Čas poslednej zmeny	☑	☑	Vzťahuje sa na súbory, ktoré boli naposledy zmenené pred alebo po zadanom čase a dátume alebo v rozmedzí zadaných dátumov.
Výsledok antivírusovej kontroly	☑	☑	Vzťahuje sa na súbory, ktoré podľa výsledku antivírusovej kontroly buď sú alebo nie sú infikované.
Obsahuje archív chránený heslom	☑	☑	Vzťahuje sa na súbory v archíve chránenom heslom.
Obsahuje poškodený archív	☑	☑	Vzťahuje sa na súbory v poškodenom archíve (ak sa napríklad nedá otvoriť).
Upravené používateľom	☑	☑	Vzťahuje sa na súbory, ktoré boli naposledy menené zadaným používateľom.

Poznámka:
Počet použitých pravidiel v protokole o kontrole môže byť vyšší ako **Počet skontrolovaných objektov** pre pravidlá, ktoré obsahujú podmienku založenú na **Type súboru**. Takáto situácia môže nastať, ak sú medzi skontrolovanými objektmi archívy alebo tzv. kontajnery, ktoré vo svojom vnútri obsahujú ďalšie súbory (napríklad *.docx*). V takomto prípade sa pri každom vnútornom súbore preverí, či nepodlieha niektorému pravidlu s podmienkou založenou na **Type súboru**. Práve z tohto dôvodu môže **Počet použitých pravidiel** presiahnuť **Počet skontrolovaných objektov**.

Akcia pravidla

V tomto okne môžete určiť, aké akcie sa majú vykonať so súbormi, ktoré spĺňajú podmienky zadefinované v pravidlách.

Poznámka:
Pre jedno pravidlo je možné pridať viacero akcií.

Pre pravidlá Filtrovania pri prístupe alebo Manuálnej kontroly databáz sú dostupné nasledujúce akcie (niektoré z uvedených možností sa z dôvodu skôr zvolených akcií nemusia zobraziť):

Názov akcie	Filtrovanie pri prístupe	Manuálna kontrola databáz	Popis
Presunúť súbor do karantény	☑	☑	Súbor bude presunutý do karantény, a to aj v tom prípade, že antivírusová karanténa je vypnutá.
Vymazať	☑	☑	Súbor bude vymazaný z databázy.
Označiť na zmazanie	☑	☑	Pri pokuse o nahratie (upload) sa súbor nenahrá a bude vymazaný počas indexovania. Pri pokuse o stiahnutie (download) bude súbor označený na zmazanie.
Blokovať	☑	☑	Nahrávanie či sťahovanie súboru bude zablokované.
Poslať oznámenie o udalosti	☑	☑	Správcovi sa zašle oznámenie o udalosti. Je potrebné povoliť funkciu Posielať oznámenia o udalostiach e-mailom a následne môžete nastaviť formát správ o udalostiach (viac informácií nájdete v popise danej položky).

Názov akcie	Filtrovanie pri prístupe	Manuálna kontrola databáz	Popis
Vyhodnotiť ďalšie pravidlá	?	?	Umožňuje vyhodnocovanie ďalších pravidiel, čo dáva správcovi možnosť zadefinovať viacero podmienok a viacero akcií, ktoré sa vykonajú s ohľadom na podmienky. Ak je táto možnosť vypnutá, kontrola podľa ďalších pravidiel nebude prebiehať, antivírusová kontrola sa však bude vykonávať aj naďalej.
Zapísať do protokolu udalostí	?	?	Umožňuje zápis informácie o uplatnení pravidla do protokolu Udalosti. Môžete nastaviť úroveň závažnosti udalostí a určiť formát správ o udalostiach (viac informácií nájdete v popise danej položky).
Preskočiť antivírusovú kontrolu	?	?	Súbor nebude skontrolovaný antivírusovým jadrom.
Nevyhodnocovať iné pravidlá	?	?	Pri používaní tejto akcie budú vynechané všetky ďalšie pravidlá, ktoré by inak mali nasledovať.

Všeobecné nastavenia

V prípade potreby si môžete prispôsobiť všeobecné nastavenia podľa potreby. Ponuka na ľavej strane hlavného okna obsahuje nasledujúce sekcie:

Počítač

V tejto časti môžete aktivovať alebo deaktivovať detekciu potenciálne nechcených, nebezpečných alebo podozrivých aplikácií, ako aj ochranu Anti-Stealth. Môžete takisto definovať procesy, súbory a priečinky vylúčené z kontroly. Ďalej môžete nastaviť Rezidentnú ochranu súborového systému, ThreatSense parametre, Ochranu s podporou cloudu (ESET LiveGrid®), Detekciu malvéru (manuálna kontrola počítača a iné možnosti kontroly), kontrolu Hyper-V a HIPS.

Aktualizácia

Môžete nakonfigurovať možnosti aktualizácie, ako napr. profily, vek detekčného jadra, snímky (snapshot) pre vrátenie zmien modulov programu, typ aktualizácie, vlastný aktualizačný server, pripojenie/proxy server, aktualizačný mirror server, prístup k aktualizačným súborom, HTTP server, podrobnosti používateľského účtu pre sieťové pripojenie atď.

Web a e-mail

V tejto sekcii môžete nakonfigurovať filtrovanie protokolov a vylúčenia (vylúčené aplikácie a IP adresy), možnosti filtrovania protokolov SSL/TLS, ochranu e-mailových klientov (integrácia, e-mailové protokoly, upozornenia a udalosti), ochranu prístupu na web (webové protokoly HTTP/HTTPS a správa URL adries) a antiphishingovú ochranu.

Správa zariadení

Môžete povoliť integráciu a nastaviť pravidlá a skupiny v rámci správy zariadení.

Konfigurácia nástrojov

Môžete si prispôsobiť nástroje, ako napr. ESET CMD, ESET RMM, poskytovateľ WMI, ESET PROTECT ciele

kontroly, upozornenia o aktualizáciách systému Windows, protokoly, proxy server, e-mailové oznámenia, diagnostika, klaster atď.

Používateľské rozhranie

Táto sekcia vám umožňuje nastaviť správanie grafického používateľského rozhrania (GUI), stavy, licenčné údaje, upozornenia a udalosti, ochranu nastavení heslom, pravidlá spúšťania nástroja eShell atď.

Počítač

Detekčné jadro zabezpečuje ochranu pred nebezpečnými útokmi ohrozujúcimi systém. Zahŕňa kontrolu súborov, e-mailov a sieťovej komunikácie. V prípade zachytenia škodlivého objektu sa začne okamžitá oprava. Detekčné jadro dokáže infiltráciu eliminovať zablokovaním a následným vyliečením, odstránením alebo presunutím do karantény.

Rezidentná ochrana s využitím strojového učenia

Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu na základe strojového učenia. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov. Môžete nakonfigurovať úrovne hlásenia a ochrany pre tieto kategórie:

Malvér

Počítačový vírus je škodlivý kód pripojený k existujúcim súborom v 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. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne nechcené aplikácie

Potenciálne nechcená aplikácia je softvér, ktorého cieľ nie je jednoznačne škodlivý, avšak môže nainštalovať ďalší neželaný softvér, zmeniť správanie zariadenia, vykonávať neschválené alebo neočakávané operácie bez vedomia používateľa, prípadne mať iné nejasné ciele.
Táto kategória zahŕňa softvér zobrazujúci reklamu, softvér sťahujúci ďalší softvér, rôzne dodatočné panely s nástrojmi pre prehliadače, softvér so zavádzajúcim správaním, softvér, ktorý inštaluje ďalší softvér, softvér na sledovanie atď.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne podozrivé aplikácie

Podozrivá aplikácia je softvér, ktorý je skomprimovaný pomocou komprimačného nástroja alebo chrániacich nástrojov. Tieto aplikácie sú často používané na zabránenie reverznému inžinierstvu alebo na skrytie obsahu spustiteľných súborov (napr. malvéru), a to špeciálnymi metódami kompresie a/alebo šifrovania.
Táto kategória zahŕňa: všetky neznáme aplikácie, ktoré sú skomprimované komprimačnými nástrojmi alebo chrániacimi nástrojmi používanými na komprimáciu malvéru.

Potenciálne nebezpečné aplikácie

Toto označenie sa používa pre legitímny komerčný softvér, ktorý môže byť zneužitý. Potenciálne nebezpečné aplikácie predstavujú v prevažnej miere komerčný a legitímny softvér, avšak v nesprávnych rukách môže dôjsť k ich zneužitiu na nekalé účely.

Táto kategória predstavuje programy, akými sú napr. nástroje určené na prelomenie ochrany softvéru, generátory licenčných kľúčov, nástroje vzdialeného prístupu, aplikácie určené na prelomenie hesiel a keyloggery (program, ktorý zaznamenáva každé stlačenie klávesu používateľom). Táto možnosť je v predvolených nastaveniach zakázaná.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Pred úpravou prahu (alebo úrovne) v rámci kategórií Hlásenia alebo Ochrana si prečítajte nižšie uvedené informácie:

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Prah hlásení môžete nastaviť tak, aby lepšie vyhovoval vášmu prostrediu a vašim potrebám. Neexistuje len jedna správna konfigurácia. Preto vám odporúčame, aby ste monitorovali správanie vo svojom prostredí a rozhodli sa, či nie je pre vás vhodnejšie iné nastavenie Hlásení.

Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi, ale posunú informáciu príslušnej vrstve ochrany, ktorá primeraným spôsobom zakročí.

Prísne	**Hlásenia nastavené na maximálnu citlivosť. Hlásené sú viaceré detekcie. Hoci sa toto nastavenie môže javiť ako najbezpečnejšie, často býva príliš citlivé, čo môže mať presne opačný účinok.** Poznámka: Prísne nastavenie môže nesprávne identifikovať objekty ako škodlivé, pričom bude s týmito objektmi vykonaná príslušná akcia (podľa nastavení Ochrany).
Vyvážené	Toto nastavenie predstavuje optimálnu rovnováhu medzi výkonom a presnosťou detekcie a počtom nesprávne identifikovaných objektov.
Mierne	Hlásenia 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 s malvérovým správaním.
Vypnuté	Hlásenia nie sú aktívne. Detekcie nie sú nájdené, nahlásené ani vyliečené. Poznámka: Hlásenia malvéru nie je možné deaktivovať, a preto nie je pri malvéri k dispozícii možnosť **Vypnuté**.

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.

Ochrana

Ak je objekt nahlásený na základe vyššie uvedenej konfigurácie a výsledkov strojového učenia, bude zablokovaný a následne bude vykonaná príslušná akcia (liečenie, odstránenie alebo presunutie do karantény).

Prísne	**Detekcie zachytené pri prísnej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).**
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).

Prísne	**Detekcie zachytené pri prísnej (alebo nižšej) úrovni nastavenia sú zablokované a automaticky dochádza k procesu nápravy (t. j. k liečeniu).**
Vypnuté	Hlásenia nie sú aktívne, detekcie nie sú zachytávané, nahlásené ani vyliečené. Poznámka: Hlásenia malvéru nie je možné deaktivovať, a preto nie je k dispozícii možnosť **Vypnuté**.

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.

Poznámka:
Predvolene sa vyššie uvedené nastavenia ochrany s využitím strojového učenia vzťahujú aj na manuálnu kontrolu počítača. V prípade potreby je možné nakonfigurovať **Manuálnu kontrolu s využitím strojového učenia** samostatne. Kliknutím na prepínač vypnite možnosť **Použiť nastavenia rezidentnej ochrany** a pokračujte v konfigurácii.

Ochrana využívajúca strojové učenie

Detekčné jadro zabezpečuje ochranu pred nebezpečnými útokmi ohrozujúcimi systém. Zahŕňa kontrolu súborov, e□mailov a sieťovej komunikácie. V prípade zachytenia škodlivého objektu sa začne okamžitá oprava. Detekčné jadro dokáže infiltráciu eliminovať zablokovaním a následným vyliečením, odstránením alebo presunutím do karantény.

Rezidentná ochrana s využitím strojového učenia

Súčasťou detekčného jadra je teraz aj pokročilé strojové učenie – pokročilá vrstva ochrany, ktorá zlepšuje detekciu na základe strojového učenia. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov. Môžete nakonfigurovať úrovne hlásenia a ochrany pre tieto kategórie:

Malvér

Počítačový vírus je škodlivý kód pripojený k existujúcim súborom v 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. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne nechcené aplikácie

Potenciálne nechcená aplikácia je softvér, ktorého cieľ nie je jednoznačne škodlivý, avšak môže nainštalovať ďalší neželaný softvér, zmeniť správanie zariadenia, vykonávať neschválené alebo neočakávané operácie bez vedomia používateľa, prípadne mať iné nejasné ciele.
Táto kategória zahŕňa softvér zobrazujúci reklamu, softvér sťahujúci ďalší softvér, rôzne dodatočné panely s nástrojmi pre prehliadače, softvér so zavádzajúcim správaním, softvér, ktorý inštaluje ďalší softvér, softvér na sledovanie atď.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne podozrivé aplikácie

Podozrivá aplikácia je softvér, ktorý je skomprimovaný pomocou komprimačného nástroja alebo chrániacich nástrojov. Tieto aplikácie sú často používané na zabránenie reverznému inžinierstvu alebo na skrytie obsahu spustiteľných súborov (napr. malvéru), a to špeciálnymi metódami kompresie a/alebo

šifrovania.
Táto kategória zahŕňa: všetky neznáme aplikácie, ktoré sú skomprimované komprimačnými nástrojmi alebo chrániacimi nástrojmi používanými na komprimáciu malvéru.

Potenciálne nebezpečné aplikácie

Toto označenie sa používa pre legitímny komerčný softvér, ktorý môže byť zneužitý. Potenciálne nebezpečné aplikácie predstavujú v prevažnej miere komerčný a legitímny softvér, avšak v nesprávnych rukách môže dôjsť k ich zneužitiu na nekalé účely.
Táto kategória predstavuje programy, akými sú napr. nástroje určené na prelomenie ochrany softvéru, generátory licenčných kľúčov, nástroje vzdialeného prístupu, aplikácie určené na prelomenie hesiel a keyloggery (program, ktorý zaznamenáva každé stlačenie klávesu používateľom). Táto možnosť je v predvolených nastaveniach zakázaná.
Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Pred úpravou prahu (alebo úrovne) v rámci kategórií Hlásenia alebo Ochrana si prečítajte nižšie uvedené informácie:

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Prah hlásení môžete nastaviť tak, aby lepšie vyhovoval vášmu prostrediu a vašim potrebám. Neexistuje len jedna správna konfigurácia. Preto vám odporúčame, aby ste monitorovali správanie vo svojom prostredí a rozhodli sa, či nie je pre vás vhodnejšie iné nastavenie Hlásení.

Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi, ale posunú informáciu príslušnej vrstve ochrany, ktorá primeraným spôsobom zakročí.

Prísne	**Hlásenia nastavené na maximálnu citlivosť. Hlásené sú viaceré detekcie. Hoci sa toto nastavenie môže javiť ako najbezpečnejšie, často býva príliš citlivé, čo môže mať presne opačný účinok.** Poznámka: Prísne nastavenie môže nesprávne identifikovať objekty ako škodlivé, pričom bude s týmito objektmi vykonaná príslušná akcia (podľa nastavení Ochrany).
Vyvážené	Toto nastavenie predstavuje optimálnu rovnováhu medzi výkonom a presnosťou detekcie a počtom nesprávne identifikovaných objektov.
Mierne	Hlásenia 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 s malvérovým správaním.
Vypnuté	Hlásenia nie sú aktívne. Detekcie nie sú nájdené, nahlásené ani vyliečené. Poznámka: Hlásenia malvéru nie je možné deaktivovať, a preto nie je pri malvéri k dispozícii možnosť **Vypnuté**.

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.

Ochrana filtra prístupu s využitím strojového učenia

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi (to je úloha príslušnej ochrannej vrstvy).

Ochrana

Konfiguráciou parametrov v sekcii Filtrovanie pri prístupe určíte, čo sa stane so zachytenými objektmi.

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.

Nakonfigurujte ochranu využívajúcu strojové učenie pomocou eShell. Názov kontextu v eShell je **MLP**. Otvorte eShell v interaktívnom režime a prejdite na MLP:

```
server av transport mlp
```

Pozrite si aktuálne nastavenie hlásení pre podozrivé aplikácie:

```
get suspicious-reporting
```

Ak chcete, aby boli hlásenia menej prísne, zmeňte nastavenia na Mierne:

```
set suspicious-reporting cautious
```

Manuálna kontrola databáz s využitím strojového učenia

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi (to je úloha príslušnej ochrannej vrstvy).

Ochrana

Konfiguráciou parametrov v sekcii Manuálna kontrola databáz určíte, čo sa stane so zachytenými objektmi.

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.

Nakonfigurujte ochranu využívajúcu strojové učenie pomocou eShell. Názov kontextu v eShell je **MLP**. Otvorte eShell v interaktívnom režime a prejdite na MLP:

```
server av transport mlp
```

Pozrite si aktuálne nastavenie hlásení pre podozrivé aplikácie:

```
get suspicious-reporting
```

Ak chcete, aby boli hlásenia menej prísne, zmeňte nastavenia na Mierne:

```
set suspicious-reporting cautious
```

Vylúčenia

Vylúčenia umožňujú nastaviť súbory a priečinky, ktoré nemajú byť kontrolované. Aby bola zaručená kontrola všetkých objektov na prítomnosť hrozieb, neodporúčame túto možnosť používať, ak to nie je naozaj nevyhnutné. Môžu však nastať situácie, keď je potrebné vylúčiť niektoré objekty z kontroly. Medzi takéto situácie patrí napríklad kontrola veľkých databázových súborov, ktorá môže spomaliť kontrolu servera, prípadne sa môže stať, že je softvér v konflikte s priebehom kontroly (napríklad zálohovací softvér).

Upozornenie:
Je potrebné nemýliť si vylúčenia s vylúčenými príponami, vylúčeniami procesov a filtrom vylúčení.

Poznámka:
Hrozba v súbore nebude detegovaná modulmi Rezidentná ochrana súborového systému a Kontrola počítača, pokiaľ súbor spĺňa kritéria pre vylúčenie z kontroly.

Ak chcete pridať nové alebo upraviť existujúce vylúčenie, vyberte typ vylúčenia a kliknite na **Upraviť**.

- Výkonnostné vylúčenia – umožňujú vylúčiť z kontroly súbory a priečinky.
- Vylúčenia detekcií – pomocou špecifických kritérií (cesta, hodnota hash súboru alebo názov detekcie) umožňujú vylúčiť z kontroly konkrétne objekty.

Výkonnostné vylúčenia

Táto funkcia umožňuje nastaviť súbory a priečinky, ktoré nemajú byť kontrolované. Výkonnostné vylúčenia sú užitočné na vylúčenie kontroly kritických aplikácií na úrovni súborov, prípadne vtedy, keď kontrola spôsobuje abnormálne správanie systému alebo znižuje jeho výkon.

Cesta

Bude vylúčená konkrétna cesta (súbor alebo adresár) pre tento počítač. Nepoužívajte zástupné znaky – hviezdičku (*) – v strede cesty. Viac informácií nájdete v nasledujúcom článku Databázy znalostí.

Poznámka:
Ak chcete vylúčiť obsah priečinka, nezabudnite pridať hviezdičku (*) na koniec cesty (*C:\Tools**).
Umiestnenie *C:\Tools* nebude vylúčené, pretože z pohľadu skenera môže *Tools* predstavovať aj názov súboru.

Poznámka

Pridajte voliteľnú **poznámku**, aby ste vylúčenie v budúcnosti ľahko rozpoznali.

Príklad:
Vylúčenia ciest s použitou hviezdičkou:
*C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (*), aby bolo zrejmé, že vylúčený má byť priečinok a celý jeho obsah (súbory a podpriečinky).
C:\Tools.** – rovnaké správanie ako v prípade *C:\Tools**, čo znamená, že ide o rekurzívnu funkcionalitu.
C:\Tools.dat* – budú vylúčené súbory *dat* v priečinku Tools.
C:\Tools\sg.dat – bude vylúčený tento konkrétny súbor nachádzajúci sa v danom umiestnení.

Príklad:
Ak chcete vylúčiť v zvolenom priečinku všetky súbory, zadajte cestu k priečinku a použite masku „*.*“.
• Na vylúčenie všetkých súborov .doc použite masku „*.doc“.
• Ak má názov spustiteľného súboru určitý počet znakov a vy presne neviete, ktoré znaky to sú (poznáte len začiatočný znak, napríklad „D“), použite nasledujúci tvar:
D????.exe (otázniky zastupujú chýbajúce/neznáme znaky).

Príklad:
Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné, ako napr. *%PROGRAMFILES%*.
• Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%*\ (nezabudnite na spätnú lomku na konci).
• Na vylúčenie všetkých súborov v konkrétnom podadresári v rámci *%HOMEDRIVE%* použite cestu *%HOMEDRIVE%**Excluded_Directory**.*.
Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Systémové premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*) nie sú podporované.

Vylúčenia detekcií

Predstavujú ďalší spôsob vylúčenia objektov z kontroly, a to pomocou názvu detekcie, cesty alebo hodnoty hash. Vylúčenia detekcií neumožňujú vylúčiť z kontroly súbory a priečinky (na rozdiel od výkonnostných vylúčení). Vylúčenia detekcií umožňujú vylúčiť objekty len vtedy, keď sú zachytené detekčným jadrom a zoznam vylúčení obsahuje príslušné pravidlo.

Vylúčenie založené na detekcii sa dá najjednoduchšie vytvoriť pomocou existujúcej detekcie v sekcii **Protokoly** > Detekcie. Pravým tlačidlom myši kliknite na záznam protokolu (detekciu) a potom na **Vytvoriť vylúčenie**. Otvorí sa sprievodca vylúčeniami s preddefinovanými kritériami.

Ak chcete vytvoriť vylúčenie detekcie manuálne, kliknite na **Upraviť** > **Pridať** (alebo **Upraviť** v prípade existujúceho vylúčenia) a uveďte aspoň jedno z nasledujúcich kritérií (kritériá možno kombinovať):

Cesta

Bude vylúčená konkrétna cesta (súbor alebo adresár). Konkrétne umiestnenie alebo súbor môžete vyhľadať v počítači alebo zadajte reťazec manuálne. Nepoužívajte zástupné znaky – hviezdičku (*) – v strede cesty. Viac informácií nájdete v nasledujúcom článku Databázy znalostí.

Poznámka:
Ak chcete vylúčiť obsah priečinka, nezabudnite pridať hviezdičku (*) na koniec cesty (*C:\Tools**).
Umiestnenie *C:\Tools* nebude vylúčené, pretože z pohľadu skenera môže *Tools* predstavovať aj názov súboru.

Hash

Môžete vylúčiť súbor na základe konkrétnej hodnoty hash (SHA1) bez ohľadu na typ súboru, jeho umiestnenie, názov alebo príponu.

Názov detekcie

Zadajte platný názov detekcie (hrozby). Vytvorenie vylúčenia len na základe názvu detekcie môže predstavovať bezpečnostné riziko. Odporúčame vám skombinovať názov detekcie s cestou. Toto kritérium vylúčenia možno použiť len pre niektoré typy detekcií.

Poznámka

Pridajte voliteľnú **poznámku**, aby ste vylúčenie v budúcnosti ľahko rozpoznali.

ESET PROTECT zahŕňa správu vylúčení detekcií, pomocou ktorej môžete vytvoriť vylúčenia detekcií a aplikovať ich na viacerých počítačoch/skupinách.

Použite zástupné znaky na pokrytie skupiny súborov. Otáznik (*?*) predstavuje jeden ľubovoľný znak a hviezdička (***) predstavuje ľubovoľnú postupnosť znakov.

Príklad:
Vylúčenia ciest s použitou hviezdičkou:
*C:\Tools** – cesta musí končiť spätnou lomkou (\) a hviezdičkou (***), aby bolo zrejmé, že vylúčený má byť priečinok a celý jeho obsah (súbory a podpriečinky).
C:\Tools.** – rovnaké správanie ako v prípade *C:\Tools**, čo znamená, že ide o rekurzívnu funkcionalitu.
C:\Tools.dat* – budú vylúčené súbory *dat* v priečinku Tools.
C:\Tools\sg.dat – bude vylúčený tento konkrétny súbor nachádzajúci sa v danom umiestnení.

Príklad:
Ak chcete vylúčiť hrozbu, zadajte platný názov detekcie v nasledujúcom formáte:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

Príklad:
Ak chcete vylúčiť v zvolenom priečinku všetky súbory, zadajte cestu k priečinku a použite masku „**.**“.
- Na vylúčenie všetkých súborov .doc použite masku „**.doc*“.
- Ak má názov spustiteľného súboru určitý počet znakov a vy presne neviete, ktoré znaky to sú (poznáte len začiatočný znak, napríklad „D“), použite nasledujúci tvar:

D????.exe (otázniky zastupujú chýbajúce/neznáme znaky).

Príklad:
Pri vytváraní vylúčení z kontroly môžete použiť aj systémové premenné, ako napr. *%PROGRAMFILES%*.
• Ak chcete vylúčiť celý priečinok Program Files pomocou príslušnej systémovej premennej, použite pri vytváraní vylúčenia cestu *%PROGRAMFILES%*\ (nezabudnite na spätnú lomku na konci).
• Na vylúčenie všetkých súborov v konkrétnom podadresári v rámci *%HOMEDRIVE%* použite cestu *%HOMEDRIVE%**Excluded_Directory**.*.
Vo formáte vylúčenia cesty je možné používať nasledujúce premenné:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Systémové premenné špecifické pre používateľa (ako *%TEMP%* alebo *%USERPROFILE%*) alebo premenné prostredia (ako *%PATH%*) nie sú podporované.

Sprievodca vytvorením vylúčenia

Odporúčané vylúčenie je prednastavené na základe typu detekcie, môžete však bližšie špecifikovať kritériá vylúčenia pre detekcie. Kliknite na **Zmeniť kritériá**:

- **Konkrétne súbory** – vylúči sa každý súbor podľa jeho hodnoty SHA-1 hash.
- **Detekcia** – na základe uvedeného názvu detekcie sa vylúči každý súbor, ktorý obsahuje túto detekciu.
- **Cesta + detekcia** – na základe uvedeného názvu detekcie a cesty (vrátane názvu súboru) sa vylúči každý súbor obsahujúci detekciu v uvedenom umiestnení.

Pridajte voliteľnú **poznámku**, aby ste vylúčenie v budúcnosti ľahko rozpoznali.

Pokročilé možnosti

Technológia Anti-Stealth

Technológia Anti-Stealth predstavuje sofistikovaný systém detekcie nebezpečných programov, ako sú napr. rootkity, ktoré sa dokážu skryť pred operačným systémom. Preto ich nie je možné detegovať pomocou bežných techník kontroly.

AMSI

Po povolení tejto možnosti bude Microsoft Antimalware Scan Interface (AMSI) kontrolovať skripty Powershell spúšťané cez Windows Script Host.

Automatické vylúčenia

Vývojári aplikácií a operačných systémov určených pre servery často odporúčajú z antimalvérovej kontroly vylúčiť niektoré kriticky dôležité súbory a adresáre daných serverových produktov. Antimalvérová kontrola môže mať totiž negatívny dopad na výkon servera, čo môže viesť k tvorbe konfliktov alebo zamedzeniu spustenia niektorých aplikácií. Vylúčenie potrebných súborov z kontroly pomáha minimalizovať riziko potenciálnych konfliktov a zvýšiť celkový výkon servera pri používaní antimalvérovej ochrany. Prezrite si kompletný zoznam súborov vylúčených z kontroly pre serverové produkty spoločnosti ESET.

ESET Security for Microsoft SharePoint automaticky identifikuje kritické aplikácie a súbory operačného systému servera a pridá ich do zoznamu vylúčení. Automatické vylúčenia sú v predvolených nastaveniach povolené. Kliknutím na prepínač môžete povoliť/zakázať automatické vylúčenia pre konkrétnu serverovú aplikáciu alebo systém, pričom výsledok bude takýto:

- Ak sú automatické vylúčenia povolené, príslušné kritické súbory a priečinky budú pridané do zoznamu súborov vylúčených z kontroly. Po každom reštarte servera vykoná systém automatickú kontrolu vylúčení a aktualizuje zoznam v prípade, že došlo k zmenám v systéme alebo aplikáciách (napríklad pri inštalácii novej serverovej aplikácie). Toto nastavenie zabezpečí, že budú vždy použité všetky odporúčané automatické vylúčenia.

- Ak sú automatické vylúčenia vypnuté, automaticky vylúčené súbory a priečinky budú odstránené zo zoznamu. Vylúčenia definované manuálne nebudú ovplyvnené.

Na identifikáciu a vygenerovanie automatických vylúčení používa ESET Security for Microsoft SharePoint vyhradenú aplikáciu *eAutoExclusions.exe*, ktorá je umiestnená v inštalačnom priečinku. Zo strany používateľa nie je potrebná žiadna interakcia, môžete si však pomocou príkazového riadka zobraziť zoznam detegovaných serverových aplikácií vo vašom systéme spustením príkazu `eAutoExclusions.exe -servers`. Ak chcete vidieť celú syntax, použite `eAutoExclusions.exe -?`.

Zdieľaná lokálna vyrovnávacia pamäť

Zdieľaná lokálna vyrovnávacia pamäť ESET zvyšuje výkon vo virtuálnych prostrediach tým, že predchádza duplicitnej kontrole na sieti. Každý súbor bude kontrolovaný len raz a uložený v lokálnej vyrovnávacej pamäti. Povoľte možnosť **Používanie vyrovnávacej pamäte**, aby sa informácie o kontrolovaných súboroch a priečinkoch na sieti ukladali do vyrovnávacej pamäte. Pri novej kontrole bude ESET Security for Microsoft SharePoint hľadať kontrolované súbory vo vyrovnávacej pamäti. Ak nájde zhodné súbory, vylúči ich z kontroly.

Nastavenia servera vyrovnávacej pamäte obsahujú nasledovné:

- **Názov hostiteľa** – názov alebo IP adresa počítača, na ktorom sa nachádza vyrovnávacia pamäť.
- **Port** – číslo portu použitého na komunikáciu (rovnaké ako pri zdieľanej lokálnej vyrovnávacej pamäti).
- **Používateľské heslo** – špecifikujte heslo pre zdieľanú lokálnu vyrovnávaciu pamäť, ak je to potrebné.

Našla sa infiltrácia

Infiltrácie sa môžu do PC dostať z rôznych zdrojov: z webových stránok, zo zdieľaných adresárov, prostredníctvom e-mailu, z vymeniteľných zariadení počítača (USB kľúče, externé disky, CD/DVD atď.).

Štandardné správanie

V programe ESET Security for Microsoft SharePoint môžu byť infiltrácie zachytené prostredníctvom nasledujúcich modulov:

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

Každá z týchto funkcií má prednastavenú štandardnú úroveň liečenia a pokúsi sa súbor buď vyliečiť a presunúť do karantény, alebo ukončiť pripojenie. Notifikácie sa zobrazujú v paneli oznámení v pravej dolnej časti obrazovky. Viac informácií o jednotlivých úrovniach liečenia a správaní nájdete v kapitole Liečenie.

Liečenie a mazanie

Ak rezidentná ochrana súborového systému nemá prednastavenú žiadnu 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, keďže infiltrácia tým pádom zostáva na svojom pôvodnom mieste a naďalej predstavuje potenciálnu hrozbu. Výnimkou je, ak máte úplnú istotu, že daný súbor bol ako infiltrácia detegovaný omylom.

Liečenie súboru sa dá aplikovať v prípade, že do zdravého súboru bola zavedená časť, ktorá obsahuje škodlivý kód. V tomto prípade má zmysel pokúsiť sa infikovaný súbor liečiť a získať tak späť pôvodný zdravý súbor. V prípade, že infiltráciou je súbor, ktorý obsahuje výlučne škodlivý kód, bude tento odstránený.

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

Viaceré hrozby

Ak niektoré infikované súbory neboli vyliečené počas kontroly počítača (alebo úroveň liečenia bola nastavená na **Neliečiť**), zobrazí sa okno, ktoré vás vyzve, aby ste vybrali akciu pre dané súbory. Vyberte akciu individuálne pre každú hrozbu v zozname alebo môžete tiež použiť možnosť **Vybrať akciu pre všetky hrozby v zozname** a vybrať jednu akciu, ktorá bude použitá pre všetky hrozby v zozname. Potom kliknite na **Dokončiť**.

Mazanie súborov v archívoch

Pri predvolenej úrovni liečenia je archív zmazaný iba v prípade, že obsahuje len infikované súbory. Archív nebude zmazaný, ak okrem infiltrácie obsahuje aj neškodné neinfikované súbory. Pri nastavení prísnej úrovne liečenia treba byť opatrný – v tomto prípade bude archív vymazaný bez ohľadu na to, či jeho obsah tvoria aj neinfikované súbory.

Rezidentná ochrana súborového systému

Rezidentná ochrana súborového systému kontroluje v systéme všetky udalosti súvisiace s malvérom. Všetky súbory, ktoré sa v počítači otvárajú, vytvárajú alebo spúšťajú, sú kontrolované na prítomnosť škodlivého kódu. Rezidentná ochrana súborového systému sa predvolene spúšťa pri štarte systému a poskytuje nepretržitú kontrolu. V špeciálnych prípadoch (napr. ak dôjde ku konfliktu s inou rezidentnou ochranou) je možné rezidentnú ochranu zastaviť zrušením výberu možnosti **Automatický štart rezidentnej ochrany súborového systému** v **Rozšírených nastaveniach** (**F5**) v sekcii **Rezidentná ochrana súborového systému** > **Základné**.

ESET Security for Microsoft SharePoint je kompatibilný so servermi využívajúcimi Azure File Sync agenta s povoleným vrstvením cloudu (cloud tiering). ESET Security for Microsoft SharePoint rozpoznáva súbory s

atribútom *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Vykonávať kontrolu týchto médií

Predvolene je nastavená kontrola všetkých typov médií:

- **Lokálne disky** – všetky pevné disky v počítači.
- **Vymeniteľné médiá** – CD/DVD, USB kľúče, zariadenia Bluetooth atď.
- **Sieťové disky** – všetky namapované disky.

Odporúčame používať predvolené nastavenia kontroly všetkých médií a meniť ich iba v špecifických prípadoch, napríklad keď pri kontrole určitého média dochádza k výraznému spomaleniu prenosu dát.

Vykonávať kontrolu pri týchto udalostiach

Predvolene sa súbory kontrolujú pri otváraní, vytváraní a spúšťaní. Odporúčame vám nemeniť tieto predvolené nastavenia, pretože tak je zabezpečená maximálna úroveň rezidentnej ochrany vášho počítača.

- **Otvorenie súboru** – kontrola prebieha pri otvorení súborov alebo pri prístupe k súborom.
- **Vytvorenie súboru** – kontrola prebieha pri vytváraní alebo úprave súborov.
- **Spustenie súboru** – kontrola prebieha pri spustení súborov.
- **Prístup na vymeniteľné médiá** – kontrola prebieha pri prístupe k vymeniteľným médiám. Po vložení alebo pripojení vymeniteľného média so zavádzacím sektorom bude tento zavádzací sektor okamžite skontrolovaný. Táto možnosť neumožňuje kontrolu súborov na vymeniteľnom médiu. Nastavenia kontroly súborov na vymeniteľnom médiu sú dostupné v sekcii **Vykonávať kontrolu týchto médií** > **Vymeniteľné médiá**. Prístup k zavádzaciemu sektoru vymeniteľného média bude možný, len ak zapnete funkciu **Zavádzacie sektory/UEFI** v sekcii Parametre ThreatSense.

Vylúčenia procesov

Vylúčenia procesov umožňujú vylúčenie konkrétneho procesu z kontroly. Napríklad proces zálohy dát, pri ktorom sú všetky operácie so súbormi ignorované, sa považuje za bezpečné riešenie, pričom sa minimalizuje možné riziko prerušenia zálohovania pri ich kontrole.

Parametre ThreatSense

Rezidentná ochrana súborového systému kontroluje všetky typy médií a aktivuje sa pri rôznych systémových udalostiach, napríklad pri prístupe k súboru. Rezidentná ochrana súborového systému môže byť nastavená tak, aby pracovala s novovytvorenými súbormi iným spôsobom, ako v prípade už dlhšie existujúcich súborov. Napríklad pri novovytvorených súboroch je možné nastaviť hlbšiu úroveň kontroly.

Na zabezpečenie minimálnych systémových nárokov pri použití rezidentnej ochrany nie sú súbory, ktoré už boli skontrolované, opakovane kontrolované (pokiaľ neboli zmenené). Súbory sú ihneď kontrolované znova po každej aktualizácii detekčného jadra. Toto správanie je kontrolované pomocou **Smart optimalizácie**. Pokiaľ je **Smart optimalizácia** zakázaná, všetky súbory sú kontrolované vždy, keď sa k nim pristupuje. Ak chcete túto možnosť zmeniť, stlačením **F5** otvorte **Rozšírené nastavenia** a kliknite na **Počítač** > **Rezidentná ochrana súborového systému**. Následne kliknite na **Parametre ThreatSense** > **Iné** a zapnite alebo vypnite možnosť **Zapnúť Smart optimalizáciu**.

Doplňujúce parametre ThreatSense

Podrobné nastavenia môžete konfigurovať v sekcii **Doplňujúce parametre ThreatSense pre vytvárané a menené súbory** a **Doplňujúce parametre ThreatSense pre spúšťané súbory**.

Parametre ThreatSense

ThreatSense je názov technológie, ktorú tvorí súbor komplexných metód detekcie infiltrácie. Táto technológia je proaktívna, poskytuje ochranu aj počas prvých hodín šírenia novej hrozby. Na odhalenie hrozieb využíva kombináciu niekoľkých metód (analýza kódu, emulácia kódu, generické signatúry, vírusové signatúry), čím efektívne spája ich výhody. Detekčné jadro je schopné kontrolovať niekoľko dátových tokov paralelne a maximalizovať tak svoj výkon a účinnosť detekcie. ThreatSense technológia dokáže účinne bojovať aj s rootkitmi.

> Poznámka:
> Podrobnejšie informácie o automatickej kontrole po štarte nájdete v kapitole Kontrola pri štarte.

ThreatSense nastavenia umožňujú nastavenie viacerých parametrov kontroly:

- **Výber typu súborov a prípon, ktoré si želáte kontrolovať.**
- **Výber kombinácie rôznych metód detekcie.**
- **Výber úrovne liečenia a pod.**

Pre zobrazenie okna s parametrami kliknite na **Nastavenie parametrov jadra ThreatSense** v **Rozšírených nastaveniach** (**F5**) príslušných modulov využívajúcich technológiu ThreatSense (pozrite nižšie). Pre rôzne druhy ochrany sa používa rôzna úroveň nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

- Filtrovanie pri prístupe
- Manuálna kontrola databáz
- Kontrola Hyper-V
- Rezidentná ochrana súborového systému
- Detekcia malvéru
- Kontrola v nečinnosti
- Kontrola pri štarte
- Ochrana dokumentov
- Ochrana e-mailových klientov
- Ochrana prístupu na web

ThreatSense parametre sú pre každý modul odlišné. Ich zmena môže mať v určitom stave značný vplyv na celkový výkon systému. Príkladom môže byť spomalenie systému pri povolení kontroly runtime archívov a pokročilej heuristiky pre rezidentnú ochranu súborov (súbory sú touto kontrolou skontrolované iba ak sú novovytvorené). Preto odporúčame ponechať pôvodné nastavenia ThreatSense pre všetky druhy 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

Kontroluje prítomnosť hrozieb, ktoré útočia na operačnú pamäť systému.

Zavádzacie sektory/UEFI

Kontrola zavádzacích sektorov na prítomnosť vírusov v tzv. zavádzači operačného systému (MBR). V prípade

virtuálneho počítača vytvoreného v prostredí Hyper-V bude MBR disku tohto počítača kontrolovaný v režime iba na čítanie.

E-mailové súbory

Program podporuje nasledujúce prípony: DBX (Outlook Express) a EML súbory.

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 iné.

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 rozbalia po spustení v pamäti počítača. Okrem podpory štandardných statických archívov (UPX, yoda, ASPack, FSG atď.) program podporuje vďaka emulácii kódu aj veľa iných typov archívov.

Možnosti kontroly

V sekcii Možnosti kontroly môžete upraviť nastavenia pokročilých metód detekcie používaných pri kontrole systému na prítomnosť infiltrácií. Na výber sú tieto možnosti:

Heuristika

Heuristika je algoritmus, ktorý analyzuje aktivitu aplikácií. Výhodou heuristiky je schopnosť odhaliť aj taký škodlivý softvér, ktorý v dobe poslednej aktualizácie detekčného jadra programu ešte neexistoval alebo nebol známy.

Pokročilá heuristika/DNA vzorky

Pokročilá heuristika je jedinečný algoritmus heuristiky vyvinutý spoločnosťou ESET, ktorý je optimalizovaný na odhaľovanie počítačových červov a trójskych koní písaných vo vyšších programovacích jazykoch. Použitie pokročilej heuristiky značne zvyšuje možnosti rozpoznávania hrozieb. Vzorky umožňujú spoľahlivo nájsť a pomenovať nové vírusy. Vďaka pravidelnej aktualizácii sú čerstvé vzorky k dispozícii zvyčajne už o niekoľko hodín. Nevýhodou je, že táto metóda odhaľuje iba známe vírusy alebo ich čiastočne pozmenené verzie.

Liečenie

Nastavenia liečenia určujú správanie kontroly pri liečení infikovaných súborov. Sú dostupné tri úrovne liečenia:

Neliečiť

Infikované súbory sa nebudú automaticky liečiť. Používateľovi sa pri detekcii zobrazí varovné okno s možnosťou výberu akcie, ktorá sa má vykonať. Táto úroveň liečenia je určená pre pokročilých používateľov,

ktorí vedia ako postupovať pri infiltráciách.

Normálne liečenie

Program sa pokúsi infikované súbory automaticky liečiť alebo zmazať na základe prednastavenej akcie (v závislosti od typu infiltrácií). Detekcia a vymazanie infikovaného súboru je oznámená notifikáciou v pravom dolnom rohu obrazovky. Ak program nevie vybrať správnu akciu automaticky, zobrazí sa varovné okno s možnosťou výberu akcie. Možnosť výberu akcie sa zobrazí aj v momente, keď sa predvolenú akciu nepodarí vykonať.

Prísne liečenie

Program vylieči alebo zmaže všetky infikované súbory. Výnimku tvoria systémové súbory. Ak nie je možné vyliečiť súbor, používateľ bude vyzvaný, aby zvolil akciu, ktorá bude vykonaná.

Upozornenie:
Pri detekcii infiltrácie v archívnom súbore sú dve možnosti. Pri prednastavenom **Normálnom liečení** bude archívny súbor zmazaný len v prípade, že všetky súbory, ktoré obsahuje, sú infikované. Pri **Prísnom liečení** bude komprimovaný súbor (archív) zmazaný v prípade, že obsahuje čo len jeden infikovaný súbor bez ohľadu na to, v akom stave sú ostatné súbory.

Dôležité:
Ak je hostiteľ Hyper-V spustený na systéme Windows Server 2008 R2 SP1, **Normálne liečenie** a **Prísne liečenie** nie sú podporované. Kontrola diskov virtuálnych počítačov prebieha v režime „iba na čítanie“, pričom nebude vykonané žiadne liečenie. Kontrola je vždy vykonávaná v režime iba na čítanie bez ohľadu na to, aká úroveň liečenia je zvolená.

Vylúčenia

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ a obsah súboru. V tejto časti nastavení ThreatSense parametrov môžete zadefinovať, ktoré typy súborov budú vylúčené z kontroly.

Iné

V časti Kontrola počítača a sekcii ThreatSense parametre sa nachádzajú aj nasledujúce možnosti v sekcii **Iné**:

Kontrolovať alternatívne dátové prúdy (ADS)

Alternatívne dátové prúdy používané súborovým systémom NTFS sú asociácie súborov a priečinkov, ktoré sú neviditeľné pre bežné techniky kontroly. Veľký počet vírusov ich preto využíva na svoje maskovanie pred prípadným odhalením.

Kontroly na pozadí vykonávať s nízkou prioritou

Každá kontrola počítača využíva nezanedbateľný výkon počítača. Ak pracujete s programami, ktoré do vysokej miery zaťažujú systém, môžete aktivovať kontrolu na pozadí s nízkou prioritou a uvoľniť tak prostriedky pre svoje aplikácie.

Zapisovať všetky objekty do protokolu

Ak je povolená táto možnosť, v protokole kontroly budú zobrazené všetky skontrolované súbory vrátane tých, ktoré sú bezpečné.

Zapnúť Smart optimalizáciu

Pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia pre 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

Obmedzenia určujúce hranice veľkostí objektov a archívov, ktoré sa budú testovať na prítomnosť vírusov:

Predvolené nastavenie objektov

Budú použité predvolené nastavenia (bez obmedzení). ESET Security for Microsoft SharePoint bude ignorovať vaše vlastné nastavenia.

Maximálna veľkosť objektu

Určuje maximálnu veľkosť kontrolovaných objektov. Daný modul ochrany bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame modifikovať len pokročilým používateľom, ktorí chcú veľké objekty vylúčiť z kontroly. Predvolená hodnota: neobmedzená.

Maximálny čas kontroly objektu (v sekundách)

Definuje maximálny povolený čas pre kontrolu objektov. Ak používateľ definuje určitú hodnotu, potom modul ochrany pri kontrole objektu po prekročení tejto hodnoty skončí prebiehajúcu kontrolu bez ohľadu na kompletnosť kontroly. Predvolená hodnota: neobmedzená.

Nastavenie kontroly archívov

Pre zmenu kontroly archivovaných súborov zrušte výber možnosti **Predvolené nastavenie kontroly archívov**.

Úroveň vnorenia archívov

Určuje maximálnu hĺbku kontroly archívov. Predvolená hodnota: 10. Pre objekty detegované Ochranou prenosu e-mailov je potrebná úroveň vnorenia +1. Prvá úroveň je totiž samotný e-mail.

> Príklad:
> Ak máte úroveň vnorenia nastavenú na 3, archív s úrovňou vnorenia 3 bude kontrolovaný na prenosovej vrstve len po úroveň 2. Preto ak chcete mať archívy kontrolované Ochranou prenosu e-mailov po úroveň 3, nastavte hodnotu pre **Úroveň vnorenia archívov** na 4.

Maximálna veľkosť súboru v archíve

Táto možnosť vám dovolí nastaviť maximálnu veľkosť kontrolovaných súborov obsiahnutých v archívoch (po rozbalení). Predvolená hodnota: neobmedzená.

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

Doplňujúce parametre ThreatSense

Doplňujúce parametre ThreatSense pre vytvárané a menené súbory

Pravdepodobnosť infikovania novovytvorených alebo menených súborov je vyššia ako u existujúcich súborov. To je dôvod, prečo program tieto súbory kontroluje s prídavnými parametrami. Spolu s kontrolou založenou na porovnávaní vzoriek sa využíva pokročilá heuristika, vďaka ktorej možno zachytiť nové hrozby skôr ako vyjde aktualizácia modulov. Okrem novovytvorených súborov sa kontrolujú aj samorozbaľovacie súbory (.sfx) a runtime archívy (interne komprimované spustiteľné súbory). Predvolene sa archívy kontrolujú do desiatej úrovne vnorenia a bez ohľadu na ich veľkosť. Pre zmenu kontroly archivovaných súborov zrušte výber možnosti **Predvolené nastavenie kontroly archívov**.

Doplňujúce parametre ThreatSense pre spúšťané súbory

Predvolene sa pokročilá heuristika používa vtedy, keď sú dané súbory spúšťané. Dôrazne odporúčame ponechať zapnutú Smart optimalizáciu a ESET LiveGrid® pre zmiernenie vplyvu na výkon vášho systému.

Prípony súborov vylúčené z kontroly

Prípona je časť názvu súboru, spravidla oddelená bodkou. Prípona určuje typ súboru. Predvolene sa kontrolujú všetky súbory bez ohľadu na príponu. Ak však potrebujete vylúčiť súbory s konkrétnou príponou, nastavenie parametrov ThreatSense vám umožňuje vylúčiť súbory z kontroly podľa ich prípony. Vylúčenie určitých typov súborov môže byť užitočné napríklad v prípade, ak kontrola daných typov súborov znemožňuje správne fungovanie niektorej aplikácie.

Príklad:
Pre pridanie novej prípony do zoznamu kliknite na **Pridať**. Zadajte príponu súboru do textového poľa (napr. `tmp`) a kliknite na **OK**. Ak označíte možnosť **Zadať viaceré hodnoty**, môžete do textového poľa zadať viacero prípon oddelených riadkami, čiarkami alebo bodkočiarkami. Môžete napríklad vybrať oddeľovač **Bodkočiarka** z roletového menu a následne zadať `edb;eml;tmp`.
Môžete tiež použiť špeciálny symbol ? (otáznik). Otáznik predstavuje akýkoľvek znak (napr. `?db`).

Poznámka:
Ak chcete, aby sa zobrazovali prípony (typ súboru) pre všetky súbory na operačnom systéme Windows, zrušte výber možnosti **Skryť prípony známych súborov** v sekcii **Ovládací panel** > **Možnosti priečinka** > **Zobrazenie**.

Vylúčenia procesov

Funkcia Vylúčenia procesov umožňuje nastaviť procesy aplikácií, ktoré nemajú byť kontrolované antimalvérovou kontrolou. Vzhľadom na mimoriadne dôležitú úlohu jednoúčelových serverov (application server, storage server atď.) sú nevyhnutnosťou pravidelné zálohy pre zabezpečenie včasnej obnovy pri rôznych typoch incidentov. Pre zlepšenie rýchlosti zálohovania, integrity procesov a dostupnosti služieb sa pri zálohovaní používajú niektoré techniky, ktoré sa dostávajú do konfliktu s ochranou pred malvérom. Podobné konflikty môžu nastať aj pri živej migrácii virtuálnych počítačov. Jediným efektívnym riešením je v tomto prípade vypnutie antimalvérového

softvéru. Vylúčením konkrétneho procesu (napr. procesu používaného pri zálohovaní) budú všetky operácie so súbormi pre daný vylúčený proces ignorované a považované za bezpečné, čím sa zároveň minimalizuje možné riziko prerušenia zálohovania dát. Pri výbere vylúčení odporúčame byť maximálne opatrný – zálohovacie nástroje vylúčené z kontroly totiž môžu pristupovať k infikovaným súborom bez toho, aby sa spustilo upozornenie, čo je vlastne dôvod, prečo sú rozšírené oprávnenia dostupné len pre modul ochrany v reálnom čase.

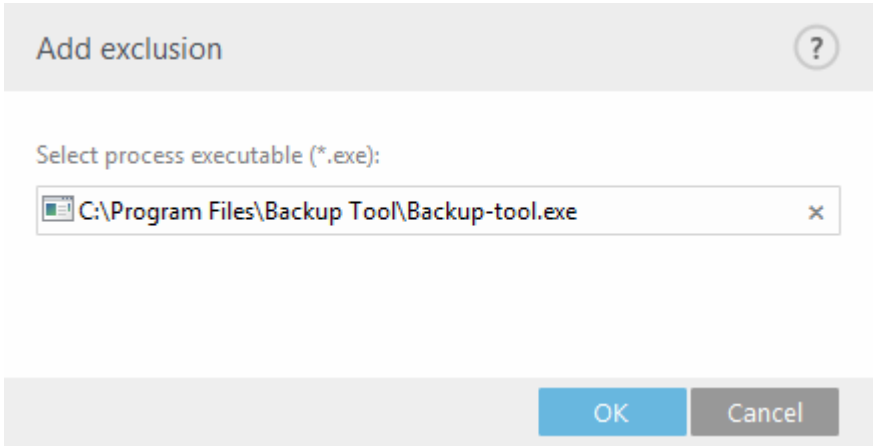
Vylúčenia procesov znižujú riziko potenciálnych konfliktov a zvyšujú výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie samotného spustiteľného súboru (*.exe*).

Spustiteľné súbory môžete pridať do zoznamu vylúčených procesov cez **Rozšírené nastavenia** (F5) > **Počítač** > **Rezidentná ochrana súborového systému** > **Základné** > **Vylúčenia procesov** alebo môžete použiť zoznam spustených procesov v hlavnom menu **Nástroje** > **Spustené procesy**.

Táto funkcia bola navrhnutá tak, aby boli automaticky vylúčené nástroje určené na vytváranie zálohy. Vylúčenie procesu nástroja určeného na vytváranie zálohy zabezpečí stabilitu systému a zároveň neovplyvní priebeh zálohovania.

Príklad:
Kliknite na **Upraviť** pre otvorenie okna **Vylúčenia procesov**, kde môžete **pridať** vylúčenia a vyhľadať spustiteľný súbor (napr. *Backup-tool.exe*), ktorý bude vylúčený z kontroly.
Akonáhle je súbor *.exe* pridaný medzi vylúčenia, ESET Security for Microsoft SharePoint nebude sledovať aktivitu tohto procesu a nebude kontrolovať jeho akcie so súbormi.

Dôležité:
Ak pri výbere spustiteľného súboru procesu nepoužívate funkciu prehľadávania, je potrebné manuálne zadať úplnú cestu k danému súboru. V opačnom prípade vylúčenie nebude správne fungovať a modul HIPS môže hlásiť chyby.



Môžete tiež **upraviť** existujúce procesy alebo ich **odstrániť** z vylúčení.

Poznámka:
Ochrana prístupu na web neberie do úvahy toto vylúčenie, preto ak napríklad vylúčite z ochrany webový prehliadač, stiahnuté súbory budú stále kontrolované. Takto je vždy možné zachytiť infiltráciu. Tento scenár je len príklad, neodporúčame vytvárať vylúčenia pre webové prehliadače.

Ochrana s podporou cloudu

ESET LiveGrid® je pokročilá ochranná technológia včasného varovania fungujúca na báze cloud-computing. Pomáha detegovať objavujúce sa hrozby na základe reputácie a optimalizuje kontrolu na základe whitelistu. Pomocou informácií, ktoré sú okamžite zdieľané na serveroch (v cloude), dokážu vírusové laboratóriá spoločnosti ESET poskytovať stálu a konzistentnú ochranu. Používateľ môže overiť reputáciu súborov a spustených procesov priamo z používateľského prostredia programu alebo z kontextového menu v ktorom sa nachádzajú dodatočné funkcie ESET LiveGrid®.

Pri inštalácii ESET Security for Microsoft SharePoint označte jednu z nasledujúcich možností:

- Môžete sa rozhodnúť neaktivovať ESET LiveGrid®. Neprídete tým o žiadnu funkcionalitu programu, ale v niektorých prípadoch môže ESET Security for Microsoft SharePoint reagovať na nové hrozby pomalšie ako aktualizácia detekčného jadra.

- Môžete sa rozhodnúť ESET LiveGrid® aktivovať, čo vám umožní odosielať informácie o nových infiltráciách. Ak je nový nebezpečný kód súčasťou súboru, celý súbor bude odoslaný na podrobnú analýzu do spoločnosti ESET. Skúmanie týchto infiltrácií nám pomôže zvýšiť schopnosť detekcie.

ESET LiveGrid® zozbiera z vášho počítača tie informácie, ktoré sa týkajú novej infiltrácie. To môže zahŕňať ukážku alebo kópiu súboru, v ktorom sa infiltrácia objavila, cestu k súboru, názov súboru, informáciu o dátume a čase detekcie, spôsob, akým sa infiltrácia dostala na váš počítač a informáciu o operačnom systéme vášho počítača.

Štandardne ESET Security for Microsoft SharePoint odosiela podozrivé vzorky do vírusového laboratória spoločnosti ESET na analýzu. Súbory s niektorými príponami, napríklad *.docx* alebo *.xlsx*, sa nikdy neodosielajú. Ak existujú ďalšie súbory, pri ktorých sa chcete vyhnúť možnosti odoslania, môžete doplniť ďalšie prípony.

Zapnúť reputačný systém ESET LiveGrid® (odporúčané)

Systém reputácie ESET LiveGrid® zlepšuje efektivitu antimalvérových riešení spoločnosti ESET pomocou porovnávania kontrolovaných súborov s databázou dôveryhodných a blokovaných súborov na serveroch spoločnosti ESET.

Zapnúť systém spätnej väzby ESET LiveGrid®

Dáta budú odoslané do výskumného laboratória ESET na ďalšiu analýzu.

Odosielať správy o zlyhaniach a diagnostické dáta

Táto možnosť slúži na odosielanie dát, ako sú napr. správy o zlyhaní, moduly alebo výpisy pamäte.

Odosielať anonymné štatistiky

Umožňuje spoločnosti ESET zbierať anonymné informácie o novonájdených hrozbách (napr. názov hrozby, dátum a čas detekcie, spôsob detekcie a súvisiace metadáta), kontrolované súbory (hash, názov súboru, pôvod súboru, telemetria), blokované a podozrivé URL adresy, verziu a konfiguráciu produktu a informácie o vašom systéme.

Kontaktný e-mail (nepovinný údaj)

Váš kontaktný e-mail bude použitý v prípade potreby doplňujúcich informácií o zachytenej infiltrácii. Tento e-mail nebude použitý na žiadny iný účel.

Odosielanie vzoriek

Automatické odosielanie infikovaných vzoriek

Týmto sa pošlú všetky infikované vzorky do spoločnosti ESET na analýzu, čo zároveň pomôže vylepšiť ich detekciu v budúcnosti.

- Všetky infikované vzorky
- Všetky vzorky okrem dokumentov
- Neposielať

Automatické odosielanie podozrivých vzoriek

Podozrivé vzorky pripomínajúce hrozby, a/alebo vzorky s neobvyklými vlastnosťami alebo správaním sú posielané spoločnosti ESET na analýzu.

- **Spustiteľné súbory** – zahŕňa typy spustiteľných súborov ako *.exe, .dll, .sys*.
- **Archívy** – zahŕňa typy archívnych súborov ako *.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab*.
- **Skripty** – zahŕňa typy skriptov, ako sú *.bat*, *.cmd*, *.hta*, *.js*, *.vbs*, *.js*, *.ps1*.
- **Iné** – zahŕňa typy súborov, ako sú *.jar*, *.reg*, *.msi*, *.swf*, *.lnk*.
- **Potenciálne spamové e-maily** – zlepšuje globálnu detekciu spamu.
- **Dokumenty** – zahŕňa dokumenty aplikácií Microsoft Office a PDF dokumenty s aktívnym obsahom.

Vylúčenia

Kliknite na Zmeniť vedľa vylúčení v sekcii ESET LiveGrid®, ak chcete nastaviť spôsob odosielania vzoriek do vírusových laboratórií spoločnosti ESET.

Maximálna veľkosť vzoriek (MB)

Určuje maximálnu veľkosť kontrolovaných vzoriek.

ESET Dynamic Threat Defense

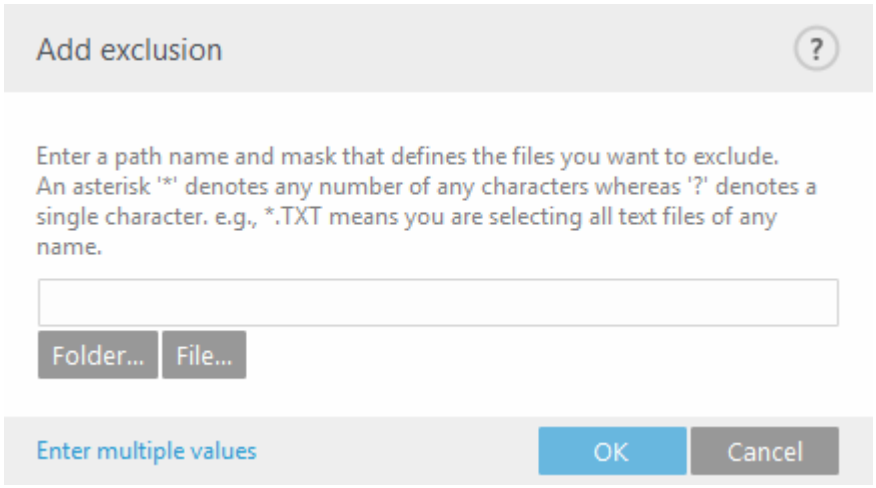
Službu ESET Dynamic Threat Defense na klientskom počítači zapnete pomocou ESET PROTECT Web Console. V ESET PROTECT Web Console vytvorte novú politiku, pripadne si otvorte niektorú z existujúcich, a po vykonaní požadovaných zmien v rámci nastavení túto politiku priraďte k zariadeniam, na ktorých chcete službu ESET Dynamic Threat Defense používať.

Filter vylúčení

Filter vylúčení vám umožňuje vylúčiť z ochrany súbory alebo adresáre (môže to byť užitočné pri dokumentoch obsahujúcich dôverné informácie). Súbory pridané do vylúčení nebudú odoslané na analýzu do vírusových laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód. Najbežnejšie typy súborov sú

predvolene vylúčené (napr. *.doc*). Do zoznamu súborov vylúčených z kontroly môžete pridávať ľubovoľné prípony.

Ak ste mali zapnutý ESET LiveGrid® a neskôr ho vypli, môže sa stať, že v počítači sú už pripravené dátové balíky na odoslanie. Tieto balíky budú odoslané do spoločnosti ESET aj pri deaktivovaní. Po odoslaní všetkých aktuálnych informácií sa už ďalšie balíky nevytvoria.



V prípade, že máte podozrivý súbor, môžete nám ho poslať na analýzu do nášho vírusového laboratória. Ak ide o nebezpečnú aplikáciu, jej detekcia bude pridaná v najbližšej aktualizácii detekčného jadra.

Detekcia malvéru

V tejto časti môžete nastaviť parametre kontroly počítača.

> Poznámka:
> Tento výber profilu sa vzťahuje na **manuálnu kontrolu** a kontrolu Hyper-V.

Aktívny profil

Určuje názov profilu, ktorého nastavenia sa použijú pri manuálnej kontrole počítača. Môžete použiť niektorý z preddefinovaných profilov kontroly alebo vytvoriť nový. Profily kontroly používajú rôzne nastavenia parametrov ThreatSense.

Zoznam profilov

Pridať nový profil je možné prostredníctvom tlačidla **Upraviť**. Zadajte názov profilu a kliknite na **Pridať**. Nový profil bude zobrazený v roletovom menu **Aktívny profil**, ktoré obsahuje existujúce profily kontroly.

Ciele kontroly

Ak si želáte skontrolovať len konkrétne súbory (ciele) na disku, kliknite na **Upraviť** a z roletového menu vyberte príslušnú možnosť, resp. príslušné cieľové umiestnenie z adresárovej (stromovej) štruktúry.

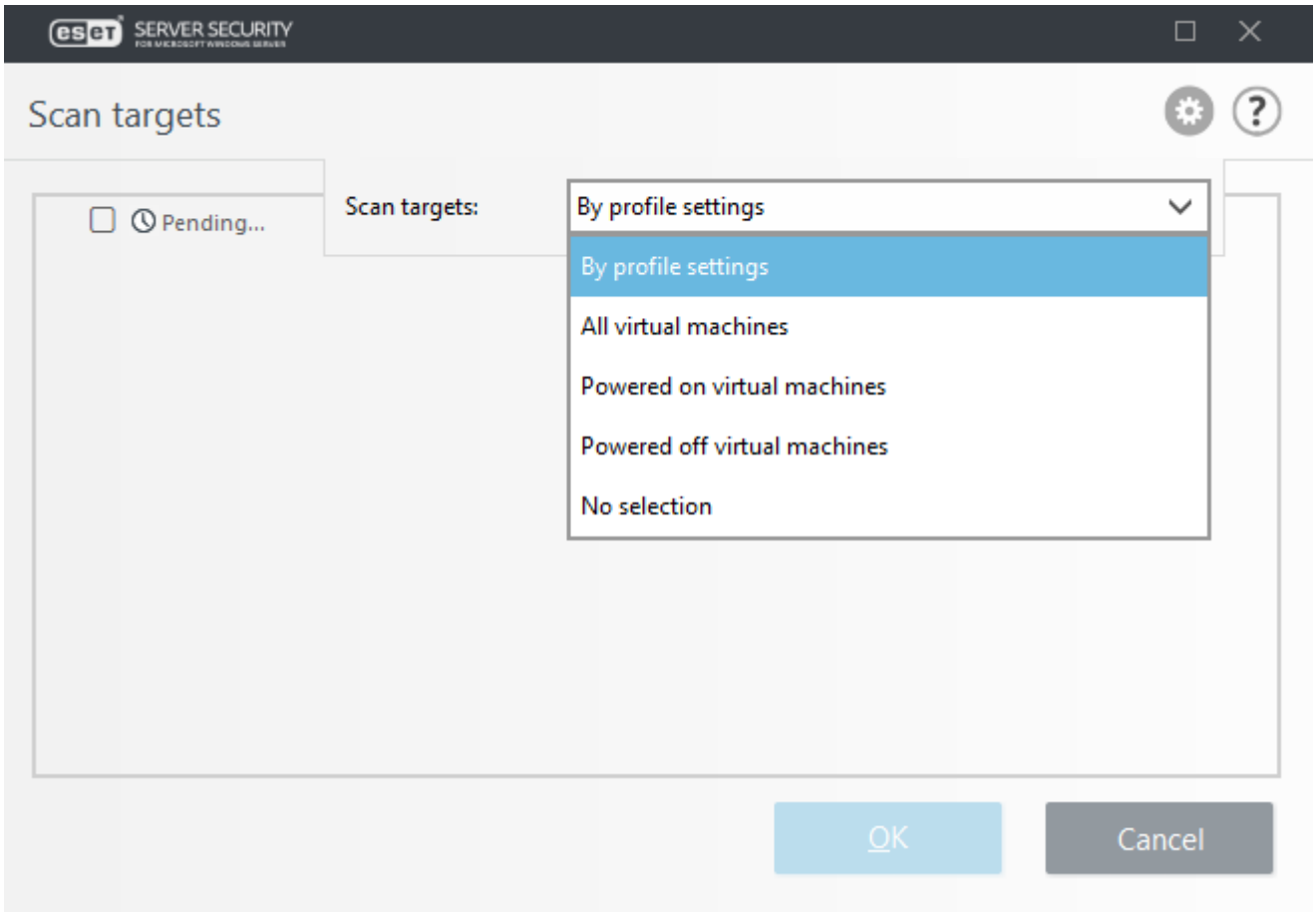
Parametre ThreatSense

V tejto sekcii môžete upraviť parametre manuálnej kontroly.

Manuálna kontrola s využitím strojového učenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia.

V okne **Kontrola Hyper-V**:



Roletové menu **Ciele kontroly** pre **Hyper-V** vám umožňuje vybrať preddefinované ciele kontroly:

Podľa nastavenia profilu	**Vyberie ciele kontroly nastavené v príslušnom profile.**
Všetky virtuálne počítače	Vyberie všetky virtuálne počítače.
Zapnuté virtuálne počítače	Vyberie všetky virtuálne počítače, ktoré sú online.
Vypnuté virtuálne počítače	Vyberie všetky virtuálne počítače, ktoré sú offline.
Bez výberu	Zruší celý výber.

Kliknutím na **Kontrolovať** spustíte kontrolu počítača s parametrami, ktoré sú nastavené. Po úspešnom dokončení všetkých kontrol si prezrite **Protokoly** > Kontrola Hyper-V.

Manažér profilov

Roletové menu **Profil kontroly** vám umožňuje vybrať niektorý z preddefinovaných profilov.

- **Smart kontrola**
- **Kontrola z kontextového menu**
- **Hĺbková kontrola**
- **Môj profil** (vzťahuje sa na Kontrolu Hyper-V a Aktualizačné profily))

Podrobný postup vytvorenia profilu kontroly, ktorý bude slúžiť vašim potrebám, nájdete v kapitole ThreatSense

parametre.

Manažér profilov sa používa v rámci ESET Security for Microsoft SharePoint na troch miestach.

Manuálna kontrola počítača

Svoje preferované nastavenia kontroly počítača si môžete uložiť do profilov. Odporúčame vytvoriť viacero profilov s rôznymi cieľmi a metódami kontroly, prípadne ďalšími nastaveniami pre často používané kontroly.

Aktualizácia

Editor profilov umožňuje vytvárať nové aktualizačné profily. Vlastné aktualizačné profily je potrebné vytvoriť len v prípade, že váš počítač sa na aktualizačné servery pripája viacerými spôsobmi.

Kontrola Hyper-V

Pridať nový profil je možné prostredníctvom tlačidla **Upraviť** v sekcii **Zoznam profilov**. Nový profil bude zobrazený v roletovom menu **Aktívny profil**, ktoré obsahuje existujúce profily kontroly.

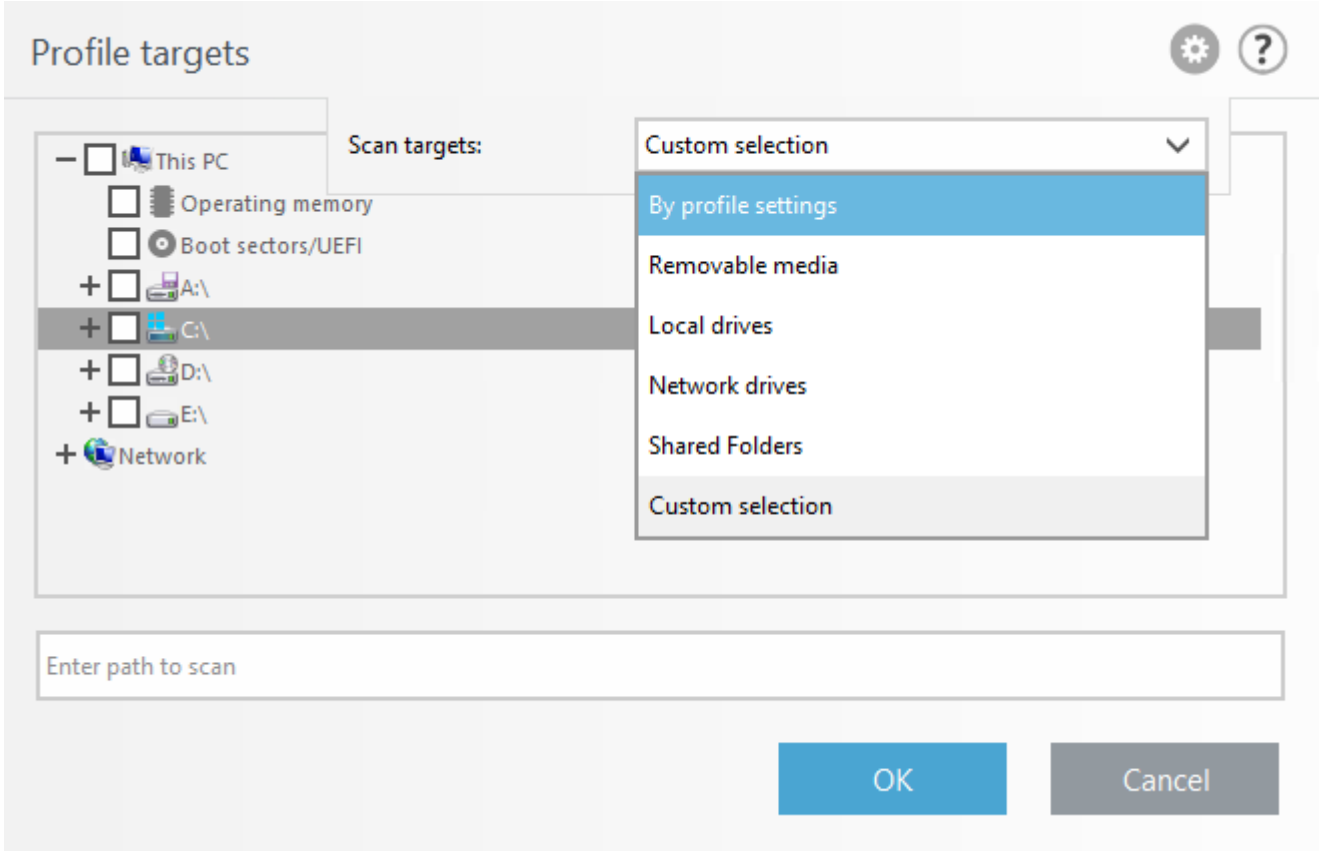
Ciele profilu

V tejto časti môžete nastaviť, ktoré položky budú kontrolované na prítomnosť infiltrácií. Vyberte objekty (pamäť, zavádzacie sektory a UEFI, disky, súbory, priečinky, sieť) zo stromovej štruktúry, ktorá obsahuje zoznam všetkých dostupných cieľov na vašom systéme. Kliknutím na ikonu ozubeného kolesa v hornom ľavom rohu sa dostanete k roletovým menu **Ciele kontroly** a **Profil kontroly**.

> Poznámka:
> Tento výber profilu sa vzťahuje na **manuálnu kontrolu** a kontrolu Hyper-V.

Operačná pamäť	Skontrolujú sa všetky procesy a dáta aktuálne používané v operačnej pamäti.
Zavádzacie sektory/UEFI	Vykoná sa kontrola prítomnosti škodlivého kódu v zavádzacích sektoroch a UEFI. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
Databáza WMI	Skontroluje sa celá databáza Windows Management Instrumentation (WMI), všetky priestory názvov, triedy inštancií a vlastnosti. Vyhľadá odkazy na infikované súbory alebo malvér vložený ako dáta.
Systémová databáza Registry	Skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadá odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Prázdne pole pod stromovou štruktúrou slúži na rýchle zadanie cesty k zvolenému cieľu kontroly (priečinku alebo súboru).



Roletové menu **Ciele kontroly** vám umožňuje vybrať preddefinované ciele kontroly:

Podľa nastavenia profilu	**Vyberie ciele kontroly nastavené v príslušnom profile.**
Vymeniteľné médiá	Vyberie CD/DVD, pamäťové zariadenia USB atď.
Lokálne disky	Vyberie všetky lokálne pevné disky v počítači.
Sieťové disky	Vyberie všetky namapované sieťové disky.
Zdieľané priečinky	Vyberie všetky zdieľané priečinky na lokálnom serveri.
Vlastný výber	Zruší celý výber. Po zrušení výberu môžete vykonať vlastný výber.

Ak chcete rýchlo prejsť k cieľu kontroly (súbor alebo priečinok) a zahrnúť ho do kontroly, zadajte jeho cestu do textového poľa umiestneného pod stromovou štruktúrou. V rámci zadávania cesty sa rozlišujú malé a veľké písmená.

Roletové menu **Profil kontroly** vám umožňuje vybrať preddefinované profily kontroly:

- **Smart kontrola**
- **Kontrola z kontextového menu**
- **Hĺbková kontrola**

Tieto profily používajú rôzne nastavenia parametrov ThreatSense.

Kontrolovať bez liečenia

Ak chcete spustiť kontrolu systému bez liečenia, označte možnosť **Kontrolovať bez liečenia**. Toto je užitočné v prípade, že chcete mať iba prehľad o tom, či sa v systéme vyskytujú infikované položky, prípadne o nich získať ďalšie podrobnosti. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na možnosť **Nastaviť...** v časti **Parametre ThreatSense** > **Liečenie**. Informácie o kontrole sa zobrazia po skončení kontroly a budú zapísané do protokolu.

Ignorovať vylúčenia

Ak použijete možnosť **Ignorovať vylúčenia**, umožní vám to vykonať kontrolu, pri ktorej budú ignorované vylúčenia.

Ciele kontroly

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

Roletové menu Ciele kontroly sa vzťahuje na nasledujúce typy kontroly:

- Manuálna kontrola
- Kontrola Hyper-V

Ak chcete rýchlo prejsť k cieľu kontroly alebo pridať nový cieľový súbor či priečinok, zadajte jeho názov do prázdneho poľa pod stromovou štruktúrou. Toto je možné len v tom prípade, ak nie sú v stromovej štruktúre vybrané žiadne ciele a v roletovom menu **Ciele kontroly** je nastavená možnosť **Bez výberu**.

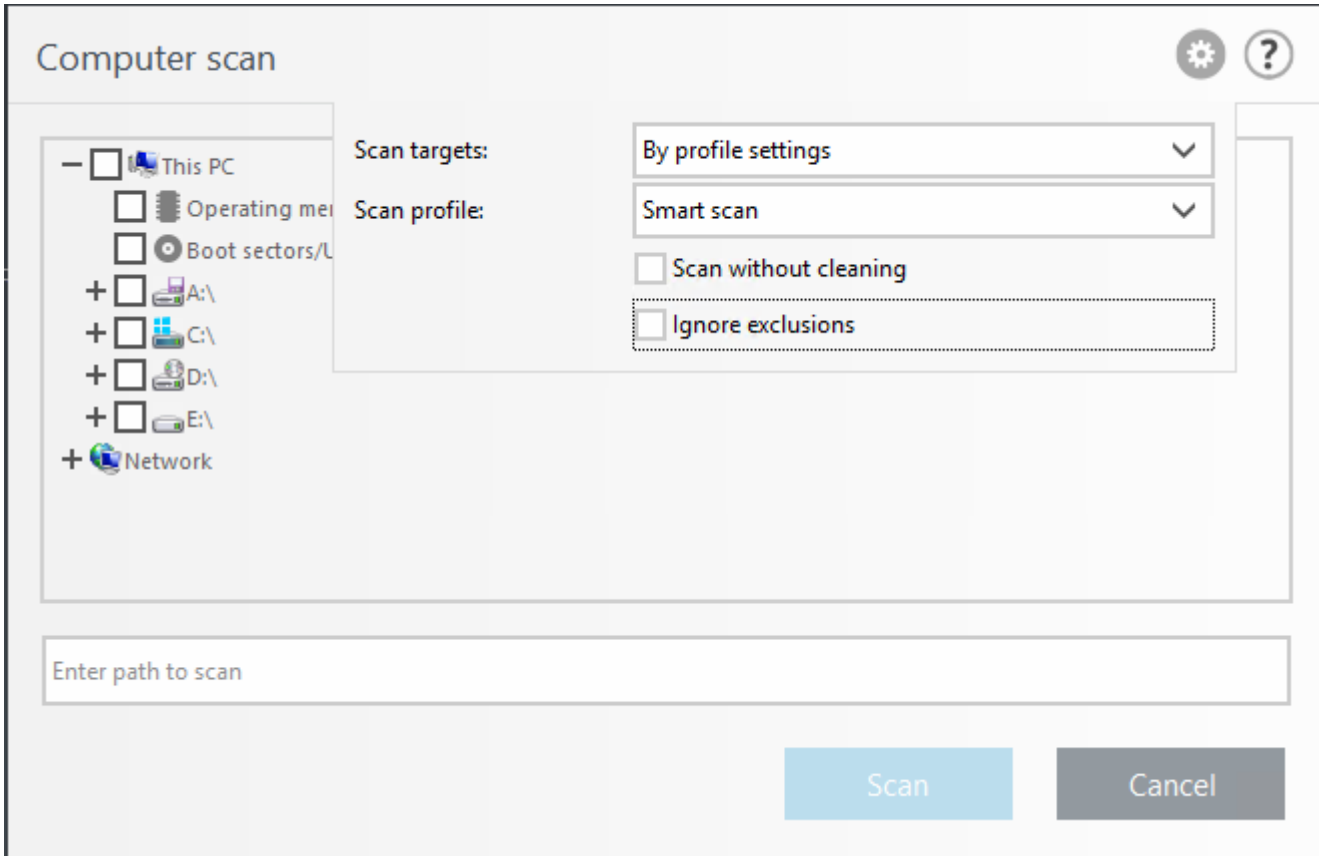
Operačná pamäť	Skontrolujú sa všetky procesy a dáta aktuálne používané v operačnej pamäti.
Zavádzacie sektory/UEFI	Vykoná sa kontrola prítomnosti škodlivého kódu v zavádzacích sektoroch a UEFI. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
Databáza WMI	Skontroluje sa celá databáza Windows Management Instrumentation (WMI), všetky priestory názvov, triedy inštancií a vlastnosti. Vyhľadá odkazy na infikované súbory alebo malvér vložený ako dáta.
Systémová databáza Registry	Skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče. Vyhľadá odkazy na infikované súbory alebo malvér vložený ako dáta. Pri liečení detekcie zostane v databáze Registry odkaz, aby sa zabránilo strate dôležitých dát.

Roletové menu **Ciele kontroly** vám umožňuje vybrať preddefinované ciele kontroly.

Podľa nastavenia profilu	Vyberie ciele kontroly nastavené v príslušnom profile.
Vymeniteľné médiá	Vyberie CD/DVD, pamäťové zariadenia USB atď.
Lokálne disky	Vyberie všetky lokálne pevné disky v počítači.
Sieťové disky	Vyberie všetky namapované sieťové disky.
Zdieľané priečinky	Vyberie všetky zdieľané priečinky na lokálnom serveri.
Vlastný výber	Zruší celý výber. Po zrušení výberu môžete vykonať vlastný výber.

Profil konfigurácie, s ktorým bude vykonaná kontrola zvolených cieľov, môžete vybrať z roletového menu **Profil** kontroly. Predvolený profil je **Smart kontrola**. Sú dostupné ďalšie dva preddefinované profily: **Hĺbková kontrola** a **Kontrola z kontextového menu**. Tieto profily používajú rôzne nastavenia parametrov ThreatSense.

Okno **Vlastná kontrola**:



Kontrolovať bez liečenia

Ak chcete spustiť kontrolu systému bez liečenia, označte možnosť **Kontrolovať bez liečenia**. Toto je užitočné v prípade, že chcete mať iba prehľad o tom, či sa v systéme vyskytujú infikované položky, prípadne o nich získať ďalšie podrobnosti. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na možnosť **Nastaviť...** v časti **Parametre ThreatSense** > **Liečenie**. Informácie o kontrole sa zobrazia po skončení kontroly a budú zapísané do protokolu.

Ignorovať vylúčenia

Môžete vykonať kontrolu, pri ktorej budú ignorované vylúčenia.

Kontrolovať

Spustenie kontroly počítača s parametrami, ktoré sú nastavené.

Kontrolovať ako správca

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

Kontrola v nečinnosti

Ak je počítač v stave nečinnosti, na pozadí sa spúšťa kontrola všetkých diskov počítača. **Kontrola v nečinnosti** sa spustí, ak je zistený jeden z nasledujúcich stavov nečinnosti:

- **vypnutá obrazovka alebo aktívny šetrič obrazovky,**

- **uzamknutý počítač,**
- **odhlásený používateľ.**

Spustiť, aj keď je počítač napájaný z batérie

V predvolených nastaveniach programu sa kontrola nečinnosti nespúšťa, ak je počítač (notebook) napájaný z batérie.

Vytvárať protokol

Túto možnosť môžete použiť v prípade, ak chcete z kontroly v nečinnosti vytvárať protokol, ktorý nájdete v časti Protokoly (v hlavnom okne programu kliknite na Protokoly a potom z roletového menu vyberte možnosť Kontrola počítača).

Parametre ThreatSense

V tejto sekcii môžete upraviť parametre kontroly (napr. metódy detekcie) pre kontrolu v nečinnosti.

Kontrola pri štarte

Pri predvolených nastaveniach programu bude po štarte systému (prihlásení používateľa) a po úspešnej aktualizácií modulov vykonaná kontrola súborov spúšťaných pri štarte. Táto kontrola je riadená nastavením plánovača a úlohami.

Nastavenia kontroly pri štarte sú súčasťou plánovanej úlohy nazvanej **Kontrola súborov spúšťaných pri štarte počítača**.

Pre zmenu/zobrazenie týchto nastavení kliknite na **Nástroje** > **Plánovač**, potom vyberte jednu z úloh pod názvom **Kontrola súborov spúšťaných pri štarte počítača** (prihlásenie používateľa alebo aktualizácia modulov) a kliknite na **Upraviť**. Prejdite sprievodcom a v poslednom kroku budete môcť zmeniť podrobné nastavenia kontroly súborov spúšťaných pri štarte počítača.

Kontrola súborov spúšťaných pri štarte počítača

Pri vytváraní úlohy Kontrola súborov spúšťaných po štarte 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 špecifické skupiny Cieľov kontroly:

Súbory spustené pred prihlásením používateľa

Ide o súbory z umiestnení, z ktorých sa môžu spúšťať súbory bez toho, aby bol používateľ prihlásený (ide

takmer o všetky startup umiestnenia, ako napr. služby, vyhľadávanie objektu pomocníka, winlogon notify, položky plánovača systému Windows, známe dll súbory atď.).

Súbory spustené po prihlásení používateľa

Ide o súbory z umiestnení, z ktorých sa spúšťajú súbory po prihlásení používateľa (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

Ide o prioritu, s ktorou bude spustená kontrola:

- **Normálna** – zaťaženie systému je normálne,
- **Nižšia** – zaťaženie systému je nižšie,
- **Najnižšia** – zaťaženie systému je najnižšie možné,
- **Počas nečinnosti** – v momente, keď nie sú vykonávané žiadne iné činnosti.

Vymeniteľné médiá

ESET Security for Microsoft SharePoint poskytuje automatickú kontrolu externých vymeniteľných médií (CD/DVD/USB). Tento modul vám umožňuje skontrolovať vymeniteľné médiá. Môže to byť užitočné v prípade, ak správca chce zabrániť používateľom v používaní externých médií s nežiaducim obsahom.

Vykonať akciu po vložení alebo pripojení vymeniteľného média

Vyberte akciu, ktorá bude vykonaná pri pripojení vymeniteľného média do počítača (CD/DVD/USB).

- **Nekontrolovať** – nebude vykonaná žiadna akcia a okno **Rozpoznané nové zariadenie** sa zatvorí.
- **Automaticky skontrolovať zariadenie** – spustí sa kontrola vymeniteľného zariadenia.
- **Zobraziť možnosti kontroly** – zobrazenie podrobných nastavení vymeniteľných médií.

Po pripojení vymeniteľného média k počítaču sa zobrazí nasledujúce okno:

- **Kontrolovať teraz** – spustí sa kontrola vymeniteľného média.
- **Kontrolovať neskôr** – kontrola vymeniteľného média bude odložená.
- **Nastavenia** – otvorí Rozšírené nastavenia.
- **Vždy použiť zvolenú možnosť** – vyberte predvolenú akciu, ktorá bude vykonaná po pripojení vymeniteľného média do počítača.

ESET Security for Microsoft SharePoint ponúka tiež možnosť správy zariadení, ktorá umožňuje používateľom definovať pravidlá pre používanie externých zariadení na počítači. Viac informácií nájdete v kapitole Správa zariadení.

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 môže byť zakázaná na účely zvýšenia výkonu na operačných systémoch Windows, ktoré nie sú vystavované veľkým počtom dokumentov balíka Microsoft Office.

Integrácia do systému

Táto možnosť vylepšuje ochranu Microsoft Office dokumentov (za normálnych okolností sa nevyžaduje).

Parametre ThreatSense

V tejto sekcii môžete upraviť parametre Ochrany dokumentov.

> Poznámka:
> Tento modul pracuje iba s aplikáciami, ktoré podporujú rozhranie Microsoft Antivirus API (napríklad Microsoft Office 2000 od verzie 9.0 a Microsoft Internet Explorer od verzie 5.0).

Kontrola Hyper-V

Aktuálna verzia kontroly Hyper-V podporuje kontrolu online alebo offline virtuálneho systému v Hyper-V. Podporované typy kontroly podľa hostiteľského systému Windows Hyper-V a stavu virtuálneho systému sú uvedené nižšie:

Virtuálne systémy s funkciou Hyper-V	Windows Server 2008 R2 SP1 Hyper-V	Windows Server 2012 Hyper-V	Windows Server 2012 R2 Hyper-V	Windows Server 2016 Hyper-V	Windows Server 2019 Hyper-V
Online virtuálny počítač	žiadna kontrola	iba na čítanie	iba na čítanie	iba na čítanie	iba na čítanie
Offline virtuálny počítač	iba na čítanie/liečenie	iba na čítanie/liečenie	iba na čítanie/liečenie	iba na čítanie/liečenie	iba na čítanie/liečenie

Hardvérové požiadavky

Server by nemal mať žiadne problémy s výkonom a zaťažením pri chode na virtuálnom počítači. Kontrola využíva prevažne prostriedky procesora. Kontrola spusteného virtuálneho počítača vyžaduje dostatok voľného miesta na disku. Voľné miesto na disku musí predstavovať aspoň dvojnásobok miesta použitého pre kontrolné body/snímky a virtuálne disky.

Špecifické obmedzenia

- Kontrola úložiska RAID, rozložených zväzkov a dynamických diskov nie je podporovaná z dôvodu povahy dynamických diskov. Odporúčame teda nepoužívať dynamické disky na vašich virtuálnych počítačoch, ak je to možné.
- Kontrola vždy prebieha na aktuálnom virtuálnom počítači a nemá vplyv na kontrolné body alebo snímky (snapshot).
- Hyper-V spustený na hostiteľovi v klastri momentálne nie je podporovaný produktom ESET Security for Microsoft SharePoint.
- Virtuálne počítače na hostiteľovi Hyper-V bežiacom na systéme Windows Server 2008 R2 SP1 môžu byť

kontrolované v režime iba na čítanie (Neliečiť) bez ohľadu na to, aká úroveň liečenia je vybraná v časti parametre ThreatSense.

> Poznámka:
> Kým ESET Security podporuje kontrolu MBR virtuálnych diskov, podporovaná je len kontrola v režime iba na čítanie. Toto nastavenie je možné zmeniť v časti **Rozšírené nastavenia** (**F5**) > **Počítač** > **Kontrola Hyper-V** > Parametre ThreatSense > **Zavádzacie sektory**.

Virtuálny počítač, ktorý má byť kontrolovaný, je offline (vypnutý)

ESET Security for Microsoft SharePoint využíva nástroj Hyper-V Management na detekciu a pripojenie k virtuálnym diskom. ESET Security for Microsoft SharePoint má takto rovnaký prístup k obsahu virtuálnych diskov ako v prípade štandardných diskov.

Virtuálny počítač, ktorý má byť kontrolovaný, je online (spustený, pozastavený, uložený)

ESET Security for Microsoft SharePoint využíva nástroj Hyper-V Management na detekciu virtuálnych diskov. Pripojenie k týmto diskom nie je možné. ESET Security for Microsoft SharePoint tým pádom vytvára kontrolné body/snímky virtuálneho počítača a potom sa k nim pripája. Po dokončení kontroly je kontrolný bod/snímka vymazaná. To znamená, že kontrola v režime iba na čítanie môže byť vykonávaná, pretože na spustené virtuálne počítače vplyv nemá.

Počkajte približne minútu, kým ESET Security for Microsoft SharePoint vytvorí počas kontroly snímku alebo kontrolný bod. Toto je potrebné mať na pamäti v prípade spustenia kontroly Hyper-V na väčšom množstve virtuálnych počítačov.

Názvová konvencia

Modul kontroly Hyper-V používa nasledujúce názvy:

```
NázovVirtuálnehoPočítača\DiskX\ZväzokY
```

kde X je číslo disku a Y je číslo zväzku. Napríklad:

```
Počítač\Disk0\Zväzok1
```

Číselná prípona sa pridá na základe poradia detekcie diskov a je totožná s poradím diskov v Správcovi virtuálnych diskov. Táto konvencia pomenovávania je použitá v strome cieľov kontroly na indikátore priebehu kontroly, ako aj v protokoloch kontroly.

Možnosti spustenia kontroly

- Manuálne – kliknite na **Kontrola Hyper-V** pre zobrazenie zoznamu virtuálnych počítačov a zväzkov, pre ktoré môže byť vykonaná kontrola. Označte virtuálne počítače, disky alebo zväzky, ktoré chcete kontrolovať a kliknite na **Kontrolovať**.
- Vytvorením naplánovanej úlohy.
- Pomocou nástroja ESET PROTECT, použitím klientskej úlohy nazvanej Kontrola servera.
- Kontrolu Hyper-V je možné spravovať a spúšťať pomocou rozhrania eShell.

Takisto je možné spustiť viacero kontrol Hyper-V súčasne. Po dokončení kontroly sa zobrazí oznámenie s odkazom na súbory protokolov.

Možné problémy

- Pri spustení kontroly online virtuálneho počítača bude vytvorená snímka daného počítača, pričom pri vytváraní snímky sú základné funkcie virtuálneho počítača obmedzené alebo úplne znemožnené.
- Ak je kontrolovaný vypnutý virtuálny počítač, nemôže byť zapnutý až do dokončenia kontroly.
- Nástroj Hyper-V Manager vám umožňuje nazvať dva rozdielne virtuálne počítače identicky, čo predstavuje problém pri rozlišovaní počítačov v protokoloch kontroly.

HIPS

HIPS (Host-based Intrusion Prevention System) chráni váš systém pred škodlivým kódom a eliminuje aktivity ohrozujúce bezpečnosť vášho počítača. Používa pokročilú analýzu správania kódu, ktorá spolu s detekčnými schopnosťami sieťového filtra zabezpečuje sledovanie spustených procesov, súborov a záznamov v databáze Registry. HIPS pracuje oddelene od firewallu aj od rezidentnej ochrany, sleduje len procesy spustené v rámci operačného systému.

> Upozornenie:
> Ak nie ste skúsený používateľ, neodporúčame meniť nastavenia systému HIPS. Nesprávne nastavenia v sekcii HIPS môžu spôsobiť nestabilitu systému.

Zapnúť Self-Defense

ESET Security for Microsoft SharePoint má vstavanú technológiu Self-Defense, ktorá slúži na to, aby zabránila pokusom škodlivého softvéru o narušenie alebo zablokovanie antimalvérovej ochrany. Zmeny v nastaveniach Zapnúť HIPS a Zapnúť SD (Self-Defense) sa prejavia až po reštarte systému Windows. Z tohto dôvodu sa aj vypnutie celého systému HIPS prejaví až po reštarte.

Zapnúť ako chránenú službu

Microsoft predstavil uvedením systému Microsoft Windows Server 2012 R2 koncept chránených služieb. Ide o ochranu služieb pred malvérovými útokmi. Je to vďaka tomu, že jadro programu ESET Security for Microsoft SharePoint automaticky beží ako chránená služba. Táto funkcia je dostupná na systéme Microsoft Windows Server 2012 R2 a novších operačných systémoch určených pre servery.

Zapnúť pokročilú kontrolu pamäte

Pokročilá kontrola pamäte v kombinácii s technológiou Exploit Blocker zvyšuje ochranu proti malvéru, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu bezpečnostných produktov. Táto možnosť je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov.

Zapnúť Exploit Blocker

Exploit Blocker slúži na ochranu najčastejšie zneužívaných aplikácií, ako sú internetové prehliadače, prehliadače PDF dokumentov, e-mailové klienty a súčasti balíka MS Office. Táto možnosť je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov.

Zapnúť Ransomware Shield

Ak chcete použiť túto funkciu, je potrebné zapnúť HIPS a ESET Live Grid. Viac o ransomvéri nájdete v slovníku

pojmov.

Režim filtrovania

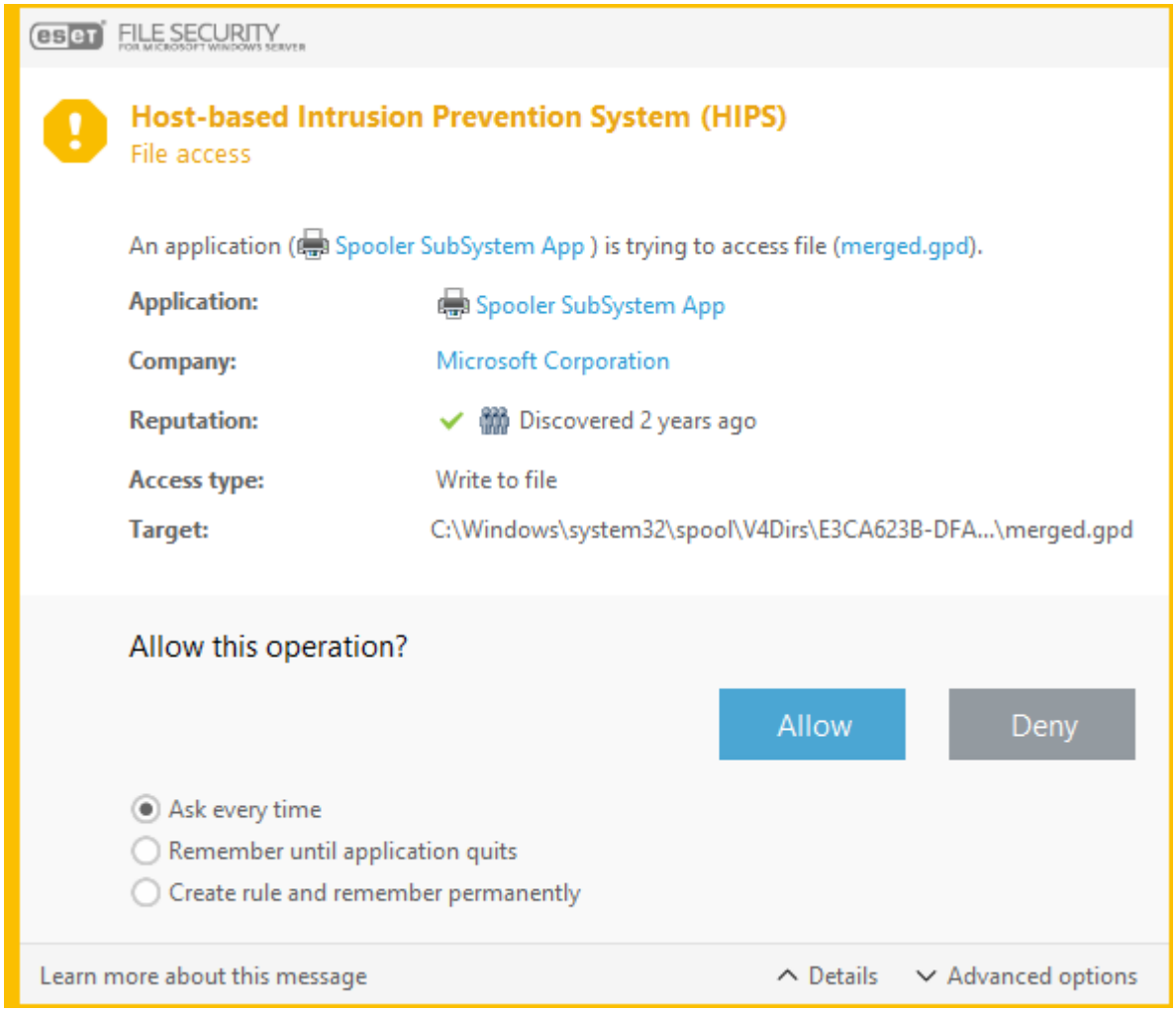
Môžete si vybrať jeden zo štyroch režimov filtrovania:

- **Automatický režim** – operácie budú povolené s výnimkou operácií blokovaných preddefinovanými pravidlami, ktoré chránia váš systém. Povolené je všetko okrem akcií, ktoré sú zakázané pravidlom.
- **Smart režim** – používateľ bude upozornený na podozrivé udalosti v systéme.
- **Interaktívny režim** – používateľ bude vyzvaný na povolenie operácií. Dostupné sú nasledujúce možnosti: Povoliť/zakázať prístup, Vytvoriť pravidlo, Dočasne si zapamätať akciu pre tento proces.
- **Režim politík** – operácie budú blokované. Akceptované sú len preddefinované pravidlá alebo pravidlá definované používateľom.
- **Učiaci sa režim** – operácie sú povolené a zároveň je vytvorené pravidlo, ktoré ich povoľuje. Pravidlá vytvorené týmto režimom sú viditeľné v editore pravidiel, ale majú nižšiu prioritu ako pravidlá vytvorené manuálne alebo pravidlá vytvorené v automatickom režime. Ak vyberiete možnosť **Učiaci sa režim** z roletového menu Režim filtrovania, sprístupní sa možnosť **Učiaci sa režim skončí**. Nastavte obdobie, počas ktorého bude zapnutý učiaci sa režim (maximálne 14 dní). Po uplynutí nastaveného obdobia, budete vyzvaný na upravenie pravidiel, ktoré boli vytvorené počas učiaceho sa režimu HIPS. Môžete tiež zvoliť iný režim filtrovania alebo oddialiť vaše rozhodnutie a používať učiaci sa režim aj naďalej.

Pravidlá

Pravidlá definujú, ktoré aplikácie môžu pristupovať ku ktorým súborom, databáze Registry a iným aplikáciám. Systém HIPS monitoruje udalosti vo vnútri operačného systému a reaguje na ne podľa pravidiel, ktoré sú štruktúrou podobné pravidlám firewallu. Ak chcete otvoriť okno správy pravidiel systému HIPS, kliknite na Upraviť. Ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností. Môžete si vybrať, či má byť operácia **povolená** alebo **blokovaná**. Ak používateľ nevyberie akciu vo vyhradenom čase, bude na základe pravidiel vytvorená nová akcia.

Dialógové okno umožňuje vytvorenie pravidla podľa akejkoľvek novej akcie detegovanej modulom HIPS a následné definovanie podmienok, ktoré musia byť splnené pre **povolenie** alebo **blokovanie** danej akcie. Bližšie informácie zobrazíte kliknutím na **Podrobnosti**. Takto vytvorené pravidlá sa vyhodnocujú rovnako, ako keby boli zadané ručne, teda pravidlo vytvorené z dialógového okna môže byť menej špecifické ako pravidlo, ktoré tento dialóg vyvolalo. To znamená, že po vytvorení takéhoto pravidla sa môže pri rovnakej udalosti zobraziť ďalšie dialógové okno, ak parametre z predchádzajúcej situácie nevyhovujú pre novú situáciu.



Vždy sa spýtať

Pri každom spustení pravidla sa zobrazí dialógové okno. Môžete si vybrať, či má byť operácia **povolená** alebo **zakázaná**.

Zapamätať si do ukončenia aplikácie

Výberom akcie **Zakázať** alebo **Povoliť** sa vytvorí dočasné pravidlo HIPS, ktoré bude použité, až kým nedôjde k zatvoreniu príslušnej aplikácie. Ak zmeníte režim filtrovania, upravíte pravidlá, prípadne dôjde k aktualizácii modulu HIPS alebo reštartujete systém, dočasné pravidlá budú vymazané.

Vytvoriť pravidlo a zapamätať natrvalo

Umožňuje vytvorenie nového pravidla HIPS. Toto pravidlo môžete neskôr upraviť v sekcii určenej na správu pravidiel HIPS.

Nastavenie pravidla HIPS

V tomto okne sa zobrazuje prehľad pravidiel HIPS.

Pravidlo	Názov pravidla určený používateľom alebo automaticky.
Zapnuté	Túto možnosť je vhodné deaktivovať v prípade, ak si želáte ponechať dané pravidlo v zozname pravidiel, avšak nechcete ho používať.

Pravidlo	Názov pravidla určený používateľom alebo automaticky.
Akcia	Pravidlo špecifikuje (práve jednu) akciu (**Povoliť**, **Blokovať**, **Spýtať sa**), ktorú je potrebné vykonať, ak sú všetky podmienky splnené.
Zdroje	Pravidlo sa uplatní len v prípade, že udalosť vyvolajú konkrétne aplikácie.
Ciele	Pravidlo sa uplatní, len ak sa operácia týka konkrétneho súboru, aplikácie alebo položky databázy Registry.
Závažnosť zapisovania do protokolu	Po zapnutí tejto možnosti budú informácie o danom pravidle zapisované do protokolu HIPS.
Oznamovať	Po spustení každej zodpovedajúcej udalosti sa v pravom dolnom rohu obrazovky zobrazí upozornenie.

Kliknutím na **Pridať** môžete vytvoriť nové pravidlo HIPS, prípadne kliknite na **Upraviť**, ak chcete upraviť označené položky.

Názov pravidla

Názov pravidla určený používateľom alebo automaticky.

Akcia

Pravidlo špecifikuje (práve jednu) akciu (**Povoliť**, **Blokovať**, **Spýtať sa**), ktorú je potrebné vykonať, ak sú všetky podmienky splnené.

Ovplyvnené operácie

Vyberte typy operácií, na ktoré bude pravidlo aplikované. Pravidlo sa uplatní len na tento typ operácie a na zvolený cieľ. Pravidlo pozostáva z častí, ktoré popisujú podmienky, za ktorých sa pravidlo spustí:

Zdrojové aplikácie

Pravidlo sa uplatní, len ak udalosť vyvolajú dané aplikácie. Vyberte možnosť **Špecifické aplikácie** z roletového menu a kliknite na **Pridať**, ak chcete pridať jednotlivé súbory alebo priečinky konkrétnej aplikácie, prípadne označte v roletovom menu možnosť **Všetky aplikácie** a pridajú sa všetky aplikácie.

> Poznámka:
> Niektoré operácie určitých pravidiel preddefinovaných modulom HIPS nemôžu byť blokované a sú predvolene povolené. Navyše, nie všetky systémové operácie sú monitorované modulom HIPS. Modul HIPS monitoruje operácie, ktoré možno považovať za nebezpečné.

Popis niektorých dôležitých aplikácií:

Operácie so súbormi:

Vymazať súbor	Aplikácia žiada o povolenie zmazať cieľový súbor.
Zapísať do súboru	Aplikácia žiada o povolenie zapisovať do cieľového súboru.
Priamy prístup na disk	Aplikácia sa snaží čítať z disku alebo naň zapisovať neštandardným spôsobom, ktorý obchádza štandardné procedúry systému Windows. Výsledkom môže byť zmena súboru bez aplikácie príslušného pravidla. Táto operácia môže byť spôsobená škodlivým kódom, ktorý sa snaží vyhnúť detekcii, ďalej zálohovacím programom, ktorý kopíruje celý obsah pevného disku, alebo správcom oblastí disku, ktorý reorganizuje diskové zväzky.

Vymazať súbor	Aplikácia žiada o povolenie zmazať cieľový súbor.
Nainštalovať globálny hook	Ide o volanie funkcie SetWindowsHookEx z knižnice MSDN.
Načítať ovládač	Inštalácia a načítanie ovládačov v systéme.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické súbory** a kliknutím na **Pridať** pridajte nové súbory alebo priečinky. Prípadne môžete v roletovom menu vybrať možnosť **Všetky súbory** a pridať tak všetky aplikácie.

Operácie s aplikáciou:

Ladiť inú aplikáciu	Pripojí ladiaci nástroj (debugger) k procesu. Pri ladení aplikácie je možné 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 z nástroja Process Explorer alebo z okna Procesy).
Spustiť novú aplikáciu	Spúšťanie nových aplikácií alebo procesov.
Zmeniť stav inej aplikácie	Zdrojová aplikácia sa pokúša zapisovať do pamäte cieľovej aplikácie, prípadne sa snaží spustiť kód v jej mene. Táto funkcia je užitočná na ochranu dôležitej aplikácie, ak ju nastavíte ako cieľovú aplikáciu pri pravidle, ktoré blokuje tieto operácie.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické aplikácie** a kliknutím na **Pridať** pridajte jednotlivé súbory alebo priečinky konkrétnej aplikácie. Prípadne môžete v roletovom menu vybrať možnosť **Všetky aplikácie** a pridať tak všetky aplikácie.

Operácie s databázou Registry:

Zmena nastavení spustenia	Ide o akékoľvek zmeny v nastaveniach definujúcich, ktoré aplikácie budú spúšťané pri štarte operačného systému Windows. Môžu byť vyhľadané napríklad pri zadaní 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.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické položky** a kliknutím na **Pridať** pridajte nové súbory alebo priečinky. Prípadne môžete v roletovom menu vybrať možnosť **Všetky položky** a pridať tak všetky aplikácie.

Poznámka:
Pri zadávaní cieľa je povolené používať zástupné znaky s istými obmedzeniami. Pri cestách k databáze Registry sa dá namiesto jedného kľúča v ceste použiť * vo význame „ľubovoľný jeden kľúč“. Napríklad *HKEY_USERS*\software can mean HKEY_USER\.default\software* nepredstavuje *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** je nesprávne uvedená cesta kľúča databázy Registry. Cesta kľúča databázy Registry obsahujúca * má špeciálny význam, znamená „tento kľúč alebo ľubovoľný podkľúč ľubovoľne hlboko“. Pri súborových cieľoch sa dajú používať zástupné znaky len týmto spôsobom. Pri vyhodnocovaní platí, že vždy sa hľadá najprv cieľ, ktorý popisuje danú cestu presne, až potom cieľ, ktorý ju popisuje s hviezdičkou (*).

Upozornenie:
Pri vytvorení príliš všeobecného pravidla sa môže zobraziť upozornenie.

Rozšírené nastavenia HIPS

Nasledujúce možnosti sú užitočné pre ladenie (debugging) a analýzu správania aplikácií.

Ovládače s povolením vždy sa načítať

Vybrané ovládače majú vždy povolenie sa načítať bez ohľadu na filtrovací režim, okrem prípadu, kedy sú zablokované používateľským pravidlom. Ovládače v tomto zozname majú vždy povolené načítanie bez ohľadu na zvolený HIPS režim filtrovania, pokiaľ nie sú blokované konkrétnym používateľským pravidlom. Môžete **Pridať** nový ovládač, prípadne **Upraviť** alebo **Odstrániť** zvolený ovládač zo zoznamu.

Poznámka:
Kliknite na **Obnoviť** pre odstránenie ovládačov pridaných používateľom. Táto možnosť je užitočná, ak ste pridali väčšie množstvo ovládačov a nie je možné ich zmazať zo zoznamu.

Zapisovať všetky zablokované operácie do protokolu

Všetky zablokované operácie sa zapíšu do HIPS protokolu.

Upozorniť na zmeny v zozname aplikácií automaticky spúšťaných pri štarte

Ak pribudne alebo ubudne aplikácia zo zoznamu aplikácií spúšťaných po štarte, zobrazí sa upozornenie.

Nastavenia aktualizácie

Nastavenie aktualizácie pozostáva zo špecifikácie zdroja aktualizácie, teda z nastavenia aktualizačných serverov a autentifikácie voči týmto serverom.

Poznámka:
Pre bezproblémové fungovanie aktualizácie je nevyhnutné mať všetky parametre nastavené správne. Ak používate firewall, treba zaistiť, aby mal program povolenú komunikáciu cez internet (napríklad HTTP komunikáciu).

⊟ Základné

Vybrať predvolený aktualizačný profil

Vyberte si z existujúcich profilov alebo vytvorte nový profil, ktorý sa bude predvolene vzťahovať na aktualizácie.

Vyčistiť aktualizačnú vyrovnávaciu pamäť

Ak máte problém s aktualizáciami, kliknite na tlačidlo **Vyčistiť** pre zmazanie obsahu adresára s dočasnými aktualizačnými súbormi.

Automaticky nastaviť maximálny vek detekčného jadra / Maximálny vek detekčného jadra (v dňoch)

Táto možnosť povoľuje nastavenie maximálneho počtu dní, po ktorom bude detekčné jadro vyhlásené za zastarané. Predvolená hodnota je 7.

Vrátenie zmien modulov

Ak máte podozrenie, že nová aktualizácia detekčného jadra alebo programových súčastí môže byť nestabilná alebo poškodená, môžete vrátiť detekčné jadro do predchádzajúceho stavu a zakázať aktualizácie na určený časový interval. Prípadne môžete povoliť predtým zakázané aktualizácie. ESET Security for Microsoft SharePoint poskytuje zálohu a obnovu detekčného jadra a programových súčastí (tzv. rollback). Pre vytvorenie snímok (snapshot) detekčného jadra ponechajte povolenú možnosť **Vytvárať snímky modulov**.

Počet záložných snímok

Určuje počet predchádzajúcich uložených snímok modulov.

Profily

Vytvoriť si vlastný aktualizačný profil je možné prostredníctvom tlačidla **Upraviť** vedľa položky **Zoznam profilov**. Zadajte **Názov profilu** a kliknite na **Pridať**. V roletovom menu **Vyberte profil na úpravu** zvoľte príslušný profil a upravte parametre pre typy **aktualizácie modulov** alebo použite možnosť **Aktualizačný mirror**.

Aktualizácie

Z roletového menu vyberte typ aktualizácie, ktorý bude použitý:

- **Priebežné aktualizácie** – predvolene je ako typ aktualizácie nastavená priebežná aktualizácia, ktorá zabezpečuje priebežné sťahovanie aktualizácií zo serverov spoločnosti ESET tak, aby pritom čo najmenej zaťažovala sieť.
- **Predbežné aktualizácie** – aktualizácie, ktoré prešli dôkladným interným testovacím procesom a čoskoro budú dostupné pre verejnosť. 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 NEMALI byť používané na serveroch výroby a pracovných staniciach, kde sa vyžaduje maximálna stabilita a dostupnosť.
- **Oneskorené aktualizácie** – umožňuje aktualizovanie zo špeciálnych aktualizačných serverov poskytujúcich nové verzie vírusových databáz s oneskorením aspoň X hodín (tzn. databázy testované v reálnom prostredí a teda považované za stabilné).

Upozorniť pred sťahovaním aktualizácií

V prípade dostupnosti aktualizácie sa miesto automatického stiahnutia zobrazí okno s potvrdením.

Upozorniť, ak veľkosť aktualizácie presiahne (kB)

V prípade, že aktualizačný súbor prekročí definovanú veľkosť, zobrazí sa upozornenie.

Nezobrazovať oznámenie o úspešnej aktualizácii

Táto možnosť zruší zobrazovanie oznámenia na paneli úloh v pravom dolnom rohu obrazovky. Použitie tejto možnosti je užitočné hlavne v prípadoch, kedy je na počítači spustená aplikácia na celú obrazovku. Majte na pamäti, že pri zapnutom Prezentačnom režime sa nezobrazujú oznámenia na obrazovke.

Aktualizácie modulov

Pre aktualizácie modulov je predvolene nastavená možnosť **Automatický výber servera**. Aktualizačný server je umiestnenie, v ktorom sú uložené aktualizácie. Ak pre aktualizáciu používate servery spoločnosti ESET, odporúčame ponechať predvolené nastavenia.

Ak používate mirror ako lokálny HTTP server, zadajte aktualizačný server v tomto formáte: *http://computer_name_or_its_IP_address:2221*
Ak používate mirror ako lokálny HTTP server s SSL, zadajte aktualizačný server v tomto formáte: *https://computer_name_or_its_IP_address:2221*
Ak používate mirror ako zdieľaný sieťový súbor, zadajte aktualizačný server v tomto formáte: *computer_name_or_its_IP_address**shared_folder*

Povoliť častejšie aktualizácie detekčných vzoriek

Detekčné jadro bude aktualizované v kratších intervaloch. Vypnutie tohto nastavenia môže mať negatívny dopad na účinnosť detekcie.

Povoliť aktualizáciu modulov z vymeniteľných médií

Táto funkcia vám umožňuje vykonávať aktualizáciu z vymeniteľného média za predpokladu, že dané médium obsahuje vytvorený mirror. Ak je zvolená **automatická** aktualizácia, aktualizácia bude prebiehať na pozadí. Ak chcete, aby sa zobrazovali aktualizačné okná, označte možnosť **Vždy sa spýtať**.

Aktualizácia programových súčastí

Pomocou roletového menu **Režim aktualizácie** nastavte, akým spôsobom má ESET Security for Microsoft SharePoint inštalovať aktualizácie programových súčastí (PCU) a mikroaktualizácie programových súčastí (µPCU) v prípade dostupnosti novej aktualizácie. Aktualizácia programových súčastí väčšinou upravuje existujúce funkcie, avšak súčasťou takejto aktualizácie môžu byť zároveň aj nové funkcie a opravy. V závislosti od zvoleného režimu môže byť aktualizácia programových súčastí vykonaná automaticky, teda bez potvrdenia či akéhokoľvek iného zásahu používateľa (vyzvaný bude iba v prípade vyžadovaného reštartu). Prípadne si môžete aktualizácie nastaviť tak, aby sa pred ich inštaláciou zobrazilo upozornenie.

Poznámka:
V niektorých prípadoch môže byť po vykonaní aktualizácie programových súčastí potrebný reštart servera.

Na výber sú nasledujúce režimy aktualizácie:

- **Spýtať sa pred vykonaním aktualizácie** – v prípade, že je dostupná nová aktualizácia produktu, zobrazí sa dialógové okno s ponukou na aktualizáciu. Toto je predvolené nastavenie. Po vykonaní aktualizácie

programových súčastí môže byť potrebný reštart servera.

• **Automatické aktualizácie** – aktualizácie programových súčastí budú stiahnuté a nainštalované automaticky. Môže sa vyžadovať reštart servera.

• **Nikdy neaktualizovať** – aktualizácia programových súčastí sa nebude vykonávať. Táto možnosť vám umožňuje vykonávať aktualizáciou programových súčastí manuálne a server reštartovať počas naplánovanej údržby.

Dôležité:
Pri použití automatických aktualizácií bude váš server po vykonaní aktualizácie reštartovaný automaticky.

Možnosti pripojenia

Proxy server

Pre prístup k nastaveniam proxy servera pre daný aktualizačný profil kliknite na **Režim proxy** a vyberte jednu z troch nasledujúcich možností:

• **Nepoužívať proxy server** – ESET Security for Microsoft SharePoint pri aktualizácii nepoužije žiadny proxy server.

• **Použiť globálne nastavenie proxy servera** – budú použité globálne nastavenia proxy servera, ktoré sú už definované v **Rozšírených nastaveniach** (F5) v sekcii **Nástroje** > Proxy server.

• **Pripojenie prostredníctvom proxy servera** – túto možnosť použite v nasledujúcich prípadoch:

Na aktualizáciu ESET Security for Microsoft SharePoint je potrebné použiť proxy server, ktorý je odlišný od proxy servera zadaného v globálnych nastaveniach (Nástroje > Proxy server). V takomto prípade je však potrebné definovať nasledujúce nastavenia: adresa Proxy servera, komunikačný Port (predvolene 3128) a v prípade potreby aj Prihlasovacie meno a Heslo pre proxy server.
Proxy server používaný pri aktualizácii ESET Security for Microsoft SharePoint je iný než globálne nastavený proxy server.
Váš počítač je pripojený na internet cez proxy server. Nastavenia sú prevzaté z prehliadača Internet Explorer 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 HTTP Proxy v tejto sekcii. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií z aktualizačných serverov.

Poznámka:
Overovacie údaje, ako **Prihlasovacie meno** a **Heslo**, sú určené pre prístup k proxy serveru. Príslušné polia vyplňte len v prípade, že sa tieto údaje vyžadujú. Berte na vedomie, že tieto polia nie sú určené pre vaše prihlasovacie meno a heslo pre ESET Security for Microsoft SharePoint a mali by byť vyplnené len v prípade, ak je na pripojenie na internet cez proxy server potrebné heslo.

Použiť priame pripojenie, ak nie je dostupný proxy server

Ak je produkt nakonfigurovaný tak, aby používal HTTP Proxy a proxy nie je k dispozícii, produkt obíde proxy a bude komunikovať priamo so servermi spoločnosti ESET.

Zdieľané lokality systému Windows

Pri aktualizácii z lokálneho servera s operačným systémom Windows sa na vytvorenie spojenia štandardne

vyžaduje overenie.

Pre pripojenie do LAN vystupovať ako

Pre nastavenie svojho účtu vyberte jednu z nasledujúcich možností:

- **Systémový účet (predvolený)** – na účely overenia použite systémový účet. Za normálnych okolností overenie nebude vykonané, ak nie sú nastavené overovacie údaje v hlavných nastaveniach aktualizácie.
- **Aktuálne prihlásený používateľ** – ak sa použije táto možnosť, program sa bude overovať pod účtom aktuálne prihláseného používateľa. Nevýhodou v prípade tohto nastavenia je absencia možnosti pripojenia na server a následnej aktualizácie, ak nie je na počítači prihlásený žiadny používateľ.
- **Určený používateľ** – táto možnosť umožňuje vybrať na účely overenia konkrétneho používateľa. 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 aktualizácia nebude stiahnutá.

Upozornenie:
Pri použití možností **Aktuálne prihlásený používateľ** a **Určený používateľ** môže nastať chyba pri zmene identity programu na požadovaného používateľa. Z toho dôvodu odporúčame pri pripojení do LAN nastaviť overovacie údaje v hlavných nastaveniach aktualizácie. V týchto nastaveniach je potrebné uviesť údaje v nasledujúcom tvare: *domain_name**user* (v prípade pracovnej skupiny je to *workgroup_name**name*) a heslo. Pri aktualizácii cez HTTP nie je štandardne potrebné zadávať overovacie údaje.

Po dokončení aktualizácie odpojiť zo servera

Táto možnosť slúži na zrušenie spojenia so serverom a môže byť použitá v prípade, keď po stiahnutí aktualizácie ostáva spojenie naďalej aktívne.

Aktualizačný mirror

Možnosti konfigurácie pre lokálny mirror server sa nachádzajú v strome **Rozšírených nastavení** (F5) v časti **Aktualizácia** > **Profily** > karta Aktualizačný mirror.

Vrátenie zmien aktualizácií

Ak kliknete na **Vrátenie zmien**, bude potrebné vybrať čas z roletového menu Časový interval, ktorý určuje, na ako dlho budú aktualizácie detekčného jadra a programových súčastí zastavené.

Ak si želáte neskôr manuálne zapnúť pravidelné aktualizácie, vyberte možnosť **Do odvolania**. Pretože táto možnosť predstavuje potenciálne bezpečnostné riziko, označenie tejto možnosti neodporúčame.

Detekčné jadro je znížené na verziu, ktorá je uložená na disku počítača ako obraz a je najstaršia.

Naplánovaná úloha – Aktualizácia

Nastavenie hlavného a alternatívneho profilu pre aktualizáciu umožňuje vykonávať aktualizáciu z dvoch miest. Alternatívny profil bude použitý v prípade, že z prvého sa aktualizáciu nepodarí vykonať. Túto možnosť je možné využiť napríklad pre notebooky, ktoré sú používané v lokálnej LAN sieti a zároveň aj v iných sieťach s pripojením na internet. V prípade neúspešnej aktualizácie z hlavného profilu s nastavením na lokálnu LAN bude aktualizácia vykonaná z alternatívneho profilu, ktorý bude nastavený pre aktualizáciu priamo zo serverov spoločnosti ESET.

Príklad:
Nižšie spomenutý postup vám pomôže pri upravovaní úlohy určenej na zmenu **pravidelnej automatickej aktualizácie**.
1. V hlavnom okne **Plánovača** vyberte úlohu **Aktualizácia** s názvom **Pravidelná automatická aktualizácia** a kliknite na **Upraviť**, čím sa otvorí sprievodca nastavením.
2. Vyberte naplánovanú úlohu a jednu z možností načasovania podľa toho, kedy chcete danú úlohu spustiť
3. Ak chcete zabrániť tomu, aby sa úloha vykonala, ak je systém napájaný z batérie (napr. UPS), kliknite na tlačidlo vedľa možnosti **Nespúšťať úlohu, ak je počítač napájaný z batérie**.
4. Vyberte aktualizačný profil, ktorý bude použitý pri aktualizácii. Vyberte akciu, ktorá bude vykonaná v prípade zlyhania úlohy.
5. Kliknite na **Dokončiť** pre dokončenie nastavenia úlohy.

Aktualizačný mirror server

Otvorte ESET Security for Microsoft SharePoint
Stlačte F5 > Aktualizácia > Profily > Aktualizačný mirror

ESET Security for Microsoft SharePoint umožňuje vytváranie kópie aktualizácie, z ktorej sa môžu aktualizovať ďalšie stanice nachádzajúce sa v sieti. Použitie funkcie „mirror“ – vytváranie kópie aktualizačných súborov na lokálnej sieti je výhodné použiť hlavne pri väčších sieťach, kde by množstvo dát pri aktualizovaní každého počítača cez internet spôsobovalo veľký prenos a vyťaženie kapacít liniek. Preto sa odporúča aktualizovať len jeden objekt v sieti priamo z aktualizačných serverov cez internet a následne aktualizáciu sprístupniť pomocou mirror servera ostatným objektom v lokálnej sieti. Aktualizáciou staníc z mirroru sa zabezpečí rozloženie zaťaženia siete a tiež zníženie prenosu dát.

Aktualizačný mirror

Vytvárať kópie aktualizácií

Sprístupnia sa nastavenia mirroru.

Úložný priečinok

Kliknite na **Odstrániť**, ak chcete zmeniť prednastavený priečinok na ukladanie aktualizačných súborov *C:\ProgramData\ESET\ESET Security\mirror.* Ak chcete vyhľadať priečinok na lokálnom počítači alebo chcete vyhľadať zdieľaný sieťový priečinok, kliknite na **Upraviť**. V prípade, že sa na prístup k priečinku vyžaduje overenie, je potrebné do príslušných polí zadať Prihlasovacie meno a Heslo. Ak je zvolený priečinok umiestnený na sieťovom disku spustenom pod operačným systémom Windows NT/2000/XP, je potrebné zadať prihlasovacie meno a heslo používateľa s oprávnením na zápis do zvoleného priečinka.
Meno používateľa zadávajte vo formáte *Domain/User* alebo *Workgroup/User*. Zároveň je potrebné zadať príslušné heslá.

Aktualizácia programových súčastí

Súbory

Pri nastavovaní mirroru môžete špecifikovať jazykové verzie aktualizácií, ktoré budú stiahnuté. Jazyk musí byť podporovaný mirror serverom nastaveným používateľom.

Automaticky aktualizovať programové súčasti

Povolí inštaláciu nových a aktualizáciu existujúcich programových súčastí. Aktualizácia môže prebiehať automaticky bez zásahu používateľa alebo s informovaním a výzvou na jej potvrdenie od používateľa. Aktualizácia samotného produktu si zvyčajne vyžaduje reštart počítača.

Aktualizovať programové súčasti

Aktualizuje programové súčasti na najnovšiu verziu.

HTTP server

Port servera

V rámci predvolených nastavení je port servera preddefinovaný na 2221. Ak používate iný port, zmeňte túto hodnotu.

Overenie

Zvoľte metódu overenia, ktorá bude použitá na prístup k aktualizačným súborom. Na výber sú tieto možnosti: **Žiadna**, **Základná** a **NTLM**.

- Zvolením možnosti **Základná** zabezpečíte, že prihlasovacie meno a heslo bude šifrované jednoduchou metódou kódovania base64.
- Možnosť **NTLM** zabezpečí kódovanie prostredníctvom bezpečnej metódy kódovania. Pri overovaní sa používajú používatelia vytvorení na stanici zdieľajúcej aktualizáciu.
- Prednastavená je možnosť **Žiadna**, ktorá sprístupňuje aktualizačné súbory bez potreby overenia.

Upozornenie:
Pri sprístupnení aktualizačných súborov prostredníctvom HTTP servera musí byť mirror priečinok umiestnený na rovnakom počítači ako ESET Security for Microsoft SharePoint, ktorý mirror vytvára.

SSL pre HTTP server

Ak chcete prevádzkovať HTTP server s podporou HTTPS (SSL), pripojte váš **súbor obsahujúci reťazec certifikátov** alebo vygenerujte certifikát s vlastným podpisom. Sú dostupné tieto typy certifikátov: PEM, PFX a ASN. Pre dodatočné zabezpečenie môžete použiť na sťahovanie súborov protokol HTTPS. Pri použití tohoto protokolu je takmer nemožné vystopovať prihlasovacie údaje a inú komunikáciu na sieti.
Typ súkromného kľúča je predvolene nastavený ako **Integrovaný** (preto nie je dostupná možnosť Súbor obsahujúci súkromný kľúč). To znamená, že súkromný kľúč je súčasťou reťaze certifikátov.

Možnosti pripojenia

Zdieľané lokality systému Windows

Pri aktualizácii z lokálneho servera s operačným systémom Windows sa na vytvorenie spojenia štandardne vyžaduje overenie.

Pre pripojenie do LAN vystupovať ako

Pre nastavenie svojho účtu vyberte jednu z nasledujúcich možností:

- **Systémový účet (predvolený)** – na účely overenia použite systémový účet. Za normálnych okolností overenie nebude vykonané, ak nie sú nastavené overovacie údaje v hlavných nastaveniach aktualizácie.
- **Aktuálne prihlásený používateľ** – ak sa použije táto možnosť, program sa bude overovať pod účtom aktuálne prihláseného používateľa. Nevýhodou v prípade tohto nastavenia je absencia možnosti pripojenia na server a následnej aktualizácie, ak nie je na počítači prihlásený žiadny používateľ.
- **Určený používateľ** – táto možnosť umožňuje vybrať na účely overenia konkrétneho používateľa. 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 aktualizácia nebude stiahnutá.

Upozornenie:
Pri použití možností **Aktuálne prihlásený používateľ** a **Určený používateľ** môže nastať chyba pri zmene identity programu na požadovaného používateľa. Z toho dôvodu odporúčame pri pripojení do LAN nastaviť overovacie údaje v hlavných nastaveniach aktualizácie. V týchto nastaveniach je potrebné uviesť údaje v nasledujúcom tvare: *domain_name**user* (v prípade pracovnej skupiny je to *workgroup_name**name*) a heslo. Pri aktualizácii cez HTTP nie je štandardne potrebné zadávať overovacie údaje.

Po dokončení aktualizácie odpojiť zo servera

Táto možnosť slúži na zrušenie spojenia so serverom a môže byť použitá v prípade, keď po stiahnutí aktualizácie ostáva spojenie naďalej aktívne.

Ochrana siete

Zapnúť ochranu pred sieťovými útokmi (IDS)

Umožňuje vám nastaviť prístup k niektorým službám bežiacim na vašom počítači z dôveryhodnej zóny a zapnúť alebo vypnúť detekciu viacerých typov útokov a zneužití, ktoré môžu poškodiť váš počítač.

Zapnúť ochranu pred botnetmi

Odhaľuje a blokuje komunikáciu spojenú s nebezpečnými riadiacimi C&C servermi rozpoznávaním charakteristík, ktoré naznačujú, že počítač je infikovaný a bot sa snaží komunikovať s riadiacim serverom.

IDS výnimky

IDS výnimky si môžete predstaviť ako pravidlá ochrany siete. Kliknutím na Upraviť ich môžete definovať.

Detekcia útokov:

Protokol SMB – odhaľuje a blokuje rôzne zraniteľnosti v SMB protokole.
Protokol RPC – odhaľuje a blokuje rôzne zraniteľnosti (CVE) v RPC protokole, ktorý bol navrhnutý pre Distributed Computing Environment (DCE).
Protokol RDP – odhaľuje a blokuje rôzne zraniteľnosti (CVE) v RDP protokole (pozri popis vyššie v tejto kapitole).
Blokovať nebezpečnú adresu po detekcii útoku – IP adresy, ktoré boli zachytené ako zdroj útokov, sú pridané na blacklist a komunikácia z nich 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 relácie SMB na zaistenie bezpečnejšieho mechanizmu autentifikácie ako v prípade LAN Manager Challenge/Response (LM). Schéma LM je považovaná za slabú a neodporúča sa ju používať.
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 služby MSRPC.

IDS výnimky

IDS (Intrusion Detection System) výnimky sú v podstate pravidlá ochrany siete. Jednotlivé výnimky sú vyhodnocované smerom zhora nadol. Editor IDS výnimiek vám umožňuje prispôsobiť správanie ochrany siete podľa rôznych IDS výnimiek. Aplikuje sa prvá zhodná výnimka, a to osobitne pre každý typ akcie (Blokovať, Oznámiť, Zapísať do protokolu). Pomocou tlačidiel **Začiatok**/**Hore**/**Dole**/**Koniec** môžete upraviť prioritu výnimiek. Pre vytvorenie novej IDS výnimky kliknite na **Pridať**. Kliknutím na **Upraviť** môžete zmeniť existujúcu IDS výnimku a kliknutím na **Odstrániť** môžete výnimku odstrániť.

Z roletového menu vyberte typ **Upozornenia**. Zadajte **Názov hrozby** a vyberte **Smer**. Vyhľadajte **Aplikáciu**, pre ktorú chcete vytvoriť výnimku. Zadajte zoznam IP adries (IPv4 alebo IPv6) alebo podsietí. Ak zadávate viacero položiek, použite ako oddeľovač čiarku.

Nastavte **Akciu** pre IDS výnimku výberom jednej z možností nachádzajúcich sa v roletovom menu (**Predvolená**, **Áno**, **Nie**). Tento postup zopakujte pre každý typ akcie (**Blokovať**, **Oznámiť**, **Zapísať do protokolu**).

> PRÍKLAD
> Ak chcete, aby sa zobrazilo oznámenie v prípade, že dôjde k výskytu IDS výnimky, a zároveň chcete, aby bol do protokolu zapísaný čas výskytu danej udalosti, ponechajte pre typ akcie **Blokovať** aktívnu možnosť **Predvolené hodnoty** a pre ostatné dva typy akcie (**Oznámiť** a **Zapísať do protokolu**) vyberte z roletového menu možnosť **Áno**.

Dočasný blacklist IP adries

Kliknutím zobrazíte zoznam IP adries, ktoré boli zachytené ako zdroj útokov a pridané na blacklist s cieľom na istý čas zablokovať spojenie. Zobrazuje zablokované **IP adresy**.

Dôvod blokovania

Zobrazuje typ zablokovaného útoku prichádzajúceho z konkrétnej adresy (napr. útok súvisiaci so skenovaním TCP portov).

Časový limit

Zobrazuje čas a dátum, keď bude adresa odstránená z blacklistu.

Odstrániť/Odstrániť všetky

Odstráni označenú IP adresu z dočasného blacklistu predtým, ako dôjde k automatickému odstráneniu, prípadne ihneď odstráni z blacklistu všetky adresy.

Pridať výnimku

Pridá výnimku firewallu do filtrovania IDS pre vybrané IP adresy.

Web a e-mail

V tejto sekcii môžete nakonfigurovať filtrovanie protokolov, ochranu e-mailových klientov, ochranu prístupu na web a antiphishingovú ochranu a zabezpečiť tak svoj server počas pripojenia na internet.

Ochrana e-mailových klientov

Kontroluje e-mailovú komunikáciu, chráni pred škodlivým kódom a umožňuje vám zvoliť si akciu, ktorá bude vykonaná v prípade zistenia infiltrácie.

Ochrana prístupu na web

Spočíva hlavne v monitorovaní komunikácie prehliadačov internetových stránok so servermi, ktorá prebieha podľa pravidiel protokolu HTTP a HTTPS. Táto funkcia vám tiež umožňuje blokovať, povoliť alebo vylúčiť z

kontroly konkrétne URL adresy.

Filtrovanie protokolov

Ide o pokročilú ochranu pre aplikačné protokoly, ktorá je vykonávaná prostredníctvom jadra ThreatSense. Táto kontrola pracuje automaticky bez ohľadu na to, či je používaný webový prehliadač alebo e-mailový klient. Pracuje tiež so šifrovanou (SSL/TLS) komunikáciou.

Antiphishingová ochrana

Umožňuje vám blokovať webové stránky známe týmto typom obsahu.

Filtrovanie protokolov

Antimalvérová ochrana aplikačných protokolov je vykonávaná prostredníctvom jadra ThreatSense, v ktorom sú sústredené viaceré pokročilé metódy detekcie škodlivého softvéru. Filtrovanie protokolov pracuje automaticky bez ohľadu na používaný webový prehliadač alebo e-mailový klient. Ak je filtrovanie protokolov povolené, ESET Security for Microsoft SharePoint bude kontrolovať komunikáciu, ktorá využíva SSL/TLS protokol. Túto funkciu môže povoliť v sekcii **Web a e-mail** > SSL/TLS.

Zapnúť kontrolu obsahu aplikačných protokolov

Moduly ESET Security for Microsoft SharePoint (**Ochrana prístupu na web**, **Ochrana e-mailových protokolov** a **Antiphishingová ochrana**) sú závislé od tohto nastavenia a nebudú bez neho funkčné.

Vylúčené aplikácie

Pre vylúčenie aplikácií z kontroly ich označte v zozname. HTTP či POP3 komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Umožňuje vylúčiť konkrétne aplikácie z filtrovania protokolov. Kliknite na **Upraviť** a **Pridať** pre ich výber zo zoznamu aplikácií.

Dôležité:
Vylúčenie aplikácie z kontroly odporúčame iba vo výnimočných prípadoch, napr. ak aplikácia v dôsledku kontroly jej komunikácie nepracuje správne a pod.

Vylúčené IP adresy

Umožňuje vylúčiť konkrétne adresy z filtrovania protokolov. IP adresy uvedené v zozname budú vylúčené z filtrovania protokolov. Obojstranná HTTP, POP3, či IMAP komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu.

Dôležité:
Túto možnosť odporúčame používať iba v prípade dôveryhodných IP adries.

Kliknite na **Upraviť** a **Pridať** pre zadanie IP adries, rozsahu adries alebo podsiete, na ktorú sa bude vzťahovať vylúčenie. Ak označíte možnosť **Zadať viaceré hodnoty**, môžete do textového poľa zadať viacero IP adries oddelených riadkami, čiarkami alebo bodkočiarkami. Ak je povolený hromadný výber, adresy sa zobrazia v zozname vylúčených IP adries.

Poznámka:
Túto možnosť odporúčame použiť v prípade, že filtrovanie protokolov obmedzuje spojenie.

Webové a e-mailové klienty

Bezpečnosť pri prezeraní web stránok je vzhľadom na veľké množstvo škodlivého kódu dôležitou súčasťou ochrany osobného počítača. Zraniteľnosti prehliadačov a rôzne klamlivé odkazy dokážu zaviesť škodlivý kód do systému bez vedomia používateľa. Z tohto dôvodu je v ESET Security for Microsoft SharePoint venovaná pozornosť internetovým prehliadačom. Každá aplikácia, ktorá pristupuje k sieti, môže byť označená ako internetový prehliadač. Aplikácie, ktoré už používajú protokoly na komunikáciu alebo aplikácie z vybranej cesty, môžu byť pridané do zoznamu Web a email klientov.

SSL/TLS

ESET Security for Microsoft SharePoint umožňuje kontrolu na prítomnosť hrozieb v komunikáciách využívajúcich protokol SSL (Secure Sockets Layer) / TLS (Transport Layer Security).

Kontrolu možno prispôsobiť podľa toho, či certifikát využívaný danou SSL komunikáciou je dôveryhodný, neznámy, alebo je v zozname certifikátov, pre ktoré sa nebude vykonávať kontrola obsahu v protokole SSL.

Zapnúť filtrovanie protokolu SSL/TLS

Ak je táto možnosť vypnutá, nebude sa používať filtrovanie komunikácie cez protokol SSL. Režim filtrovania protokolu SSL/TLS je dostupný v nasledujúcich režimoch:

- **Automatický režim** – bude vykonávaná kontrola každej komunikácie cez protokol SSL/TLS, okrem komunikácie využívajúcej certifikáty vylúčené z kontroly. Pri komunikácii využívajúcej nový - zatiaľ neznámy certifikát, ktorý je dôveryhodne podpísaný, nebude používateľ upozornený a komunikácia sa bude automaticky filtrovať. Ak používateľ pristupuje na server používajúci nedôveryhodne podpísaný certifikát, pričom bol tento používateľom označený ako dôveryhodný (zaradený do zoznamu dôveryhodných certifikátov), prístup bude povolený a komunikácia bude filtrovaná.
- **Interaktívny režim** – v prípade, že zadáte novú stránku chránenú protokolom SSL/TLS (s neznámym certifikátom), zobrazí sa okno s možnosťou výberu akcie. Tento režim umožňuje vytvoriť zoznam certifikátov, pre ktoré sa nebude vykonávať kontrola v protokole SSL/TLS.
- **Režim politiky** – v režime politiky budú všetky SSL/TLS pripojenia okrem vylúčení filtrované.

Zoznam SSL/TLS-filtrovaných aplikácií

Môžete pridať filtrovanú aplikáciu a nastaviť jednu z akcií kontroly. Pomocou zoznamu SSL/TLS-filtrovaných aplikácií môžete prispôsobiť správanie ESET Security for Microsoft SharePoint pre konkrétne aplikácie, ako aj nastaviť zapamätanie zvolených akcií v prípade, že je pre **Režim filtrovania protokolu SSL/TLS** vybraná možnosť **Interaktívny režim**.

Zoznam známych certifikátov

Umožňuje vám nastaviť správanie programu ESET Security for Microsoft SharePoint pre konkrétne SSL certifikáty. Tento zoznam je možné zobraziť a spravovať kliknutím na Upraviť vedľa **Zoznamu známych certifikátov**.

Vylúčiť komunikáciu s dôveryhodnými doménami

Umožňuje vylúčiť komunikáciu využívajúcu SSL certifikát s rozšíreným overením (EV, Extended Validation) z kontroly protokolu.

Blokovať šifrovanú komunikáciu používajúcu zastaraný protokol SSLv2

Komunikácia využívajúca túto staršiu verziu SSL protokolu bude automaticky blokovaná.

Koreňový certifikát

Pre správne fungovanie SSL/TLS komunikácie v danom prehliadači/e-mailovom kliente je nevyhnutné, aby do jeho zoznamu známych koreňových certifikátov (vydavateľov) bol pridaný aj certifikát spoločnosti ESET. Možnosť Pridať koreňový certifikát do známych prehliadačov by teda mala ostať označená. Voľba zabezpečuje jeho automatické pridanie do známych prehliadačov (napr. Opera, Firefox). Prehliadače používajúce ukladací priestor systémových certifikátov pridaný automaticky (napr. Internet Explorer).

Pre nepodporované prehliadače môže byť certifikát exportovaný cez tlačidlo **Zobraziť certifikát** > **Podrobnosti** > **Kopírovať do súboru...** a následne manuálne importovaný do prehliadača.

Platnosť certifikátu

Ak sa nedá overiť platnosť certifikátu pomocou certifikačného úložiska TRCA

V niektorých prípadoch nie je možné overiť platnosť certifikátu webovej stránky pomocou certifikačných autorít (**Trusted Root Certification Authorities** – TRCA). To znamená, že certifikát je niekým samostatne podpísaný (napr. správcom 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. Pomocou možnosti **Zablokovať komunikáciu využívajúcu daný certifikát** sa vždy zablokuje komunikácia s webovou stránkou využívajúcou neoverený certifikát.

Ak je certifikát neplatný alebo poškodený

Znamená to, že mu vypršala platnosť alebo bol nesprávne podpísaný. V tomto prípade sa odporúča ponechať možnosť **Zablokovať komunikáciu využívajúcu daný certifikát** označenú.

Zoznam známych certifikátov

Pomocou zoznamu známych certifikátov môžete prispôsobiť správanie ESET Security for Microsoft SharePoint pre konkrétne SSL/TLS certifikáty, ako aj nastaviť zapamätanie zvolených akcií v prípade, že je pre Režim filtrovania protokolu SSL/TLS vybraná možnosť **Interaktívny režim**. Môžete nastaviť zvolený certifikát alebo použiť možnosť **Pridať** pre pridanie certifikátu z URL adresy alebo súboru. Keď sa nachádzate v okne Pridať certifikát, kliknite na URL alebo Súbor a upresnite URL adresu certifikátu alebo vyhľadajte súbor certifikátu. Nižšie nájdete zoznam polí, ktoré sú automaticky vyplnené pomocou údajov z certifikátu:

- **Názov certifikátu** – názov certifikátu.
- **Vydavateľ certifikátu** – meno tvorcu certifikátu.
- **Predmet certifikátu** – identifikácia entity asociovanej s verejným kľúčom uloženým v poli predmet verejného kľúča.

Akcia prístupu

- **Automaticky** – povolenie dôveryhodných a pýtanie sa na nedôveryhodné certifikáty.
- **Povoliť alebo Blokovať** – povolenie alebo blokovanie komunikácie zabezpečenej týmto certifikátom bez ohľadu na jeho dôveryhodnosť.
- **Spýtať sa** – zobrazí sa výzva s výberom akcie pre konkrétny certifikát.

Akcia kontroly

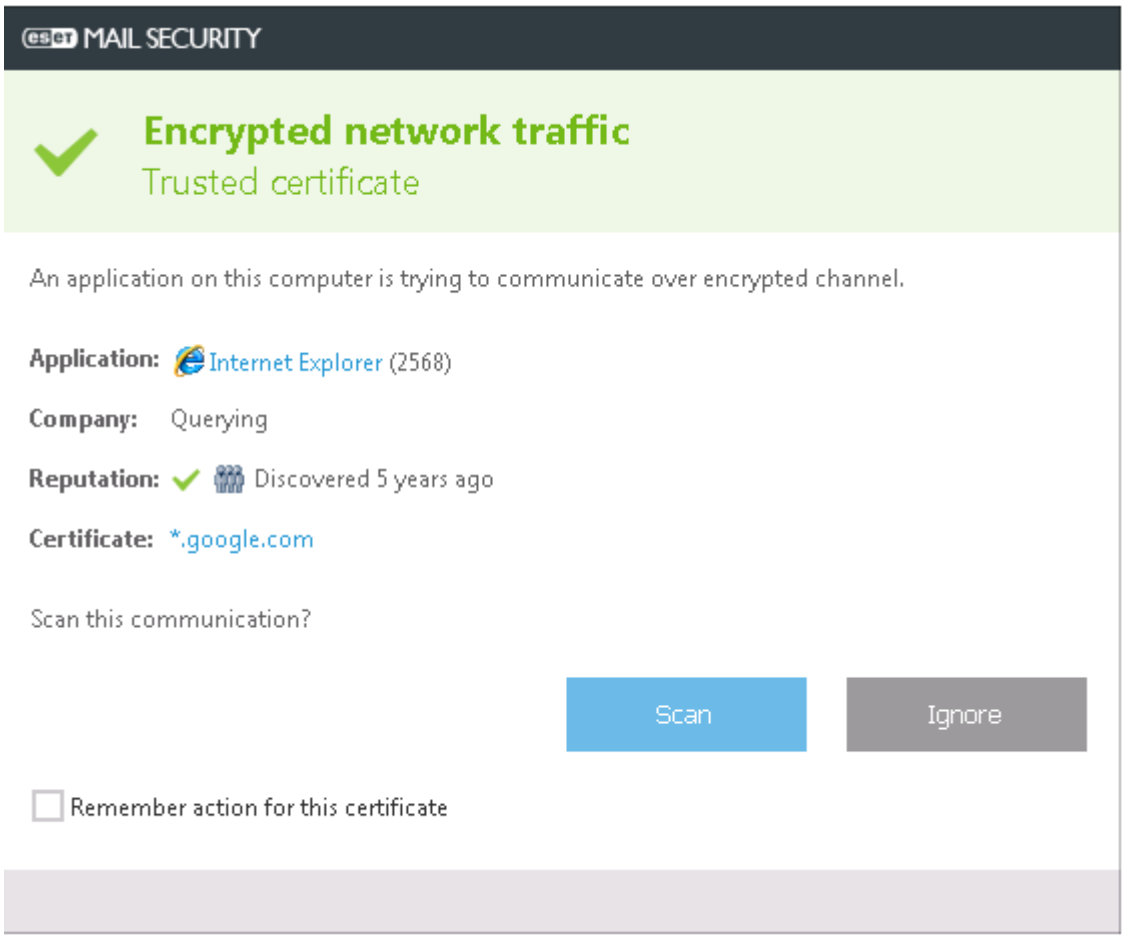
- **Automaticky** – kontrola v automatickom režime a pýtanie sa v interaktívnom režime.
- **Kontrolovať alebo Ignorovať** – akcia kontroly pri komunikácii zabezpečenej týmto certifikátom.
- **Spýtať sa** – zobrazí sa výzva s výberom akcie pre konkrétny certifikát.

Šifrovaná SSL komunikácia

Ak je počítač nastavený na kontrolu protokolu SSL, môže sa pri pokuse o šifrovanú komunikáciu zobraziť výstražné okno s možnosťami výberu, a to v dvoch situáciách:

Prvá situácia nastáva, ak stránka používa neoveriteľný alebo neplatný certifikát a program ESET Security for Microsoft SharePoint je nastavený tak, aby sa v takýchto prípadoch pýtal používateľa (predvolene len pri neoveriteľných). Zobrazí sa dialógové okno s možnosťami **Blokovať** alebo **Povoliť** spojenie.

Druhá situácia nastáva, ak je **Režim filtrovania protokolu SSL** nastavený na **Interaktívny režim**. V tom prípade sa zobrazí dialógové okno pre každú webovú stránku s možnosťami **Kontrolovať** alebo **Ignorovať** spojenia. Niektoré aplikácie kontrolujú, či ich SSL komunikácia nie je zmenená alebo sledovaná inou aplikáciou. V takomto prípade musí ESET Security for Microsoft SharePoint **Ignorovať** komunikáciu týchto aplikácií, aby nedošlo k obmedzeniu ich funkčnosti.



V oboch hore uvedených prípadoch zobrazenia výstražných okien je možné zapamätať danú akciu. Zapamätané akcie sú uložené v Zozname známych certifikátov.

Ochrana e-mailových klientov

Integrácia ESET Security for Microsoft SharePoint a e-mailových klientov zlepšuje možnosť aktívnej ochrany pred škodlivým kódom v e-mailových správach. V prípade, že je daný e-mailový klient podporovaný, je vhodné povoliť jeho integráciu s ESET Security for Microsoft SharePoint. Pri integrácii dochádza k vloženiu panela nástrojov ESET Security for Microsoft SharePoint priamo do e-mailového klienta (okrem novších verzií Windows Live Mail), čo prispieva k efektívnejšej kontrole e-mailových správ.

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 doplnku. Hlavnou výhodou je nezávislosť od použitého protokolu. V prípade šifrovanej komunikácie program takto od e-mailového klienta dostáva už dešifrované správy na kontrolu. V prípade, že integráciu nepovolíte, bude e-mailová komunikácia chránená modulom ochrany e-mailových klientov (POP3, IMAP). Kompletný zoznam podporovaných e-mailových klientov a ich verzií nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Vypnúť kontrolu pri zmene obsahu priečinka s doručenou poštou

Túto možnosť odporúčame použiť v prípade, ak pozorujete spomalenie pri práci s e-mailovým klientom (platí len pre Microsoft Outlook). Uvedená situácia môže nastať napríklad v prípade prijímania správ z úložiska správ prostredníctvom Kerio Outlook Connector Store.

Zapnúť e-mailovú ochranu prostredníctvom pluginov klienta

Pomocou tejto možnosti môžete vypnúť ochranu e-mailových klientov bez odstránenia integrácie so svojím e-mailovým klientom. Doplnky môžete vypnúť všetky naraz alebo môžete osobitne vypnúť nasledovné:

- **Prijaté e-maily** – zapnutie/vypnutie kontroly prijatých správ.
- **Odoslané e-maily** – zapnutie/vypnutie kontroly odosielaných správ.
- **Prečítané e-maily** – zapnutie/vypnutie kontroly čítaných správ.

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 e-mail** – program upozorní na infikované prílohy a odstráni celú správu.
- **Presunúť e-mail do priečinka vymazaných správ** – program bude automaticky presúvať infikované správy do priečinka Vymazané správy.
- **Presunúť e-mail do priečinka** – 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

Zapína opätovnú kontrolu po aktualizácii detekčného jadra.

Zohľadniť výsledky kontroly z iných modulov

Zohľadnenie výsledku kontroly vykonanej iným modulom (kontrola protokolov POP3, IMAP).

E-mailové protokoly

Zapnúť e-mailovú ochranu prostredníctvom filtrovania protokolov

IMAP a POP3 sú najrozšírenejšie protokoly slúžiace na príjem e-mailovej komunikácie prostredníctvom e-mailového klienta. ESET Security for Microsoft SharePoint poskytuje pre tieto protokoly ochranu bez ohľadu na používaný e-mailový klient.

ESET Security for Microsoft SharePoint podporuje kontrolu protokolov IMAPS a POP3S, ktoré používajú šifrovaný kanál na výmenu informácií medzi klientom a serverom. ESET Security for Microsoft SharePoint kontroluje aj komunikáciu šifrovanú pomocou šifrovacích metód SSL (Secure Socket Layer) a TLS (Transport Layer Security). Kontrolované sú len porty používané **protokolom IMAPS/POP3S**, pričom nezáleží na operačnom systéme.

Nastavenie kontroly protokolu IMAPS/POP3S

Šifrovaná komunikácia nie je kontrolovaná, ak sú použité predvolené nastavenia. Pre povolenie kontroly šifrovanej komunikácie prejdite do sekcie Kontrola protokolu SSL/TLS.

Číslo portu určuje, o aký port ide. Nižšie nájdete predvolené e-mailové porty pre:

Názov portu	Číslo portu	Popis
POP3	110	Predvolený POP3 nešifrovaný port.
IMAP	143	Predvolený IMAP nešifrovaný port.

Názov portu	Číslo portu	Popis
Zabezpečený IMAP (IMAP4-SSL)	585	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.
IMAP4 cez SSL (IMAPS)	993	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.
Zabezpečený POP3 (SSL-POP)	995	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.

Upozornenia a udalosti

Ochrana e-mailových klientov zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3 a IMAP. Pomocou doplnku pre Microsoft Outlook a ďalšie e-mailové klienty zabezpečuje ESET Security for Microsoft SharePoint kontrolu všetkej komunikácie daného klienta (POP3, MAPI, IMAP, HTTP). Pri kontrole prijímaných správ sú použité všetky pokročilé metódy kontroly obsiahnuté v skenovacom jadre ThreatSense. Tým je zabezpečená detekcia nebezpečných programov ešte pred aktualizáciou detekčného jadra. Kontrola protokolov POP3 a IMAP je nezávislá od typu e-mailového klienta.

Program umožňuje do kontrolovaných správ pridávať poznámku s informáciou o výsledku kontroly. Používateľ môže **Pridávať poznámku do prijatých a čítaných e-mailov**, **Pridávať do predmetu prijatých a čítaných infikovaných e-mailov** alebo tiež **Pridávať poznámku do odosielaných e-mailov**. Na tieto poznámky sa nemožno úplne spoliehať, keďže 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. Sú dostupné tieto možnosti:

- **Nikdy** – do správ nebudú pridávané žiadne poznámky s informáciou o výsledku kontroly.
- **Pridávať len do infikovaných e-mailov** – program bude pridávať poznámky len do infikovaných správ (predvolené nastavenie).
- **Do všetkých skontrolovaných e□mailov** – program bude pridávať poznámky do všetkých skontrolovaných e□mailov.

Pridávať do predmetu odosielaných infikovaných e-mailov

Túto možnosť vypnite v prípade, ak nechcete, aby bolo do predmetu infikovanej správy pridávané upozornenie týkajúce sa vírusu. Táto funkcia sa dá využiť pre jednoduché filtrovanie infikovaných správ podľa predmetu, pokiaľ to e-mailový klient umožňuje. Reťazec tiež vzbudzuje dôveryhodnosť u adresáta správy a poskytuje hodnotnú informáciu o bezpečnosti správy.

Šablóna pridávaná do predmetu infikovaných e-mailov

Túto šablónu upravte v prípade, ak chcete zmeniť formát predpony predmetu infikovanej správy. Táto funkcia doplní k pôvodnému predmetu správy, ktorý znie napríklad `Hello`, príponu `[virus]`, takže výsledný formát predmetu bude: `[virus] Hello`. Premenná `%VIRUSNAME%` predstavuje typ nájdenej hrozby.

Panel nástrojov MS Outlook

Ochrana programu Microsoft Outlook je vykonávaná prostredníctvom doplnku. Po nainštalovaní ESET Security for Microsoft SharePoint je do programu Microsoft Outlook pridaný panel obsahujúci nastavenia ochrany:

ESET Security for Microsoft SharePoint

Kliknutím na **ikonu** produktu sa otvorí hlavné okno ESET Security for Microsoft SharePoint.

Opätovná kontrola správ

Umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete tiež vybrať správy, ktoré budú kontrolované, a aktivovať opakovanú kontrolu prijatých správ. Viac informácií sa nachádza v kapitole Ochrana e-mailových klientov.

Nastavenia antivírusu

Otvorí okno s nastaveniami Ochrany e-mailových klientov.

Panel nástrojov v Outlook Express a Windows Mail

Ochrana programu Outlook Express alebo Windows Mail je vykonávaná prostredníctvom doplnku. Po nainštalovaní ESET Security for Microsoft SharePoint je do programu Outlook Express alebo Windows Mail pridaný panel s nastaveniami ochrany:

ESET Security for Microsoft SharePoint

Kliknutím na **ikonu** produktu sa otvorí hlavné okno ESET Security for Microsoft SharePoint.

Opätovná kontrola správ

Umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete tiež vybrať správy, ktoré budú kontrolované, a aktivovať opakovanú kontrolu prijatých správ. Viac informácií sa nachádza v kapitole Ochrana e-mailových klientov.

Nastavenia antivírusu

Otvorí okno s nastaveniami Ochrany e-mailových klientov.

Prispôsobiť vzhľad

Môžete si prispôsobiť vzhľad panela pre svojho e-mailového klienta. Označte túto možnosť pre prispôsobenie vzhľadu panela.

- **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

Dialógové okno s možnosťou potvrdenia alebo zamietnutia zvolenej akcie slúži ako ubezpečenie sa, že používateľ chce danú akciu naozaj vykonať, čo slúži na obmedzenie možných omylov. Dialógové okno ponúka aj možnosť vypnúť zobrazovanie potvrdzovacích správ úplne.

Opätovná kontrola správ

Integrovaný ovládací panel produktu ESET Security for Microsoft SharePoint v e-mailovom kliente umožňuje používateľom nastaviť rôzne druhy kontroly e-mailových správ. Prostredníctvom možnosti **Opätovná kontrola správ** je možné spustiť dva režimy kontroly:

- **Všetky správy v aktuálnom priečinku** – budú kontrolované všetky správy v priečinku, ktorý je aktuálne zobrazený.
- **Iba označené správy** – kontrole budú podliehať len správy, ktoré používateľ priamo označil.
- **Kontrolovať aj správy, ktoré už boli prekontrolované** – táto možnosť zabezpečí, aby sa do kontroly zahrnuli aj správy, ktoré už boli v minulosti kontrolované.

Ochrana prístupu na web

Ochrana prístupu na web spočíva hlavne v monitorovaní komunikácie prehliadačov webových stránok so servermi, ktorá prebieha podľa pravidiel protokolu HTTP a HTTPS.

Prístup na web stránky, ktoré sú známe ich 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 2 vrstvy ochrany, blokovanie na základe blacklistu a blokovanie podľa obsahu.

Základné

Odporúčame ponechať **Ochranu prístupu na web** zapnutú. Nastavenia ochrany prístupu na web sú dostupné takisto z hlavného okna ESET Security for Microsoft SharePoint v sekcii **Nastavenia** > **Web a e-mail** > **Ochrana prístupu na web**.

Zapnúť rozšírenú kontrolu skriptov prehliadača

V rámci predvolených nastavení sú všetky JavaScript programy spúšťané webovými prehliadačmi kontrolované detekčným jadrom.

Webové protokoly

Môžete nastaviť monitorovanie pre štandardné protokoly používané väčšinou webových prehliadačov. Predvolene je ESET Security for Microsoft SharePoint nakonfigurovaný na monitorovanie HTTP protokolu používaného väčšinou webových prehliadačov.

ESET Security for Microsoft SharePoint tiež podporuje šifrovanú komunikáciu HTTPS. Pri tejto komunikácii sú údaje prenášané medzi serverom a klientom šifrované. ESET Security for Microsoft SharePoint kontroluje aj komunikáciu šifrovanú pomocou šifrovacích metód SSL (Secure Socket Layer) a TLS (Transport Layer Security). Kontrolované sú len **porty používané protokolom HTTPS**, pričom nezáleží na operačnom systéme.

Šifrovaná komunikácia nie je kontrolovaná, ak sú ponechané predvolené nastavenia. Ak chcete povoliť kontrolu šifrovanej komunikácie, použite možnosť **Rozšírené nastavenia** (**F5**) > **Web a e-mail** > SSL/TLS.

Parametre ThreatSense

V tejto sekcii nájdete podrobnejšie nastavenia kontroly, ako napr. typy kontroly (e-maily, archívy, vylúčenia, obmedzenia atď.) a metódy detekcie pre Ochranu prístupu na web.

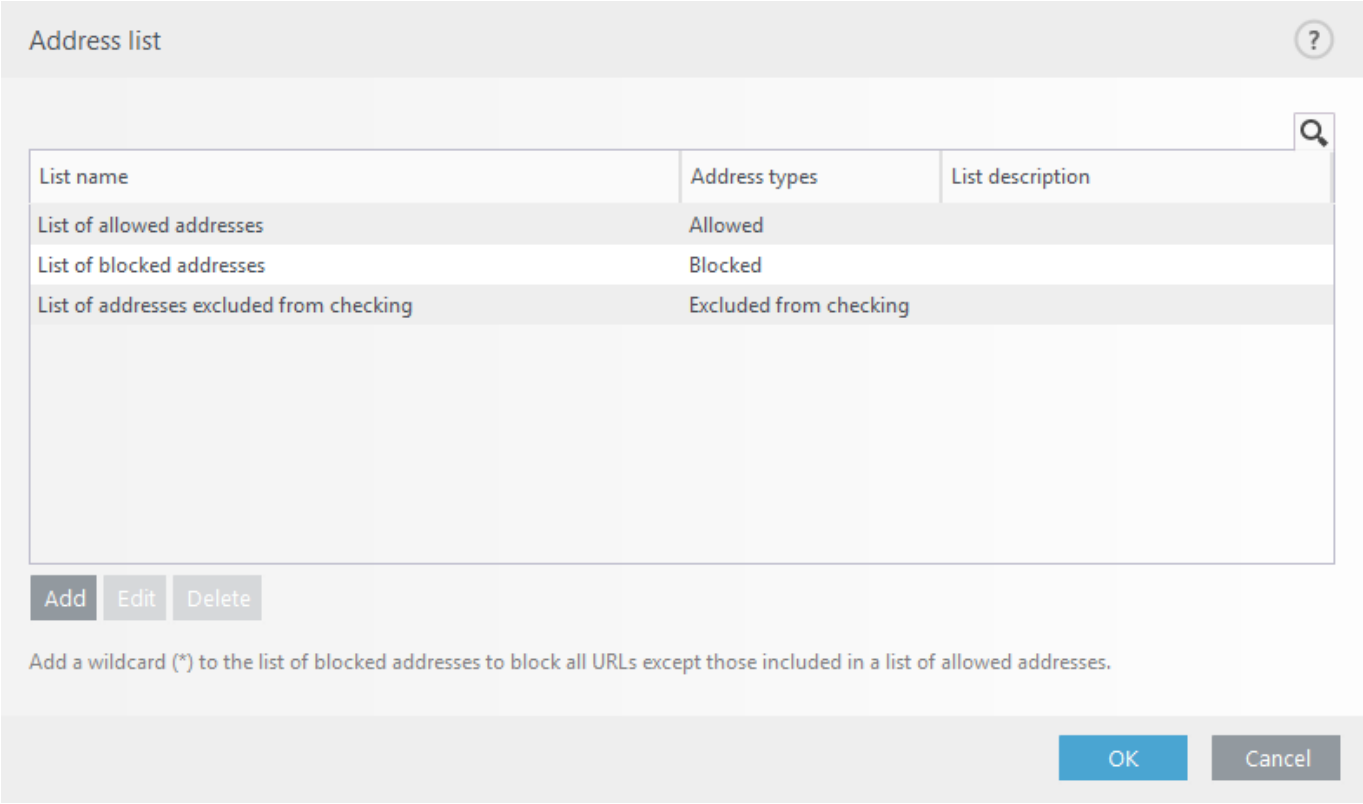
Manažment URL adries

Manažment URL adries umožňuje definovať zoznamy adries HTTP, ktoré budú blokované, povolené alebo vylúčené z kontroly. Webové adresy na zozname blokovaných adries nebudú prístupné, pokiaľ nebudú uvedené aj v zozname povolených adries. Webové adresy na zozname adries vylúčených z kontroly sú prístupné, ale nie sú kontrolované na prítomnosť škodlivého kódu. Filtrovanie protokolu SSL/TLS musí byť povolené, ak chcete okrem HTTP adries filtrovať aj adresy HTTPS. V opačnom prípade budú pridané len domény HTTPS adries, ktoré ste navštívili, a nie celé URL adresy.

Jeden zoznam blokovaných adries môže obsahovať adresy z externého verejného blacklistu a ďalší zoznam môže obsahovať váš vlastný blacklist, čo uľahčuje aktualizáciu externých zoznamov, pričom váš používateľský zoznam nebude narušený.

Kliknutím na **Upraviť** a **Pridať** vytvoríte nový zoznam adries k vopred zadefinovaným zoznamom. Toto môže byť užitočné, ak chcete logicky rozdeliť niekoľko skupín adries. Na základe predvolených nastavení sú k dispozícii tri zoznamy:

- **Zoznam adries vylúčených z kontroly** – adresy uvedené v tomto zozname nebudú kontrolované na prítomnosť škodlivého kódu.
- **Zoznam povolených adries** – ak je aktívna možnosť Povoliť prístup iba na HTTP adresy uvedené v zozname povolených adries a zoznam blokovaných adries obsahuje znak * (všetko), používateľovi bude umožnený prístup iba na adresy uvedené v zozname povolených adries. Adresy v tomto zozname budú povolené aj vtedy, keď sa nachádzajú v zozname blokovaných adries.
- **Zoznam blokovaných adries** – na adresy v tomto zozname nebude používateľom povolený prístup, ak sa súčasne nenachádzajú aj v zozname povolených adries.



Do zoznamu môžete **pridať** novú URL adresu. Zadať môžete aj viaceré hodnoty použitím oddeľovača. Kliknutím na **Upraviť** môžete zmeniť existujúcu adresu v zozname a kliknutím na **Odstrániť** môžete adresu odstrániť. Vymazať je možné len adresy pridané pomocou funkcie **Pridať**, nie je možné vymazať adresy, ktoré boli importované.

Vo všetkých zoznamoch je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Hviezdička nahrádza ľubovoľný reťazec a otáznik nahrádza ľubovoľný znak. Pri pridávaní adries vylúčených z kontroly treba byť obzvlášť opatrný, pretože tento zoznam by mal obsahovať iba overené a dôveryhodné adresy. Rovnako je potrebné dbať na správne používanie špeciálnych znakov * a ? v tomto zozname.

> Poznámka:
> Ak chcete zablokovať všetky HTTP adresy okrem adries zaradených na zoznam povolených adries, pridajte znak * do zoznamu blokovaných adries.

Vytvorenie nového zoznamu

Tento zoznam bude obsahovať požadované URL adresy/masky domén, ktoré budú blokované, povolené alebo vylúčené z kontroly. Pri vytváraní nového zoznamu je potrebné zadať nasledovné:

- **Typ zoznamu adries** – vyberte typ (Vylúčené z kontroly, Blokované alebo Povolené) z roletového menu.
- **Názov zoznamu** – názov nového zoznamu. Toto pole bude neprístupné, ak meníte nastavenia predvoleného zoznamu.
- **Popis zoznamu** – podrobné informácie k vytváranému zoznamu (nepovinné). Toto pole bude neprístupné, ak meníte nastavenia predvoleného zoznamu.
- **Zoznam je aktívny** – použite prepínač na deaktiváciu zoznamu. V prípade potreby ho môžete aktivovať neskôr.

- **Upozorniť pri použití adresy zo zoznamu** – označte túto možnosť, ak chcete byť upozornený o použití konkrétneho zoznamu pri vyhodnocovaní HTTP/HTTPS stránky, ktorú ste navštívili. Pri prístupe na blokovanú alebo povolenú stránku zo zoznamu sa zobrazí oznámenie na ploche. Oznámenie bude obsahovať názov zoznamu, v ktorom sa stránka nachádza.

- **Závažnosť zapisovania do protokolu** – z roletového menu vyberte závažnosť zapisovania do protokolu (Žiadne, Diagnostické, Informácie alebo Upozornenie). Záznamy so závažnosťou **Upozornenie** môžu byť zozbierané nástrojom ESET PROTECT.

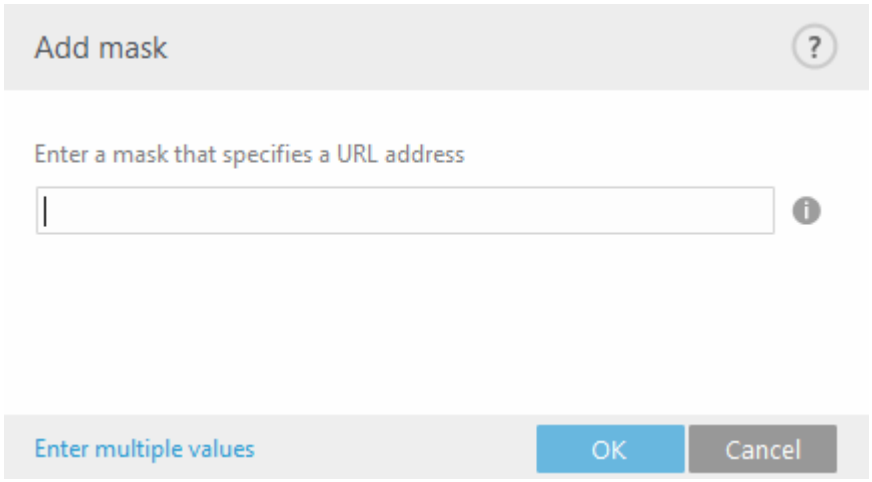
ESET Security for Microsoft SharePoint umožňuje používateľovi zablokovať prístup ku konkrétnej webovej stránke a zabrániť webovému prehliadaču v zobrazení jej obsahu. Navyše, používateľ môže definovať adresy, ktoré by mali byť z kontroly vylúčené. Ak úplný názov vzdialeného servera nie je známy alebo chce používateľ špecifikovať celú skupinu vzdialených serverov, tzv. masky môžu byť použité na identifikovanie takejto skupiny.

Masky obsahujú symboly ? a *:

- použite znak ? ako náhradu symbolu
- použite znak * ako náhradu textového reťazca

> Príklad:
> *.c?m* sa vzťahuje na všetky adresy, kde posledná časť začína písmenom c, končí písmenom m a obsahuje neznámy symbol medzi týmito dvoma znakmi (*.com*, *.cam* atď.).

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 *https://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 pre celú doménu vrátane jej subdomén použiť jednotnú masku. Napríklad maskou **.domain.com* bude vyhodnotená aj adresa *https://domain.com*. Použitie masky **domain.com* by bolo nesprávne, pretože by to mohlo tiež zodpovedať adrese *https://anotherdomain.com*.



Zadať viaceré hodnoty

Ak označíte túto možnosť, môžete do textového poľa zadať viacero URL adries oddelených novými riadkami, čiarkami alebo bodkočiarkami. Ak je povolený hromadný výber, adresy sa zobrazia v zozname.

Importovať

URL adresy môžete naimportovať z textového súboru (formát súboru `*.txt` v kódovaní UTF-8, kde budú

jednotlivé adresy oddelené novým riadkom).

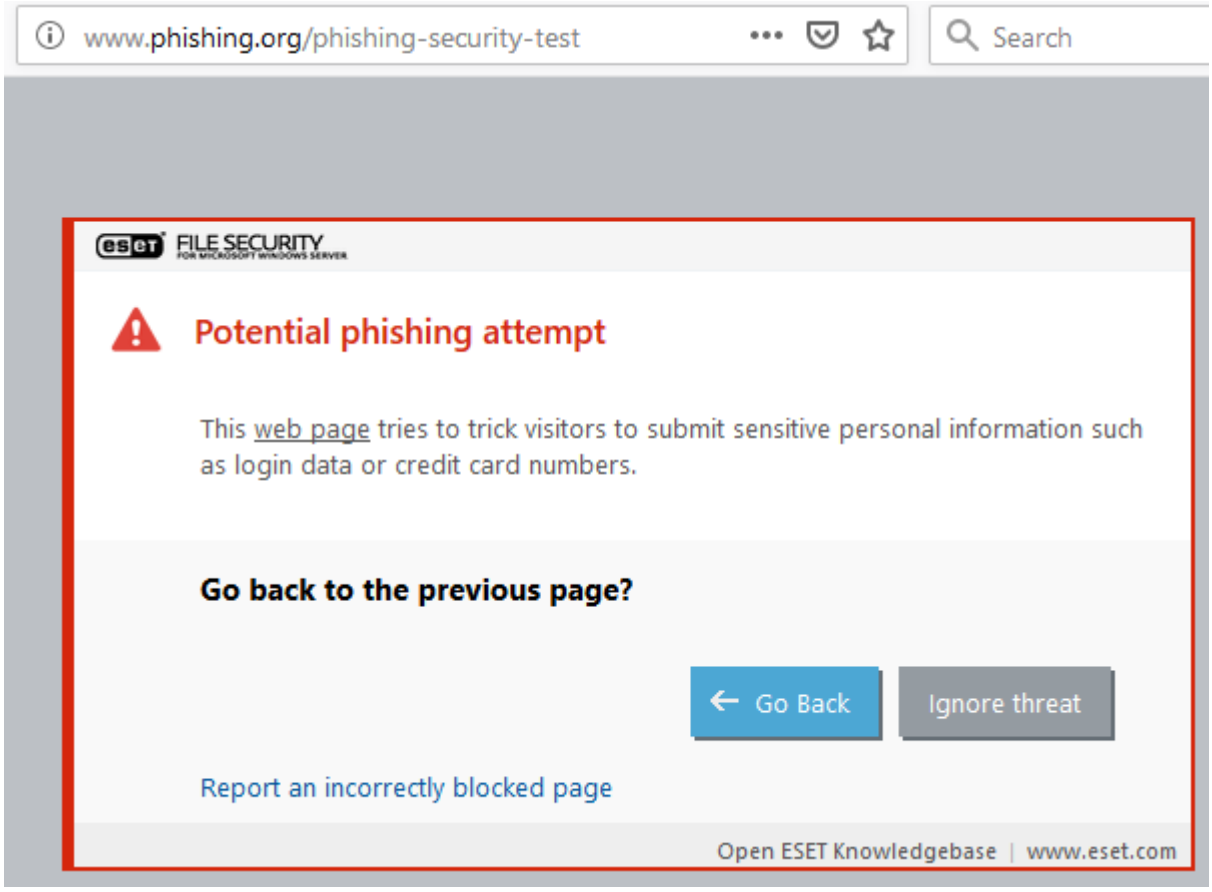


Antiphishingová ochrana

Pojmom phishing sa definuje kriminálna činnosť využívajúca tzv. sociálne inžinierstvo (manipulačné techniky na získanie dôverných informácií). Cieľom je získať citlivé údaje, ako napríklad heslá k bankovým účtom, PIN kódy a pod.

ESET Security for Microsoft SharePoint má zabudovanú antiphishingovú ochranu, ktorá blokuje webové stránky známe týmto typom obsahu. Odporúčame, aby ste povolili Antiphishingovú ochranu v programe ESET Security for Microsoft SharePoint. Viac informácií o Antiphishingovej ochrane v ESET Security for Microsoft SharePoint nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Ak otvoríte phishingovú stránku, otvorí sa vám v prehliadači nasledujúce upozornenie. Ak aj napriek tomu chcete prejsť na stránku, kliknite na možnosť **Ignorovať hrozbu** (neodporúča sa).



Poznámka:
Potenciálne phishingové stránky, ktoré boli horeuvedeným spôsobom pridané na whitelist, vypršia v produkte po niekoľkých hodinách. Pre trvalé povolenie konkrétnej webovej stránky použite nástroj Manažment URL adries.

Nahlásiť phishingovú stránku

V prípade, že sa stretnete s podozrivou webovou stránkou, môžete ju odoslať do spoločnosti ESET na analýzu. Predtým, ako webovú stránku odošlete, sa však uistite, že spĺňa nasledujúce podmienky:

- webová stránka ešte nie je v programe detegovaná,
- webová stránka sa nesprávne deteguje ako hrozba. V takomto prípade kliknite na odkaz Toto nie je phishingová stránka.

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.).

Správa zariadení

ESET Security for Microsoft SharePoint poskytuje automatickú správu externých zariadení (CD/DVD/USB atď.). Tento modul umožňuje kontrolovať (skenovať), blokovať a nastavovať rozšírené prístupové práva a pravidlá filtrovania, ako aj nastavovať prístup konkrétneho používateľa k zariadeniu. Toto môže byť užitočné v prípade, že správca chce, aby používatelia nemohli používať externé zariadenia s nežiaducim obsahom.

Poznámka:
Ak povolíte správu zariadení pomocou možnosti **Integrácia do systému**, v ESET Security for Microsoft SharePoint sa aktivuje funkcia Správa zariadení. Aby sa táto zmena prejavila, je nutné reštartovať počítač.

Správa zariadení sa stane aktívnou a vy budete môcť upravovať príslušné nastavenia. Ak je detegované zariadenie, ktoré je blokované existujúcim pravidlom, v pravom dolnom rohu sa zobrazí príslušné oznámenie a prístup k zariadeniu bude zamietnutý.

Pravidlá

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

Skupiny

Kliknutím na možnosť Upraviť môžete spravovať skupiny zariadení. Pridať alebo odstrániť zariadenia zo zoznamu môžete vytvorením novej skupiny zariadení alebo vybraním existujúcej.

Poznámka:
V sekcii Protokoly si môžete prezrieť záznamy protokolu správy zariadení.

Pravidlá zariadení

Zariadenia môžu byť povolené alebo blokované vzhľadom na používateľa, skupinu používateľov alebo podľa vybraných parametrov nastavených v pravidle. Zoznam pravidiel pozostáva z niekoľkých parametrov, akými sú názov, typ externého zariadenia, akcia vykonaná po zistení zariadenia a rozsah vytvorených protokolov.

Môžete **pridať** nové pravidlo alebo upraviť nastavenia existujúceho pravidla. Do poľa **Názov** zadajte popis pravidla pre 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

Pravidlá môžete obmedziť pomocou časových intervalov. Najprv vytvorte časový interval, ktorý sa následne zobrazí v roletovom menu.

Typ zariadenia

Z roletového menu vyberte typ externého zariadenia (disk, prenosné zariadenie, Bluetooth, FireWire atď.). Typ zariadenia je prevzatý od operačného systému a je uvedený v systémovej Správe zariadení (Device manager), ak je zariadenie pripojené k počítaču. Úložné zariadenia môžu byť externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Čítačky Smart kariet zahŕňajú všetky čítačky kariet s integrovaným obvodom, ako sú SIM karty alebo overovacie karty. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty, ktoré neposkytujú informácie o používateľovi, iba o jeho akciách. Z toho vyplýva, že môžu byť blokované len globálne pre všetkých používateľov.

Akcia

Prístupové práva k zariadeniam bez úložiska môžu byť povolené alebo blokované. Prístupové práva k zariadeniam s úložiskom môžu byť nasledovné:

- **Čítanie/Zápis** – všetky práva nad zariadením.
- **Blokovať** – prístup k zariadeniu nebude povolený.
- **Iba na čítanie** – používateľovi bude umožnený prístup k zariadeniu v režime „iba na čítanie“.
- **Upozorniť** – pri každom pripojení zariadenia k počítaču bude používateľ informovaný, či bolo zariadenie povolené alebo zablokované, a zároveň bude daná udalosť zaznamenaná do protokolu. Program si zariadenia nepamätá, čo znamená, že príslušné oznámenie sa zobrazí aj pri opätovnom pripojení rovnakého zariadenia.

> Poznámka:
> Niektoré akcie nemusia byť podporované pri niektorých zariadeniach. Ak má však zariadenie úložisko, všetky štyri akcie sú dostupné. Pre zariadenia bez úložiska sú dostupné len dve akcie (napríklad akcia **Iba na čítanie** nie je dostupná pri zariadeniach s technológiou Bluetooth, tieto zariadenia sa dajú len povoliť alebo blokovať).

Nasledujúce parametre môžu byť použité na vyladenie pravidla pre čo najlepšie prispôsobenie pravidla danému zariadeniu. Všetky parametre rozlišujú malé a veľké písmená:

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

> Poznámka:
> Ak sú hore spomenuté popisy prázdne, pravidlo bude tieto polia počas filtrovania ignorovať. Parametre vo všetkých poliach okna rozlišujú malé a veľké písmená a nepoužívajú zástupné znaky (*, ?).

Na zistenie parametrov zariadenia pripojeného k počítaču najprv vytvorte pravidlo pre povolenie daného typu zariadení a po pripojení zariadenia k počítaču nájdete jeho parametre v Protokole správy zariadení.

Z roletového menu vyberte **Závažnosť zapisovania do protokolu**:

- **Vždy** – do protokolu budú zaznamenávané všetky udalosti.
- **Diagnostické** – do protokolu budú zaznamenávané informácie potrebné pre ladenie programu.
- **Informácie** – zaznamenáva informatívne správy, napríklad o úspešnej aktualizácii, ako aj udalosti s vyššou závažnosťou.
- **Upozornenie** – zaznamenávané budú varovné správy a kritické chyby.
- **Žiadne** – nebudú vytvárané žiadne protokoly.

Pravidlo môže byť obmedzené len na určitých používateľov alebo skupiny používateľov ich pridaním do **Zoznamu používateľov**. Kliknutím na **Upraviť** vykonáte zmeny v zozname používateľov.

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

> Poznámka:
> Nie všetky typy zariadení je možné filtrovať pomocou používateľských pravidiel (napríklad zobrazovacie zariadenia neposkytujú informácie o používateľoch, ale iba o vykonaných akciách).

Na výber sú tieto funkcie:

Upraviť

Môžete zmeniť názov zvoleného pravidla alebo parametre zariadení nachádzajúcich sa v danej skupine (výrobca, model a sériové číslo zariadenia).

Kopírovať

Táto funkcia slúži na vytvorenie nového pravidla s parametrami označeného pravidla.

Odstrániť

Slúži na vymazanie označeného pravidla. Ak chcete pravidlo zakázať, môžete tiež prípadne použiť začiarkavacie políčko vedľa daného pravidla. Táto možnosť je užitočná, ak nechcete pravidlo zmazať, ale len dočasne zakázať.

Načítať

Zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné. Po výbere zariadenia zo zoznamu nájdených zariadení a kliknutí na **OK** sa zobrazí okno editora pravidiel s vopred definovanými údajmi (všetky nastavenia môžete meniť).

Pravidlá, ktoré sú v zozname vyššie, majú vyššiu prioritu. Pravidlá môžete hromadne označiť a aplikovať akcie; môžete ich napríklad vymazať alebo presunúť nižšie/vyššie pomocou šípok – **Začiatok**/**Hore**/**Dole**/**Koniec**.

Skupiny zariadení

Okno Skupiny zariadení je rozdelené na dve časti. Na ľavej strane okna je zoznam existujúcich skupín a po pravej strane sa nachádza zoznam zariadení patriacich do konkrétnej skupiny. Vyberte skupinu, ktorej zariadenia chcete zobraziť.

Môžete vytvoriť viaceré skupiny zariadení, na ktoré sa budú aplikovať rôzne pravidlá. Môžete vytvoriť aj jedinú skupinu zariadení, na ktorú sa bude vzťahovať nastavenie, resp. režim **Čítanie/Zápis** alebo **Iba na čítanie**. Týmto docielite, že nerozpoznané zariadenia budú po pripojení k vášmu počítaču blokované.

> Upozornenie:
> Externé zariadenia pripojené k vášmu počítaču môžu predstavovať bezpečnostné riziko.

Na výber sú tieto funkcie:

Pridať

Vytvorenie novej skupiny zariadení zadaním jej názvu alebo pridanie zariadenia do existujúcej skupiny (môžete upresniť aj podrobnosti, ako napr. názov výrobcu, model a sériové číslo).

Upraviť

Môžete zmeniť názov vybranej skupiny alebo parametre zariadení nachádzajúcich sa v danej skupine (výrobca, model a sériové číslo zariadenia).

Odstrániť

Odstránenie vybranej skupiny alebo zariadenia. Ak chcete pravidlo zakázať, môžete tiež prípadne použiť začiarkavacie políčko vedľa daného pravidla. Táto možnosť je užitočná, ak nechcete pravidlo zmazať, ale len dočasne zakázať.

Spustiť import

Importuje zo súboru zoznam sériových čísel zariadení.

Načítať

Zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné. Po výbere zariadenia zo zoznamu nájdených zariadení a kliknutí na **OK** sa zobrazí okno editora pravidiel s vopred definovanými údajmi (všetky nastavenia môžete meniť).

Po dokončení úprav kliknite na **OK**. Ak chcete opustiť okno **Skupiny zariadení** bez zmeny nastavení, kliknite na **Zrušiť**.

> Poznámka:
> Niektoré akcie nemusia byť podporované pri niektorých zariadeniach. Ak má však zariadenie úložisko, všetky štyri akcie sú dostupné. Pre zariadenia bez úložiska sú dostupné len dve akcie (napríklad akcia Iba na čítanie nie je dostupná pri zariadeniach s technológiou Bluetooth, tieto zariadenia sa dajú len povoliť alebo blokovať).

Konfigurácia nástrojov

V sekcii Nástroje môžete zmeniť rozšírené nastavenia pre nasledujúce položky:

- Časové intervaly
- Ciele kontroly v ESET PROTECT
- Režim prepísania
- ESET CMD
- ESET RMM
- Licencia
- Poskytovateľ WMI
- Protokoly
- Proxy server
- E-mailové oznámenia
- Prezentačný režim
- Diagnostika
- Klaster

Časové intervaly

Časové intervaly sa používajú v rámci pravidiel správy zariadení a slúžia na obmedzovanie pravidiel v prípade, že sú aplikované. Môžete vytvoriť časový interval a použiť ho pri pridávaní nových pravidiel alebo pri úprave existujúcich pravidiel (parameter **Uplatňovať v intervale**). Toto vám umožní definovať bežne používané časové intervaly (pracovný čas, víkend atď.) a následne ich jednoducho opäť použiť bez potreby opätovného definovania časových rozsahov pre každé pravidlo. Časový interval by sa mal vzťahovať na akýkoľvek relevantný typ pravidla,

ktoré podporuje ovládanie pomocou času.

Microsoft Windows® Update

Aktualizácie systému poskytujú dôležité opravy potenciálnych zraniteľností v systéme a pomáhajú zabezpečiť maximálnu úroveň ochrany vášho počítača. Preto je vhodné nainštalovať aktualizácie systému Microsoft Windows hneď ako sú dostupné. ESET Security for Microsoft SharePoint vás informuje o chýbajúcich systémových aktualizáciách na úrovni, ktorú je možné nastaviť. Sú dostupné tieto úrovne:

- **Žiadne aktualizácie** – nebudú ponúkané žiadne aktualizácie.
- **Voliteľné aktualizácie** – 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.

Modul kontroly cez príkazový riadok

Manuálnu kontrolu môžete okrem eShell spustiť aj prostredníctvom príkazového riadka pomocou nástroja `ecls.exe`, ktorý je umiestnený v inštalačnom priečinku produktu ESET Security for Microsoft SharePoint.

Nižšie je uvedený zoznam parametrov a prepínačov:

Možnosti:

`/base-dir=FOLDER`	načítať moduly z PRIEČINKA
`/quar-dir=FOLDER`	umiestniť PRIEČINOK do karantény
`/exclude=MASK`	vylúčiť z kontroly súbory zodpovedajúce MASKE
`/subdir`	kontrolovať podpriečinky (predvolené)
`/no-subdir`	nekontrolovať podpriečinky
`/max-subdir-level=LEVEL`	podpriečinky kontrolovať len do úrovne
`/symlink`	sledovať symbolické prepojenia (predvolené)
`/no-symlink`	preskočiť symbolické prepojenia
`/ads`	kontrolovať ADS (predvolené)
`/no-ads`	nekontrolovať ADS
`/log-file=FILE`	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=SIZE	kontrolovať len súbory menšie ako VEĽKOSŤ MB (predvolene 0 = neobmedzené)
/max-arch-level=LEVEL	podradené archívy kontrolovať len do úrovne
/scan-timeout=LIMIT	archívy kontrolovať najviac LIMIT s
/max-arch-size=SIZE	kontrolovať len súbory v archíve menšie ako VEĽKOSŤ MB (predvolene 0 = neobmedzené)
/max-sfx-size=SIZE	kontrolovať len súbory v samorozbaľovacích archívoch menšie ako VEĽKOSŤ MB (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=EXTENSIONS	vylúčiť z kontroly súborové PRÍPONY oddelené dvojbodkou

`/clean-mode=MODE`	použiť REŽIM liečenia infikovaných objektov Sú dostupné tieto možnosti: • `none` (predvolené) – nenastane žiadne automatické liečenie. • `standard` – ecls.exe sa pokúsi o automatické vyliečenie alebo odstránenie infikovaných súborov. • `strict` – ecls.exe sa pokúsi o automatické vyliečenie alebo odstránenie infikovaných súborov bez zásahu používateľa (pred odstránením súborov sa vám nezobrazí výzva na potvrdenie akcie). • `rigorous` – ecls.exe odstráni súbory bez pokusu o vyliečenie, a to bez ohľadu na to, o aké súbory ide. • `delete` – ecls.exe odstráni súbory bez pokusu o vyliečenie, ale nepristúpi k odstráneniu citlivých súborov, ako sú systémové súbory vo Windows.
`/quarantine`	uložiť kópie infikovaných súborov (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 k súborom

Návratové hodnoty:

`0`	nenašla sa žiadna infekcia
`1`	našla sa infekcia, ale bola odstránená
`10`	niektoré súbory nemohli byť skontrolované (a môžu obsahovať infekciu)
`50`	našla sa infekcia
`100`	chyba (návratové hodnoty väčšie ako 100 znamenajú, že súbor nebol skontrolovaný a nemožno ho považovať za čistý)

ESET CMD

Táto funkcia umožňuje používať pokročilé príkazy ecmd. Umožňuje vám importovať a exportovať nastavenia pomocou príkazového riadka (ecmd.exe). Doposiaľ bolo možné importovať a exportovať nastavenia len prostredníctvom grafického používateľského rozhrania. ESET Security for Microsoft SharePoint nastavenia môžu byť exportované ako súbor *.xml*.

Po povolení 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** – na import konfigurácie zo súboru *.xml* sa vyžaduje heslo. Tento súbor musí byť podpísaný (bližšie informácie o podpisovaní konfiguračného súboru *.xml* nájdete nižšie). Predtým, ako môže byť importovaná nová konfigurácia, musí byť zadané heslo špecifikované v Nastaveniach prístupu. Ak nemáte nastavenú ochranu heslom, heslá sa nezhodujú alebo konfiguračný súbor *.xml* nie je podpísaný, konfigurácia nebude importovaná.

Po povolení ESET CMD môžete používať príkazový riadok na import/export konfigurácie programu ESET Security for Microsoft SharePoint. Môžete to vykonávať manuálne alebo si vytvoriť skript na účely automatizácie.

Dôležité:
Pre použitie pokročilých ecmd príkazov ich budete musieť spúšťať s oprávneniami správcu alebo spustením príkazového riadku systému Windows pomocou možnosti **Spustiť ako správca**. V opačnom prípade sa zobrazí chybové hlásenie **Error executing command.**. Pri exportovaní konfigurácie musí tiež existovať cieľový priečinok. Príkaz pre export funguje aj v prípade, že je vypnutá možnosť ESET CMD.

Príklad:
Príkaz pre export nastavení:
`ecmd /getcfg c:\config\settings.xml`

Príkaz pre import nastavení:
`ecmd /setcfg c:\config\settings.xml`

Poznámka:
Pokročilé ecmd príkazy môžu byť spúšťané len lokálne. Spustenie klientskej úlohy **Spustiť príkaz** pomocou nástroja ESET PROTECT nebude fungovať.

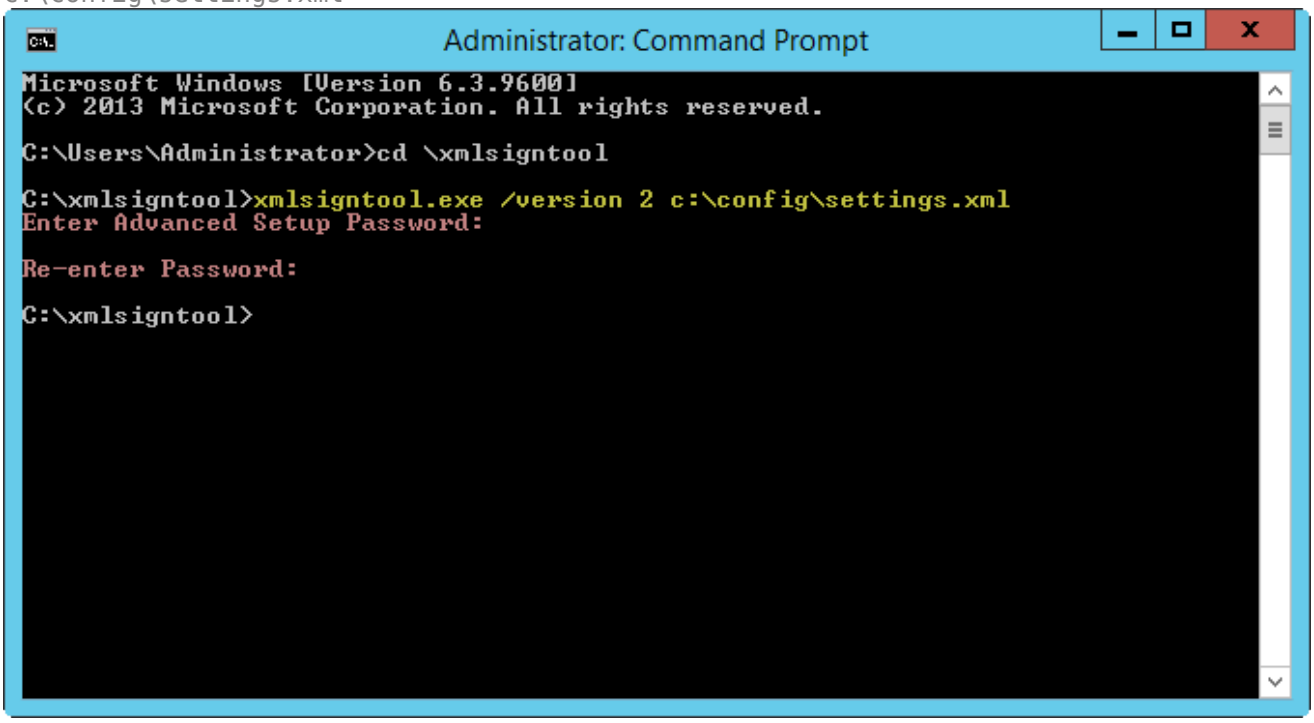
Podpisovanie konfiguračných súborov *.xml*:

1. Stiahnite si XmlSignTool.
2. Otvorte príkazový riadok systému Windows použitím možnosti **Spustiť ako správca**.
3. Prejdite do priečinka, kde sa nachádza nástroj `xmlsigntool.exe`.
4. Konfiguračný súbor *.xml* podpíšte nasledujúcim príkazom: `xmlsigntool /version 1|2 <xml_file_path>`.

Dôležité:
Hodnota parametra `/version` závisí od verzie vášho produktu ESET Security for Microsoft SharePoint. Pre ESET Security for Microsoft SharePoint 7 a novšie verzie použite `/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 môže byť pomocou ESET CMD použitý na importovanie v rámci ďalšej inštalácie ESET Security for Microsoft SharePoint.

Príklad:
Príkaz na podpísanie exportovaného konfiguračného súboru: `xmlsigntool /version 2 c:\config\settings.xml`



Poznámka:
Ak sa zmení heslo v rámci Nastavení prístupu a chcete importovať konfiguráciu, ktorá bola podpísaná skôr prostredníctvom starého hesla, môžete podpísať konfiguračný súbor *.xml* znova, a to použitím aktuálneho hesla. Tento postup vám umožní použiť starší konfiguračný súbor bez potreby jeho exportovania na iný počítač, na ktorom je spustený program ESET Security for Microsoft SharePoint.

ESET RMM

Vzdialený monitoring a správa (RMM) slúži na spravovanie a riadenie softvérových systémov (napr. na stolových počítačoch, serveroch a mobilných zariadeniach) pomocou lokálne nainštalovaného agenta, ktorý je dostupný prostredníctvom MSP (Managed Service Provider).

Zapnúť RMM

Zapne vzdialený monitoring a správu. Nato, aby ste mohli používať nástroj RMM, musíte mať oprávnenia správcu.

Pracovný režim

Z roletového menu vyberte pracovný režim pre RMM:

- **Iba bezpečné operácie –** zapne rozhranie RMM iba pre bezpečné operácie a operácie len na čítanie
- **Všetky operácie –** zapne rozhranie RMM pre všetky operácie

Spôsob overenia

Z roletového menu vyberte spôsob overenia RMM:

- **Žiadne** – nebude vykonaná žiadna kontrola cesty k aplikácii, *ermm.exe* môžete spustiť pomocou

akejkoľvek aplikácie.
- **Cesta k aplikácii** – vyberte aplikáciu, ktorá bude mať povolené spúšťať *ermm.exe*.

Súčasťou predvolenej inštalácie ESET Endpoint Security je súbor *ermm.exe*, ktorý sa nachádza v adresári produktu ESET Security for Microsoft SharePoint (predvolené umiestnenie je C:*Program Files**ESET**ESET Security for Microsoft SharePoint*). *ermm.exe* zabezpečuje výmenu dát s pluginom RMM, ktorý komunikuje s agentom RMM prepojeným so serverom RMM.

- *ermm.exe* – nástroj príkazového riadka vyvinutý spoločnosťou ESET, ktorý umožňuje správu produktov určených pre koncové zariadenia a zároveň komunikáciu s akýmkoľvek pluginom RMM.
- Plugin RMM – aplikácia tretej strany, ktorá beží lokálne na koncovom zariadení so systémom Windows. Tento plugin bol navrhnutý tak, aby komunikoval s konkrétnym agentom RMM (napr. Kaseya) a s *ermm.exe*.
- Agent RMM – aplikácia tretej strany (napr. Kaseya), ktorá beží lokálne na koncovom zariadení so systémom Windows. Agent komunikuje s pluginom RMM a serverom RMM.
- Server RMM – beží ako služba na serveri tretej strany. Medzi podporované systémy RMM patria Kaseya, Labtech, Autotask, Max Focus a Solarwinds N able.

Viac informácií o ESET RMM v ESET Security for Microsoft SharePoint nájdete v tomto článku Databázy znalostí spoločnosti ESET.

Plugin ESET Direct Endpoint Management pre riešenia RMM tretích strán

Server RMM beží ako služba na serveri tretej strany. Viac informácií nájdete v online používateľských príručkách ESET Direct Endpoint Management:

- Plugin ESET Direct Endpoint Management pre ConnectWise Automate
- Plugin ESET Direct Endpoint Management pre DattoRMM
- ESET Direct Endpoint Management pre Solarwinds N-Central
- ESET Direct Endpoint Management pre NinjaRMM

Licencia

ESET Security for Microsoft SharePoint sa pripája na licenčný server ESET niekoľkokrát za hodinu s cieľom vykonať kontrolu. Parameter **Interval kontroly** je predvolene nastavený ako **Automatický**. Ak chcete znížiť objem sieťovej komunikácie v dôsledku kontrol licencií, zmeňte Interval kontroly na **Obmedzený** a kontrola licencií sa bude vykonávať iba raz denne (a tiež po reštarte servera).

Ak je Interval kontroly nastavený ako **Obmedzený**, všetky zmeny ESET Security for Microsoft SharePoint, ktoré súvisia s licenciou a boli uskutočnené prostredníctvom nástrojov ESET Business Account a ESET MSP Administrator, sa môžu prejaviť až po jednom dni.

Poskytovateľ WMI

Funkcia Windows Management Instrumentation (WMI) je implementáciou Web-Based Enterprise Management (WBEM) od spoločnosti Microsoft, ktorá je snahou o vytvorenie technologického štandardu pre prístup k informáciám na vzdialenú správu softvéru vo firemnom prostredí.

Viac informácií nájdete na webovej stránke http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx.

ESET Poskytovateľ WMI

Účel funkcie poskytovateľa WMI je povolenie vzdialeného sledovania produktov spoločnosti ESET vo firemnom prostredí bez nutnosti inštalácie ďalšieho softvéru od spoločnosti ESET. Sprístupnením základných informácií o produkte ako napr. stavu ochrany, štatistík cez WMI rozširuje možnosti správy pre správcov firemných sietí. Správca môže na sledovanie stavu produktov spoločnosti ESET využiť niekoľko metód prístupu, ktoré WMI ponúka (príkazový riadok, skripty, monitorovacie nástroje tretích strán).

Súčasná implementácia poskytuje len prístup na čítanie k základným informáciám, akými sú nainštalované súčasti programu, stav ochrany, štatistiky kontroly, protokoly.

WMI poskytovateľ vám umožňuje použitie infraštruktúry a nástrojov Windows WMI na sledovanie stavu a protokolov bezpečnostných produktov.

Poskytnuté údaje

Všetky triedy WMI týkajúce sa produktov ESET sa nachádzajú na adrese „root\ESET“. Podporované sú nasledujúce triedy:

Všeobecné

- **ESET_Product**
- **ESET_Features**
- **ESET_Statistics**

Protokoly

- **ESET_ThreatLog**
- **ESET_EventLog**
- **ESET_ODFileScanLogs**
- **ESET_ODFileScanLogRecords**
- **ESET_ODServerScanLogs**
- **ESET_ODServerScanLogRecords**
- **ESET_HIPSLog**
- **ESET_URLLog**
- **ESET_DevCtrlLog**
- **ESET_GreylistLog**
- **ESET_MailServeg**
- **ESET_HyperVScanLogs**
- **ESET_HyperVScanLogRecords**

ESET_Product

Trieda ESET_Product môže mať len jednu inštanciu. Vlastnosti tejto triedy popisujú základné informácie o nainštalovanom produkte ESET:

- **ID** – skratka (identifikátor) vyjadrujúca typ produktu, napríklad „emsl“.
- **Name** – názov produktu, napríklad „ESET Mail Security“.

- **FullName** – úplný názov produktu, napríklad „ESET Mail Security pre IBM Domino“.
- **Version** – verzia produktu, napríklad „6.5.14003.0“.
- **VirusDBVersion** – verzia detekčného jadra, napríklad „14533 (20161201)“.
- **VirusDBLastUpdate** – dátum a čas poslednej aktualizácie detekčného jadra. Reťazec obsahuje časovú pečiatku vyjadrenú vo WMI formáte, napríklad „20161201095245.000000+060“.
- **LicenseExpiration** – dátum skončenia platnosti licencie. Reťazec obsahuje časovú pečiatku vyjadrenú vo WMI formáte.
- **KernelRunning** – hodnota typu boolean vyjadrujúca, či je služba „ekrn“ spustená na počítači (napr. „TRUE“).
- **StatusCode** – číslo vyjadrujúce stav ochrany produktu: 0 – Zelený (V poriadku), 1 – Žltý (Varovanie), 2 – Červený (Chyba)
- **StatusText** – správa vyjadrujúca dôvod zmeneného stavu ochrany, ak je stav ochrany iný ako 0.

ESET_Features

Počet inštancií sa rovná počtu funkcií produktu ESET. Každá inštancia obsahuje:

- **Name** – názov funkcie (zoznam názvov je k dispozícii nižšie).
- **Status** – stav funkcie: 0 – neaktívna, 1 – vypnutá, 2 – zapnutá

Zoznam reťazcov predstavujúcich funkcionality produktu:

- **CLIENT_FILE_AV** – rezidentná ochrana súborového systému.
- **CLIENT_WEB_AV** – ochrana prístupu na web.
- **CLIENT_DOC_AV** – ochrana dokumentov.
- **CLIENT_NET_FW** – firewall.
- **CLIENT_EMAIL_AV** – antivírusová ochrana e-mailového klienta.
- **CLIENT_EMAIL_AV** – antispamová ochrana e-mailového klienta.
- **SERVER_FILE_AV** – rezidentná ochrana súborov na chránenom serveri, napríklad súborov v databázach obsahu SharePointu v prípade programu ESET Security for Microsoft SharePoint.
- **SERVER_EMAIL_AV** – antivírusová ochrana e-mailov na chránenom serveri, napríklad e-maily v MS Exchange alebo IBM Lotus Domino.
- **SERVER_EMAIL_AS** – antispamová ochrana e-mailov na chránenom serveri, napríklad e-maily v MS Exchange alebo IBM Lotus Domino.
- **SERVER_GATEWAY_AV** – antivírusová ochrana sieťových protokolov v bráne.
- **SERVER_GATEWAY_AS** – antispamová ochrana sieťových protokolov v bráne.

ESET_Statistics

Počet inštancií sa rovná počtu typov kontroly v produkte ESET. Každá inštancia obsahuje:

- **Scanner** – reťazec pre každý druh kontroly v programe, napríklad „CLIENT_FILE“.
- **Total** – celkový počet skontrolovaných súborov.
- **Infected** – počet nájdených infikovaných súborov.
- **Cleaned** – počet vyliečených súborov.
- **Timestamp** – čas poslednej zmeny štatistík. Je vyjadrený vo WMI formáte, napríklad „20130118115511.000000+060“.
- **ResetTime** – čas posledného vynulovania počítadla štatistík. Je vyjadrený vo WMI formáte, napríklad „20130118115511.000000+060“.

Zoznam reťazcov predstavujúcich typy kontroly v produkte:

- **CLIENT_FILE**
- **CLIENT_EMAIL**
- **CLIENT_WEB**
- **SERVER_FILE**
- **SERVER_EMAIL**
- **SERVER_WEB**

ESET_ThreatLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Zachytené infiltrácie“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Scanner** – typ kontroly, pri ktorej bol protokol vytvorený.
- **ObjectType** – typ objektu, ktorý vytvoril tento protokol.
- **ObjectName** – názov objektu, ktorý vytvoril tento protokol.
- **Threat** – názov hrozby/infiltrácie, ktorá bola odhalená v objekte pomocou vlastností ObjectName a ObjectType.
- **Action** – akcia vykonaná po identifikovaní hrozby.
- **User** – používateľský účet, v ktorom bol protokol vytvorený.
- **Information** – dodatočné informácie o udalosti.
- **Hash** – hash objektu, ktorý vytvoril tento protokol.

ESET_EventLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Udalosti“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Module** – názov modulu, ktorý vytvoril tento protokol.
- **Event** – popis udalosti.
- **User** – používateľský účet, v ktorom bol protokol vytvorený.

ESET_ODFileScanLogs

Počet inštancií sa rovná počtu záznamov v protokole typu „Kontrola počítača“. Ide o ekvivalent protokolov kontroly počítača v používateľskom prostredí. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **Targets** – cieľové priečinky/objekty kontroly.
- **TotalScanned** – celkový počet skontrolovaných objektov.
- **Infected** – počet nájdených infikovaných objektov.
- **Cleaned** – počet vyliečených objektov.
- **Status** – stav procesu kontroly.

ESET_ODFileScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_ODFileScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol počítača. Pri filtrovaní inštancie len určitého protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- **LogID** – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_ODFileScanLogs).
- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Log** – správa z protokolu.

ESET_ODServerScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly servera“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **Targets** – cieľové priečinky/objekty kontroly.
- **TotalScanned** – celkový počet skontrolovaných objektov.
- **Infected** – počet nájdených infikovaných objektov.
- **Cleaned** – počet vyliečených objektov.
- **RuleHits** – celkový počet uplatnení pravidla.
- **Status** – stav procesu kontroly.

ESET_ODServerScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_ODServerScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol počítača. Pri filtrovaní inštancie len určitého protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- **LogID** – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_ ODServerScanLogs).
- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Log** – správa z protokolu.

ESET_SmtpProtectionLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Protokol SMTP ochrany“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.

- **HELODomain** – názov reťazca HELO.
- **IP** – IP adresa zdroja.
- **Sender** – odosielateľ e-mailu.
- **Recipient** – príjemca e-mailu.
- **ProtectionType** – typ použitej ochrany.
- **Action** – vykonaná akcia.
- **Reason** – dôvod vykonania akcie.
- **TimeToAccept** – počet minút, po ktorých bude e-mail prijatý.

ESET_HIPSLog

Počet inštancií sa rovná počtu záznamov v protokole typu „HIPS“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Application** – zdrojová aplikácia.
- **Target** – typ operácie.
- **Action** – akcia vykonaná modulom HIPS (napr. povolenie, zamietnutie atď.).
- **Rule** – názov pravidla, na základe ktorého je akcia vykonaná.
- **AdditionalInfo**

ESET_URLLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Filtrované webové stránky“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **URL** – URL adresa.
- **Status** – vyjadruje, čo sa stalo s URL adresou (napr. „Blokované webovou kontrolou“).
- **Application** – aplikácia, ktorá sa pokúsila získať prístup k URL adrese.
- **User** – používateľský účet, pod ktorým bola aplikácia spustená.

ESET_DevCtrlLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Správa zariadení“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Device** – názov zariadenia.
- **User** – názov používateľského účtu.
- **UserSID** – SID používateľského účtu.
- **Group** – názov skupiny používateľov.

- **GroupSID** – SID skupiny používateľov.
- **Status** – vyjadruje, čo sa stalo so zariadením (napr. „Blokovaný zápis“).
- **DeviceDetails** – dodatočné informácie o zariadení.
- **EventDetails** – dodatočné informácie o udalosti.

ESET_MailServerLog

Počet inštancií sa rovná počtu záznamov v protokole typu „E-mailový server“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **IPAddr** – IP adresa zdroja.
- **HELODomain** – názov reťazca HELO.
- **Sender** – odosielateľ e-mailu.
- **Recipient** – príjemca e-mailu.
- **Subject** – predmet e-mailovej správy.
- **ProtectionType** – typ ochrany, ktorá vykonala akciu zaznamenanú v protokole (napr. antimalvérová ochrana, antispam alebo pravidlá).
- **Action** – vykonaná akcia.
- **Reason** – dôvod, prečo bola akcia vykonaná konkrétnym typom ochrany („ProtectionType“) pre daný objekt.

ESET_HyperVScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly Hyper-V“. Ide o ekvivalent protokolov kontroly Hyper-V v používateľskom prostredí. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **Targets** – cieľové počítače/disky/zväzky, pre ktoré bude vykonaná kontrola.
- **TotalScanned** – celkový počet skontrolovaných objektov.
- **Infected** – počet nájdených infikovaných objektov.
- **Cleaned** – počet vyliečených objektov.
- **Status** – stav procesu kontroly.

ESET_HyperVScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_HyperVScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol Hyper-V. Pri filtrovaní inštancie len určitého protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- **LogID** – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_HyperVScanLogs).
- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.

- **Log** – správa z protokolu.

ESET_NetworkProtectionLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Ochrana siete“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Event** – udalosť, ktorá spúšťa akciu ochrany siete.
- **Action** – akcia vykonaná ochranou siete.
- **Source** – zdrojová adresa sieťového zariadenia.
- **Target** – cieľová adresa sieťového zariadenia.
- **Protocol** – protokol sieťovej komunikácie.
- **RuleOrWormName** – názov pravidla alebo červa súvisiaceho s udalosťou.
- **Application** – aplikácia, ktorá iniciovala sieťovú komunikáciu.
- **User** – používateľský účet, v ktorom bol protokol vytvorený.

ESET_SentFilesLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Odoslané súbory“. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo záznamu protokolu.
- **Timestamp** – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Sha1** – Sha-1 hash odoslaného súboru.
- **File** – odoslaný súbor.
- **Size** – veľkosť odoslaného súboru.
- **Category** – kategória odoslaného súboru.
- **Reason** – dôvod odoslania súboru.
- **SentTo** – oddelenie spoločnosti ESET, kde bol súbor odoslaný.
- **User** – používateľský účet, v ktorom bol protokol vytvorený.

ESET_OneDriveScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly OneDrive“. Ide o ekvivalent protokolov kontroly OneDrive v používateľskom prostredí. Každá inštancia obsahuje:

- **ID** – jedinečné identifikačné číslo protokolu OneDrive.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **Targets** – cieľové priečinky/objekty kontroly.
- **TotalScanned** – celkový počet skontrolovaných objektov.
- **Infected** – počet nájdených infikovaných objektov.
- **Cleaned** – počet vyliečených objektov.
- **Status** – stav procesu kontroly.

ESET_OneDriveScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_OneDriveScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol OneDrive. Pri filtrovaní inštancie len určitého protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- **LogID** – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_OneDriveScanLogs).
- **ID** – jedinečné identifikačné číslo protokolu OneDrive.
- **Timestamp** – dátum a čas vytvorenia protokolu (vo WMI formáte).
- **LogLevel** – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- **Log** – správa z protokolu.

Prístup k poskytnutým údajom

Nasleduje niekoľko príkladov, ako pristupovať k dátam cez ESET WMI z príkazového riadka Windows PowerShell, ktoré by mali fungovať na všetkých verziách operačného systému Windows. Sú však dostupné aj iné cesty ako sa dostať k týmto dátam pomocou skriptovacích jazykov alebo iných nástrojov.

Cez príkazový riadok bez skriptov

Nástroj príkazového riadka `wmic` môže byť použitý na prístup k vopred definovaným triedam WMI.

Zobrazenie kompletných informácií o produkte na lokálnom počítači:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Zobrazenie čísla verzie produktu na lokálnom počítači:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Zobrazenie kompletných informácií o produkte na vzdialenom počítači s IP adresou 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Zobrazenie kompletných informácií o produkte na lokálnom počítači:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Zobrazenie kompletných informácií o produkte na vzdialenom počítači s IP adresou 10.1.118.180:

```
$cred = Get-Credential # promts the user for credentials and stores it in the
variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -cred
$cred
```

Ciele kontroly v ESET PROTECT

Táto funkcia umožňuje nástroju ESET PROTECT používať ciele kontroly (Manuálnej kontroly databáz e-mailových schránok a Kontroly Hyper-V) pri spustení klientskej úlohy **Kontrola servera** na serveri s nainštalovaným produktom ESET Security for Microsoft SharePoint. Nastavenie cieľov kontroly v rámci nástroja ESET PROTECT je dostupné len v prípade, že máte nainštalovaného ESET Management Agenta, v opačnom prípade bude táto možnosť nedostupná.

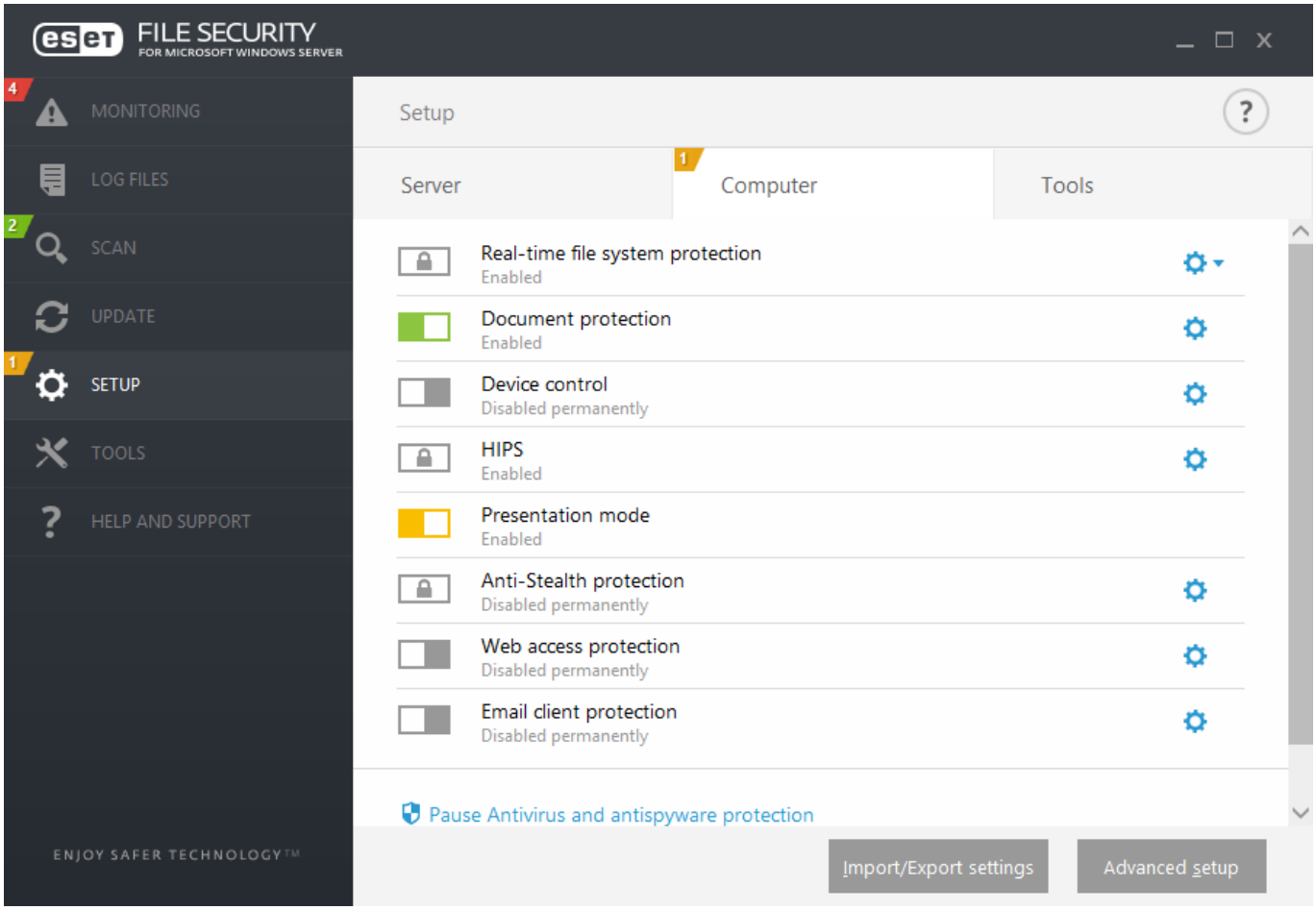
Ak povolíte **Generovanie zoznamu cieľov**, ESET Security for Microsoft SharePoint vytvorí zoznam dostupných cieľov kontroly. Tento zoznam je vytváraný v pravidelných intervaloch na základe zadaného **Intervalu aktualizácie**.

> Poznámka:
> Po prvom použití funkcie **Generovať zoznam cieľov** bude nástroju ESET PROTECT trvať približne polovicu z času zadaného pre **Interval aktualizácie**, kým si vygenerovaný zoznam cieľov preberie. Napríklad, ak je **Interval aktualizácie** nastavený na 60 minút, zoznam cieľov kontroly bude k dispozícii v nástroji ESET PROTECT približne po 30 minútach. Ak potrebujete v ESET PROTECT získať zoznam cieľov skôr, nastavte kratší interval aktualizácie. Dobu aktualizácie môžete kedykoľvek zvýšiť.

Ak chce nástroj ESET PROTECT spustiť klientsku úlohu **Kontrola servera**, vytvorí zoznam a umožní vám vybrať ciele Kontroly Hyper-V pre daný server.

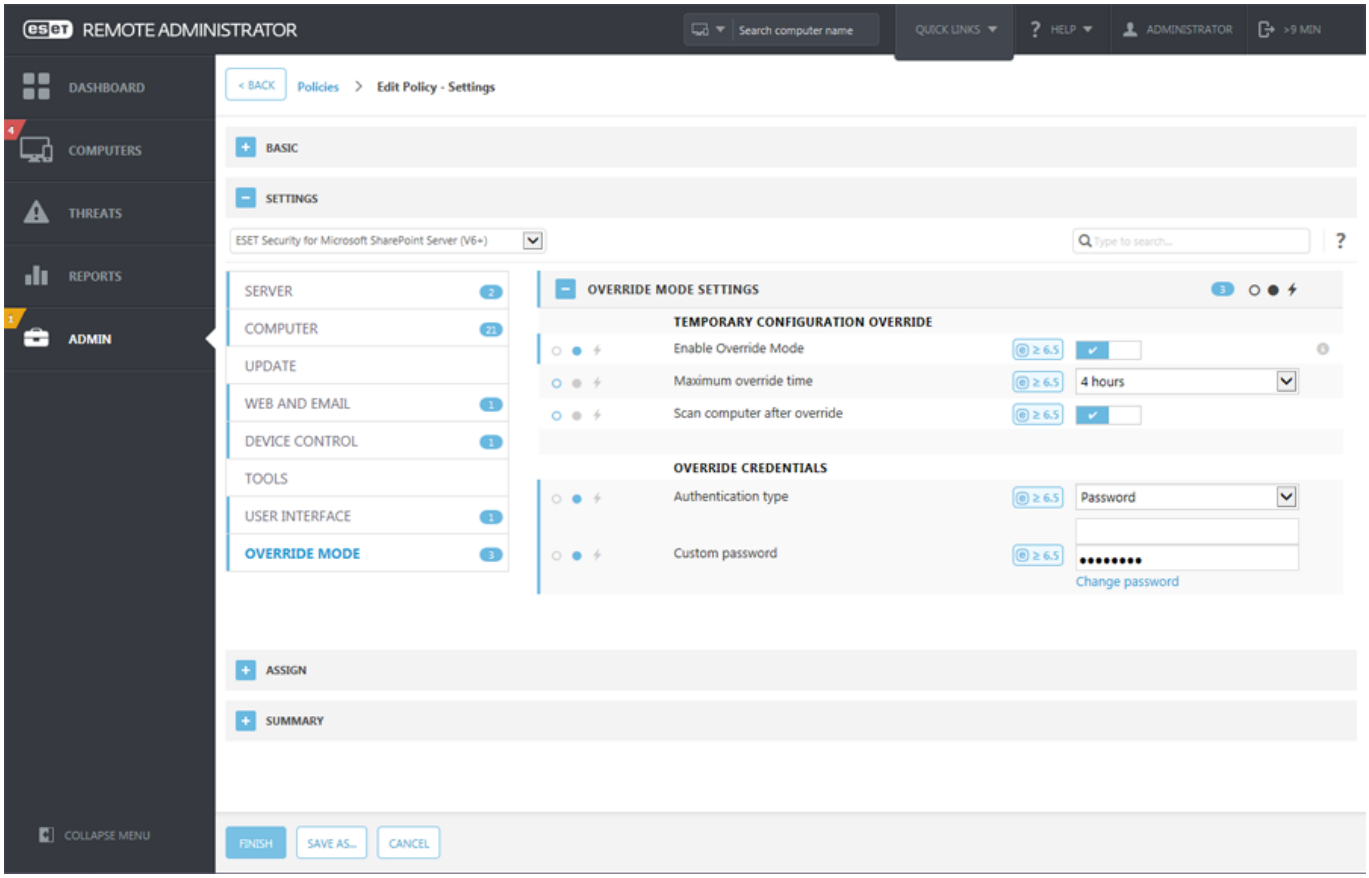
Režim prepísania

Ak máte na ESET Security for Microsoft SharePoint aplikovanú ESET PROTECT politiku, miesto prepínača Povoliť/Zakázať v sekcii Nastavenia bude zobrazený zámok , podobne ako v prípade prepínača v okne **Rozšírené nastavenia**.

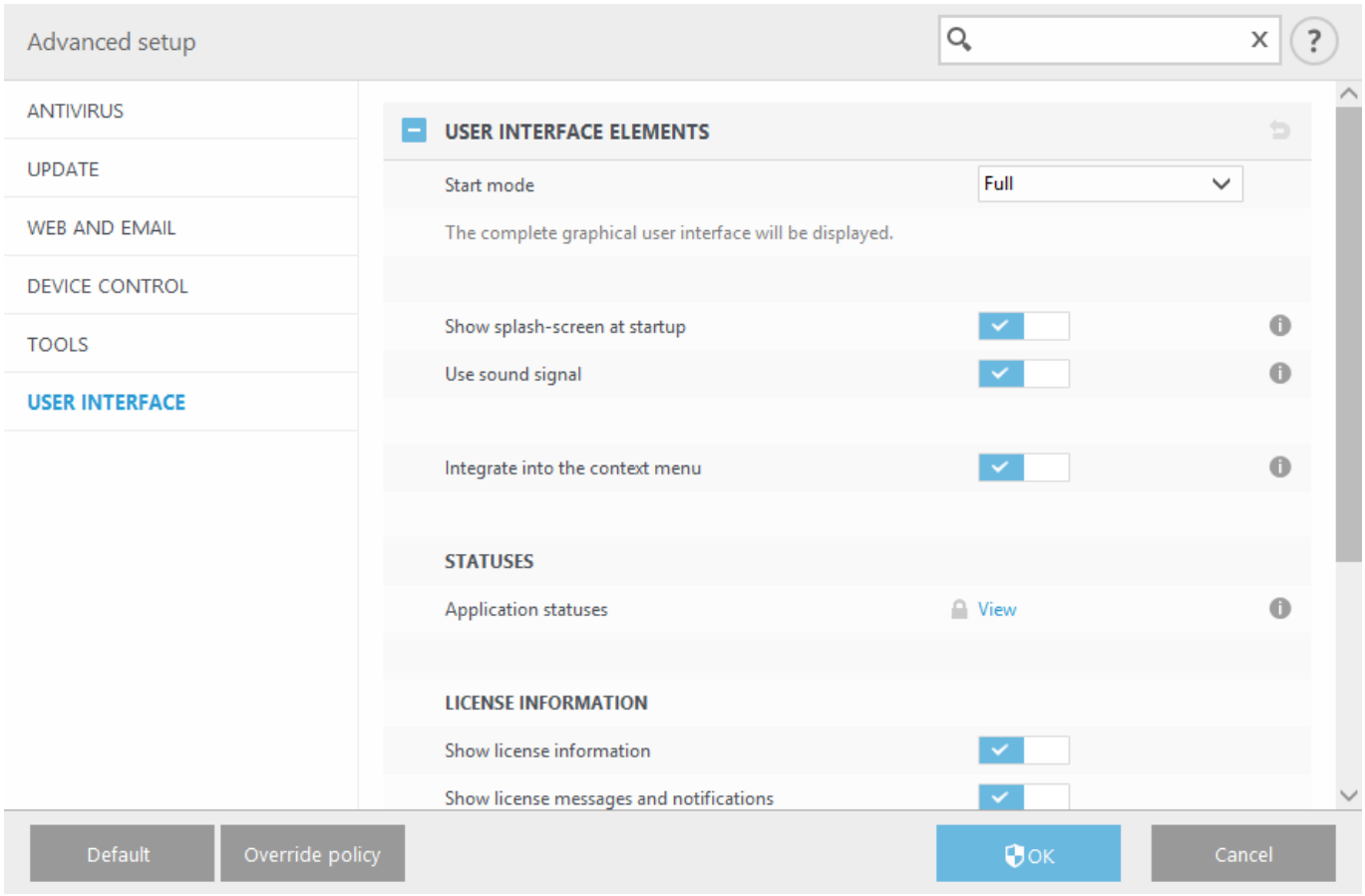


Za normálnych okolností nastavenia konfigurované prostredníctvom ESET PROTECT politiky nie je možné modifikovať. Režim prepísania vám umožňuje dočasne odomknúť tieto nastavenia. Je však potrebné povoliť **Režim prepísania** pomocou ESET PROTECT politiky.

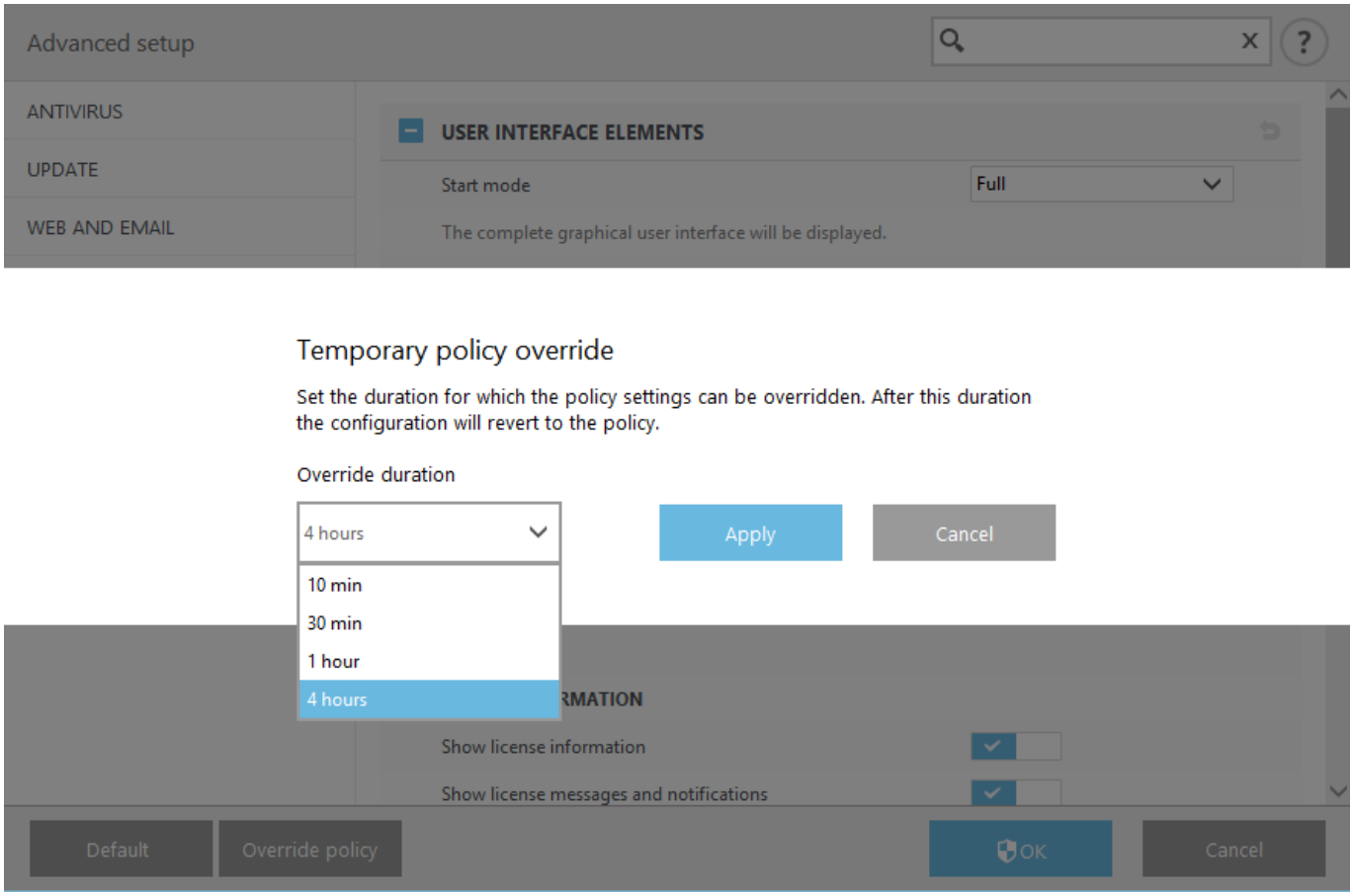
Prihláste sa do ESET PROTECT Web Console, prejdite do časti **Politiky** a vyberte a upravte existujúcu politiku, ktorá je aplikovaná na ESET Security for Microsoft SharePoint, prípadne vytvorte novú politiku. V **Nastaveniach** kliknite na **Režim prepísania**, povoľte ho a dokončite konfiguráciu vrátane Typu autentifikácie (**Používateľ Active Directory** alebo **Heslo**).



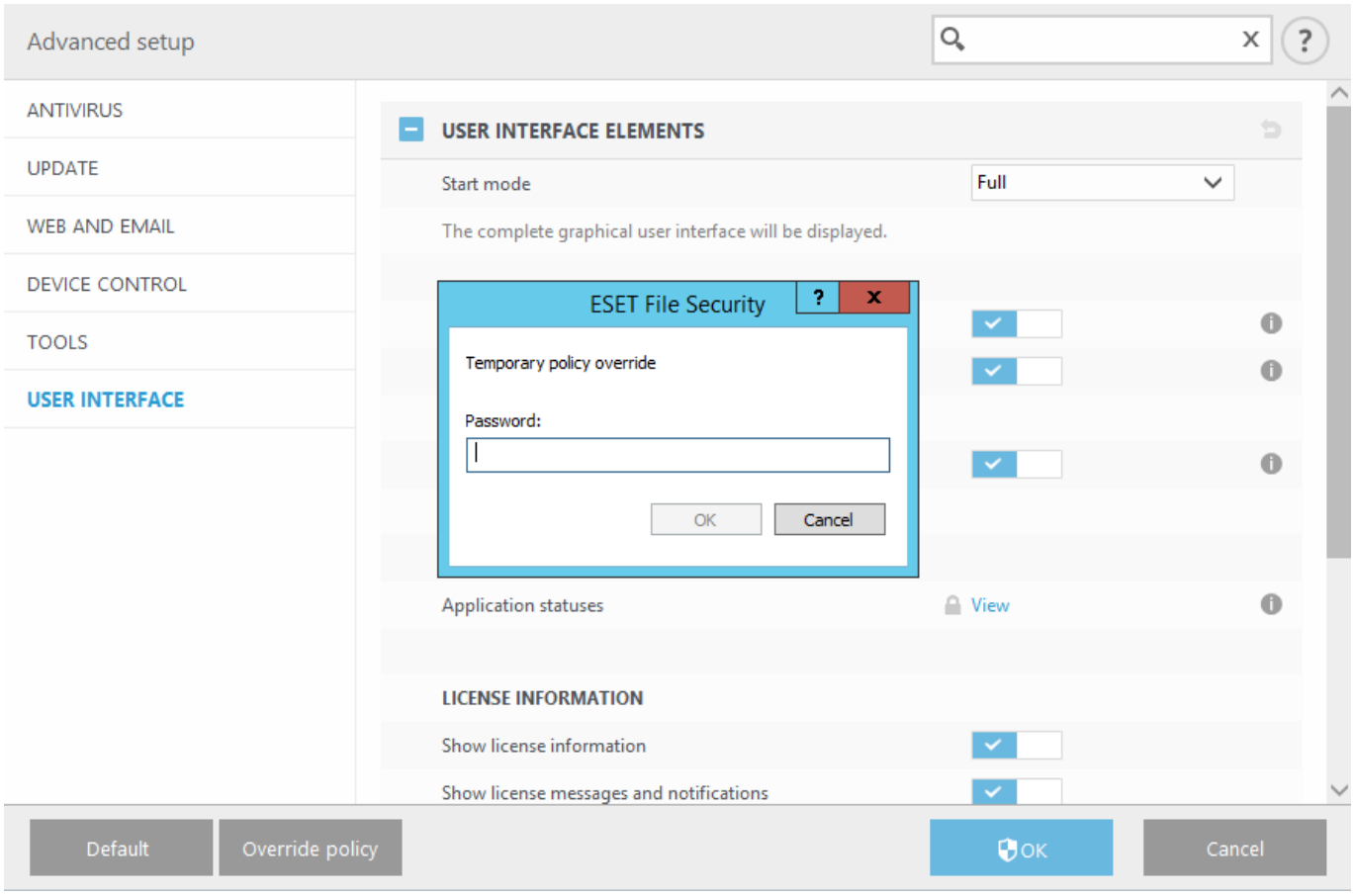
Po úprave politiky alebo aplikovaní novej politiky na ESET Security for Microsoft SharePoint sa v okne Rozšírené nastavenia zobrazí tlačidlo Prepísať politiku.



Kliknite na tlačidlo **Prepísať politiku**, nastavte dĺžku trvania a kliknite na **Uložiť**.



Ak ste ako typ autentifikácie vybrali možnosť **Heslo**, zadajte heslo pre prepísanie politiky.



Po uplynutí stanovenej doby trvania režimu prepísania budú akékoľvek zmeny vykonané v konfigurácii vrátené

späť na pôvodné nastavenia vynútené ESET PROTECT politikou. Predtým, ako doba trvania režimu prepísania uplynie, sa zobrazí oznámenie.

Režim prepísania však môžete ukončiť kedykoľvek použitím možnosti **Ukončiť prepisovanie** v sekcii Monitorovanie alebo v okne **Rozšírené nastavenia**.

Protokoly

Táto sekcia vám umožňuje upravovať nastavenia týkajúce sa zapisovania do protokolov v rámci programu ESET Security for Microsoft SharePoint.

Filter zápisu do protokolu

Keďže sú predvolene aktivované všetky možnosti zapisovania do protokolu, bude dochádzať k vytváraniu veľkého množstva dát. Odporúčame vám deaktivovať zozbieravanie dát z tých komponentov, ktoré nesúvisia s vaším aktuálne riešeným problémom.

> Poznámka:
> Ak chcete zapnúť zapisovanie do protokolov, je potrebné najprv povoliť **Diagnostické zapisovanie do protokolu** na úrovni programu v hlavnom menu > **Nastavenia** > Nástroje. Po povolení zapisovania do protokolov bude ESET Security for Microsoft SharePoint vytvárať podrobné protokoly v závislosti od funkcií povolených v tejto sekcii.

Pomocou prepínačov povolíte alebo zakážete konkrétne funkcie. Tieto možnosti je možné aj kombinovať v závislosti od dostupnosti jednotlivých komponentov v rámci ESET Security for Microsoft SharePoint.

- **Diagnostické protokoly súvisiace so SharePointom** – zapisovanie podrobných informácií do protokolov, hlavne na účely riešenia problémov.
- **Diagnostické protokoly klastra** – protokoly klastra budú súčasťou diagnostických protokolov.

Protokoly

V tejto sekcii je možné určiť spôsob spravovania protokolov. Toto je dôležité hlavne z hľadiska šetrenia miesta na disku. Predvolené nastavenia umožňujú automatické mazanie starších protokolov s cieľom šetriť miesto na disku.

Automaticky odstraňovať záznamy protokolov staršie ako (dni)

Protokoly staršie ako nastavená hodnota budú automaticky zmazané.

Automaticky odstraňovať staré záznamy, ak je prekročená veľkosť protokolu

Ak veľkosť protokolu prekročí **maximálnu veľkosť protokolu [MB]**, staré protokoly budú odstránené, kým nebude dosiahnutá **redukovaná veľkosť protokolu [MB]**.

Zálohovať automaticky vymazané protokoly

Automaticky vymazané protokoly a súbory budú zálohované do vybraného adresára a komprimované do ZIP

archívu, ak komprimovanie povolíte.

Zálohovať diagnostické protokoly

Diagnostické protokoly budú automaticky zálohované. Ak táto možnosť nie je povolená, diagnostické protokoly nebudú zálohované.

Priečinok na zálohy

Priečinok na ukladanie záloh protokolov. Môžete povoliť komprimovanie zálohy do ZIP archívu.

Automaticky optimalizovať protokoly

Táto možnosť slúži na automatickú defragmentáciu protokolov, ak počet nevyužitých záznamov prekročí definovaný pomer v percentách nastavený v poli **Ak počet nepoužívaných záznamov prekročí (%)**. Kliknite na **Optimalizovať** 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.

Zapnúť textový protokol

Túto možnosť použite v prípade, ak chcete ukladať protokoly v odlišnom formáte ako v prípade Protokolov:

- **Cieľový adresár** – adresár, v ktorom budú uložené protokoly (platí len pre **Text**/**CSV**). Každá skupina protokolov má vlastný súbor s predvoleným názvom (napríklad, *virlog.txt* sú protokoly skupiny Zachytené infiltrácie).
- **Typ** – formát **Text** ukladá protokoly do textového súboru, dáta sú oddelené tabulátormi. Formát **CSV** tvoria tiež textové súbory, avšak oddelené čiarkami. Ak vyberiete možnosť **Udalosť**, protokoly budú ukladané v denníku udalostí systému Windows, ktorý je dostupný v Zobrazovači udalostí nachádzajúcom sa v Ovládacom paneli.
- **Odstrániť všetky protokoly** – vymaže všetky protokoly označené v roletovom menu **Typ**.

Poznámka:
Pre urýchlenie riešenia problémov môžete byť vyzvaný na zaslanie protokolov z vášho počítača. Nástroj ESET Log Collector zjednodušuje zozbieranie potrebných informácií. Viac informácií o nástroji ESET Log Collector nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Protokol auditu

Umožňuje vám sledovať zmeny v konfigurácii produktu alebo v jeho stave ochrany. Keďže zmeny v konfigurácii produktu môžu výrazne ovplyvniť jeho fungovanie, sledovanie zmien môže byť užitočné z pohľadu auditu. Záznamy o zmenách nájdete v sekcii **Protokoly** > Protokol auditu.

Proxy server

V prostredí, kde sa používa rozsiahlejšia lokálna sieť, je väčšinou pripojenie do internetu zabezpečované cez tzv. proxy server. V takomto prípade musia byť nastavenia proxy servera správne definované. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií. Nastavenie proxy servera je možné v ESET Security for Microsoft SharePoint definovať na dvoch odlišných miestach v rámci štruktúry **Rozšírených nastavení** (**F5**):

1. **Rozšírené nastavenia** (**F5**) > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia** > HTTP Proxy
Toto nastavenie je platné pre konkrétny profil aktualizácie a je ho vhodné nastaviť, ak ide o prenosný počítač, ktorý vykonáva aktualizáciu z rôznych miest.

2. **Rozšírené nastavenia** (**F5**) > **Nástroje** > **Proxy server**
Proxy server zadaný v tejto sekcii bude použitý programom ESET Security for Microsoft SharePoint ako globálne nastavenie proxy servera. Tieto nastavenia budú používané všetkými modulmi, ktoré sa pripájajú na internet.

Pre upresnenie nastavení proxy servera na tejto úrovni povoľte možnosť **Používať proxy server**, zadajte adresu proxy servera do poľa **Proxy server** a číslo portu do poľa **Port**.

Proxy server vyžaduje overenie

Ak sieťová komunikácia cez proxy server vyžaduje overenie, povoľte túto možnosť a zadajte **Prihlasovacie meno** a **Heslo**.

Vyhľadať proxy server

Pre automatické vyhľadanie nastavení proxy servera kliknite na tlačidlo **Vyhľadať**. Pomocou tlačidla sa prenesú nastavenia z programu Internet Explorer.

> Poznámka:
> Týmto spôsobom nie je možné získať overovacie údaje (prihlasovacie meno a heslo) – je potrebné ich zadať.

Použiť priame pripojenie, ak nie je dostupný proxy server

Ak je produkt nakonfigurovaný tak, aby používal HTTP Proxy a proxy nie je k dispozícii, produkt obíde proxy a bude komunikovať priamo so servermi spoločnosti ESET.

Oznámenia

Upozornenia na pracovnej ploche sú informačnými prostriedkami, ktoré neponúkajú a ani nevyžadujú interakciu používateľa. Zobrazujú sa v paneli oznámení v pravej dolnej časti obrazovky. Ďalšie možnosti (ako dĺžka zobrazenia upozornenia a priehľadnosť tohto okna) možno nastaviť nižšie. Povolením možnosti **Nezobrazovať oznámenia pri spúšťaní aplikácií na celú obrazovku** budú pozastavené oznamovacie okná v prípade, že bude spustená aplikácia na celú obrazovku.

Zobrazovať oznámenia o úspešnej aktualizácii

Po úspešnej aktualizácii sa zobrazí príslušné oznámenie.

Posielať oznámenia o udalostiach e-mailom

Kliknutím na túto možnosť aktivujete posielanie e-mailových oznámení.

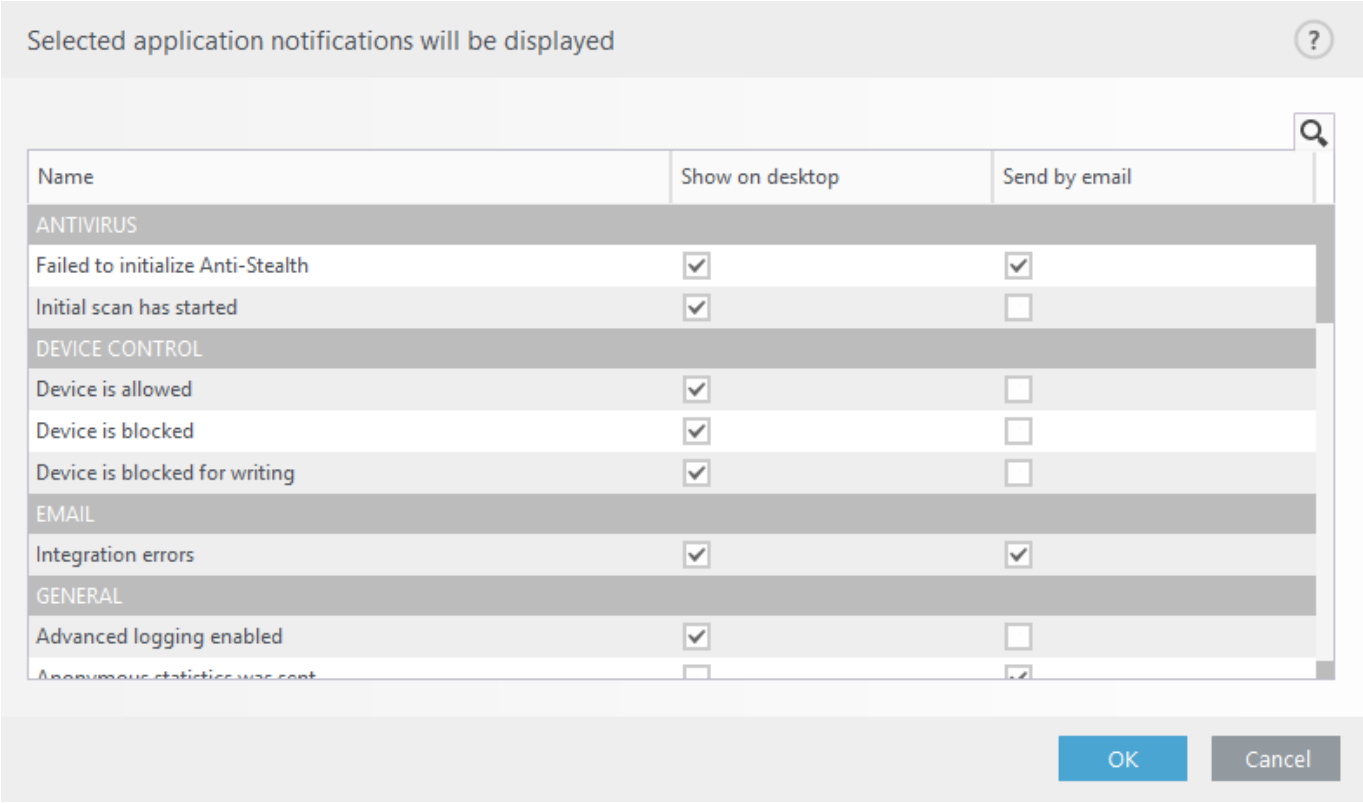
Oznámenia aplikácie

Kliknutím na Upraviť zapnete alebo vypnete zobrazovanie oznámení aplikácie.

Oznámenia aplikácie

ESET Security for Microsoft SharePoint oznámenia môžete nastaviť tak, aby sa zobrazovali na ploche alebo aby boli odosielané e-mailom.

Poznámka:
Ak chcete používať e-mailové oznámenia, uistite sa, že je povolená možnosť **Posielať oznámenia o udalostiach e-mailom** v sekcii **Základné** a následne nakonfigurujte SMTP server a ostatné podrobnosti podľa potreby.



Oznámenia na ploche

V tejto sekcii je možné nastaviť výstražné a informačné hlásenia programu ESET Security for Microsoft SharePoint (napr. správy o úspešnej aktualizácii). Nastaviť je možné napríklad **Trvanie** zobrazenia oznámenia, ako aj **Priehľadnosť** okna s oznámením (len na systémoch, ktoré podporujú notifikácie).

V roletovom menu **Zobrazovať udalosti od úrovne** je možné nastaviť, aké závažné udalosti sa budú zobrazovať. Na výber sú tieto možnosti:

- **Diagnostické** – zobrazené budú informácie dôležité pre ladenie programu, ako aj všetky udalosti s vyššou závažnosťou.
- **Informačné** – informatívne správy, napríklad o úspešnej aktualizácii, ako aj všetky udalosti s vyššou závažnosťou.
- **Varovania** – varovné správy a kritické chyby.
- **Chyby** – chyby typu „Chyba pri sťahovaní súboru“ a kritické chyby.
- **Kritické** – zobrazené budú len kritické chyby.

Pole s názvom **Vo viacpoužívateľskom prostredí zobrazovať oznámenia tomuto používateľovi** predstavuje meno používateľa, ktorému budú zasielané dôležité systémové hlásenia na systéme umožňujúcom prihlásenie viacerých používateľov súčasne. Štandardne je týmto používateľom správca systému alebo siete. Túto možnosť je vhodné použiť na terminálovom serveri za predpokladu, že všetky systémové hlásenia budú odosielané správcovi.

E-mailové oznámenia

ESET Security for Microsoft SharePoint podporuje automatické odosielanie oznámení e‑mailom, ak sa vyskytne udalosť s nastavenou úrovňou zápisu.

> Poznámka:
> ESET Security for Microsoft SharePoint podporuje SMTP servery, ktoré využívajú šifrovanie TLS.

SMTP server

Názov SMTP servera použitého na odosielanie oznámení a upozornení. Zvyčajne je to názov vášho Microsoft Exchange Servera.

Prihlasovacie meno a heslo

V prípade, že SMTP server vyžaduje overenie, musí byť táto možnosť zapnutá a pre prístup k SMTP serveru musí byť nastavené správne prihlasovacie meno a heslo.

E-mailová adresa odosielateľa

Upresnite adresu odosielateľa, ktorá bude zobrazená v hlavičke e‑mailovej správy obsahujúcej oznámenie. Ide o adresu, ktorú príjemca uvidí v poli **Od**.

E-mailová adresa príjemcu

Zadajte e‑mailovú adresu príjemcu, **pre** ktorého je oznámenie určené.

Zapnúť TLS

Zapne odosielanie správ a upozornení s podporou šifrovania typu TLS.

Nastavenia e-mailu

Posielať udalosti od úrovne

Určuje minimálnu úroveň podrobností odosielaných oznámení.

Interval, v akom sa budú e‑mailom posielať nové oznámenia (v minútach)

Časový interval v minútach, po ktorom sa odošle nové oznámenie prostredníctvom e‑mailu. Ak chcete, aby sa e-maily odosielali okamžite, nastavte túto hodnotu na 0.

Posielať každé oznámenie v samostatnom e-maile

Každé oznámenie bude odoslané v samostatnom e-maile. Výsledkom môže byť veľký počet odosielaných e-

mailov za krátky čas.

Formát správy

Komunikácia medzi programom a používateľom, správcom alebo zodpovednou osobou je zabezpečená prostredníctvom e-mailov alebo oznamovacích správ (pomocou služby Windows messenger service). Vírusové správy a upozornenia systému majú prednastavený formát, ktorý sa neodporúča meniť. V niektorých prípadoch je potrebné pozmeniť formát správ o udalostiach.

Formát správ o udalostiach

Formát správ o udalostiach zobrazovaných na vzdialenom počítači, ktorý je špecifikovaný v nastaveniach odosielania.

Formát správ o hrozbách

Správy obsahujúce upozornenia a oznámenia o hrozbách majú preddefinovaný formát. Meniť tento formát sa neodporúča. Formát môžete meniť napríklad v prípade, že používate systém na automatické spracovanie e-mailov.

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 infikovaného súboru, e-mailovej správy atď.
- **%VirusName%** – názov vírusu.
- **%ErrorDescription%** – popis chyby.

Kľúčové slová **%InfectedObject%** a **%VirusName%** sa využívajú iba v upozorneniach týkajúcich sa hrozieb, kým kľúčové slovo **%ErrorDescription%** sa využíva iba v informatívnych upozorneniach.

Znaková sada

V roletovom menu si môžete vybrať kódovanie znakov. E-mailová správa bude skonvertovaná podľa zvoleného kódovania.

Použiť Quoted-printable kódovanie

Zdroj e-mailovej správy bude zakódovaný do Quoted-printable (QP) formátu, ktorý používa ASCII znaky a vie správne preložiť špeciálne znaky do 8-bitového formátu (áéíóú).

Prispôsobenie

Táto správa bude zobrazená v päte vybraných upozornení.

Predvolená správa v oznámeniach

Predvolená správa, ktorá sa zobrazí v päte upozornenia.

Hrozby

Automaticky nezatvárať oznámenia o malvéri

Ak použijete túto možnosť, upozornenia o malvéri ostanú na obrazovke až kým ich nezatvoríte manuálne.

Použiť predvolenú správu

Môžete vypnúť odosielanie predvolenej správy a nastaviť si vlastnú **správu upozorňujúcu na hrozbu**, ktorá sa zobrazí v prípade, že došlo k zablokovaniu hrozby.

Správa upozorňujúca na hrozbu

Zadajte vlastnú správu, ktorá sa zobrazí v prípade, že došlo k zablokovaniu hrozby.

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 programu ESET Security for Microsoft SharePoint. Zapnutím prezentačného režimu budú zakázané všetky oznámenia programu a aktivity plánovača. Samotná ochrana je aj naďalej spustená v pozadí, avšak nevyžaduje žiadne zásahy používateľa.

Automaticky zapnúť prezentačný režim pri spúšťaní aplikácií na celú obrazovku

Prezentačný režim sa aktivuje automaticky pri spustení aplikácie v režime na celú obrazovku. Ak je prezentačný režim aktívny, nebudú sa zobrazovať oznámenia alebo zmeny stavu vášho programu ESET Security for Microsoft SharePoint.

Automaticky vypnúť prezentačný režim po určenom čase

Môžete si tiež zvoliť túto možnosť a určiť čas v minútach, po uplynutí ktorého sa prezentačný režim automaticky vypne.

Diagnostika

Diagnostika poskytuje výpisy aplikácie pri zlyhaní procesov ESET (napr. *ekrn*). Ak aplikácia zlyhá, vygeneruje sa výpis. Výpis môže pomôcť vývojárom pri oprave rôznych problémov produktu ESET Security for Microsoft SharePoint.

Kliknite na roletové menu vedľa položky **Typ výpisu** a vyberte jednu z nasledujúcich možností:

- **Žiadny** – použitím tejto možnosti vypnete túto funkciu.
- **Skrátený** (predvolené) – zaznamená najmenšiu sadu užitočných informácií, ktoré môžu pomôcť identifikovať dôvod, prečo aplikácia nečakane zlyhala. Tento typ výpisu môže byť užitočný, keď je obmedzený priestor na disku. Pre obmedzené množstvo zahrnutých informácií však chyby, ktoré neboli priamo spôsobené vláknom (threadom) aktívnym v čase problému, nemusia byť pri analýze tohto súboru

objavené.

• **Úplný** – zaznamená celý obsah systémovej pamäte, keď sa aplikácia nečakane zastaví. Kompletný výpis 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

Po kliknutí na možnosť **Otvoriť** sa tento priečinok zobrazí v novom okne *Windows Prieskumníka*.

Vytvoriť diagnostický výpis

Ak chcete v cieľovom priečinku vytvoriť diagnostický výpis, kliknite na **Vytvoriť**.

Vytváranie rozšírených protokolov

Zapnúť rozšírené protokoly správy zariadení

Zaznamenávať sa budú všetky udalosti správy zariadení s cieľom umožniť diagnostiku a riešenie problémov.

Zapnúť rozšírené protokoly jadra

Zaznamenávať sa budú všetky udalosti v jadre ESET (`ekrn`) s cieľom umožniť diagnostiku a riešenie problémov.

Zapnúť rozšírené protokoly licencovania

Zaznamenávaná bude všetka komunikácia produktu s licenčným serverom.

Zapnúť rozšírené protokoly ochrany siete

Zaznamenávané budú všetky sieťové dáta prechádzajúce ochranou siete v PCAP formáte. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa ochrany siete.

Zapnúť rozšírené protokoly operačného systému

Budú zozbierané dodatočné informácie o operačnom systéme, ako sú spustené procesy, aktivita procesora a operácie disku.

Zapnúť rozšírené protokoly filtrovania protokolov

Zaznamenávané budú všetky dáta prechádzajúce jadrom filtrovania protokolov v PCAP formáte. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa filtrovania protokolov.

Zapnúť rozšírené protokoly aktualizačného jadra

Zaznamenávané budú všetky udalosti, ktoré nastanú počas procesu aktualizácie. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa aktualizačného jadra.

Technická podpora

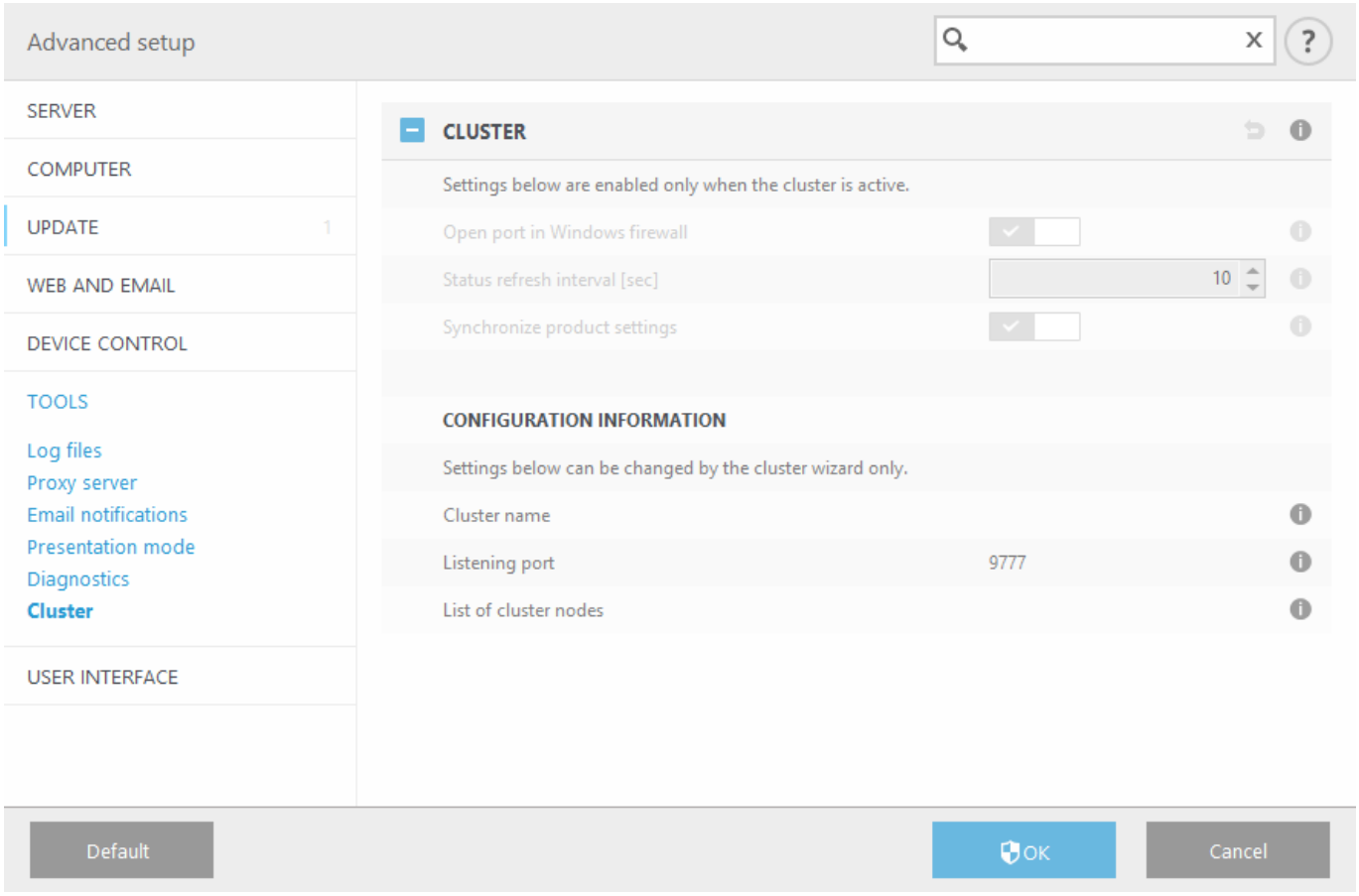
Odoslať systémové nastavenia

Z roletového menu vyberte možnosť **Vždy odosielať** (ak nechcete, aby sa vám pred odoslaním konfiguračných údajov programu ESET Security for Microsoft SharePoint technickej podpore vždy zobrazila výzva) alebo možnosť **Spýtať sa pred odoslaním**.

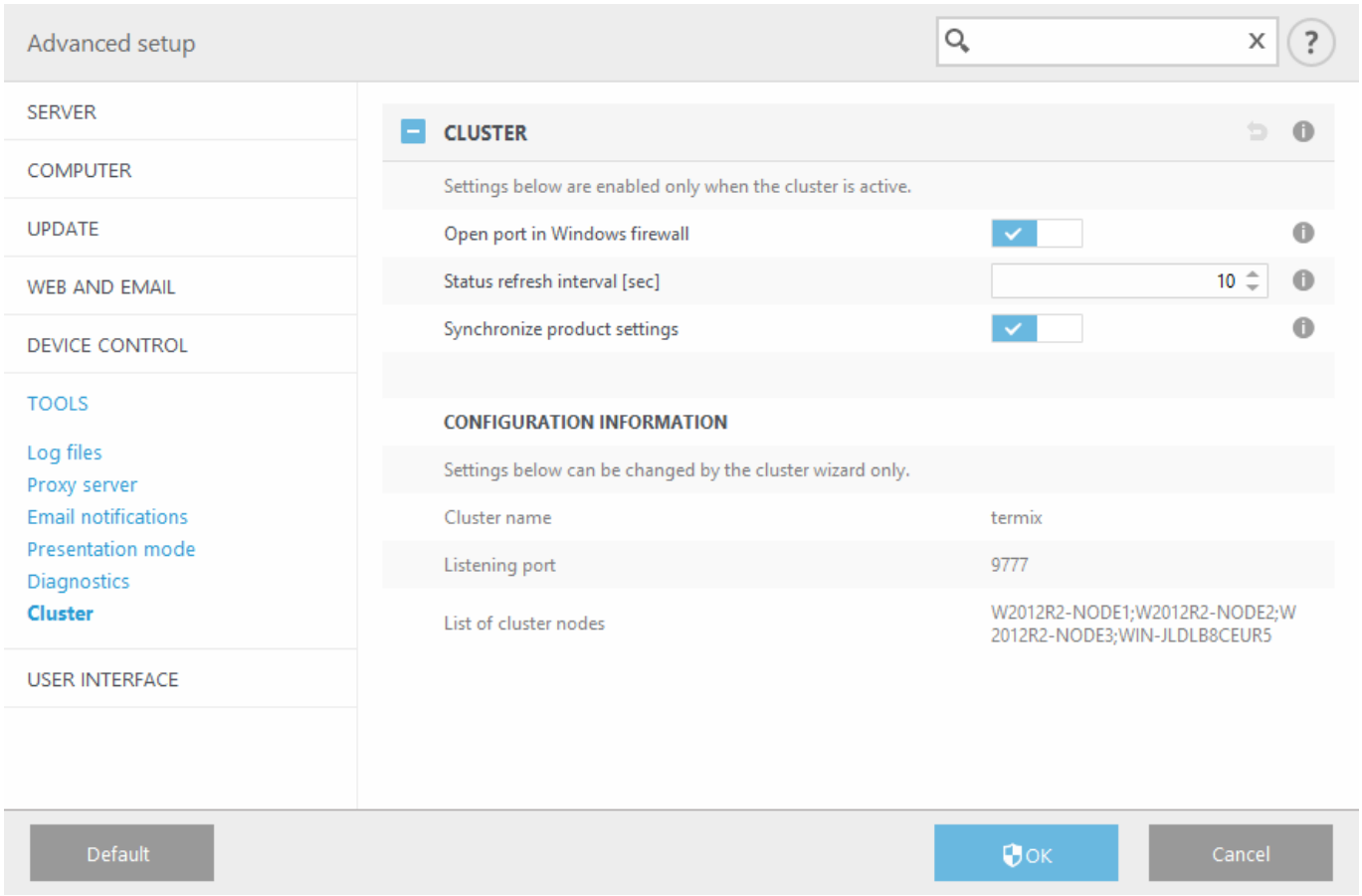
Klaster

Možnosť Povoliť klaster je automaticky zapnutá, ak je nastavený klaster ESET. Klaster môžete zakázať v okne **Rozšírené nastavenia** (**F5**) kliknutím na prepínač (napríklad, ak potrebujete zmeniť nastavenia bez toho, aby to ovplyvnilo ostatné uzly v klastri ESET). Prepínač slúži len na zapnutie alebo vypnutie funkcie klastra ESET. Pre nastavenie alebo odstránenie klastra je potrebné použiť Sprievodcu konfiguráciou klastra alebo **zrušiť klaster** v sekcii **Nástroje** > **Klaster** hlavného okna programu.

Klaster ESET nie je nastavený alebo je vypnutý:



Klaster ESET je nastavený:



Používateľské rozhranie

V tejto sekcii môžete nastaviť grafické používateľské rozhranie programu ESET Security for Microsoft SharePoint. Môžete si prispôsobiť vizuálnu stránku programu a použité efekty.

Prvky používateľského rozhrania

V roletovom menu Štartovací režim sú na výber nasledujúce možnosti zobrazenia grafického používateľského rozhrania:

- **Úplný** – zobrazuje sa kompletné grafické rozhranie.
- **Terminál** – nezobrazujú sa ani oznámenia ani varovania. Tento režim môže spustiť len správca. Grafické rozhranie by malo byť prepnuté na Terminál, ak zobrazovanie prvkov grafického rozhrania programu spomaľuje výkon vášho počítača alebo spôsobuje problémy. Vypnutie GUI je tiež užitočné pre terminálový server. Viac informácií o ESET Security for Microsoft SharePoint nainštalovanom na terminálovom serveri nájdete v časti Vypnutie grafického rozhrania (GUI) na terminálovom serveri.

Zobrazovať úvodný obrázok pri štarte

Vypnite túto možnosť, ak nechcete, aby sa napr. pri prihlásení do systému zobrazoval úvodný obrázok ESET Security for Microsoft SharePoint.

Používať zvukové upozornenia

ESET Security for Microsoft SharePoint prehráva pri dôležitých udalostiach zvukové efekty (napríklad pri

nájdení hrozieb, kontrole počítača alebo pri dokončení kontroly), ktoré môžu byť zapnuté alebo vypnuté pomocou tejto možnosti.

Pridať do kontextového menu

Ovládacie prvky programu ESET Security for Microsoft SharePoint budú integrované do kontextového menu. Kontextové menu sa zobrazuje po kliknutí pravým tlačidlom myši na súbor v prieskumníkovi. Obsahuje zoznam akcií, ktoré možno so súborom vykonať.

Stavy aplikácie

Kliknutím na Upraviť môžete vybrať stavy aplikácie, ktoré budú zobrazované v okne Monitorovanie. Môžete tiež použiť ESET PROTECT politiky na konfiguráciu vašich stavov aplikácií. Stav aplikácie bude tiež zobrazený, ak váš produkt nie je aktivovaný alebo vypršala vaša licencia.

Zobrazovať licenčné informácie

Ak je táto možnosť povolená, budú zobrazované správy a oznámenia týkajúce sa vašej licencie.

Upozornenia a okná správ

V tejto časti môžete zmeniť správanie upozornení pri detekcii ohrození a správanie systémových upozornení. Tie môžu byť zmenené tak, aby vyhovovali vašim požiadavkám. Ak sa rozhodnete nezobrazovať určité upozornenia, budú zobrazené v časti Vypnuté správy a stavy. Môžete kontrolovať ich stav, zobraziť viac informácií alebo ich odstrániť.

Nastavenia prístupu

Akýmkoľvek neoprávneným zmenám môžete predísť použitím Nastavení prístupu. Pomocou týchto nastavení môžete zaistiť vysokú mieru zabezpečenia.

ESET Shell

Konfigurácia prístupových práv k nastaveniam, funkciám a dátam programu prostredníctvom nástroja eShell je možná zmenou politiky spustenia nástroja ESET Shell.

Ikona na paneli úloh

Vrátiť späť všetky nastavenia v tejto sekcii

Upozornenia a okná správ

V tejto sekcii je možné nastaviť výstražné a informačné hlásenia programu ESET Security for Microsoft SharePoint (napr. správy o úspešnej aktualizácii). Nastaviť je možné napríklad **Trvanie** zobrazenia oznámenia, ako aj **Priehľadnosť** okna s oznámením (len na systémoch, ktoré podporujú notifikácie).

Zobrazovať interaktívne upozornenia

Vypnite túto funkciu, ak si neprajete, aby program ESET Security for Microsoft SharePoint zobrazoval akékoľvek upozornenia v oblasti oznámení systému Windows v pravom dolnom rohu obrazovky.

Zoznam interaktívnych upozornení

Túto možnosť využijete na automatizáciu. Ak nechcete zobraziť upozornenie a čakať na interakciu používateľa, môžete v rámci automatizácie pre konkrétne položky zrušiť výber možnosti **Spýtať sa používateľa** a vybrať požadovanú akciu, ktorú má produkt vykonať.

Okná správ sú používané na zobrazovanie krátkych textových správ alebo otázok.

Okná správ zatvárať automaticky

Dĺžku zobrazenia informačných okien je možné nastaviť v poli vedľa tejto možnosti. Po uplynutí nastaveného času sa okno oznámenia zatvorí automaticky, ak ho nezatvorí sám používateľ.

Potvrdzovacie správy

Po kliknutí na možnosť **Upraviť** sa zobrazí okno so zoznamom potvrdzovacích správ, ktoré ESET Security for Microsoft SharePoint zobrazí pred vykonaním konkrétnej akcie. Použitím začiarkavacích políčok môžete upraviť nastavenia pre potvrdzovacie správy.

Nastavenia prístupu

Správne nastavenie ESET Security for Microsoft SharePoint je veľmi dôležité pre zachovanie maximálnej bezpečnosti vášho systému. Neoprávnené zmeny nastavení môžu vystaviť systém nebezpečenstvu, prípadne spôsobiť stratu dát. Ak chcete zabrániť neoprávneným zmenám, môžete si v rámci ESET Security for Microsoft SharePoint nastaviť ochranu nastavení heslom.

> Dôležité:
> Ak sa pokúsite odinštalovať ESET Security for Microsoft SharePoint v prípade, keď je aktívna ochrana nastavení heslom, bude potrebné zadať príslušné heslo. V opačnom prípade nebude možné ESET Security for Microsoft SharePoint odinštalovať.

Ochrana nastavení heslom

Zapína/vypína uzamknutie nastavení vami zadaným heslom. Po kliknutí sa otvorí okno **Nastavenie hesla**.

Nastaviť heslo

Pre zmenu nastaveného hesla kliknite na **Nastaviť**. Aby ste predišli neoprávneným zmenám nastavení, rozšírené nastavenia produktu ESET Security for Microsoft SharePoint sa dajú ochrániť heslom. Pre zmenu hesla najprv zadajte staré heslo do poľa **Pôvodné heslo**, potom zadajte nové heslo do polí **Nové heslo** a **Potvrdiť heslo** a následne potvrďte zmenu hesla kliknutím na **OK**. Toto heslo bude odteraz vyžadované pre všetky ďalšie zmeny v nastaveniach ESET Security for Microsoft SharePoint.

Vyžadovať úplné práva správcu aj pre účty s obmedzenými právami

Túto možnosť použite v prípade, že chcete, aby bol aktuálny používateľ (ak nemá práva správcu) vyzvaný na zadanie prihlasovacích údajov pri pokuse o zmenu niektorých systémových parametrov (napr. vypnutie modulov ochrany).

Poznámka:
Ak sa zmení heslo pre Nastavenie prístupu a chcete importovať konfiguračný súbor *xml* (podpísaný pred zmenou hesla) pomocou príkazového riadku ESET CMD, je potrebné ho podpísať znova pomocou vášho aktuálneho hesla. Tento postup vám umožní použiť starší konfiguračný súbor bez potreby jeho exportovania na inom počítači, na ktorom je spustený program ESET Security for Microsoft SharePoint.

ESET Shell

Konfigurácia prístupových práv k nastaveniam, funkciám a dátam programu prostredníctvom nástroja eShell je možná zmenou **politiky spustenia nástroja ESET Shell**. Predvolene je nastavené **Obmedzené skriptovanie**, pričom ďalšie možnosti sú: Vypnutý, Iba na čítanie a Úplný prístup.

Vypnutý

eShell nemôže byť použitý. Je povolená len konfigurácia samotného nástroja eShell v `ui eshell` kontexte. Môžete zmeniť vzhľad nástroja eShell, nemáte však prístup k bezpečnostných nastaveniam a dátam.

Iba na čítanie

Nástroj eShell môže byť použitý len na monitorovanie. Všetky nastavenia môžete zobraziť v oboch režimoch, nemôžete však zmeniť žiadne nastavenia, funkcie alebo dáta.

Obmedzené skriptovanie

V interaktívnom režime môžete zobraziť a zmeniť všetky nastavenia, funkcie alebo dáta. V Batch režime bude nástroj eShell pracovať v režime Iba na čítanie, ak však používate podpísané batch súbory, budete môcť upravovať nastavenia aj dáta.

Úplný prístup

Prístup ku všetkým nastaveniam v interaktívnom aj batch režime. Môžete zobraziť a zmeniť všetky nastavenia. eShell musíte používať s právami správcu. Taktiež musíte mať povolenú UAC (user account control) a eleváciu.

Vypnutie grafického používateľského rozhrania (GUI) na terminálovom serveri

Táto kapitola vysvetľuje, ako vypnúť grafické rozhranie (GUI) programu ESET Security for Microsoft SharePoint pre používateľov prihlásených na terminálovom serveri.

Za normálnych okolností sa grafické rozhranie (GUI) programu ESET Security for Microsoft SharePoint spustí pri každom prihlásení používateľa na terminálový server. Toto je väčšinou nežiaduce, pokiaľ ide o terminálové servery. Ak si želáte vypnúť GUI pre terminálové pripojenia, môžete to urobiť pomocou nástroja eShell spustením príkazu `set ui ui gui-start-mode none`. Tento príkaz prepne GUI do terminálu. Sú dostupné nasledujúce dve možnosti:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode none
```

Ak chcete zistiť, ktorá z dvoch možností zobrazenia GUI je zapnutá, spustite príkaz `get ui ui gui-start-mode`.

> Poznámka:
> Ak používate ESET Security for Microsoft SharePoint na serveri Citrix, odporúčame použiť nastavenia popísané v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Vypnuté správy a stavy

Potvrdzovacie správy

Zobrazí vám zoznam potvrdzovacích správ, pre ktoré môžete zvoliť, či sa majú alebo nemajú zobrazovať.

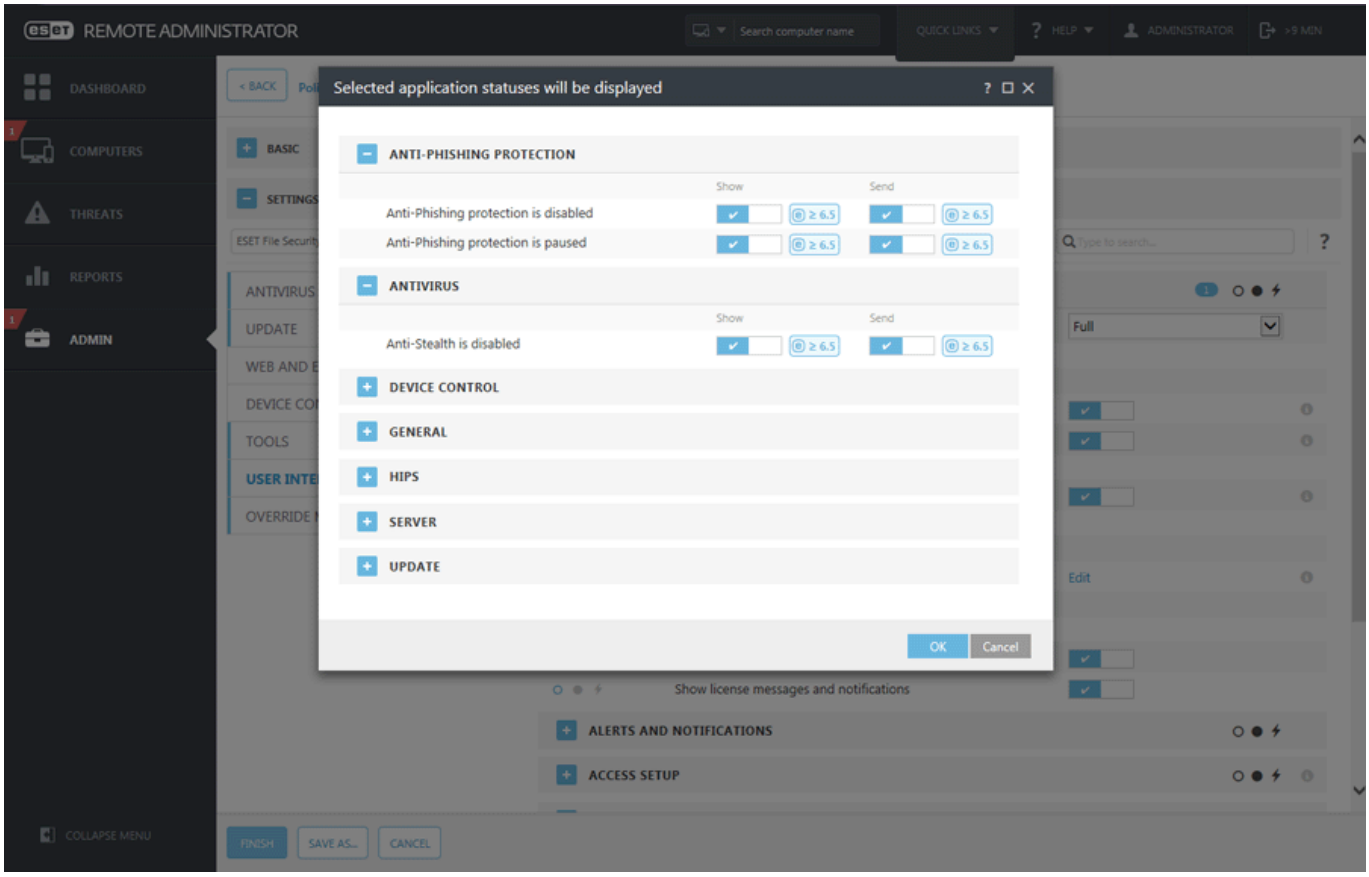
Nastavenia stavov aplikácie

Umožňuje zapnúť alebo vypnúť zobrazenie stavu v okne Monitorovanie, ktoré sa nachádza v hlavnom menu.

Nastavenia stavov aplikácie

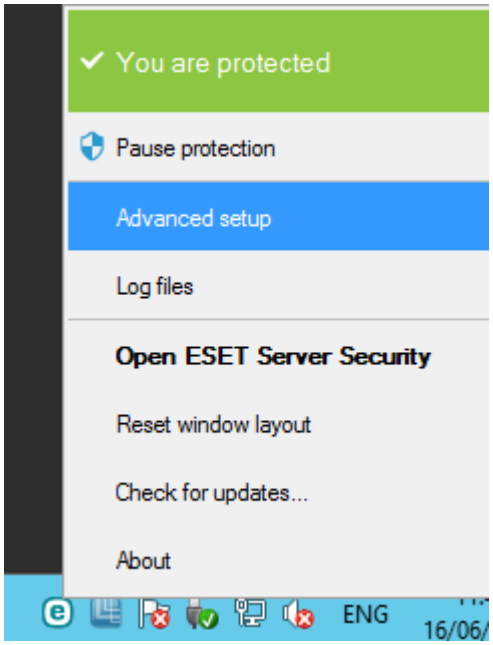
Toto dialógové okno vám umožňuje definovať, ktoré stavy aplikácie budú alebo nebudú zobrazované. Napríklad, ak pozastavíte antivírusovú a antispyvérovú ochranu, výsledkom bude zmena stavu ochrany, čo bude následne zobrazené v sekcii Monitorovanie. Stav aplikácie bude tiež zobrazený, ak váš produkt nie je aktivovaný alebo vypršala vaša licencia.

Stavy aplikácie je možné spravovať prostredníctvom ESET PROTECT politík. Kategórie a stavy sú zobrazené v zozname s dvomi možnosťami: **Zobraziť** a **Odoslať** stav. Stĺpec „Odoslať“ pre stavy aplikácie je viditeľný len v konfigurácii ESET PROTECT politiky. ESET Security for Microsoft SharePoint zobrazuje nastavenia s ikonou zámku. Pre dočasnú zmenu stavov aplikácie môžete použiť Režim prepísania.



Ikona na paneli úloh

Ikona na paneli úloh slúži na rýchly prístup k často používaným funkciám programu ESET Security for Microsoft SharePoint. Tieto funkcie a položky sú dostupné v menu, ktoré sa zobrazí po kliknutí pravým tlačidlom myši na ikonu programu v paneli úloh .



Viac informácií

Otvorí sa okno Monitorovanie, kde bude zobrazený aktuálny stav ochrany a súvisiace správy.

Pozastaviť ochranu

Zobrazí sa potvrdzovacie dialógové okno, ktoré vypne Antivírusovú a antispyvérovú ochranu, ktorá chráni pred škodlivými systémovými útokmi pomocou kontroly súborov, webu a e-mailovej komunikácie. Keď pozastavíte antivírusovú a antispyvérovú ochranu pomocou ikony programu v oblasti oznámení systému, zobrazí sa okno **Pozastaviť ochranu**. Táto možnosť vypína ochranu systému pred malvérom na stanovený čas. Ak chcete ochranu vypnúť natrvalo, môžete to urobiť v **Rozšírených nastaveniach**. Pri vypínaní ochrany buďte opatrný, pretože váš systém bude vystavený hrozbám.

Rozšírené nastavenia

Otvorí sa okno s **Rozšírenými nastaveniami** pre daný program.

Protokoly

Protokoly obsahujú informácie o všetkých systémových udalostiach a poskytujú prehľad zistených ohrození.

Skryť ESET Security for Microsoft SharePoint

Skryje hlavné okno programu ESET Security for Microsoft SharePoint z obrazovky.

Obnoviť rozmiestnenie okien

Obnoví prednastavenú veľkosť a umiestnenie okna ESET Security for Microsoft SharePoint na obrazovke.

Overiť dostupnosť aktualizácií

Spustí aktualizáciu modulov, ktorá je dôležitou súčasťou zabezpečenia komplexnej ochrany pred škodlivým kódom.

O programe

Informácie o programe ESET Security for Microsoft SharePoint, v ktorých môžete nájsť verziu produktu, licenčné informácie a informácie o nainštalovaných moduloch. Informácie o operačnom systéme a systémových prostriedkoch sú zobrazené v dolnej časti okna.

Vrátiť späť na predvolené nastavenia

Nastavenia môžete v rámci **rozšírených nastavení** vrátiť späť na pôvodné hodnoty. Existujú dva spôsoby. Na predvolené hodnoty môžete vrátiť buď všetko, alebo iba nastavenia pre konkrétnu sekciu (nastavenia v ostatných sekciách ostanú nezmenené).

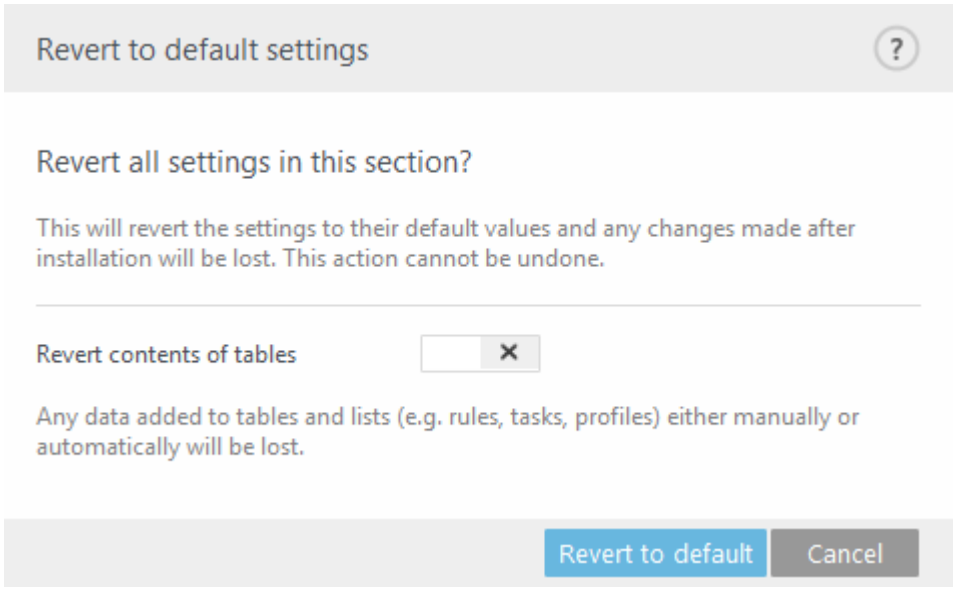
Vrátiť späť všetky nastavenia

Všetky nastavenia vo všetkých sekciách rozšírených nastavení budú obnovené do stavu po inštalácii ESET Security for Microsoft SharePoint. V podstate ide o *obnovenie továrenských nastavení*.

> Poznámka:
> Majte na pamäti, že po kliknutí na možnosť **Vrátiť späť na predvolené** budú všetky vykonané zmeny stratené. Túto akciu nie je možné vrátiť späť.

Vrátiť späť všetky nastavenia v tejto sekcii

Nastavenia modulov vo vybranej sekcii budú vrátené na pôvodné hodnoty. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.



Vrátiť späť obsah tabuliek

Po povolení tejto možnosti budú stratené pravidlá, úlohy alebo profily pridané či už manuálne, alebo automaticky.

Pomocník a podpora

ESET Security for Microsoft SharePoint obsahuje nástroj poskytujúci pomoc pri riešení známych problémov, prostredníctvom ktorého možno kontaktovať technickú podporu spoločnosti ESET.

Pomocník

Hľadať v Databáze znalostí spoločnosti ESET

Databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najrýchlejší nástroj na riešenie rozličných druhov problémov.

Otvoriť pomocníka

Kliknutím na túto možnosť otvoríte online pomocníka pre ESET Security for Microsoft SharePoint.

Nájsť rýchle riešenie

Pomocník obsahuje niekoľko návodov na riešenie častých problémov. Predtým, ako kontaktujete technickú podporu, vám odporúčame prečítať si túto sekciu.

Technická podpora

Odoslať žiadosť na technickú podporu

V prípade problému, na ktorý nenájdete odpoveď, je možné kontaktovať priamo pracovníkov technickej podpory prostredníctvom formulára na webovej stránke spoločnosti ESET.

Podrobnosti pre technickú podporu

Podrobné informácie (názov produktu, verzia produktu atď.) určené pre technickú podporu.

Podporné nástroje

Encyklopédia hrozieb

Odkaz na encyklopédiu hrozieb spoločnosti ESET, ktorá obsahuje informácie o nebezpečenstvách a symptómoch rôznych druhov infiltrácií.

ESET Log Collector

Odkaz na webovú stránku, kde si môžete stiahnuť nástroj ESET Log Collector. ESET Log Collector je nástroj určený na zhromažďovanie informácií a protokolov zo servera pre rýchlejšie vyriešenie problému.

História detekčného jadra

Odkaz na ESET Virus radar, ktorý obsahuje informácie o verziách detekčných modulov ESET.

ESET Specialized Cleaner

ESET Specialized Cleaner je nástroj na odstraňovanie rozšíreného malvéru a infiltrácií, ako napr. Conficker, Sirefef, Necurs atď.

Informácie o produkte a licencii

Aktivovať produkt / Zmeniť licenciu

Kliknite na túto možnosť pre otvorenie okna Aktivácia produktu. Vyberte si jednu z dostupných možností aktivácie programu ESET Security for Microsoft SharePoint.

O ESET Security for Microsoft SharePoint

Zobrazuje informácie o vašej kópii programu ESET Security for Microsoft SharePoint.

Odoslať žiadosť na technickú podporu

Na účely poskytnutia pomoci čo možno najrýchlejšie a najpresnejšie bude od vás spoločnosť ESET vyžadovať informácie o konfigurácii vášho produktu ESET Security for Microsoft SharePoint, podrobné systémové informácie, spustené procesy (protokol nástroja ESET SysInspector) a tiež údaje databázy Registry. Spoločnosť ESET použije tieto informácie len na účely poskytnutia technickej podpory. Toto nastavenie môžete zmeniť aj v časti **Rozšírené nastavenia** (**F5**) > **Nástroje** > **Diagnostika** > **Technická podpora**.

> Poznámka:
> Ak ste sa rozhodli odoslať systémové nastavenia, je potrebné vyplniť a odoslať webový formulár, v opačnom prípade vaša požiadavka na technickú podporu nebude vytvorená.

Ak odosielate webový formulár, vaše systémové nastavenia budú poskytnuté spoločnosti ESET. Zvoľte možnosť

Vždy odosielať tieto informácie, ak chcete, aby bola akcia pre tento proces zapamätaná.

Neodoslať informácie

Túto možnosť použite v prípade, ak si neprajete odosielať údaje. Budete presmerovaný na webovú stránku technickej podpory spoločnosti ESET.

O programe ESET Security for Microsoft SharePoint

Toto okno obsahuje podrobnosti o nainštalovanej verzii produktu ESET Security for Microsoft SharePoint. Vrchná časť okna obsahuje informácie o vašom operačnom systéme a systémových prostriedkoch, ako aj o práve prihlásených používateľoch. Okrem toho tu nájdete aj úplný názov počítača.

Nainštalované súčasti

Kliknutím na túto možnosť sa zobrazí zoznam nainštalovaných súčastí a podrobnosti o nich. Kliknutím na **Kopírovať** skopírujete zoznam do schránky. Môže to byť užitočné v prípade hľadania problému alebo pri kontaktovaní technickej podpory spoločnosti ESET.

Slovník pojmov

Bližšie informácie o technických termínoch, hrozbách a internetovej bezpečnosti nájdete v Slovníku pojmov.

Licenčná dohoda s koncovým používateľom

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 (ďalej len „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(ďalej len „ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou (ďalej len „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. Ak s niektorými podmienkami a požiadavkami tejto Dohody 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 (ďalej len „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 Dohody a dodržiavate všetky jej zmluvné podmienky, Poskytovateľ vám udeľuje nasledujúce práva (ďalej len „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 (ďalej len „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 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) **Business Edition.** Pre 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.** OEM Softvér sa viaže na počítač, s ktorým ste ho získali. 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 zániku Licencie musíte Softvér a všetky jeho záložné kópie okamžite zničiť alebo na vlastné 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 z času na čas vydať aktualizáciu Softvéru („Update“), avšak nie je 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. Na účely poskytovania 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.

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 (ďalej len „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 a informácie o zariadeniach v lokálnych sieťach, ako sú typ, dodávateľ, model a/alebo názov zariadenia (ďalej len „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. Týmto súhlasíte s prijímaním oznámení a správ vrátane, okrem iného, marketingových informácií.

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 Zmluvy 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, čím nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Zmluvy.

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. 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 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. 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 (ďalej iba 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 (ďalej iba Zákony na kontrolu vývozu); 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 (ďalej iba Sankčné zákony).

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.

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. V prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí anglická verzia. Zmeny tejto Dohody sú možné iba v písomnej forme, pričom za Poskytovateľa musí takúto zmenu podpísať štatutárny zástupca alebo osoba k tomuto úkonu výslovne splnomocnená.

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.

EULA ID: BUS-STANDARD-20-01

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
  - 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;
  - informácie o zariadeniach v lokálnej sieti, ako napríklad typ, dodávateľ, model a/alebo názov zariadenia;
  - informácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;
  - 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.

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