ESET Server Security

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

Copyright ©2024 ESET, spol. s r.o.

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

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

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

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

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

REV. 2024-01-16

1 Představení ... 1
1.1 Klíčové funkce ... 1
1.2 Co je nového? ... 2
1.3 Druhy ochrany ... 2
2 Příprava na instalaci ... 3
2.1 Systémové požadavky ... 4
2.2 Vyžadovaná kompatibilita s SHA-2 ... 5
2.3 ESET Server Security – průvodce instalací ... 6
2.3 Exportovat nastavení nebo odinstalovat produkt ... 10
2.4 Tichá / bezobslužná instalace ... 11
2.4 Instalace z příkazového řádku ... 12
2.5 Aktivace produktu ... 15
2.5 ESET Business Account ... 16
2.5 Úspěšná aktivace ... 16
2.5 Neúspěšná aktivace ... 16
2.5 Licence ... 17
2.6 Aktualizace na nejnovější verzi ... 17
2.6 Aktualizace prostřednictvím ESET PROTECT ... 18
2.6 Aktualizace prostřednictvím ESET clusteru ... 20
2.7 Instalace v clusteru ... 23
2.8 Terminálový server ... 23
2.9 Aktualizace zajišťující bezpečnost a stabilitu ... 24
3 Začínáme ... 24
3.1 Správa prostřednictvím ESET PROTECT ... 24
3.2 Přehled ... 25
3.2 Stavy ochrany ... 27
3.2 Jsou dostupné aktualizace Windows ... 28
3.2 Izolace od sítě ... 28
4 Práce s ESET Server Security ... 29
4.1 Kontrola ... 30
4.1 Okno a protokol kontroly ... 32
4.2 Protokoly ... 34
4.2 Filtrování protokolu ... 37
4.3 Aktualizace ... 39
4.4 Nastavení ... 41
4.4 Server ... 42
4.4 Počítač ... 43
4.4 Síť ... 44
4.4 Průvodce řešením problémů ... 45
4.4 Web a mail ... 45
4.4 Nástroje – Diagnostické protokolování ... 46
4.4 Import a export nastavení ... 47
4.5 Nástroje ... 48
4.5 Spuštěné procesy ... 49
4.5 Sledování aktivity ... 50
4.5 Statistiky ochrany ... 51
4.5 Cluster ... 52
4.5 Průvodce clusterem – výběr uzlů ... 54
4.5 Průvodce clusterem – konfigurace clusteru ... 55
4.5 Průvodce clusterem – možnosti konfigurace ... 56

4.5 Průvodce clusterem – ověření uzlů ... 56
4.5 Průvodce clusterem – instalace uzlů a aktivace clusteru ... 58
4.5 ESET Shell ... 61
4.5 Použití ... 63
4.5 Příkazy ... 67
4.5 Dávkové soubory / skriptování ... 70
4.5 ESET SysInspector ... 71
4.5 ESET SysRescue Live ... 72
4.5 Plánovač ... 73
4.5 Vytvoření naplánované úlohy ... 74
4.5 Typ úlohy ... 77
4.5 Opakování úlohy ... 78
4.5 Při události ... 78
4.5 Spuštění aplikace ... 79
4.5 Neprovedení úlohy ... 79
4.5 Přehled naplánované úlohy ... 79
4.5 Odeslat soubor k analýze ... 79
4.5 Podezřelý soubor ... 80
4.5 Podezřelá stránka ... 81
4.5 Falešně detekovaný soubor ... 81
4.5 Falešně detekovaná stránka ... 82
4.5 Ostatní ... 82
4.5 Karanténa ... 82
4.6 Nastavení OneDrive kontroly ... 84
4.6 Registrace aplikace ESET OneDrive skener ... 87
4.6 Odregistrace aplikace ESET OneDrive skener ... 92
5 Rozšířená nastavení ... 96
5.1 Detection engine ... 97
5.1 Ochrana s využitím strojového učení ... 99
5.1 Výjimky ... 101
5.1 Výkonnostní výjimky ... 101
5.1 Průvodce vytvořením výjimky ... 104
5.1 Rozšířená nastavení ... 104
5.1 Automatické výjimky ... 105
5.1 Sdílená lokální cache ... 105
5.1 Byla nalezena infiltrace ... 105
5.1 Rezidentní ochrana souborového systému ... 106
5.1 ThreatSenseParametry skenovacího jádra ... 108
5.1 Doplňující parametry skenovacího jádra ThreatSense ... 111
5.1 Typy rozšíření vyloučených z kontroly ... 111
5.1 Vyloučené procesy ... 112
5.1 Cloudová ochrana ... 113
5.1 Filtr výjimek ... 115
5.1 Detekce škodlivého kódu ... 115
5.1 Správa profilů ... 117
5.1 Cíle profilu ... 117
5.1 Cíle kontroly ... 119
5.1 Kontrola při nečinnosti ... 121
5.1 Kontrola souborů zaváděných při startu počítače ... 121
5.1 Automatická kontrola souborů spouštěných při startu počítače ... 121
5.1 Výměnná média ... 122

5.1 Ochrana dokumentů ... 123
5.1 Hyper-V kontrola ... 123
5.1 OneDrive kontrola ... 125
5.1 HIPS ... 126
5.1 Nastavení pravidel HIPS ... 128
5.1 Rozšířená nastavení HIPS ... 131
5.2 Konfigurace aktualizací ... 131
5.2 Obnovení předchozí verze modulů ... 135
5.2 Aktualizace naplánované úlohy ... 135
5.2 Aktualizační mirror ... 135
5.3 Síťová ochrana ... 137
5.3 Známé sítě ... 137
5.3 Přidat síť ... 138
5.3 Zóny ... 139
5.4 Ochrana proti síťovým útokům ... 139
5.4 IDS výjimky ... 140
5.4 Zablokována podezřelá hrozba ... 141
5.4 Seznam dočasně blokovaných IP adres ... 141
5.4 Ochrana proti útokům hrubou silou ... 142
5.4 Pravidla ochrany proti útokům hrubou silou ... 142
5.4 Výjimky ochrany proti útokům hrubou silou ... 142
5.5 Web a mail ... 143
5.5 Filtrování protokolů ... 143
5.5 Weboví a poštovní klienti ... 144
5.5 SSL/TLS ... 144
5.5 Seznam známých certifikátů ... 146
5.5 Šifrovaná SSL/TLS komunikace ... 146
5.5 Ochrana poštovních klientů ... 147
5.5 Poštovní protokoly ... 148
5.5 Upozornění a oznámení ... 149
5.5 Nástrojová lišta Microsoft Outlook ... 150
5.5 Panel nástrojů v Outlook Express a Windows Mail ... 150
5.5 Potvrzovací dialog ... 151
5.5 Opakovaná kontrola zpráv ... 151
5.5 Ochrany přístupu na web ... 151
5.5 Správa URL adres ... 152
5.5 Vytvoření nového seznamu ... 153
5.5 Anti-Phishingová ochrana ... 154
5.6 Správa zařízení ... 155
5.6 Editor pravidel ... 156
5.6 Skupiny zařízení ... 158
5.7 Nástroje ... 159
5.7 Časové sloty ... 160
5.7 Aktualizace operačního systému Windows ... 160
5.7 Skener příkazového řádku ... 160
5.7 ESET CMD ... 162
5.7 ESET RMM ... 164
5.7 Licence ... 165
5.7 Poskytovatel WMI ... 165
5.7 Poskytovaná data ... 166
5.7 Přístup k poskytovaným datům ... 176

5.7 Cíle kontroly: ESET konzole pro vzdálenou správu 176
5.7 Dočasná změna nastavení 177
5.7 Protokoly 179
5.7 Proxy server 180
5.7 Oznámení 181
5.7 Oznámení aplikace 182
5.7 Oznámení na pracovní ploše 182
5.7 Oznámení e-mailem 183
5.7 Přizpůsobení 184
5.7 Prezentační režim 185
5.7 Diagnostika 185
5.7 Technická podpora 187
5.7 Cluster 187
5.8 Uživatelské rozhraní 188
5.8 Upozornění a informační okna 189
5.8 Přístup k nastavení 190
5.8 ESET Shell 191
5.8 Deaktivace grafického rozhraní na terminálovém serveru 191
5.8 Vypnout zprávy a stavy 192
5.8 Nastavení stavů aplikace 192
5.8 Ikona v oznamovací oblasti Windows 193
5.9 Obnovit na standardní nastavení 194
5.10 Nápověda a podpora 195
5.10 Založit požadavek na technickou podporu 195
5.10 O programu ESET Server Security 196
5.11 Slovník pojmů 196
6 Licenční ujednání s koncovým uživatelem 196
7 Zásady ochrany osobních údajů 203

Představení

ESET Server Security je integrované řešení speciálně vyvinuté pro serverové prostředí Microsoft Windows. ESET Server Security přináší efektivní a stabilní ochranu před škodlivým kódem. Poskytuje dva druhy ochrany: Anti-Malware a Antispyware.

Přečtěte si také kapitoly Klíčové funkce a Co je nového v nejnovější verzi.

Klíčové funkce

V této kapitole uvádíme přehled funkcí, které produkt ESET Server Security nabízí. ESET Server Security podporuje většinu edicí Microsoft Windows Server 2008 R2 SP1, 2012, 2016 a 2019 provozovaných samostatně i v prostředí clusteru. Ve velkých sítích můžete ESET PROTECT spravovat vzdáleně prostřednictvím ESET Server Security.

Nativní 64-bitové jádro	**Jádro produktu je výkonnější a stabilnější.**
Anti-Malware	Oceňovaná a inovativní ochrana proti škodlivému kódu. Díky nejmodernějším technologiím s podporou cloudu zabraňujeme s vysokou úspěšností útokům a eliminujeme všechny typy hrozeb včetně virů, ransomware, rootkitů, červů a spywaru. Zároveň nezatěžuje systém, šetří systémové prostředky a nemá negativní vliv na výkon. Anti-malwarové jádro využívá více-vrstvý bezpečnostní model. Každá vrstva (fáze) se skládá z několika technologií. V pre-execution fázi se na detekci podílí UEFI skener, ochrana proti síťovým útokům, reputace a cache, produktový sandbox a DNA detekce. Při spuštění objektu (execution fázi) je aktivní Exploit Blocker, ochrana proti ransomware, Advanced Memory Scanner a modul kontroly skriptů (AMSI). V post-execution fázi dokáže objekt detekovat ochrana proti zapojení do botnetu, Cloud Malware Protection System a sandboxing. Kombinace těchto "core" technologií vám poskytuje bezkonkurenční úroveň ochrany.
OneDrive kontrola	Prostřednictvím této nové funkce můžete kontrolovat obsah uložený na cloudovém úložišti OneDrive. Ta je dostupná pro Office 365 business účty.
Hyper-V kontrola	Pomocí této možnosti zkontrolujete disky virtuálních počítačů na Microsoft Hyper-V Serveru bez toho, aniž byste museli na virtuální počítač instalovat "agenta".
ESET LiveGuard Advanced	Cloudová služba zajišťovaná společností ESET. Pokud ESET Server Security detekuje podezřelý kód nebo chování vzorku, zabrání další potenciálně škodlivé aktivitě dočasným přesunutím objektu do ESET LiveGuard Advanced karantény. Podezřelý vzorek je zároveň automaticky odeslán na ESET LiveGuard Advanced server, kde je analyzován prostřednictvím pokročilých detekčních technik. Po dokončení analýzy obdrží ESET Server Security její výsledek. V závislosti na výsledku a konfiguraci produktu je provedena, ať již se souborem nebo zprávou, odpovídající akce.
ESET Cluster	Prostřednictvím funkce ESET Cluster můžete spravovat více serverů z jednoho místa. Díky tomu si zapojením jednotlivých uzlů do clusteru usnadníte jejich správu – distribucí jednotné konfigurace mezi všemi členy clusteru. Samotný cluster vytvoříte z libovolné instalace produktu, z níž následně můžete provést instalaci na ostatní uzly clusteru a jejich inicializaci. Serverové produkty ESET dokáží komunikovat mezi sebou, vyměňovat si data jako je konfigurace, upozornění a synchronizovat data potřebná pro správné fungování skupiny produktů. Tím zajistíte stejnou konfiguraci produktu na všech členech clusteru. ESET Server Security podporuje Windows Failover a Network Load Balancing (NLB) clustery. Kdykoli můžete do ESET Cluster přidat členy ručně, a nemusí být součásti Windows Clusteru. ESET Cluster je dostupná jak v doménovém prostředí, tak pracovní skupině (workgroup).
Automatické výjimky	Program automaticky zjistí a vytvoří výjimky na kritické soubory aplikací a operačního systému pro zajištění plynulého chodu serveru.

Nativní 64-bitové jádro	Jádro produktu je výkonnější a stabilnější.
Vyloučené procesy	Prostřednictvím této funkce vyloučíte činnost konkrétních procesů z anti-malware kontroly. Tato kontrola může v některých případech způsobovat konflikt, například při zálohování nebo živé migraci virtuálních strojů. Pomocí těchto výjimek můžete minimalizovat riziko vzniku konfliktu a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (.exe).
eShell (ESET Shell)	Nová generace (eShell 2.0) příkazového řádku pro pokročilé uživatelé a administrátory určeného pro správu serverových produktů ESET.
ESET PROTECT	Vylepšená integrace s ESET PROTECT zahrnuje možnost plánování volitelných kontrol. Další informace najdete v online nápovědě k ESET PROTECT.
Instalace po komponentách	Kdykoli se můžete rozhodnout a komponenty přidat nebo odebrat.

Co je nového?

Nové funkce a vylepšení v ESET Server Security:

- Nativní 64-bitové jádro
- OneDrive kontrola
- ESET LiveGuard Advanced
- Podpora ESET Inspect
- ESET RMM
- Izolace od sítě
- Ochrana s využitím strojového učení
- Audit log
- mikro aktualizace programových komponent
- Ochrana proti útokům hrubou silou

Druhy ochrany

K dispozici jdou dva typy ochrany:

- Anti-malwarová ochrana
- Antispywarová ochrana

Anti-Malwarová a Antispywarová ochrana je jednou ze základních funkcí produktu ESET Server Security. Chrání systém před škodlivým kódem, který by se do systému dostal prostřednictvím souborového systému, e-mailu nebo internetové komunikace. V případě zjištění škodlivého kódu jej detekční modul dokáže eliminovat zablokováním, následným vyléčením, odstraněním nebo přesunutím do karantény.

Příprava na instalaci

Před tím, než se pustíte do instalace produktu, doporučujeme provést následující kroky:

- Po zakoupení licence si z webových stránek společnosti ESET stáhněte instalační *.msi* balíček produktu ESET Server Security.

- Ujistěte se, že server, na který se chystáte produkt ESET Server Security nasadit, splňujesystémové požadavky

- Přihlaste se na server pod administrátorským účtem.

> Instalační soubor je nutné spouštět po přihlášení do vestavěného administrátorského účtu, případně musíte být přihlášeni v účtu doménového administrátora (pokud je lokální účet administrátora deaktivovaný). Jakýkoliv jiný uživatelský účet, byť je členem administrátorské skupiny, nemá dostatečná práva pro instalaci. Při použití jiného účtu (než lokálního nebo doménového administrátora), nemusí být instalace úspěšně dokončena.

- Pokud se chytáte aktualizovat existující instalaci produktu ESET Server Security, doporučujeme provést zálohu konfigurace prostřednictvím funkce pro export nastavení.

- Ujistěte se, že v systému není nainstalováno jiné bezpečnostní řešení. Pokud ano, odinstalujte jej. Doporučujeme vám použít nástroj ESET AV Remover. Seznam antivirových programů třetích stran, které lze odstranit pomocí programu ESET AV Remover, naleznete v Databázi znalostí.

- Před zahájením instalace ESET Server Security na Windows Server 2016 společnost Microsoft doporučuje ze systému odinstalovat Windows Defender a odebrat Windows Defender ATP, abyste předešli problémům způsobeným tím, že je v počítači nainstalováno více antivirových produktů.

- Před zahájením instalace ESET Server Security na Windows Server 2019 nebo Windows Server 2022 společnost Microsoft doporučuje přepnout Windows Defender do pasivního režimu, aby nedocházelo ke konfliktu s dalším bezpečnostním produktem.

Instalační balíček produktu ESET Server Security můžete spustit ve dvou režimech:

- Grafické uživatelské rozhraní (GUI)
  Doporučený způsob instalace prostřednictvím grafického průvodce.

- Tichá / bezobslužná instalace
  V případě potřeby můžete produkt ESET Server Security nainstalovat tiše prostřednictvím příkazového řádku.

- Aktualizace na nejnovější verzi
  Pokud používáte starší verzi produktu ESET Server Security, vyberte si pro vás nejvhodnější způsob aktualizace.

> Pokud je to možné, doporučujeme nainstalovat ESET Server Security na nově instalovaný a nakonfigurovaný operační systém. V případě, kdy ESET Server Security instalujete na již existující systém, doporučujeme nejprve odinstalovat původní verzi ESET Server Security, restartovat server a následně nainstalovat nejnovější verzi produktu.

Po dokončení instalace ESET Server Security nebo aktualizace mohou být vyžadovány další kroky:

- Aktivace produktu

Dostupnost jednotlivých metod závisí na zemi a způsobu distribuce.

- Konfigurace produktu

Úpravou rozšířených nastavení si přizpůsobte produkt ESET Server Security vašim potřebám.

Systémové požadavky

Podporované operační systémy:

- Microsoft Windows Server 2022 (Server Core a Desktop Experience)
- Microsoft Windows Server 2019 (Server Core a Desktop Experience)
- Microsoft Windows Server 2016 (Server Core a Desktop Experience)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 s nainstalovanou aktualizací KB4474419 a KB4490628 (přečtěte si informace týkající se vyžadované podpory SHA-2)
- Server Core (Microsoft Windows Server 2008 R2 SP1, 2012, 2012 R2)

Na Windows Server 2008 R2 SP1 se standardně neinstaluje součást **Síťová ochrana** (při vybrání možnosti **typická** instalace). Pokud chcete tuto součást nainstalovat, v instalačním průvodci vyberte **vlastní** způsob instalace.

Pro instalaci nebo aktualizaci produktů ESET vydaných po konci července 2023 je nutné nainstalovat podporu Podepisování kódu pomocí Azure do všech operačních systémů Windows. Další informace. Pokud používáte Windows Server 2008 R2 SP1, ujistěte se, že máte nainstalovanou sadu KB5006728, která podporuje program Podepisování kódu Azure. Pro instalaci KB5006728 jsou vyžadovány ESU (Extended Security Updates).

Storage, Small Business a MultiPoint servery:

- Microsoft Windows Storage Server 2016
- Microsoft Windows Storage Server 2012 R2
- Microsoft Windows Storage Server 2012
- Microsoft Windows Server 2019 Essentials
- Microsoft Windows Server 2016 Essentials
- Microsoft Windows Server 2012 R2 Essentials
- Microsoft Windows Server 2012 Essentials
- Microsoft Windows Server 2012 Foundation

- Microsoft Windows Small Business Server 2011 SP1 (x64) s nainstalovanou aktualizací KB4474419 a KB4490628
- Microsoft Windows MultiPoint Server 2012
- Microsoft Windows MultiPoint Server 2011
- Microsoft Windows MultiPoint Server 2010

Podporované hostitelské operační systém s Hyper-V rolí:

- 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 – zkontrolovat je možné pouze offline virtuální počítače

Hardwarové požadavky závisí na používané verzi operačního systému. Pro detailní informace o hardwarových požadavcích doporučujeme prostudovat dokumentaci operačního systému Microsoft Windows Server.

> Před nainstalováním bezpečnostního produktu doporučujeme nainstalovat veškeré aktualizace a Service Packy pro daný operační systém. Veškeré aktualizace a opravy Windows doporučujeme instalovat ve chvíli, kdy jsou dostupné.

Minimální hardwarové požadavky:

Komponenty	Požadavky
Procesor	Jednojádrový x64 AMD nebo Intel
Paměť	256 MB volné paměti
Pevný disk	700 MB volného místa
Rozlišení obrazovky	800 x 600 pixelů a vyšší

Vyžadovaná kompatibilita s SHA-2

Společnost Microsoft označila hashovací funkci Secure Hash Algorithm 1 (SHA-1) za zastaralou a počátkem roku 2019 zahájila migraci na SHA-2. Z tohoto důvodu nejsou certifikáty podepsané SHA-1 algoritmem akceptovány, což povede k bezpečnostním upozorněním. Algoritmus SHA-1 se stal v čase méně bezpečným z důvodu objevených slabin, rostoucímu výkonu procesů a nástupu cloud computingu.

Hashovací funkce SHA-2, jakožto nástupce SHA-1, je preferovaná při ověření zabezpečení SSL protokolu. Další informace o ukončení podpory algoritmu SHA-1 naleznete na v článku Hash and Signature Algorithm v Databázi znalostí společnosti Microsoft.

To znamená, že se na operačních systémech bez podpory SHA-2 nebudou schopny bezpečnostní produkty ESET aktualizovat (a to včetně detekčního jádra), a nebudou funkční. V důsledku toho se nebude ESET Server Security plně funkční a nebude zajišťovat potřebnou ochranu.

Pokud používáte Microsoft Windows Server 2008 R2 SP1 nebo Microsoft Windows Small Business Server 2011 SP1, ujistěte se, že je kompatibilní s SHA-2. V závislosti na systému doinstalujte odpovídající aktualizace:

- **Microsoft Windows Server 2008 R2 SP1** — aplikujte KB4474419 a KB4490628 (může být vyžadován další restart)

- **Microsoft Windows Small Business Server 2011 SP1 (x64)** - aplikujte KB4474419 a KB4490628 (může být vyžadován další restart)

Po nainstalování aktualizací a restartování systému otevřete hlavní okno programu ESET Server Security a zkontrolujte jeho stav. V případě, že bude oranžový, restartujte systém ještě jednou. Následně by již měl být stav zelený, což znamená maximální ochranu.

Doporučujeme nainstalovat nejnovější Service Pack pro váš operační systém Microsoft Server a aplikaci. Veškeré aktualizace a opravy Windows doporučujeme instalovat ve chvíli, kdy jsou dostupné.

ESET Server Security – průvodce instalací

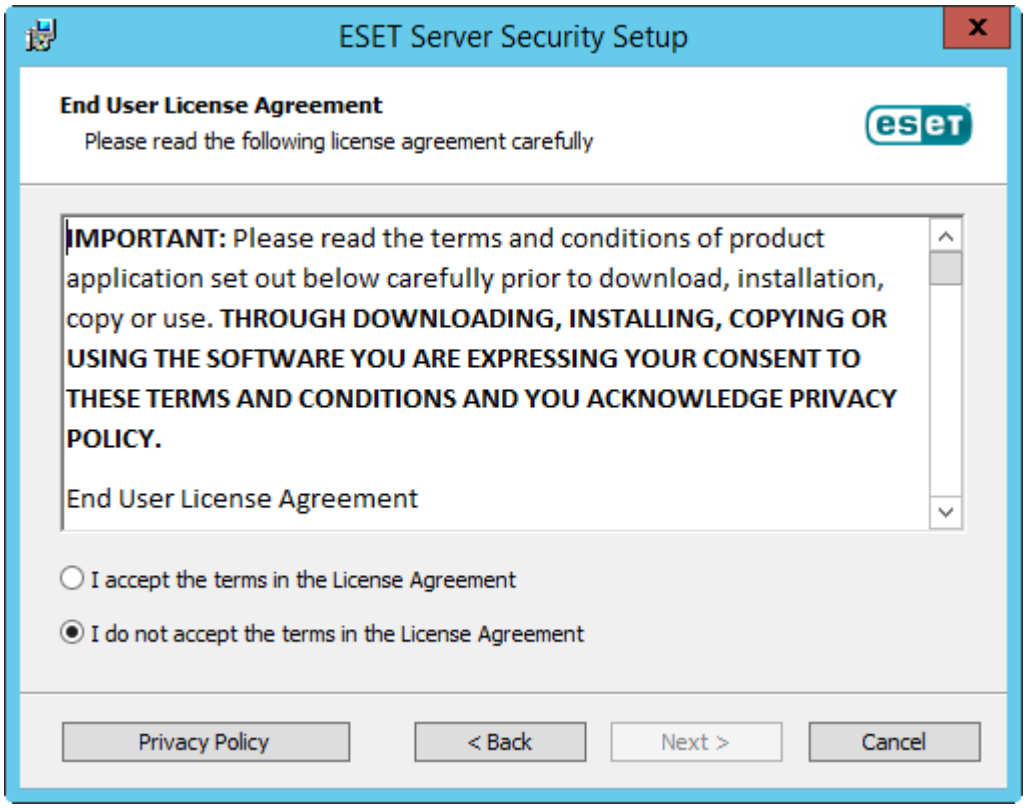
Jedná se o typického průvodce instalací prostřednictvím grafického uživatelského rozhraní. Dvakrát klikněte na instalační *.msi* balíček produku ESET Server Security a postupujte podle kroků na obrazovce:

1. Pro pokračování klikněte na tlačítko **Další**, v opačném případě kliknutím na **Zrušit** ukončete instalaci.

2. Průvodce instalací se spustí automaticky v jazyce, který je vybrán v dialogovém okně **Oblast** > **Místo** > **Umístění počítače** (v případě starších systémů **Oblast a jazyk** > **Místo** > **Aktuální umístění**). Z rozbalovacího menu **Jazyk produktu** si vyberte ten, ve kterém chcete ESET Server Security nainstalovat. Výběr jazyka pro ESET Server Security nemá vliv na jazyk průvodce instalací.



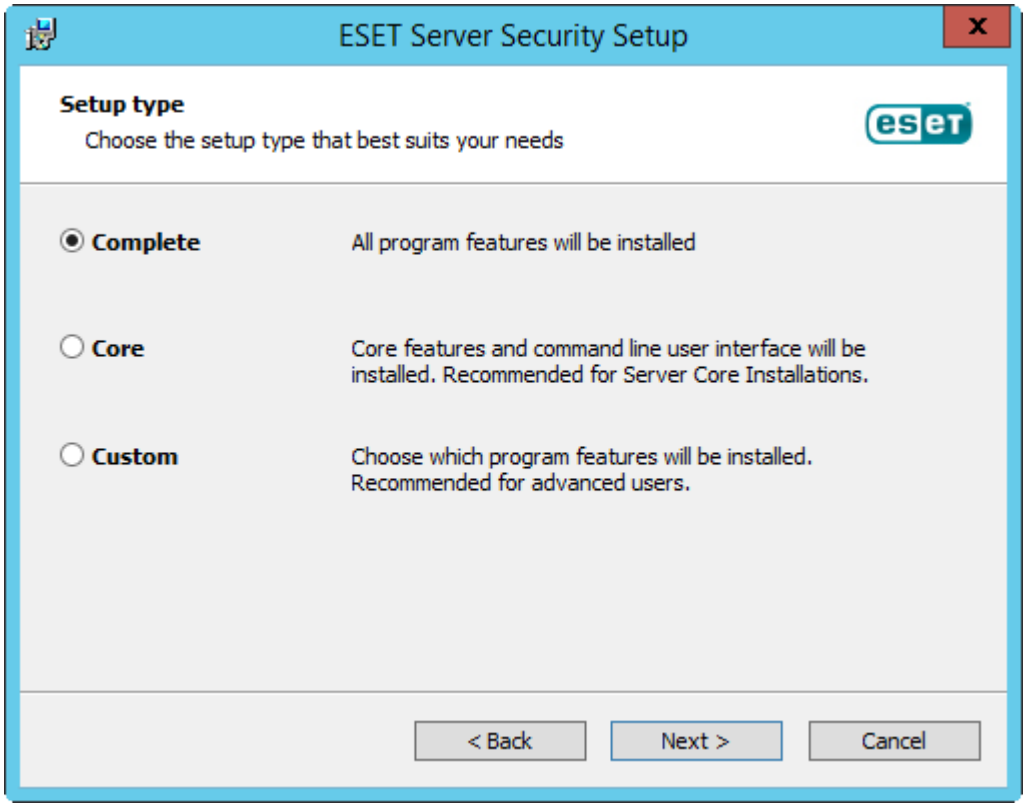
3. Pro zobrazení Licenční ujednání s koncovým uživatelem klikněte na tlačítko **Další**. Po potvrzení souhlasu s licenčním ujednáním s koncovým uživatelem (EULA) a zásadami ochrany osobních údajů pokračujte kliknutím na tlačítko **Další**.



4. Dále si vyberte způsob instalace (dostupnost jednotlivých možností závisí na vámi používaném operačním systému):

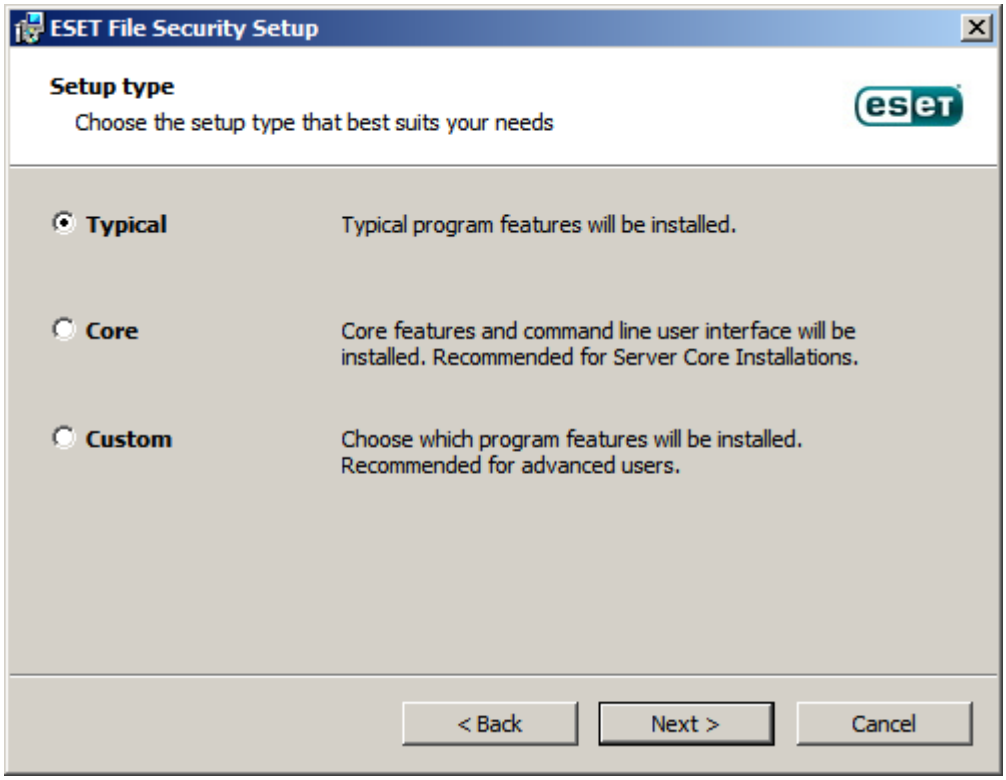
Úplná

Po vybrání této možnosti se nainstalují všechny funkce programu ESET Server Security. Tato instalace se nazývá rovněž kompletní. Jedná se o doporučený typ instalace a je dostupný na Windows Server 2012, 2012 R2, 2016, 2019, Windows Server 2012 Essentials, 2012 R2 Essentials, 2016 Essentials a 2019 Essentials.



Typická

Po vybrání této možnosti se nainstalují doporučené funkce programu ESET Server Security. Tento typ je dostupný na 2008 R2 SP1 a 2011.



Core

Tento typ instalace je určen pro edice Windows Server Core. Průběh instalace je stejný jako v případě úplné instalace, ale nainstalují se pouze základní funkce a příkazový řádek pro ovládání programu. Ačkoli je tento typ instalace určen především na Windows Server Core, můžete ji v případě zájmu nainstalovat na běžnou edici Windows Server. Mějte na paměti, že bezpečnostní produkt ESET nebude v tomto případě disponovat grafickým rozhraním. To znamená, že ESET Server Security bude možné ovládat pouze prostřednictvím příkazového řádku. Pro více informací a seznam dalších instalačních parametrů přejděte do kapitoly instalace z příkazového řádku.

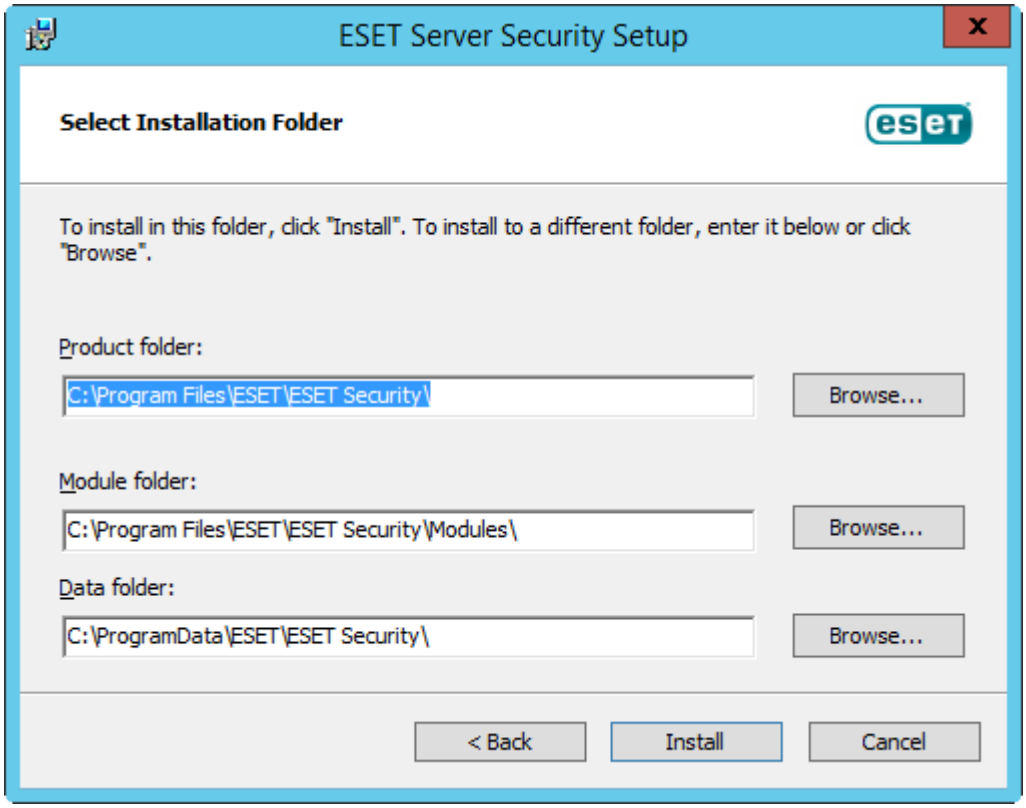
Pro spuštění core instalace prostřednictvím příkazového řádku použijte níže uvedených vzorový příkaz:
`msiexec /qn /i efsw_nt64.msi ADDLOCAL=_Base`

Vlastní

Po vybrání této možnosti si můžete vybrat funkce a komponenty ESET Server Security, které chcete nainstalovat. Seznam dostupných modulů a funkcí se zobrazí před zahájením instalace. Tuto možnost využijte v případě, kdy si chcete přizpůsobit ESET Server Security, a nainstalovat komponenty, které potřebujete.

Na Windows Server 2008 R2 SP1 se standardně neinstaluje součást **Síťová ochrana** (při vybrání možnosti **typická** instalace). Pokud chcete tuto funkci nainstalovat, v instalačním průvodci vyberte **vlastní** způsob instalace.

5. Dále vyberte umístění, do kterého chcete ESET Server Security nainstalovat. Standardně se program nainstaluje do složky *C:\Program Files\ESET\ESET Server Security*. Pro změnu umístění klikněte na tlačítko **Procházet** (nedoporučujeme).

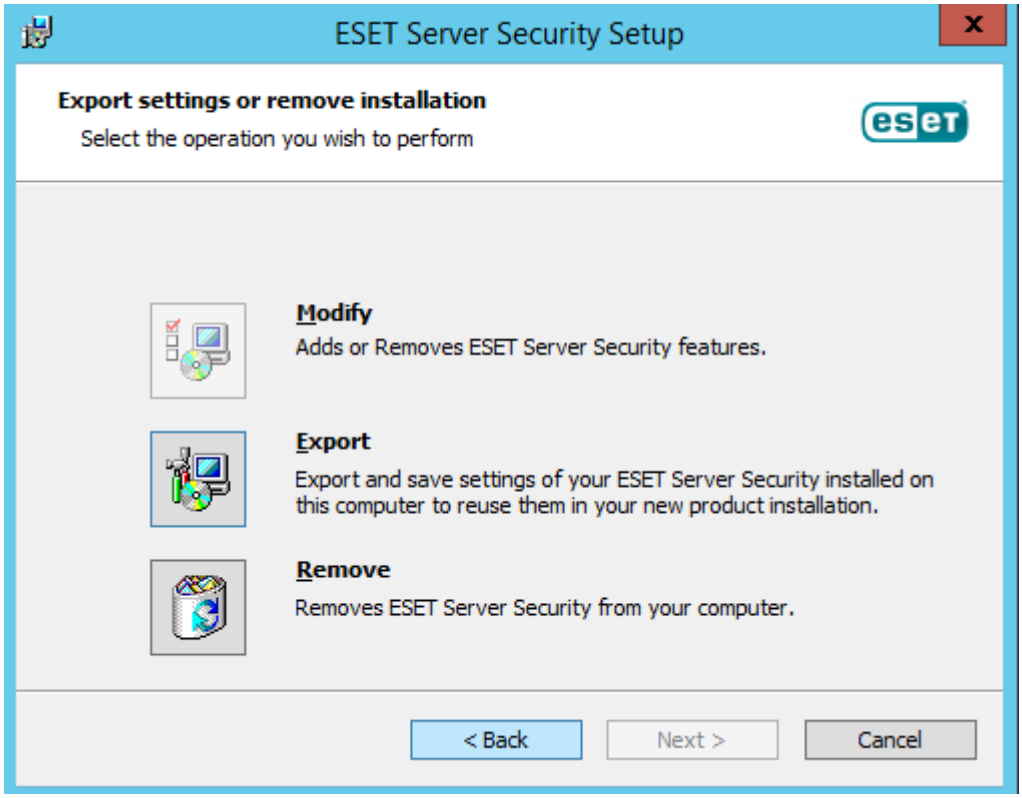


6. Pro zahájení instalace klikněte na tlačítko **Instalovat**. Po dokončení instalace se spustí grafické rozhraní produktu a v oznamovací oblasti Windows se zobrazí ikona produktu.

Exportovat nastavení nebo odinstalovat produkt

Můžete exportovat a uložit nastavení nebo zcela odebrat instalaci. Chcete-li tak učinit, spusťte instalační balíček .msi, který jste použili během počáteční instalace, nebo přejděte na **Programy a funkce** (přístupné z Ovládacích panelů systému Windows), klikněte pravým tlačítkem myši ESET Server Security a vyberte **Změnit**.

Nastavení ESET Server Security můžete **Exportovat** nebo můžete ESET Server Security **Odebrat** (odinstalovat) úplně.



Tichá / bezobslužná instalace

Produkt automaticky nainstalujete z příkazového řádku, bez zobrazení průvodce instalací, příkazem v následujícím formátu: `msiexec /i <packagename> /qn /l*xv msi.log`

Na Windows Server 2008 R2 SP1 se standardně neinstaluje součást **Síťová ochrana**.

Pro ověření úspěšné instalace, případně zjištění problémů souvisejících s instalací si otevřete Prohlížeč událostí a v **Protokolu aplikací** hledejte Zdroj: MsiInstaller).

Úplná instalace produktu na 64-bitový systém:

```
msiexec /i efsw_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Instalace produktu v **požadovaném jazyce** (čeština):

```
msiexec /i efsw_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```

Více informací o **jazykových kódech** naleznete v kapitole instalace z příkazového řádku

Po dokončení instalace se spustí grafické rozhraní produktu a v oznamovací oblasti Windows se zobrazí ikona produktu.

Při použití parametru `REINSTALL` definujte všechny ostatní funkce, které jste nepoužili v parametrech `ADDLOCAL` a `REMOVE`. Pro správný průběh instalace z příkazového řádku je nutné, abyste uvedli všechny funkce jako hodnoty parametrů `REINSTALL`, `ADDLOCAL` a `REMOVE`. Při vynechání parametru `REINSTALL` se nemusí podařit přidání/odebrání komponent.
Úplný seznam všech funkcí naleznete v kapitole instalace z příkazového řádku.

Produkt ze 64-bitového systému kompletně **odeberete** následujícím příkazem:
`msiexec /x efsw_nt64.msi /qn /l*xv msi.log`

Server se po odinstalování produktu automaticky restartuje.

Instalace z příkazového řádku

Následující nastavení jsou určena pro použití **pouze se sníženou**, **základní** a **žádnou** úrovní uživatelského rozhraní. Informace o tom, jaké přepínače příkazového řádku podporuje konkrétní verze **msiexec**, naleznete v dokumentaci.

Podporované parametry:

APPDIR=<path>

- cesta – platná cesta ke složce.
- Složka, do které se aplikace nainstaluje.
- Příklad: `efsw_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

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

MODULEDIR=<path>

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

ADDLOCAL=<list>

- Komponenty k instalaci – seznam nepovinných funkcí, které se lokálně nainstalují.
- Příklad použití `.msi` balíčku: `efsw_nt64.msi /qn ADDLOCAL=<list>`
- Pro více informací o vlastnosti `ADDLOCAL` přejděte do databáze znalostí společnosti Microsoft: https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal
- `ADDLOCAL` Je seznam funkcí oddělených čárkou, které chcete nainstalovat.
- Po vybrání funkce, kterou chcete instalovat, je nutné definovat úplnou cestu (včetně jejich rodičů).

REMOVE=<list>

- Komponenty k instalaci – nadřazená funkce, kterou nechce nainstalovat.
- Příklad použití `.msi` balíčku: `efsw_nt64.msi /qn REMOVE=<list>`

- Pro více informací o vlastnosti `REMOVE` přejděte do databáze znalostí společnosti Microsoft: https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove

- `REMOVE` je seznam funkcí oddělených čárkou, které nebudou nainstalován (případně budou odebrány z existující instalace).

- Postačí definovat pouze nadřazenou funkci. Není nutné explicitně vyjmenovávat všechny potomky funkce.

ADDEXCLUDE=<list>

- `ADDEXCLUDE` je seznam funkcí oddělených čárkou, které nechcete nainstalovat.

- Po vybrání funkce, kterou nechcete instalovat, je nutné definovat úplnou cestu (včetně jejich podfunkcí) a související neviditelné funkce.

- Příklad použití `.msi` balíčku: `efsw_nt64.msi /qn ADDEXCLUDE=<list>`

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

Přítomnost funkce

- **Povinná** – tato komponenta musí být vždy nainstalována

- **Volitelná** – instalaci těchto komponent můžete zrušit

- **Neviditelná** – povinná součást pro nadřazené komponenty

Seznam funkcí produktu ESET Server Security:

> V názvech funkcí se rozlišuje velikost písmen. `RealtimeProtection` není to samé jako `REALTIMEPROTECTION`.

Název funkce	Přítomnost funkce
`SERVER`	Povinná
`RealtimeProtection`	Povinná
`WMIProvider`	Povinná
`HIPS`	Povinná
`Updater`	Povinná
`eShell`	Povinná
`UpdateMirror`	Povinná
`DeviceControl`	Volitelná
`DocumentProtection`	Volitelná
`WebAndEmail`	Volitelná
`ProtocolFiltering`	Neviditelná
`NetworkProtection`	Volitelná
`IdsAndBotnetProtection`	Volitelná
`Rmm`	Volitelná
`WebAccessProtection`	Volitelná

Název funkce	Přítomnost funkce
EmailClientProtection	Volitelná
MailPlugins	Neviditelná
Cluster	Volitelná
_Base	Povinná
eula	Povinná
ShellExt	Volitelná
_FeaturesCore	Povinná
GraphicUserInterface	Volitelná
SysInspector	Volitelná
SysRescue	Volitelná
EnterpriseInspector	Volitelná

Pokud se rozhodnete odebrat některou z následujících funkcí, musíte odebrat celou skupinu funkcí. V opačném případě nedojde k odebrání funkce. Níže jsou dvě skupiny (každý řádek představuje jednu skupinu):

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailP
lugins,EmailClientProtection
```

✓ Odebrání **NetworkProtection** prostřednictvím parametru `REMOVE` a definováním pouze nadřazené funkce:
`msiexec /i efsw_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection`
Volitelně můžete použít parametr `ADDEXCLUDE`, poté však definuje všechny podřízené funkce:
`msiexec /i efsw_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^ ProtocolFiltering,MailPlugins,EmailClientProtection`

✓ Příklad core instalace:
`msiexec /qn /i efsw_nt64.msi /l*xv msi.log ADDLOCAL=RealtimeProtection,Rmm`

Pokud chcete produkt ESET Server Security automaticky nakonfigurovat po dokončení instalace, použijte v instalačním příkazu základní konfigurační parametry.

✓ Instalace ESET Server Security s vypnutou funkcí ESET LiveGrid®:
`msiexec /qn /i efsw_nt64.msi ADDLOCAL=RealtimeProtection,Rmm,GraphicUserInterface CFG_LIVEGRID_ENABLED=0`

Seznam CFG_ parametrů:

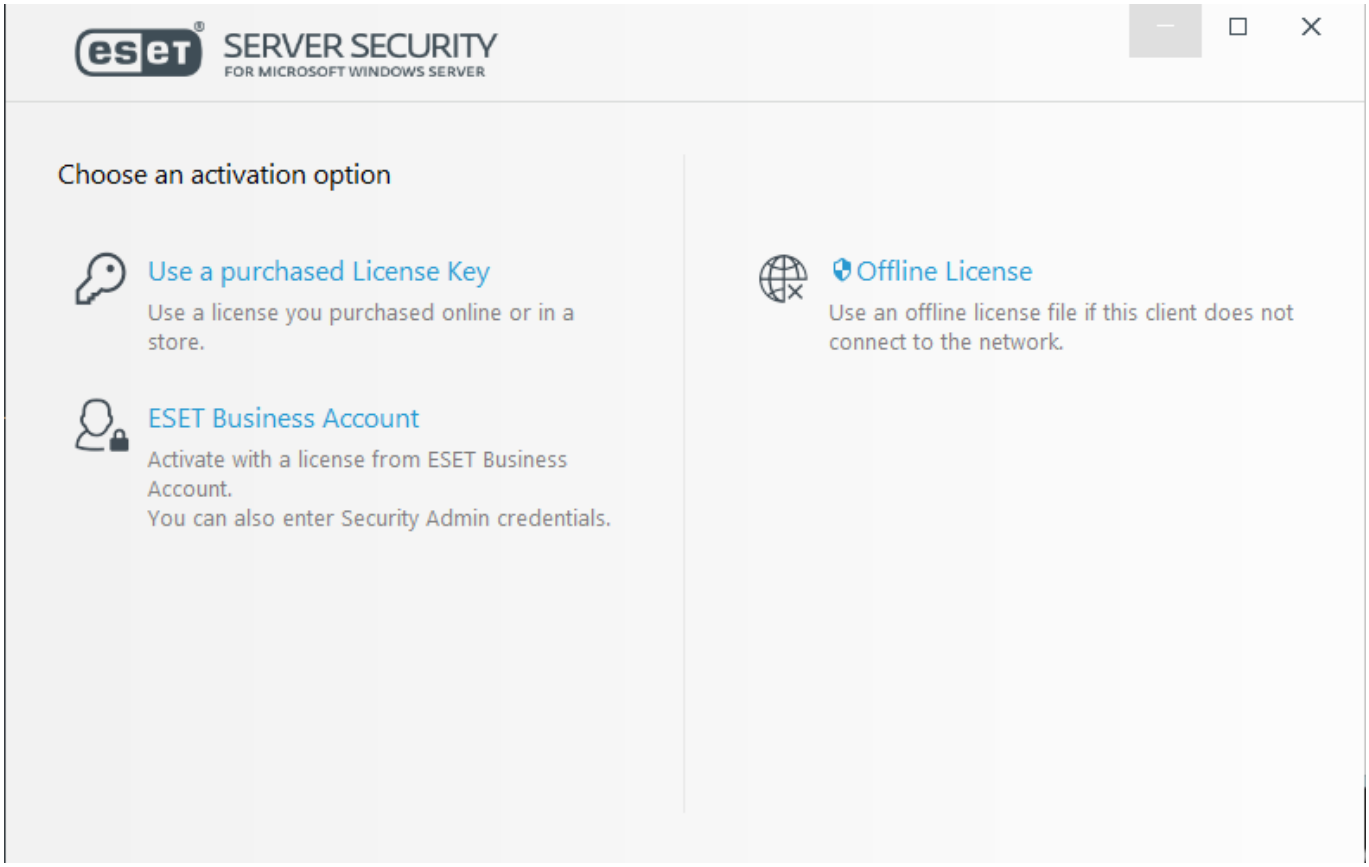
Přepínač	Hodnota
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 – vypnuto, 1 – zapnuto
CFG_LIVEGRID_ENABLED=1/0	0 – vypnuto, 1 – zapnuto
FIRSTSCAN_ENABLE=1/0	0 – vypnuto, 1 – zapnuto
CFG_PROXY_ENABLED=0/1	0 – vypnuto, 1 – zapnuto
CFG_PROXY_ADDRESS=<ip>	IP adresa proxy serveru
CFG_PROXY_PORT=<port>	Port proxy serveru
CFG_PROXY_USERNAME=<user>	Uživatelské jméno pro autentifikaci
CFG_PROXY_PASSWORD=<pass>	Heslo pro autentifikaci

Parametry jazyka: Jazyk produktu (definovat je nutné oba parametry)

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

Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu.



ESET Server Security můžete aktivovat níže uvedenými způsoby:

Licenční klíč

Unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.

ESET Business Account

Tuto možnost použijte, pokud máte založen účet na portále ESET Business Account a přidali jste do něj licenci na ESET Server Security. Zadat můžete také přihlašovací údaje Bezpečnostního administrátora z portálu ESET License Administrator .

Offline licenční soubor

Automaticky generovaný soubor obsahující informace o licenci. Offline licenční soubor si můžete vygenerovat na licenčním portále a použít jej pro aktivaci stanic, které nejsou připojeny k internetu - nedokáží se spojit s licenční autoritou.

Možnost **Aktivovat později** použijte v případě, že je váš počítač součástí spravované sítě a váš správce provede vzdálenou aktivaci prostřednictvím ESET PROTECT. Tuto možnost můžete použít také v případě, kdy chcete klienta aktivovat později jiným způsobem.

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

Po úspěšné aktivaci se otevře hlavní okno produktu ESET Server Security a na záložce Přehled se zobrazí aktuální stav. V některých případech může být vyžadována interakce z vaší strany, například zapojení do systému ESET LiveGrid®.

V hlavním okně programu se dále zobrazují oznámení z jednotlivých součástí produktu, například informace o dostupnosti aktualizací operačního systému Windows nebo zastaralého detekčního jádra. Po vyřešení všech oznámení se stav ochrany změní na zelenou a zobrazí se informace **Maximální ochrana**.

Produkt můžete aktivovat také v hlavním okně po kliknutí na záložku **Nápověda a podpora** > **Aktivovat licenci** nebo **Stav ochrany** > **Aktivovat licenci**.

Prostřednictvím ESET PROTECT můžete aktivovat produkt vzdáleně a plně automaticky.

ESET Business Account

Prostřednictvím účtu na portále ESET Business Account můžete spravovat více licencí pohodlně z jednoho místa. Pokud ještě účet nemáte, po kliknutí na tlačítko Vytvořit účet budete přesměrováni na stránku, kde si nastavíte přihlašovací údaje ke vašemu účtu na portále ESET Business Account.

Další informace najdete v online nápovědě k ESET Business Account.

Pokud jste používali účet Bezpečnostního administrátora na portále ESET Licence Administrator a zapomněli jste heslo ke svému účtu, klikněte na možnost **Zapomněl jsem heslo**. Následně budete přesměrováni na portál ESET License Administrator. Na portále zadejte svoji e-mailovou adresu a potvrďte kliknutím na tlačítko Odeslat. Na e-mail následně obdržíte instrukce pro reset hesla.

Úspěšná aktivace

Aktivace byla úspěšná a ESET Server Security je nyní aktivován. Odteď bude ESET Server Security pravidelně stahovat aktualizace o nejnovějších hrozbách pro zajištění maximální úrovně ochrany počítače. Pro pokračování klikněte na tlačítko **Dokončit**.

Neúspěšná aktivace

Produkt ESET Server Security se nepodařilo aktivovat. Ujistěte se, že jste správně zadali **Licenční klíč** nebo použili platný **Offline licenční soubor**. Pokud máte jiný **offline licenční soubor**, použijte jej. Pro ověření zadaného licenčního klíče klikněte na tlačítko **zkontrolovat licenční klíč**, případně **použijte jinou licenci**.

Pokud se vám produkt přesto nepodaří aktivovat, využijte našeho průvodce řešením problémů souvisejícím s neúspěšnou aktivací.

Licence

Ze seznamu dostupných licencí vyberte tu, kterou chcete použít pro aktivaci produktu ESET Server Security. Kliknutím na tlačítko **Pokračovat** přejdete k aktivaci.

Aktualizace na nejnovější verzi

Nové verze produktu ESET Server Security opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů. Dostupné možnosti:

Odinstalace/instalace

Odebrání starší verze před instalací nové. Z webových stránek společnosti ESET si stáhněte nejnovější verzi ESET Server Security. Pokud potřebujete zachovat konfiguraci produktu ESET Server Security, ze stávající instalace si exportujte nastavení. ESET Server Security odinstalujete a restartujete server. Prostřednictvím staženého instalačního balíčku provedete čistou instalaci. Naimportujete nastavení do nové instalace produktu. Tento scénář doporučujeme v prostředí, kdy ESET Server Security provozujete na jednom serveru.

Místní

Způsob, kdy nainstalujete novou verzi produktu ESET Server Security přes již existující instalaci.

Před zahájením aktualizace se ujistěte, že máte nainstalovány všechny aktualizace operačního systému (nejsou k dispozici žádné k instalaci) a není vyžadován restart (ať již důvodu aktualizací OS, instalace jiné aplikace, atp.). Pokud provedete in-place upgrade navzdory čekajícím aktualizacím Windows nebo vyžadovanému restartu serveru, nemusí dojít ke korektnímu odebrání existující instalace ESET Server Security. Se stejnými potížemi se můžete setkat také při pokusu o manuální odebrání staré verze ESET Server Security.

Po provedení aktualizace ESET Server Security bude vyžadován restart serveru.

Vzdálená

Ve velkých sítích spravovaných prostřednictvím ESET PROTECT. Jedná se v podstatě o čistý upgrade, pouze je spouštěn vzdáleně. Tento postup je vhodný v případě, kdy provozujete ESET Server Security na více serverech.

Průvodce konfigurací ESET Cluster

Aktualizaci na novou verzi můžete provést také prostřednictvím ESET clusteru. Tento způsob doporučujeme, pokud ESET Server Security provozujete na dvou a více serverech. Jedná se v podstatě o in-place upgrade, ale provádí jej ESET Cluster. Po dokončení aktualizace můžete dále využívat ESET Cluster se všemi jeho výhodami.

Po dokončení aktualizace produktu ESET Server Security doporučujeme projít veškerá nastavení a zkontrolovat, zda odpovídá vašim představám.

Aktualizace prostřednictvím ESET PROTECT

ESET PROTECT umožňuje aktualizovat více serverů se starší verzí ESET Server Security. Předností této metody je provedení aktualizace ESET Server Security na velkém množství serverů zároveň při současném sjednocení konfigurace (pokud je to žádoucí).

Vzdálená aktualizace se skládá z těchto kroků:

- Nejprve **ručně aktualizujte jeden server**. Stáhněte si z webových stránek společnosti ESET nejnovější verzi a nainstalujte ji přes stávající. V průběhu instalace nové verze dojde k zachování stávající konfigurace produktu ESET Server Security (včetně pravidel, seznamu povolených či blokovaných adres/odesílatelů, atp. Tento krok provádíte lokálně na serveru, kde je ESET Server Security nainstalován.

- **Vyžádejte si konfiguraci** z nové verze ESET Server Security a převeďte ji do ESET PROTECT politiky. Tuto politiku později aplikujete na všechny aktualizované servery. Tento a následující kroky provedete již z ESET PROTECT.

- Na ostatních serverech odinstalujte ESET Server Security prostřednictvím klientské úlohy na **odinstalaci aplikace**.

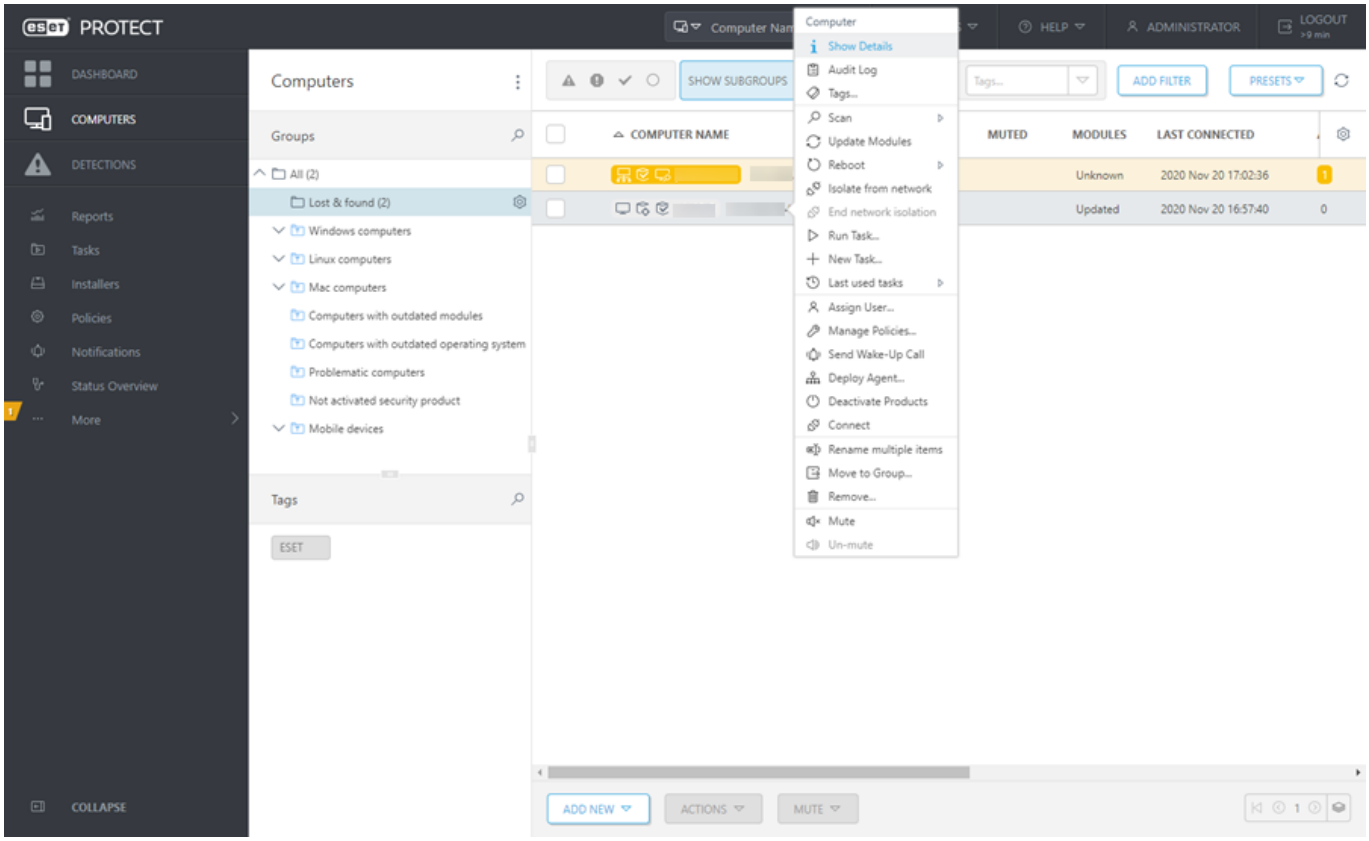
- Prostřednictvím klientské úlohy na **instalaci aplikaci** nainstalujte nejnovější verzi ESET Server Security na ostatní servery.

- Aktualizovaným serverům **přiřaďte politiku**, kterou jste vytvořili z aktualizovaného produktu ESET Server Security.

Krok za krokem:

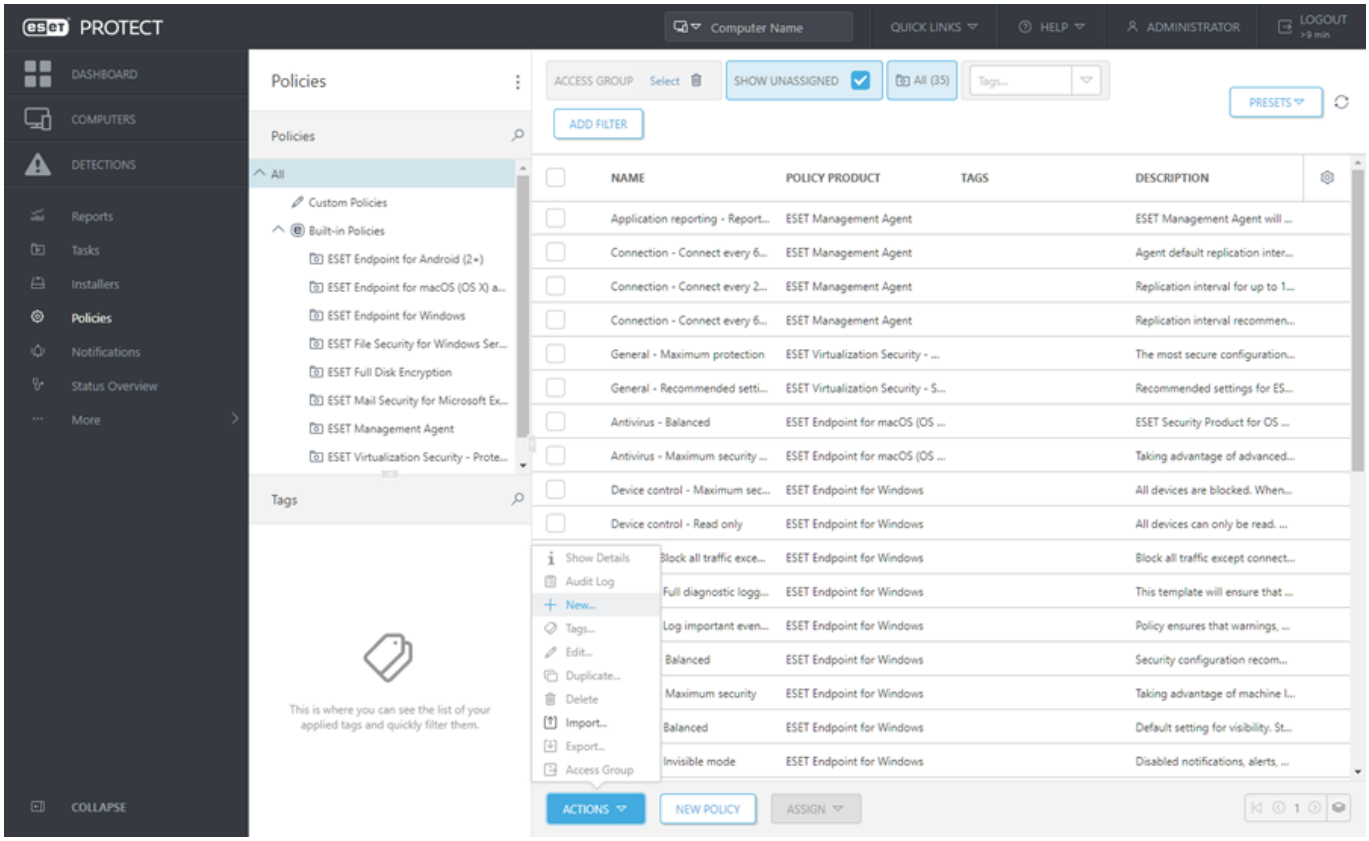
1. Přihlaste se na jeden ze serverů, na kterém běží ESET Server Security. Stáhněte si instalační balíček nové verze produktu z webových stránek společnosti ESET a proveďte aktualizaci ručně jeho spuštěním. Postupujte podle kroků platných pro typickou instalaci. V průběhu aktualizace produktu ESET Server Security bude zachována stávající konfigurace. V průběhu aktualizace produktu ESET Server Security bude zachována stávající konfigurace.

2. Přihlaste se do ESET PROTECTWeb Console a najděte aktualizovaný server. Klikněte na něj pravým tlačítkem myši a z kontextového menu vyberte možnost **Zobrazit detaily.**



3. V zobrazeném okně přejděte na záložku Konfigurace a klikněte na tlačítko **Vyžádat konfiguraci** pro získání konfigurace ze všech spravovaných produktů. Konfigurace by měla být dostupná do dvou intervalů replikace (připojení agenta k serveru). V seznamu konfigurací klikněte na položku **Bezpečnostní produkt** a z kontextového menu vyberte možnost **Otevřít konfiguraci**.

4. V zobrazeném okně klikněte na tlačítko **Převést do politiky**. Zadejte **název** nové politiky a klikněte na tlačítko **Dokončit**.



5. Přejděte do sekce **Klientské úlohy** a vytvořte úlohu pro Odinstalaci aplikace. Po odinstalování aplikace doporučujeme restartovat server. Můžete to provést automaticky tím, že zaškrtnete možnost **Automaticky restartovat, když je potřeba**. Po vytvoření úlohy vyberte cíle, ze kterých chcete produkt odinstalovat.

6. Ujistěte se, že se ESET Server Security skutečně odinstaloval.

7. Vytvořte klientskou úlohu na instalaci aplikace a na požadované cíle nainstalujte nejnovější verzi ESET Server Security.

8. Vytvořenou politiku z kroku 4 **přiřaďte serverům**, na které jste nainstalovali nejnovější verzi ESET Server Security.

Aktualizace prostřednictvím ESET clusteru

Prostřednictvím ESET Clusteru můžete aktualizovat více serverů, na kterých je nainstalována starší verze ESET Server Security. Tento způsob představuje alternativu k aktualizaci produktu prostřednictvím ESET PROTECT. Tuto možnost doporučujeme využít v případě, kdy máte ve svém prostředí nainstalován ESET Server Security na dvou a více serverech.

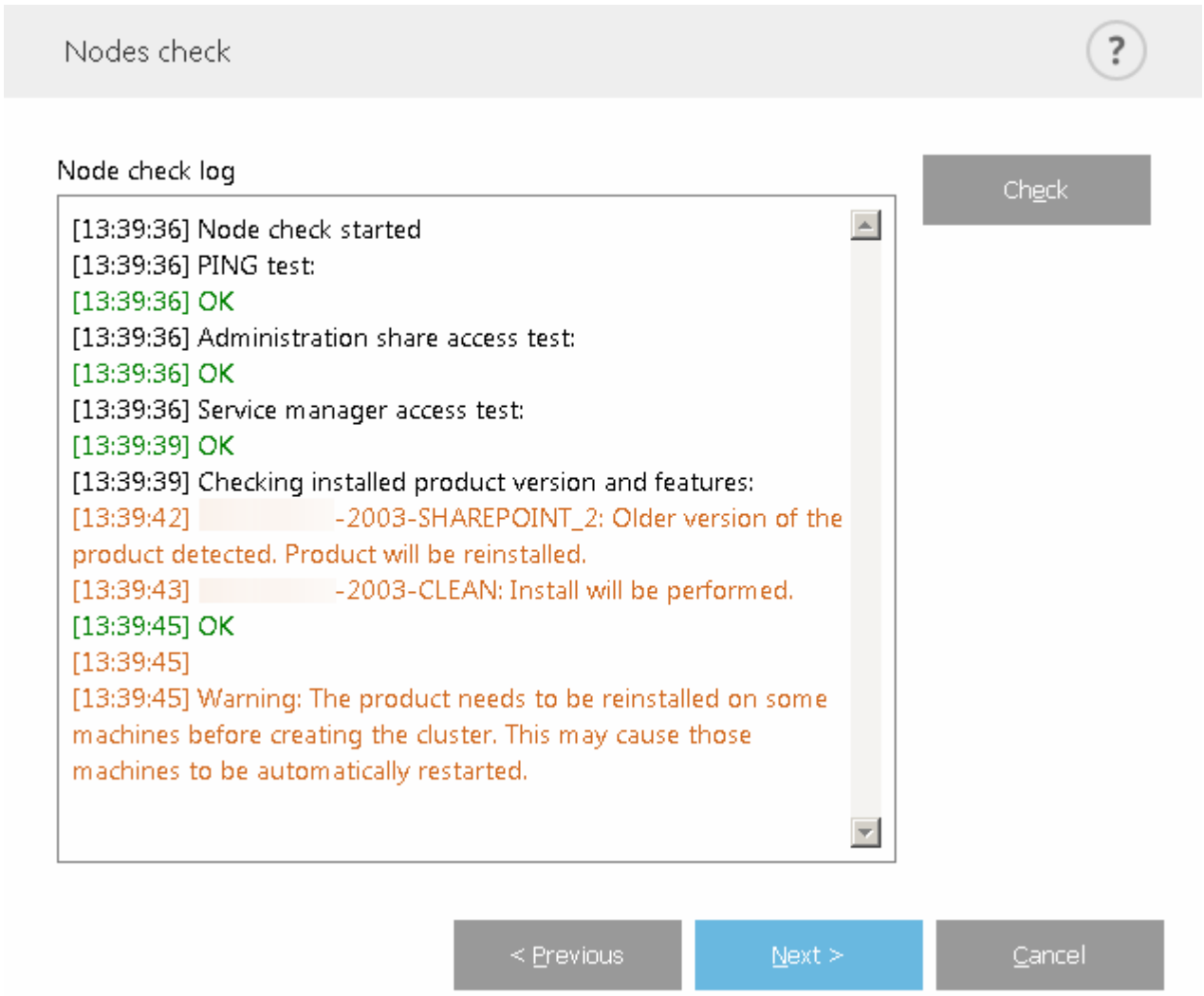
Při aktualizaci prostřednictvím průvodce ESET clusterem zůstane cluster funkční, jednotlivé uzly clusteru si stále budou vyměňovat data a synchronizovat nastavení produktu ESET Server Security.

Pro aktualizaci postupujte podle níže uvedených kroků:

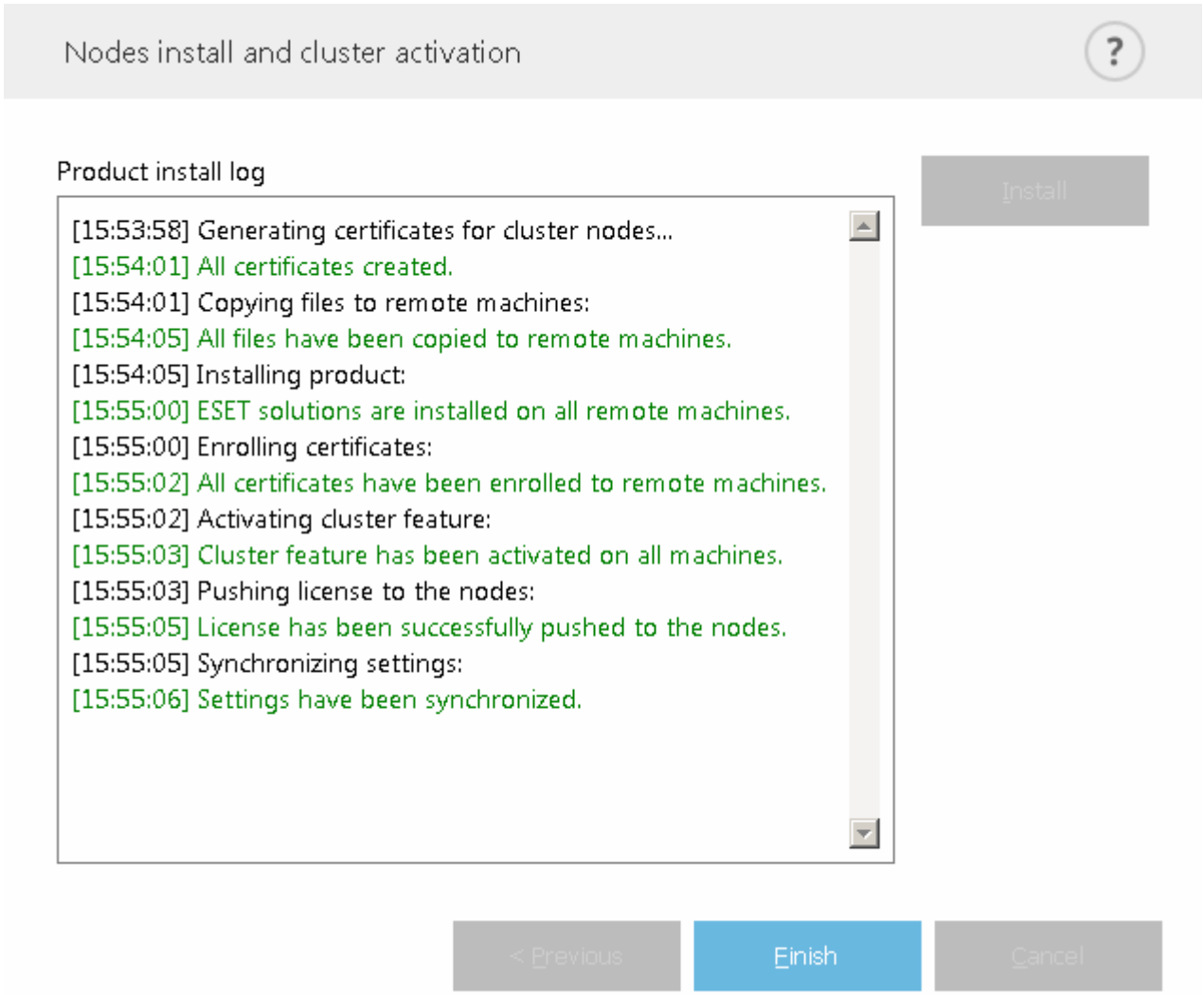
1. Přihlaste se na jeden ze serverů, na kterém běží ESET Server Security a je členem ESET Clusteru. Stáhněte si instalační balíček nové verze produktu z webových stránek společnosti ESET a proveďte aktualizaci ručně jeho spuštěním. Postupujte podle kroků platných pro typickou instalaci. V průběhu aktualizace produktu ESET Server Security bude zachována stávající konfigurace.

2. Otevřete si průvodce ESET Clusterem a přidejte uzly clusteru, na kterých chcete ESET Server Security aktualizovat na novou verzi. V případě potřeby můžete také přidat servery, na kterých dosud není ESET Server Security nainstalován. Další možnosti (název clusteru a způsob instalace) ponechte beze změny a ujistěte se, že je vybrána možnost **Odeslat licenci na uzly s neaktivovaným produktem**.

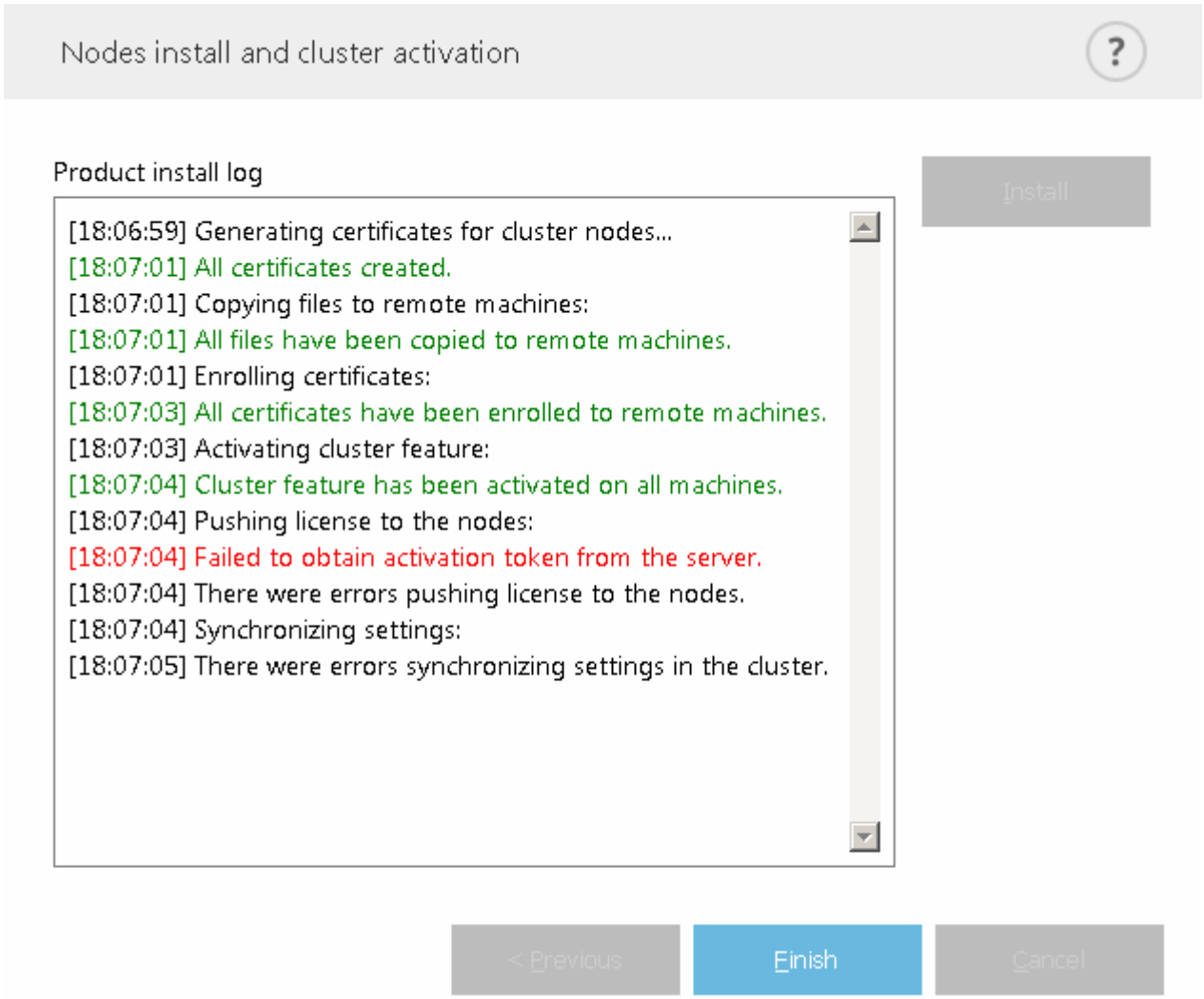
3. V dalším kroku se provede **kontrola uzlů** a zobrazí se její výsledek Servery se staršími verzemi produktů jsou uvedeny a označeny jako pro aktualizaci (přeinstalaci). ESET Server Security se nainstaluje také na další přidané servery, na kterých ESET Server Security chybí.



4. Průběh instalace se zobrazí na obrazovce **Instalace uzlů a aktivace clusteru**. Po úspěšném dokončení instalace by se měl zobrazit výsledek podobný tomu na obrázku:



Pokud nemáte správně nakonfigurovanou síť nebo máte chybně nastaveny DNS záznamy, může se po provedení aktualizace zobrazit chyba: **Nepodařilo se získat aktivační token ze serveru**. V takovém případě spusťte znovu průvodce vytvořením ESET Clusteru. Prostřednictvím něj zničíte stávající cluster a vytvoříte nový bez nutnosti provádět opravnou instalaci produktu. Následně by se měl produkt úspěšně aktivovat. V případě přetrvávajících potíží zkontrolujte konfiguraci sítě a nastavení DNS.



Instalace v clusteru

ESET Server Security můžete provozovat také v prostředí clusteru, například na failover clusteru. V tomto případě doporučujeme ESET Server Security nejprve nainstalovat na aktivní uzel clusteru a následně z produktu provést instalaci na ostatní/pasivní uzly prostřednictvím funkce ESET Cluster.

Kromě samotné instalace ESET Cluster zajistí synchronizaci nastavení ESET Server Security na jednotlivých uzlech clusteru, což je potřeba pro správný běh v prostředí clusteru.

Terminálový server

Pokud instalujete ESET Server Security na Windows server, který zároveň slouží jako Terminálový server, můžete vypnout zobrazení grafického rozhraní ESET Server Security, čím zabráníte jeho spouštění při každém přihlášení uživatele. Návod, jak deaktivovat grafické rozhraní, naleznete v kapitole Deaktivace grafického rozhraní na terminálovém serveru.

Aktualizace zajišťující bezpečnost a stabilitu

Pravidelná aktualizace produktu ESET Server Security je důležitá pro zajištění komplexní ochrany před škodlivým kódem. Každá nová verze produktu ESET Server Security obsahuje opravy chyb a vylepšení funkcí. Abyste zajistili ochranu před hrozbami a eliminovali možnost zneužití bezpečnostních zranitelností, důrazně vám doporučujeme ESET Server Security pravidelně aktualizovat.

Stejně jako u jiných produktů ESET, i ESET Server Security má svůj životní cyklus. Doporučujeme se seznámit s životním cyklem firemních produktů.

Pro více informací týkajících se změny v produktu ESET Server Security přejděte do Databáze znalostí.

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

Začínáme

Následující kapitoly vám pomohou v prvotním používání ESET Server Security.

Přehled

V této části jsou zobrazeny informace o aktuálním stavu ESET Server Security a zabezpečení serveru. Ihned na první dobrou zde zjistíte, zda produkt nevyžaduje vaši pozornost.

Správa prostřednictvím ESET PROTECT

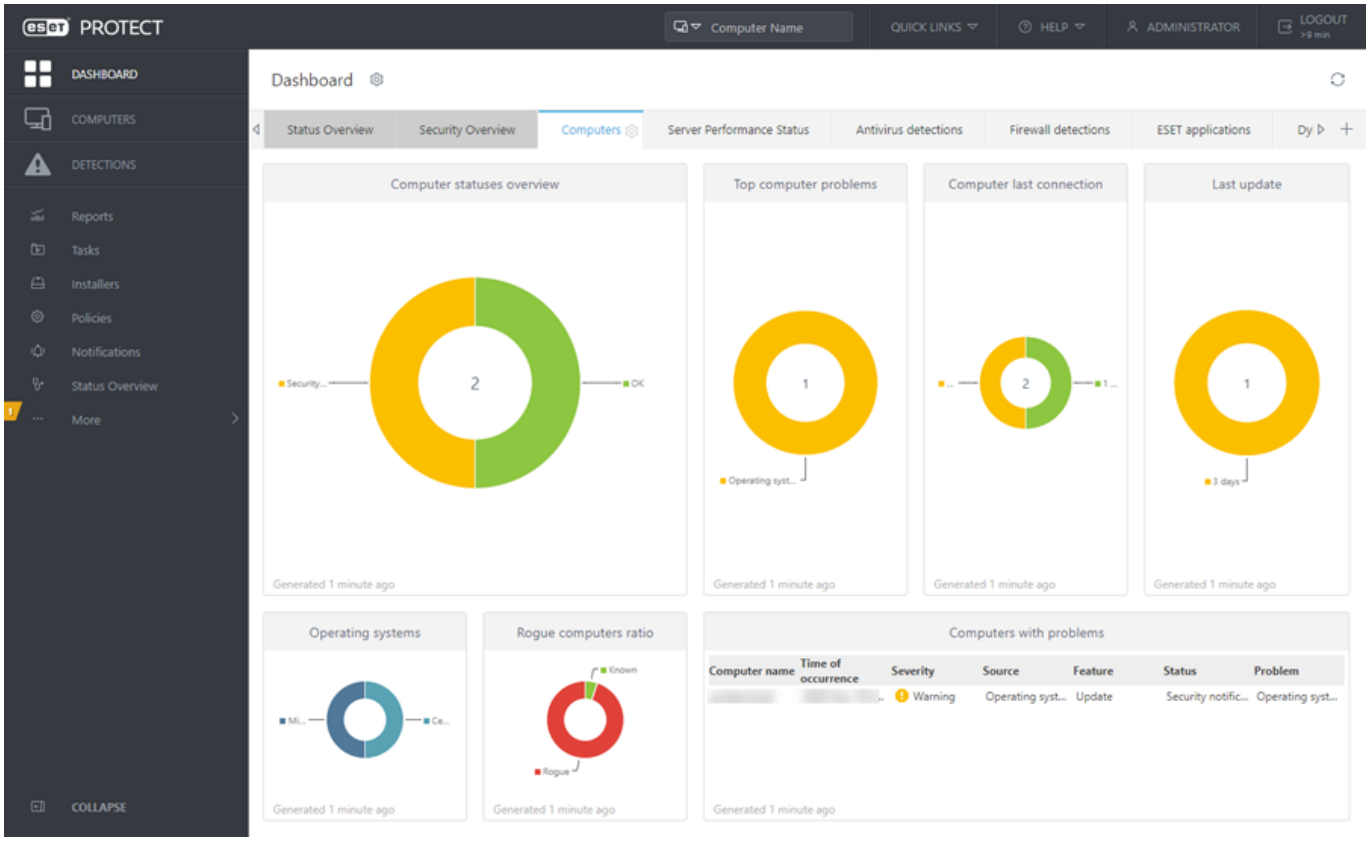
ESET PROTECT můžete vzdáleně spravovat prostřednictvím ESET Server Security.

Správa prostřednictvím ESET PROTECT

ESET PROTECT je aplikace, prostřednictvím které můžete spravovat produkty ESET na stanicích, serverech i mobilních zařízeních z jednoho centrálního místa v síti. Systém správy úloh ESET PROTECT umožňuje instalovat bezpečnostní řešení ESET na vzdálené počítače a rychle reagovat na nové problémy a hrozby.

ESET PROTECT neposkytuje ochranu proti škodlivému kódu sám o sobě, ale spoléhá se na přítomnost bezpečnostních řešení ESET na každém klientovi.

Bezpečnostní řešení ESET je možné nasadit je v kombinovaném síťovém prostředí. Produkty ESET jsou dostupné nejen pro operační systém Windows, ale také na Linux a macOS, stejně tak pro mobilní zařízení (smartphony a tablety).



Další informace o ESET PROTECT naleznete v online nápovědě k ESET PROTECT.

Přehled

Na záložce **Přehled** jsou zobrazeny informace o aktuálním stavu ochrany vašeho serveru. Dále jsou zde uvedeny souhrnné informace o činnosti produktu ESET Server Security.

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

Červená barva stavu ochrany, symbol "!" a informace Není zajištěna maximální ochrana signalizuje kritické problémy. Seznam možných stavů ochrany naleznete v kapitole Stavy ochrany.

Žlutá barva stavu ochrany, symbol "i" a informace ESET vyžaduje vaši pozornost nepředstavuje kritický problém.



Pokud všechny moduly pracují správně, stav ochrany je zelený. V případě, že některý z modulů není plně funkční, zobrazí se červený nebo oranžový vykřičník. V horní části okna jsou následně uvedeny detailními informace.

Společně s nimi se zobrazí návrh na možné řešení problému pro obnovení maximální ochrany. Stav jednotlivých modulů můžete změnit na záložce Nastavení pomocí odpovídajících přepínačů.

V dolní části okna se zobrazují základní informace o produktu a serveru:

- **Verze produktu** – číslo verze ESET Server Security.
- **Název serveru** – FQDN nebo název stroje.
- **Systém** – podrobnosti o operačním systému.
- **Počítač** – informace o hardwaru.
- **Doba od spuštění** – informace o době běhu operačního systému od posledního startu.

Pokud uvedený návrh na řešení problému nezabral, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zkuste prohledat nápovědu nebo ESET Databázi znalostí. Pokud i přesto budete potřebovat pomoc, můžete založit požadavek na technickou podporu. Specialisté technické podpory ESET vám odpoví v co nejkratším možném čase, a pomohou vám s řešením problému.

Stav

V hlavním okně programu ESET Server Security se na záložce Přehled zobrazují detailní informace o operačním systému a jeho ochraně. Za normálních okolností je ikona stavu ochrany zelená (). Stav ochrany se však v závislosti na okolnostech může změnit. Může být oranžový () nebo dokonce červený (). Společně se změnou stavu ochrany se zobrazí chybová zpráva. Níže uvádíme nejčastější z nich:

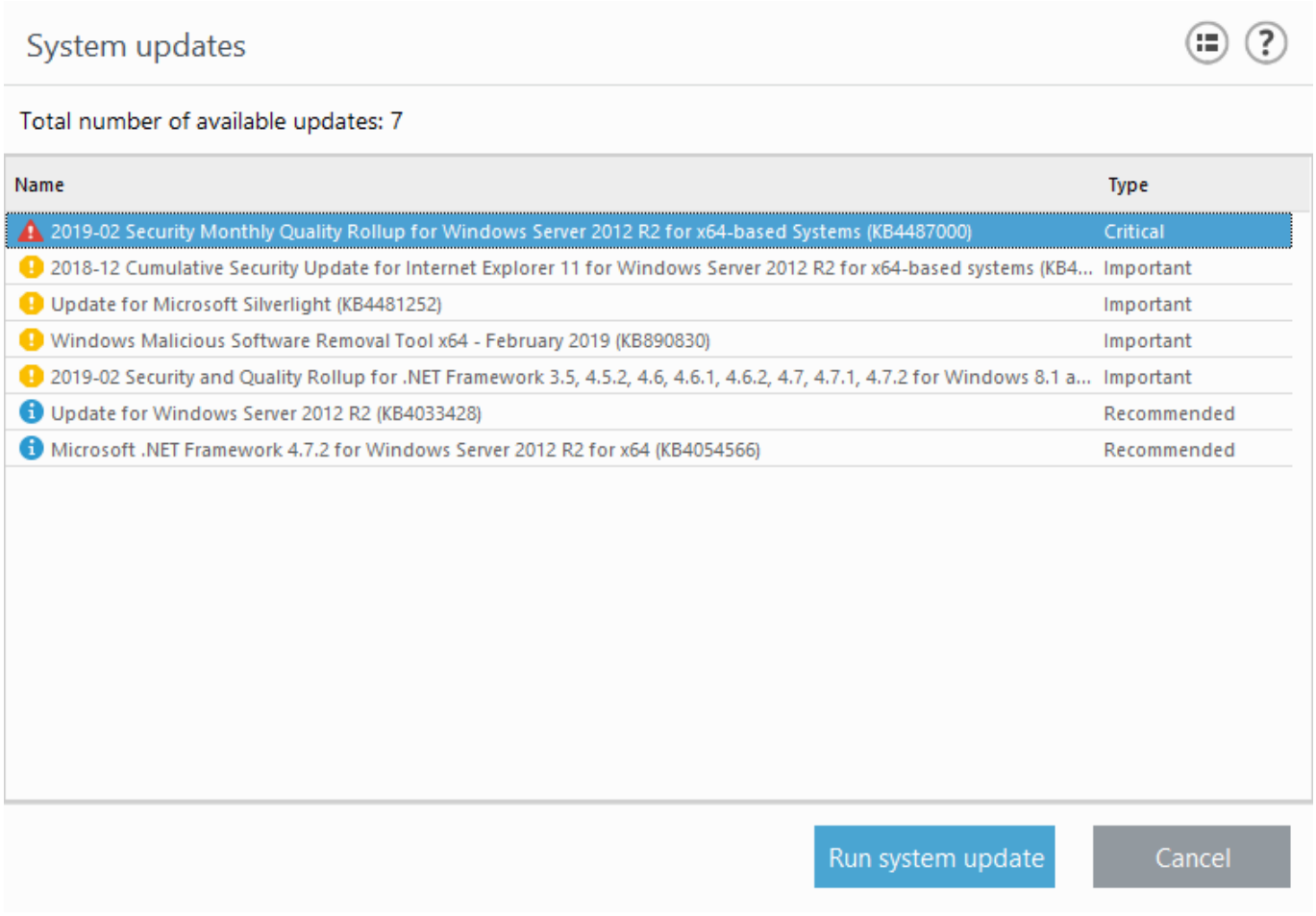
Chybová zpráva	Detailní informace
Detekce potenciálně nechtěných aplikací není nastavena	Potenciálně nechtěné aplikace (PUA) jsou programy, které obsahují adware, instalují do systému toolbary nebo mají záměr, který není na první pohled znám. Existují však situace, kdy mohou benefity potenciálně nechtěné aplikace převážit potenciální riziko.
Rezidentní ochrana souborového systému je dočasně vypnutá	Znovu zapnout ji můžete na záložce Přehled kliknutím na možnost Zapnout rezidentní ochranu, případně na záložce Nastavení pomocí přepínače **Rezidentní ochrana souborového systému**.
Anti-Phishingová ochrana není funkční	Tato funkce neběží, protože vyžaduje další moduly programu, které však nejsou aktivní.
ESET LiveGrid® je vypnutý	Informace, že máte v **rozšířeném nastavení** vypnutou technologii ESET LiveGrid®.
Filtrování protokolů je vypnuté	Pro zapnutí klikněte na možnost Zapnout filtrování protokolů.
Operační systém není aktuální	V tomto dialogovém okně naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat.
Ochrana vašeho zařízení brzy skončí	Pro zobrazení detailních informací týkajících se aktualizace vámi používaného operačního systému Microsoft Windows klikněte na možnost Jaké mám možnosti. Pokud používáte Microsoft Windows Server 2008 R2 SP1 nebo Microsoft Windows Small Business Server 2011 SP1, ujistěte se, že je kompatibilní s SHA-2. V závislosti na systému doinstalujte odpovídající aktualizace.
Prezentační režim je zapnutý	Je potlačeno zobrazování pop-up oken a jsou pozastaveny naplánované úlohy.
Ochrana proti síťovým útokům (IDS) je pozastavena	Pro její zapnutí klikněte na možnost Zapnout ochranu proti síťovým útokům (IDS)
Ochrana proti zapojení do botnetu je pozastavena	Pro její zapnutí klikněte na možnost Zapnout ochranu proti zapojení do botnetu
Ochrana přístupu na web je dočasně vypnutá	Znovu zapnout ji můžete na záložce **Přehled** kliknutím na možnost Zapnout ochranu přístupu na web, případně na záložce Nastavení pomocí přepínače **Ochrana přístupu na web**.
Správa zařízení je dočasně vypnutá	Pro zapnutí klikněte na možnost Zapnout Správu zařízení.
Produkt není aktivován nebo Platnost licence vypršela	V tomto případě je ikona stavu ochrany červená. Produkt se není schopen po vypršení licence aktualizovat. Postupujte podle kroků na obrazovce pro prodloužení licence nebo aktivaci produktu novou licencí.
Dočasná změna nastavení je aktivní	Je možné dočasně konfigurovat nastavení, které je jinak striktně vynucené politikou, typicky za účelem řešení problému. Pokud ESET Server Security spravujete prostřednictvím ESET PROTECT a máte k němu přiřazenou politiku, bude stavový odkaz uzamčen (zašedlý) v závislosti na tom, jaké funkce patří k dané politice.

Chybová zpráva	Detailní informace
Vyžadován restart zařízení	Pro okamžité restartování systému klikněte na **Restartovat zařízení**, případně **Zamítnout** pro restartování později. Tato zpráva se zobrazí po nainstalování aktualizace programových komponent (PCU), resp. mikro aktualizace programových komponent (µPCU). Více informací o PCU a µPCU naleznete v kapitole Nastavení aktualizace.

Pokud uvedený návrh na řešení problému nezabral, zkuste prohledat ESET Databázi znalostí. Pokud i přesto budete potřebovat pomoc, můžete založit požadavek na technickou podporu. Specialisté technické podpory ESET vám odpoví v co nejkratším možném čase, a pomohou vám s řešením problému.

Jsou dostupné aktualizace Windows

V tomto dialogovém okně naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Vedle názvu aktualizace se zobrazuje její priorita. Po kliknutí pravým tlačítkem myši na danou aktualizaci a vybrání možnosti **Více informací** se zobrazí podrobné informace o aktualizaci:



Pro zobrazení dialogového okna **Windows Update** klikněte na tlačítko **Spustit aktualizaci systému**.

Izolace od sítě

Pod názvem Izolace od sítě nabízí ESET Server Security funkci pro zablokování síťové komunikace vašeho serveru. Izolování serveru od sítě můžete v extrémních scénářích využít jako preventivní opatření. Například v případě infikování serveru škodlivým kódem nebo po jeho kompromitování.

Po izolaci od sítě bude blokována veškerá síťová komunikace, kromě:

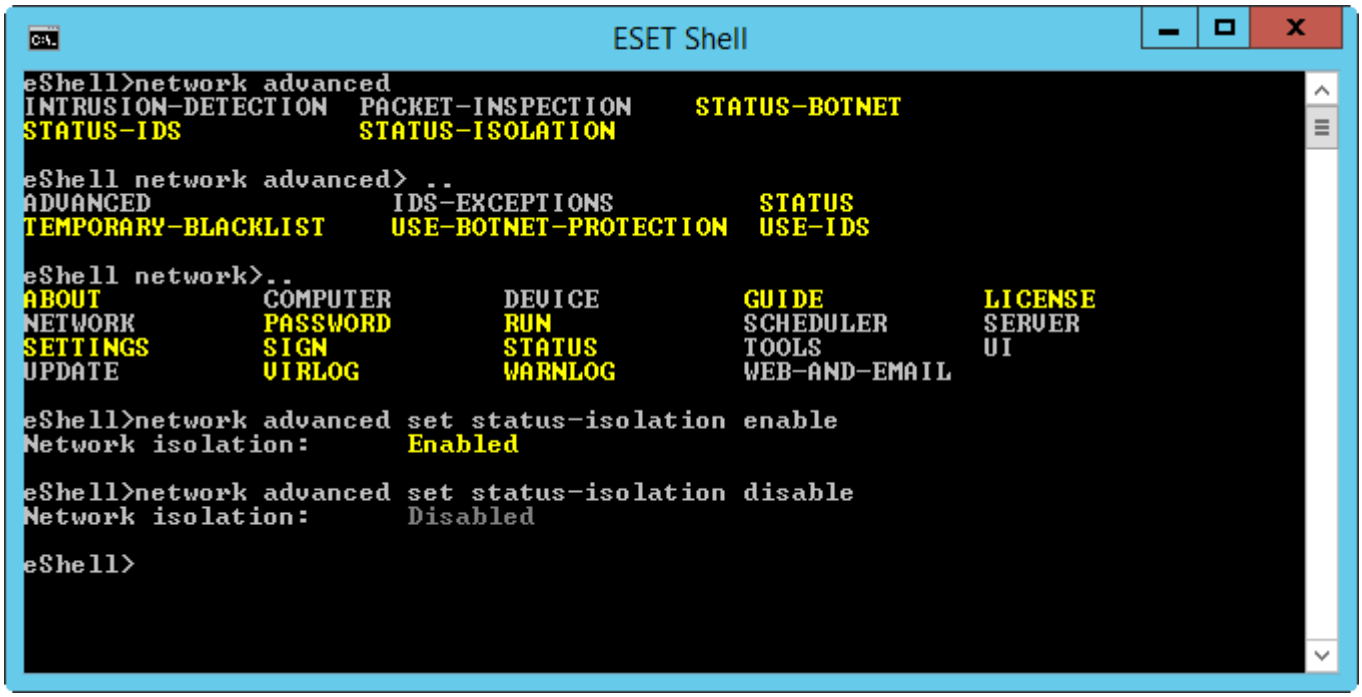
- Spojení s doménovým řadičem
- Komunikace produktu ESET Server Security
- ESET Management Agent a ESET InspectConnector, pokud je nainstalován

Izolaci od sítě můžete aktivovat nebo deaktivovat pomocí eShell nebo klientskou úlohou v ESET PROTECT.

eShell

V interaktivním režimu:

- Pro izolování použijte příkaz: `network advanced set status-isolation enable`
- Pro ukončení izolace použijte příkaz: `network advanced set status-isolation disable`



Alternativně si můžete vytvořit dávkový soubor a spustit jej v režimu skriptování.

ESET PROTECT

- Aktivujte izolaci sítě prostřednictvím klientské úlohy.
- Ukončení izolace od sítě prostřednictvím klientské úlohy.

Po izolování serveru od sítě se změní stav produktu ESET Server Security na červený a zobrazí se hlášení **Přístup k síti byl zablokován**.

Práce s ESET Server Security

V této části naleznete detailní popis uživatelského rozhraní a seznámíme vás s používáním produktu ESET Server Security.

V hlavním okně programu máte k dispozici následující sekce:

- Přehled
- Protokoly
- Kontrola počítače
- Aktualizace
- Nastavení
- Nástroje

Kontrola počítače

Důležitou součástí ESET Server Security je tzv. volitelná kontrola (On-demand). Prostřednictvím ní můžete individuálně zkontrolovat soubory a složky ve vašem počítači. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infekci soubory, ale v rámci prevence i průběžně.

Hloubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech (například jednou měsíčně), aby byly detekovány případné viry, které v době zápisu na disk nebyly zachyceny rezidentní ochranou. Taková situace může nastat, pokud byla rezidentní ochrana v té době vypnutá, program používal neaktuální detekčních moduly, případně soubor v době zápisu na disk program nebyl vyhodnocen jako hrozba.

V ESET Server Security jsou dostupné následující volitelné kontroly:

Kontrola úložiště

Zkontroluje všechny sdílené složky na lokálním serveru. Pokud není tato možnost dostupná, na serveru nejsou žádné sdílené složky.

Provést kontrolu počítače

Touto možností spustíte rychlou kontrolu počítače, která léčí infikované soubory bez potřeby zásahu uživatele. Výhodou této kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. V průběhu kontroly se zkontrolují všechny soubory na lokálních jednotkách a případně hrozby produkt automaticky vyléčí nebo odstraní. Úroveň léčení je nastavena na standardní úroveň. Pro podrobnější informace týkající se možností léčení si prostudujte kapitolu Léčení.

> Doporučujeme provádět kontrolu počítače alespoň jednou měsíčně. Pro pravidelnou kontrolu můžete využít naplánovanou úlohu.

Volitelná kontrola

Vhodné řešení pro případ, kdy chcete definovat parametry kontroly – profil a cíle – podle svých představ. Výhodou volitelné kontroly je možnost podrobně specifikovat její parametry. Různé konfigurace můžete ukládat jako profily definované uživatelem, které jsou užitečné zejména pokud je potřeba periodicky opakovat kontrolu se stejnými parametry.

Kontrola výměnných médií

Funguje podobně jako možnost Provést kontrolu počítače – spustí rychlou kontrolu výměnných médií (CD/DVD/USB), která jsou aktuálně připojené k počítači. To může být užitečné ve chvíli, kdy si přeje zkontrolovat obsah připojeného USB zařízení k počítači na škodlivý software a další potenciální hrozby. Tuto kontrolu můžete také spustit tak, že při definování Volitelné kontroly kliknete na ozubené kolečko, v rozbalovacím menu Cíle kontroly vyberete možnost Výměnná média a kliknete na tlačítko Zkontrolovat.

Hyper-V kontrola

Tato možnost je dostupná pouze v případě, kdy je na serveru, na kterém běží ESET Server Security, nainstalován Správce technologie Hyper-V. Pomocí této možnosti zkontrolujete disky virtuálních počítačů na Microsoft Hyper-V Serveru bez toho, abyste museli na virtuální počítač instalovat "agenta".

OneDrive kontrola

Zajišťuje kontrolu uživatelských souborů umístěných ve OneDrive cloudovém úložišti.

Opakovat poslední kontrolu

Zopakuje poslední kontrolu se stejným nastavením.

Možnost opakovat poslední kontrolu není dostupná pro volitelnou kontrolu databáze.



K dispozici máte níže uvedené možnosti, které můžete využít pro získání podrobnějších informací o probíhajících kontrolách:

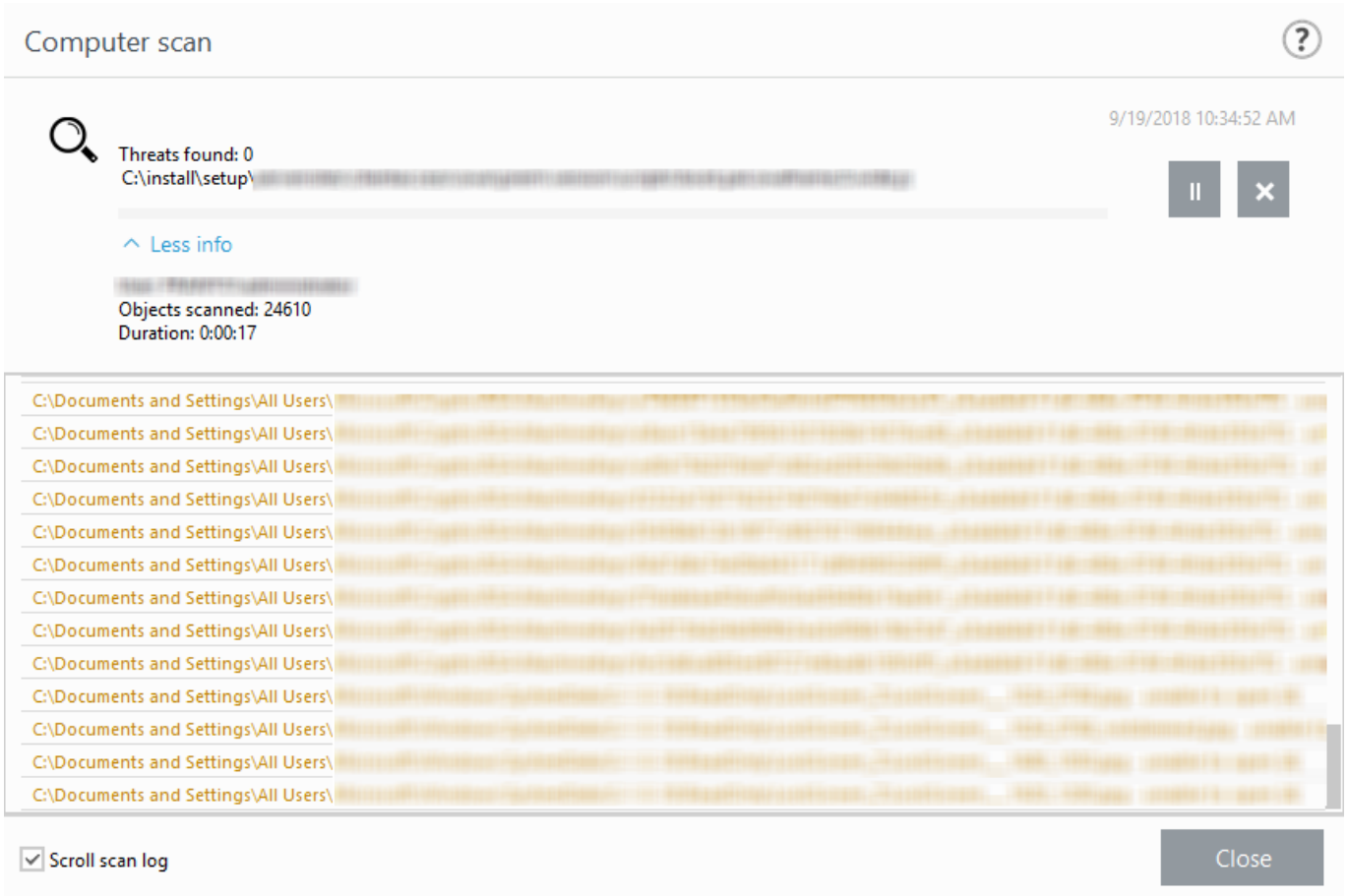
Drag and drop	**Na vyznačené místo v okně ESET Server Security přetáhněte soubory, které chcete zkontrolovat. Po přetažení souborů budou ihned zkontrolovány.**

Drag and drop	Na vyznačené místo v okně ESET Server Security přetáhněte soubory, které chcete zkontrolovat. Po přetažení souborů budou ihned zkontrolovány.
Zavřít/Zavřít vše	Kliknutím zavřete danou zprávu.
Stav kontroly	Zobrazuje informace o probíhající kontrole. Zda byla dokončena nebo přerušena uživatelem.
Zobrazit protokol	Kliknutím zobrazíte detailní informace o kontrole.
Více informací	V průběhu kontroly si můžete kliknutím zobrazit informaci, jaký uživatel kontrolu spustil, počtu kontrolovaných objektů a **době kontroly**.
Otevřít okno kontroly	Okno průběhu kontroly zobrazuje aktuální stav kontroly a počet souborů, které obsahují škodlivý kód.

Okno a protokol kontroly

V horní části dialogového okna protokolu kontroly naleznete informaci o aktuálně kontrolovaném objektu společně s úplnou cestou. Dále je zde uveden počet nalezených hrozeb, celkový počet zkontrolovaných souborů, doba kontroly a uživatel, který kontrolu spustil. V dolní části okna naleznete v protokolu informace o verzi použitého detekčního jádra, datu kontroly a cílech.

Probíhající kontrolu můžete pozastavit pomocí tlačítka **Pozastavit**. Pozastavenou kontrolu obnovíte kliknutím na tlačítko **Pokračovat**.

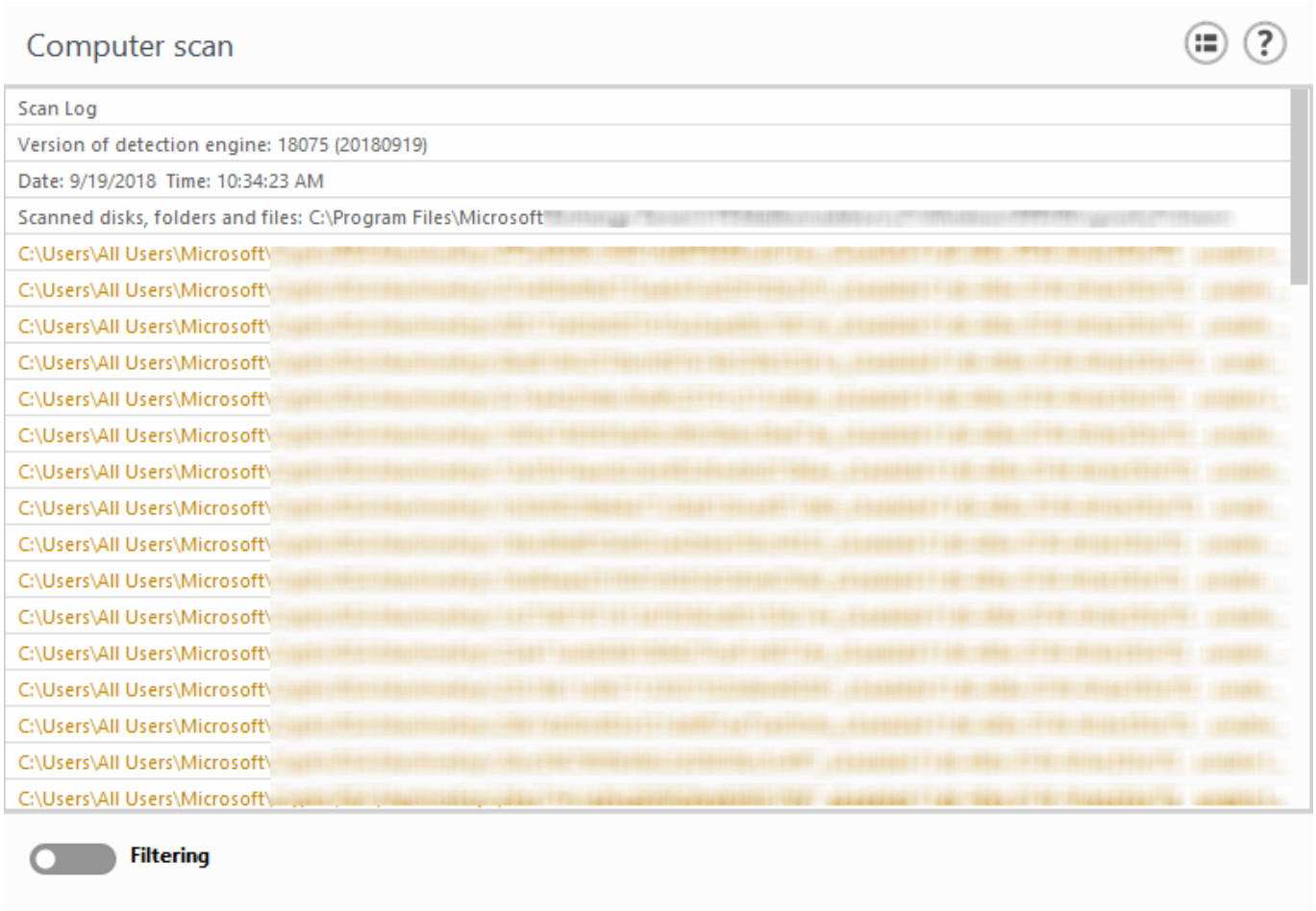


Rolovat výpis protokolu kontroly

Pokud je tato možnost povolena, starší protokoly budou automaticky rolovat a v okně Protokoly se zobrazí pouze ty nejnovější.

Běžně dochází k tomu, že některé soubory nelze skenovat, například soubory chráněné heslem nebo soubory používané výhradně systémem (obvykle *pagefile.sys* a určité protokoly).

Po dokončení kontroly se v protokolu kontroly zobrazí všechny související informace.



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

Akce	Použití	Klávesová zkratka	Více informací
Filtrovat záznamy stejného typu	Po aktivování tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování, …).	Ctrl + Shift + F	
Filtrovat…	Po kliknutí se otevře nové okno Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů.		Filtrování protokolu
Zapnout filtr	Kliknutím aktivujete filtr. Pokud jste dosud žádný filtr nedefinovali, zobrazí se průvodce jeho vytvořením. Při opětovném kliknutí se automaticky aktivuje naposledy použitý filtr.		
Zrušit filtr	Vypne filtrování (stejné jako kdybyste opětovně použili přepínač pro zapnutí filtru).		
Kopírovat	Zkopíruje vybrané záznamy do schránky.	Ctrl + C	
Kopírovat vše	Zkopíruje všechny záznamy z daného okna.		
Exportovat…	Kliknutím uložíte vybrané záznamy do .XML souboru.		

Akce	Použití	Klávesová zkratka	Více informací
Exportovat vše…	Uloží všechny záznamy do .XML formátu.		

Protokoly

Protokoly obsahují informace o všech důležitých událostech programu, které nastaly a poskytují přehled o detekovaných hrozbách. Záznamy v protokolech představují důležitý nástroj pro systémové analýzy, detekci hrozeb a řešení problémů. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové informace a protokoly si můžete prohlédnout i archivovat přímo v prostředí ESET Server Security.

Z rozbalovacího menu si vyberte požadovaný typ protokolu. Dostupné jsou následující typy protokolů:

Detekce

Protokol detekcí poskytuje detailní informace týkající se infiltrací zachycených moduly produktu ESET Server Security. Informace zahrnují čas detekce, název infiltrace, umístění, provedenou činnost a uživatele přihlášeného v době detekce.

Dvojklikem na záznam protokolu otevřete detaily v samostatném okně. V případě potřeby můžete detekční výjimku vytvořit přímo z protokolu – klikněte pravým tlačítkem na záznam (detekci) a z kontextového menu vyberte možnost **Vytvořit výjimku**. Následně se otevře průvodce vytvořením výjimky, ve kterém již budou předdefinována kritéria. Pokud je u vyloučeného souboru uveden i název detekce, znamená to, že v souboru je vyloučena pouze tato detekce. Není však vyloučen soubor jako celek. V případě, že bude později nakažen jiným škodlivým kódem, jeho detekce proběhne.

Události

Protokol obsahuje informace o všech akcích produktu ESET Server Security. Obsahuje informace o událostech a chybách, které se v produktu vyskytly. Tento protokol je navržen tak, aby systémovým administrátorům a uživatelům pomohl při řešení potíží. Informace z tohoto protokolu mohou pomoci najít příčiny problémů, případně jejich řešení.

Kontrola počítače

Protokol kontroly počítače obsahuje výsledky dokončené ruční nebo naplánované kontroly. Každý řádek náleží samostatné kontrole. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.

Blokované soubory

Obsahuje přehled souborů, k nimž byl zablokován přístup. V protokolu je uveden důvod blokace, modul, který přístup k souboru zablokoval, stejně jako uživatel a aplikace, prostřednictvím ní bylo k souboru přistupováno.

Odeslané soubory

Obsahuje přehled souborů zpracovaných cloudovou ochranou (ESET LiveGuard Advanced a ESET LiveGrid®).

Audit log

Obsahuje záznamy o provedených změnách v konfiguraci nebo stavu ochrany a vytváří snapshoty pro pozdější použití. Klikněte pravým tlačítkem myši na libovolný záznam typu Změna nastavení a k zobrazení podrobných

informací o provedené změně vyberte v kontextovém menu položku Zobrazit změny. Pokud se chcete vrátit k předchozímu nastavení, klikněte na položku Obnovit. Pro smazání záznamů použijte možnost Odstranit vše. Pro zapnutí auditování přejděte v Rozšířeném nastavení do sekce Nástroje > Protokoly > Audit log.

HIPS

Protokoly obsahují záznamy konkrétních pravidel, která se mají zaznamenávat. V protokolu je zobrazena aplikace, která danou operaci vyvolala, výsledek (tzn. zda bylo pravidlo povoleno, nebo zakázáno) a název vytvořeného pravidla.

Síťová ochrana

Protokol obsahuje přehled událostí zablokovaných ochranou proti zapojení do botnetu a IDS.

Filtrované webové stránky

Seznam webových stránek zablokovaných ochranou přístupu na web . Protokol obsahuje čas, URL, uživatele a aplikaci, která navázala spojení s danou stránkou.

Správa zařízení

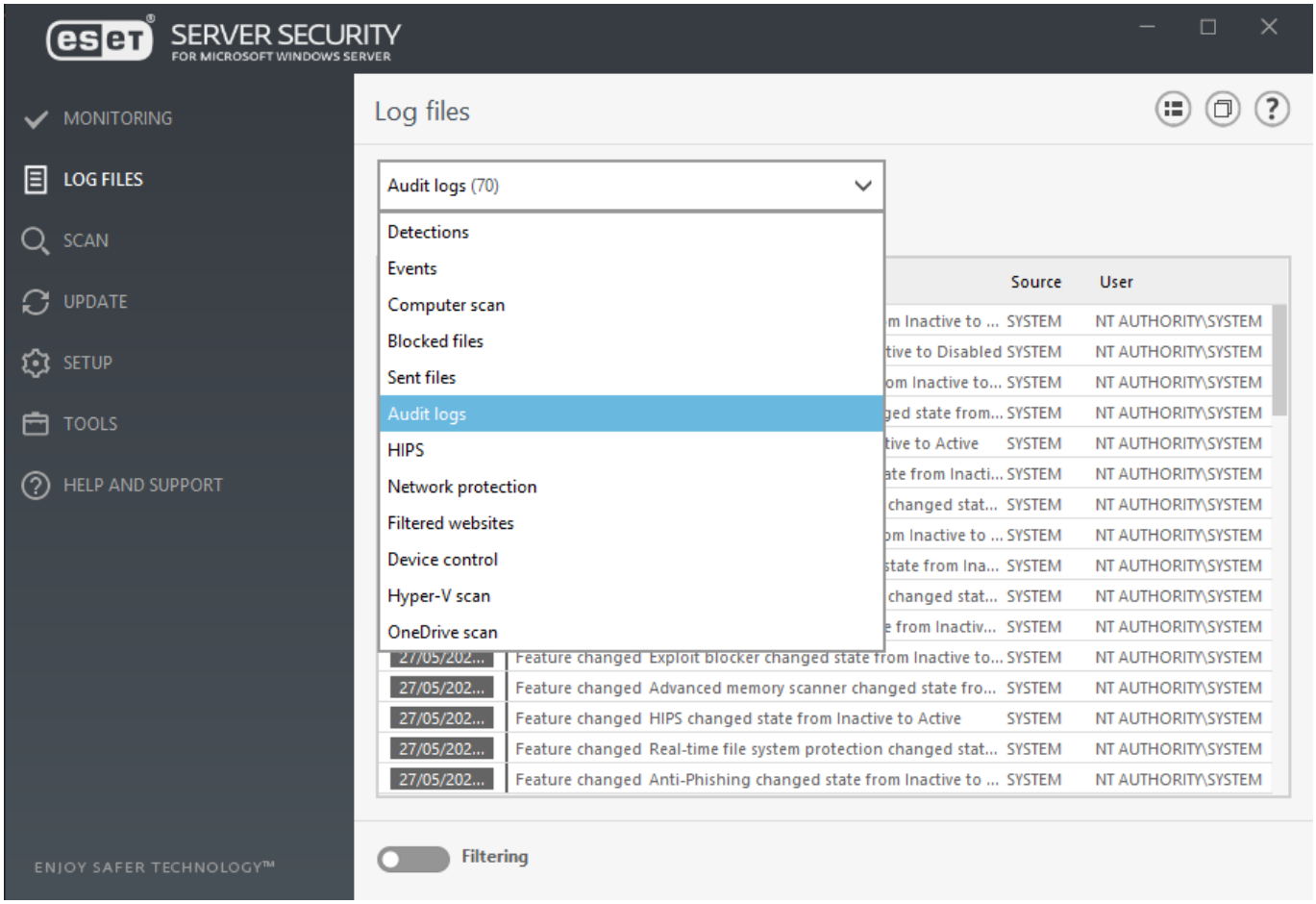
Obsahuje záznamy o výměnných médiích nebo zařízeních připojených k počítači. V protokolu se zobrazí pouze zařízení, na která byla aplikována pravidla Správce zařízení. Pokud nebylo na zařízení aplikováno žádné pravidlo, záznam v protokolu se nevytvoří. Pro každé zařízení se zobrazí také informace o typu zařízení, sériové číslo, název výrobce a velikost média (pokud jsou dostupné).

Hyper-V kontrola

Obsahuje seznam provedených Hyper-V kontrol. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.

OneDrive kontrola

Obsahuje seznam všech provedených OneDrive kontrol.



Prostřednictvím kontextové menu (dostupné po kliknutí pravým tlačítkem) máte dostupné akce nad vybraným záznamem protokolu.

Akce	Použití	Klávesová zkratka	Více informací
Zobrazit	Zobrazí v novém okně všechny záznamy protokolu (případně proveďte dvojklik na daný záznam).		
Filtrovat záznamy stejného typu	Po aktivování tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování, …).	Ctrl + Shift + F	
Filtrovat…	Po kliknutí se otevře nové okno Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů.		Filtrování protokolu
Zapnout filtr	Kliknutím aktivujete filtr. Pokud jste dosud žádný filtr nedefinovali, zobrazí se průvodce jeho vytvořením. Při opětovném kliknutí se automaticky aktivuje naposledy použitý filtr.		
Zrušit filtr	Vypne filtrování (stejné jako kdybyste opětovně použili přepínač pro zapnutí filtru).		
Kopírovat	Zkopíruje vybrané záznamy do schránky.	Ctrl + C	
Kopírovat vše	Zkopíruje všechny záznamy z daného okna.		
Odstranit	Odstraní vybrané záznamy – tato akce vyžaduje oprávnění administrátora.	Del	
Odstranit vše	Odstraní všechny záznamy v daném okně – tato akce vyžaduje oprávnění administrátora.		
Exportovat…	Kliknutím uložíte vybrané záznamy do .XML souboru.		
Exportovat vše…	Po kliknutí uložíte všechny záznamy do .XML formátu.		

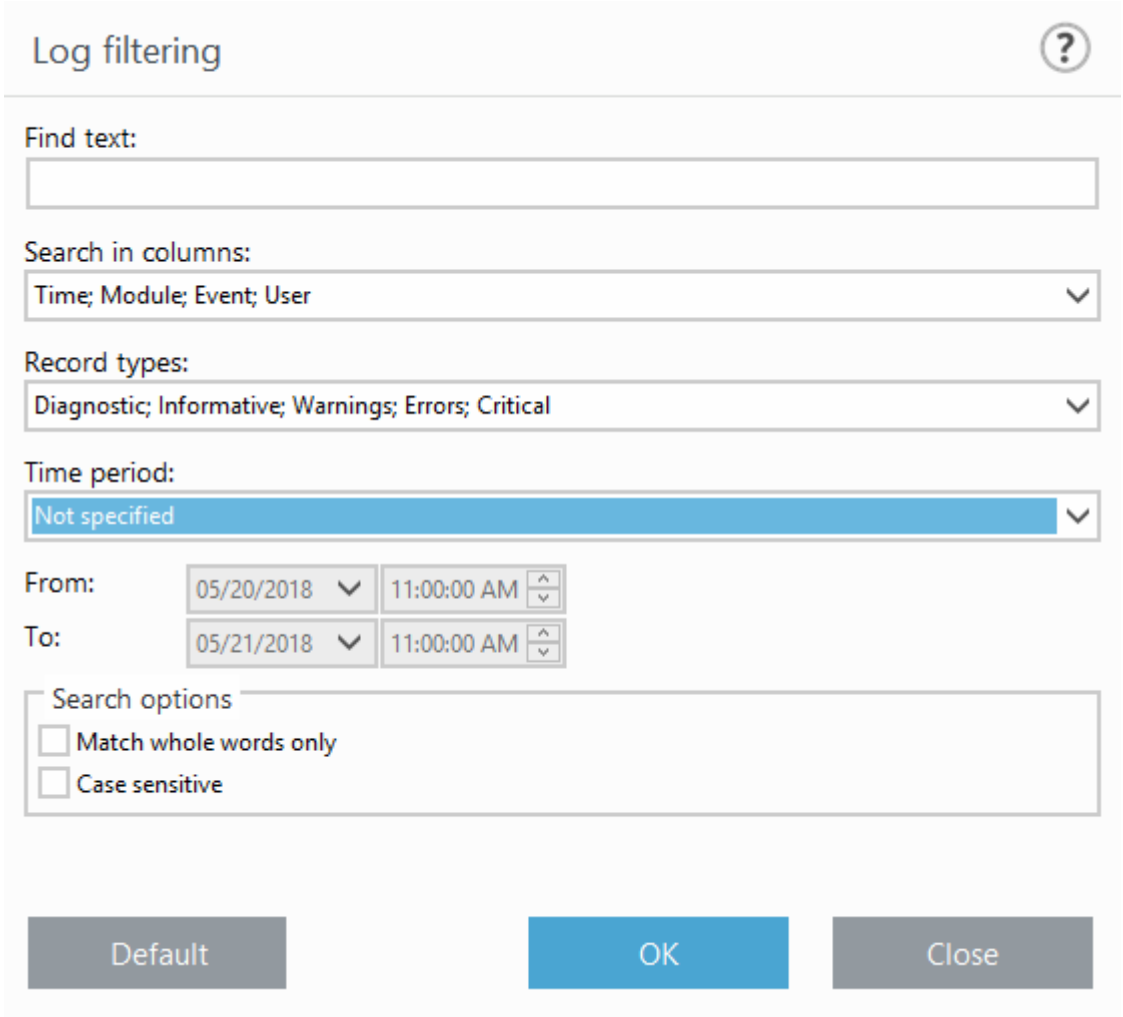
Akce	Použití	Klávesová zkratka	Více informací
Hledat…	Otevře dialogové okno Vyhledávání v protokolu a umožní vám definovat kritéria vyhledávání. Vyhledávat je možné též v již filtrovaných výsledcích, což je užitečné při velkém množství záznamů.	Ctrl + F	Vyhledávání v protokolu
Hledat další	Najde další výskyt hledaného výrazu.	F3	
Hledat předchozí	Najde předchozí výskyt hledaného výrazu.	Shift + F3	
Vytvořit výjimku	Zobrazí průvodce pro vytvoření výjimky na základě názvu detekce, cesty nebo kontrolního součtu.		Vytvoření výjimky

Filtrování protokolu

Protokoly obsahují různé druhy záznamů o důležitých událostech. Prostřednictvím funkce filtrování můžete zobrazit pouze záznamy určitého druhu. Konkrétní záznamy v protokolech můžete najít také prostřednictvím vyhledávání.

To je užitečné v případě, kdy hledáte pouze záznamy určitého druhu, například záznamy, které obsahují určitý řetězec.

Zadejte klíčové slovo do pole **Hledat text:**, které chcete vyhledat. Pokud chcete vyhledávat klíčové slovo pouze v konkrétních sloupcích, změňte filtrování v rozbalovacím menu **Hledat ve sloupcích**. Z rozbalovacího menu si vyberte **typy záznamů**, které chcete zobrazit: Specifikovat můžete také **Časové období**, ve kterém chcete klíčové slovo vyhledat. Pro získání přesných výsledků můžete aktivovat možnost **Hledat pouze celá slova** a **Rozlišovat velká a malá písmena**.



Hledat text

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

Hledat ve sloupcích

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

Typy záznamů

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

- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy.
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy.
- **Varování** – obsahují varovné zprávy a kritické chyby.
- **Chyby** – obsahují chyby typu "Chyba při stahování souboru aktualizace" a kritické chyby.
- **Kritické chyby** – obsahují pouze kritické chyby.

Rozsah času

Definujte časové období, za které chcete zobrazit výsledky:

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

Hledat pouze celá slova

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

Rozlišovat velká a malá písmena

Tuto možnost zapněte, pokud chcete při vyhledávání rozlišovat velikost písmen. Po dokončení konfigurace filtru pro vyhledávání v protokolu klikněte na tlačítko **OK**, případně **Najít** pro zahájení vyhledávání.

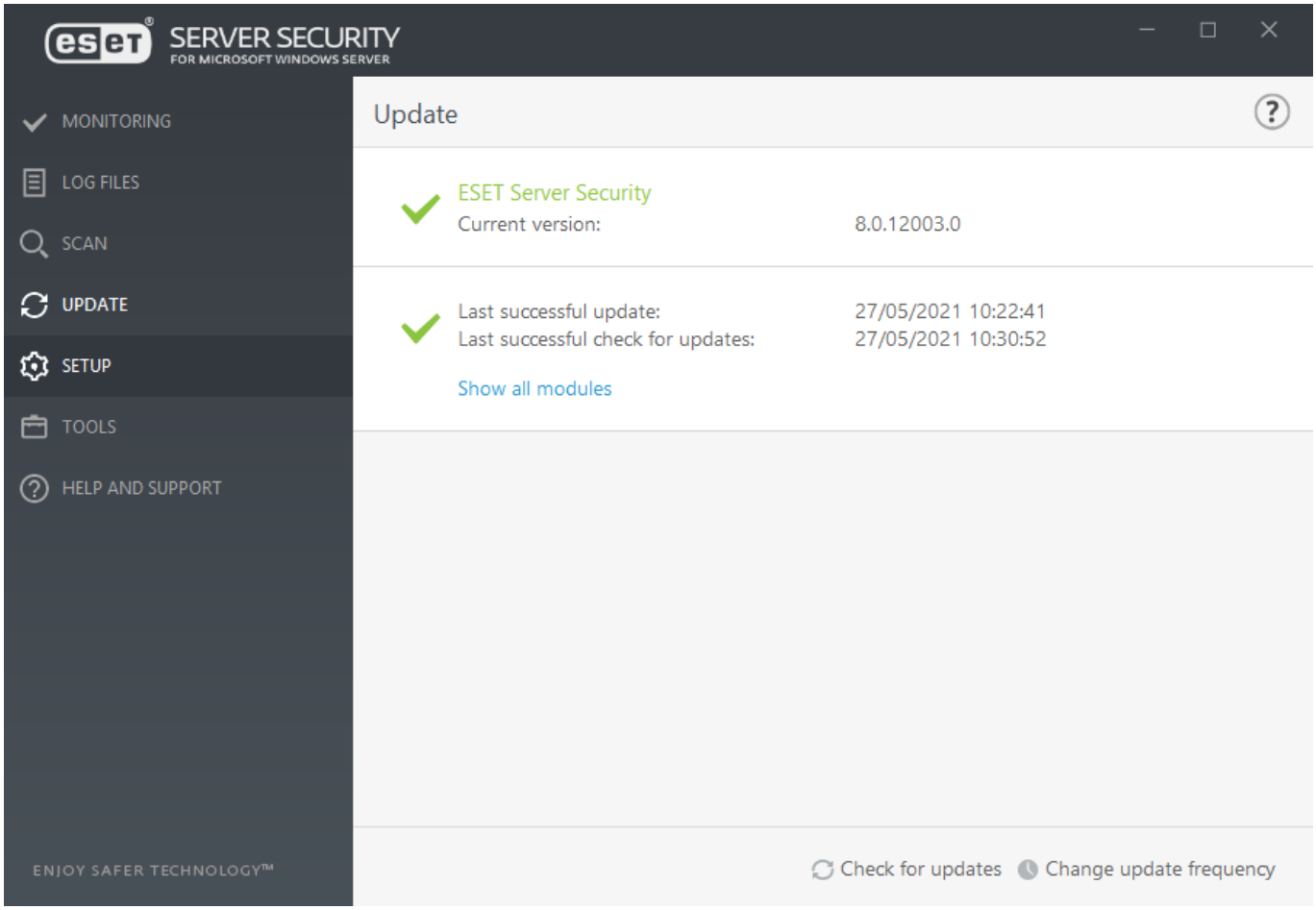
Protokol se prohledává ze shora dolů a začíná se na aktuální pozici (zvýrazněném záznamu). Vyhledávání se zastaví na prvním vyhovujícím záznamu. Pro zobrazení dalšího výsledku vyhledávání stiskněte klávesu **F3**, případně klikněte pravým tlačítkem myši, zvolte **Najít** a upřesněte parametry vyhledávání.

Aktualizace

Informace o aktuálním stavu aktualizace jsou zobrazovány na záložce Aktualizace v hlavním okně programu ESET Server Security. Pravidelná aktualizace ESET Server Security je základním předpokladem pro zajištění maximální bezpečnosti systému.

Modul Aktualizace se stará o to, aby byl program používal nejnovější detekční jádro a programové moduly. Aktualizace detekčního jádra a programových komponent představuje důležitou součást v ochraně pro škodlivému kódu.

> Pokud jste produkt dosud neaktivovali (například licenčním klíčem), budete k tomu vyzváni právě teď. Dokud nebude program aktivován, nebudou se stahovat aktualizace. Pro aktivování produktu přejděte do sekce **Nápověda a podpora** a klikněte na tlačítko **Aktivovat produkt**.



Aktuální verze

Číslo reprezentující nainstalovanou verzi produktu ESET Server Security.

Poslední úspěšná aktualizace

Datum a čas poslední úspěšné aktualizace detekčního jádra a programových modulů. Pokud nevidíte dnešní datum, moduly nemusí být aktuální.

Poslední kontrola dostupnosti aktualizace

Datum a čas posledního pokusu o zjištění dostupnosti nové verze modulů.

Zobrazit všechny moduly

Kliknutím si zobrazíte seznam používaných programových modulů.

Zkontrolovat aktualizace

Kliknutím vynutíte ověření dostupnosti nové verze modulů.

Změnit interval aktualizace

Kliknutím můžete upravit interval spuštění naplánované úlohy pro pravidelnou automatickou aktualizaci

Pokud se nebudou delší dobu moduly aktualizovat, zobrazí se některá z níže uvedených chyb:

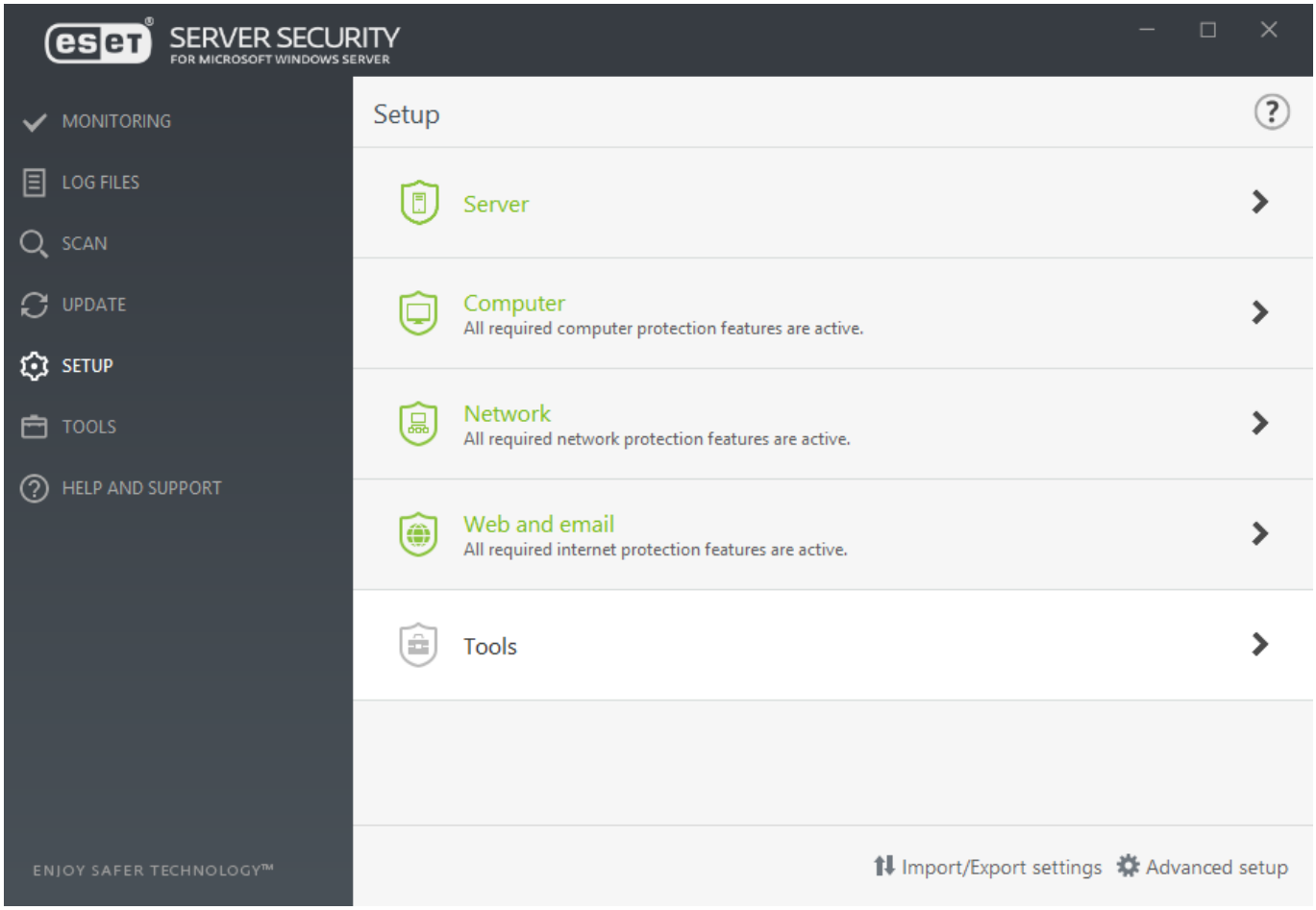
Chybová zpráva	Popis
Moduly nejsou aktuální	Tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o ověření dostupnosti aktualizace. V takovém případě doporučujeme zkontrolovat nastavení. Mezi nejčastější důvody patří chybná aktivace nebo špatně nastavené připojení
Moduly se nepodařilo aktualizovat – produkt není aktivován	Chybně jste nastavili způsob aktualizace. Doporučujeme ověřit informace pro autentifikaci vůči aktualizačnímu serveru. To provedete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) v sekci **Aktualizace**. Případně produkt aktivujte správnou licencí. V takovém případě v hlavním okně programu přejděte na záložku **Nápověda a podpora** a klikněte na tlačítko Správa licence/Aktivovat produkt a zadejte nový licenční klíč.
Chyba při stahování aktualizačních souborů	Chyba může souviset s nesprávným nastavením připojení k internetu. Doporučujeme zkontrolovat připojení k internetu (otevřením jakékoliv webové stránky ve webovém prohlížeči). Pokud se stránka neotevře, nedošlo k navázání spojení nebo situace poukazuje na problém ve vašem počítači. Pokud není připojení k internetu funkční, kontaktujte svého poskytovatele (ISP).
Moduly se nepodařilo aktualizovat Error 0073	Klikněte na **Aktualizace** > **Zkontrolovat aktualizace**. Pro více informací přejděte do Databáze znalostí.

V jednotlivých aktualizačních profilech můžete mít rozdílně nastaven proxy server. Potřebné nastavení aktualizačního profilu naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) v sekci **Aktualizace** > Profil.

Nastavení

Záložka Nastavení obsahuje následující sekce:

- Server
- Počítač
- Síť
- Web a mail
- Nástroje – Diagnostické protokolování



Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Server

V této části můžete pomocí přepínače jednotlivé komponenty zapnout nebo vypnout. Pokud chcete konkrétní část konfigurovat, klikněte na ikonu ozubeného kolečka .

Automatické výjimky

Součást, která identifikuje kritické soubory serverového operačního systému a nainstalovaných aplikací a

automaticky je přidá na seznam výjimek. Prostřednictvím této funkce můžete minimalizovat možné konflikty a zvýšit celkový výkon serveru při současně spuštěném software na detekci hrozeb.

Cluster

Tuto možnost použijte pro konfiguraci funkce ESET Cluster.

Nastavení OneDrive kontroly

Pomocí této možnosti můžete zaregistrovat nebo odregistrovat ESET OneDrive skener do/z vašeho Microsoft OneDrive.

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Počítač

ESET Server Security nabízí všechny potřebné komponenty pro ochranu serveru jako počítače. Na záložce Počítač naleznete možnosti pro konfiguraci následujících součástí:

Rezidentní ochrana souborového systému

Všechny soubory, které se v počítači otevírají, vytvářejí a spouštějí, jsou kontrolovány na přítomnost škodlivého kódu. V kontextovém menu je přímo dostupná možnost pro **konfiguraci** úrovně ochrany a **úpravu seznamu výjimek**, na který můžete přidat soubory a složky, které chcete vyloučit z kontroly.

Správa zařízení

Tento modul umožňuje kontrolovat, blokovat nebo upravovat rozšířené filtry nebo oprávnění a definovat schopnost uživatele přistupovat k danému zařízení a pracovat s ním.

Host Intrusion Prevention System (HIPS)

Monitoruje události uvnitř operačního systému a reaguje na ně na základě pravidel předdefinovaných pravidel společností ESET.

- Advanced memory scanner

- Exploit Blocker
- Ochrana proti ransomware

Prezentační režim

Funkce uživatele softwaru, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru. Po aktivování této funkce se v hlavním okně programu zobrazí oranžová výstraha týkající se aktivovaného prezentačního režimu a uživateli se zobrazí výhradně varování související s potenciálním bezpečnostním rizikem.

Dočasně vypnout antivirovou a antispywarovou ochranu

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

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Síť

V této části naleznete součásti, které vám umožní vytvořit povolovací a blokovací pravidla pro ovlivnění síťové komunikace. Zajišťují ochranu před útoky vedenými ze vzdálených počítačů a blokují některé potenciálně nebezpečné služby.

V modulu síťové ochrany můžete zapínat a vypínat následující součásti:

Ochrana proti síťovým útokům (IDS)

Analyzuje obsah síťové komunikace a chrání vás před síťovými útoky. Dále blokuje škodlivou komunikaci.

Ochrana proti zapojení do botnetu

Tato součást detekuje a blokuje komunikaci botnetu. Prostřednictvím této součásti jste schopni rychle a přesně identifikovat škodlivý kód v systému.

Seznam dočasně blokovaných IP adres (zablokované adresy)

Kliknutím si zobrazíte seznam IP adres, které byly označeny jako zdroj útoku a komunikace z těchto adres byla dočasně zablokována.

Průvodce řešením problémů (naposledy zablokované aplikace nebo zařízení)

Tento průvodce vám pomůže identifikovat problém s konektivitou způsobenou součástí síťové ochrany.

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Průvodce řešením problémů

Průvodce řešením problémů sleduje všechna blokovaná připojení a provede vás při řešení problémů s ochranou proti síťovým útokům u konkrétních aplikací nebo zařízení. Následně vám navrhne vytvoření sady pravidel, pro vyřešení problému.

Web a mail

Na záložce Web a mail naleznete možnosti pro konfiguraci následujících součástí:

Ochrany přístupu na web

Pokud je zapnuta, veškerá komunikace přes HTTP nebo HTTPs je kontrolována na přítomnost škodlivého kódu.

Ochrana poštovních klientů

Monitoruje komunikaci přijímanou POP3 a IMAP protokoly.

Anti-Phishingová ochrana

Chrání vás před legitimně vypadajícími stránkami a zprávami vytvořenými za účelem získání hesel, bankovních informací a dalších citlivých informací.

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

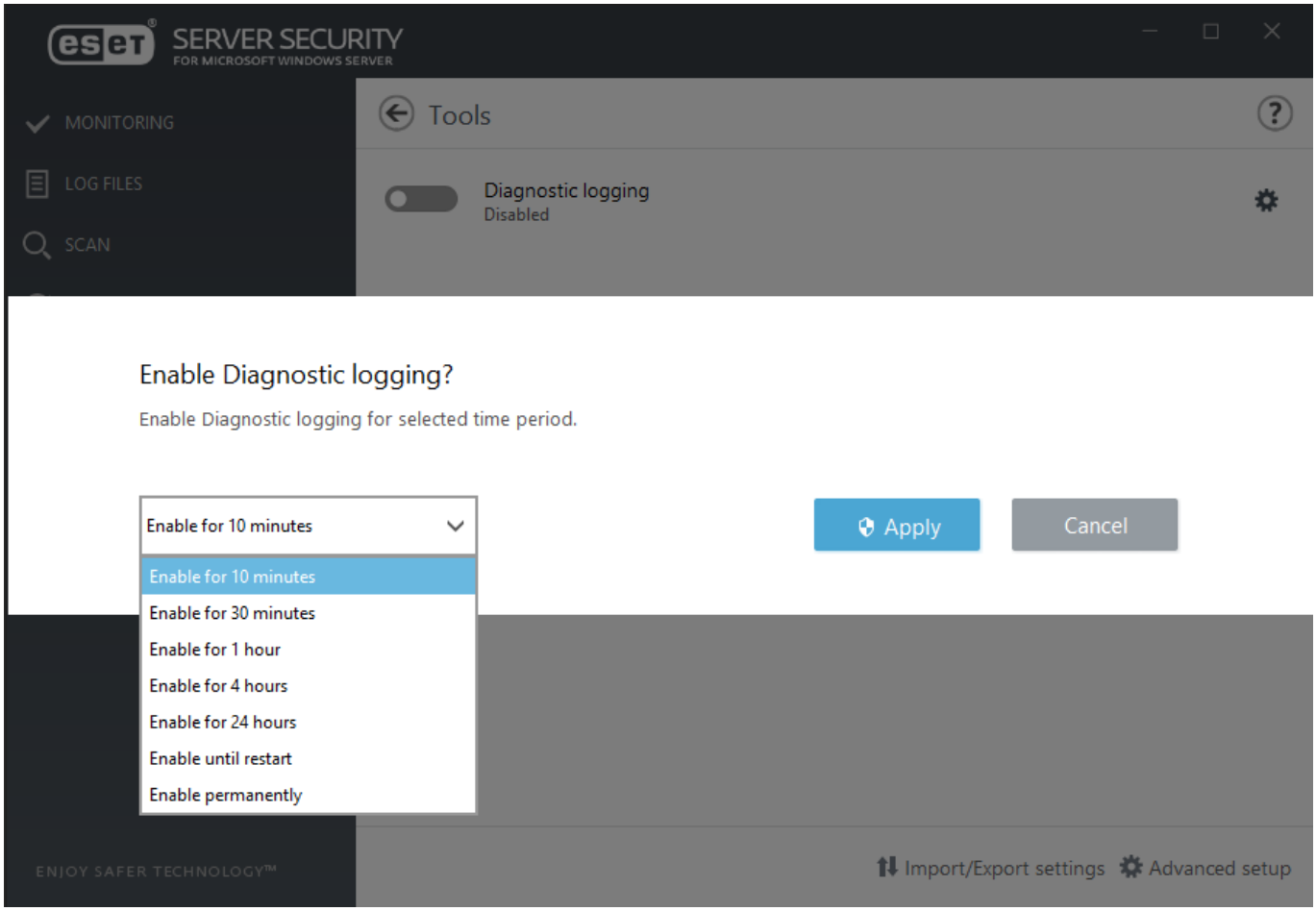
Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Nástroje – Diagnostické protokolování

Diagnostické protokoly poskytují detailní informace o běhu jednotlivých součástí ESET Server Security a jsou užitečné při řešení potíží. Po kliknutí na ikonu ozubeného kolečka se zobrazí rozšířené nastavení, kde si můžete vybrat součásti, jejichž běh chcete po aktivaci této funkce protokolovat.

Po aktivování diagnostického protokolování vyberte interval, na jak dlouho chcete diagnostiku aktivovat (10 minut, 30 minut, 1 hodinu, 4 hodiny, 24 hodin, do restartu, trvale). Následně začne ESET Server Security sbírat detailní protokoly z daných součástí.



Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tímto

můžete snížit úroveň zabezpečení serveru.

Pro opětovné aktivování vypnutého bezpečnostního modulu klikněte na červený přepínač . Následně bude daná součást opět funkční.

Pro přístup do detailního nastavení konkrétního modulu klikněte na ozubené kolečko .

Import a export nastavení

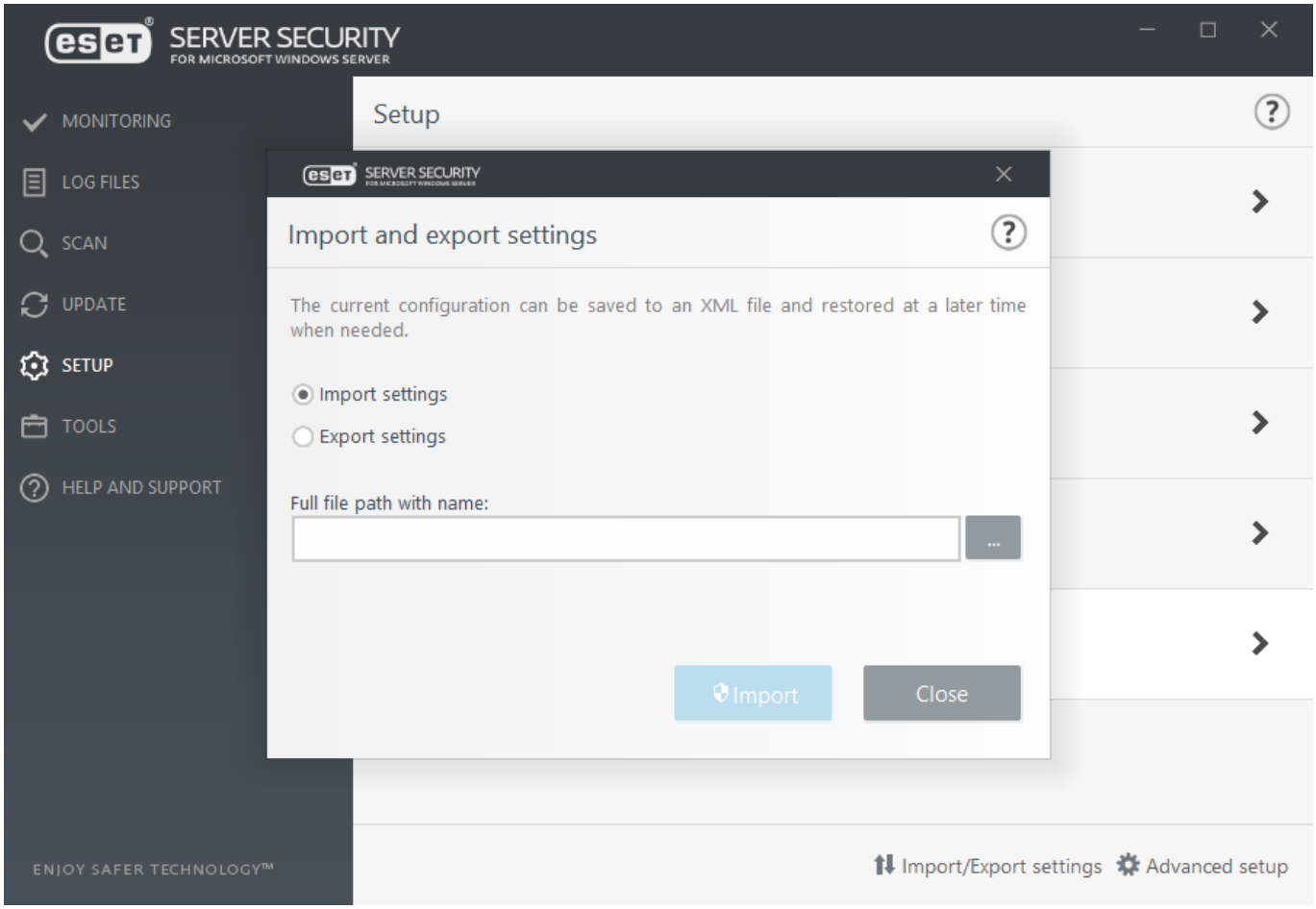
Pomocí této možnosti můžete načíst již existující konfiguraci z *.xml* souboru, případně si konfiguraci uložit a zálohovat.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. Pro přístup do **rozšířeného nastavení** stiskněte kdekoli v hlavním okně programu klávesu **F5**.

Import a export nastavení

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET Server Security a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení produktu ESET Server Security použít na více serverech. Nastavení produktu se exportuje do *.xml* souboru.



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

Nástroje

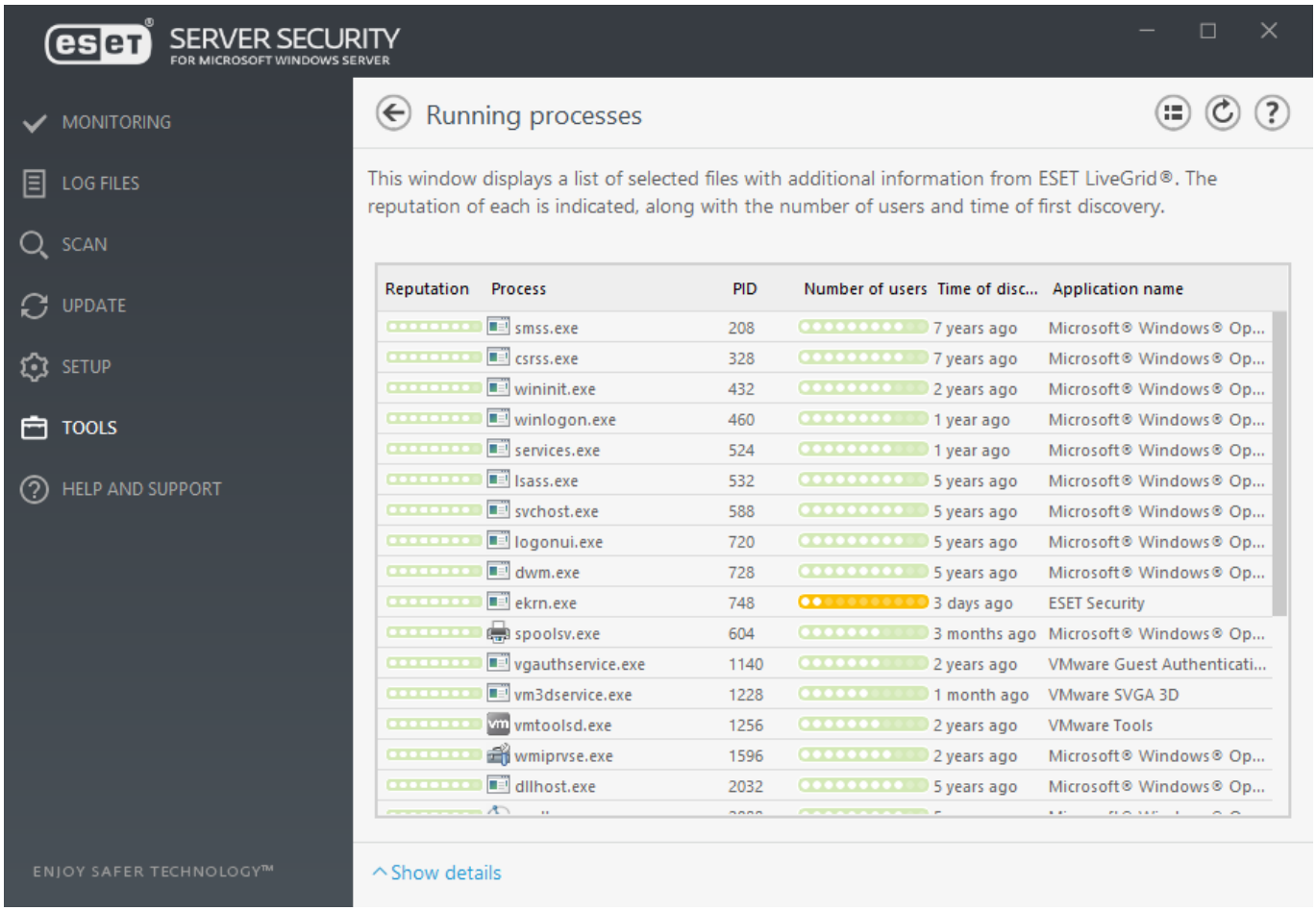
V této části programu naleznete možnosti pro správu ESET Server Security:

- Spuštěné procesy
- Sledování aktivity
- Statistiky ochrany
- Cluster
- ESET Shell
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live
- Plánovač
- Odeslat soubor k analýze
- Karanténa



Spuštěné procesy

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



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

Reputace	**Ve většině případů přiřazuje ESET Server Security a technologie ESET LiveGrid® objektům (souborům, procesům, klíčům registru apod.) úroveň rizika na základě sady heuristických pravidel, které reprezentují pravděpodobnost škodlivosti objektu. Poté na základě těchto výsledků přidělí procesům úroveň rizika od 9 – Nejlepší reputace (zelený) až po 0 – Nejhorší reputace (červený).**
Proces	Název aplikace nebo procesu, který aktuálně běží na počítači. Pro zobrazení všech běžících programů na počítači můžete použít také Správce úloh systému Windows. Správce úloh můžete otevřít kliknutím pravým tlačítkem myši na prázdnou oblast na hlavním panelu a poté kliknutím na Správce úloh nebo stisknutím kláves CTRL + SHIFT + ESC.
PID	ID běžícího procesu v operačním systému Windows.
Počet uživatelů	Počet uživatelů, kteří používají danou aplikaci. Tyto informace se shromažďují pomocí technologie ESET LiveGrid®.
První výskyt	Doba, kdy byl proces poprvé objeven pomocí technologie ESET LiveGrid®.
Název aplikace	Název aplikace, které proces patří.

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

Zobrazit detaily

Pokud kliknete na některý proces, v dolní části okna se zobrazí následující informace:

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

Přidat mezi vyloučené procesy

Po kliknutí pravým tlačítkem myši na konkrétní proces můžete pro něj přímo vytvořit výjimku. Cesta k danému procesu se přidá na seznam Vyloučených procesů

Sledování aktivity

V dialogovém okně Sledování aktivity můžete prostřednictvím grafů sledovat aktivitu:

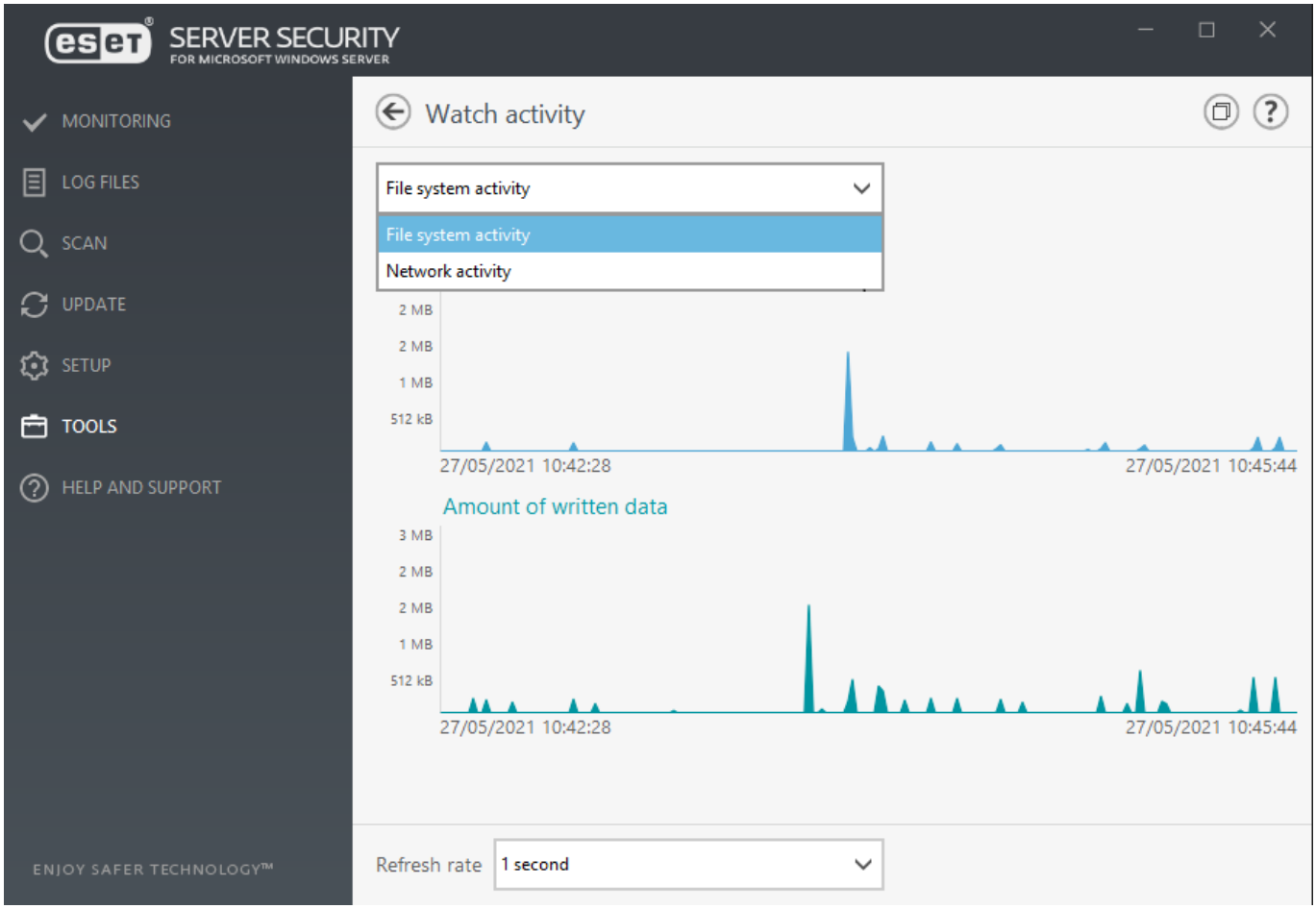
Aktivita souborového systému

Množství přečtených a zapsaných dat. Svislá osa grafu představuje načtená data (modrá) a zapsaná data (zelená).

Síťová aktivita

Množství přijatých a odeslaných dat. Svislá osa grafu představuje přijatá data (modrá) a odeslaná data (zelená).

Osa X reprezentuje časovou osu. Pro změnu měřítka a intervalu aktualizace použijte rozbalovací menu Rychlost aktualizace.



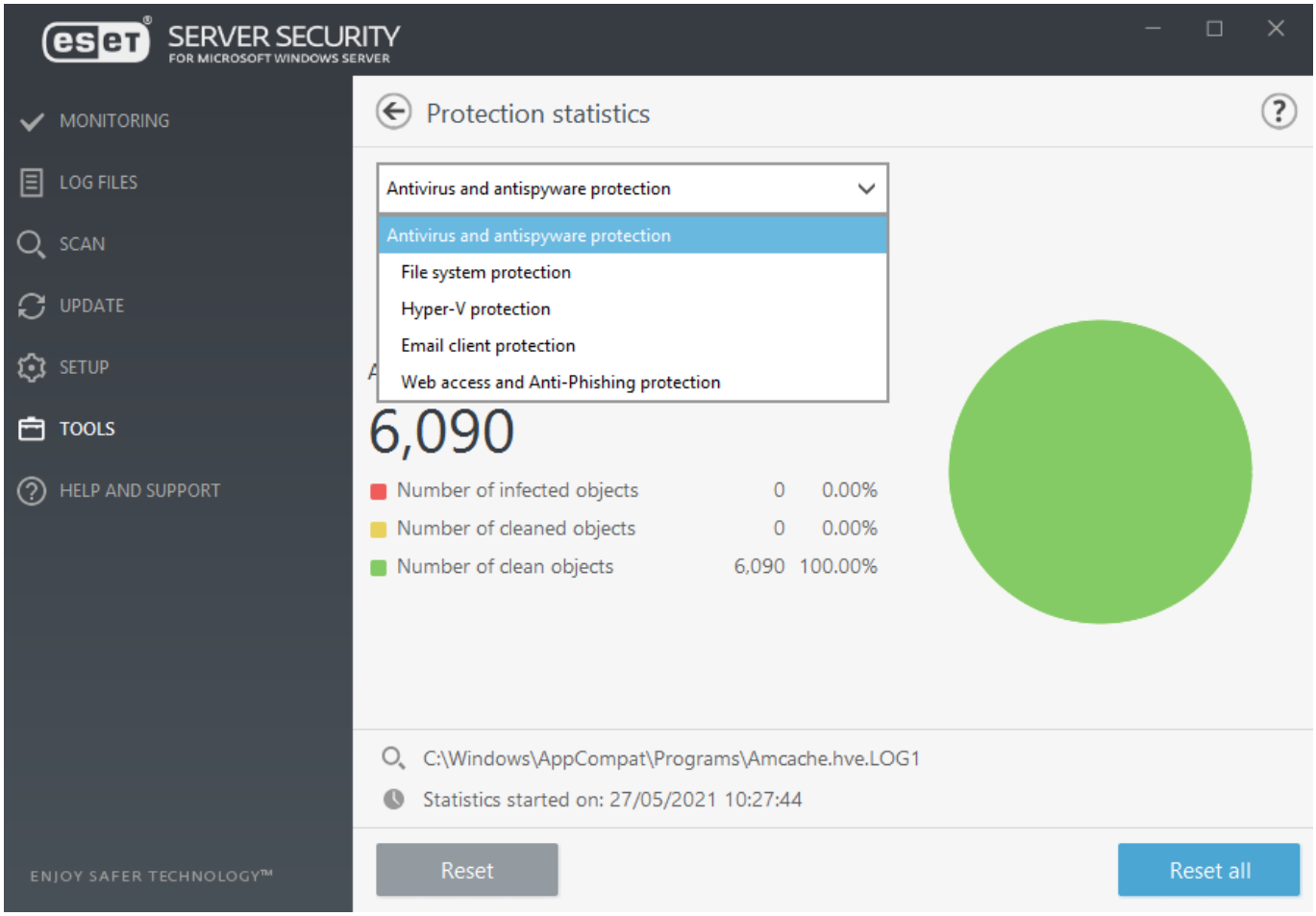
K dispozici jsou následující možnosti:

1 sekunda	**graf se obnoví každou sekundu a časová osa zobrazuje posledních 10 minut.**
1 minuta (posledních 24 hodin)	Graf se obnoví každou minutu a časová osa zobrazuje posledních 24 hodin.
1 hodina (poslední měsíc)	Graf se obnoví každou hodinu a časová osa zobrazuje poslední měsíc.

Statistiky ochrany

Pro zobrazení statistických informací souvisejících z moduly ochrany produktu ESET Server Security použijte rozbalovací menu. Statistickými informacemi máme na mysli celkový počet kontrolovaných objektů, počet infikovaných, vyléčených a čistých objektů.

Po najetí kurzorem myši na vybrané položky legendy se v grafu zobrazí pouze daná položka. Pro vymazání statistických informací pro aktuální modul ochrany klikněte na tlačítko **Vynulovat**. Pomocí tlačítka **Vynulovat vše** vymažete data ze všech modulů.



ESET Server Security poskytuje následující statistické informace:

Antivirová a antispywarová ochrana

Zobrazuje celkový počet infikovaných a vyléčených objektů.

Rezidentní ochrana souborového systému

Zobrazuje pouze objekty, které byly čteny nebo zapisovány na souborový systém.

Hyper-V ochrana

Zobrazuje celkový počet infikovaných, vyléčených a čistých objektů. (pouze na systémech s Hyper-V).

Ochrana poštovních klientů

Zobrazuje pouze objekty, které byly přijaty nebo odeslány pomocí poštovních klientů.

Ochrana přístupu na web a Anti-Phishingová ochrana

Zobrazuje pouze objekty, které byly staženy pomocí internetových prohlížečů.

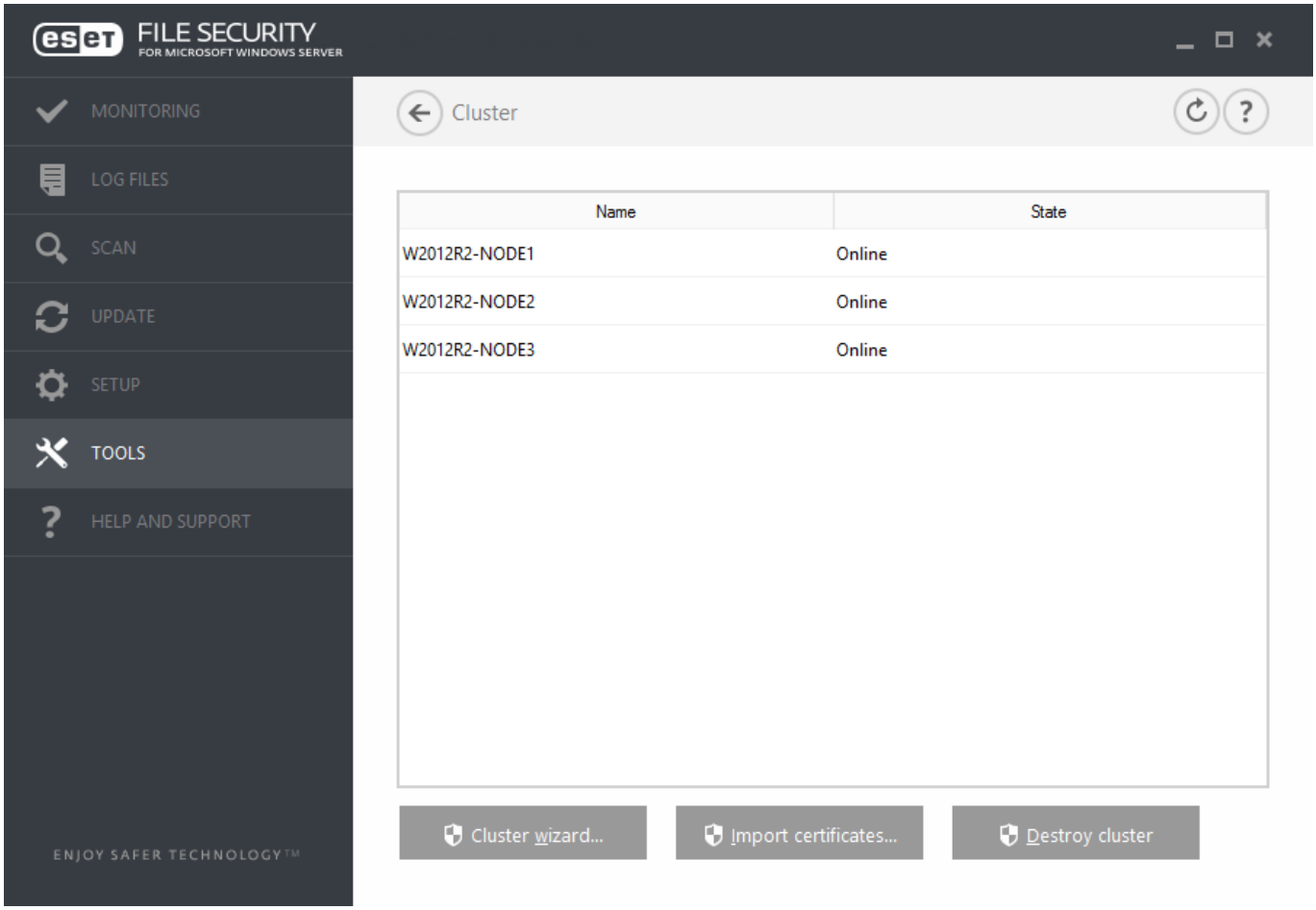
Cluster

ESET Cluster zajišťuje P2P komunikaci mezi produkty ESET určenými pro ochranu Microsoft Windows Server.

Tato infrastruktura zajišťuje vzájemnou komunikaci mezi serverovými produkty ESET a výměně dat jako je konfigurace, upozornění a zajišťuje jejich vzájemnou synchronizaci pro správné fungování všech instancí ve skupině. Příkladem může být skupina uzlů Windows Failover Cluster nebo Network Load Balancing (NLB) Cluster s nainstalovanými produkty ESET, u kterých vyžadujete stejnou konfiguraci napříč celým clusterem. Prostřednictvím ESET Clusteru zajistíte konzistentnost jednotlivých instancí.

Mezi uzly ESET clusteru nesynchronizuje nastavení uživatelského rozhraní stejně tak naplánované úlohy. Toto chování je záměrné.

Informace o stavu ESET Clusteru naleznete v hlavním okně programu na záložce **Nástroje** > **Cluster**. V případě korektně nakonfigurovaného clusteru bude obrazovka vypadat podobně jako na obrázku níže:



ESET Cluster není možné vytvořit mezi ESET Server Security a ESET File Security pro Linux.

Při konfiguraci ESET Clusteru můžete uzly přidat dvěma způsoby:

- **Automaticky detekovat** – pokud již provozujete Windows Failover Cluster / NLB Cluster, pomocí této možnosti se existující uzly automaticky přidají do ESET Clusteru.

- **Procházet** – uzly můžete přidat ručně zadáním názvu serveru, který je součástí stejné domény nebo stejné pracovní skupiny.

Při doručení zprávy z karantén ESET Server Security ignoruje MIME hlavičku `To:`, protože je snadné ji podvrhnout. Místo tohoto se použije informace o příjemci z příkazu `RCPT TO:` SMTP spojení. Tím je zajištěno doručení zprávy správnému příjemci.

Po přidání uzlů do ESET Clusteru je dalším krokem instalace ESET Server Security na každý uzel. K ní dojde automaticky v průběhu konfigurace ESET Clusteru. Pro vzdálenou instalaci ESET Server Security na uzly clusteru je nutné zadat přihlašovací údaje:

- **Doménový scénář** – přihlašovací údaje správce domény.
- **Scénář pracovní skupiny** - Je třeba zajistit, aby všechny uzly používaly stejné přihlašovací údaje k účtu místního správce.

ESET Cluster může obsahovat uzly automaticky získané z již existujícího Windows Failover Cluster / NLB Cluster, stejně tak ručně přidané uzly (ze stejné domény).

Uzly domény nelze kombinovat s uzly pracovní skupiny.

Dalším požadavkem pro instalaci ESET Server Security na uzly ESET Clusteru je povolené **Sdílení souborů a tiskáren** v Bráně Windows Firewall.

Nové uzly do již existujícího ESET Clusteru můžete přidat kdykoli prostřednictvím Průvodce clusterem

Importování certifikátů

Při použití HTTPS kanálu jsou certifikáty používány pro ověření důvěryhodnosti komunikace mezi jednotlivými uzly. Každý ESET Cluster používá nezávislou hierarchii certifikátů. Hierarchie má jeden kořenový certifikát a sadu certifikátů pro jednotlivé uzly podepsané kořenovým certifikátem. Privátní klíč kořenového certifikátu se smaže po vytvoření certifikátů pro všechny uzly clusteru. Po přidání nového uzlu do clusteru se vždy vytvoří nová hierarchie certifikátů. Pro importování certifikátů přejděte do složky s certifikáty (vygenerované v průběhu konfigurace clusteru). Vyberte soubor a klikněte na tlačítko **Otevřít**.

Zničení clusteru

ESET Cluster můžete kdykoli jednoduše zrušit kliknutím na tlačítko Zničit cluster. Následně se do protokolu každého uzlu ESET Clusteru zapíše informace o zničení clusteru. Po dokončení akce se odstraní všechna pravidla z Brány Windows Firewall, které vytvořil produkt ESET. Uzly budou vráceny do jejich původního stavu a můžete je v případě potřeby zapojit do jiného ESET Clusteru.

Průvodce clusterem – výběr uzlů

Prvním krokem při konfiguraci ESET Clusteru je přidání uzlů. Uzly můžete **Automaticky detekovat** nebo je, vybrat ručně po kliknutí na tlačítko **Procházet…**. Alternativně zadejte název serveru do zobrazeného textového pole a klikněte na tlačítko **Přidat**.

Automaticky detekovat

Po kliknutí se automaticky přidají všechny uzly z existujícího Windows Failover Cluster / Network Load Balancing (NLB) Cluster. Pro automatické načtení uzlů musí být server, na kterém ESET Cluster vytváříte, členem Windows Failover Cluster / NLB Cluster. Pro správnou detekci uzlů musí být na NLB Clusteru aktivní funkce **Povolit vzdálené ovládání**. Po načtení všech uzlů můžete konkrétní uzly, které nechcete mít v ESET Clusteru, odstranit.

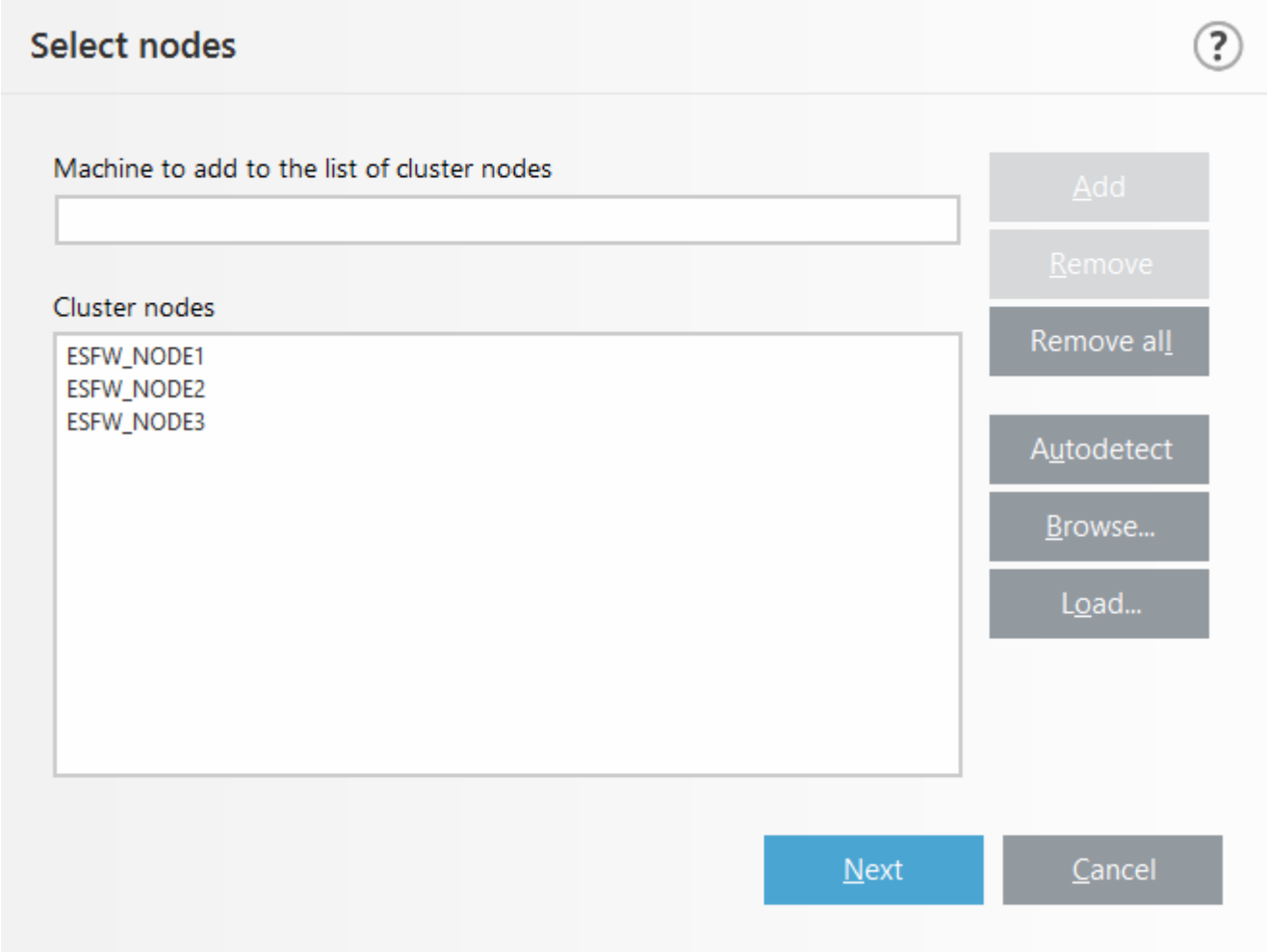
Procházet

Tuto možnost využijte pro ruční výběr počítačů v doméně (Domain) nebo pracovní skupině (Workgroup). Tímto

způsobem můžete do ESET Clusteru přidáte uzly ručně. Případně uzel definujte ručně zadáním názvu serveru a klikněte na tlačítko **Přidat**.

Načíst

Kliknutím můžete seznam uzlů načíst z externího souboru.



Pro odebrání konkrétního uzlu ze seznamu **uzlů clusteru** klikněte na vybranou položku a klikněte na tlačítko **Odebrat**. Celý seznam vymažete kliknutím na tlačítko **Odebrat vše**.

Již existující ESET Cluster můžete kdykoli upravit a přizpůsobit jeho seznam uzlů. V tomto případě postupujte podle stejných kroků.

Všechny uzly na seznamu musí být online a dosažitelné z daného serveru. Localhost je automaticky přidán do seznamu uzlů clusteru.

Průvodce clusterem – konfigurace clusteru

Zadejte název clusteru a v případě potřeby upravte síťovou konfiguraci.

Název clusteru

Zadejte název clusteru a klikněte na tlačítko Další.

Port (standardně 9777)

Pokud máte v síti port 9777 obsazen, zadejte jiné číslo portu.

Otevřít port v bráně Windows Firewall

Pokud aktivujete tuto možnost, pro komunikaci na definovaném portu se vytvoří povolování pravidlo ve Windows Firewall.

Průvodce clusterem – možnosti konfigurace

Vyberte způsob distribuce certifikátu a rozhodněte se, jakým způsobem chcete uzly instalovat produkt ESET.

Distribuce certifikátu

- **Automaticky vzdáleně** – certifikát bude nainstalován automaticky.
- **Ručně** – po kliknutí na tlačítko **Generovat** se zobrazí dialogové okno, ve které vyberte složku pro uložení certifikátů. Do definované složky se vygeneruje kořenový certifikát společně s certifikáty pro jednotlivé uzly, kterou jsou důležité pro konfiguraci ESET Clusteru. Kliknutím na tlačítko **Ano** následně zaregistrujete vygenerované certifikáty na lokálním stroji.

Instalace produktu na jiné uzly

- **Automaticky vzdáleně** – ESET Server Security se nainstaluje automaticky na každý uzel (platí pro případ, že je na všech uzlech OS se stejnou architekturou).
- **Ručně** – tuto možnost vyberte v případě, pokud chcete ESET Server Security instalovat ručně (například ve smíšeném prostředí, kdy máte na uzlech OS s odlišnou architekturou).

Odeslat licenci na uzly s neaktivovaným produktem

Tuto možnost vyberte, pokud chcete bezpečnostní produkt ESET instalovaný na uzly clusteru automaticky aktivovat.

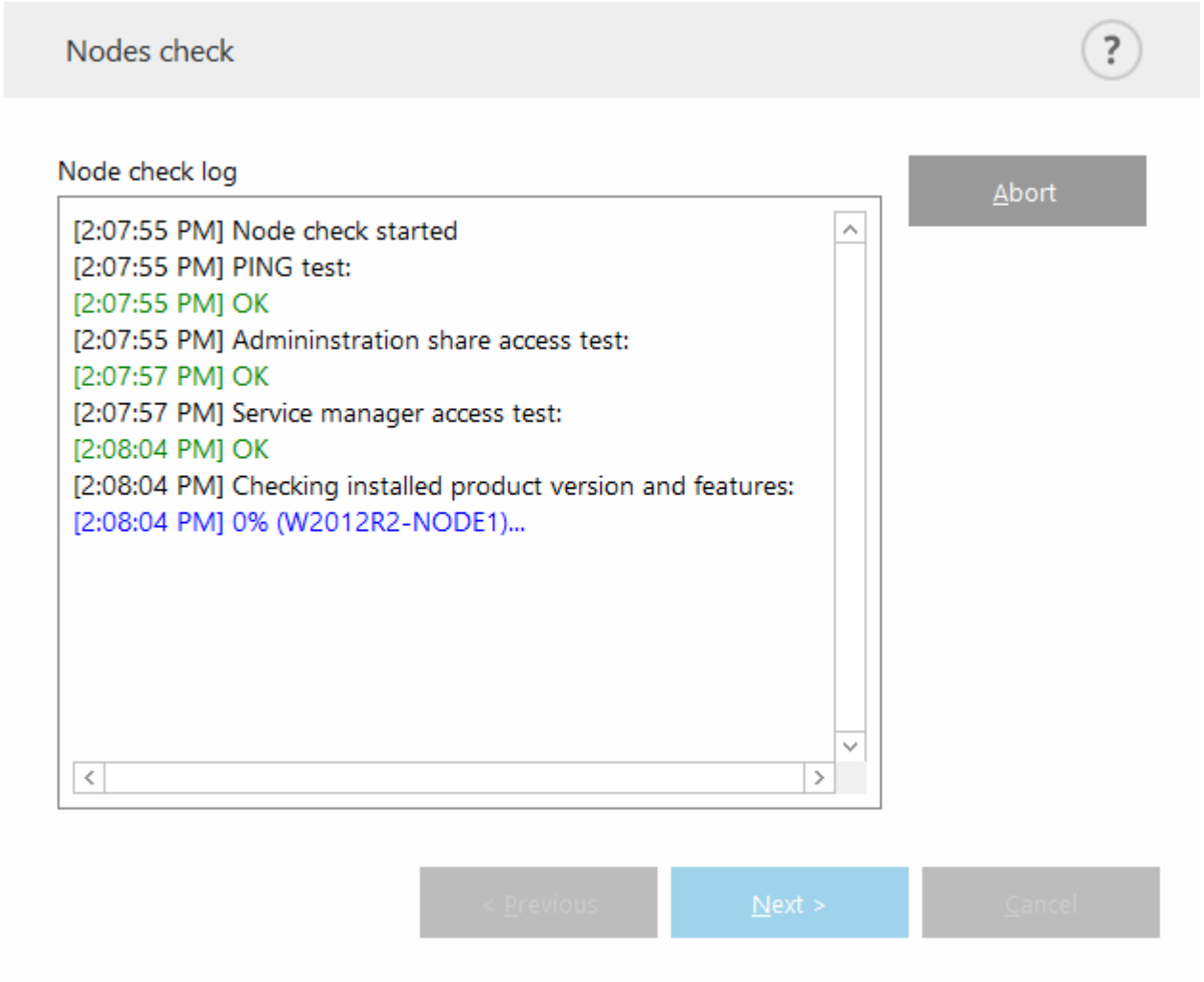
> Pokud chcete vytvořit ESET Cluster ve smíšeném prostředí s rozdílnou systémovou architekturou (32-bit a 64-bit), bude nutné nainstalovat ESET Server Security ručně. O tom, že se jedná o smíšené prostředí vás průvodce informuje v další kroku.

Průvodce clusterem – ověření uzlů

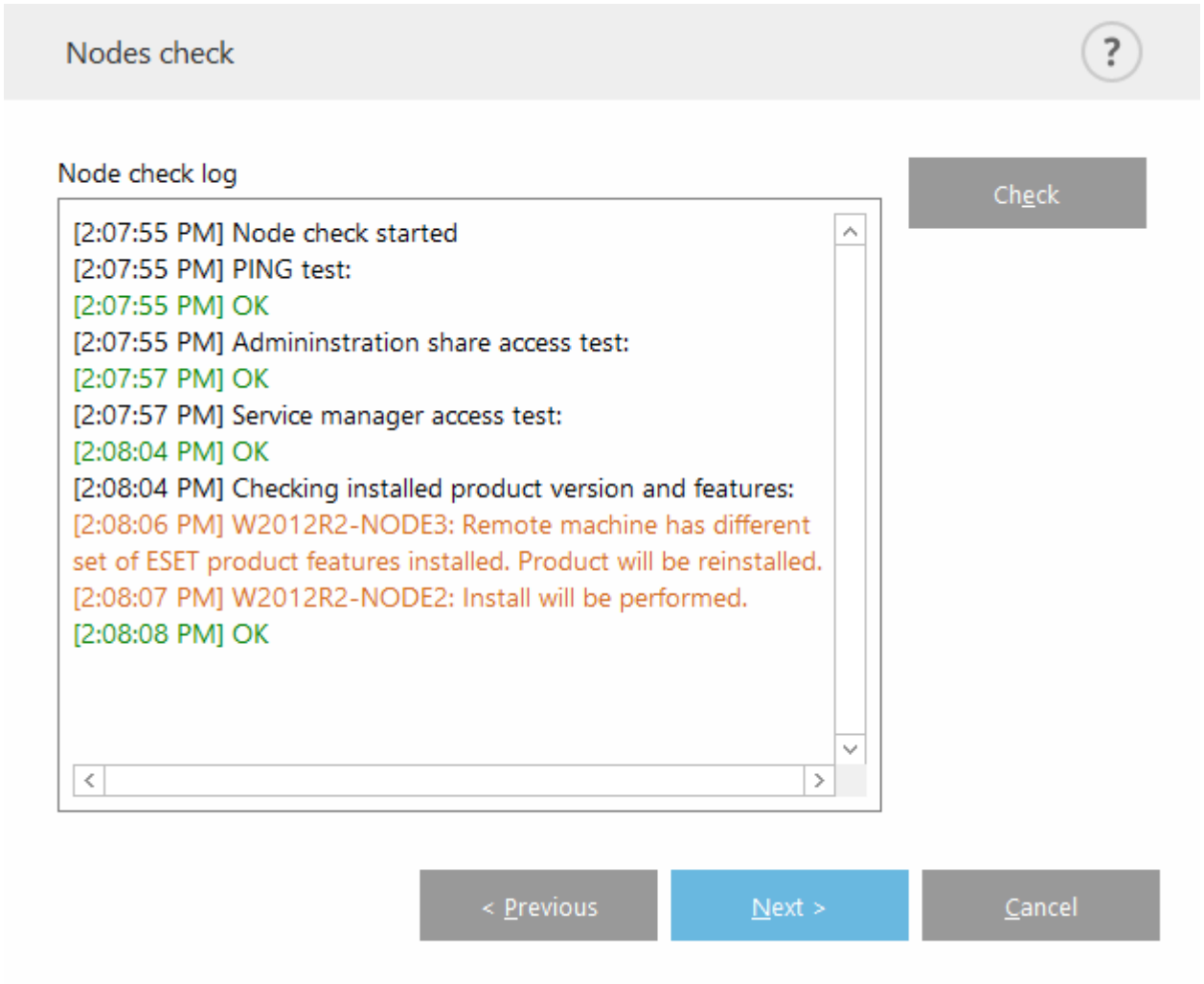
V dalším kroku dojde k ověření uzlů. V **protokolu** se zobrazí informace, zda:

- jsou existující uzly v ESET Clusteru online,
- jsou nově přidané uzly dosažitelné,
- jsou uzly online,
- jsou na uzlech dostupná administrativní sdílení,

- je na uzlech možné vzdáleně spouštět soubory,
- je na uzlech nainstalována správná verze produktu ESET,
- jsou na uzlech zaregistrovány nové certifikáty.

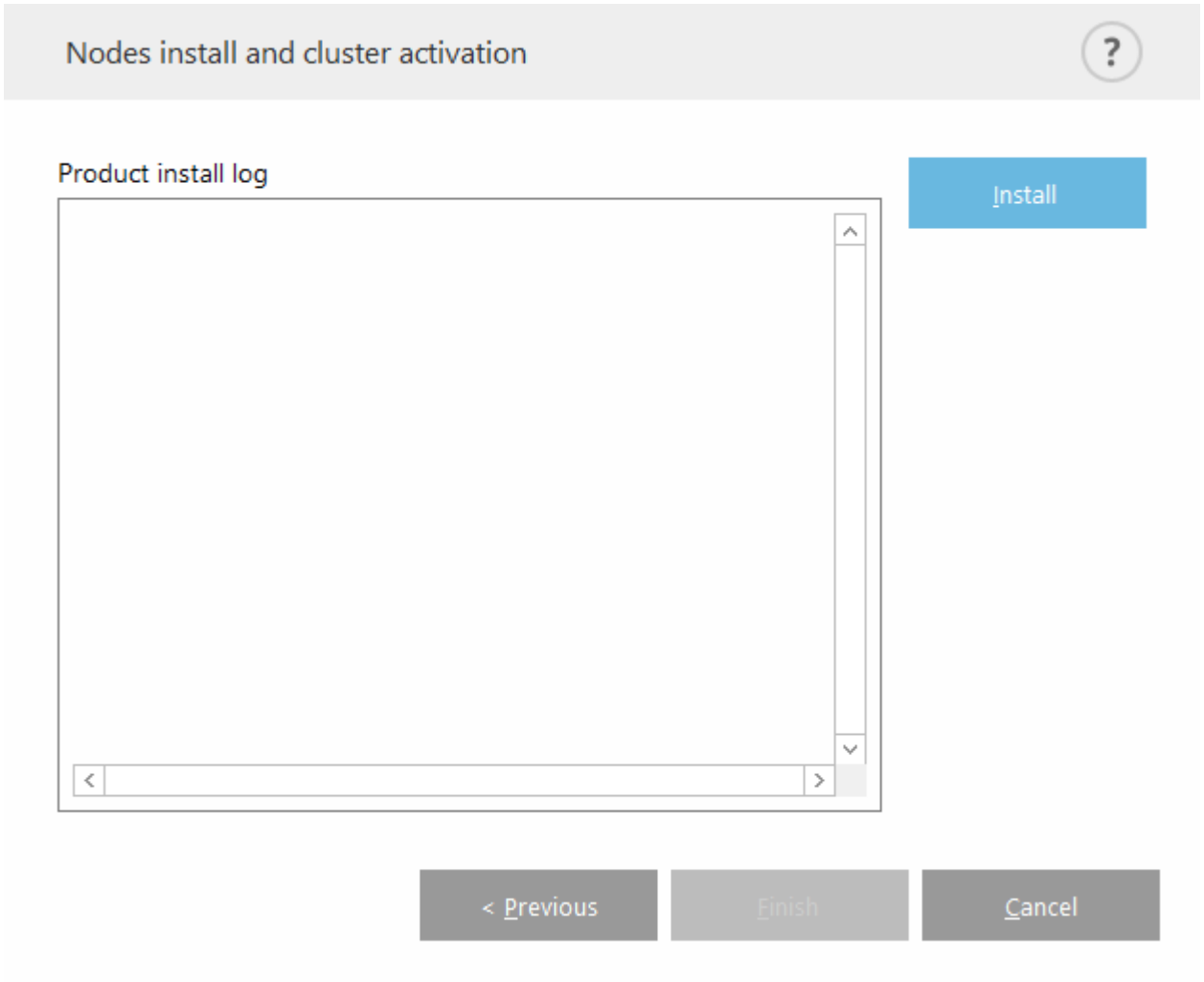


Po dokončení kontroly se zobrazí výsledek:

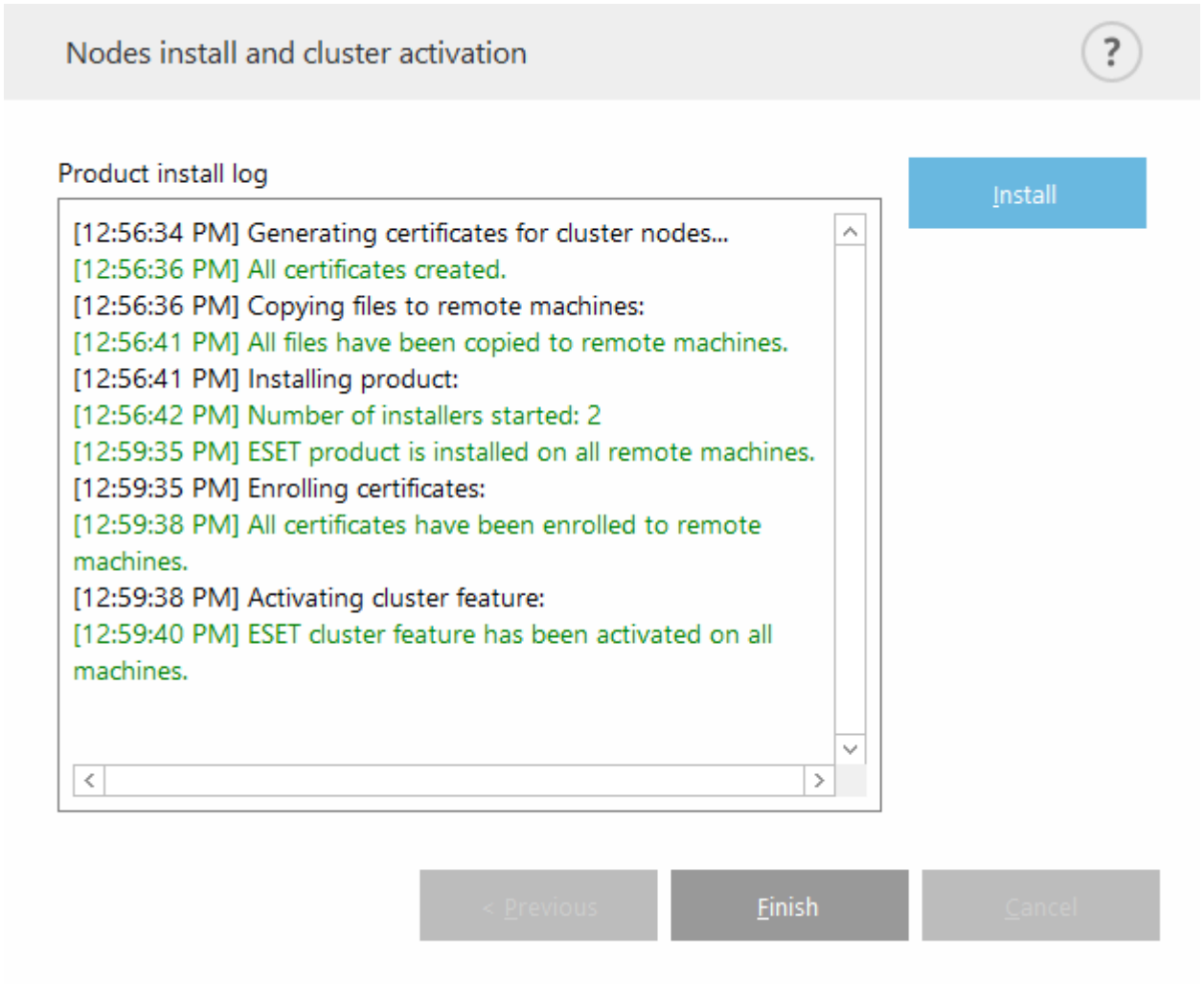


Průvodce clusterem – instalace uzlů a aktivace clusteru

Při vzdálené instalaci v průběhu inicializace ESET Clusteru se průvodce pokusí instalační balíček vyhledat ve složce *%ProgramData%\ESET\ESET Security\Installer*. Pokud nebude v dané složce instalační balíček nalezen, uživateli se zobrazí výzva a bude nutné jej vybrat ručně.

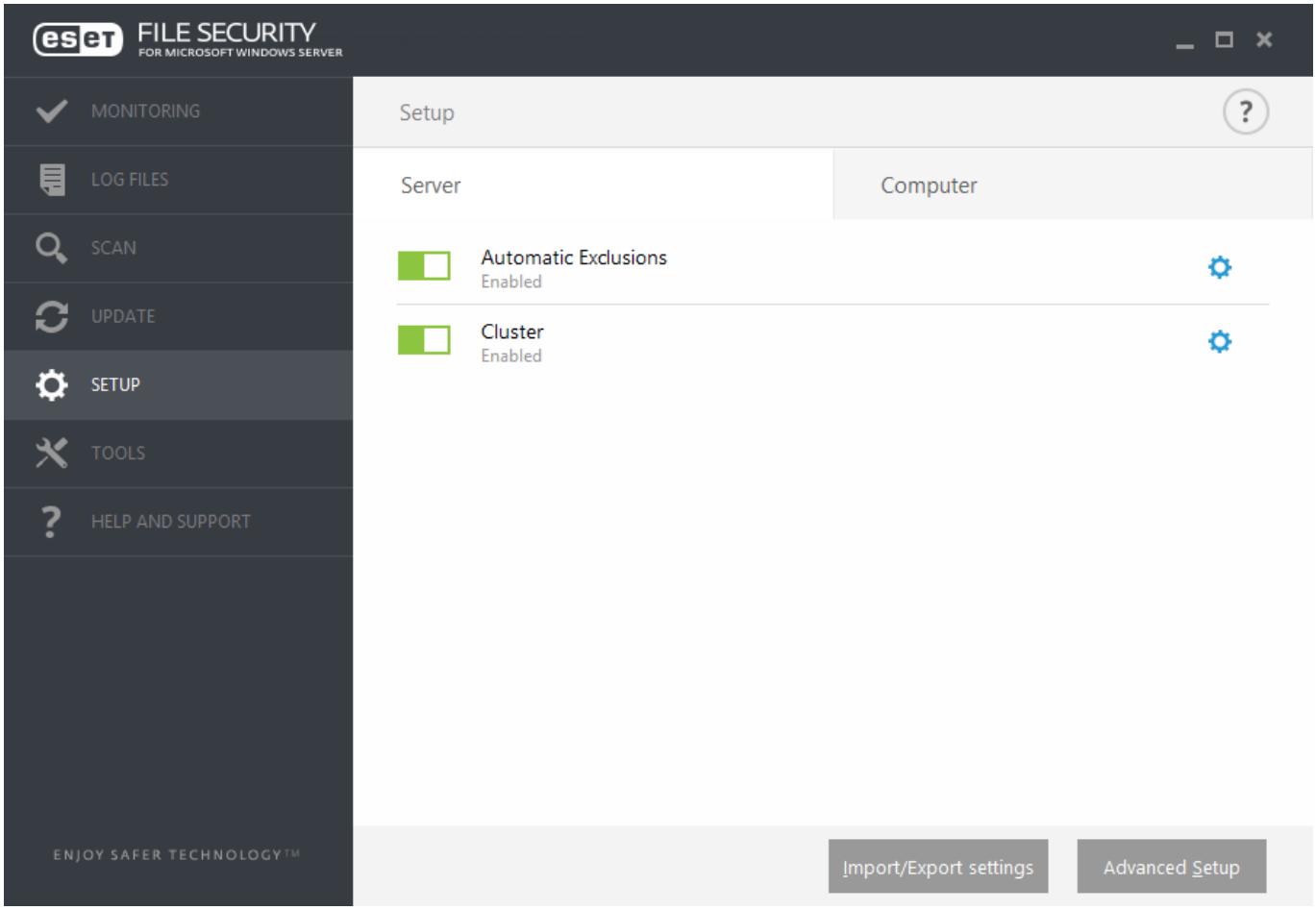


Pokud se pokoušíte vzdáleně instalovat na uzly s odlišnou architekturou operačního systému (32-bit versus 64-bit), budete na to upozornění a vyzváni k ruční instalaci produktu ESET na jednotlivé uzly.



Pokud jste správně nakonfigurovali ESET Cluster, v hlavním okně programu na záložce **Nastavení** > **Server** bude tato funkce bude aktivní.

Pokud je na některých uzlech nainstalována starší verze produktu ESET Server Security, budete upozornění, že je nutné provést aktualizaci. Mějte na paměti, že při provedení aktualizace produktu ESET Server Security prostřednictvím průvodce vytvořením clusteru může dojít k restartování serveru, na kterém je nainstalována starší verze.



Aktuální stav ESET Clusteru si zobrazíte v hlavním menu na záložce **Nástroje** > **Cluster**.

ESET Shell

ESET Shell (zkráceně eShell) je prostředí příkazového řádku produktu ESET Server Security. Jedná se o alternativu ke grafickému uživatelskému rozhraní (GUI). eShell má všechny funkce a možnosti, které vám poskytuje GUI. Prostřednictvím eShell dokážete konfigurovat a spravovat celý program bez použití GUI.

Kromě všech funkcí a vlastností, které jsou dostupné pomocí uživatelského rozhraní, vám dále nabízí možnost automatizace pomocí spouštění skriptů pro nastavení konfigurace, změnu konfigurace nebo provedení akce. Rovněž eShell může být velmi užitečný pro administrátory, kteří dávají přednost příkazového řádku před GUI.

Pro dostupnost všech funkcí doporučujeme eShell spouštět jako administrátor. To samé platí pro případ, kdy budete příkazy spouštět z příkazového řádku Windows (cmd). Spusťte jej jako administrátor. Pokud příkazový řádek nespustíte jako správce, nebudete moci spouštět příkazy, protože nebude mít dostatečné oprávnění.

eShell můžete používat ve dvou režimech:

1. **Interaktivní režim** – ten je užitečný v případě, kdy chcete používat eShell (nikoli pro jednorázové spuštění příkazu), například pro nastavovaní konfigurace, prohlížení protokolů atd. Interaktivní režim můžete používat pokud neznáte všechny příkazy. Interaktivní režim vám ulehčí orientaci v eShell. Rovněž vám zobrazí příkazy, které můžete používat v rámci daného kontextu.

2. **Spuštění jednotlivého příkazu/dávkový režim** – můžete jej používat, pokud potřebujete spustit příkaz bez přechodu do interaktivního režimu eShell. Stačí z příkazového řádku Windows napsat `eshell` s potřebnými

parametry.

✔ `eshell get status nebo eshell computer set real-time status disabled 1h`

Spuštění příkazů z příkazového řádku Windows nebo vytvoření dávkových souborů je nejprve nutné konfigurovat. V opačném případě se z bezpečnostních důvodů zobrazí zpráva **Přístup odepřen**. Jedná se o bezpečnostní opatření.

ℹ Pro použití příkazů z příkazového řádku systému Windows je třeba provést změny v nastavení eShell. Pro další informace týkající se dávkových příkazů přejděte do samostatné kapitoly.

Pro spuštění eShell v interaktivním režimu můžete použít jeden z následujících postupů:

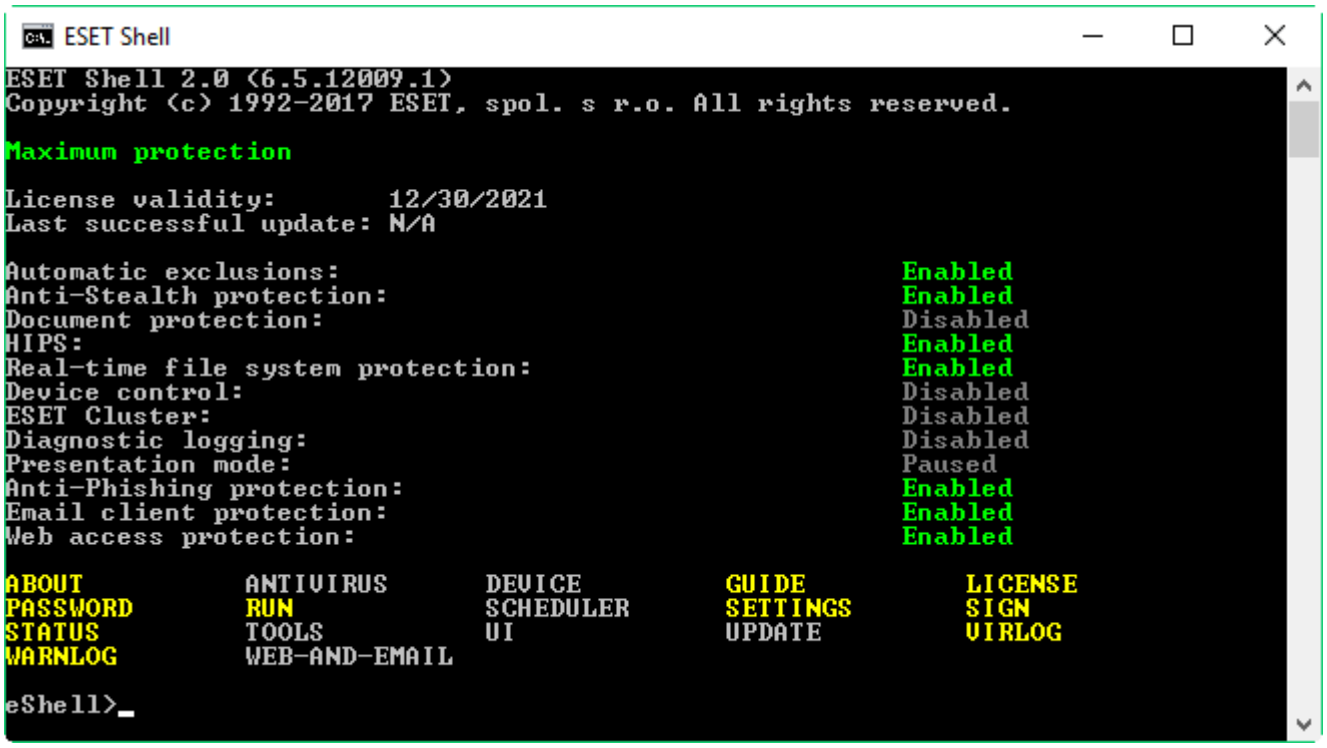
1. V **Nabídce Start** klikněte na Start > Všechny programy > ESET > ESET File Security > ESET Shell
2. V **příkazovém řádku Windows** zadejte `eshell` a stiskněte klávesu Enter.

⚠ Pokud se vám zobrazí chyba `'eshell' is not recognized as an internal or external command`, od instalace ESET Server Security se ještě nezaregistrovaly nové záznamy do proměnného prostředí. V takovém případě si otevřete nový příkazový řádek a znovu zadejte eShell. V případě přetrvávajících potíží nebo na core instalaci produktu ESET Server Security spusťte eShell použitím absolutní cesty. Příklad: `"%PROGRAMFILES%\ESET\ESET File Security\eShell.exe"` (uvozovky v příkazu ponechte, jinak nebude funkční).

Při prvním spuštění eShell v interaktivním režimu se zobrazí obrazovka prvotního spuštění.

ℹ Pro zobrazení prvotní obrazovky v budoucnu, zadejte příkaz `guide`. Zobrazí se základní příklady použití eShell se syntaxí, prefixem, cestou příkazu, aliasy atp.

Při každém dalším spuštění eShell se zobrazí následující obrazovka:



Příkazy nerozlišují velikost písmen. Používat můžete jak velká, tak i písmena, a přesto se příkaz se provede.

Přizpůsobení eShell

Vzhled eShell si můžete přizpůsobit v kontextu `ui eshell`. Nastavit si můžete aliasy, barvy, jazyk, politiku pro spouštění skriptů, nastavení pro skryté příkazy a mnohem více.

Použití

Syntaxe

Zadávané příkazy musí odpovídat syntaxi a dále mohou obsahovat prefix, kontext, argumenty, další možnosti atp. Níže je uvedena všeobecná syntaxe používaná v rámci celého eShell:

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

Příklad (tento příkaz aktivuje ochranu dokumentů):

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

`SET` – prefix

`COMPUTER SCANS DOCUMENT` – cesta ke konkrétnímu příkazu, kontext, ve kterém se příkaz nachází

`REGISTER` – samotný příkaz

`ENABLED` – argument pro daný příkaz

Použitím `?` jako argumentu pro příkaz si zobrazíte syntaxi daného příkazu. Například `STATUS ?` zobrazí syntaxi pro příkaz `STATUS`.

SYNTAXE:

```
[get] status
```

OPERACE:

`get` – vrátí stav všech modulů ochrany

Můžete si všimnout, že `[get]` je v hranatých závorkách. Prefix `get` je výchozí pro příkaz `status`. To znamená, že když provedete příkaz `status` bez zadání prefixu, použije se výchozí prefix (v tomto případě `get status`). Použitím příkazů bez prefixu ušetříte čas při jejich psaní. Výchozím prefixem pro většinu příkazů je `get`, ovšem měli byste si být jistí, že výchozí prefix existuje pro konkrétní příkaz, který chcete provést.

Příkazy nerozlišují velikost písmen. Používat můžete velká i malá a příkaz se provede.

Prefix / Operace

Prefix představuje operaci. Například prefix `GET` vrátí informaci o tom, jak je ESET Server Security nastaven nebo zobrazí aktuální stav (například `GET COMPUTER REAL-TIME STATUS` vrátí aktuální stav rezidentní ochrany). Naopak prefix `SET` nastaví funkci nebo změní její stav (například `SET COMPUTER REAL-TIME STATUS ENABLED` aktivuje rezidentní ochranu).

Níže uvádíme seznam prefixů, které můžete v eShell použít. Příkaz nemusí podporovat všechny uvedené prefixy:

GET	vrátí aktuální nastavení/stav
SET	nastaví hodnotu/stav
SELECT	vybere položku
ADD	přidá položku
REMOVE	odstraní položku
CLEAR	odstraní všechny položky/soubory
START	spustí akci
STOP	úplně zastaví akci
PAUSE	pozastaví akci
RESUME	obnoví běh pozastavené akce
RESTORE	obnoví původní nastavení/objekt/soubor
SEND	odešle objekt/soubor
IMPORT	importuje ze souboru
EXPORT	exportuje do souboru

Prefixy GET a SET se používají s většinou příkazů, ovšem některé příkazy (jako EXIT) prefixy nepoužívají.

Cesta příkazu / Kontext

Příkazy jsou umístěné do kontextů, které tvoří stromovou strukturu. Vrchní úroveň stromu je kořen (root). Po spuštění eShell se nacházíte na úrovni kořene:

```
eShell>
```

Příkaz můžete provést přímo odsud nebo pro přechod do stromové struktury zadejte kontextový název. Pokud například zadáte kontext TOOLS, zobrazí se všechny dostupné příkazy a subkontexty.



Žluté jsou příkazy, které můžete provést. Šedivé jsou podkontexty, do kterých můžete přejít. Podkontexty

obsahují další příkazy.

Pro návrat na vyšší úroveň použijte `..` (dvě tečky).

> ✓ Pokud se nacházíte v:
> `eShell computer real-time>`
> zadáním `..` se dostanete o jednu úroveň výše do:
> `eShell computer>`

Pokud se chcete vrátit zpět na kořen z `eShell computer real-time>` (z podkontextu, který je o dvě úrovně níže než kořen), jednoduše zadejte `.. ..` (dvě tečky a dvě tečky oddělené mezerou). Po zadání tohoto příkazu se dostanete o dvě úrovně výše, v tomto případě na úroveň kořene. Použitím zpětného lomítka `\` se vrátíte přímo do kořene bez ohledu na to, jak hluboko se nacházíte. Pro návrat do konkrétního kontextu na vyšší úrovni použijte odpovídající počet `..` v příkazu s využitím mezery jako oddělovače. Například, pokud se chcete vrátit o tři úrovně výše, zadejte `.. .. ..`

Cesta je relativní k aktuálnímu kontextu. Pokud je příkaz dostupný v aktuálním kontextu, cestu nezadávejte. Například na provedení `GET COMPUTER REAL-TIME STATUS` zadejte:

`GET COMPUTER STATUS` – pokud jste v kontextu root (příkazový řádek ukazuje eShell>)

`GET STATUS` – pokud jste v kontextu COMPUTER (příkazový řádek ukazuje eShell computer>)

`.. GET STATUS` – pokud jste v kontextu COMPUTER REAL-TIME (příkazový řádek ukazuje eShell computer real-time>)

Používat můžete jednoduše jen jednu `.` (tečka) místo dvou `..`, protože jedna tečka představuje zkratku dvou teček.

> ✓ `. GET STATUS` – pokud jste v kontextu `COMPUTER REAL-TIME` (příkazový řádek ukazuje `eShell computer real-time>`)

Argument

Je akce, která je provedená určitým příkazem. Například příkaz `CLEAN-LEVEL` (umístěný v`COMPUTER REAL-TIME ENGINE`) může být použit s následujícími argumenty:

`rigorous` – vždy vyřešit infekci

`safe` – pokud je to bezpečné, vyřešit infekci, jinak ponechat

`normal` – pokud je to bezpečné, vyřešit detekci, jinak se dotázat

`none` – vždy se dotázat koncového uživatele

Dalším příkladem jsou argumenty `ENABLED` nebo `DISABLED`, které se používají pro zapnutí nebo vypnutí určité funkce.

Zkrácená forma příkazů

eShell vám umožňuje zkracovat kontexty, příkazy a argumenty (za předpokladu, že argument je přepínač nebo alternativní možnost). Prefix nebo argument, který je konkrétní hodnotou, jako číslo, název nebo cesta, není možné zkrátit. Používat můžete čísla`1` a `0` jako alternativu argumentů enabled a disabled.

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

Příklad zkrácené formy:

```
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 případě, že dva příkazy nebo kontexty začínají stejným písmenem (například `ADVANCED` a `AUTO-EXCLUSIONS` a zadáte A jako zkrácený příkaz, eShell nebude schopný rozhodnout, který z těchto dvou příkazů chcete provést. Proto zobrazí chybovou zprávu a seznam příkazů začínající písmenem "A", ze kterých si můžete vybrat:

```
eShell>a

The following command is not unique: a
```

V kontextu `COMPUTER` jsou dostupné následující podkontexty:

```
ADVANCED

AUTO-EXCLUSIONS
```

Přidáním jednoho nebo více písmen (například `AD` místo pouhého `A`) eShell nabídne příkaz `ADVANCED`, čímž se stává unikátní. Stejný princip platí pro zkrácené příkazy.

> Pokud si chcete být jistí, že se příkaz provede tak jak potřebujete, poté nedoporučujeme zkracovat příkazy, argumenty atp., ale používat jejich plnou formu. Tímto způsobem eShell provede příkaz tak, jak si přejete, a předejdete nežádoucím chybám. Toto obzvláště platí pro dávkové soubory / skripty.

Automatické dokončování

Nová funkce v eShell 2.0 je velmi podobná automatickému dokončování v příkazovém řádku Windows. Příkazový řádek ve Windows umí automaticky dokončovat cesty a názvy souborů, eShell automaticky dokončuje názvy příkazů, kontextů i operací. Podporováno není pouze dokončování argumentů. Pro dokončení příkazu stačí stisknout klávesu TAB, případně opakovaným stisknutím zobrazte další možný příkaz v pořadí. Pomocí kláves SHIFT + TAB se vrátíte na předchozí automaticky doplněný příkaz. Kombinace zkrácené formy příkazů a automatického dokončování není podporována. Vždy využijte pouze jednu z obou možností. Například pokud zadáte `computer real-time additional`, po stisku klávesy TAB se nic nestane. Místo toho zadejte `com` a následně stiskněte Tab pro doplnění `computer`. Pokračujte napsáním `real` + Tab a `add` + Tab, a nakonec stiskněte klávesu Enter. Zadáním `on` a opětovným stisknutím klávesy Tab se budete přepínat mezi všemi dostupnými možnosti: `on-execute-ah`, `on-execute-ah-removable`, `on-write-ah`, `on-write-archive-default`, atd.

Aliasy

Alias je alternativní název, které můžete použít pro provedení příkazu (za předpokladu, že příkaz má přiřazený alias). Existuje několik předdefinovaných aliasů:

`(global) close` – konec

`(global) quit` – konec

`(global) bye` – konec

`warnlog` – protokol událostí

`virlog` – protokol detekcí

"(global)" znamená, že příkaz může být použitý kdekoli bez ohledu na aktuální kontext. Jeden příkaz může mít přiděleno více aliasů (například příkaz `EXIT` má aliasy `CLOSE`, `QUIT` a `BYE`). Pokud chcete zavřít eShell, můžete použít samotný příkaz `EXIT`, nebo jakýkoli z jeho aliasů. `VIRLOG` je alias pro příkaz `DETECTIONS`, který se nachází v kontextu `TOOLS LOG`. Tím je příkaz DETECTIONS dostupný z kontextu `ROOT` a tedy dostupnější (nemusíte zadávat `TOOLS`, subkontext `LOG`, a následně jej spouštět přímo z kontextu`ROOT`).

eShell vám umožňuje definovat vlastní aliasy. Příkaz `ALIAS` naleznete v kontextu `UI ESHELL`.

Ochrana produktu heslem

Přístup do nastavení produktu ESET Server Security můžete chránit heslem. Heslo můžete nastavit v grafickém rozhraní nebo pomocí eShell příkazem `set ui access lock-password`.

Toto heslo bude nutné zadávat při provádění některých příkazů v interaktivním režimu (protože mohou měnit nastavení nebo upravovat data). Pokud se chytáte používat eShell delší dobu a nechcete neustále zadávat heslo, můžete eShell nastavit tak, aby si heslo zapamatoval. To provedete pomocí příkazu `set password` (spuštěného z kontextu `root`). Heslo bude v tomto případě automaticky doplněno ke každému příkazu, který vyžaduje zadání hesla. eShell si heslo zapamatuje do chvíle, než bude ukončen. To znamená, že při spuštění nové relace eShell bude nutné pro zapamatování hesla opět použít příkaz `set password`.

Průvodce / nápověda

Pokud spustíte příkaz `GUIDE` nebo `HELP`, zobrazí se obrazovka prvotního spuštění s vysvětlením, jak eShell používat. Tento příkaz je dostupný výhradně z kontextu `ROOT` (`eShell>`).

Historie příkazů

eShell uchovává historii dříve provedených příkazů. Toto platí pouze pro aktuální interaktivní eShell relaci. Po ukončení eShell se historii vymaže. Pro navigaci v historii použijte klávesy šipka nahoru / dolu. Pokud najdete hledaný příkaz, můžete jej znovu spustit nebo upravit a nemusíte celý příkaz zadávat ručně.

CLS / Vymazat obrazovku

Příkaz `CLS` můžete použít na vymazání obrazovky. Funguje stejně jako v příkazovém řádku Windows nebo podobných rozhraních příkazového řádku.

EXIT / CLOSE / QUIT / BYE

Pro zavření nebo ukončení eShell použijte jakýkoli z následujících příkazů (`EXITCLOSE`, `QUIT` nebo`BYE`).

Příkazy

V této kapitole naleznete seznam základních eShell příkazů společně s popisem každého příkazu.

> Příkazy nerozlišují velikost písmen. Používat můžete velká i malá a příkaz se provede.

Vzorové příkazy, které se nachází v kontextu ROOT:

ABOUT

Zobrazí informace o programu a operačním systému. K dispozici jsou následující informace:

- Název ESET bezpečnostního řešení včetně čísla verze.
- Informace o operačním systému a hardwarových prostředcích.
- Aktuálně přihlášený uživatel (včetně domény), úplný název server (FQDN v případě domény) a název klienta na licenčním portále.
- Instalované komponenty ESET bezpečnostního řešení včetně čísla verzí.

KONTEXT:

```
root
```

PASSWORD

Z bezpečnostních důvodů je ve výchozím stavu ke spuštění příkazů chráněných heslem vyžadováno zadání hesla. Jedná se o příkazy, pomocí kterých můžete vypnout ochranu a jiným způsobem ovlivnit funkčnost ESET Server Security. Při každém spuštění takového příkazu proto budete vyzváni k zadání hesla. Abyste nemuseli heslo zadávat pokaždé, můžete jej definovat. V tomto případě si eShell heslo zapamatuje a použije jej automaticky při spuštění příkazů chráněných heslem.

> K zapamatování hesla dojde pouze pro aktuální eShell interaktivní relaci. Po ukončení eShell bude definované heslo zapomenuto. Při příštím eShell bude potřeba hesla definovat znovu.

Definování hesla je velmi užitečné při spouštění dávkových souborů / skriptů. Abyste mohli spouštět nepodepsané dávkové soubory, je nutné nastavit ESET Shell politiku na Úplný přístup. Příklad nepodepsaného dávkového souboru:

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

Pomocí výše příkazu spustíte dávkový režim, definujete heslo a vypnete ochranu.

> Podepsané dávkové soubory vám doporučujeme používat, kdykoli budete moci. Jedině tak zabráníme tomu, aby heslo nebylo ve skriptu v čitelné podobě (jako na příkladu výše). Pro více informací přejděte od kapitoly Dávkové soubory.

KONTEXT:

```
root
```

SYNTAXE:

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

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

OPERACE:

`get` – zobrazí heslo

`set` – nastaví nebo zruší heslo

`restore` – zruší heslo

ARGUMENTY:

`plain` – přepne zadání hesla jako na parametr

`password` – heslo

PŘÍKLADY:

`set password plain <yourpassword>` – nastaví heslo, které se automaticky použije při spouštění příkazů chráněných heslem

`restore password` – zruší heslo

PŘÍKLADY:

`get password` – tento příkaz použijte pro zjištění, zda je heslo definováno (zobrazí pouze hvězdičky "*", nikoli heslo v čitelné podobě). Pokud se nezobrazí hvězdičky, znamená to, že heslo není nastavené

`set password plain <yourpassword>` – Tento příkaz použijte pro definování hesla

`restore password` – tento příkaz použijte pro zrušení definovaného hesla

STATUS

Zobrazí informace o aktuálním stavu ochrany ESET Server Security a umožní dočasně pozastavit / obnovit ochranu (podobně jako v GUI).

KONTEXT:

`computer real-time`

SYNTAXE:

```
[get] status

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

restore status
```

OPERACE:

`get` – vrátí aktuální nastavení/stav

`set` – nastaví hodnotu/stav

`restore` – obnoví původní nastavení/objekt/soubor

ARGUMENTY:

`enabled` – zapne ochranu/funkci

`disabled` – vypne ochranu/funkci

`10m` – deaktivuje na 10 minut

`30m` – deaktivuje na 30 minut

`1h` – deaktivuje na 1 hodinu

`4h` – deaktivuje na 4 hodiny

`temporary4h` – deaktivuje do restartování

> Pomocí jednoho příkazu není možné vypnout všechny součásti ochrany. Spravovat jednotlivé funkce a moduly můžete samostatně prostřednictvím opakovaného použití příkazu `status`. Každá součást ochrany nebo modul má vlastní příkaz `status`.

Seznam funkcí, u kterých je dostupný příkaz `status`:

Funkce	Kontext a příkaz
Automatické výjimky	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Rezidentní ochrana souborového systému	`COMPUTER REAL-TIME STATUS`
Správa zařízení	`DEVICE STATUS`
Ochrana proti zapojení do botnetu	`NETWORK ADVANCED STATUS-BOTNET`
Ochrana proti síťovým útokům (IDS)	`NETWORK ADVANCED STATUS-IDS`
Izolace od sítě	`NETWORK ADVANCED STATUS-ISOLATION`
ESET Cluster	`TOOLS CLUSTER STATUS`
Diagnostické protokolování	`TOOLS DIAGNOSTICS STATUS`
Prezentační režim	`TOOLS PRESENTATION STATUS`
Anti-Phishingová ochrana	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Ochrana poštovních klientů	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Ochrany přístupu na web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

Jedná se o alias k příkazu `DETECTIONS`. Užitečný pro zobrazení informací týkajících se detekce.

WARNLOG

Jedná se o alias k příkazu `EVENTS`. Užitečný pro zobrazení informací o různých událostech.

Dávkové soubory / skriptování

eShell můžete použít jako skriptovací nástroj pro automatizaci. K tomu stačí vytvořit dávkový soubor, ve kterém použijete příkaz eShell.

```
✔ eshell get computer real-time status
```

Příkazy můžete v případě potřeby také řetězit. Pokud chcete například zjistit typ naplánované úlohy, zadejte

následující příkaz:

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

Výběr položky, v tomto případě úlohy s číslem 4, bude platný pouze pro aktuální instanci eShell. Pokud byste spustili oba příkazy samostatně, provedení druhého příkazu by selhalo s chybou "Nevybrali jste žádnou úlohu nebo tato úloha neexistuje".

Z bezpečnostních důvodů je ve výchozím stavu použita politika **omezeného skriptování**. Díky tomu si můžete používat eShell pro sběr dat, ale není možné prostřednictvím skriptů provádět změny v konfiguraci ESET Server Security. Při pokusu o spuštění příkazů, které mohou ovlivnit bezpečnost (například vypnutí rezidentní ochrany), se vám zobrazí zpráva **Přístup odepřen**. Abyste mohli spouštět příkazy, které mění konfiguraci produktu, doporučujeme používat podepsané dávkové soubory.

V některých případech je nutné změnit konfiguraci příkazového řádku Windows a udělit eShell oprávnění pro plný přístup. Pro přidělení úplného přístupu použijte v interaktivním režimu eShell příkaz `ui eshell shell-execution-policy`. Tuto možnost případně nastavte v **Rozšířených nastaveních** (dostupných v hlavním okně programu po stisknutí klávesy **F5**) > **Uživatelské rozhraní** > ESET Shell.

Podepsané dávkové soubory

eShell dokáže prostřednictvím podpisu zabezpečit běžné dávkové soubory (**.bat*). Skripty jsou podepsány heslem používaným pro přístup do nastavení programu. Abyste tedy mohli skripty podepisovat, je nutné nejprve zapnout ochranu nastavení. To provedete buď v rozšířených nastaveních programu nebo v eShell příkazem `set ui access lock-password`. Jakmile si nastavíte ochranu heslem, můžete začít podepisovat dávkové soubory.

> **i** Po změna hesla pro přístup do nastavení bude nutné znovu podepsat všechny dávkové soubory. V opačném případě se skript neprovede. Je to z důvodu, že heslo zadané při podepisování skriptu musí souhlasit s heslem nastaveném na cílové stanici.

Pro podepsání dávkového souboru spusťte příkaz `sign <script.bat>` z kontextu root eShell, kde *script.bat* nahraďte cestou ke skriptu, který chcete podepsat. Následně zadejte a potvrďte heslo, které budete používat k podepisování. Heslo musí odpovídat hesle použitého pro ochranu nastavení produktu. Podpis se umístí na konec dávkového souboru jako komentář. Pokud je již soubor podepsán, původní podpis se nahradí.

> **i** Pokud změníte již dříve podepsaný dávkový soubor, bude nutné jej podepsat znovu.

Pro spuštění podepsaného dávkového souboru z Příkazového řádku nebo prostřednictvím Plánovače použijte následující příkaz:

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

Kde script.bat je cesta k dávkovému souboru.

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

ESET SysInspector

ESET SysInspector je aplikace, která důkladně zkontroluje počítač a shromáždí podrobné informace o součástech systému, jako jsou nainstalované ovladače a aplikace, síťová připojení nebo důležité položky registru, a vyhodnotí jejich rizikovost.

Tyto informace mohou být užitečné při zjišťování příčiny podezřelého chování systému ať už vlivem nekompatibility software/hardware nebo infekce škodlivým kódem.

Klikněte na tlačítko **Vytvořit** a zadejte krátký **komentář** popisující protokol. Následně vyčkejte na vytvoření ESET SysInspector protokolu (ve sloupci Stav se zobrazí informace Vytvořeno). Vytvoření protokolu může v závislosti na výkonu počítače a množství dat v systému chvíli trvat.

V okně ESET SysInspector se nachází informace o vytvořených protokolech:

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

Dostupné jsou následující akce:

- **Zobrazit** – zobrazí vytvořený záznam. Případně klikněte pravým tlačítkem na vybraný záznam a z kontextového menu vyberte možnost Zobrazit.
- **Porovnat** – porovná dva vytvořené záznamy.
- **Vytvořit** – vytvoří nový záznam. Klikněte na tlačítko **Vytvořit** a zadejte krátký komentář popisující protokol. Následně vyčkejte na vytvoření protokolu ESET SysInspector (ve sloupci **Stav** se zobrazí informace Vytvořeno).
- **Odstranit**– kliknutím odeberete vybraným záznam ze seznamu.

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

- **Zobrazit** – otevře vybraný protokol v ESET SysInspector (stejné jako dvojklik na vybraný záznam),
- **Porovnat** – porovná dva vytvořené záznamy.
- **Vytvořit** – vytvoří nový záznam. Klikněte na tlačítko **Vytvořit** a zadejte krátký komentář popisující protokol. Následně vyčkejte na vytvoření protokolu ESET SysInspector (ve sloupci **Stav** se zobrazí informace Vytvořeno).
- **Odstranit**– kliknutím odeberete vybraným záznam ze seznamu.
- **Odstranit vše** – vymaže všechny záznamy.
- **Exportovat** – uloží záznamy do souboru *.xml* nebo do archivu *.zip*.

ESET SysRescue Live

ESET SysRescue Live je bezplatný nástroj, který umožňuje vytvořit záchranné bootovací médium (CD, DVD nebo USB). Infikovaný počítač můžete spustit ze záchranného média, vyhledat škodlivý kód a vyčistit infikované soubory.

Hlavní výhodou ESET SysRescue Live je, že bezpečnostní řešení ESET běží nezávisle na hostitelském operačním systému, ale má přímý přístup k disku a souborovému systému. To mu umožňuje odstranit hrozby, které by normálně nemohly být odstraněny (například když je spuštěn operační systém atd.).

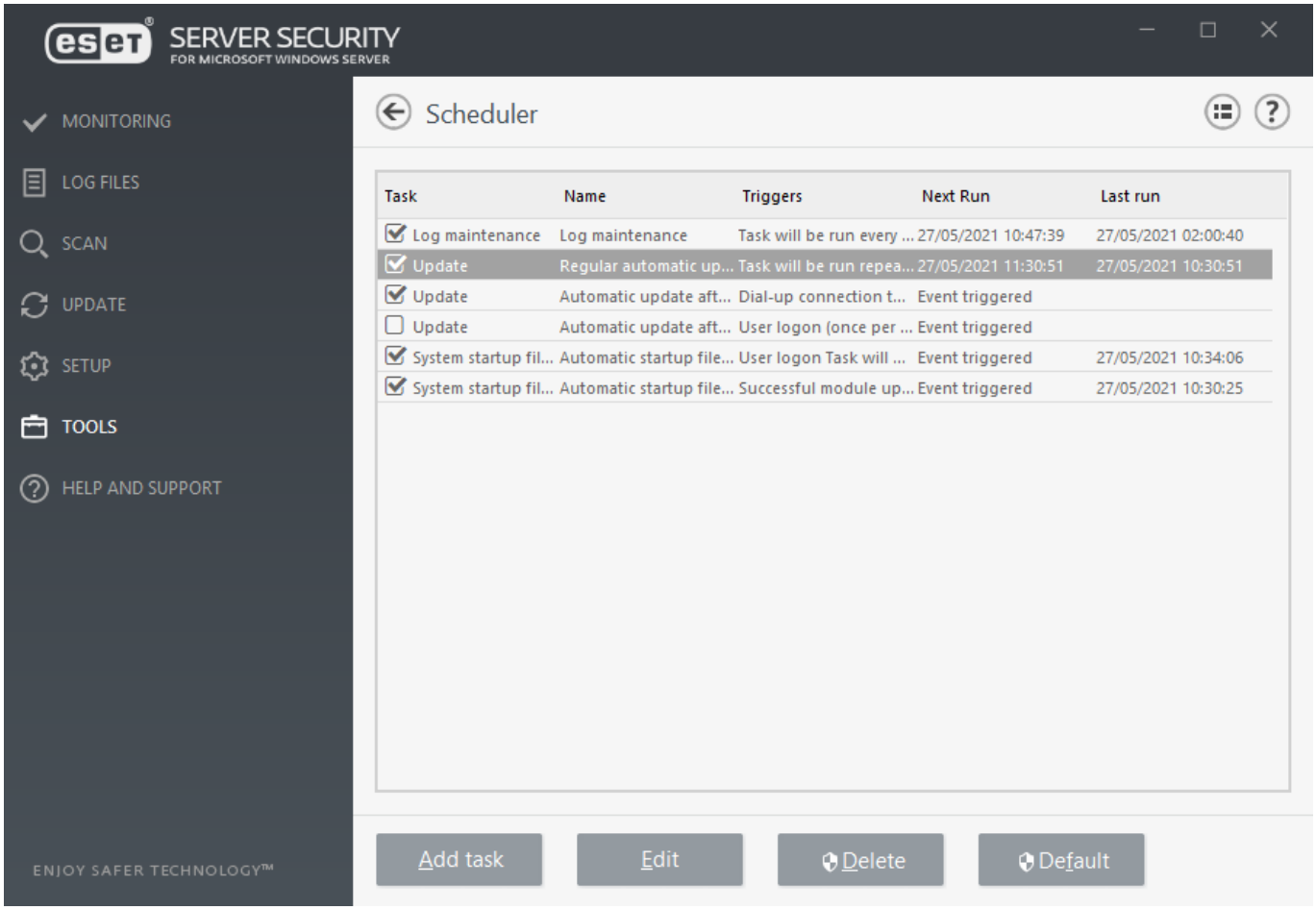
Plánovač

Plánovač spravuje a spouští naplánované úlohy s předem nakonfigurovaným nastavením. Plánovač obsahuje přehledný seznam všech naplánovaných úloh, jejich nastavení a vlastností, které se provádějí ve stanovený čas pomocí definovaných profilů. Novou úlohu můžete vytvořit po kliknutí na tlačítko Přidat úlohu. Pro úpravu již existující vyberte úlohu a klikněte na tlačítko **Změnit**. Pokud jste úlohy modifikovali, kliknutím na tlačítko **Standardní** a potvrzením kliknutím na **Obnovit na standardní zahodíte provedené změny. Zároveň dojde k odstranění** všech vámi vytvořených úloh.

K dispozici jsou tyto předdefinované typy úloh:

- Údržba protokolů
- Pravidelná automatická aktualizace (tuto úlohu použijte pro změnu intervalu aktualizace)
- Automatická aktualizace po modemovém spojení
- Automatická aktualizace po přihlášení uživatele
- Kontrola souborů spouštěných po startu (při přihlášení uživatele)
- Kontrola souborů spouštěných po startu (při úspěšné aktualizaci modulů)

Pomocí zaškrtávacího pole úlohu aktivujete/deaktivujete.



Po kliknutí pravým tlačítkem na úlohu se zobrazí kontextové menu, ve kterém jsou dostupné tyto akce:

Zobrazit detaily úlohy	**Zobrazí detailní informace o naplánované úloze.**
Spustit nyní	Spustit vybranou úlohu a provedení definované akce.
Přidat…	Otevře průvodce vytvořením nové naplánované úlohy.
Změnit…	Kliknutím upravíte parametry existující úlohy.
Odstranit	Kliknutím odstraníte existující úlohu.

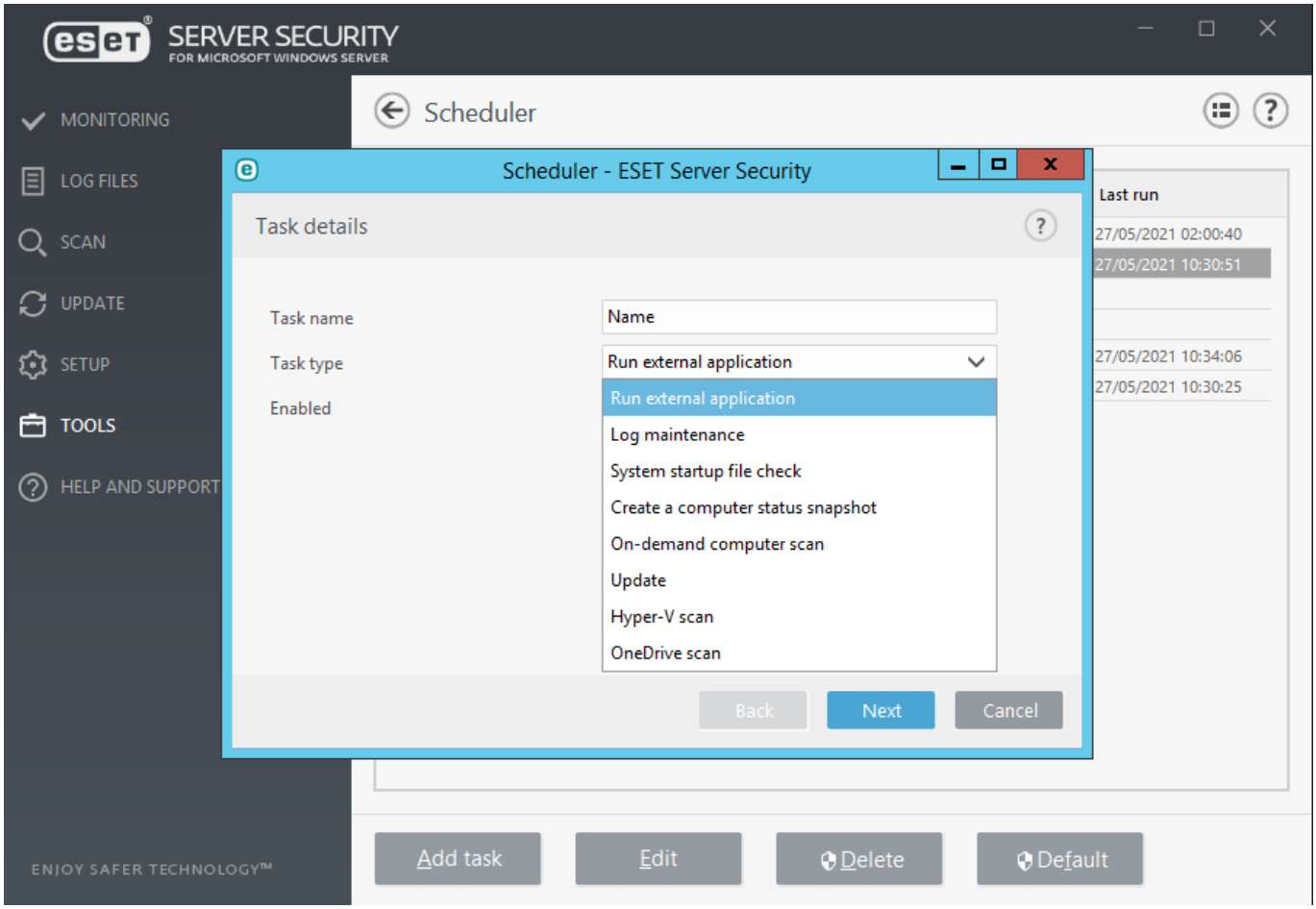
Vytvoření naplánované úlohy

Pro vytvoření nové naplánované úlohy:

1. Klikněte na tlačítko **Přidat**.

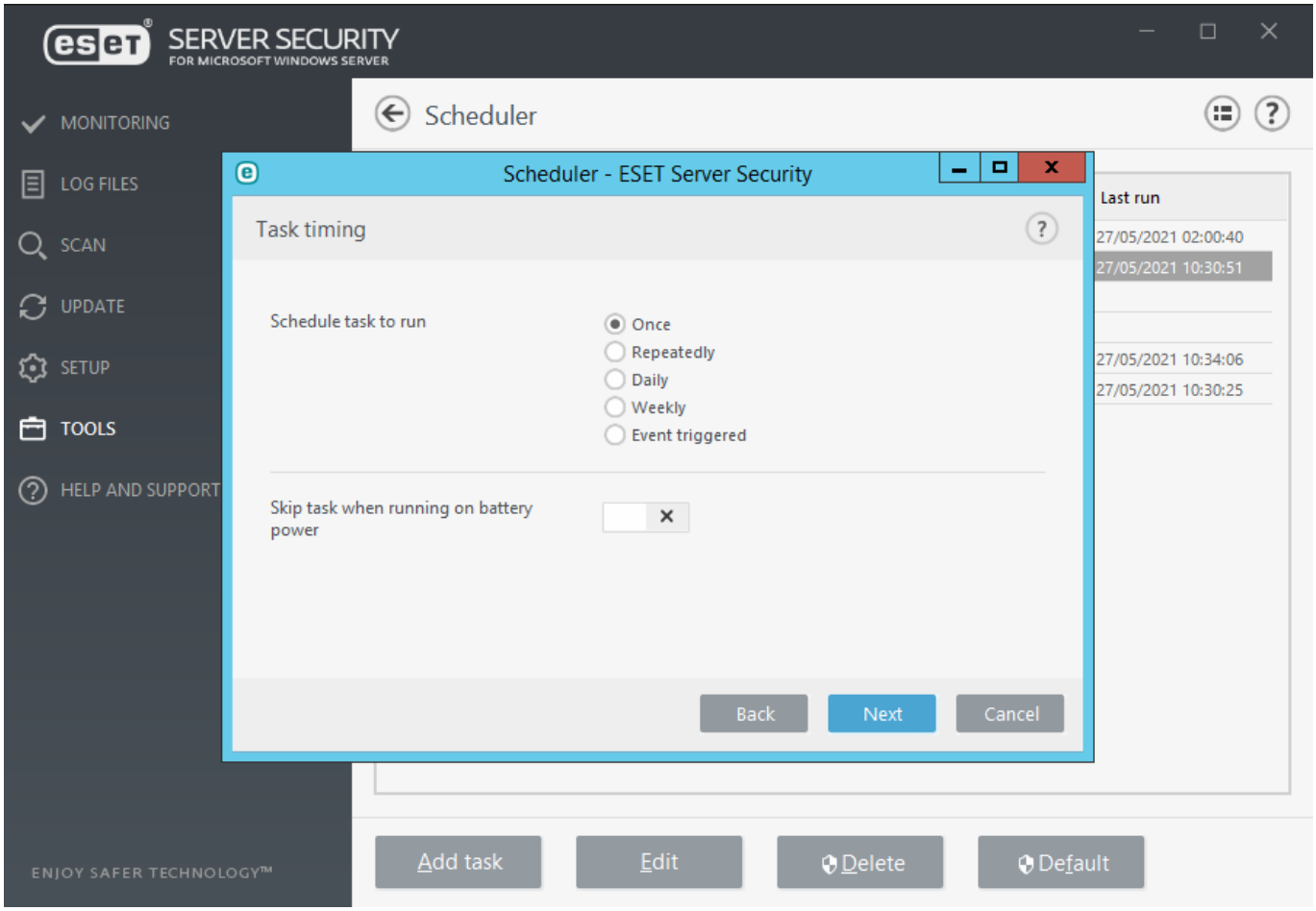
2. Zadejte **název úlohy** a nastavte její parametry.

3. Z rozbalovacího menu **vyberte** typ úlohy.

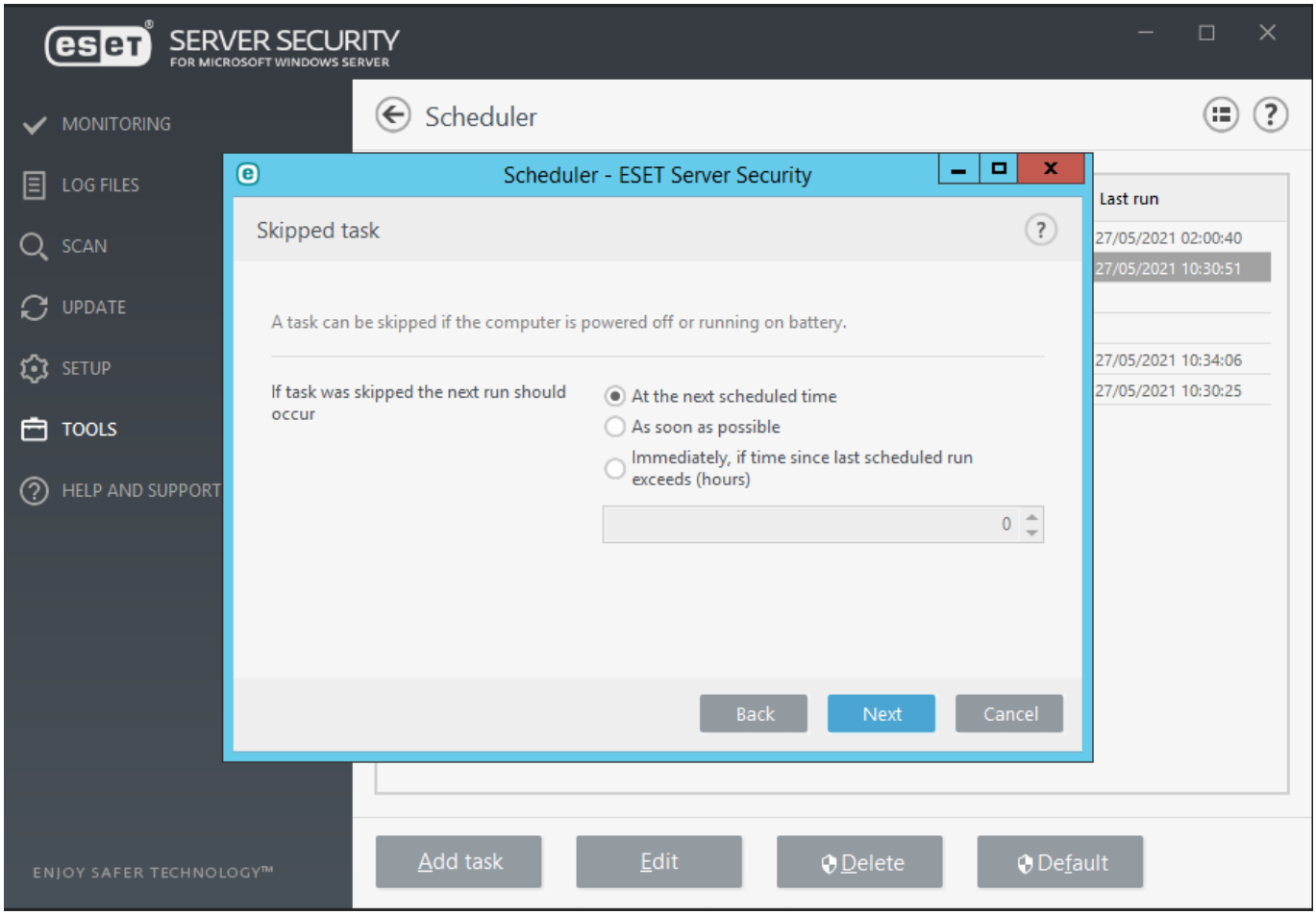


Pokud si úlohu zatím chcete jen připravit, pomocí přepínače **Zapnuto** úlohu deaktivujte. Kdykoli ji můžete aktivovat později v Plánovači.

4. Provedení úlohy – v tomto dialogovém okně se rozhodněte, kdy (jak často) chcete úlohu spoustit. V závislosti na výběru budete v dalším kroku vyzváni k zadání konkrétního data a času, intervalu opakování nebo výběru události.



5. Neprovedení úlohy – v případě, že se naplánovanou úlohu nepodaří spustit v určeném čase (počítač byl vypnutý nebo běžel na baterii), můžete nastavit způsob, jak program bude postupovat.***



6. Spuštění aplikace – pokud jste jako typ úlohy vybrali spuštění aplikace, v této části vyberte spustitelný soubor.

7. Pokud potřebujete provést změny v konfiguraci úlohy, můžete se kdykoli vrátit pomocí tlačítka **Zpět**.

8. Pro dokončení klikněte na tlačítko **Dokončit**.

Vytvořená úloha se zobrazí v seznamu naplánovaných úloh

Typ úlohy

Průvodce vytvořením úlohy se liší v závislosti na typu úlohy Zadejte **název úlohy** a z rozbalovací nabídky vyberte její **typ**:

- **Spuštění externí aplikace** – poskytne výběr aplikace, kterou má plánovač spustit.
- **Údržba protokolů** – defragmentace odstraní prázdné záznamy v protokolech. Viditelné zlepšení práce s protokoly po optimalizaci je především při větším množství záznamů v protokolech.
- **Kontrola souborů spouštěných při startu** – kontroluje soubory, které se spouštějí při startu nebo po přihlášení do systému.
- **Vytvoření záznamu o stavu počítače** – vytvoří záznam systému pomocí ESET SysInspector, který slouží k důkladné kontrole stavu počítače a umožňuje zobrazit získané údaje v jednoduché a čitelné formě.
- **Volitelná kontrola počítače** – provede volitelnou kontrolu disků, jednotlivých složek a souborů na počítači.

- **Aktualizace** – zajišťuje aktualizaci detekčního jádra a programových modulů.
- **Hyper-V kontrola** – provede kontrolu Hyper-V virtuálních disků.
- **OneDrive kontrola** – pomocí této možnosti si můžete naplánovat kontrolu souborů uložených na OneDrive.

Pokud si úlohu zatím chcete jen připravit, pomocí přepínače **Zapnuto** úlohu deaktivujte. Kdykoli ji můžete aktivovat později v Plánovači. Kliknutím na tlačítko **Další** přejděte na další krok.

Opakování úlohy

Vyberte jednu z níže uvedených možností:

- **Jednou** – úloha se provede pouze jednou v naplánovaném čase. Tuto možnost využijte pro jednorázové spuštění úlohy. Po vybrání této možnosti definujte datum a čas pro **spuštění úlohy**.
- **Opakovaně** – úloha se bude provádět opakovaně každých x minut. Po vybrání této možnosti definujte **interval**, po jehož uplynutí se úloha spustí.
- **Denně** – úloha se provede každý den ve stanový čas.
- **Týdně** – úloha bude provedena v určitý den v týdnu ve stanovený čas. Tuto možnost využijte pro opakované spouštění úlohy v konkrétní den a čas. Nejprve vyberte čas, ve kterém chcete úlohu spustit. Poté vyberte den nebo dny v týdnu, ve kterých chcete úlohu spustit.
- Při události – Úloha bude provedena po výskytu konkrétní události.

Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii, aktivujte možnost **Nespouštět úlohu, pokud je počítač napájen z baterie**. Totéž platí pro počítač běžící na UPS.

Při události

Pokud plánujete provedení úlohy při události, můžete definovat minimální interval mezi dvěma provedeními úlohy.

Úlohu může spustit kterákoli z následujících událostí:

- Při každém startu počítače
- Při prvním startu počítače během dne
- Při modemovém připojení na internet/připojení do VPN
- Při úspěšné aktualizaci modulů
- Při úspěšné aktualizaci programu
- Přihlášení uživatele – úloha se provede při přihlášení uživatele do systému. Pokud se přihlašujete na počítač vícekrát za den, nastavením intervalu provedení na 24 hodin se tato úloha spustí pouze při prvním přihlášení a poté až následující den.

- Při detekci hrozby

Spuštění aplikace

Výběr a nastavení parametrů aplikace, která má být spuštěna plánovačem.

- **Spustitelný soubor** – vyberte spustitelný soubor nebo zadejte cestu k souboru ručně.
- **Pracovní složka** – definuje pracovní složku externí aplikace. Všechny dočasné soubory související se spustitelným souborem budou vytvořeny v této složce.
- **Parametry** – parametry příkazového řádku s nimiž bude aplikace spuštěna (nepovinné).

Neprovedení úlohy

V případě, že se naplánovanou úlohu nepodaří spustit v určeném čase (počítač byl vypnutý nebo běžel na baterii), můžete nastavit způsob, jak program bude postupovat:

- **Při dalším naplánovaném termínu** – úloha bude provedena v dalším naplánovaném termínu (například za 24 hodin).
- **Jakmile to bude možné** – úloha se provede okamžitě nebo vzápětí po odstranění problémů, které bránily spuštění dané úlohy.
- **Ihned, pokud čas od posledního spuštění překročí zadanou hodnotu** – Čas od posledního spuštění (v hodinách). Po výběru této možnosti se bude úloha automaticky spouštět znovu ve frekvenci, kterou zadáte (v hodinách).

Přehled naplánované úlohy

V tomto dialogovém okně naleznete detailní informace o vybrané úloze. Zobrazit jej můžete dvojklikem na danou úlohu v**plánovači** nebo kliknutím pravým tlačítkem na úlohu a vybráním možnosti **Zobrazit detaily úlohy** ze zobrazeného kontextového menu.

Odeslat soubor k analýze

Prostřednictvím tohoto dialogového okna můžete zaslat vzorek nebo webovou stránku k analýze do společnosti ESET. V případě, že máte soubor s podezřelým chováním nebo jste narazili na infikovanou stránku, můžete tato data odeslat na analýzu do virové laboratoře ESET. Pokud se ukáže, že se jedná o nebezpečnou aplikaci nebo webovou stránku, její detekce bude přidána v některé z nejbližších aktualizací.

Případně můžete soubory odesílat e-mailem. Pokud dáváte přednost této možnosti, prosím dbejte na to, abyste soubor přidali do archivu WinRAR/ZIP a ochránili archiv heslem `infected` předtím, než jej odešlete na adresu samples@eset.com. Prosím, uveďte také co nejvíce informací o zahrnující výrobce, verzi produktu a také internetové adrese, ze které jste aplikaci (resp. soubor) stáhli.

Před odesláním souboru do společnosti ESET se ujistěte, že splňuje alespoň jedno z následujících kritérií:

- soubor není programem ESET detekován
- soubor je detekován nesprávně jako hrozba

Pokud nebude splněna alespoň jedna z výše uvedených podmínek, neobdržíte žádnou odpověď, dokud tyto informace neposkytnete.

Z rozbalovacího menu **Důvod odeslání souboru** vyberte možnost, která nejlépe vystihuje danou situaci:

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

Soubor/Stránka

Cesta k souboru nebo webové stránce, kterou chcete zaslat k analýze.

Kontaktní e-mail

Na tento e-mail vás budou pracovníci virové laboratoře ESET kontaktovat, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné. Mějte na paměti, že pokud nebudeme od vás požadovat další informace, neobdržíte od nás žádnou zpětnou vazbu. Je to z důvodu, že denně do společnosti ESET chodí několik desítek tisíc souborů a není možné na každý e-mail reagovat.

Odeslat anonymně

Po vybráním možnosti **Odeslat anonymně** nebude vyžadováno zadání vaší e-mailové adresy.

Podezřelý soubor

Pozorované projevy a příznaky infekce

Uveďte, prosím, co nejdetailnější popis chování souboru v systému pro přesnější analýzu souboru.

Původ souboru (URL adresa nebo výrobce aplikace)

Uveďte původ, zdroj, výrobce souboru (pokud je znám), pro jeho lepší identifikaci, a způsob, jak se k vám dostal.

Poznámky a doplňující informace

Zde můžete uvést veškeré další informace, které by mohly pomoci při identifikaci a zpracování souboru.

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

Podezřelá stránka

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

Infikovaná

Webová stránka obsahuje viry nebo jiný škodlivý kód.

Phishing

Často využíván pro získání citlivých jako jsou číslo bankovních účtů, PIN kódy a další citlivé informace. Více informací o tomto typu útoku naleznete ve slovníku pojmů.

Scam

Podvodné webové stránky vytvořené za účelem rychlého zisku.

Ostatní

Tuto možnost vyberte, pokud žádná z výše uvedených neodpovídá obsahu stránky.

Poznámky a doplňující informace

Zadáním dalších informací a popisu pomůžete při analyzování podezřelé stránky.

Falešně detekovaný soubor

Prosíme vás, abyste nám zasílali soubory, které byly detekovány jako škodlivé, ale ve skutečnosti nejsou. Pomůžete nám tak vylepšit detekční jádro a zvýšit účinnost ochrany pro ostatní uživatele. Falešný poplach (False positive, zkráceně FP) může nastat, když struktury souboru mají stejné charakteristiky jako vzorky obsažené v detekčním jádru.

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

Název a verze aplikace

Název a verze pro identifikaci aplikace (například číselné označení, alias, kódový název).

Původ souboru (URL adresa nebo výrobce aplikace)

Uveďte původ, zdroj, výrobce souboru (pokud je znám), pro jeho lepší identifikaci, a způsob, jak se k vám dostal.

Účel aplikace

Charakterizujte účel a typ aplikace (např. prohlížeč, přehrávač médií, …) pro rychlejší zařazení a identifikaci.

Poznámky a doplňující informace

Zadáním dalších informací a popisu pomůžete při analyzování podezřelého souboru.

Falešně detekovaná stránka

Při odesílání stránky, která je falešně detekována jako infikovaná, scam nebo phishing, ale ve skutečnosti není, vyžadujeme zadání dalších informací. Falešný poplach (False positive, zkráceně FP) může nastat, když struktury stránky mají stejné charakteristiky jako vzorky obsažené v detekčním jádru. Poskytnutím těchto informací pomůžete vylepšit naše detekční jádro a zvýšit účinnost ochrany pro ostatní uživatele.

Poznámky a doplňující informace

Zadáním dalších informací a popisu pomůžete při analyzování podezřelého souboru.

Ostatní

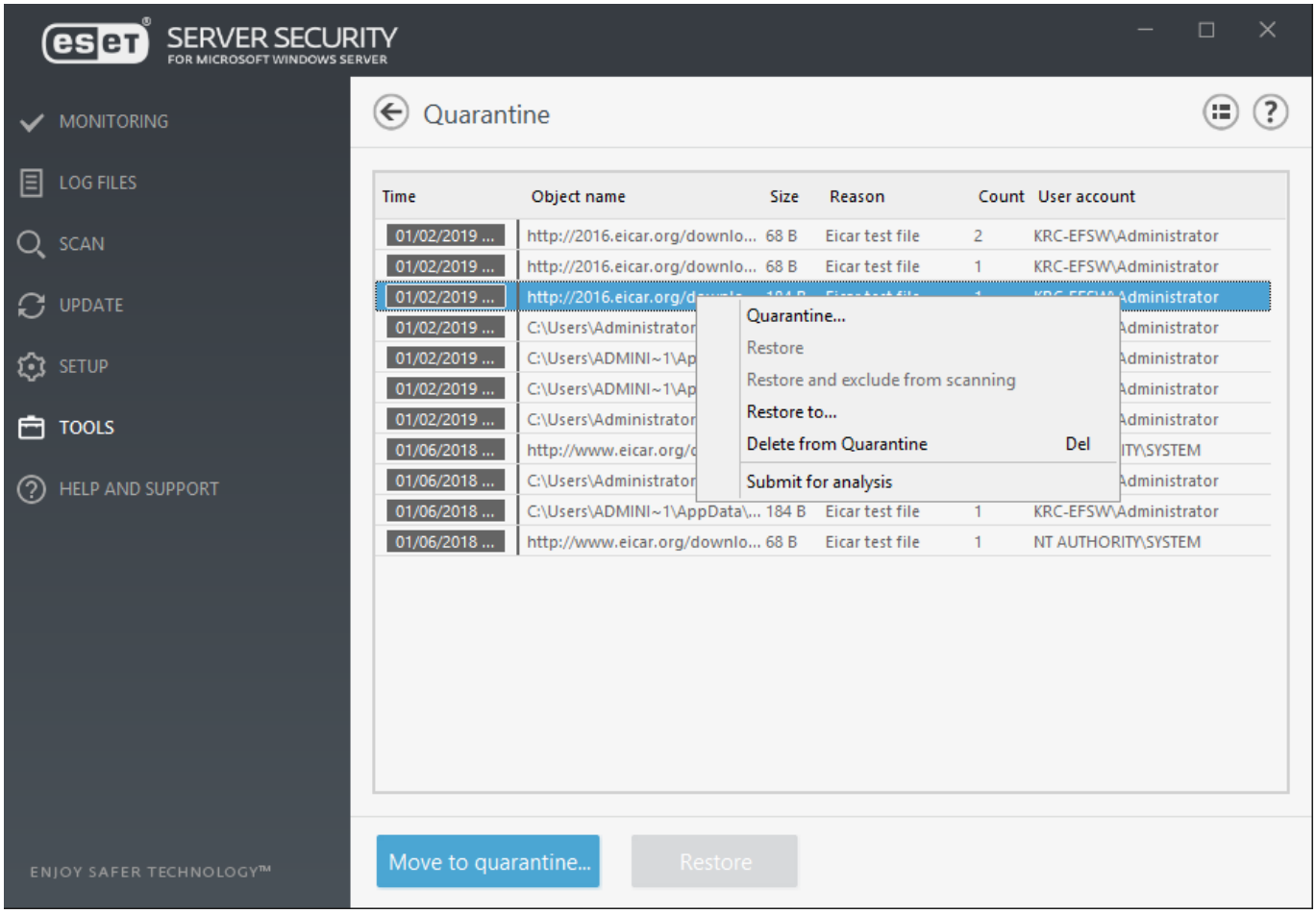
Tento formulář použijte v případě, že soubor nevyhovuje definici Podezřelý soubor nebo Falešný poplach.

Důvod odesílání souboru

Uveďte prosím důvod odeslání souboru a co nejpřesnější popis souboru.

Karanténa

Hlavní funkcí karantény je bezpečně uschovat infikované soubory. Soubory jsou uloženy do karantény produktu ESET Server Security v případě, že nemohou být léčeny, pokud není bezpečné a doporučené jejich odstranění (systémové soubory) nebo pokud byly detekovány nesprávně (tzv. falešný poplach). Do karantény můžete také ručně přidat libovolný soubor. Tento postup je vhodný, pokud soubor vykazuje podezřelou aktivitu, ale nebyl zachycen detekčním jádrem. Soubory v karanténě můžete následně odeslat na analýzu do virové laboratoře ESET.



Soubory uložené v karanténě si můžete prohlédnout v přehledné tabulce včetně informací o datu a čase přidání souboru do karantény, cesty k původnímu umístění souboru, jeho velikosti v bajtech, důvodu, proč byl přidán do karantény (např. objekt přidaný uživatelem), a počtu infiltrací (např. pokud archiv obsahoval více infikovaných souborů).

V případě e-mailových objektů je zobrazena cesta ve formátu poštovní schránka/složka/název souboru.

Přidání do karantény

ESET Server Security automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nevypnuli v okně s upozorněním). Pokud uznáte za vhodné, může pomocí tlačítka **Přidat do karantény…** do karantény přidat podezřelý soubor ručně. V takovém případě se soubor ze svého původního umístění smaže. Stejná možnost je dostupná v kontextovém menu **Karantény**, kdy vyberte rovněž možnost **Přidat do karantény…**.

Obnovení z karantény

Soubory uložené v karanténě můžete vrátit do jejich původního umístění, odkud byly vymazány. Můžete použít funkci **Obnovit**, která je dostupná z kontextového menu po kliknutí pravým tlačítkem myši na daný soubor v okně karantény. Pokud se jedná o potenciálně nechtěnou aplikaci, v takovém případě bude v kontextovém menu dostupná možnost **Obnovit a vyloučit z kontroly**. Kontextová nabídka nabízí také možnost **Obnovit do**, která umožňuje obnovit soubor do jiného umístění, než ze kterého byl odstraněn.

Pokud program do karantény umístil soubor z důvodu falešného poplachu, vytvořte pro něj výjimku z kontroly a zašlete jej na technickou podporu společnosti ESET.

Odeslání souboru z karantény k analýze

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

Odstranění souboru z karantény

Klikněte pravým tlačítkem myši na požadovaný objekt a z kontextového menu vyberte možnost **Odstranit z karantény**. Případně na klávesnici stiskněte klávesu **Delete**.

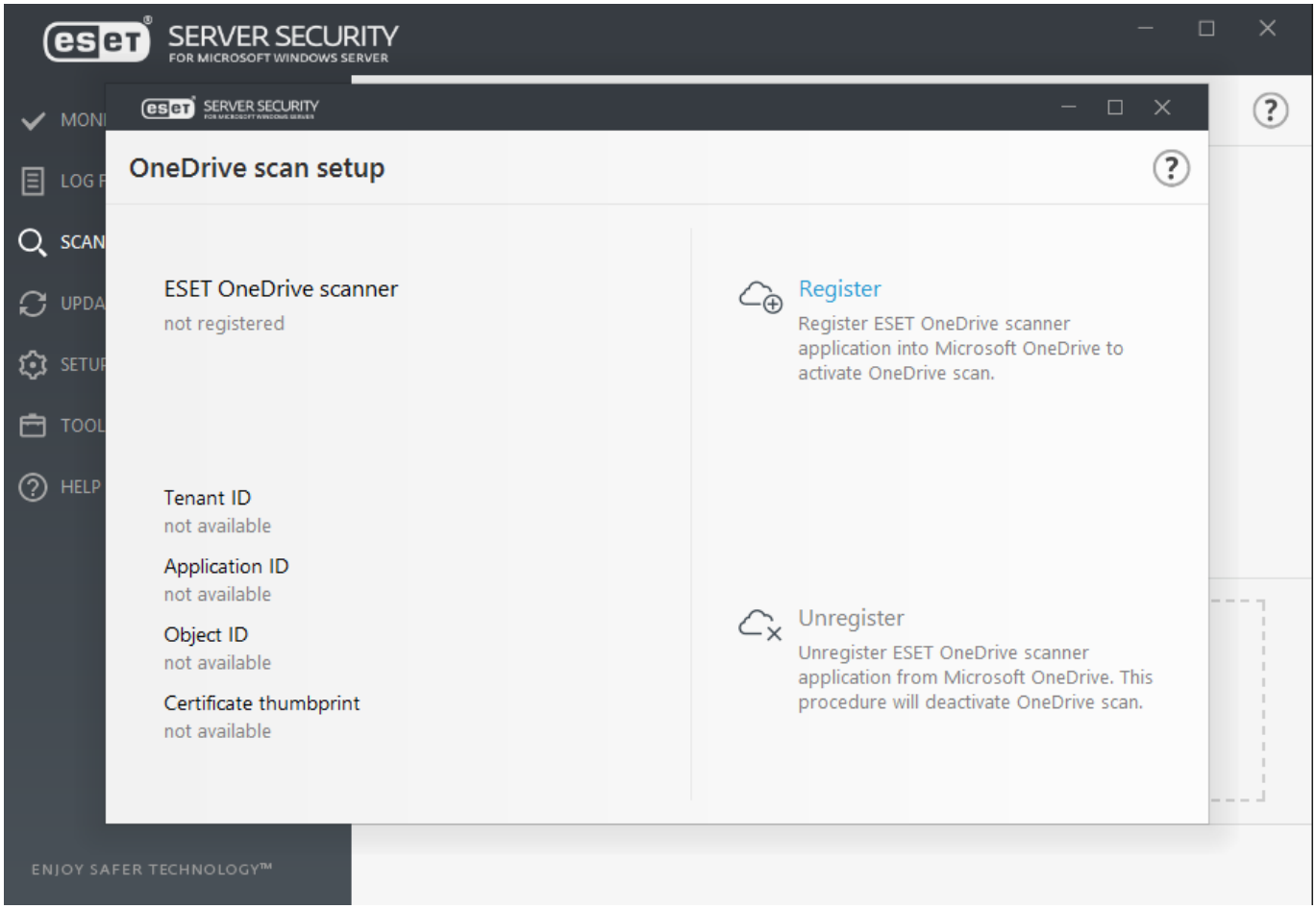
Nastavení OneDrive kontroly

Prostřednictvím této funkce můžete kontrolovat soubory uložené v cloudovém úložišti Microsoft OneDrive for Business. OneDrive kontrola produktu ESET Server Security dokáže zpracovat výhradně soubory a složky, neposkytuje kontrolu dalších typů dat, jako jsou e-maily, SharePoint soubory, kontakty nebo kalendáře.

Rychlé odkazy

- Registrace aplikace ESET OneDrive skener
- Odregistrace aplikace ESET OneDrive skener

Pro využívání OneDrive kontroly produktem ESET Server Security, zaregistruje aplikaci ESET OneDrive skener do svého Microsoft OneDrive / Microsoft Office 365 / Microsoft Azure účtu. V dialogovém okně Nastavení OneDrive kontroly naleznete informace o stavu registrace, případně ESET OneDrive skener můžete zaregistrovat nebo odregistrovat. Pokud již byla provedena zobrazí se zde tenant ID, ID aplikace, ID objektu a otisk certifikátu. Pomocí této možnosti můžete zaregistrovat nebo odregistrovat ESET OneDrive skener:



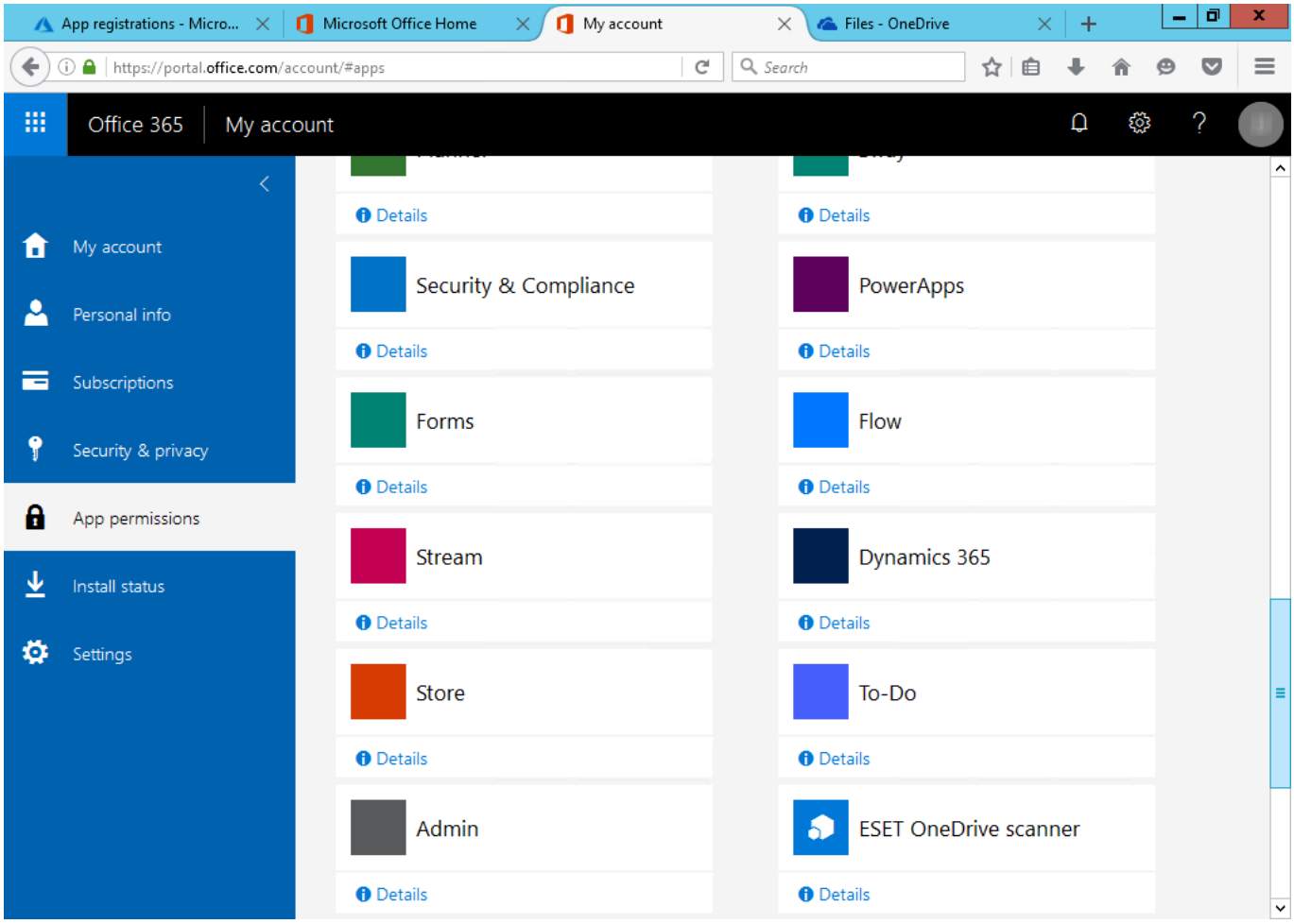
Po úspěšné registraci se v hlavním okně programu v sekci Kontrola zobrazí možnost pro spuštění OneDrive kontroly. Po jejím vybrání se zobrazí seznam uživatelů se stromovou strukturou, kterou je možné zkontrolovat. Prostřednictvím OneDrive kontroly prováděné produktem ESET Server Security můžete zkontrolovat všechny soubory, které mají uživatelé uloženy na OneDrive for Business.

ESET Server Security v průběhu OneDrive kontroly stahuje soubory z cloudového úložiště OneDrive for Business a jejich kontrolu provádí lokálně. Po dokončení kontroly jsou stažené soubory smazány. Mějte na paměti, že stahování velkého objemu dat z OneDrive bude mít dopad na síťový provoz.

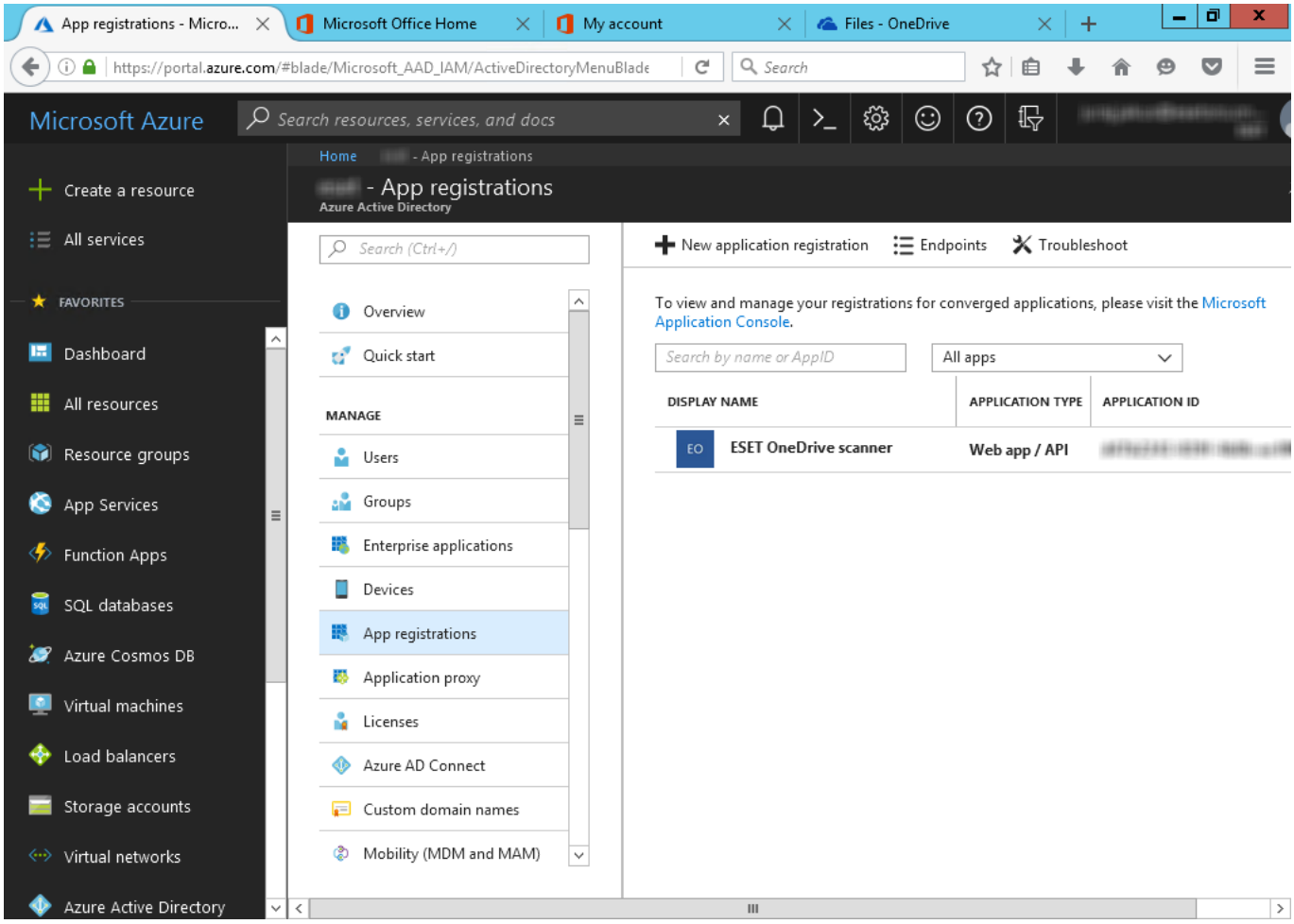
Přeregistrace k jinému účtu: Pokud se rozhodnete ESET Server Security OneDrive skener zaregistrovat do jiného Microsoft OneDrive for Business / Office 365 účtu, nejprve ze stávajícího účtu ESET OneDrive skener odregistrujte a následně proveďte registraci do nového Microsoft OneDrive for Business / Office 365 účtu.

Zaregistrovanou aplikaci ESET OneDrive skener naleznete na portále Office 365 a Azure. Pro její zobrazení postupujte podle následujících kroků:

Office 365 portál – v sekci My account klikněte na **App permissions**. Následně v seznamu aplikací najděte ESET OneDrive scanner.



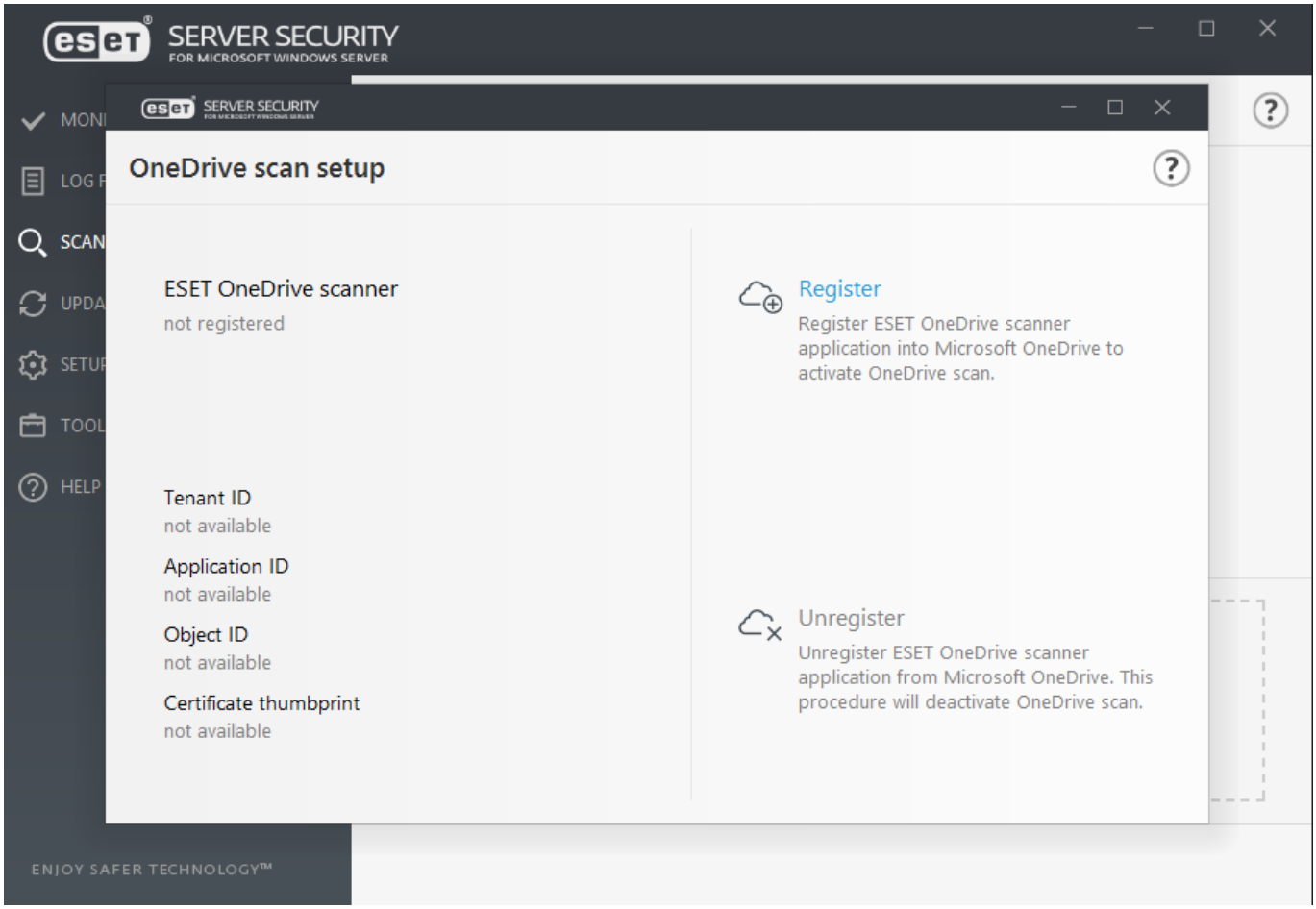
Azure – na portále přejděte do sekce **Azure Active Directory** > **App registrations**, klikněte na tlačítko **View all applications**. V seznamu aplikací najděte ESET OneDrive scanner. Pro zobrazení detailních informací klikněte na název aplikace.



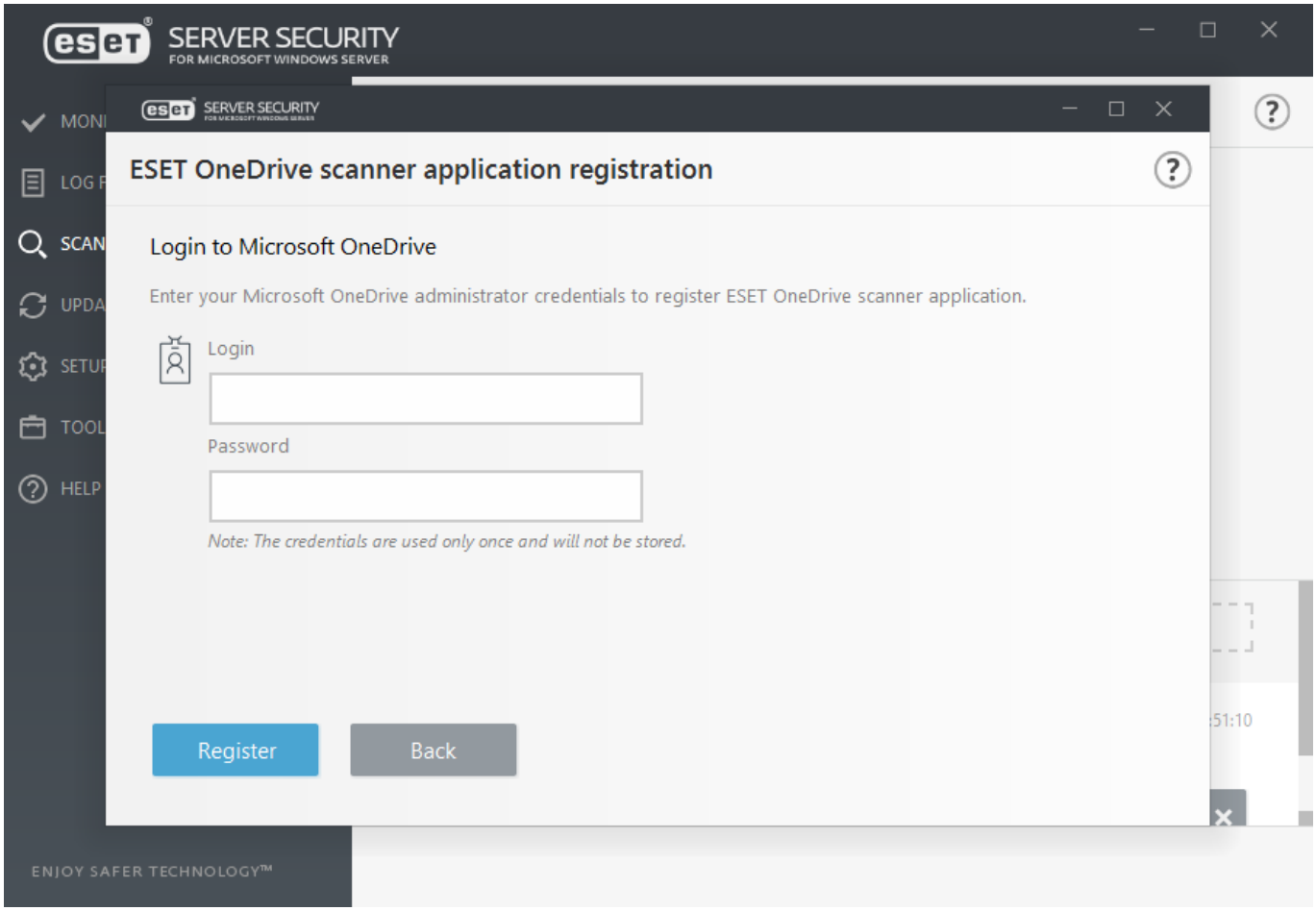
Registrace aplikace ESET OneDrive skener

Pomocí níže uvedených kroků zaregistrujete aplikaci ESET OneDrive scanner do vašeho Microsoft OneDrive / Office 365 / Azure účtu:

1. Pro spuštění průvodce registrací vyberte možnost **Registrovat**.

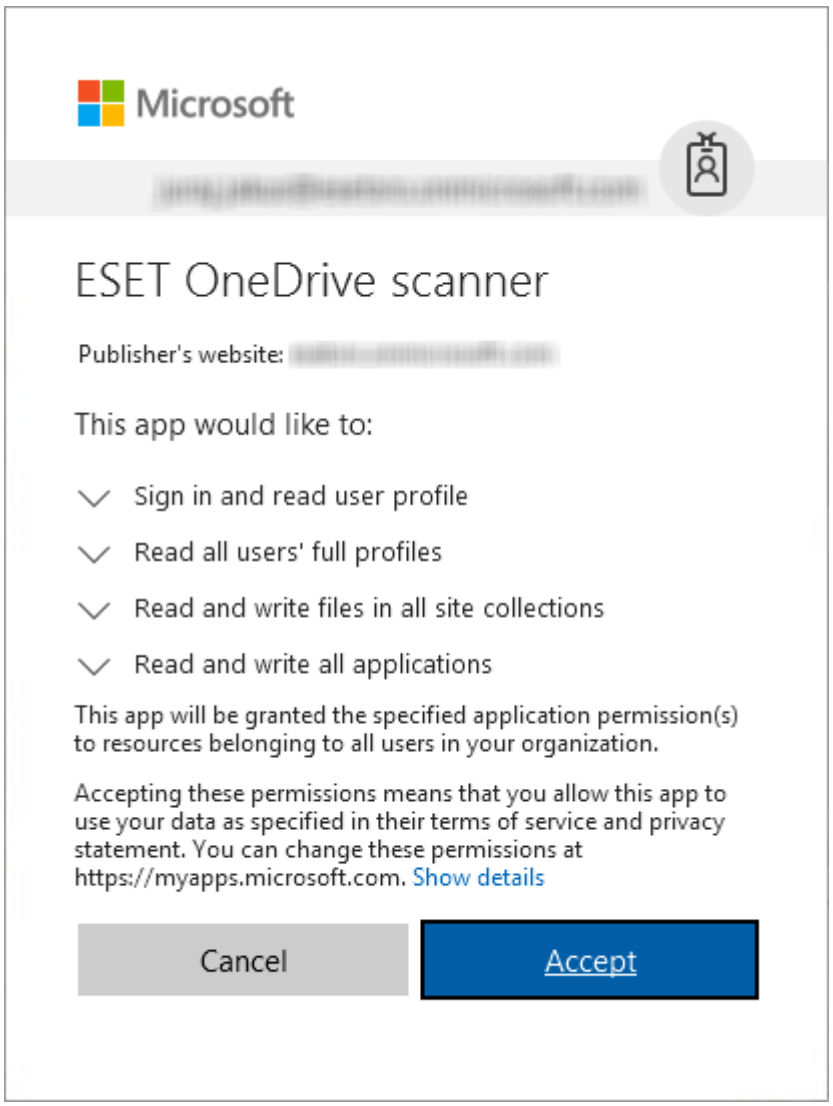


2. V zobrazeném dialogovém okně zadejte přihlašovací údaje Microsoft OneDrive / Office 365 administrátora. Vyčkejte na dokončení registrace ze strany Microsoft OneDrive.



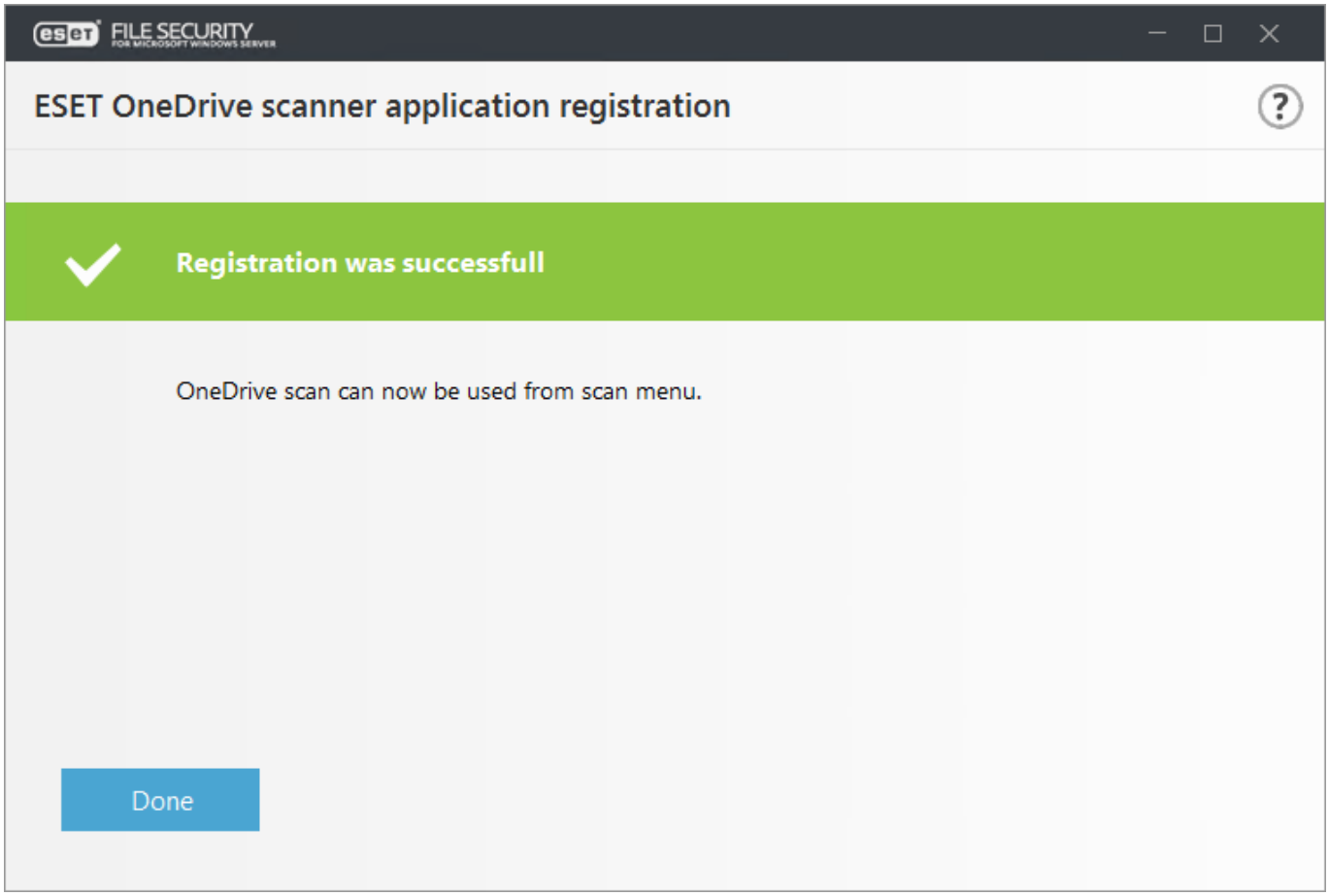
3. Následně se v internetovém prohlížeči otevře webová stránka (**Pick an account**) společnosti Microsoft. Vyberte účet, který chcete použít, případně znovu zadejte údaje Microsoft OneDrive / Office 365 administrátora, a klikněte na tlačítko **Přihlásit se**.

4. Dále se zobrazí seznam oprávnění, která aplikace ESET OneDrive scanner vyžaduje. Kliknutím na tlačítko **Přijmout** umožníte OneDrive skeneru produktu ESET Server Security přístup k datům uloženým ve vašem cloudovém úložišti OneDrive.



5. Pokud se prohlížeč dotáže na odeslání informací, klikněte na tlačítko **Continue** (data jsou odeslána pouze na server, kde běží ESET Server Security a OneDrive tímto způsobem oznamuje produktu úspěšnou registraci).

6. Po uzavření internetového prohlížeče zobrazí průvodce registrací ESET OneDrive skener informaci o úspěšné registraci. Klikněte na **Hotovo**.



Proces registrace aplikace ESET OneDrive scanner se může drobně lišit, v závislosti na tom, zda jste přihlášení na některém z portálů společnosti Microsoft (OneDrive, Office 365, Azure, ...) jako administrátor, nebo nikoli. V průběhu registrace postupujte podle instrukcí zobrazených na obrazovce.

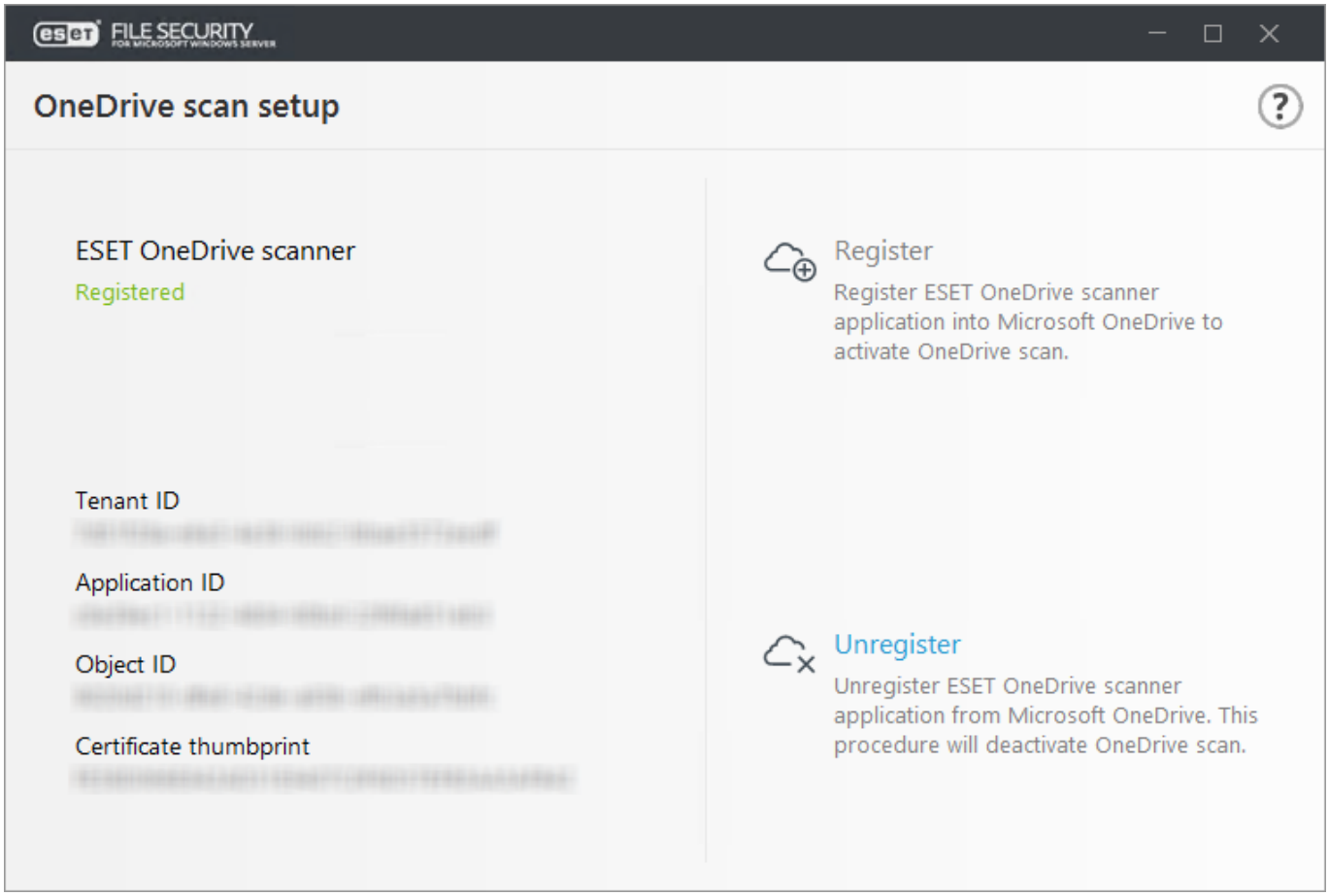
Pokud se vám v průběhu registrace aplikace ESET OneDrive scanner zobrazí některé z níže uvedených chybových hlášení, vyzkoušejte pro vyřešení situace navržené řešení.

Chybová zpráva	Detaily chybové zprávy
Vyskytla se neočekávaná chyba.	Může se jednat o chybu v produktu ESET Server Security. Zkuste spustit registraci aplikace ESET OneDrive scanner později. V případě přetrvávajících potíží kontaktujte technickou ESET Technickou podporu.
Nelze se připojit k Microsoft OneDrive.	Zkontrolujte připojení k internetu a spusťte znovu registraci aplikace ESET OneDrive scanner.
Microsoft OneDrive vrátil neočekávanou chybu.	Microsoft OneDrive server vrátil HTTP 4xx chybu bez bližší chybové zprávy. V případě přetrvávajících potíží kontaktujte technickou ESET Technickou podporu.
Microsoft OneDrive vrátil následující chybu.	Microsoft OneDrive server vrátil konkrétní chybovou zprávu. Pro více informací klikněte na Zobrazit chybu.
Platnost konfigurační úlohy vypršela.	Konfigurační úloha na registraci aplikace ESET OneDrive scanner běžela příliš dlouho. Zkuste spustit registraci aplikace ESET OneDrive scanner později.
Konfigurační úloha byla zrušena.	Přerušili jste běh konfigurační úlohy pro registraci aplikace. Pokud chcete registraci dokončit, spusťte úlohu na registraci ESET OneDrive skeneru znovu.
Probíhá jiná konfigurační úloha.	Již běží jiná konfigurační úloha na registraci aplikace. Vyčkejte na její dokončení.

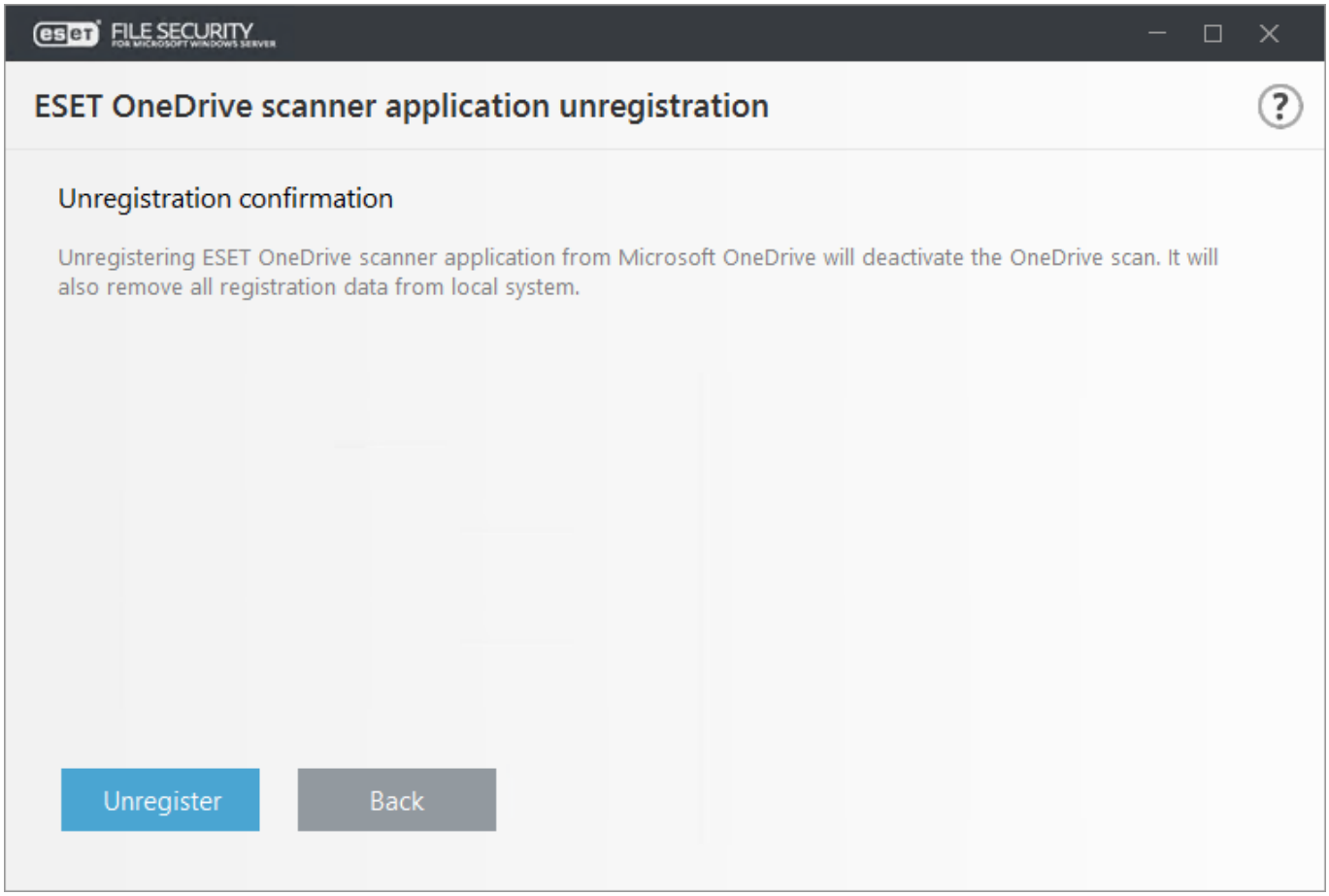
Odregistrace aplikace ESET OneDrive skener

Pomocí níže uvedených kroků odeberete certifikát a odregistrujete aplikaci ESET OneDrive scanner z vašeho Microsoft OneDrive / Office 365 / Azure účtu. Zároveň tím dojde k odstranění všech lokálních závislostí, a bude možné provést novou registraci.

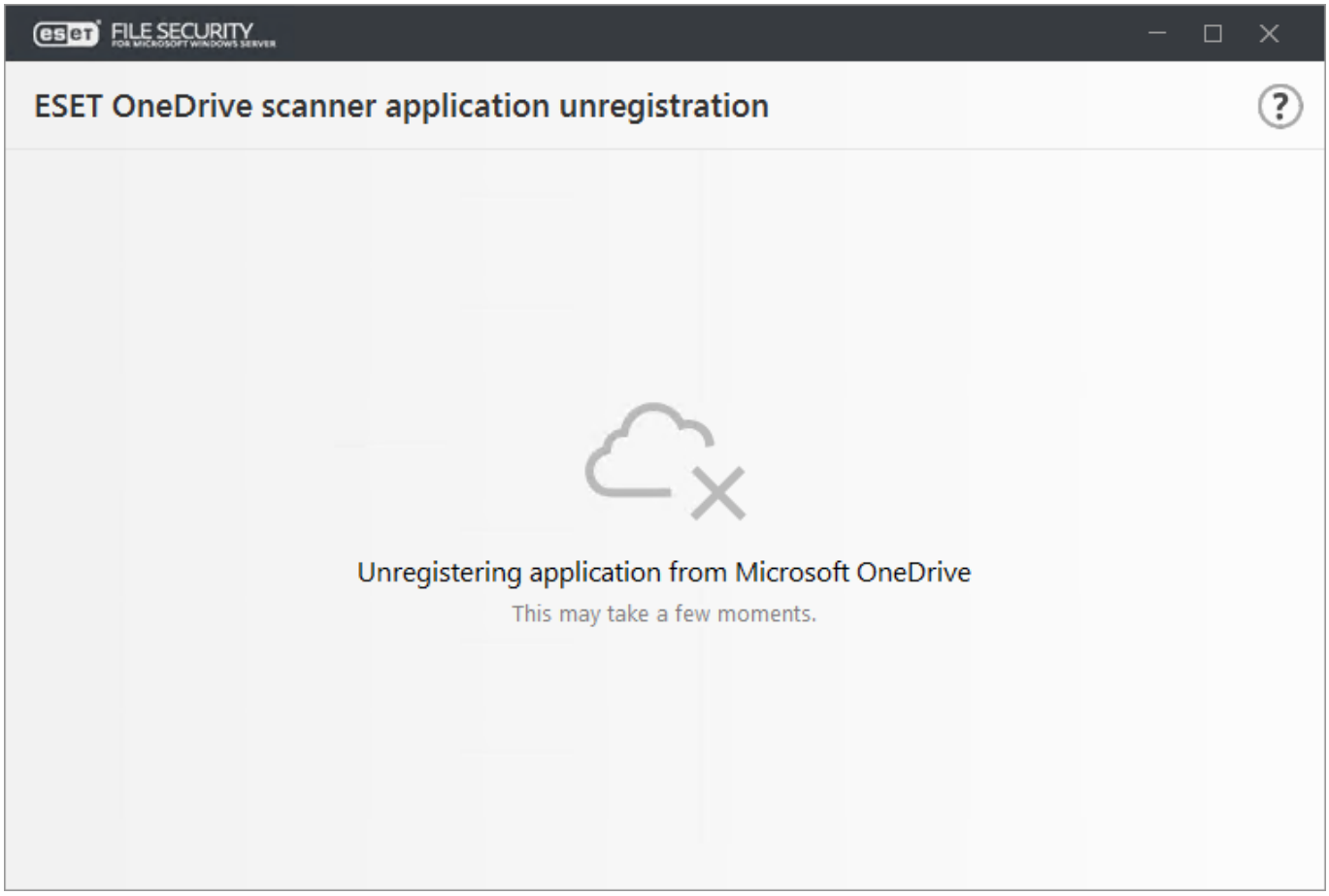
1. Pro spuštění průvodce odregistrací vyberte možnost **Odregistrovat**.



2. V dalším kroku kliknutím na tlačítko **Odregistrovat** potvrďte odebrání aplikace ESET OneDrive scanner.

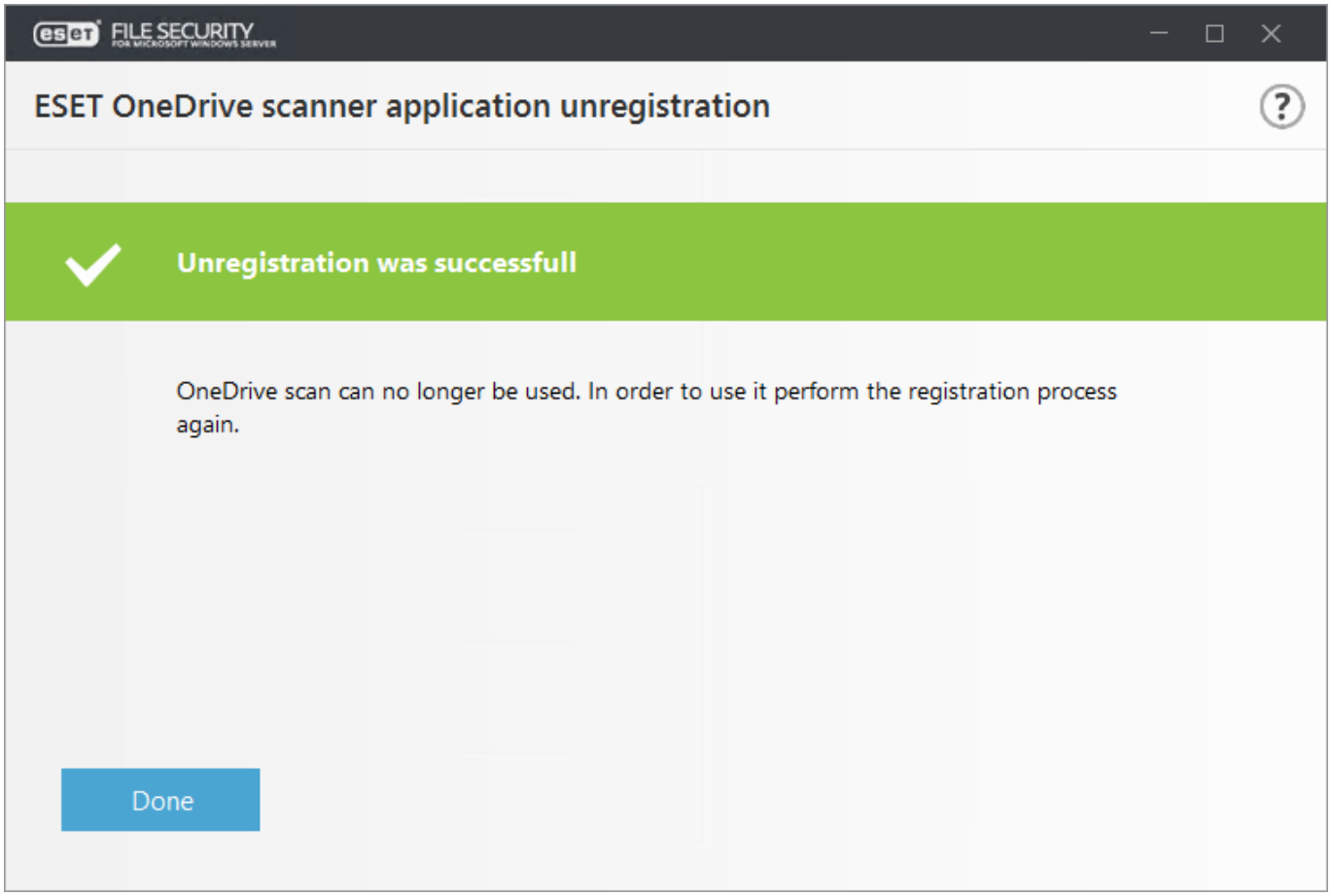


3. Vyčkejte na dokončení odregistrování aplikace z Microsoft OneDrive.



4. Po dokončení operace zobrazí produkt informaci o úspěšném odregistrování aplikace ESET OneDrive

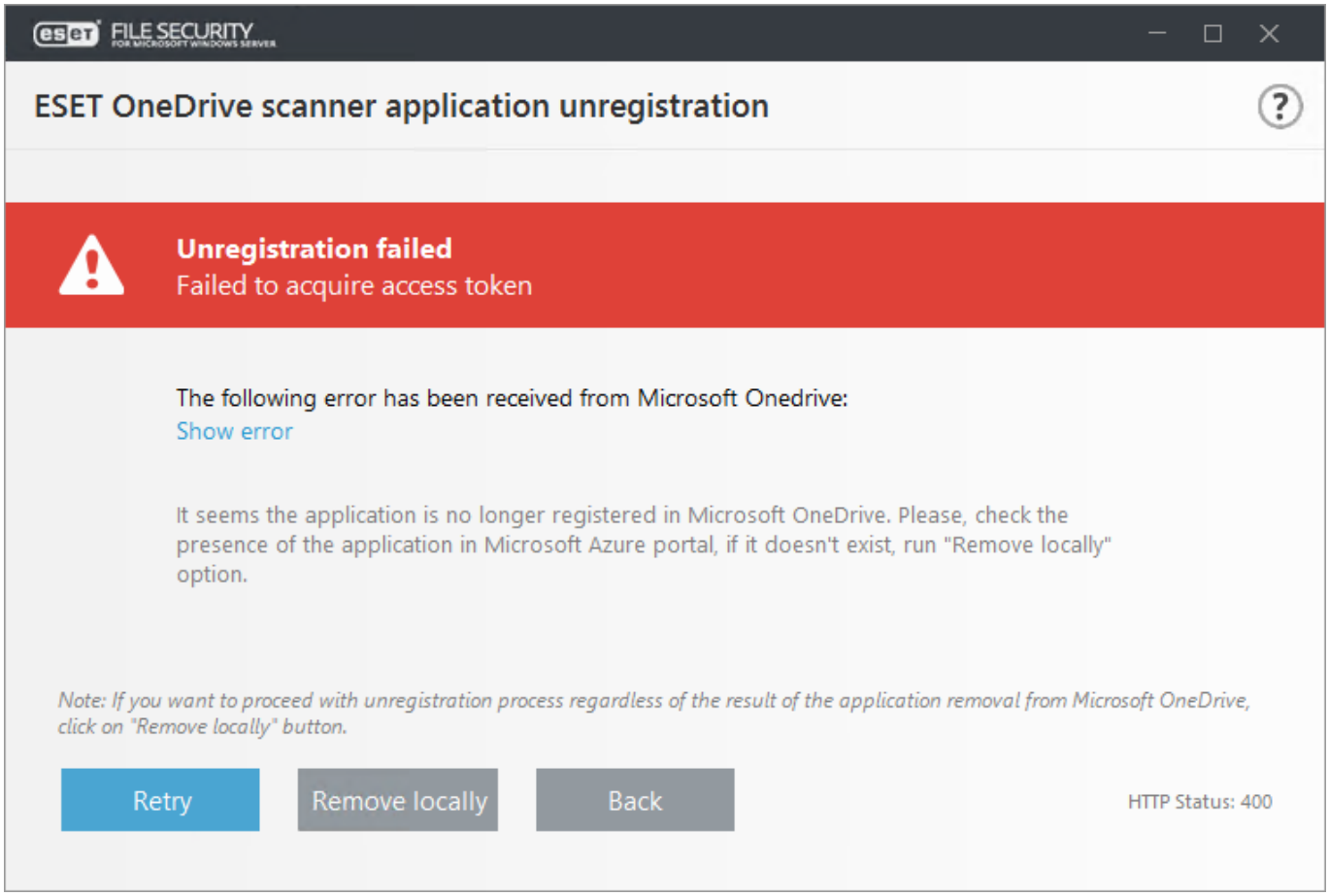
scanner.



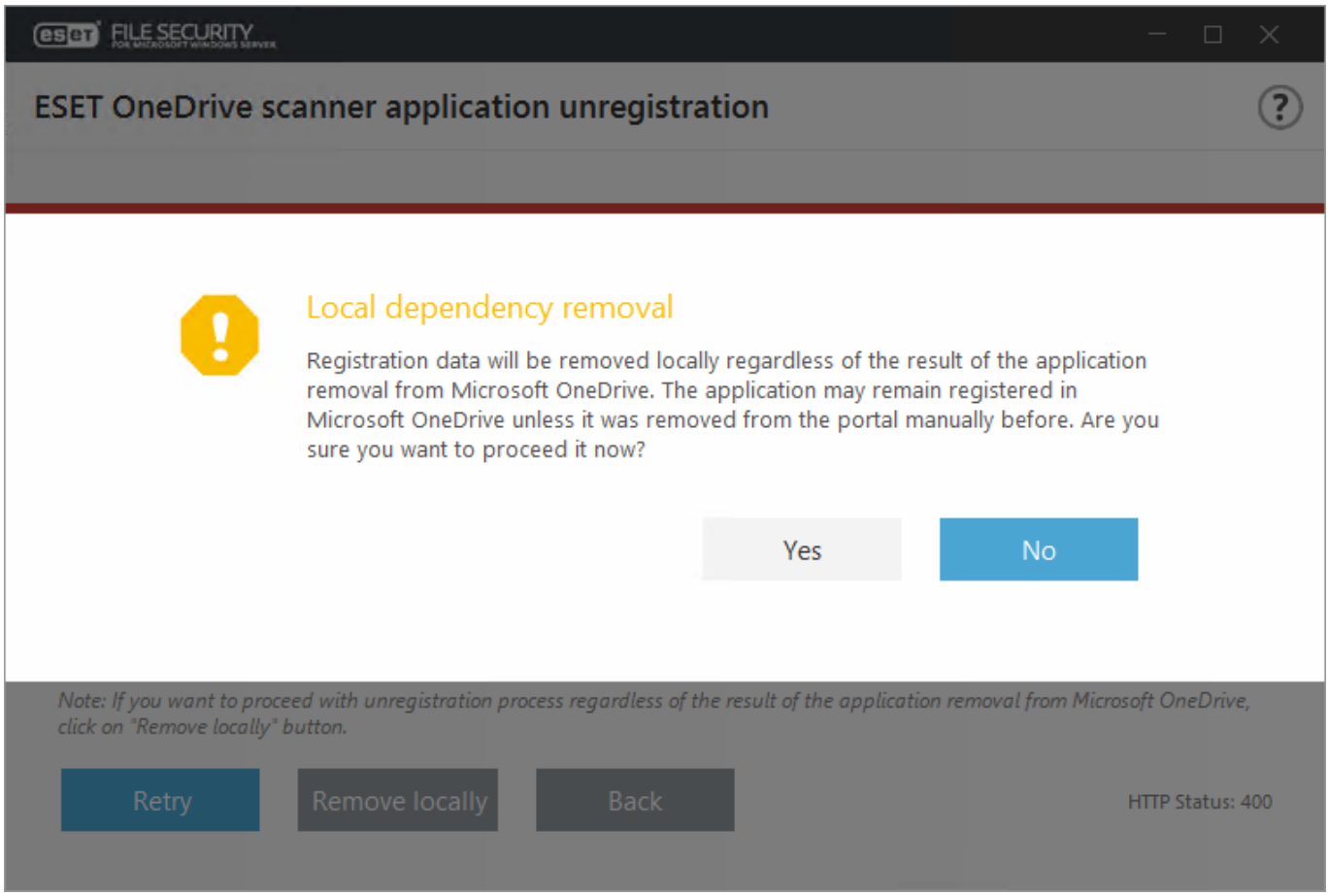
Chybové hlášení o neúspěšné odregistraci se může zobrazit z mnoha důvodů. Počínaje obecnou síťovou chybou, přes nefunkční připojení k Microsoft OneDrive serverům až po chybějící aplikaci ESET OneDrive scanner na Microsoft OneDrive. Seznam možných chybových hlášení společně s navrhovaným řešením naleznete v tabulce na konci této kapitoly.

Při výskytu některých chybových hlášení je k dispozici možnost pro lokální odebrání závislostí (při problémech s konektivitou, neexistující aplikaci v Microsoft OneDrive, ...). Pro lokální odebrání aplikace ESET OneDrive scanner postupujte podle následujících kroků:

Pokud se po kliknutí na tlačítko **Opakovat** situace nevyřeší, klikněte na tlačítko **Odebrat lokálně** pro inicializaci odregistrace, která odebere lokální závislosti aplikace ESET OneDrive scanner.



5. V dalším kroku potvrďte kliknutím na tlačítko **Ano** odebrání lokálních závislostí. Po dokončení nebude OneDrive kontrola dostupná a opět bude možné provést registraci.



Odebrání lokálních závislostí nezpůsobí žádné změny v seznamu registrovaných aplikací na Azure portále, ani v oprávněních přidělených aplikacím na Office 365 portále. Pokud jste aplikaci odebrali lokálně z důvodu nedostupnosti připojení k internetu/serverům Microsoft OneDrive, bude nutné aplikaci ESET OneDrive scanner odebrat ručně ze seznamu registrovaných aplikací na Azure portále. Instrukce, jak najít a smazat aplikaci ESET OneDrive scanner z portálu Azure, naleznete v kapitole nastavení kontroly OneDrive.

Pokud se vám v průběhu registrace aplikace ESET OneDrive scanner zobrazí některé z níže uvedených chybových hlášení, vyzkoušejte pro vyřešení situace navržené řešení.

Chybová zpráva	Detaily chybové zprávy
Připojení k Azure aplikaci nebylo úspěšné. Žádné připojení k internetu.	Zkontrolujte připojení k internetu a spusťte znovu odregistraci aplikace ESET OneDrive scanner. Pro dokončení odregistrace bez odebrání aplikace z Microsoft OneDrive klikněte na možnost Odebrat lokálně.
Nepodařilo se získat přístupový token. Microsoft OneDrive vrátil neočekávanou chybu.	Vypadá to, že aplikace ESET OneDrive scanner již není zaregistrována v Microsoft OneDrive. Aplikace ESET OneDrive scanner mohla být ručně odebrána z portálu Azure. Zkontrolujte přítomnost aplikace ESET OneDrive scanner v Microsoft OneDrive nebo portálu Azure. Pokud se v seznamu aplikací nenachází, pro odregistraci pokračujte kliknutím na tlačítko **Odebrat lokálně**.
Nepodařilo se získat přístupový token. Microsoft OneDrive vrátil chybu serveru.	Microsoft OneDrive vrátil chybu HTTP 5xx. Nyní není možné odregistraci dokončit. Zkuste to později.
Microsoft OneDrive vrátil následující chybu.	Microsoft OneDrive server vrátil konkrétní chybovou zprávu. Pro více informací klikněte na Zobrazit chybu.
Probíhá jiná konfigurační úloha.	Již běží jiná úloha na odregistraci aplikace. Vyčkejte na její dokončení.

Rozšířená nastavení

V rozšířeném nastavení můžete konfigurovat detailní nastavení programu a přizpůsobit si jeho chování vašim potřebám. V levé části okna se nachází následující kategorie:

Detection engine

V této části můžete zapnout nebo vypnout detekci potenciálně nechtěných, podezřelých a zneužitelných aplikací, stejně tak Anti-Stealth ochranu. Dále zde můžete definovat výjimky na procesy, soubory a složky. Nachází se zde detailní parametry rezidentní ochrany souborového systému, skenovacího jádra ThreatSense, cloudové ochrany (ESET LiveGrid®), detekce škodlivého kódu (volitelná kontrola počítače a další možnosti kontroly), Hyper-V kontroly a součásti HIPS.

Aktualizace

Na této záložce naleznete možnosti pro konfiguraci aktualizačních profilů (zahrnující typ aktualizace, jejich zdroj, používání proxy, detailní konfiguraci sítě a možnost pro tvorbu aktualizačního mirroru), přípustného stáří detekčního jádra a vytváření záloh aktualizací.

Web a mail

V této části můžete konfigurovat způsob filtrování aplikačních protokolů a definovat výjimky (na aplikace a IP adresy), možnosti pro filtrování protokolu SSL/TLS, ochranu poštovních klientů (zahrnující integraci, definování používaných portů a oznámení), ochranu přístupu na web (možnosti pro definování HTTP/HTTPS protokolů a správu URL adres) a Anti-Phishingovou ochranu.

Správa zařízení

V této části aktivujete modul pro správu výměnných médií a můžete zde konfigurovat pravidla a skupiny zařízení.

Nástroje

V této sekci máte přístup ke konfiguraci ESET CMD, ESET RMM, poskytovateli WMI, ESET PROTECT cílů kontroly, oznámení na dostupnost aktualizací operačního systému Windows, sběru protokolů, proxy serveru, zasílání oznámení e-mailem, diagnostiky, clusteru, atp.

Uživatelské rozhraní

Zde naleznete možnosti pro změnu chování grafického rozhraní (GUI), potlačení stavů aplikací, zobrazování informací o licenci, nastavení hesla pro ochranu produktu, režim politiky pro spuštění eShell skriptů atp.

Detection engine

Detekční jádro chrání systém před škodlivým kódem, který by se do něj mohl dostat prostřednictvím souborového systému, e-mailu nebo síťové komunikace. Pokud detekuje objekt klasifikovaný jako malware, zahájí akci pro vyřešení situace. Detekční jádro může eliminovat objekt jeho zablokováním a následným vyléčením, odstraněním nebo přesunutím do karantény.

Rezidentní ochrana s využitím strojového učení

Pokročilé strojové učení je nyní součástí detekčního jádra. Funguje jako pokročilá vrstva ochrany a vylepšuje detekci na základě strojového učení. Více informací o tomto typu ochrany naleznete ve slovníku pojmů . Pro níže uvedené kategorie můžete konfigurovat úrovně hlášení a detekce:

Malware

Počítačový virus je škodlivý kód, který je připojený na začátek a konec souboru nacházejícího se ve vašem počítači. Termín "virus" se však často používá nesprávně. Vhodnějším výrazem je "malware" (škodlivý software). Detekci škodlivého kódu provádí modul detekčního jádra v kombinaci s komponentou strojového učení. Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Potenciálně nechtěné aplikace (PUA)

Potenciálně nechtěné aplikace zpravidla nepředstavují bezpečnostní riziko, ale mohou do systému instalovat další nechtěný software, měnit jeho vzhled a chování. To vše bez vašeho vědomí. Případně se aplikace nechová tak, jak byste od ní čekali.

Do této kategorie řadíme aplikace zobrazující reklamy, download wrappery, toolbary do internetových prohlížečů, bundleware, trackware, atp. Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Potenciálně podezřelé aplikace

Jako podezřelé aplikace označujeme software komprimovaný pomocí packerů nebo protektorů. Tyto nástroje využívají pro komprimování a šifrování dat proprietární metody a autoři aplikací je často používají pro zabránění reverzního inženýrství nebo obfuskaci zdrojového kódu (například pro ukrytí škodlivého kódu).

Do této kategorie řadíme všechny neznámé aplikace komprimované packery nebo protektory, které často využívají tvůrci škodlivého kódu ve snaze vyhnout se detekci ze strany antivirových řešení.

Potenciálně zneužitelné aplikace

Jako potenciálně zneužitelné aplikace označujeme legitimní programy, které mohou být v nesprávných rukách zneužity. Potenciálně zneužitelné aplikace jsou legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti.

Do této kategorie řadíme nástroje pro cracking, hacking a lámání hesel, generátory licenčních klíčů, aplikace pro získání produktových klíčů z operačního systému, software pro vzdálený přístup nebo ovládání počítače, keyloggery atp. Tato možnost je standardně vypnuta.
Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Před změnou prahu (úrovně) hlášení nebo ochrany si přečtěte níže uvedené informace:

Hlášení

Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Úroveň hlášení si můžete nastavit dle svých potřeb a s ohledem na prostředí. Nelze tedy říci, která konfigurace je ta správná. Proto doporučujeme sledovat chování ve vašem prostředí, a na základě dat vybrat úroveň hlášení, která vám bude vyhovovat.
Hlášení neprovádí s objekty žádnou akci. Pouze předává informaci odpovídající vrstvě ochrany, která na jeho základě provede odpovídající akci.

Agresivní	**Hlášení je nakonfigurováno na nejvyšší citlivost. Hlášeno bude větší množství detekcí. Agresivní nastavení se může jevit jako nejbezpečnější. Jeho použití však může být kontraproduktivní, protože může být v některých případech příliš citlivé.** i V agresivním nastavení může docházet k chybné identifikaci objektů jako škodlivé, a následně se, v závislosti na nastavení ochrany, provede definovaná akce.
Vyváženě	Toto nastavení je optimalizováno s ohledem na výkon, přesnost detekce a množství falešných poplachů.
Mírně	Hlášení je nakonfigurováno tak, aby se minimalizoval počet falešných poplachů při zachování dostatečné úrovně zabezpečení. Objekty budou hlášeny pouze v případě vysoké pravděpodobnosti a shody chování.
Vypnuto	Hlášení není aktivní. Objekty nebudou detekovány, reportovány ani léčeny. i Není možné deaktivovat detekci škodlivého kódu. V rámci ochrany před škodlivým kódem není k dispozici možnost Vypnuto.

Pro obnovení nastavení v této sekci na výchozí hodnoty klikněte na šipku zpět v jejím záhlaví. Všechny změny provedené v této sekci budou ztraceny.

Ochrana

Pokud na základě výše uvedené konfigurace a výsledku strojového učení dojde k detekci objektu, program jej zablokuje, a následně vyléčí, odstraní nebo přesune do karantény.

Agresivní	**Detekce zachycené s úrovní Agresivní (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení).**
Vyváženě	Detekce zachycené s úrovní Vyváženě (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Mírně	Detekce zachycené s úrovní Opatrně jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Vypnuto	Hlášení není aktivní, objekty nebudou detekovány, reportovány ani léčeny. i Není možné deaktivovat detekci škodlivého kódu. V rámci ochrany před škodlivým kódem není k dispozici možnost Vypnuto.

Pro obnovení nastavení v této sekci na výchozí hodnoty klikněte na šipku zpět v jejím záhlaví.

Ve výchozím nastavení se tato nastavení strojového učení aplikují rovněž na volitelnou kontrolu počítače. V případě potřeby jej můžete konfigurovat samostatně v sekci **Volitelná kontrola s využitím strojového učení**. Deaktivujte pomocí přepínače možnost **Použít nastavení rezidentní ochrany** a upravte konfiguraci dle svých potřeb.

Ochrana s využitím strojového učení

Detekční jádro chrání systém před škodlivým kódem, který by se do něj mohl dostat prostřednictvím souborového systému, e-mailu nebo síťové komunikace. Pokud detekuje objekt klasifikovaný jako malware, zahájí akci pro vyřešení situace. Detekční jádro může eliminovat objekt jeho zablokováním a následným vyléčením, odstraněním nebo přesunutím do karantény.

Rezidentní ochrana s využitím strojového učení

Pokročilé strojové učení je nyní součástí detekčního jádra. Funguje jako pokročilá vrstva ochrany a vylepšuje detekci na základě strojového učení. Více informací o tomto typu ochrany naleznete ve slovníku pojmů . Pro níže uvedené kategorie můžete konfigurovat úrovně hlášení a detekce:

Malware

Počítačový virus je škodlivý kód, který je připojený na začátek a konec souboru nacházejícího se ve vašem počítači. Termín "virus" se však často používá nesprávně. Vhodnějším výrazem je "malware" (škodlivý software). Detekci škodlivého kódu provádí modul detekčního jádra v kombinaci s komponentou strojového učení. Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Potenciálně nechtěné aplikace (PUA)

Potenciálně nechtěné aplikace zpravidla nepředstavují bezpečnostní riziko, ale mohou do systému instalovat další nechtěný software, měnit jeho vzhled a chování. To vše bez vašeho vědomí. Případně se aplikace nechová tak, jak byste od ní čekali.

Do této kategorie řadíme aplikace zobrazující reklamy, download wrappery, toolbary do internetových prohlížečů, bundleware, trackware, atp. Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Potenciálně podezřelé aplikace

Jako podezřelé aplikace označujeme software komprimovaný pomocí packerů nebo protektorů. Tyto nástroje využívají pro komprimování a šifrování dat proprietární metody a autoři aplikací je často používají pro zabránění reverzního inženýrství nebo obfuskaci zdrojového kódu (například pro ukrytí škodlivého kódu).

Do této kategorie řadíme všechny neznámé aplikace komprimované packery nebo protektory, které často využívají tvůrci škodlivého kódu ve snaze vyhnout se detekci ze strany antivirových řešení.

Potenciálně zneužitelné aplikace

Jako potenciálně zneužitelné aplikace označujeme legitimní programy, které mohou být v nesprávných rukách zneužity. Potenciálně zneužitelné aplikace jsou legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti.

Do této kategorie řadíme nástroje pro cracking, hacking a lámání hesel, generátory licenčních klíčů, aplikace pro získání produktových klíčů z operačního systému, software pro vzdálený přístup nebo ovládání počítače, keyloggery atp. Tato možnost je standardně vypnuta.

Více informací o tomto typu aplikací naleznete ve slovníku pojmů .

Před změnou prahu (úrovně) hlášení nebo ochrany si přečtěte níže uvedené informace:

Hlášení

Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Úroveň hlášení si můžete nastavit dle svých potřeb a s ohledem na prostředí. Nelze tedy říci, která konfigurace je ta správná. Proto doporučujeme sledovat chování ve vašem prostředí, a na základě dat vybrat úroveň hlášení, která vám bude vyhovovat.
Hlášení neprovádí s objekty žádnou akci. Pouze předává informaci odpovídající vrstvě ochrany, která na jeho základě provede odpovídající akci.

Agresivní	**Hlášení je nakonfigurováno na nejvyšší citlivost. Hlášeno bude větší množství detekcí. Agresivní nastavení se může jevit jako nejbezpečnější. Jeho použití však může být kontraproduktivní, protože může být v některých případech příliš citlivé.** V agresivním nastavení může docházet k chybné identifikaci objektů jako škodlivé, a následně se, v závislosti na nastavení ochrany, provede definovaná akce.
Vyváženě	Toto nastavení je optimalizováno s ohledem na výkon, přesnost detekce a množství falešných poplachů.
Mírně	Hlášení je nakonfigurováno tak, aby se minimalizoval počet falešných poplachů při zachování dostatečné úrovně zabezpečení. Objekty budou hlášeny pouze v případě vysoké pravděpodobnosti a shody chování.
Vypnuto	Hlášení není aktivní. Objekty nebudou detekovány, reportovány ani léčeny. Není možné deaktivovat detekci škodlivého kódu. V rámci ochrany před škodlivým kódem není k dispozici možnost Vypnuto.

Pro obnovení nastavení v této sekci na výchozí hodnoty klikněte na šipku zpět v jejím záhlaví. Všechny změny provedené v této sekci budou ztraceny.

OneDrive ochrana s využitím strojového učení

Hlášení
Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Úroveň hlášení nemá vliv na provedenou akci (tu zajišťuje odpovídající vrstva ochrany).
Ochrana
Prostřednictvím parametrů v sekci OneDrive ochrana ovlivníte akci, která se provede nad detekovanými objekty.
Pro obnovení nastavení v této sekci na výchozí hodnoty klikněte na šipku zpět v jejím záhlaví. Všechny změny provedené v této sekci budou ztraceny.
Konfigurace ochrany s využitím strojového učení prostřednictvím eShell: Název kontextu v eShell je **MLP**. Spusťte eShell v interaktivním režimu a přejděte do kontextu MLP:

```
computer onedrive mlp
```

Pro zobrazení aktuální úrovně hlášení pro podezřelé aplikace použijte příkaz:

```
get suspicious-reporting
```

Pokud chcete nižší (méně přísnou) úroveň hlášení, pomocí níže uvedeného příkazu změňte nastavení na Mírně:

```
set suspicious-reporting cautious
```

Hyper-V ochrana s využitím strojového učení

Hlášení
Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Úroveň hlášení nemá vliv na provedenou akci (tu zajišťuje odpovídající vrstva ochrany).
Ochrana
Prostřednictvím parametrů v sekci Hyper-V kontrola ovlivníte akci, která se provede nad detekovanými objekty. Pro obnovení nastavení v této sekci na výchozí hodnoty klikněte na šipku zpět v jejím záhlaví. Všechny změny provedené v této sekci budou ztraceny.
Konfigurace ochrany s využitím strojového učení prostřednictvím eShell: Název kontextu v eShell je **MLP**. Spusťte eShell v interaktivním režimu a přejděte do kontextu MLP:

```
computer hyperv mlp
```

Pro zobrazení aktuální úrovně hlášení pro podezřelé aplikace použijte příkaz:

```
get suspicious-reporting
```

Pokud chcete nižší (méně přísnou) úroveň hlášení, pomocí níže uvedeného příkazu změňte nastavení na Mírně:

```
set suspicious-reporting cautious
```

Výjimky

Prostřednictvím výjimek můžete vyloučit soubory nebo složky z kontroly. Pro zajištění kontroly všech objektů na hrozby doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Příkladem, kdy je nutné vyloučit objekt z kontroly (například velké databázové soubory), je situace, kdy v průběhu kontroly dochází ke zpomalení serveru nebo konfliktu s právě používanou aplikací (například v průběhu zálohování).

Nezaměňujte tuto funkci s možností pro vyloučení přípon souborů z kontroly, vyloučení procesů nebo filtrem výjimek.

Soubory zařazené do výjimek nebudou kontrolovány rezidentní ochranou ani naplánovanou nebo ručně spuštěnou kontrolou počítače, i když budou napadeny škodlivým kódem.

Vyberte si typ výjimky, klikněte na možnost **Změnit** a následně si vytvořte novou výjimku nebo upravte již existující:

- Výkonnostní výjimky – prostřednictvím výkonnostních výjimek můžete vyloučit soubory nebo složky z kontroly.
- Detekční výjimky – prostřednictvím detekčních výjimek můžete vyloučit objekt z kontroly na základě cesty, kontrolního součtu nebo názvu detekce.

Výkonnostní výjimky

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

Cesta

Vyloučí konkrétní cestu (soubor nebo adresář) v tomto počítači. Hvězdičku (*) nepoužívejte uprostřed cesty. Další informace naleznete v Databázi znalostí.

Pro vyloučení veškerého obsahu složky nezapomeňte na konec cesty přidat hvězdičku (*): *C:\Tools**. *C:\Tools* nebude vyloučena, protože, z pohledu skeneru, může *Tools* představovat rovněž název souboru.

Komentář

Pro snadnější identifikaci výjimky v budoucnu si můžete volitelně přidat Komentář.

Použití hvězdičky ve výjimce:
C:\Tools* – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce, včetně jejich podložek
C:\Tools*.* – se chová stejně jako C:\Tools* Znamená, že se složky prochází rekurzivně
C:\Tools*.dat – vyloučí dat soubory ve složce Tools
C:\Tools\sg.dat – vyloučí konkrétní soubor v přesně definované cestě

Pro vyloučení všech souborů v konkrétní složce zadejte cestu ke složce a použijte masku *.*. Pro vyloučení pouze .doc souborů použijte masku *.doc.
Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční, použijte (řekněme "D"), použijte následující formát:
D????.exe (otazníky nahrazují chybějící a neznámé znaky)

Při vytváření výjimek můžete použít systémové proměnné jako %PROGRAMFILES%.
Chcete-li vyloučit složku Program Files pomocí této systémové proměnné, použijte cestu %PROGRAMFILES%\ (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty)
Pokud chcete vyloučit všechny soubory z podsložky %HOMEDRIVE%, zadejte cestu ke složce %HOMEDRIVE%\Excluded_Directory*.*
Při definování výjimky podle cesty můžete použít následující proměnné:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Systémové proměnné specifické pro uživatele (jako %TEMP% nebo %USERPROFILE%) nebo proměnné prostředí (jako %PATH%) nejsou podporovány.

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

Nejsnadněji výjimku vytvoříte přímo z protokolu detekcí (v hlavním okně programu na záložce **Protokoly** a z rozbalovacího menu vyberte možnost Detekce). Klikněte pravým tlačítkem na záznam (detekci) a z kontextového menu vyberte možnost **Vytvořit výjimku**. Následně se otevře průvodce vytvořením výjimky, ve kterém již budou předdefinována kritéria.

Pro ruční vytvoření detekční výjimky klikněte na **Změnit** > **Přidat** (v případě existující výjimky na **Změnit** a definujte jedno nebo více kritérií (můžete je kombinovat).

Cesta

Zadejte cestu (k souboru nebo složce). Pro vybrání umístění/souboru využijte průzkumníka nebo ji zadejte ručně. Hvězdičku (*) nepoužívejte uprostřed cesty. Další informace naleznete v Databázi znalostí.

Pro vyloučení veškerého obsahu složky nezapomeňte na konec cesty přidat hvězdičku (*): C:\Tools*. *C:\Tools* nebude vyloučena, protože, z pohledu skeneru, může *Tools* představovat rovněž název souboru.

Kontrolní součet

Vyloučí konkrétní objekt na základě jeho SHA1 kontrolního součtu, bez ohledu na jeho umístění, název nebo příponu.

Název detekce

Zadejte platný název detekce (hrozby). Vytvoření výjimky pouze na název detekce může představovat bezpečnostní riziko. Doporučujeme název detekce kombinovat zároveň s cestou. Tím zajistíte, že výjimka bude platní pouze pro konkrétní typy detekcí.

Komentář

Pro snadnější identifikaci výjimky v budoucnu si můžete volitelně přidat **Komentář**.

ESET PROTECT umožnuje nastavovat detekční výjimky a vytvořené výjimky použít na více počítačů/skupin.

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

Použití hvězdičky ve výjimce:
C:\Tools* – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce, včetně jejich podložek
C:\Tools*.* – se chová stejně jako C:\Tools* Znamená, že se složky prochází rekurzivně
C:\Tools*.dat – vyloučí dat soubory ve složce Tools
C:\Tools\sg.dat – vyloučí konkrétní soubor v přesně definované cestě

Pro vyloučení hrozby zadejte platný název detekce v následujícím formátu:
@NAME=Win32/Adware.Optmedia
@NAME=Win32/TrojanDownloader.Delf.QQI
@NAME=Win32/Bagle.D

Pro vyloučení všech souborů v konkrétní složce zadejte cestu ke složce a použijte masku *.*. Chcete-li vyloučit pouze soubory doc, použijte masku *.doc
Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční, použijte (řekněme "D"), použijte následující formát:
D????.exe (otazníky nahrazují chybějící a neznámé znaky)

Při vytváření výjimek můžete použít systémové proměnné jako *%PROGRAMFILES%*.
Chcete-li vyloučit složku Program Files pomocí této systémové proměnné, použijte cestu %PROGRAMFILES%\ (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty)
Pokud chcete vyloučit všechny soubory z podsložky %HOMEDRIVE%, zadejte cestu %HOMEDRIVE%\Excluded_Directory*.*
Při definování výjimky podle cesty můžete použít následující proměnné:
%ALLUSERSPROFILE%
%COMMONPROGRAMFILES%
%COMMONPROGRAMFILES(X86)%
%COMSPEC%
%HOMEDRIVE%
%HOMEPATH%
%PROGRAMFILES%
%PROGRAMFILES(X86)%
%SystemDrive%
%SystemRoot%
%WINDIR%
%PUBLIC%
Systémové proměnné specifické pro uživatele (jako %TEMP% nebo %USERPROFILE%) nebo proměnné prostředí (jako %PATH%) nejsou podporovány.

Průvodce vytvořením výjimky

Na základě typu detekce je vždy předvybrána doporučená výjimka. V případě potřeby můžete kritéria detekce změnit. Klikněte na možnost **Změnit kritéria**:

- **Konkrétní soubory** – pomocí této možnosti vyloučíte konkrétní soubor podle jeho SHA-1 kontrolního součtu.
- **Detekce** – zadejte název detekce, kterou nechcete v souboru detekovat.
- **Cesta + Detekce** – zadejte název detekce, kterou nechcete v konkrétní cestě (včetně názvu souboru) detekovat.

Pro snadnější identifikaci výjimky v budoucnu si můžete volitelně přidat **Komentář**.

Rozšířená nastavení

Anti-Stealth ochrana

Jedná se o sofistikovaný systém pro detekci nebezpečných programů, jako jsou např. rootkity, které se po svém spuštění dokáží skrýt v operačním systému. Tyto typy programů jsou obvykle pomocí standardních technik nedetekovatelné.

AMSI

Po zapnutí této možnosti bude Microsoft Antimalware Scan Interface (AMSI) kontrolovat skripty PowerShellu spouštěné nástrojem Windows Script Host.

Automatické výjimky

Vývojáři většiny aplikací a operačních systémů určených pro servery doporučují v bezpečnostních řešeních vytvořit výjimky na kritické soubory a složky, aby nedocházelo k jejich kontrole. Je to zejména kvůli tomu, že jejich kontrola může mít negativní vliv na výkon serveru a může dokonce způsobit konflikty vedoucí k nefunkčnosti serverové aplikace. Vytvořením výjimek minimalizujete možné konflikty a zvýšíte celkový výkon serveru při současném běhu bezpečnostního řešení. Úplný seznam souborů, které produkty ESET nekontrolují, naleznete v Databázi znalostí.

ESET Server Security detekuje kritické serverové aplikace a soubory operačního systému a automaticky je zařazuje na seznam výjimek. Automatické výjimky se pro všechny podporované aplikace vytváří automaticky. Pomocí přepínače můžete vypnout/zapnout vytvoření výjimek pro konkrétní serverové aplikace, přičemž chování je následující:

- Pokud je přepínač zapnutý, na seznam výjimek se přidají všechny kritické soubory a složky dané aplikace. Při každém startu serveru se ověří, zda se výjimky stále na seznamu nacházejí. Pokud došlo ve změně v systému nebo aplikaci (například nainstalování nové aplikace), zároveň dojde k jeho aktualizaci. Tímto nastavením zajistíte, že se vždy aplikují doporučené automatické výjimky.

- Pokud je přepínač vypnutý, ze seznamu výjimek dojde k odebrání souborů a složek pro danou aplikaci. Ostatní uživatelem ručně zadané výjimky nejsou výše uvedeným nastavení nijak ovlivněny.

Pro zjištění a vygenerování automatických výjimek používá ESET Server Security samostatnou aplikaci eAutoExclusions.exe, která se nachází v instalační složce produktu. Z vaší strany nevyžaduje žádnou interakci. Spuštěním příkazu eAutoExclusions.exe -servers si v případě zájmu můžete kdykoli zobrazit seznamu detekovaných serverových aplikací. Pro zobrazení úplné syntaxe použijte příkaz `eAutoExclusions.exe -?`.

Sdílená lokální cache

Sdílená lokální cache výrazně zrychluje kontrolu počítače ve virtuálních prostředích odstraněním duplicitní kontroly souborů v síti. Každý soubor je zkontrolován pouze jednou a výsledek je uložen do sdílené cache. Aktivováním možnosti **Používat cache** se budou ukládat informace o kontrolovaných souborech a složkách ve vaší síti do lokální cache. Pokud následně spustíte novou kontrolu, ESET Server Security se nejprve podívá do cache. V případě, že byl již identický soubor jiným produktem v síti zkontrolován, vyloučí jej z aktuální kontroly.

Nastavení Cache serveru jsou následující:

- **Adresa serveru** – název počítače nebo IP adresa, na kterém běží ESET Shared Local Cache.

- **Port** – port, který při komunikaci využívá lokální cache produktu ESET.

- **Heslo** – zadejte heslo ke sdílené lokální cache, pokud je vyžadováno.

Byla nalezena infiltrace

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

Standardní chování

ESET Server Security dokáže zachytit infiltrace pomocí následujících modulů:

- Rezidentní ochrana souborového systému
- Ochrany přístupu na web
- Ochrana poštovních klientů
- Volitelná kontrola počítače

Každý z těchto modulů používá standardní úroveň léčení. Program se pokusí soubor vyléčit a přesunout do Karantény, nebo přeruší spojení. Oznámení se zobrazují v pravé dolní části obrazovky. Pro více informací o jednotlivých úrovních léčení a jejich chování se podívejte do kapitoly Léčení.

Léčení a mazání

Pokud rezidentní ochrana nemá předdefinovanou akci pro daný typ souboru, zobrazí se dialogové okno s výběrem dostupných možností. Obvykle jsou k dispozici možnosti **Léčit**, **Vymazat** a **Žádná akce**. Výběr možnosti **Žádná akce** nedoporučujeme, protože v tomto případě zůstane infekce nevyléčena. Výjimkou z tohoto pravidla může být situace, kdy jste si jisti, že soubor je neškodný a byl detekován omylem.

Léčení souboru je možné provést, pokud do zdravého souboru byla zavedena část, která obsahuje škodlivý kód. V tomto případě se nejprve program pokusí infikovaný soubor vyléčit, aby se tím obnovil do původního stavu. Pokud soubor sestává výhradně ze škodlivého kódu, bude vymazán.

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

Více hrozeb

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

Vyberte **akci**, kterou chcete provést jednotlivě nebo hromadně pro všechny nalezené hrozby a akci dokončete kliknutím na tlačítko **Dokončit**.

Mazání souborů v archivech

Pokud je zjištěna infiltrace uvnitř archivu, bude archiv při standardní úrovni léčení odstraněn pouze v případě, že obsahuje pouze infikovaný soubor. Jinými slovy, archiv nebude vymazán, pokud kromě infiltrace obsahuje také nezávadné soubory.

Opatrnost je potřeba dodržovat při nastavení přísné úrovně léčení, kdy v tomto případě bude archiv vymazán, bez ohledu na to, zda jeho obsah tvoří také zdravé soubory.

Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému kontroluje veškeré dění v počítači. Všechny soubory, které se v počítači otevírají, vytvářejí a spouštějí, jsou kontrolovány na přítomnost škodlivého kódu. Standardně se rezidentní ochrana spustí vždy při startu operačního systému.

Ve zvláštních případech (například pokud dochází ke konfliktu s jiným rezidentním programem), je možné spuštění

rezidentní ochrany zastavit pomocí přepínače **Zapnout rezidentní ochranu souborového systému** v Rozšířeném nastavení (F5) v sekci **Detekční jádro > Rezidentní ochrana souborového systému** > **Obecné**.

ESET Server Security je kompatibilní se stroji využívající Azure File Sync agenta s aktivní funkcí cloud tiering. ESET Server Security rozpoznává soubory s atributem *FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS*.

Kontrola médií

Standardně je nastavena kontrola všech typů médií na možné hrozby:

- **Lokální disky** – kontrola lokálních pevných disků v počítači.
- **Výměnná média** – kontrola CD, DVD, USB klíčů, Bluetooth zařízení a dalších.
- **Síťové disky** – kontrola namapovaných síťových disků.

Doporučujeme ponechat toto nastavení. Změnu doporučujeme pouze ve zvláštních případech, např. pokud při kontrole určitého média dochází k výraznému zpomalení.

Kontrola při událostech

Ve výchozím nastavení jsou kontrolovány soubory při jejich otevření, vytvoření nebo spuštění. Doporučujeme ponechat standardní nastavení, které poskytuje maximální možnou ochranu vašeho počítače.

- **Otevření souboru** – tato možnost zajistí kontrolu souborů při jejich otevírání a přístupu k nim.
- **Vytvoření souboru** – tato možnost zajistí kontrolu souborů při jejich vytváření nebo změně.
- **Spuštění souboru** – tato možnost zajistí kontrolu souborů při jejich spouštění.
- **Přístup na výměnné zařízení** – tato možnost zajistí kontrolu po přístupu k výměnným médiím. Pokud vložené výměnné médium obsahuje boot sektor, po aktivování této možnosti dojde automaticky k jeho zkontrolování po připojení zařízení. Nejedná se o nastavení, které zajistí kontrolu souborů uložených na výměnném médiu. Tuto možnost naleznete výše v sekci **Provádět kontrolu těchto médií** > **Výměnná média**. Pro správné fungování kontroly boot sektoru výměnných médií ponechte v sekci parametry skenovacího jádra ThreatSense aktivní možnost Boot sektory/UEFI.

Vyloučené procesy

V této části můžete vytvořit výjimky z rezidentní ochrany pro konkrétní procesy. To můžete využít například pro zálohování řešení, kdy po vyloučení konkrétních procesů budou ignorovány všechny soubory, ke kterým tyto procesy přistupují, což minimalizuje zásahy aplikací třetích stran do procesu zálohování.

Parametry skenovacího jádra ThreatSense

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí jako je přístup k souboru. Chování rezidentní ochrany může být odlišné u nově vytvářených než existujících souborů. Například, pro nově vytvářené soubory můžete nastavit hlubší úroveň kontroly.

Pro zajištění minimálních systémových nároků, nejsou již dříve kontrolované soubory znovu kontrolovány (pokud nebyly změněny). Soubory jsou opět kontrolovány pouze po každé aktualizaci detekčního jádra. Toto chování můžete ovlivnit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje.

Pokud chcete upravit možnosti kontroly, otevřete **Rozšířené nastavení** (stisknutím klávesy **F5** v hlavním okně programu), přejděte na záložku **Detection engine** > **Rezidentní ochrana souborového systému**. Dále přejděte na záložku **Parametry skenovacího jádra ThreatSense > Ostatní a aktivujte** nebo **vypněte** možnost **Používat Smart optimalizaci**.

Doplňující parametry skenovacího jádra ThreatSense

Detailní možnosti můžete konfigurovat v sekci **Doplňující parametry ThreatSense pro vytvářené a změněné soubory** a **Doplňující parametry ThreatSense pro spouštěné soubory**.

ThreatSenseParametry skenovacího jádra

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní, poskytuje ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury aj.), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně a tak maximalizovat svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat i rootkity.

Pro více informací o automatické kontrole zaváděných při startu přejděte do kapitoly Kontrola po startu.

V nastavení skenovacího jádra ThreatSense můžete definovat následující parametry:

- Typu souborů a přípon, které se mají kontrolovat,
- Kombinace různých metod detekce,
- Úrovně léčení apod.

Pro zobrazení nastavení klikněte na záložku **Parametry skenovacího jádra** v **Rozšířeném nastavení** (**F5**) jakéhokoli modulu, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. V rámci technologie ThreatSense můžete konfigurovat následující moduly:

- Hyper-V kontrola
- OneDrive kontrola
- Rezidentní ochrana souborového systému
- Kontroly škodlivých kódů
- Kontrola při nečinnosti
- Kontrola souborů zaváděných při startu počítače
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrany přístupu na web

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime archivů a rozšířené

heuristiky pro rezidentní ochranu souborového systému (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense parametrů. Určitou volnost v konfiguraci ponechává modul Kontrola počítače.

Objekty ke kontrole

V této sekci můžete vybrat součásti počítače a soubory, které budou kontrolovány na přítomnost infiltrace.

Operační paměť
Kontrola přítomnosti hrozeb, které mohou být zavedeny v operační paměti počítače.

Boot sektory/UEFI
Kontrola přítomnosti boot virů v MBR sektorech disků, kde se nachází tzv. zavaděč operačního systému. V případě virtuálního počítače Hyper-V je jeho disk MBR kontrolován v režimu jen pro čtení.

WMI databáze
Prohledává WMI databáze, vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor.

Registr systému
Prohledá systémový registr, všechny klíče a podklíče, vyhledá odkazy na infikované soubory nebo škodlivý kód vložený jako data.

Kontrolovat poštovní soubory (standardně)
Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

Archivy
Program podporuje následující rozšíření: *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO, BIN, NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE* a další.

Samorozbalovací archivy
Samorozbalovací archivy – archivy které nepotřebují pro své rozbalení jiné programy. Jedná se o SFX (Self-extracting) archivy.

Runtime packery
Po spuštění jsou runtime packery (na rozdíl od standardních archivních typů) dekomprimovány v paměti. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG,...) skener podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

V této sekci můžete vybrat metody, které se použijí při kontrole počítače na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika
Heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Výhodou heuristiky je schopnost odhalit i takový škodlivý software, který v době poslední aktualizace antivirového programu ještě neexistoval nebo nebyl znám.

Rozšířená heuristika/DNA vzorky
Rozšířená heuristika používá jedinečný heuristický algoritmus vyvinutý společností ESET, který dokáže detekovat počítačové červy a trojské koně napsané ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopnosti produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých virů (nebo jejich mírně pozměněných verzí).

Léčení

Nastavení léčení ovlivňuje chování virového skeneru. V případě rezidentní ochrana i dalších modulech jsou k dispozici níže uvedené úrovně léčení.

Vždy vyřešit infekci

V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Výjimku tvoří systémové soubory. Pokud nelze detekci vyléčit, bude detekovaný objekt ponechán v původním umístění.

Pokud je to bezpečné, vyřešit infekci, jinak ponechat

V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci vyléčit v systémových souborech nebo archivech obsahujícími neinfikované i infikovanými soubory zároveň, bude detekovaný objekt ponechán v původním umístění.

Pokud je to bezpečné, vyřešit infekci, jinak se dotázat

V tomto režimu se program pokusí vyléčit detekované objekty. Pokud ESET Server Security nedokáže v některých případech provést automatickou akci, výběr akce bude přenechán na uživateli (odstranění nebo ignorování detekce). Toto nastavení je doporučené pro většinu případů.

Vždy se dotázat uživatele

ESET Server Security neprovede žádnou automatickou akci. Výběr akce bude přenechán na uživateli.

Výjimky

Přípona souboru je součástí jeho názvu a je oddělena tečkou. Přípona označuje typ a obsah souboru. V této části nastavení parametrů ThreatSense můžete nastavit typy souborů, které budou vyloučeny z kontroly.

Ostatní

Při konfiguraci parametrů Detekčního jádra ThreatSense jsou v sekci **Ostatní** k dispozici následující možnosti:

Kontrolovat alternativní datové proudy (platí pouze pro kontrolu počítače)

Alternativní datové proudy (resource/data forks) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a adresářům. Mnoho infiltrací je proto využívá na své maskování před případným odhalením.

Spustit kontrolu na pozadí s nízkou prioritou

Každá kontrola počítače využívá určité množství systémových zdrojů. Pokud právě pracujete s programy náročnými na výkon procesoru, přesunutím kontroly na pozadí jí můžete přiřadit nižší prioritu a získat více prostředků pro ostatní aplikace.

Zapisovat všechny objekty do protokolu

Pokud je tato možnost aktivní, do protokolu se zapíší všechny zkontrolované soubory, i když nejsou infikované.

Zapnout Smart optimalizaci

Při zapnuté Smart optimalizaci je použito nejoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při nastavení kontroly pouze uživatelské nastavení jádra ThreatSense.

Zachovat čas přístupu k souborům

Po vybrání této možnosti nebude při kontrole souboru změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

V sekci Omezení můžete nastavit maximální velikost objektů, archivů a úroveň zanoření, které se budou testovat na přítomnost škodlivého kódu:

Standardní nastavení objektů

Tato možnost je standardně aktivní a znamená, že nejsou aplikovány žádné limity a ESET Server Security neuplatňuje níže definovaná nastavení.

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován.

Definuje největší možnou velikost souborů, které budou zkontrolovány. Modul ochrany bude kontrolovat pouze objekty s velikostí menší, než je definovaná hodnota. Doporučujeme, aby tuto hodnotu měnili jen pokročilí uživatelé, kteří mají důvod vyloučení větších objektů z kontroly. Standardní hodnota: neomezeno.

Maximální čas kontroly objektu (v sekundách)

Definuje maximální povolený čas na kontrolu objektu. Pokud uživatel nastaví hodnotu, modul ochrany přestane kontrolovat objekt po uplynutí nastavené doby, bez ohledu na to, zda byla kontrola objektu dokončena či nikoli. Standardní hodnota: neomezeno.

Nastavení kontroly archivů

Pro změnu nastavení nejprve vypněte možnost **Standardní nastavení kontroly archivů**.

Úroveň vnoření archivů

Definuje maximální hloubku vnoření při kontrole archivů. Výchozí hodnota: 10. Pro objekty detekované ochranou transportu zpráv musíte nastavit požadovanou úroveň vnoření + 1. První úroveň je totiž samotný e-mail.

Nastavíte-li úroveň vnoření na 3, archiv se třemi vnořeními bude transportní ochranou zkontrolován pouze do druhé úrovně. Proto pokud chcete transportní ochranou kontrolovat archivy do třetí úrovně vnoření, je nutné do pole **úroveň vnoření archivů** zadat hodnotu 4.

Maximální velikost souboru v archivu

Pomocí této možnosti nastavíte maximální reálnou velikost souborů v archivech (po jejich rozbalení), které budou zkontrolovány. Standardní hodnota: neomezeno.

Nedoporučujeme měnit výchozí hodnoty. Za normálních okolností by neměl být důvod k jejich přenastavení.

Doplňující parametry skenovacího jádra ThreatSense

Doplňující parametry ThreatSense – parametry pro vytvářené a změněné soubory

Pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s přidanými parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána pokročilá heuristika, čímž se výrazně zvyšuje úroveň detekce, i když škodlivý kód ještě není znám před vydáním aktualizace detekčních modulů. Kromě nově vytvářených souborů se kontrolují také samorozbalovací soubory (.sfx) a runtime archivy (interně komprimované spustitelné soubory).

Standardně jsou archivy kontrolovány do 10 úrovní vnoření bez ohledu na jejich velikost. Pro změnu kontroly archivů deaktivujte možnost **Standardní nastavení archivů**.

Doplňující parametry ThreatSense pro spouštěné soubory

Standardně se Rozšířená heuristika se používá pro spouštěné soubory. Pokud je aktivní, pro snížení dopadu na výkon systému doporučujeme ponechat aktivní Smart optimalizaci a také technologii ESET LiveGrid®.

Typy rozšíření vyloučených z kontroly

Přípona souboru je součástí jeho názvu a je oddělena tečkou. Přípona označuje typ a obsah souboru. Standardně se kontrolují všechny soubory bez ohledu na příponu. Pokud však potřebujete vyloučit soubory s kontrétní příponou, nastavení parametrů ThreatSense vám umožní vyloučit soubory z kontroly na základě jejich rozšíření.

To může být užitečné, pokud kontrola určitých typů souborů zabraňuje správnému spuštění aplikace.

Pro přidání přípony klikněte na tlačítko **Přidat**. Zadejte příponu do textového pole (například tmp) a klikěte na tlačítko **OK**. Pokud vyberete možnost **Zadat více hodnot**, můžete přidat více přípon souborů oddělených řádky, čárkami nebo středníky (například z rozevírací nabídky vyberte možnost **Středník** jako oddělovač a napište `edb;eml;tmp`).
Při definování seznamu výjimek můžete použít jako zástupný znak ? (otazník). Otazník (?) reprezentuje jeden znak (například `?db`).

Chcete-li zobrazit příponu (typ souboru) pro všechny soubory v operačním systému Windows, zrušte zaškrtnutí možnosti **Skrýt přípony známých typů souborů** v **Ovládacích panelech** > **Možnosti složky** > **Zobrazit**.

Vyloučené procesy

Pomocí této funkce vyloučíte z rezidentní ochrany činnost konkrétních procesů. V případě obnovy dedikovaných serverů (aplikačních, souborových, …) ze zálohy do funkčního stavu hraje kritickou roli čas.

Pro zvýšení rychlosti zálohování, zajištění integrity dat a dostupnosti služeb jsou některé techniky zálohovacích řešení v konfliktu s antivirovou ochranou souborového systému. Ke stejným problémům může dojít také při pokusu o živou migraci virtuálních strojů.

Jediným řešením pro zabránění konfliktu bývá v uvedených případech deaktivace bezpečnostního řešení. Vyloučením činnosti konkrétních procesů (například zálohovacího agenta) z kontroly je veškerá jejich činnost ignorována a považována za důvěryhodnou, čímž je minimalizován vliv na celý průběh operace (například zálohování). Při vytváření výjimek však buďte obezřetní, při přístupu zálohovacího agenta k infikovanému souboru nedojde k detekci hrozby. Z tohoto důvodu je možné výjimky vytvářet pouze z rezidentní ochrany souborového systému.

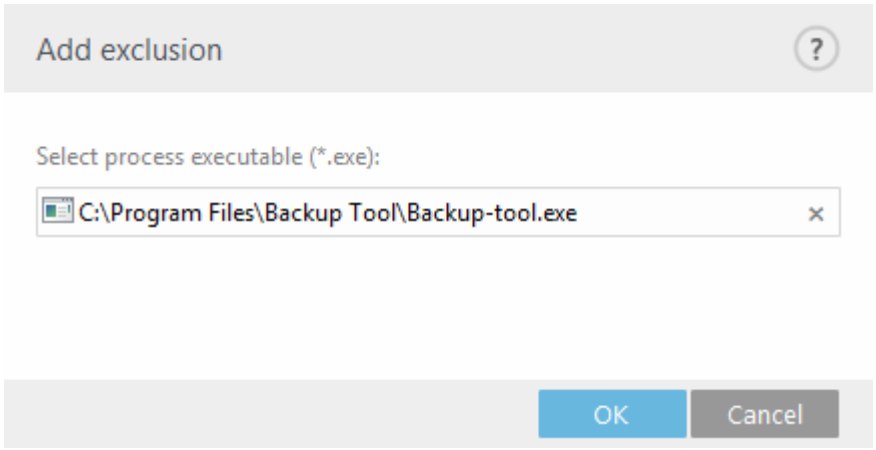
Prostřednictvím těchto výjimek můžete minimalizovat možné konflikty a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (*.exe*).

Spustitelný soubor můžete na seznam výjimek přidat v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) v sekci **Detection engine** > **Rezidentní ochrana souborového systému** > **Obecné** > **Vyloučené procesy** nebo přímo ze seznamu běžících procesů (v hlavním okně programu na záložce **Nástroje** > **Spuštěné procesy**).

Tato funkce byla navržena pro vytvoření výjimek na zálohovací nástroje. Vyloučením zálohovacích nástrojů z kontroly nemá pouze vliv na stabilitu systému, ale také rychlost zálohování.

Kliknutím na **Změnit** si otevřete správce **Vyloučených procesů**, kde pomocí tlačítka **Přidat** a použitím průzkumníka vyberete spustitelný soubor (například Backup-tool.exe), který chcete vyloučit z kontroly. Po přidání *.exe* souboru na seznam výjimek přestane ESET Server Security monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

Pokud pro výběr procesu nevyužijete průzkumníka, zadejte absolutní cestu k procesu manuálně. V opačném případě nebude výjimka fungovat korektně a HIPS může generovat chyby.



Seznam procesů vyloučených z kontroly můžete kdykoli **upravit**, stejně tak proces ze seznamu výjimek **odstranit**.

Pro vyloučené procesy se vytvoří výjimka pouze v rezidentní ochraně souborového systému. Pokud například vyloučíte spustitelný soubor internetového prohlížeče, soubory stahované z internetu budou nadále kontrolovány ochranou přístupu na web. Tím je zajištěno, že hrozba, která se snaží dostat do počítače touto cestou, bude detekována. Jedná se pouze o příklad, z bezpečnostních důvodů nedoporučujeme vytvářet výjimku na internetový prohlížeč.

Cloudová ochrana

ESET LiveGrid® je pokročilý systém včasného varování před novými hrozbami využívající cloudové technologie. Tento systém využívá reputaci souborů, díky čemuž pomáhá při detekci zcela nových hrozeb a zvyšuje výkon kontroly souborů na základě seznamu čistých souborů. Informace o nových hrozbách je v reálném čase předávána do cloudu, což umožňuje specialistům z virových laboratoří ESET udržovat ochranu před hrozbami na nejvyšší možné úrovni. Uživatelé mají díky tomuto systému možnost ověřit přímo z rozhraní produktu ESET, případně kontextového menu, reputaci souborů a spuštěných procesů – a získat o těchto objektech další informace ze systému ESET LiveGrid®.

Po dokončení instalace ESET Server Security si vyberte jednu z následujících možností:

- Můžete se rozhodnout, že nechcete zapínat ESET LiveGrid®. Nepřijdete tím o žádnou funkci, ale v některých případech může ESET Server Security reagovat na nové hrozby se zpožděním – dokud nedojde k aktualizaci detekčního jádra.

- Můžete ESET LiveGrid® nakonfigurovat pro odesílání anonymních informací o nových hrozbách společně s informací, kde byl soubor detekován. Tyto informace mohou být odeslány do virových laboratoři ESET k bližší analýze. Jejich analýza nám pomůže vylepšovat detekční schopnosti programu a aktualizovat detekční moduly.

ESET LiveGrid® shromažďuje z vašeho počítače pouze informace, které se týkají nových infiltrací. To může zahrnovat vzorek nebo kopii souboru, ve kterém se infiltrace objevila, název složky, kde se soubor nacházel, název souboru, informaci o datu a čase detekce, způsob, jakým se infiltrace dostala do počítače a informaci o používaném operačním systému.

Standardně ESET Server Security odesílá podezřelé soubory do virové laboratoře ESET pro detailní analýzu. Soubory s některými příponami, například .docx nebo .xlsx, se neodesílají. Na seznam výjimek můžete přidat další přípony souborů, jejichž obsah nechcete vy nebo vaše organizace odesílat.

Zapnout reputační systém ESET LiveGrid® (doporučeno)

Systém ESET LiveGrid® pracující na základě reputace zvyšuje účinnost antivirového řešení ověřováním souborů vůči online databázi povolených a zakázaných souborů.

Zapnout systém zpětné vazby ESET LiveGrid®

Po aktivování této možnosti budou data zasílána k bližší analýze do virových laboratoří ESET.

Odesílat informace o pádech a diagnostická data

Po aktivování se budou do společnosti ESET odesílat informace o pádech programu a jednotlivých modulů.

Odesílat anonymní statistiky

Aktivováním této možnosti povolíte sběr informací o nově detekovaných hrozbách jako je název hrozby, datum a čas detekce, modul, který hrozbu detekoval a související metadata, kontrolované soubory (kontrolní součet, název souboru, zdroj souboru, telemetrie), blokované a podezřelé URL, verzi produktu a jeho konfiguraci včetně informací o operačním systému.

Kontaktní e-mail

Zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Pokud nejsou vyžadovány další informace, standardně nebudete kontaktováni.

Odesílání vzorků

Automatické odesílání infikovaných vzorků
Aktivováním této možnosti se budou všechny infikované vzorky odesílat do společnosti ESET k analýze a vylepšení detekce. K dispozici jsou následující možnosti:
- Všechny infikované vzorky
- Všechny vzorky kromě dokumentů
- Neodesílat

Automatické odesílání podezřelých souborů
Podezřelé soubory, pravděpodobné infiltrace nebo nežádoucí chování bude odesíláno do společnosti ESET prostřednictvím technologie.
- **Spustitelné soubory** – zahrnuje následující typy souborů: .exe, .dll, .sys
- **Archivy** – zahrnuje následující typy souborů: .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Skripty** – zahrnuje následující typy souborů: .bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Ostatní** – zahrnuje následující typy souborů: .jar, .reg, .msi, .swf, .lnk
- **Pravděpodobný spam** – aktivováním této možnosti pomůže vylepšit globální detekci nevyžádané pošty.
- **Dokumenty** – zahrnuje Microsoft Office dokumenty a PDF s aktivním obsahem.

Výjimky
Klikněte na Změnit a definujte seznam souborů, které nebudou prostřednictvím ESET LiveGrid® odesílány k analýze do virových laboratoří ESET.
Maximální velikost vzorku (MB)
Definujte maximální velikost vzorku, který může být odeslán.

ESET LiveGuard Advanced

Službu ESET LiveGuard Advanced je možné na klientské stanici aktivovat prostřednictvím ESET PROTECT Web Console. V ESET PROTECT Web Console vytvořte novou politiku, nebo si otevřete některou z existujících, a po provedení požadovaných změn ji přiřaďte zařízením, na kterých chcete ESET LiveGuard Advanced zapnout.

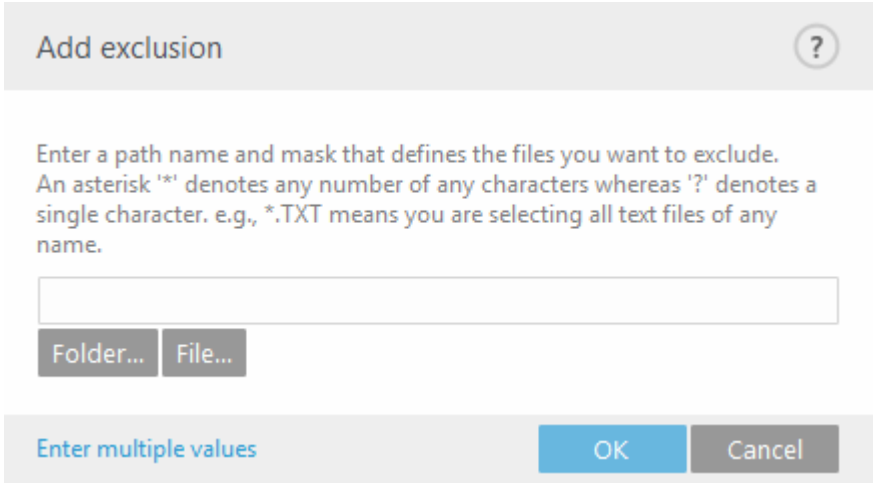
Filtr výjimek

To může být užitečné v případě souborů, které mohou obsahovat důvěryhodné informace, jako jsou dokumenty nebo tabulky.

Vypsané soubory nebudou nikdy zaslány laboratořím ESET k analýze, ani kdyby obsahovaly škodlivý kód

Ve výchozím nastavení jsou vyloučeny nejběžnější typy souborů (*.doc*). Do seznamu výjimek můžete přidat vlastní typy souborů.

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



Pokud naleznete podezřelý soubor, můžete jej okamžitě odeslat na analýzu do virové laboratoře ESET. V případě, že se jedná o škodlivou aplikaci, její detekce bude přidána do další aktualizace detekčního jádra.

Detekce škodlivého kódu

V této části můžete specifikovat parametry volitelných kontrol počítače.

Výběr profilu kontroly je platný pro **Volitelnou kontrolu**, Hyper-V kontrolu a OneDrive kontrolu.

Vybraný profil

Sada parametrů používaná skenerem volitelné kontroly. Vyberte si některý z předdefinovaných profilů kontroly nebo si vytvořte nový. Jednotlivé profily se od sebe mohou lišit nastavením parametrů skenovacího jádra ThreatSense.

Seznam profilů

Pro vytvoření nového profilu, klikněte na **Změnit**: Zvolte jméno pro profil a klikněte na **Přidat**. Nový profil bude následně dostupný v rozbalovacím menu **Vybraný profil** společně s již existujícími profily kontroly.

Cíle kontroly

Pro definování cíle klikněte na **Změnit** a využijte rozbalovací menu případně si vyberte vlastní cíle ze stromové

struktury.

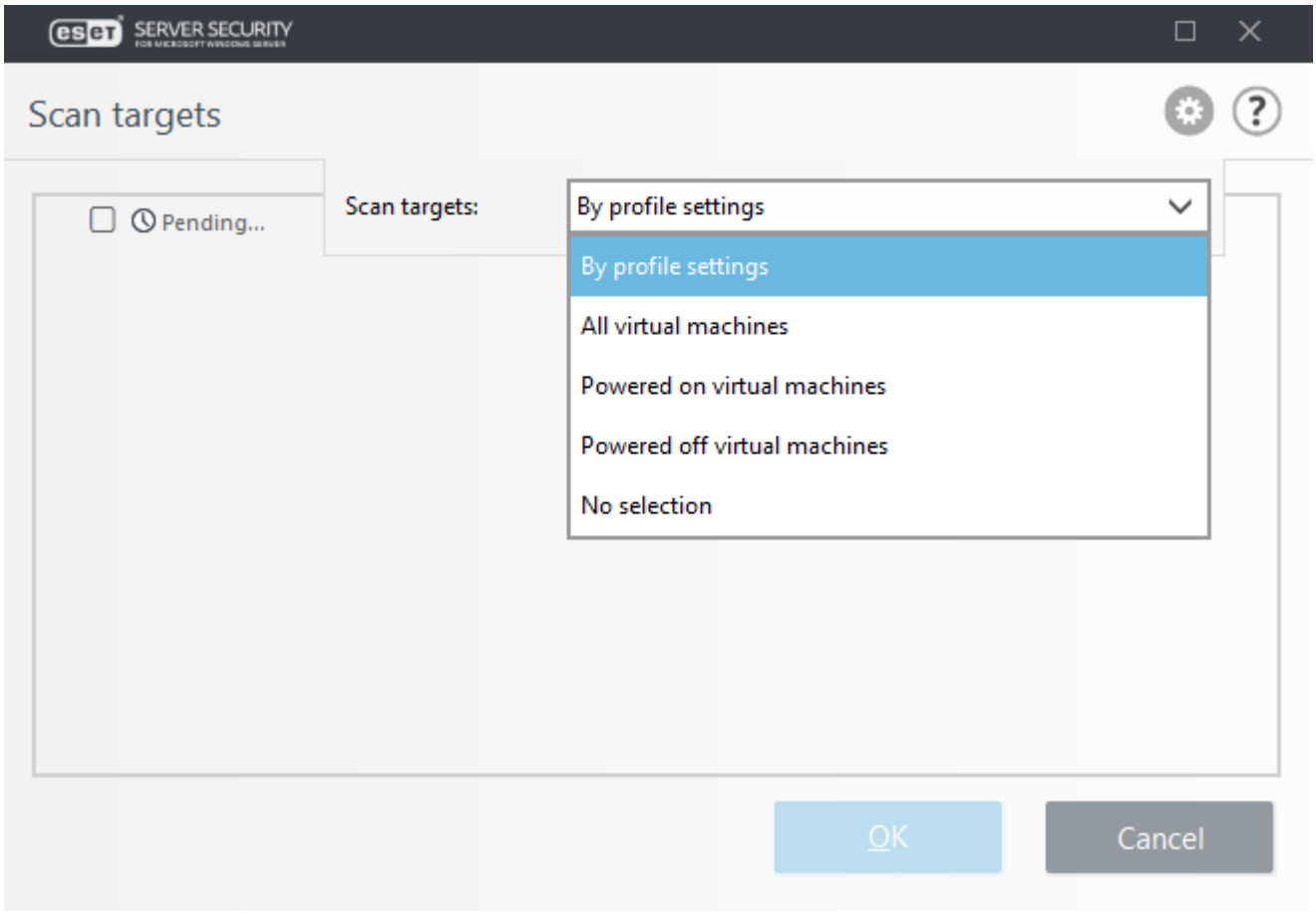
Parametry skenovacího jádra ThreatSense

V této sekci upravíte parametry pro volitelnou kontrolu počítače.

Volitelná kontrola s využitím strojového učení

Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení.

Okno Hyper-V kontroly:



Při definování **Hyper-V kontroly** můžete v rozbalovacím menu **Cíle kontroly** pro vybrat následující předdefinované cíle:

Podle nastavení profilu	**Vybere cíle definované v profilu kontroly.**
Všechny virtuální stroje	Vybere všechny virtuální stroje.
Zapnuté virtuální stroje	Vybere všechny online VM.
Vypnuté virtuální stroje	Vybere všechny offline VM.
Bez výběru	Vymaže výběr.

Kliknutím na tlačítko **Kontrolovat** spustíte kontrolu počítače s nastavenými parametry. Po dokončení kontroly si protokol můžete prohlédnout v hlavním menu v sekci **Protokoly** > Hyper-V kontrola.

Správa profilů

V rozbalovacím menu Profil kontroly jsou dostupné následující předdefinované profily:

- Smart kontrola
- Kontrola počítače z kontextového menu
- Hloubková kontrola počítače
- Můj profil (aplikuje se naHyper-V kontrolu, modul aktualizace a OneDrive kontrolu)

Při vytváření profilu vyhovující vašim potřebám se můžete inspirovat v kapitole Nastavení parametrů skenovacího jádra ThreatSense, ve které je popsán každý parametr kontroly.

Správce profilů naleznete v nastavení produktu ESET Server Security na následujících místech:

Volitelná kontrola počítače

Oblíbená nastavení kontroly počítače si můžete uložit do profilů pro jejich opakované použití v budoucnu. Doporučujeme vytvořit nový profil (s různými cíli kontroly, metodami a dalšími parametry) pro každou pravidelně používanou kontrolu.

Aktualizace

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

Hyper-V kontrola

Pro vytvoření nového profilu klikněte na řádku **Seznam profilů** na **Změnit**. Nový profil bude následně dostupný v rozbalovacím menu **Vybraný profil** společně s již existujícími profily kontroly.

OneDrive kontrola

Pro vytvoření nového profilu klikněte na řádku **Seznam profilů** na **Změnit**. Nový profil bude následně dostupný v rozbalovacím menu **Vybraný profil** společně s již existujícími profily kontroly.

Cíle profilu

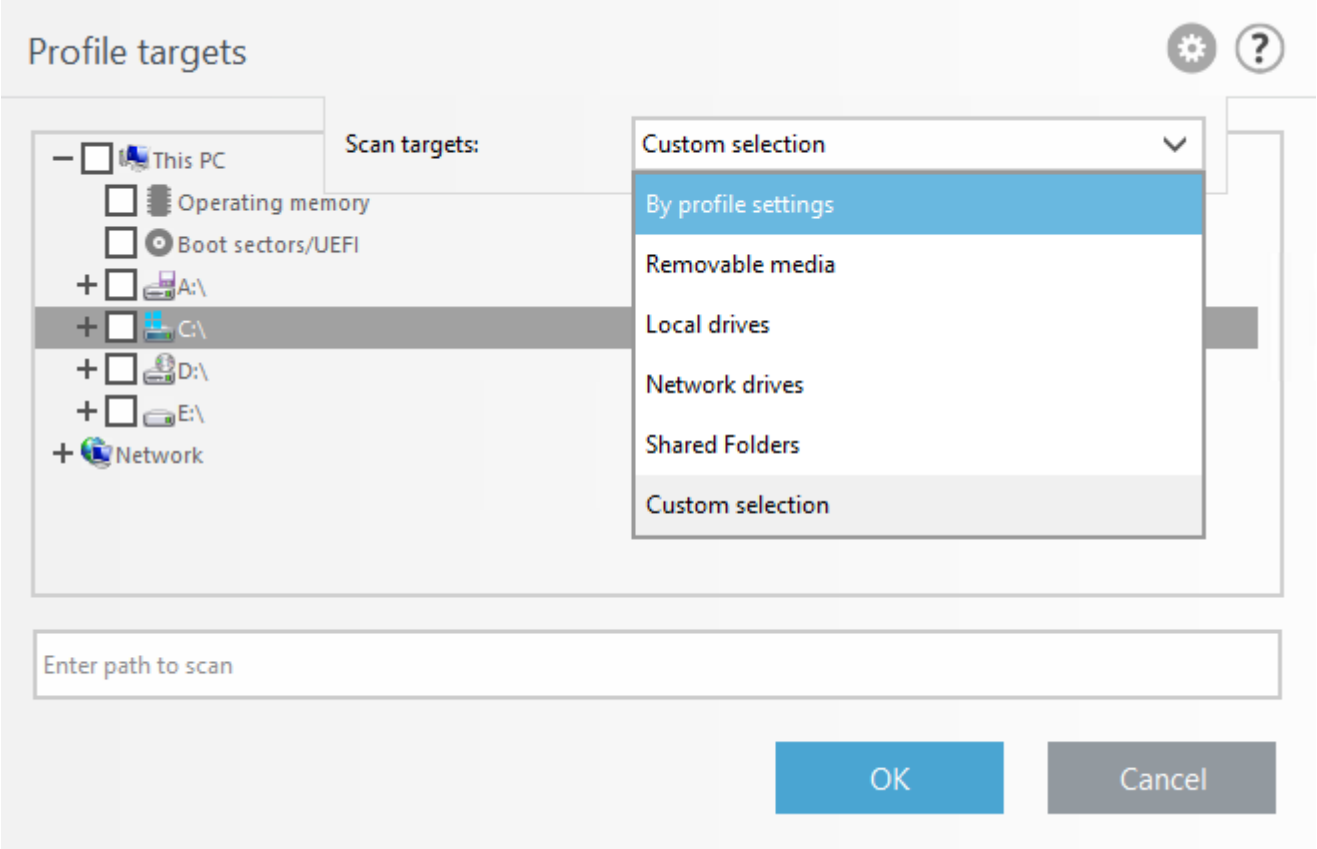
V této sekci můžete určit, co budete kontrolovat na možné infiltrace. Vyberte objekt (paměť, bootovací sektor a UEFI, disky, soubory, složky nebo síť) ze stromové struktury zahrnující dostupné cíle vašeho systému. Kliknutím na ikonu ozubeného kola v levém horním rohu otevřete rozbalovací nabídky **Cíl skenování** a **Profil skenování**.

Výběr profilu kontroly je platný pro Volitelnou kontrolu, Hyper-V kontrolu a OneDrive kontrolu.

Operační paměť	Kontrola všech procesů a dat aktuálně nahraných v operační paměti.
Boot sektory/UEFI	Kontrola přítomnosti škodlivého kódu v boot sektorech disků a UEFI. Pro více informací o UEFI skeneru přejděte do slovníku pojmů.

Operační paměť	Kontrola všech procesů a dat aktuálně nahraných v operační paměti.
WMI databáze	Kontrola celé Windows Management Instrumentation (WMI) databáze, všech jmenných prostorů, tříd instancí a vlastností. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor.
Registr systému	Kontrola celého registru systému, všech klíčů a podklíčů. Vyhledává odkazy na infikované soubory nebo malware vložený jako datový soubor. Při léčení detekce zůstane v registru odkaz, aby se zabránilo ztrátě důležitých dat.

Pro rychlejší přechod k cílové složce nebo souboru určených ke kontrole zadejte cestu do prázdného pole pod stromovou strukturou.



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

Podle nastavení profilu	Vybere cíle definované v profilu kontroly.
Výměnná média	Vybere disky, USB flash disky, CD/DVD.
Lokální disky	Vybere všechny pevné disky v systému.
Síťové disky	Vybere všechny namapované síťové disky.
Sdílené složky	Vybere všechny sdílené složky na lokálním serveru.
Bez výběru	Vymaže výběr. Vymazání můžete provést pomocí vlastního výběru.

Chcete-li rychle přejít na cíl kontroly (soubor nebo složka) a zahrnout jej do kontroly, zadejte jeho cestu do textového pole pod stromovou strukturou. Textové pole rozlišuje velká a malá písmena.

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

- Smart kontrola
- Kontrola počítače z kontextového menu

- Hloubková kontrola počítače

Profily kontroly používají různé parametry skenovacího jádra ThreatSense.

Kontrolovat bez léčení

V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, vyberte možnost **Kontrolovat bez léčení**. Tuto možnost využijte, pokud chcete získat pouze přehled o aktuálním stavu bezpečnosti počítače – zda je infikován, a jakými objekty. Kliknutím na **Nastavit** můžete následně na záložce **Parametry skenovacího jádra ThreatSense pomocí rozbalovacího menu Léčení** nastavit tři úrovně léčení kontrolovaných souborů. Informace o provedené kontrole se uloží do protokolu.

Ignorovat výjimky

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

Cíle kontroly

Pokud nechcete kontrolovat celý disk, ale pouze specifickou oblast, při definování **Volitelné kontroly** využijte některé z předdefinovaných cílů v rozbalovacím menu **Cíle kontroly**, případně si vyberte vlastní cíle ze stromové struktury.

Cíle definované v profilu kontroly jsou platné pro:

- Volitelnou kontrolu
- Hyper-V kontrola
- OneDrive kontrola

Chcete-li rychle přejít na cíl kontroly nebo přidat nový cílový soubor nebo složku, zadejte název do prázdného pole pod seznamem složek. To je možné pouze tehdy, pokud nejsou ve stromové struktuře vybrány žádné cíle a nabídka **Cíle kontroly** je nastavena na **Bez výběru**.

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

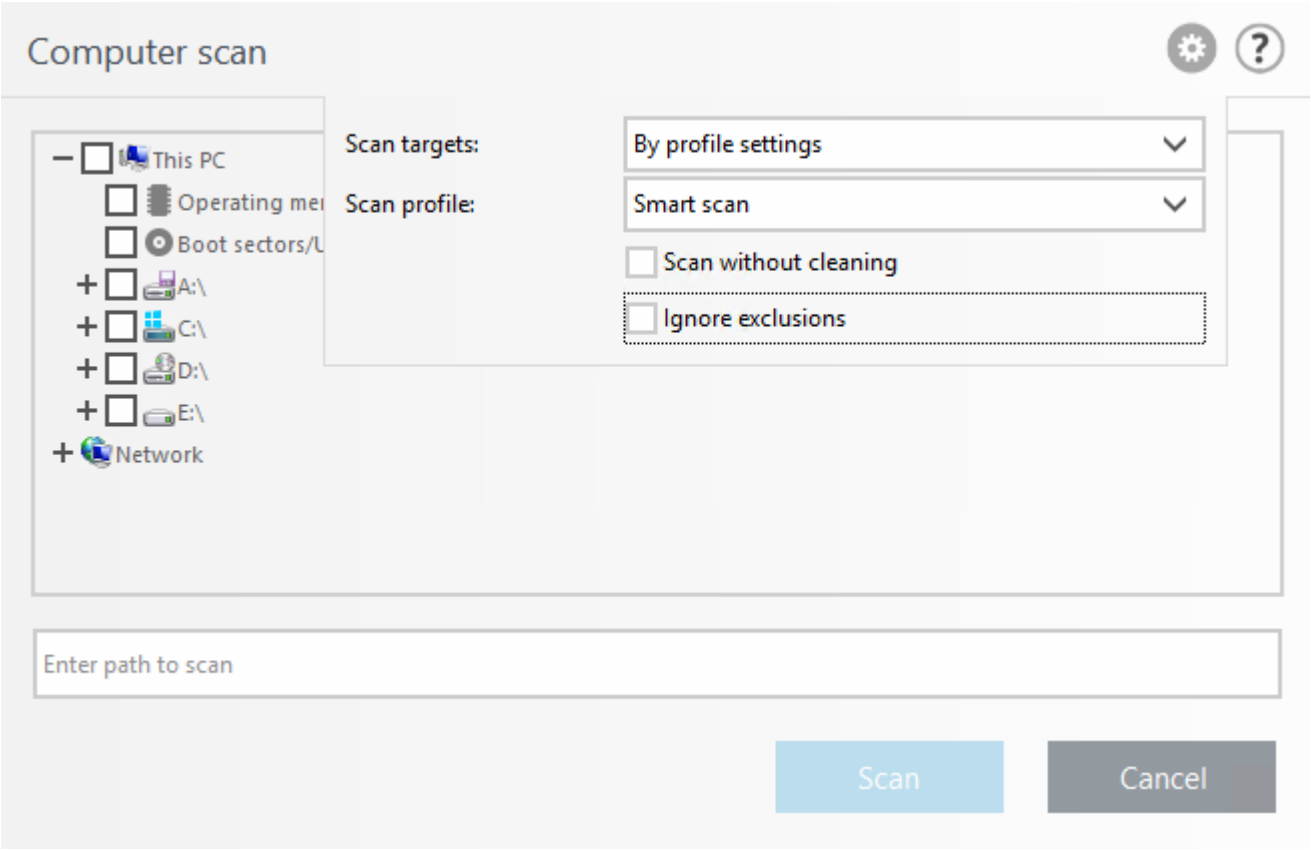
Při definování kontroly můžete v rozbalovacím menu **Cíle kontroly** vybrat následující cíle:

Podle nastavení profilu	Vybere cíle definované v profilu kontroly.
Výměnná média	Vybere disky, USB flash disky, CD/DVD.
Lokální disky	Vybere všechny pevné disky v systému.
Síťové disky	Vybere všechny namapované síťové disky.

Podle nastavení profilu	Vybere cíle definované v profilu kontroly.
Sdílené složky	Vybere všechny sdílené složky na lokálním serveru.
Bez výběru	Vymaže výběr. Vymazání můžete provést pomocí vlastního výběru.

Profil můžete vybrat z rozbalovací nabídky Profilu kontroly, která se použije pro kontrolu vybraných cílů. Výchozí profil je **Smart kontrola**. K dispozici jsou dále dva předdefinované profily kontroly: **Hloubková kontrola** a **kontrola z kontextového menu**. Profily kontroly používají různé parametry skenovacího jádra ThreatSense.

Okno **volitelné kontroly**:



Kontrolovat bez léčení

V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, vyberte možnost **Kontrolovat bez léčení**. Tuto možnost využijte, pokud chcete získat pouze přehled o aktuálním stavu bezpečnosti počítače – zda je infikován, a jakými objekty. Kliknutím na **Nastavit** můžete následně na záložce **Parametry skenovacího jádra ThreatSense pomocí rozbalovacího menu Léčení** nastavit tři úrovně léčení kontrolovaných souborů. Informace o provedené kontrole se uloží do protokolu.

Ignorovat výjimky

Po vybrání této možnosti nebudou brány v potaz výjimky a dané soubory se zkontrolují.

Kontrola počítače

Kliknutím spustíte kontrolu počítače s definovanými parametry.

Kontrolovat jako administrátor

Pomocí této možnosti spustíte kontrolu pod účtem Administrátora. Tuto funkci použijte v případě, že aktuálně

přihlášený uživatel nemá dostatečná práva pro kontrolu souborů. Mějte na paměti, že tlačítko není dostupné, pokud uživatel nemůže provádět UAC operace jako administrátor.

Kontrola při nečinnosti

Tichá kontrola všech lokálních disků v počítači se spouští v případě, že je počítač ve stavu nečinnosti. **Kontrola při nečinnosti** se může spustit při těchto událostech:

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

Spuštění i při napájení počítače z baterie

Standardně se kontrola při nečinnosti nespouští, pokud je počítač (notebook) napájen z baterie. Toto nastavení můžete změnit zaškrtnutím možnosti Spustit také při napájení počítače z baterie.

Zapisovat do protokolu

Vyberte možnost Zapisovat do protokolu, pokud chcete průběh kontroly zapisovat do protokolu a mít k výsledkům přístup ze sekce Nástroje > Protokoly > Kontrola počítače.

Parametry skenovacího jádra ThreatSense

V této sekci upravíte parametry skeneru při nečinnosti.

Kontrola souborů zaváděných při startu počítače

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

Možnosti nastavení kontroly po startu jsou součástí naplánované úlohy **Kontrola souborů spouštěných po startu**.

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

Automatická kontrola souborů spouštěných při startu počítače

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

Pomocí rozbalovacího menu Cíle kontroly můžete upravit množství souborů, které se má kontrolovat. Možnosti kontroly jsou seřazeny vzestupně podle následujících kritérií:

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

Mezi tyto možnosti patří také tyto dvě:

Soubory spouštěné před přihlášením uživatele

Zahrnuje soubory z míst, ke kterým může být přistupováno bez toho, aby byl uživatel přihlášen (typicky všechny položky po spuštění jako jsou služby, browser helper objects, winlogon oznámení, záznamy plánovače Windows, známé dll atd.)

Soubory spouštěné po přihlášení uživatele

Soubory spouštěné po přihlášení uživatele – zahrnuje soubory z míst, ke kterým může být přistupováno až po přihlášení uživatele (typicky soubory, které jsou spouštěny pro daného uživatele, nejčastěji umístěné v klíči registru *HKEY_CURRENT_USER**SOFTWARE**Microsoft**Windows**CurrentVersion**Run*).

Seznamy souborů ke kontrole jsou pro každou skupinu pevně definovány.

Priorita kontroly

Umožňuje nastavit úroveň priority, při které se spustí kontrola počítače:

- **Normální** – zatížení systému je běžné,
- **Nižší** – zatížení systému je nižší,
- **Nejnižší** – zatížení systému je nejnižší,
- **Při nečinnosti** – úloha se provede pouze v době, kdy je systém nečinný.

Výměnná média

ESET Server Security dokáže automaticky kontrolovat výměnná média (CD/DVD/USB/...). Tento modul umožňuje kontrolovat vložená média. Tuto funkci můžete využít pro zvýšení zabezpečení, kdy chcete zabránit uživatelům v připojování médií s infikovaným obsahem.

Akce po vložení výměnného média

Vyberte akci, kterou chcete provést při vložení výměnného média (CD/DVD/USB) do počítače.

- **Nekontrolovat** – neprovede se žádná akce a nezobrazí se okno s možností výběru akce. Okno Detekováno nové zařízení se nezobrazí.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí volitelná kontra obsahu.

- **Zobrazit možnosti kontroly** – zobrazí uživateli okno s možností výběru akce.

Pokud vyberete Zobrazit možnosti kontroly, po připojení média se zobrazí upozornění s výběrem akcí:

- **Zkontrolovat nyní** - spustí se ruční kontrola výměnného média,
- **Zkontrolovat později** – neprovede se žádná akce a okno Detekováno nové zařízení se zavře,
- **Nastavení...** – otevře Rozšířená nastavení
- **Vždy použít vybranou možnost** – pokud zaškrtnete toto pole, při příštím připojení výměnného média se provede vámi vybraná akce.

Kromě toho ESET Server Security disponuje pokročilými funkcemi pro správu zařízení, které vám umožňují definovat pravidla pro zacházení s externími zařízeními. Více informací naleznete v kapitole Správa zařízení.

Ochrana dokumentů

Ochrana dokumentů – tato funkce zajišťuje kontrolu Microsoft Office dokumentů ještě předtím, než jsou otevřeny, a zároveň kontroluje automaticky stahované soubory v Internet Exploreru jako jsou Microsoft ActiveX prvky, Tento modul přidává další bezpečnostní vrstvu do rezidentní ochrany a může být deaktivován pro zvýšení výkonu systému, na kterých neotevíráte velké množství dokumentů Microsoft Office.

Pomocí přepínače Integrovat do systému aktivujete ochranu webkamery.

Pomocí této možnosti zapnete rozšířenou ochranu Microsoft Office dokumentů (za běžných okolností není vyžadována.

Parametry skenovacího jádra ThreatSense

V této části můžete modifikovat parametry ochrany dokumentů.

> Tento modul pracuje pouze s aplikacemi, které podporují rozhraní Microsoft Antivirus API (například Microsoft Office 2000 a novější nebo Microsoft Internet Explorer 5.0 a novější).

Hyper-V kontrola

Aktuální verze Hyper-V kontroly podporuje online nebo offline skenování virtuálního systému v Hyper-V. Jsou zde uvedeny podporované typy skenování podle hostovaného systému Windows Hyper-V a stav virtuálního systému:

Virtuální systémy s funkcí Hyper-V	online virtuální počítač	offline virtuální počítač
Windows Server 2022 Hyper-V	pouze pro čtení	pouze pro čtení / léčení
Windows Server 2019 Hyper-V	pouze pro čtení	pouze pro čtení / léčení
Windows Server 2016 Hyper-V	pouze pro čtení	pouze pro čtení / léčení
Windows Server 2012 R2 Hyper-V	pouze pro čtení	pouze pro čtení / léčení
Windows Server 2012 Hyper-V	pouze pro čtení	pouze pro čtení / léčení
Windows Server 2008 R2 SP1 Hyper-V	ne	pouze pro čtení / léčení

Hardwarové požadavky

Po spuštění kontroly byste neměli zaznamenat negativní dopad na výkon virtuálních počítačů. Činnost kontroly využívá primárně prostředky procesoru. Pro kontrolu online virtuálních počítačů je nutné volné místo na jeho discích. Pokud kontrolovaný virtuální počítač běží, musí být na virtuálním počítači volné místo na disku (alespoň dvojnásobné než je místo, které zabírá samotný virtuální disk + snapshoty).

Specifická omezení

- Kontrola RAID úložiště, rozdělených svazků a dynamických disků není podporována vzhledem k tomu, jak se dynamické disky chovají. Pokud je to možné, z tohoto důvodu se vyhněte použití dynamických disků.
- Kontrola je vždy prováděna na samotném virtuálním stroji. Kontrolní body/snapshoty nebudou ovlivněny.
- ESET Server Security nepodporuje Hyper-V běžící v clusteru.
- Na virtuálních počítačích běžících na Hyper-V hostovaných na Windows Server 2008 R2 SP1 není k dispozici standardní a přísná úroveň léčení. Kontrola disků virtuálních strojů v tomto případě probíhá pouze v režimu pro čtení, bez ohledu na konfiguraci parametrů skenovacího jádra ThreatSense.

> While ESET Security supports the scan of virtual disk MBRs, read-only scanning is the only method supported for these targets. Nastavení můžete v případě potřeby změnit v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) v sekci **Detection engine** > **Hyper-V scan** > parametry skenovacího jádra ThreatSense > **Boot sektory**.

Kontrolovaný virtuální počítače je offline (vypnutý)

Prostřednictvím nástroje Hyper-V Management a podporou virtuálních disků dokáže ESET Server Security detekovat disky s operačním systémem a připojit je. Tímto způsobem má ESET Server Security stejný přístup k obsahu virtuálních disků, jaké má při přístupu k datům a souborům na jakékoli jiné jednotce.

Kontrolovaný virtuální počítač je online (běží, pozastavený, uložený)

Prostřednictvím nástroje Hyper-V Management s podporou virtuálních disků dokáže ESET Server Security detekovat disky s operačním systémem. Protože v tomto případě není možné disk připojit. Z tohoto důvodu ESET Server Security vytvoří checkpoint/snapshot virtuálního počítače, k němuž se následně připojí. Po dokončení kontroly je kontrolní bod/snapshot odstraněn. Kontrola v režimu pouze pro čtení může být provedeno, protože spuštěné virtuální počítače nejsou ovlivněny aktivitou kontroly.

To povoluje ESET Server Security až jednu minutu k vytvoření snapshotu během skenování. Před spuštěním Hyper-V kontroly na velký počet virtuálních počítačů zvažte dopady na vaši infrastrukturu.

Jmenná konvence

Modul Hyper-V kontroly používá níže uvedenou jmennou konvenci:

```
VirtualMachineName\DiskX\VolumeY
```

kde X je číslo disku a Y číslo jednotky. Příklad:

```
Computer\Disk0\Volume1
```

Číselná přípona jednotky se odvíjí od pořadí disku, tak jak jej vidíte ve správci disků virtuálního počítače. Uvedená jmenná konvence je použita také při výběru cílů, zobrazena v průběhu kontroly a protokolech.

Provedení kontroly

- On-demand - Click **Hyper-V Scan** to view a list of Virtual Machines and volumes available for scanning. Vyberte virtuální počítač/-e, disk/-y nebo svazky a klikněte na **Kontrola**.
- Vytvořením naplánované úlohy.
- Prostřednictvím klientské úlohy Kontrola serveru zaslané z ESET PROTECT.
- Hyper-V kontrolu můžete nastavit a spustit prostřednictvím eShell.

Můžete spustit několik Hyper-V kontrol současně. Po dokončení kontroly se zobrazí oznámení s odkazem na protokol kontroly.

Možné problémy

- Při provádění kontroly online virtuálního počítače je třeba vytvořit kontrolní bod/snímek konkrétního virtuálního počítače. Během vytváření kontrolního bodu/snímku mohou být omezeny nebo zakázány některé obecné akce virtuálního počítače.
- Pokud je kontrola virtuálního počítače prováděna offline, nelze jej zapnout, dokud není skenování dokončeno.
- Hyper-V Manager umožňuje pojmenovat dva rozdílné virtuální počítače stejným jménem. Při procházení protokolů kontroly můžete mít problém s odlišením těchto počítačů.

Hyper-V ochrana s využitím strojového učení

Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení.

Parametry skenovacího jádra ThreatSense

Úprava parametrů pro Hyper-V kontrolu.

OneDrive kontrola

Obecné

V této části můžete konfigurovat akci a nastavit pravidla karantény.
Akce, pokud je soubor infikován:
- **Žádná akce** - se souborem nebude provedena žádná akce.
- **Odstranit** - soubor bude přesunut do karantény a odstraněn z OneDrive. Stále však bude dostupná v OneDrive koši.

Přesunout infikované soubory do karantény
Pokud je tato možnost aktivní, soubory označené ke smazání budou přesunuty do karantény. Po jejím vypnutí nebudou soubory uchovávány v karanténě.

Rozšířené

V této části naleznete informace související s registrací OneDrive kontroly (ID aplikace, ID objektu v portálu Azure, Certifikát otisku prstu). Můžete nakonfigurovat časové limity a souběžný limit stahování.

Profily

Pro vytvoření nového profilu klikněte na **Změnit** vedle položky **Seznam profilů**, následně klikněte na **Přidat** a zadejte vlastní **Název profilu**. Nový profil bude následně dostupný v rozbalovacím menu **Vybraný profil** společně s již existujícími profily kontroly.
Prostřednictvím rozbalovacího menu **Cíle kontroly** můžete vybrat ke kontrole předdefinované cíle.
- **Podle nastavení profilu** – Vybere cíle definované v profilu kontroly.
- **Všichni uživatelé** – Vybere všechny uživatele.
- **Bez výběru** – Vymaže výběr.

Kliknutím na tlačítko **Kontrolovat** spustíte kontrolu počítače s nastavenými parametry. Po dokončení kontroly si protokol můžete prohlédnout v hlavním menu v sekci **Protokoly** > OneDrive kontrola.
Parametry skenovacího jádra ThreatSense
V této sekci upravíte parametry OneDrive skeneru.
OneDrive kontrola s využitím strojového učení
Hlášení zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení.

HIPS

HIPS (Host-based Intrusion Prevention System) chrání operační systém před škodlivými kódy a eliminuje aktivity ohrožující bezpečnost počítače. HIPS používá pokročilou analýzu chování kódu, která spolu s detekčními schopnostmi síťového filtru zajišťuje efektivní kontrolu běžících procesů, souborů a záznamů v registru Windows. HIPS je nezávislý na rezidentní ochraně a firewallu a monitoruje pouze běžící procesy v operačním systému.

> ⚠ Pokud nejste zkušený uživatel, nedoporučujeme měnit nastavení systému HIPS. Chybnou úpravou nastavení HIPS se může systém stát nestabilní.

Zapnout ochranu součástí produktu ESET (Self-Defense)

ESET Server Security má vestavěnou technologii Self-Defense, která brání škodlivé aplikaci v narušení nebo zablokování ochrany proti škodlivému kódu. Self-Defense chrání soubory a klíče v registru, které jsou kritické pro správnou funkci produktu a neumožňuje potenciálnímu škodlivému software přístup k těmto záznamům a jejich úpravu. Změny nastavení provedete pomocí možnosti Zapnout HIPS a Zapnout ochranu součástí produktu ESET (Self-Defense) a projeví se až po restartu operačního systému. Z tohoto důvodu se také vypnutí celého systému HIPS projeví až po restartu počítače.

Spustit službu produktu ESET jako protected service

Microsoft představil koncept protected services v Microsoft Windows Server 2012 R2. Tato funkce chrání běžící službu před útoky ze strany škodlivých kódů. Jádro ESET Server Security běží ve výchozí konfiguraci jako protected service. Tato možnost je dostupná na systémech Microsoft Windows Server 2012 R2 a novějších.

Zapnout pokročilou kontrolu paměti (Advanced Memory Scanner)

V kombinaci s Exploit Blockerem poskytuje účinnou ochranu proti škodlivému kódu, který proti detekci antimalwarovými produkty využívá obfuskaci a šifrování. Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve slovníku pojmů .

Blokovat zneužití bezpečnostních děr (Exploit Blocker)

Tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, pdf čtečky a komponenty Microsoft Office). Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve slovníku pojmů .

Zapnout ochranu proti ransomware

Pro využití této funkce musí být aktivní funkce HIPS a ESET Live Grid. Více informací o ransomwaru naleznete ve slovníku pojmů.

Režim filtrování

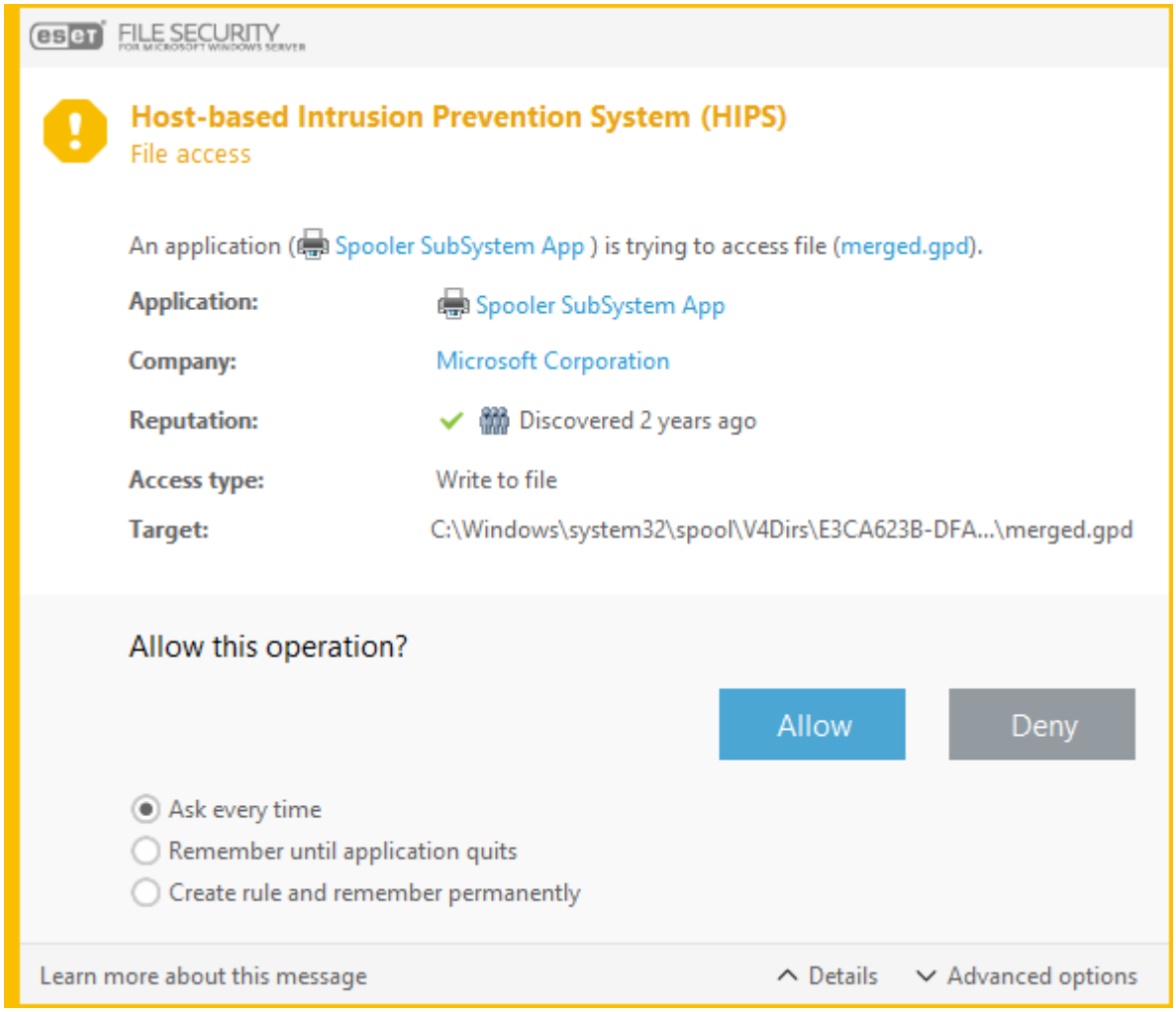
K dispozici jsou následující režimy filtrování:

- **Automatický režim** – operace budou povoleny s výjimkou předdefinovaných pravidel. Vše je povoleno, kromě akcí blokovaných pravidly.
- **Smart režim** – uživatel bude upozorněn pouze na velmi podezřelé události.
- **Interaktivní režim** – uživatel bude vyzván k výběru akce. Dostupné možnosti: Povolit / Blokovat přístup, Vytvořit pravidlo, Dočasně zapamatovat akci.
- **Administrátorský režim** – operace jsou zablokovány. Povoleny jsou pouze operace definované v uživatelských a předdefinovaných pravidlech.
- **Učící režim** – operace jsou povoleny a zároveň je vytvořeno pravidlo, které je povoluje. Pravidla vytvořená tímto režimem jsou viditelná v Editoru pravidel, ale mají nižší prioritu než pravidla vytvořená ručně nebo z dotazovacího dialogu v interaktivní režimu. Při zapnutém učícím režimu se zpřístupní možnost Učící režim bude ukončen. Vyberte datum, do kdy bude učící režim aktivní (maximální počet dní je 14). Po uplynutí tohoto času se zobrazí dialog, ve kterém budete vyzváni ke zhodnocení vytvořených pravidel. Následně si vyberte jiný režim filtrování, odložte rozhodnutí na později nebo ponechte učící režim aktivní.

Pravidla

Pravidla vyhodnocují, zda mají mít aplikace přístup ke konkrétním souborům, částem registru nebo dalším aplikacím. Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům firewallu. Kliknutím na Změnit otevřete editor pravidel HIPS. Pokud je v pravidlech jako akce nastavena možnost **Dotázat se** (standardně), zobrazí se uživateli dialogové okno. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**. Pokud nevyberete žádnou akci, použije se standardní pravidlo z již předdefinovaných.

Přímo z okna HIPS oznámení můžete vytvořit pravidlo na základě akce, které modul HIPS detekoval, a definovat podmínky, za kterých bude tato operace **povolena** nebo **blokována**. Podrobné informace a možnosti konfigurace si zobrazíte kliknutím na **Více informací**. Pravidla vytvořená prostřednictvím tohoto dialogového okna jsou rovnocenná ručně vytvořeným pravidlům. Nicméně ručně vytvořená pravidla mohou být méně specifická než pravidla, která se týkají akce zachycené v tomto dialogovém okně. To znamená, že navzdory vytvořenému pravidlu se může zobrazit výše uvedené okno při detekci operace.



Vždy se dotázat

Po vybrání této možnosti se toto okno zobrazí při každém aktivování pravidla. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**.

Dočasně zapamatovat do ukončení aplikace

Po vybrání možnosti **Zablokovat** nebo **Povolit** se vytvoří dočasné pravidlo, které bude platné do ukončení aplikace, která tuto operaci vyvolala. Pravidlo se smaže rovněž po změně režimu filtrování, úpravě pravidel, aktualizaci modulu HIPS nebo restartování počítače.

Vytvořit pravidlo a trvale zapamatovat

Vybráním této možnosti vytvoříte nové HIPS pravidlo. Kdykoli ho můžete změnit pomocí editoru HIPS.

Úprava pravidla HIPS

Pomocí tohoto dialogové okna můžete spravovat pravidla HIPS.

Pravidlo	Uživatelský nebo automaticky zadaný název pravidla.
Zapnuto	Tento přepínač deaktivujte, pokud chcete ponechat pravidlo v seznamu pravidel, ale nepoužívat ho.

Pravidlo	Uživatelský nebo automaticky zadaný název pravidla.
Akce	Pravidlo specifikuje (právě jednu) akci – Povolit, Zablokovat, Dotázat se – která se má provést, pokud jsou všechny podmínky splněny.
Zdroje	Pravidlo se uplatní, pouze pokud událost vyvolají definované aplikace.
Cíle	Pravidlo se uplatní, pouze pokud se operace provádí nad definovanými aplikacemi, soubory nebo záznamy registru.
Zaznamenávat od úrovně	Pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do protokolu HIPS.
Upozornit uživatele	Pokud dojde ke spuštění události, v oznamovací oblasti Windows se zobrazí oznámení.

Pro vytvoření nového pravidla klikněte na tlačítko **Přidat**, případně vyberte existující a klikněte na **Změnit**.

Název pravidla

Uživatelský nebo automaticky zadaný název pravidla.

Akce

Pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Operace ovlivní

Vyberte typ operace, pro kterou má být pravidlo platné. Konkrétní pravidlo je možné použít pouze pro jeden typ operace nad vybraným cílem. Pravidlo se skládá z částí, které definují podmínky, za kterých se pravidlo uplatní.

Zdrojové aplikace

Pravidlo se uplatní, pouze pokud událost vyvolají definované aplikace. Pro vybrání **konkrétní aplikace** klikněte na tlačítko **Přidat** a vyberte jednotlivé soubory nebo složky aplikace. Pro monitorování všech aplikací vyberte z rozbalovacího menu možnost **Všechny aplikace**.

> Některé operace zvláštních pravidel předefinovaných systémem HIPS nemohou být zablokovány a standardně jsou povoleny. HIPS nemonitoruje všechny systémové operace. HIPS monitoruje operace, které mohou být považovány za nebezpečné.

Popis důležitých operací:

Souborové operace

Vymazat soubor	Aplikace žádá o povolení vymazat cílový soubor.
Zápis do souboru	Aplikace žádá o povolení zapisovat do cílového souboru.
Přímý přístup na disk	Aplikace se snaží číst nebo zapisovat na disk nestandardním způsobem, který obchází běžné procedury Windows. Výsledkem může být změna souboru bez použití příslušného pravidla. Tato operace může být způsobena škodlivým kódem, který se snaží vyhnout se detekci, zálohovacím programem, který kopíruje celý obsah pevného disku nebo správcem oddílů který reorganizuje diskové oddíly.
Nainstalovat globální hook	Volání funkce SetWindowsHookEx z MSDN knihovny pomocí dané aplikace.
Načíst ovladač	Instalace a načítání ovladače do systému.

Pravidlo se uplatní, pouze pokud se operace provádí nad definovaným cílem. Pro vybrání **konkrétních souborů** klikněte na tlačítko **Přidat** a vyberte jednotlivé soubory nebo složky. Pro monitorování všech souborů vyberte z rozbalovacího menu možnost **Všechny soubory**.

Operace s aplikací

Ladění jiné aplikace	Připojení debuggeru k procesu. Při debuggingu můžete sledovat a měnit chování aplikace a přistupovat k jejím datům.
Zachytávat události jiné aplikace	Zdrojová aplikace se pokouší zachytit události cílové aplikace (například pokud se keylogger snaží zachytit aktivitu webového prohlížeče).
Ukončit/přerušit jinou aplikaci	Pozastavení, obnovení nebo ukončení procesu (může být vyvoláno přímo ze Správce úloh nebo ze záložky Procesy).
Spustit novou aplikaci	Spuštění nové aplikace nebo procesu.
Změnit stav jiné aplikace	Zdrojová aplikace se pokouší zapisovat do paměti cílové aplikace, případně se snaží spustit kód pod jejím jménem. Tato funkce je užitečná pro ochranu důležité aplikace, pokud ji nastavíte jako cílovou aplikaci v pravidle, které blokuje tyto operace.

Pravidlo se uplatní, pouze pokud se operace provádí nad definovaným cílem. Pro vybrání **konkrétní aplikace** klikněte na tlačítko **Přidat** a vyberte jednotlivé soubory nebo složky aplikace. Pro monitorování všech aplikací vyberte z rozbalovacího menu možnost **Všechny aplikace**.

Operace se záznamy registru

Úprava nastavení spuštění	Všechny změny v nastavení, definující, které aplikace budou spouštěny při startu operačního systému Windows. Zobrazíte je například vyhledáním klíče Run v Editoru registru Windows.
Vymazání z registru	Vymazání klíče nebo hodnoty.
Přejmenování klíče registru	Přejmenování konkrétního klíče.
Úprava registru	Vytvoření nové hodnoty nebo změna existujících hodnot. Přesouvání dat v rámci datové struktury. Nastavení uživatelských nebo skupinových práv pro dané klíče registru.

Pravidlo se uplatní, pouze pokud se operace provádí nad definovaným cílem. Pro vybrání **konkrétních záznamů** klikněte na tlačítko **Přidat** a vyberte jednotlivé klíče nebo hodnoty. Pro monitorování celého registru vyberte z rozbalovacího menu možnost **Všechny záznamy**.

Při zápisu cíle můžete použít zástupné znaky s jistými omezeními. Místo konkrétního klíče můžete použít v cestě k registru * (hvězdičku) ve významu "libovolný jeden klíč". Například *HKEY_USERS***\software can mean HKEY_USER**.default**software* nepředstavuje *HKEY_USERS**S-1-2-21-2928335913-73762274-491795397-7895**.default**software*. *HKEY_LOCAL_MACHINE**system**ControlSet** není platná cesta ke klíči registru. Cesta registru ukončená * má speciální význam, znamená "tento klíč nebo libovolný podklíč libovolně hluboko." U souborových cílů se dá používat hvězdička pouze tímto způsobem. U vyhodnocování platí, že vždy se hledá nejprve cíl, který popisuje danou cestu přesně, a až poté cíl, který ji popisuje hvězdičkou ((*)).

Pokud vytvoříte příliš obecné pravidlo, program vás na to upozorní.

Rozšířená nastavení HIPS

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

Ovladače, jejichž načtení je vždy povoleno

Vybrané ovladače budou vždy načteny bez ohledu na nastavený režim filtrování, pokud nejsou explicitně blokovány uživatelským pravidlem. Ovladače zobrazené v tomto seznamu budou načteny bez ohledu na režim filtrování HIPS, pokud nejsou výslovně blokovány pravidlem uživatele. Do seznamu můžete **Přidat** nový ovladač, nebo **Upravit** či **Odstranit** stávající.

> Po kliknutí na tlačítko **Obnovit** vymažete všechny ovladače, které jste přidali ručně. Tento postup lze využít v případě, že jste přidali více ovladačů, a nemůžete je ze seznamu vymazat manuálně.

Zapisovat všechny zablokované operace do protokolu

Všechny zablokované operace se zapíší do protokolu HIPS.

Upozornit na změny v seznamu aplikací automaticky spouštěných při startu

Při změně počtu aplikací spouštěných po startu operačního systému se zobrazí oznámení.

Konfigurace aktualizací

Nastavení aktualizace se skládá ze zadání zdroje aktualizace, tedy z nastavení aktualizačních serverů a autentifikace vůči těmto serverům.

> Pro úspěšnou aktualizaci musíte mít správně nastaveny parametry aktualizace. Pokud používáte firewall, ujistěte se, že má produkt ESET povolenou HTTP komunikaci do internetu.

Obecné

Vyberte výchozí aktualizační profil
Vyberte profil, který chcete, aby produkt používal standardně pro stahování aktualizací. Případně si vytvořte nový.
Vyprázdnit aktualizační cache
Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit**.
Aktualizace produktu / Automatické aktualizace
Tato možnost je standardně zapnutá. V případě+ potřeby můžete pomocí tohoto přepínače dočasně zakázat automatické aktualizace produktu ESET Server Security. Tuto možnost doporučujeme ponechat zapnutou, aby si produkt ESET Server Security mohl instalovat nejnovější aktualizace programových komponent (PCU) a mikro aktualizace programových komponent (µPCU) ve chvíli, kdy budou dostupné.

ℹ Aktualizace se aplikují při příštím restartování serveru.

Upozornění na neaktuální detekční jádro

Nastavit automaticky maximální stáří detekčního jádra / Maximální stáří detekčního jádra (ve dnech)
Pro nastavení vlastního stáří detekčního jádra (ve dnech) deaktivujte pomocí přepínače tuto možnost. Bude-li starší, zobrazí se informace, že je detekční jádro zastaralé. Předdefinovaná doporučená hodnota je 7 dní.
Záloha modulů
Pokud máte podezření, že nová verze detekčního jádra/programových modulů nestabilní nebo poškozená, můžete se vrátit k jejich předchozí verzi a na stanovený časový interval zakázat aktualizace. Opačně, pokud jste zakázali na neurčito další aktualizaci, v této sekci ji znovu můžete povolit. ESET Server Security zálohuje detekční jádro a jednotlivé programové moduly pro případ, že byste se potřebovali vrátit ke starší verzi. Aby se mohly vytvářet tzv. snapshoty detekčního jádra, ponechte zapnout možnost vytváření snapshotů modulů.
Počet vytvářených záloh
Určuje počet obrazů předchozích modulů uložených na lokálním disku počítače.
Záloha modulů
Kliknutím na tlačítko Vrátit obnovíte předchozí verze modulů a dočasně zakážete jejich aktualizaci.

Profily
Pro vytvoření nového profilu klikněte na **Změnit** vedle položky **Seznam profilů**. Následně zadejte vlastní **Název profilu** a klikněte na **Přidat**. Následně vámi vytvořený profil vyberte z rozbalovacího menu Profil, a upravte si parametry aktualizace modulů, případně **aktualizačního mirroru**.

Aktualizace

Z rozbalovacího menu si vyberte typ aktualizace, které chcete stahovat:
• **Standardní aktualizace** – tato možnost je vybrána standardně a tím je zajištěno automatické stahování aktualizací ze serverů společnosti ESET.
• **Testovací aktualizace** – jsou aktualizace, které prošly důkladným interním testováním a budou brzy dostupné široké veřejnosti. V předstihu tak získáte přístup k novějším funkcím, opravám a metodám detekce škodlivého kódu. Protože předběžné aktualizace nereprezentují finální kvalitu, neměli byste je instalovat na produkční stroje a pracovní stanice, u kterých je vyžadována stabilita a dostupnost.
• **Opožděné aktualizace** – vybráním této možnosti se aktualizace budou stahovat z aktualizačního severu, na který jsou umisťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

Povolit optimalizaci doručení aktualizací
Po aktivování této možnosti se mohou aktualizační soubory stahovat z CDN (content delivery network). Po vypnutí tohoto nastavení však může dojít ke zpomalení nebo přerušení stahování, pokud budou dedikované servery společnosti ESET přetížené. Zakázání je užitečné, pokud je brána firewall omezena pouze na přístup k aktualizačním serverům ESET na základě jejich IP adres nebo pokud nefunguje připojení ke službám CDN.

Dotázat se před stahováním aktualizací
Vyberete-li možnost, před stažením nové aktualizace se zobrazí informace, že je dostupná aktualizace.

Dotázat se, pokud je velikost aktualizačního souboru větší než (kB)
V případě, že aktualizační soubor bude větší než mezní hranice definovaná v poli Dotázat se, pokud je velikost aktualizačního souboru větší než (kB), zobrazí se oznámení.

Aktualizace modulů
Standardně je vybrána možnost **Automatický výběr serveru**. Aktualizační server představuje místo, kde jsou uložené aktualizační soubory. Pokud chcete stahovat aktualizace ze serverů společnosti ESET, ponechte tuto možnost beze změny.

Pokud používáte lokální HTTP server, aktualizační server by měl být zadán následovně: http://computer_name_or_its_IP_address:2221
Pokud používáte lokální HTTP server s SSL šifrováním, aktualizační server by měl být zadán následovně: https://computer_name_or_its_IP_address:2221
Pokud používáte lokální sdílenou složku, aktualizační server by měl být zadán následovně: \\computer_name_or_its_IP_address\shared_folder

Zapnout častější aktualizace detekčních signatur
Aktivováním této možnosti zkrátíte interval aktualizace detekčního jádra. Vypnutí této možnosti negativně ovlivní detekční schopnosti.

Povolit aktualizaci modulů z výměnného média
Pomocí této možnosti můžete provést aktualizaci z výměnného média, pokud je na něm uložena kopie mirroru. Při nastavené možnosti **Automaticky** se aktualizace provede automaticky na pozadí po připojení výměnného média. Pokud před provedením aktualizace chcete zobrazit potvrzovací dialog, vyberte možnost **Vždy se dotázat**.

Aktualizace produktu
Pozastavením automatických aktualizací v konkrétním aktualizačním profilu dočasně zakážete automatické aktualizace produktu při připojení k internetu pomocí jiných sítí nebo připojení účtovaných podle objemu dat. Pro zajištění neustálého přístupu k nejnovějším funkcím a nejvyšší možné ochrany, je nutné ponechat toto nastavení zapnuté.


Po dokončení aktualizace produktu může být v některých případech vyžadován restart serveru.

Možnosti připojení

Proxy server

Pro přístup k nastavení proxy serveru pro daný aktualizační profil přejděte do této sekce a v rozbalovacím menu Režim proxy vyberte jednu z níže uvedených možností:

- **Nepoužívat proxy server** – vybráním této možnosti nebude ESET Server Security pro aktualizaci používat proxy server.
- **Use global proxy server settings** - Proxy server configuration specified in the Advanced setup (F5) > Tools > Proxy server will be used.
- **Připojení prostřednictvím proxy serveru** – tuto možnosti vyberte v případě, že:

Pro aktualizaci ESET Server Security potřebujete použít jiné, než globální nastavení proxy serveru definované v Rozšířeném nastavení v sekci Nástroje > Proxy server. Pokud vyberte tuto možnost, je potřeba zadat: adresu proxy serveru, komunikační port (standardně 3128), případné také Uživatelské jméno a Heslo (pokud je vyžadováno).

Nebylo definováno globální nastavení proxy serveru, ale pro aktualizaci ESET Server Security se má používat proxy.

Počítač je připojen k internetu pomocí proxy serveru. Nastavení bylo v průběhu instalace programu převzato z Internet Exploreru, ale v průběhu času došlo ke změně nastavení proxy serveru (například z důvodu přechodu k jinému poskytovatel internetu). V tomto případě doporučujeme zkontrolovat nastavení proxy zobrazené v tomto okně a případně jej změnit pro zajištění funkčnosti aktualizací.

Autentifikační údaje, jako **Uživatelské jméno** a **Heslo**, slouží pro přístup k proxy serveru. Tato pole vyplňte pouze v případě, že je proxy server vyžaduje. Mějte na paměti, že se nejedná o údaje, které jste obdrželi při koupi produktu ESET Server Security.

Použít přímé spojení, pokud není dostupný proxy server

Pokud má produkt nastaveno využívání HTTP Proxy a ten nebude dostupný, po aktivování této možnosti se produkt zkusí připojit k serverům ESET bez použití proxy.

Windows sdílení

Při stahování aktualizací ze složky z lokálního Windows serveru je pro vytvoření spojení standardně vyžadována autentifikace pomocí jména a hesla.

Pro připojení do LAN vystupovat jako

Při definování účtu, který bude přistupovat k složce, si vyberte jednu z níže uvedených možností:

- **Systémový účet (standardně)** – pro ověření se použije systémový účet. Za normálních okolností ověření neproběhne, pokud nejsou nastaveny autentifikační údaje v hlavním nastavení aktualizace.
- **Aktuálně přihlášený uživatel** – pokud vyberete tuto možnost, program se bude autentifikovat pod účtem aktuálně přihlášeného uživatele. Nevýhodou tohoto nastavení je nemožnost připojení na server a následné provedení aktualizace, pokud není na počítači přihlášen žádný uživatel.
- **Definovaný uživatel** – po vybrání této možnosti zadejte přihlašovací údaje uživatele, pod kterým se bude aplikace autentifikovat. Tuto možnost doporučujeme v případě, že se nezdaří připojení pod lokálním systémovým účtem. V tomto případě dejte pozor na to, aby měl daný uživatelský účet měl práva pro přístup do složky s aktualizačními soubory na serveru. V opačném případě se spojení nezdaří a aktualizace se nestáhne.

Pokud vyberete možnost **Aktuálně přihlášený uživatel** nebo **Definovaný uživatel**, může nastat chyba při změně identity programu na požadovaného uživatele. Z tohoto důvodu doporučujeme u připojení do LAN nastavit autentifikační údaje v hlavním nastavení aktualizace. V tomto nastavení je potřeba uvést údaje ve tvaru název_domény\uživatel (případně pracovní skupiny: název_pracovní_skupiny\uživatel) a heslo uživatele. Při aktualizaci prostřednictvím HTTP není standardně potřeba autentifikační údaje zadávat.

Po dokončení aktualizace odpojit ze serveru

Pokud aktivujete tuto možnost, po dokončení aktualizace se vynutí ukončení spojení se serverem.

Aktualizační mirror

Možnosti konfigurace lokálního mirroru naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci **Aktualizace** > **Profily** > Aktualizační mirror.

Obnovení předchozí verze modulů

Pokud kliknete na tlačítko **Vrátit**, vyberte z rozbalovacího menu Časový interval, na jak dlouho chcete aktualizaci detekčního jádra a programových modulů pozastavit.

Možnost **Do odvolání** vyberte v případě, kdy chcete aktualizace modulů obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Verze databáze detekčního jádra bude vrácena do posledního uloženého bodu jako snapshot v systému souborů místního počítače.

Aktualizace naplánované úlohy

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

Níže uvedené kroky vás provedou úkolem upravit stávající **Pravidelnou automatickou aktualizaci**.
1. Na hlavní obrazovce **Plánovač** vyberte úlohu **Aktualizovat** s názvem **Pravidelná automatická aktualizace** a klikněte na tlačítko **Upravit**. Otevře se průvodce konfigurací.
2. Nastavení úlohy plánovače, která má být spuštěna, vyberte jednu z následujících možností časování, abyste mohli definovat, kdy má být naplánovaná úloha spuštěna.
3. Chcete-li zabránit spuštění úlohy, když je systém napájen z baterie (například UPS), klikněte na přepínač vedle položky **Přeskočit úlohu při napájení z baterie**.
4. Vyberte možnost Aktualizovat profil pro její provedení. Vyberte akci, která se provede v případě neprovedení úlohy z jakéhokoli důvodu.
5. Pro dokončení klikněte na tlačítko **Dokončit**.

Aktualizační mirror

ESET Server Security dokáže vytvářet kopie aktualizací, z níž lze pak aktualizovat další stanice v lokální síti. Vytváření kopií aktualizačních souborů (tzv. mirroru) je výhodné použít zejména ve velkých sítích, kde by aktualizace každé jedné stanice z Internetu způsobovala velký přenos dat a vytížení linek. Proto je doporučeno aktualizovat z internetu pouze jednoho klienta v síti a následně aktualizaci zpřístupnit pomocí tzv. mirroru (zrcadla) ostatním klientům v lokální síti. Aktualizace stanic z mirroru optimalizuje vyvážení zátěže sítě a šetří šířku pásma internetového připojení.

Aktualizační mirror

Vytvářet aktualizační mirror
Po aktivování se zpřístupní možnosti pro konfiguraci mirroru.
Složka pro uložení
Aktualizační soubory se standardně ukládají do složky C:\ProgramData\ESET\ESET Security\mirror. Pokud ji chcete změnit, nejprve klikněte na **Vymazat**. Pro změnu této složky klikněte na **Změnit** a následně vyberte složku na lokálním serveru nebo sdílenou složku. Pokud je pro přístup do složky vyžadována autentifikace, je nutné definovat Uživatelské jméno a Heslo. Pokud se požadovaná složka nachází na síťovém umístění, které pohání operační systém řady NT, musí mít uživatel, pod kterým se připojujete, oprávnění pro zápis do definovaného umístění.
Uživatelské jméno zadávejte ve formátu Doména/Uživatel nebo Pracovní skupina/Uživatel. Nezapomeňte vyplnit heslo.

Aktualizace programových komponent

Soubory
Při konfiguraci mirroru můžete vybrat jazykovou verzi aktualizací, kterou chcete stahovat. Výběr jazyka musí podporovat server, ze kterého aktualizace stahujete.
Automaticky aktualizovat programové komponenty
Aktivováním této možnosti zajistíte automatickou instalaci nových a aktualizaci stávajících funkcí. Může probíhat automaticky bez zásahu a potvrzení uživatele, nebo s potvrzením. Instalace nových programových komponent obvykle vyžaduje restart počítače.
Aktualizovat programové komponenty
Kliknutím na tlačítko aktualizujete programové komponenty na nejnovější verzi.

HTTP server

Port serveru
Standardně server běží na portu 2221. V případě potřeby definujte vlastní číslo portu.
Autentifikace
Definujte způsob ověření pro přístup k aktualizačním souborům. K dispozici jsou následující možnosti: **Žádné**, **Základní** a **NTLM**.
- Vybráním možnosti **Základní** zajistíte, že uživatelské jméno a heslo bude šifrováno jednoduchou metodou kódování base64.
- Možnost **NTLM** zajistí bezpečné zakódování uživatelského jména a hesla. Pro autentifikaci se používají uživatelé vytvoření na stanici poskytující kopie aktualizací.
- Výchozi možnost **Žádná** zpřístupní kopie aktualizací bez nutnosti autentifikace.

> Při této metodě zpřístupnění mirroru musí být složka mirroru na stejném počítači, na kterém je ESET Server Security nainstalován.

SSL pro HTTP Server
Pro běh HTTP serveru s HTTPS (SSL) podporou vyberte vlastní soubor obsahující **řetězec certifikátu** nebo vygenerujte certifikát podepsaný sám sebou K dispozici jsou následující typy certifikátu: PEM, PFX a ASN. Pro zvýšení bezpečnosti můžete použít zabezpečený HTTPS protokol pro stahovací kopií aktualizačních souborů. V takovém případě je téměř nemožné zjistit přenášená data a použité přístupové údaje.
Jako **typ soukromého klíče** je standardně vybrána možnost **Integrovaný** (proto je možnost vybrat soubor obsahující soukromý klíč standardně nedostupná). To znamená, že soukromý klíč je součástí souboru s řetězcem certifikátů.

Možnosti připojení

Windows sdílení
Při stahování aktualizací ze složky z lokálního Windows serveru je pro vytvoření spojení standardně vyžadována autentifikace pomocí jména a hesla.
Pro připojení do LAN vystupovat jako
Při definování účtu, který bude přistupovat k složce, si vyberte jednu z níže uvedených možností:
• **Systémový účet (standardně)** – pro ověření se použije systémový účet. Za normálních okolností ověření neproběhne, pokud nejsou nastaveny autentifikační údaje v hlavním nastavení aktualizace.
• **Aktuálně přihlášený uživatel** – pokud vyberete tuto možnost, program se bude autentifikovat pod účtem aktuálně přihlášeného uživatele. Nevýhodou tohoto nastavení je nemožnost připojení na server a následné provedení aktualizace, pokud není na počítači přihlášen žádný uživatel.
• **Definovaný uživatel** – po vybrání této možnosti zadejte přihlašovací údaje uživatele, pod kterým se bude aplikace autentifikovat. Tuto možnost doporučujeme v případě, že se nezdaří připojení pod lokálním systémovým účtem. V tomto případě dejte pozor na to, aby měl daný uživatelský účet měl práva pro přístup do složky s aktualizačními soubory na serveru. V opačném případě se spojení nezdaří a aktualizace se nestáhne.

⚠ Pokud vyberete možnost **Aktuálně přihlášený uživatel** nebo **Definovaný uživatel**, může nastat chyba při změně identity programu na požadovaného uživatele. Z tohoto důvodu doporučujeme u připojení do LAN nastavit autentifikační údaje v hlavním nastavení aktualizace. V tomto nastavení je potřeba uvést údaje ve tvaru název_domény\uživatel (případně pracovní skupiny: název_pracovní_skupiny\uživatel) a heslo uživatele. Při aktualizaci prostřednictvím HTTP není standardně potřeba autentifikační údaje zadávat.

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

Síťová ochrana

Pro správu síťové ochrany klikněte na možnost Změnit a následně si vytvořte novou nebo upravte již existující:

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

• Zóny – seznam zón můžete konfigurovat ručně v Rozšířeném nastavením (dostupném po stisknutí klávesy F5 v hlavním okně programu) v sekci Síťová ochrana > Obecné > Známé sítě po kliknutí na Změnit.

Známé sítě

Pokud počítač často připojujete k veřejným sítím nebo sítím mimo vaši pracovní síť, doporučujeme vám ověřit důvěryhodnost takových sítí. Po prvotním definování sítě, ESET Server Security může rozpoznat důvěryhodnou síť na základě parametrů definovaných v sekci Identifikace sítě.

To je užitečné pro počítače, které se připojují často do sítí s IP adresami podobnými důvěryhodné zóně. V některých případech, ESET Server Security může prohlásit neznámou síť za důvěryhodnou. Pro eliminaci takového případu doporučujeme používat možnost Autentifikace sítě.

Po připojení počítače k síti nebo změně konfigurace sítě prohledá ESET Server Security seznam známých sítí, zda pro ni nenalezne odpovídající záznam. V případě, že Identifikace sítě a Autentifikace sítě (nepovinné) bude vyhovovat záznamu, síť bude označená jako připojená.

V případě, že nebude nalezena žádná známá síť, vytvoří se nová na základě zjištěné konfigurace sítě. Ve výchozím nastavení bude nové síťové připojení používat typ síťové ochrany jako u veřejné sítě.

Po připojení k takové síti se zobrazí dialog Zjištěno připojení k nové síti, pomocí kterého nastavíte režim ochrany v

síti – Domácí nebo firemní síť / Veřejná síť, případně můžete vybrat možnost Převzít nastavení z Windows. Pokud se připojíte k již známé síti, jejíž režim ochrany je nastaven na Domácí nebo firemní síť, všechny podsítě této sítě budou přidány do důvěryhodné zóny.

Typ ochrany nové sítě

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

Známé sítě můžete konfigurovat ručně pomocí Editoru známých sítí.

Přidat síť

Nastavení sítě je rozloženo do následujících záložek.

Síť

V této sekci můžete definovat **název sítě** a **typ ochrany**. Další adresy zadané do pole **Další důvěryhodné adresy** budou vždy přidány do důvěryhodné zóny adaptéru připojeného do této sítě (bez ohledu na režim ochrany sítě).

- Upozornit na slabě zabezpečenou Wi-Fi síť – po aktivování této možnosti vás ESET Server Security upozorní při připojení nezabezpečené nebo slabě zabezpečené bezdrátové síti.
- Profil firewallu bude zděděn ze síťového adaptéru.
- Aktualizační profil – vyberte profil, který se použije pro aktualizaci při připojení k této síti.

Identifikace sítě

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

Autentifikace sítě

V síti se vyhledává specifický server a pro vlastní autentifikaci vůči serveru používá asymetrické šifrování (RSA). Název autentifikované sítě musí odpovídat názvu sítě definovaném v nastavení autentifikačního serveru. V názvu sítě se rozlišuje velikost písmen. Zadejte název serveru, port, na kterém poslouchá server a veřejný klíč, který odpovídá soukromému klíči serveru. Název serveru můžete zadat ve formě IP adresy, DNS nebo NetBios názvu, a za názvem serveru může následovat cesta upřesňující umístění klíče na serveru (např. jméno_serveru/složka1/složka2/autentifikace). Také můžete zadat více serverů, oddělených středníkem.

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

- PEM zašifrovaný veřejný klíč (.pem). Tento klíč je možné vygenerovat prostřednictvím ESET Authentication Serveru.
- Šifrovaný veřejný klíč
- Veřejný klíč certifikátu (.crt)

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

Autentifikace k serveru nebyla úspěšná. Neplatný nebo neodpovídající podpis.	**Podpis serveru neodpovídá zadanému veřejnému klíči.**
Autentifikace k serveru nebyla úspěšná. Název sítě nesouhlasí.	Tento přepínač deaktivujte, pokud chcete ponechat pravidlo v seznamu pravidel, ale nepoužívat ho.
Autentifikace k serveru nebyla úspěšná. Neplatná nebo žádná odpověď od serveru.	Žádná odpověď, server neběží nebo není dostupný. Neplatnou odpověď můžete obdržet, pokud na dané adrese běží jiný HTTP server.
Zadaný veřejný klíč je neplatný.	Ověřte, že je veřejný klíč zadán správně.

Zóny

Zóna představuje skupinu síťových adres, které dohromady tvoří logickou skupinu IP adres. To je užitečné při opakovaném použití stejné sady adres ve více pravidlech. Každá adresa ve skupině má daná práva, která jsou platná pro celou skupinu. Příkladem takové skupiny je Důvěryhodná zóna. Důvěryhodná zóna představuje skupinu síťových adres, které nejsou firewallem nijak blokovány.

Klikněte na tlačítko **Přidat**, zadejte **název** a **popis** zóny, a nakonec zadejte vzdálenou adresu počítače (definovanou pomocí IPv4/IPv6 adresy, rozsahu, masky).

Ochrana proti síťovým útokům

Zapnout ochranu proti síťovým útokům (IDS)

Pomocí této možnosti můžete ovlivnit přístup ke službám běžícím ve vašem počítači z důvěryhodné zóny a dále můžete zapnout/vypnout detekci některých typů útoků, které by mohly poškodit váš počítač.

Ochrana proti zapojení do botnetu

Tato součást na základě charakteristických vzorků detekuje a blokuje komunikaci se škodlivými (C&C) servery, která známkou toho, že se infikovaný počítač stal členem botnetové sítě.

IDS výjimky

Intrusion Detection System (IDS) výjimky si můžete představit jako pravidla síťové ochrany. Pro definování výjimek klikněte na Změnit.

> V prostředích s vysoce výkonnými sítěmi (10GbE a více) doporučujeme prostudovat článek z naší Databáze znalostí, ve kterém zjistíte, jak optimalizovat výkon sítě při provozování ESET Server Security.

Ochrana proti útokům hrubou silou

Tato součást produktu ESET Server Security sleduje obsah síťové komunikace a dokáže blokovat pokusy o uhádnutí hesel.

Rozšířená nastavení

V této části můžete konfigurovat rozšířené možnosti filtrování síťové komunikace za účelem detekce různých typů útoků a zranitelností, které by mohly ohrozit váš počítač.

Detekce útoků

Protokol SMB – detekce a blokování mnoha zranitelností v SMB protokolu.
Protokol RPC – detekce a blokování CVE v systémové službě vzdálené volání procedur určené pro Distributed Computing Environment (DCE).
Protokol RDP – detekce a blokování CVE v RDP protokolu (viz výše).
Blokovat nebezpečnou adresu po detekci útoku – pokud je zjištěn útok z určité adresy, veškerá komunikace z ní bude blokována.
Zobrazit upozornění po detekci útoku – po detekci útoku se zobrazí upozornění v oznamovací oblasti Windows v pravém dolním rohu obrazovky.
Zobrazit upozornění při pokusu o zneužití bezpečnostních děr – upozorní, pokud bude zjištěn pokus o zneužití bezpečností díry případně bude zaznamenán pokus o její využití zranitelnosti k přístupu do systému.

Kontrola paketů

Povolit příchozí spojení k správcovským sdíleným položkám prostřednictvím SMB protokol – administrativní sdílení jsou standardní síťová sdílení, které sdílí celé diskové oddíly (C$, D$, ...) stejně jako systémové složky (ADMIN$). Zakázáním připojení k administrátorským sdíleným položkám snížíte bezpečnostní riziko. Například červ Conficker provádí slovníkový útok pro získání přístupu k administrátorským sdíleným položkám.
Zakázat staré (nepodporované) SMB dialekty – zakáže SMB relaci se starým dialektem SMB, který nepodporuje IDS. Nejnovější operační systémy Windows podporují staré dialekty SMB z důvodu zpětné kompatibility s předchozími verzemi, například Windows 95. Útočník může využít starší dialekt SMB záměrně, aby se vyhnul kontrole paketů. Zakažte staré SMB dialekty, pokud nepotřebujete sdílet soubory se staršími verzemi operačního systému Windows.
Zakázat SMB relace bez bezpečnostních rozšíření – bezpečnostní rozšíření mohou být využita během navazování SMB relace pro zajištění bezpečnostní autentifikace pomocí mechanismu LAN Manager Challenge/Response (LM). Schéma LM je považované za slabé a nedoporučuje se jej používat.
Povolit komunikaci se službou Security Account Manager – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SAMR].
Povolit komunikaci se službou Local Security Authority – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-LSAD] a [MS-LSAT].
Povolit komunikaci se službou Vzdálený registr – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-RRP] .
Povolit komunikaci se službou Správce řízení služeb – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SCMR].
Povolit komunikaci se službou Server – pro více informací o této službě přejděte do databáze znalostí společnosti Microsoft, [MS-SRVS].
Povolit komunikaci s ostatními službami – ostatní MSRPC služby.

IDS výjimky

Výjimky Intrusion Detection System (IDS) jsou v zásadě pravidla síťové ochrany. Výjimky jsou hodnoceny shora dolů. IDS výjimky můžete použít pro přizpůsobení chování a detekci IDS pomocí firewallu. První odpovídající výjimka je použita pro každý typ akce (Blokovat, Upozornit, Protokol) zvlášť. **Nahoru/Výše/Dolů/Níže** umožní přizpůsobit pořadí vyhodnocování pravidel (vyhodnocována jsou ze shora dolů). **Přidat** – vytvoří novou IDS výjimku. Aktuální seznam upravíte kliknutím na tlačítko **Změnit**, vymažete kliknutím na **Odstranit**.

Z rozbalovacího menu vyberte typ **upozornění**. Zadejte název **hrozby** a **směr**. Vyhledejte **Aplikace**, pro které chcete vytvořit výjimku. Zadejte seznam adres IP (IPv4 nebo IPv6) nebo podsítí. Pro více položek použijte čárku jako oddělovač.

Nakonfigurujte **akci** pro výjimku IDS výběrem jedné z možností z rozevírací nabídky (**Výchozí**, **Ano**, **Ne**). Udělejte to pro každý typ akce (**Blokovat**, **Upozornit**, **Protokol**).

Chcete-li, aby se oznámení zobrazilo v případě výstrahy výjimky IDS, stejně jako čas zaznamenané události, ponechte typ **Blokované** akce jako **Výchozí** a pro další dva typy akcí (**Upozornit** a **Protokol**) vyberte z rozbalovacího menu možnost **Ano**.

Zablokována podezřelá hrozba

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

- Hrozba – název hrozby.
- Zdroj – zdrojovou síťovou adresu,
- Cíl – cílovou síťovou adresu,
- Zastavit blokování – kliknutím vytvoříte IDS pravidlo pro danou podezřelou hrozbu takové, že bude komunikace povolena.
- Nadále blokovat – kliknutím zablokujete detekovanou hrozbu. Pro vytvoření IDS pravidla pro tuto hrozbu zaškrtněte možnost Znovu neupozorňovat.

Zobrazená informace se může lišit podle detekované hrozby. Pro více informací o hrozbách a souvisejících pojmech přejděte do kapitoly Typy vzdálených útoků nebo Typy detekcí.

Seznam dočasně blokovaných IP adres

Kliknutím si zobrazíte seznam IP adres, které byly označeny jako zdroj útoku a komunikace z těchto adres byla dočasně zablokována (na dobu jedné hodiny). Tyto **IP adresy** byly na základě označení uzamknuty.

Důvod blokování

V tomto sloupci je uveden typ útoku, kterému bylo zabráněno (například kontrolování portů).

Časový limit

V tomto sloupci je uvedena doba, na jak dlouho bude komunikace z dané adresy blokována.

Odstranit / Odstranit vše

Kliknutím odstraníte vybranou IP adresu ze seznamu a komunikace z této adresy již nebude blokována.

Přidat výjimku

Kliknutím přidáte vybrané IP adresy na seznam IDS výjimek.

Ochrana proti útokům hrubou silou

Ochrana proti útokům hrubou silou blokuje pokusy o uhádnutí hesel pro RDP a SMB služby. Útok hrubou silou je metoda, kdy se systematicky zkouší možné kombinace písmen, číslic a znaků za účelem prolomení hesla.

- **Zapnout ochranu proti útoku hrubou silou** – tato součást produktu ESET Server Security sleduje obsah síťové komunikace a dokáže blokovat pokusy o uhádnutí hesel.

- Pravidla – v editoru pravidel ochrany proti útokům hrubou silou si můžete zobrazit existující pravidla pro příchozí a odchozí síťová spojení, stejně tak si vytvářet vlastní a kdykoli je upravovat.

- Výjimky – seznam detekcí vyloučených z kontroly definovaný na základě IP adresy nebo cesty k aplikaci. Výjimky je možné vytvářet a upravovat prostřednictvím vaší ESET PROTECT webové konzole.

Pravidla ochrany proti útokům hrubou silou

V editoru pravidel ochrany proti útokům hrubou silou si můžete zobrazit existující pravidla pro příchozí a odchozí síťová spojení, stejně tak si vytvářet vlastní a kdykoli je upravovat. Předdefinovaná pravidla není možné upravit ani odstranit.

Pro vytvoření nového pravidla klikněte na tlačítko **Přidat**, případně vyberte existující a klikněte na **Změnit**.

Pomocí tohoto dialogového okna můžete spravovat pravidla ochrany proti útokům hrubou silou.

Název	Uživatelský nebo automaticky zadaný název pravidla.
Zapnuto	Tento přepínač deaktivujte, pokud chcete ponechat pravidlo v seznamu pravidel, ale nepoužívat ho.
Akce	Pravidlo specifikuje (právě jednu) akci – Povolit nebo Zablokovat – která se má provést, pokud jsou všechny podmínky splněny.
Protokol	Informace, pro který síťový protokol pravidlo platí.
Profil	Vlastní pravidla mohou být platná pouze pro některé profily.
Maximální počet pokusů	Maximální počet povolených pokusů o opakování útoku, dokud nebude IP adresa zablokována a přidána na seznam blokovaných.
Doba uchovávání adres na seznamu blokovaných	Definujte dobu, za jak dlouho bude adresa odstraněna ze seznamu blokovaných. Interval, ve kterém se pokusy počítají, je předdefinován na 30 minut.
Zdrojová IP adresa	Seznam IP adres, rozsahů nebo podsítí. Více záznamů oddělte čárkou.
Zdrojové zóny	Po kliknutí na tlačítko Přidat si můžete vybrat z předdefinovaných zón nebo si vytvořit vlastní na základě rozsahu IP adresu.

Výjimky ochrany proti útokům hrubou silou

Prostřednictvím výjimek na útoky hrubou silou můžete na základě specifického kritéria potlačit detekci útoku hrubou silou. Tyto výjimky je možné vytvořit v ESET PROTECT na základě detekce útoku hrubou silou. Seznam výjimek se zobrazí v případě, kdy administrátor vytvoří IDS výjimku v ESET PROTECT Web Console. Na seznamu výjimek se mohou nacházet pouze povolovací pravidla. Vyhodnocována jsou dříve, než IDS pravidla.

- **Detekce** – typ detekce.

- **Aplikace** – kliknutím na … vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace.

- **Vzdálená IP** – seznam IPv4, IPv6 adres / rozsahů adres / podsítí. Více záznamů oddělte čárkou.

Web a mail

V této části můžete konfigurovat součásti pro ochranu serveru připojeného k internetu – filtrování aplikačních protokolů, ochranu poštovních klientů, ochranu přístupu na web a anti-phishingovou ochranu.

Ochrana poštovních klientů

Zabezpečuje kontrolu poštovní komunikace, chrání před škodlivým kódem a zobrazí výzvu, při detekci infiltrace.

Ochrany přístupu na web

Monitoruje komunikace mezi internetovým prohlížečem a vzdálenými servery a aplikuje na ní definovaná HTTP/HTTPS pravidla. Můžete tak povolit přístup na konkrétní stránky, blokovat některé stránky nebo požadované adresy vyloučit z detekce.

Filtrování protokolů

Antivirová ochrana aplikačních protokolů je prováděna prostřednictvím skenovacího jádra ThreatSense. Tato kontrola pracuje automaticky nezávisle užívaném na prohlížeči nebo e-mailovém klientu. Dokáže rovněž analyzovat šifrovanou (SSL/TLS) komunikaci.

Anti-Phishingová ochrana

Dokáže blokovat přístup na webové stránky, na kterých se nachází phishingový obsah.

Filtrování protokolů

Ochrana před malware na úrovni aplikačních protokolů je prováděna prostřednictvím skenovacího jádra ThreatSense, které obsahuje všechny pokročilé metody detekce škodlivého softwaru. Filtrování protokolů pracuje zcela nezávisle na použitém internetovém prohlížeči nebo poštovním klientovi. Pokud je povoleno filtrování protokolů, ESET Server Security bude kontrolovat komunikaci používající protokol SSL/TLS. Nastavení zkontrolujete v programu v sekci **web a e-mail** > SSL/TLS.

Zapnout kontrolu obsahu aplikačních protokolů

Pokud tuto možnost vypnete, některé moduly ESET Server Security závislé na funkcích Ochrana přístupu na web, Ochrana poštovních klientů a Anti-Phishingová ochrana nebudou fungovat.

Vyloučené aplikace

Chcete-li z filtrování obsahu vyloučit komunikaci specifických aplikací využívajících síť, vyberte je v seznamu. HTTP/POP3 komunikace vybraných aplikací nebude kontrolována na hrozby. Umožňuje vyloučit konkrétní aplikaci z filtrování protokolů. Kliknutím na **Změnit** a **Přidat** vyberte spustitelný soubor ze seznamu aplikací, který chcete vyloučit z filtrování protokolů.

Tuto možnost doporučujeme použít pouze ve výjimečných případech, například pokud aplikace v důsledku kontroly komunikace nepracuje správně.

Vyloučené IP adresy

Umožňuje vyloučit konkrétní adresu z filtrování protokolů. IP adresy v tomto seznamu budou vyloučeny z filtrování obsahu protokolu. HTTP/POP3/IMAP komunikace vybraných adres nebude kontrolována na hrozby.

Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Kliknutím na tlačítko **Upravit** a **Přidat** přidejte adresu IP, rozsah adres nebo podsít, na které bude vyloučení použito. Pokud vyberete možnost **Zadat více hodnot**, můžete přidat více IP adres oddělených řádky, čárkami nebo středníky. Je-li aktivováno více výběrů, budou adresy zobrazeny v seznamu vyloučených adres IP.

Výjimky mohou být užitečné při řešení problémů s filtrování protokolů.

Weboví a poštovní klienti

Vzhledem k obrovskému množství škodlivého kódu kolujícího po internetu je bezpečné procházení internetu velmi důležitou součástí ochrany počítače. Zranitelnosti prohlížečů a podvodné odkazy dokáží zavést škodlivý kód do systému bez vědomí uživatele. Z tohoto důvodu je v ESET Server Security věnována pozornost bezpečnosti internetových prohlížečů. Každá aplikace, která přistupuje k síti, může být označena jako internetový prohlížeč. Aplikace, které již používají protokoly pro komunikaci nebo aplikace z vybraných cest, mohou být přidány do seznamu webových a e-mailových klientů.

SSL/TLS

ESET Server Security dokáže vyhledávat hrozby také v komunikaci využívající SSL / TLS protokol.

Kontrolu můžete přizpůsobit podle toho, zda je certifikát využíván danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL.

Zapnout filtrování protokolu SSL/TLS

Pokud je tato možnost aktivní, bude se provádět kontrola každé šifrované komunikace pomocí protokolu SSL/TLS. K dispozici jsou následující režimy filtrování protokolu SSL/TLS:

- **Automatický režim** – vyberte tuto možnost, pokud chcete kontrolovat veškerou komunikaci chráněnou protokolem SSL/TLS kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru využívající nedůvěryhodný certifikát označený jako důvěryhodný, komunikace bude povolena a přenášený obsah bude filtrován.

- **Interaktivní režim** – při přístupu k nové stránce chráněné protokolem SSL (s neznámým certifikátem) se zobrazí dialogové okno s výběr akce. Pomocí tohoto režimu můžete vytvořit seznam SSL certifikátů, které chcete vyloučit z kontroly.

- **Administrátorský režim** – filtrována bude veškerá SSL/TLS komunikace kromě definovaných výjimek.

Seznam SSL/TLS filtrovaných aplikací

Pomocí této možnosti můžete vytvořit seznam aplikací, u kterých bude komunikace SSL kontrolována. Pomocí této možnosti můžete přizpůsobit chování ESET Server Security pro konkrétní aplikace. V tomto seznamu naleznete aplikace, pro které jste v **Interaktivním režimu** nastavili **zapamatování vybrané akce**.

Seznam známých certifikátů

Pomocí této možnosti můžete přizpůsobit chování ESET Server Security, při detekci konkrétních SSL certifikátů. **Seznam** si zobrazíte kliknutím na Změnit.

Nekontrolovat komunikaci s důvěryhodnými doménami

Pokud je tato možnost aktivní, komunikace s URL využívajícími rozšířenou kontrolu certifikátu (například portály internetového bankovnictví) nebude kontrolována.

Blokovat šifrovanou komunikaci používající zastaralý protokol SSL v2

Po vybrání této možnosti bude komunikace využívající starší verzi protokolu SSL automaticky blokována.

Kořenový certifikát

Pro správné fungování kontroly SSL/TLS komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost Přidat kořenový certifikát do známých prohlížečů by měla být zapnuta.

Pomocí této možnosti zajistíte automatické přidání kořenového certifikátu společnosti ESET do známých prohlížečů (například prohlížeče Opera nebo Firefox). Do prohlížečů využívající systémové úložiště kořenových certifikátů se certifikát přidá automaticky (například prohlížeče Internet Explorer).

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

Platnost certifikátu

Pokud nelze ověřit platnost certifikátu pomocí systémového úložiště (TRCA)

V některých případech nelze certifikát webové stránky ověřit pomocí **systémového úložiště kořenových certifikátů** (TRCA). To znamená, že certifikát je někým samostatně podepsán (například administrátorem webového serveru nebo malou firmou) a považování tohoto certifikátu za důvěryhodný nemusí vždy představovat riziko. Většina velkých obchodních společností (například banky) používá certifikát podepsaný certifikační autoritou, která se nachází v TRCA.

Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** se vždy zablokuje komunikace s webovou stránkou využívající nedůvěryhodný certifikát.

Pokud je certifikát neplatný nebo poškozený

Znamená to, že certifikátu vypršela platnost nebo nebyl správně podepsán. V tomto případě doporučujeme **blokovat komunikaci využívající daný certifikát**.

Seznam známých certifikátů

Slouží k nastavení chování ESET Server Security pro konkrétní certifikáty SSL (Secure Sockets Layer) / Transport Layer Security (TLS) a uložení vybrané akce, pokud je v **Interaktivním režimu** filtrování protokolu nastaveno filtrování protokolůSSL / TLS. Vybraný certifikát můžete nakonfigurovat nebo **přidat** z URL nebo souboru.

Jakmile se nacházíte v okně **Přidat certifikát**, klikněte na možnost **URL** nebo **Soubor** a zadejte adresu URL certifikátu nebo vyhledejte soubor certifikátu. Následující data budou automaticky vyplněna pomocí údajů z certifikátu:

- **Název** – název certifikátu.
- **Vydavatel certifikátu** – jméno vydavatele certifikátu.
- **Předmět certifikátu** – identifikace entity asociované s veřejným klíčem uloženým v poli předmět veřejného klíče.

Přístup k nastavení

- **Automaticky** - povolení důvěryhodných certifikátů a vyžádání nedůvěryhodných certifikátů.
- **Povolit nebo Blokovat** – pro povolení nebo zablokování komunikace využívající daný certifikát bez ohledu na jeho důvěryhodnost.
- **Dotázat se** – zobrazení výzvy při komunikaci s určitým certifikátem.

Akce při kontrole

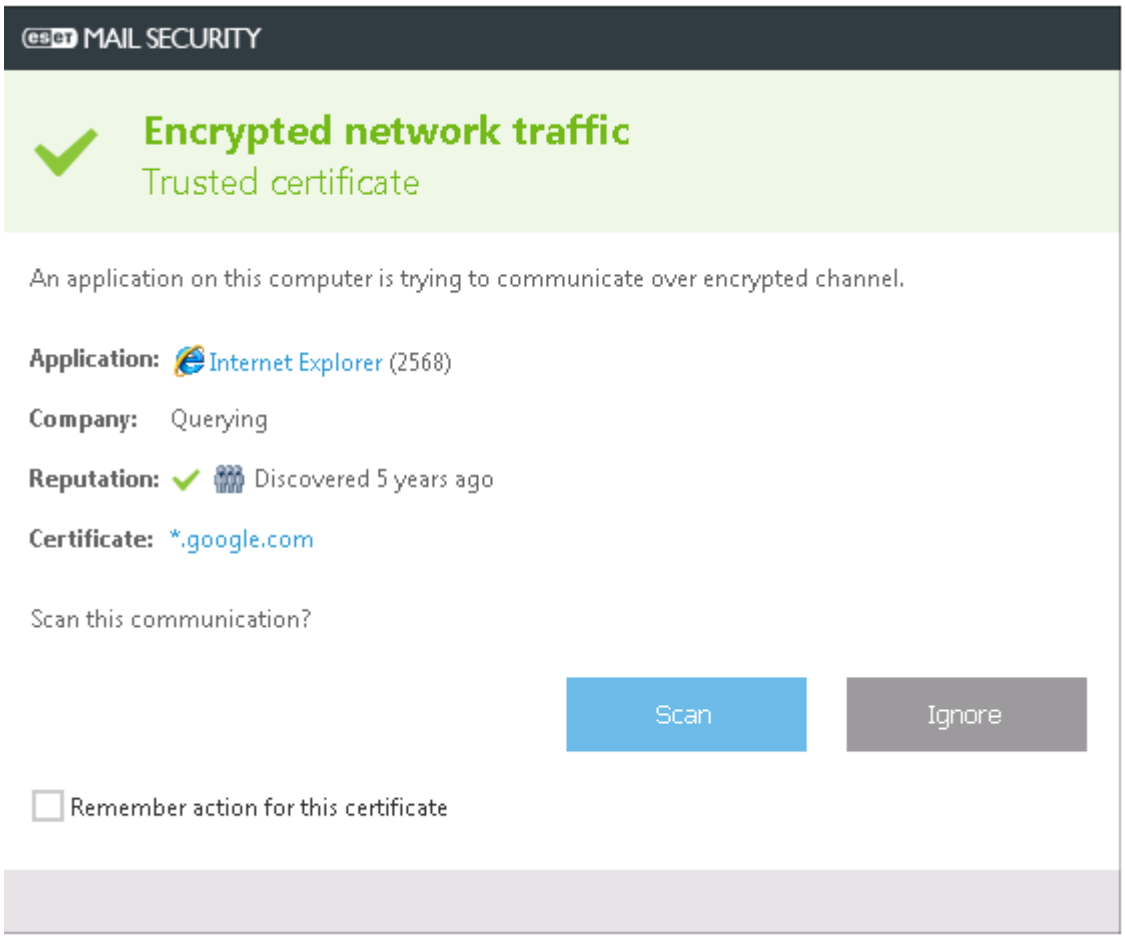
- **Automaticky** – komunikace bude kontrolována v automatickém režimu a výzva s výběrem akce se zobrazí v interaktivním režimu.
- **Kontrolovat nebo Ignorovat** – rozhodněte se, zda chcete kontrolovat nebo ignorovat komunikaci zabezpečeným certifikátem.
- **Dotázat se** – zobrazení výzvy při komunikaci s určitým certifikátem.

Šifrovaná SSL/TLS komunikace

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

Webová stránka používá neověřený nebo neplatný certifikát a ESET Server Security je nakonfigurován tak, aby se dotázal uživatele (standardně je tato možnost aktivní pro neověřené certifikáty, nikoli neplatné), zda chcete komunikaci **Povolit** nebo **Zakázat**.

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



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

Ochrana poštovních klientů

Integrace ESET Server Security do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdrženým prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET Server Security podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET Server Security do poštovního klienta (panel nástrojů není dostupný pro nejnovější verze Windows Live Mail), což přispívá k efektivnější kontrole e-mailových zpráv.

Integrace do poštovních klientů

Modul ochrany poštovních klientů podporuje Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Ochrana je zajišťována pomocí zásuvného doplňku v těchto programech. Hlavní výhodou doplňku je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Pokud není nastavena integrace, e-mailová komunikace je stále chráněna modulem ochrany poštovních klientů (POP3, IMAP).

Úplný seznam podporovaných poštovních klientů a jejich verzí naleznete v Databázi znalostí.

Nekontrolovat při změně obsahu složky s doručenou poštou

Tuto možnost doporučujeme použít v případě, že pociťujete propad výkonu při práci s poštovním klientem (platné pouze pro Microsoft Outlook). Uvedená situace může nastat například, že přijímáte zprávy z úložiště zpráv prostřednictvím Kerio Outlook Connector.

Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta

Pomocí této možnosti můžete částečně vypnout poštovní ochranu bez zrušení integrace v poštovním klientovi. Doplněk můžete deaktivovat kompletně, případně jen pro určité zprávy:

- **Příchozí zprávy** – zapne/vypne kontrolu přijatých zpráv.
- **Odchozí zprávy** – zapne/vypne kontrolu odesílaných zpráv.
- **Čtené zprávy** – zapne/vypne kontrolu prohlížených zpráv.

S infikovanými zprávami provést následující akci

- **Žádná akce** – program upozorní na zprávy s infikovanými přílohami, avšak neprovede žádnou akci.
- **Vymazat zprávu** – program upozorní na infikované přílohy a odstraní celou zprávu.
- **Přesunout zprávu do složky s odstraněnými zprávami** – program bude přesouvat infikované zprávy do složky s vymazanými zprávami.
- **Přesunout zprávu do složky** – program bude přesouvat infikované zprávy do vybrané složky.
- **Složka** – definujte vlastní složku, do které chcete přesouvat infikované zprávy.

Opakovat kontrolu po aktualizaci

Pomocí této možnosti zapnete/vypnete opětovnou kontrolu zpráv po provedení aktualizace detekčního jádra.

Zohlednit výsledky kontroly provedené dalšími moduly

Po vybrání této možnosti bude modul poštovní ochrany přijímat také výsledky kontroly provedené jinými moduly (kontrolou protokolu POP3, IMAP).

Poštovní protokoly

Zapnout ochranu pošty prostřednictvím modulu filtrování protokolů

Protokol POP3 a IMAP je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím aplikace poštovního klienta. ESET Server Security zajišťuje ochranu těchto protokolů zcela nezávisle na používaném klientovi.

ESET Server Security podporuje kontrolu protokolů IMAPS a POP3S, které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET Server Security kontroluje komunikaci využívající protokol SSL (Secure Socket Layer) a TLS (Transport Layer Security). Komunikace bude kontrolována pouze na definovaných **Portech používaných protokolem IMAPS/POP3S**, bez ohledu na verzi operačního systému.

Možnosti IMAPS/POP3S skeneru

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace je nutné zapnout kontrolu protokolu SSL/TLS.

Jednotlivé protokoly jsou reprezentovány číslem portu. Níže uvádíme porty, které ve výchozím nastavení

kontroluje:

Název portu	Číslo portu	Popis
POP3	110	Výchozí port pro nešifrovaný POP3.
IMAP	143	Výchozí port pro nešifrovaný IMAP.
Secure IMAP (IMAP4-SSL)	585	Povolte filtrování protokolů SSL/TLS. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.
IMAP4 over SSL (IMAPS)	993	Povolte filtrování protokolů SSL/TLS. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.
Zabezpečený POP3 (SSL-POP)	995	Povolte filtrování protokolů SSL/TLS. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujte čárkou.

Upozornění a oznámení

Poštovní ochrana zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Pomocí pluginu pro Microsoft Outlook a další e-mailové klienty zajišťuje ESET Server Security kontrolu veškeré komunikace z e-mailového klienta (POP3, MAPI, IMAP, HTTP).

Při kontrole přijímaných zpráv jsou použity všechny pokročilé metody obsažené ve skenovacím jádře ThreatSense. Tím je zajištěna detekce nebezpečných programů ještě před aktualizací detekčního jádra. Kontrola POP3 a IMAP protokolu je nezávislá na použitém poštovním klientovi.

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do příchozích a čtených zpráv**, **Přidávat do předmětu příchozích a čtených infikovaných zpráv** nebo pouze **Přidávat do odchozích zpráv**.

Samozřejmě, na tyto podpisy se nelze zcela spoléhat, protože nemusí být doplněny do problematických HTML zpráv a také mohou být zfalšovány škodlivým kódem. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy.

Dostupné možnosti:

- **Nikdy** – program nebude přidávat podpisy do žádných kontrolovaných zpráv.
- **Přidávat pouze do infikovaných zpráv** – program bude přidávat podpisy pouze do infikovaných zpráv.
- **Přidávat do všech kontrolovat zpráv** program bude přidávat podpisy do všech kontrolovaných zpráv.

Přidávat do předmětu odchozích infikovaných zpráv

Vypnutím této funkce se nebude do předmětu infikované zprávy přidávat informace o tom, že obsahuje infiltraci. Tato funkce se dá využít pro snadné filtrování infikovaných zpráv podle předmětu, pokud to poštovní klient umožňuje. Dále zvyšuje tato informace důvěryhodnost pro příjemce zprávy. Pokud zpráva obsahuje hrozbu, poskytne tato možnost hodnotné informace o úrovni hrozby.

Šablona přidávaná do předmětu infikovaných zpráv

Pokud chcete změnit formát předpony předmětu infikovaného e-mailu, upravte tuto šablonu. Tato funkce přidá k původnímu předmětu zprávy `Ahoj` předponu [virus] a formát výsledného předmět bude: `[virus] Ahoj`. Proměnná `%VIRUSNAME%` označuje zjištěnou hrozbu.

Nástrojová lišta Microsoft Outlook

Ochrana Microsoft Outlook pracuje jako zásuvný modul (plug-in). Po instalaci ESET Server Security se v Microsoft Outlook zobrazí nový panel nástrojů, který obsahuje možnosti pro ochranu před škodlivým kódem:

ESET Server Security

Kliknutím na ikonu otevřete hlavní okno ESET Server Security.

Opakovaná kontrola zpráv

Umožňuje ručně spustit kontrolu e-mailů. Zde můžete nastavit zprávy, které budou zkontrolovány, a můžete aktivovat opakovanou kontrolu přijatého e-mailu. Více informací naleznete v kapitole ochrana poštovních klientů.

Možnosti kontroly

Otevře okno s nastavením ochrany poštovních klientů.

Panel nástrojů v Outlook Express a Windows Mail

Ochrana Outlook Express a Windows Mail pracuje jako zásuvný modul. Po instalaci ESET Server Security se v Outlook Express a Windows Mail zobrazí nový panel nástrojů, který obsahuje možnosti pro ochranu před škodlivým kódem:

ESET Server Security

Kliknutím na ikonu otevřete hlavní okno ESET Server Security.

Opakovaná kontrola zpráv

Umožňuje ručně spustit kontrolu e-mailů. Zde můžete nastavit zprávy, které budou zkontrolovány, a můžete aktivovat opakovanou kontrolu přijatého e-mailu. Více informací naleznete v kapitole ochrana poštovních klientů.

Možnosti kontroly

Otevře okno s nastavením ochrany poštovních klientů.

Přizpůsobit vzhled

Pomocí této možnosti změníte vzhled panelu nástrojů v poštovním klientu. Zrušením této možnosti se vzhled panelu nástrojů přizpůsobí podle nastavení poštovního klienta.

- **Zobrazit text** – u ikon se zobrazí text s popisem.
- **Text vpravo** – text s popisem se zobrazí vpravo vedle ikony.
- **Velké ikony** – na panelu nástrojů se zobrazí velké ikony.

Potvrzovací dialog

Dialog s možností potvrzení nebo zamítnutí dané akce slouží pro ověření, že chcete akci opravdu provést. Předejdete tím také akcím, jejichž provedení jste nastavili nedopatřením. Zároveň můžete tato upozornění vyžadující potvrzení zcela vypnout.

Opakovaná kontrola zpráv

Prostřednictvím panelu nástrojů ESET Server Security integrovaném v poštovním klientovi můžete kliknutím na Kontrola zpráv provést kontrolu stávajících zpráv. **Kontrola zpráv** provést kontrolu stávajících zpráv. Dostupné jsou dvě možnosti kontroly:

- **Všechny zprávy v aktuální složce** – zkontrolují se všechny zprávy ve složce, která je aktuálně zobrazena.
- **Pouze označené zprávy** – zkontrolují se pouze zprávy, které jste vybrali ručně.
- Možnost **Kontrolovat zprávy, které již byly překontrolovány** zajistí nové zkontrolování zpráv, které již byly v minulosti zkontrolovány.

Ochrana přístupu na web

Ochrana přístupu na web monitoruje komunikaci mezi webovými prohlížeči a vzdálenými servery, díky čemuž vás chrání před online hrozbami. Dále uplatňuje pravidla na HTTP (Hypertext Transfer Protocol) a HTTPS (šifrovanou) komunikaci.

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

Obecné

V rámci zajištění bezpečnosti doporučujeme **Ochranu přístupu na web** ponechat zapnutou. Podrobné možnosti konfigurace ESET Server Security naleznete v **Nastavení** na záložce **Web a mail** > **Ochrana přístupu na web**.
Zapnout rozšířenou kontrolu skriptů v prohlížeči
Standardně jsou kontrolovány všechny javascriptové programy spouštěné internetovým prohlížečem.

Webové protokoly

Umožňují konfigurovat monitorování standardních protokolů používaných internetovými prohlížeči. Standardně je ESET Server Security nakonfigurován tak, aby monitoroval HTTP protokol používaný nejrozšířenějšími internetovými prohlížeči.
ESET Server Security rovněž podporuje kontrolu HTTPS protokolů. Při HTTPS komunikaci se používá šifrovaný kanál pro výměnu informací mezi klientem a serverem ESET Server Security kontroluje komunikaci šifrovanou metodami SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program kontroluje pouze přenos dat na portech definovaných v **Porty používané protokolem HTTPS** bez ohledu na verzi operačního systému.
Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) na záložku **Web a email** > SSL/TLS.

Parametry skenovacího jádra ThreatSense

Konfigurujte nastavení, jako jsou typy skenování (e-maily, archivy, vyloučení, limity atd.) a metody detekce Ochrany přístupu na web.

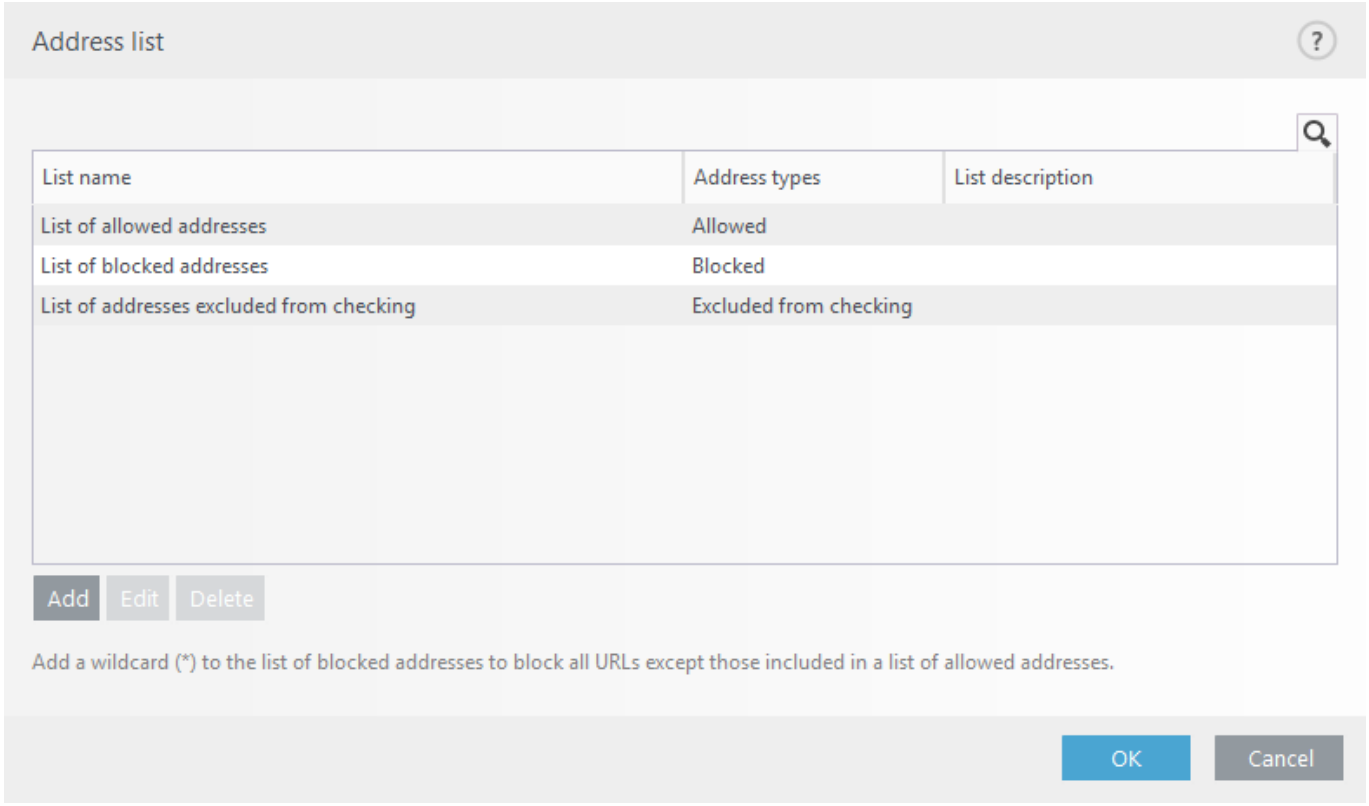
Správa URL adres

Prostřednictvím správy URL adres můžete definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly. Webové stránky zařazené na Seznamu blokovaných adres nebudou dostupné, na rozdíl od adres na Seznamu povolených adres. Webové stránky zařazené na Seznamu adres vyloučených z kontroly nebudou kontrolovány na přítomnost škodlivého kódu. Filtrování protokolu SSL/TLS musí být aktivní, pokud chcete filtrovat HTTPS adresy. V opačném případě by byl zakázán pouze přístup na nešifrovanou verzi webové stránky.

Na jeden seznam si můžete přidat adresy z veřejných blacklistů, do druhého stránky, které chcete blokovat. V tomto případě se vám budou externí seznamy adres pohodlněji aktualizovat.

Klikněte na **Změnit** a **Přidat** pro vytvoření nového seznamu adres, který bude vedle těch předdefinovaných. Toho můžete využít při tvorbě logických skupin adres. Standardně jsou k dispozici tři seznamy:

- **Seznam adres vyloučených z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na škodlivý kód.
- **Seznam povolených adres** – pokud do seznam blokovaných adres vložíte hvězdičku (*), bude uživateli povolen přístup pouze na adresy uvedené v tomto seznamu. Přístup na tyto adresy bude povolen i v případě, že se zároveň nachází na seznamu blokovaných adres.
- **Seznam blokovaných adres** – na adresy v tomto seznamu nebude povolen přístup, pokud se zároveň nenachází na seznamu povolených adres.



Pro přidání záznamu na seznam adres klikněte na tlačítko **Přidat**. Při použití oddělovače můžete přidat hromadně

více záznamů. Aktuální seznam upravíte kliknutím na tlačítko **Změnit**, vymažete kliknutím na **Odstranit**. Odstranit je možné **výhradně vámi vytvořené seznamy**, vestavěné seznamy není možné odstranit.

V seznamech můžete používat speciální znaky * (hvězdičku) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám, proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Rovněž je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu.

Pokud chcete zablokovat všechny HTTP adresy kromě těch definovaných na Seznamu povolených adres, zadejte do seznamu blokovaných adres * (hvězdičku).

Vytvoření nového seznamu

V této sekci můžete definovat seznamy adres/masek, které budou blokovány, povoleny, nebo vyloučeny z kontroly. Při vytváření vlastního seznamu definujte:

- **Typ seznamu** – z rozbalovacího menu vyberte, zda se jedná o seznam blokovaných, povolených nebo vyloučených adres.
- **Název seznamu** – zadejte název nového seznamu. Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.
- **Popis seznamu** – zadejte krátký popis pro nově vytvářený seznam (nepovinné). Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.
- **Seznam je aktivní** – pomocí této možnosti aktivujete daný seznam. Kdykoli jej můžete deaktivovat.
- **Upozornit při přístupu na adresy ze seznamu** – tuto možnost zapněte, pokud byla při přístupu na HTTP/HTTPS stránku použita adresa nacházející se na konkrétním seznamu. V takovém případě se zobrazí informace o tom, že přistupujete na webovou stránku zařazenou na seznamu například blokovaných nebo povolených stránek. V oznámení bude uveden název seznamu, na kterém se daná webová stránka nachází.
- **Zaznamenávat od úrovně** – z rozbalovacího menu vyberte úroveň protokolování (Žádné, Diagnostické, Informativní, Varování). Záznamy s úrovní Varování mohou být přenášeny do ESET PROTECT.

ESET Server Security dokáže uživateli zablokovat přístup na konkrétní webové stránky a zabránit internetovému prohlížeči v zobrazení jejich obsahu. Dále umožňuje specifikovat adresy, které mají být vyloučeny z kontroly. Pokud neznáte celý název vzdáleného serveru, nebo chcete specifikovat celou skupinu vzdálených serverů, můžete použít tzv. masky.

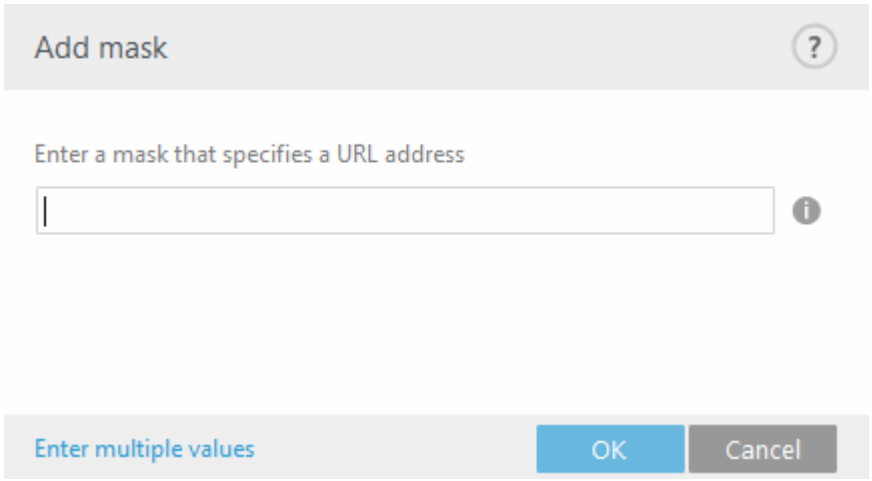
V tomto případě jsou povoleny zástupné znaky – otazník (?) a hvězdička (*) přičemž:

- ? nahrazuje libovolný symbol,
- * nahrazuje libovolný řetězec.

Například **.c?m* bude platit pro všechny adresy, jejichž poslední část adresy začíná znakem c, končí znakem m a uprostřed se nachází libovolný znak (*.com*, *.cam* apod.).

Zástupný znak * můžete použít výhradně na začátku názvu domény. Mějte na paměti, že zástupný znak hvězdičky * v tomto případě nenahrazuje lomítko. Je to z důvodu, aby se zabránilo obcházení, např., aby se maska

*.domena.cz nevyhodnocovala jako *https://jakakolidomena.cz/jakakolikcesta#.domena.cz* (jako přípona může být připojena k jakékoli URL adrese bez toto, aby došlo k zablokování stahování). Dále, hvězdička (*) v tomto případě představuje prázdný znak. To proto, aby bylo možné spárovat celou doménu, včetně všech subdomén, pomocí jediné masky. Například maska *domena.cz bude odpovídat také adrese *https://domena.cz* . Ovšem použití masky *domena.cz není správné, protože bude použita také pro vyhodnocení adresy https://jinadomena.cz.

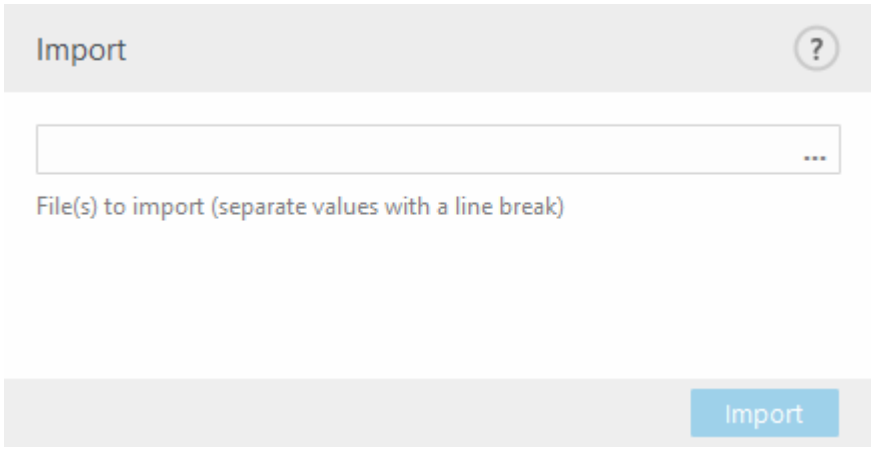


Zadat více hodnot

Pro zadání více adres vyberte tuto možnost a definujte oddělovač hodnot: nový řádek, čárka nebo středník. Zadané hodnoty se následně hromadně přidají do seznamu.

Importovat

V případě potřeby můžete seznam adres naimportovat z `*.txt` souboru v UTF-8 kódování, kde budou jednotlivé záznamy odděleny novým řádkem.

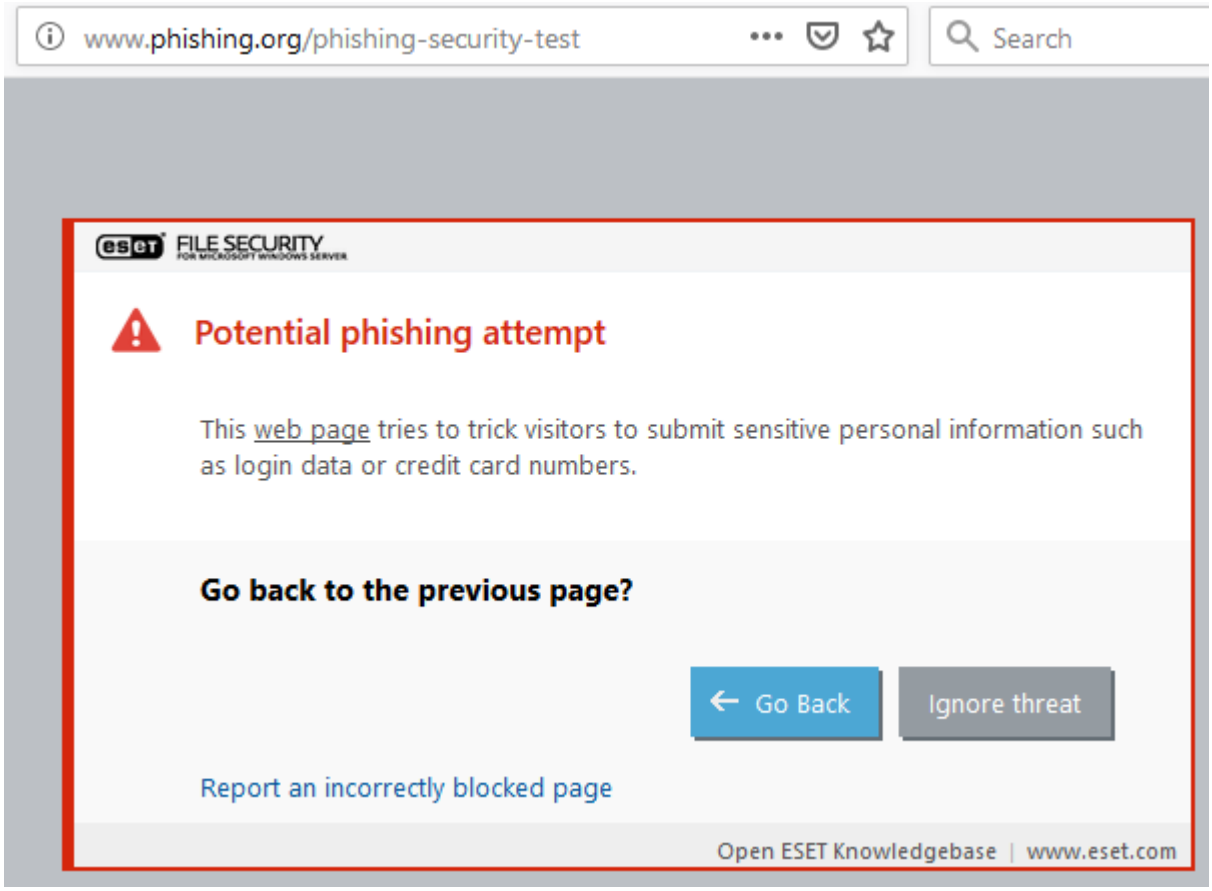


Anti-Phishingová ochrana přístupu na web

Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Phishing je často využíván pro získání citlivých informací, jako jsou číslo bankovních účtů, PIN kódy a další.

ESET Server Security obsahuje anti-phishingovou ochranu, která blokuje internetové stránky s tímto obsahem. Důrazně doporučujeme aktivovat Anti-Phishingovou ochranu programu ESET Server Security. Podrobnější informace o fungování Anti-Phishingové ochrany ESET Server Security naleznete v ESET Databázi znalostí.

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



> V případě, že budete pokračovat na potenciální phishingovou stránku, na několik hodin se pro ni vytvoří výjimka. Následně bude přístup opět blokován. Pokud chcete stránky povolit natrvalo, použijte nástroj Správce URL adres.

Nahlášení phishingové stránky

Pokud narazíte na podezřelý web, který se zdá být phishing nebo jinak škodlivý, můžete jej nahlásit společnosti ESET pro analýzu. Předtím, než odešlete stránku do společnosti ESET, se ujistěte, že splňuje alespoň jedno z níže uvedených kritérií:

- stránka není detekována jako škodlivá,
- soubor je detekován nesprávně jako hrozba. V tomto případě použijte tento odkaz.

Případně můžete odeslat odkaz e-mailem. Ten, prosím, včetně vložené adresy stránky odešlete e-mailem na adresu samples@eset.com. Nezapomeňte vyplnit předmět e-mailu a přiložte maximální možné množství informací o dané stránce (jak jste se k ní dostali, od koho jste odkaz na ní obdrželi apod.)

Správa zařízení

ESET Server Security zahrnuje automatickou správu zařízení, jako jsou CD/DVD/USB Tento modul umožňuje kontrolovat, blokovat nebo upravovat rozšířené filtry nebo oprávnění a definovat schopnost uživatele přistupovat k danému zařízení a pracovat s ním. To může být užitečné v případě, kdy například administrátor potřebuje zajistit, aby uživatelé nevkládali výměnná média s nežádoucím obsahem do počítače.

Pokud povolíte ovládání zařízení pomocí přepínače **Integrovat do systému**, funkce Ovládání zařízení ESET Server Security se aktivuje. Aby se tato změna projevila, je nutné restartovat systém.

Ovládání zařízení se aktivuje a můžete upravit jeho nastavení. Pokud do počítače vložíte externí zařízení, na které se aplikuje blokovací pravidlo, zobrazí se v pravém dolním rohu obrazovky informační okno a přístup k zařízení bude zakázán.

Pravidla

Pravidla definují akce, které má modul provést, pokud po připojení zařízení k počítači vyhovuje tomuto pravidlu.

Skupiny

Kliknutím na Změnit můžete spravovat skupinu zařízení. Vytvořit si můžete novou nebo do existující přidat další záznamy (zařízení). Vytvořte novou skupinu zařízení nebo vyberte existující skupinu pro přidání nebo odebrání zařízení ze seznamu.

Položky protokolu zařízení můžete zobrazit v souborech protokolu.

Editor pravidel

Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování.

Kliknutím na tlačítko **Přidat** vytvoříte nové pravidlo, případně upravte některé z již existujících. Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla. Zaškrtnutím možnosti **Pravidlo je aktivní** dané pravidlo povolíte. Tuto možnost využijete, pokud pravidlo nechcete natrvalo smazat.

Aplikovat v době

Prostřednictvím časových slotů může být pravidlo aktivní pouze v definované době. Nejprve sloty vytvořte, poté je můžete vybrat v tomto rozbalovacím menu.

Typ zařízení

Z rozbalovacího menu vyberte typ zařízení (diskové úložiště/přenosné zařízení/Bluetooth/FireWire/…). Typy zařízení se přebírají ze systému a můžete si je prohlédnout v systémovém Správci zařízení, který poskytuje informace o zařízeních připojených k počítači. Úložná média zahrnuje externí disky nebo čtečky paměťových karet připojených pomocí USB nebo FireWire. Čtečky čipových karet zahrnují čtečky karet s integrovanými elektronickými obvody jako jsou SIM karty nebo přístupové karty. Příkladem zobrazovacích zařízení jsou fotoaparáty a kamery, které neposkytují informace o uživateli, pouze vyvolávají akce. To znamená, že tato zařízení mohou být blokována pouze globálně.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

- **Čtení/Zápis** – plný přístup k zařízení.

- **Blokovat** – přístup k zařízení bude zakázán.
- **Pouze pro čtení** – uživatel může pouze číst soubory na daném zařízení.
- **Upozornit** – při každém připojení zařízení se uživateli zobrazí upozornění, že byl přístup na zařízení povolen/zakázán a zároveň se informace zapíše do protokolu. Informace o zařízení se neukládá. Při příštím připojení stejného zařízení se znovu uživateli zobrazí upozornění.

> Mějte na paměti, že uvedená práva (akce) nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze dvě akce (například akce **Pouze pro čtení** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen nebo zakázán).

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se nerozlišuje velikost písmen.

- **Výrobce** – filtruje podle názvu výrobce nebo ID.
- **Model** – filtruje podle názvu zařízení.
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.

> Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. V parametrech filtrování se rozlišuje velikost písmen a nejsou podporovány zástupné znaky ((*, ?)). Data musí být zadána tak, jak je poskytuje výrobce.

Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a podívejte se do protokolu správy zařízení.

V rozbalovacím menu **Zaznamenávat od úrovně** si vyberte jednu s následujících možností:

- **Vše** – zaznamenají se všechny události.
- **Diagnostické** – do protokolu se zapíší diagnostické informace pro řešení problémů.
- **Informační** – zaznamenány budou informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíší kritické chyby a varovná hlášení.
- **Žádné** – nebudou zaznamenávány žádné události nevytvoří se žádné protokoly.

Pravidla můžete přiřadit konkrétnímu uživateli nebo celé skupině uživatelů pomocí dialogového okna Seznam uživatelů. Pro úpravu **Seznamu uživatelů** klikněte na **Změnit**.

- **Přidat** – kliknutím otevřete systémové okno Vybrat typ objektu: Uživatelé nebo Skupiny, ve kterém vyberte požadované uživatele.
- **Odstranit** – odebere vybraného uživatele ze seznamu.

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

K dispozici jsou následující ovládací prvky:

Změnit

Kliknutím můžete změnit název pravidla a parametry (informace o zařízení zahrnující výrobce, model a sériové číslo).

Kopírovat

Kliknutím vytvoříte nové pravidlo z již existujícího pravidla.

Odstranit

Kliknutím smažete konkrétní pravidlo. Pravidlo můžete případně pouze deaktivovat pomocí zaškrtávacího pole ve sloupci Zapnuto. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Načíst

Po kliknutí se zobrazí informace o všech aktuálně připojených zařízeních jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné). Po vybrání zařízení ze seznamu klikněte na tlačítko **OK** a do editoru pravidel se automaticky předvyplní informace o zařízení, které si následně můžete upravit.

Pravidla jsou seřazena dle priority, tedy pravidlo s nejvyšší prioritou je umístěno nahoře. Po vybrání více pravidel můžete provádět hromadné akce, například pravidla odstranit nebo změnit jejich pořadí pomocí tlačítek **Nahoru/Výše/Dolů/Níže** (se symbolem šipek).

Skupina zařízení

Dialogové okno skupin zařízení je rozděleno na dvě části. V levé části se nachází seznam existujících skupin a v pravé části se zobrazují zařízení, která patří do dané skupiny. Pro zobrazení seznamu zařízení nejprve vyberte požadovanou skupinu.

Na každou vytvořenou skupinu zařízení můžete aplikovat rozdílná pravidla. Vytvořit si můžete jednu skupinu zařízení s oprávněním **Čtení/Zápis** nebo **Pouze pro čtení**. Tím zablokujete veškerá nerozpoznaná zařízení a nebude je možné připojit k počítači.

⚠ Připojení externích zařízení k počítači představuje bezpečnostní riziko.

K dispozici jsou následující ovládací prvky:

Přidat

Kliknutím vytvoříte novou skupinu nebo přidáte zařízení do již existující skupiny, kdy můžete specifikovat výrobce, model a sériové číslo.

Změnit

Kliknutím můžete změnit název skupiny, případně jejích obsah (informace o zařízení zahrnující výrobce, model a sériové číslo).

Odstranit

Kliknutím vymažete vybranou skupinu nebo konkrétní zařízení. Pravidlo můžete případně pouze deaktivovat pomocí zaškrtávacího pole ve sloupci Zapnuto. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Importovat

Kliknutím importujete seznam zařízení ze souboru.

Načíst

Po kliknutí se zobrazí informace o všech aktuálně připojených zařízeních jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné). Po vybrání zařízení ze seznamu klikněte na tlačítko **OK** a do editoru pravidel se automaticky předvyplní informace o zařízení, které si následně můžete upravit.

Po dokončení konfigurace klikněte na tlačítko **OK**. Kliknutím na tlačítko **Zrušit** opustíte dialogové okno **Skupiny zařízení** bez uložení změn.

> Mějte na paměti, že uvedená práva (akce) nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze dvě akce (například akce Pouze pro čtení není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen nebo blokován).

Nástroje

V rozšířeném nastavení naleznete v sekci Nástroje následující možnosti:

- Časové sloty
- Aktualizace operačního systému Windows
- ESET CMD
- ESET RMM
- Licence
- Poskytovatel WMI
- Cíle kontroly: ESET konzole pro vzdálenou správu
- Protokoly
- Proxy server
- Oznámení
- Prezentační režim
- Diagnostika
- Cluster

Časové sloty

Časové sloty můžete používat při tvorbě pravidel pro správu zařízení a pomocí nich definovat rozsah platnosti pravidel. Vytvořte si časový slot a následně při tvorbě pravidel si požadovaný časový slot vyberte v rozbalovacím menu **Aplikovat v době**. Díky této logice si můžete vytvořit časové sloty pro často používané rozsahy času (pracovní doba, víkend aj.) a následně je více násobně používat při tvorbě pravidel – aniž byste museli čas pokaždé znovu definovat. Časové sloty můžete používat v pravidlech, které podporují správu času.

Aktualizace operačního systému Windows

Aktualizace operačního systému Windows představují důležitou součást pro zajištění ochrany uživatelů před zneužitím bezpečnostních děr a tím pádem možným infikováním systému. Z tohoto důvodu je vhodné instalovat aktualizace Microsoft Windows co nejdříve po jejich vydání. V ESET Server Security můžete nastavit, od jaké úrovně chcete být informováni na chybějících systémové aktualizace. K dispozici jsou následující možnosti:

- **Žádné aktualizace** – nebudou nabízeny žádné aktualizace,
- **Volitelné aktualizace** – budou nabízeny aktualizace s nízkou prioritou a vyšší,
- **Doporučené aktualizace** – budou nabízeny běžné aktualizace a s vyšší prioritou,
- **Důležité aktualizace** – budou nabízeny důležité aktualizace a všechny s vyšší prioritou,
- **Kritické aktualizace** – budou nabízeny pouze kritické aktualizace.

Kliknutím na tlačítko **OK** uložíte změny. Zobrazení okna dostupných aktualizací proběhne po ověření stavu na aktualizačním serveru. Samotné zobrazení dostupných aktualizací proto nemusí nutně proběhnout ihned po uložení změn.

Skener příkazového řádku

Volitelnou kontrolu můžete kromě eShell spustit prostřednictvím příkazového řádku pomocí nástroje `ecls.exe`, který se nachází v instalační složce produktu ESET Server Security.

Níže uvádíme seznam parametrů a přepínačů:

Možnosti:

`/base-dir=FOLDER`	načíst moduly ze SLOŽKY
`/quar-dir=FOLDER`	SLOŽKA s karanténou
`/exclude=MASK`	vyloučí soubory odpovídající MASCE z kontroly
`/subdir`	kontrolovat podsložky (standardně)
`/no-subdir`	nekontrolovat podsložky
`/max-subdir-level=LEVEL`	podsložky kontrolovat pouze do definované ÚROVNĚ vnoření
`/symlink`	následovat symbolické odkazy (standardně)
`/no-symlink`	přeskočit symbolické odkazy

/ads	kontrolovat ADS (standardně)
/no-ads	nekontrolovat ADS
/log-file=FILE	zapisovat výstup do SOUBORU
/log-rewrite	přepisovat protokol (standardně se záznamy přidají na konec souboru)
/log-console	zapisovat výstup do konzole (standardně)
/no-log-console	nezapisovat výstup do konzole
/log-all	zaznamenat do protokolu také čisté soubory
/no-log-all	nezaznamenávat do protokolu čisté soubory (standardně)
/aind	zobrazit průběh aktivity
/auto	automaticky zkontrolovat a vyléčit všechny lokální disky

Možnosti skeneru:

/files	kontrolovat soubory (standardně)
/no-files	nekontrolovat soubory
/memory	kontrolovat paměť
/boots	kontrolovat boot sektory
/no-boots	nekontrolovat boot sektory (standardně)
/arch	kontrolovat archivy (standardně)
/no-arch	nekontrolovat archivy
/max-obj-size=SIZE	kontrolovat pouze soubory menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/max-arch-level=LEVEL	archivy kontrolovat do definované ÚROVNĚ vnoření
/scan-timeout=LIMIT	archivy kontrolovat nejdéle po definovaný LIMIT v sekundách
/max-arch-size=SIZE	kontrolovat pouze soubory v archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/max-sfx-size=SIZE	kontrolovat pouze soubory v samorozbalovacích archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/mail	kontrolovat poštovní soubory (standardně)
/no-mail	nekontrolovat poštovní soubory
/mailbox	kontrolovat poštovní schránky (standardně)
/no-mailbox	nekontrolovat poštovní schránky
/sfx	kontrolovat samorozbalovací archivy (standardně)
/no-sfx	nekontrolovat samorozbalovací archivy
/rtp	kontrolovat runtime packery (standardně)
/no-rtp	nekontrolovat runtime packery
/unsafe	detekovat potenciálně zneužitelné aplikace
/no-unsafe	nedetekovat potenciálně zneužitelné aplikace (standardně)
/unwanted	detekovat potenciálně nechtěné aplikace
/no-unwanted	nedetekovat potenciálně nechtěné aplikace (standardně)
/suspicious	detekovat podezřelé aplikace (standardně)
/no-suspicious	nedetekovat podezřelé aplikace

/pattern	používat signatury (standardně)
/no-pattern	nepoužívat signatury
/heur	zapnout heuristiku (standardně)
/no-heur	vypnout heuristiku
/adv-heur	zapnout rozšířenou heuristiku (standardně)
/no-adv-heur	vypnout rozšířenou heuristiku
/ext-exclude=EXTENSIONS	vyloučit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=MODE	použít REŽIM léčení infikovaných objektů K dispozici jsou následující možnosti: • none (standardně) – automaticky se nevyléčí žádné objekty. • standard – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit. • strict – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit bez interakce uživatele (nebudete dotázáni na vymazání souboru). • rigorous – ecls.exe automaticky odstraní soubor bez pokusu o jeho vyléčení. • delete – ecls.exe automaticky odstraní soubor bez pokusu se jeho vyléčení, ale neodstraní se důležité systémové soubory.
/quarantine	uložit infikované soubory (při léčení) do karantény (doplňková akce při léčení souborů)
/no-quarantine	neukládat infikované soubory do karantény

Všeobecné možnosti:

/help	zobrazit tuto nápovědu a ukončit
/version	zobrazit informaci o verzi a ukončit
/preserve-time	zachovat čas přístupu k souborům

Návratové hodnoty:

0	nenalezeny žádné hrozby
1	hrozba nalezena a vyléčena
10	některé soubory nemohly být zkontrolovány (mohou obsahovat hrozby)
50	nalezena hrozba
100	chyba (návratové hodnoty větší než 100 znamenají, že soubor nebyl zkontrolován a nemůže být považován za čistý)

ESET CMD

Aktivováním této funkce povolíte provádění ecmd příkazů. Prostřednictvím této funkce můžete importovat a exportovat konfiguraci produktu pomocí příkazového řádku (ecmd.exe). Pokud tuto funkci neaktivujete, konfiguraci programu ESET Server Security můžete importovat/exportovat do *.xml* souboru výhradně prostřednictvím grafického rozhraní.

Po aktivování funkce ESET CMD (v rozšířeném nastavení v sekci Nástroje > ESET CMD) si vyberte způsob ověření:

- **Žádný** – bez autorizace. Tuto možnost nedoporučujeme, protože představuje potenciální bezpečnostní riziko, protože bude možné importovat nepodepsané konfigurace.

• **Heslo pro přístup do nastavení** – pro ověření se použije heslo, které chrání přístup do nastavení produktu. V tomto případě při importování konfigurace z .xml souboru dojde k ověření, zda je soubor podepsán (návod na podepsání naleznete níže) a podpis odpovídá heslu pro přístup do nastavení. Konfigurace se neimportuje pokud nemáte nastavenu ochranu heslem, heslo nesouhlasí nebo importovaný .xml není podepsán.

Poté co aktivujete funkci ESET CMD, můžete pro importování a exportování konfigurace produktu ESET Server Security používat příkazový řádek. Příkazy můžete pouštět manuálně, případně si operace v rámci automatizace naskriptovat.

Pro použití ecmd příkazů musíte mít oprávnění administrátora, resp. příkazový řádek **spustit jako administrátor**. V opačném případě se zobrazí chyba **Error executing command**. Při exportování konfigurace musí cílová složka existovat. Export je možný i v případě, kdy funkce ESET CMD není v produktu aktivní.

Konfiguraci z nainstalovaného produktu exportujete příkazem:
`ecmd /getcfg c:\config\settings.xml`

Konfiguraci do nainstalovaného produktu naimportujete příkazem:
`ecmd /setcfg c:\config\settings.xml`

ecmd příkazy jsou určeny výhradně pro lokální použití. Pokud příkaz spustíte vzdáleně prostřednictvím klientské úlohy **Spustit příkaz** v ESET PROTECT, neprovede se. V případě vzdálené správy konfigurujte produkt prostřednictvím politik.

Jak podepsat *.xml* konfigurační soubor:

1. Z webových stránek společnosti ESET si stáhněte nástroj XmlSignTool. Jedná se o oficiální nástroj určený pro podepisování konfiguračních souborů.

2. **Jako administrátor** si otevřete příkazový řádek (cmd).

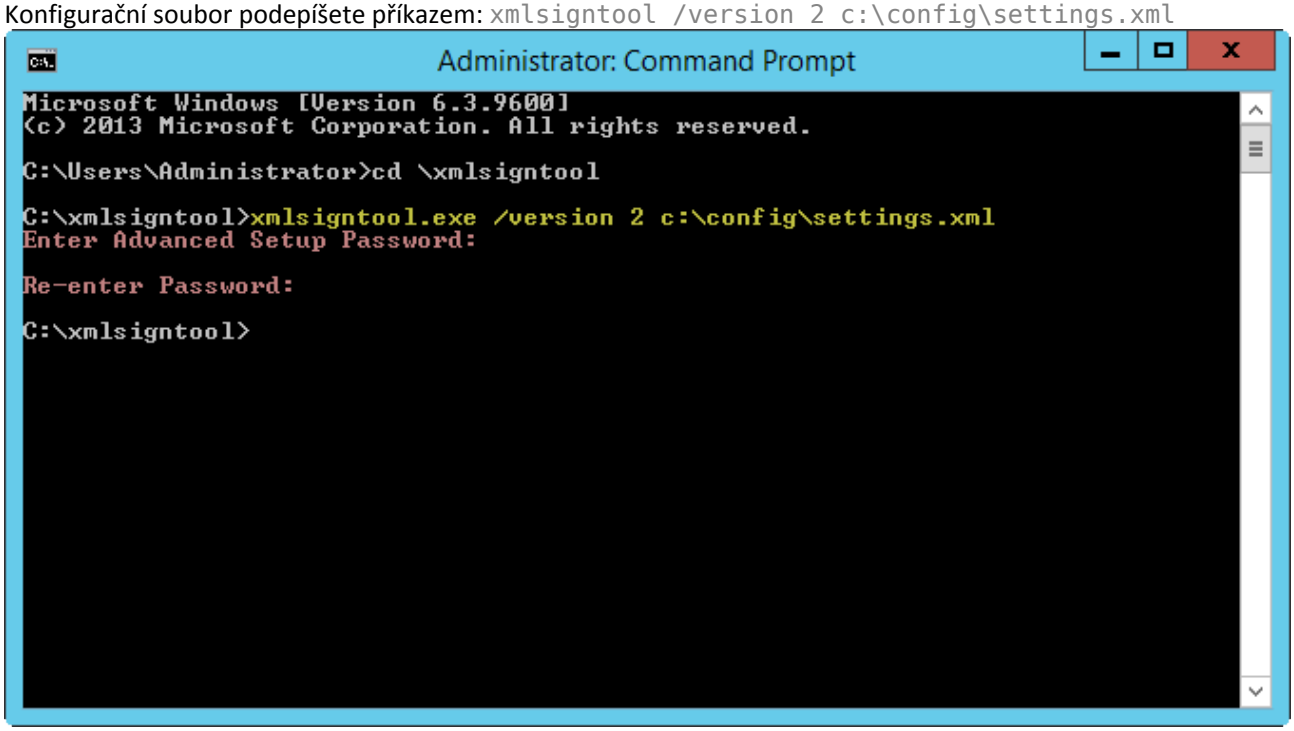
3. Přejděte do složky se staženým nástrojem `xmlsigntool.exe`.

4. Konfigurační příkaz *.xml* podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`

Hodnota parametru `/version` závisí na verzi ESET Server Security. Pro verzi ESET Server Security 7 a novější použijte `/version 2`.

5. Zaejte heslo, které jste si nastavili pro přístup do nastavení. Následně bude váš *.xml* soubor s konfigurací programu podepsán a můžete jej prostřednictvím ESET CMD importovat do jiné instalace ESET Server Security, kde máte nastaveno ověření stejným heslem.

Konfigurační soubor podepíšete příkazem: `xmlsigntool /version 2 c:\config\settings.xml`



V případě, že změníte heslo pro přístup do nastavení a budete chtít prostřednictvím ESET CMD importovat konfiguraci z *.xml* souboru podepsaného původním heslem, podepište jej nejprve aktuálním heslem. V opačném případě byste museli konfiguraci znovu exportovat z jiné instalace ESET Server Security.

ESET RMM

Remote Monitoring and Management (RMM) je způsob pro vzdálené monitorování a ovládání aplikací z jednoho místa (počítačů, serverů i mobilních zařízení) prostřednictvím agenta instalovaného na koncových stanicích.

Zapnout RMM

Aktivuje RMM. Abyste mohli používat nástroj RMM, je třeba mít oprávnění správce.

Učící režim

Vyberte učící režim RMM z rozbalovacího menu.

- **Pouze bezpečné operace** – tuto možnost vyberte v případě, kdy RMM rozhraní chcete aktivovat pouze v režimu pro čtení a provádění bezpečných operací
- **Všechny operace** – tuto možnost vyberte v případě, kdy prostřednictvím RMM rozhraní chcete provádět všechny operace

Způsob ověření

Z rozbalovací nabídky nastavte metodu autorizace RMM:

- **Žádný** – po vybrání této možnosti nebude vyhodnocováno, jaká aplikace spouští *ermm.exe*
- **Cesta k aplikaci** - vyberte aplikaci, která bude mít oprávnění pro spouštění *ermm.exe*

Soubor *ermm.exe* naleznete standardně ve složce s produktem ESET Server Security (například *c:\Program Files\ESET\ESET Server Security*). Binárka *ermm.exe* zajišťuje výměnu dat s RMM doplňkem, který komunikuje s RMM agentem napojeným na RMM server.

- *ermm.exe* – nástroj příkazového řádku vyvinutý společností ESET, který umožňuje správu firemních bezpečnostních produktů a komunikaci s RMM doplňkem.

- RMM doplněk je aplikace třetí strany, která běží lokálně na Windows stanici chráněné produktem ESET Endpoint. Doplněk byl navržen ke komunikaci RMM Agenta (například Kaseya) a *ermm.exe*.

- RMM Agent je aplikace třetí strany (například Kaseya), která běží lokálně na Windows stanici chráněné produktem ESET Endpoint. Agent komunikuje s RMM doplňkem a RMM serverem.

- RMM Server je server třetí strany. Podporované RMM systémy: Kaseya, Labtech, Autotask, Max Focus a Solarwinds N-able.

Podrobnější informace o ESET RMM ESET Server Security naleznete v ESET Databázi znalostí.

ESET Direct Endpoint Management pluginy pro RMM řešení třetích stran

RMM Server běží jako služba na serveru třetí strany. Pro více informací se podívejte do konkrétních online uživatelských příruček:

- ESET Direct Endpoint Management Plug-in pro ConnectWise Automate

- ESET Direct Endpoint Management Plugin pro DattoRMM

- ESET Direct Endpoint Management pro Solarwinds N-Central

- ESET Direct Endpoint Management pro NinjaRMM

Licence

ESET Server Security se několikrát za hodinu připojuje k licenčním serverům ESET. Ve výchozím nastavení je **Interval ověření** nastaven na **Automaticky**. V případě potřeby můžete změnou nastavení na **Omezeně** snížit množství přenášených dat. Mějte na paměti, že produkt se následně k licenčním serverům připojí jednou za den, případně po restartování počítače.

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

Poskytovatel WMI

Služba Windows Management Instrumentation (WMI) je implementace správy WBEM (Web-Based Enterprise Management) společnosti Microsoft. Správa WBEM je iniciativa k ustanovení standardů pro přístup a sdílení informací správy v rozlehlé síti.

Více informací o WMI naleznete v databázi znalostí společnosti Microsoft:
http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx

ESET WMI Provider

Účelem ESET WMI Provider je zajistit vzdálené sledování produktů ESET v podnikovém prostředí bez nutnosti instalovat další aplikace a nástroje ESET. Poskytnutím základních informací o produktu, stavu a statistikách prostřednictvím WMI výrazně rozšiřujeme možnosti podnikových administrátorů při monitorování produktů ESET.

Administrátoři tak mohou využít množství přístupových metod (příkazový řádek, skripty a nástroje pro monitorování podnikových systémů třetích stran), které WMI nabízí ke sledování stavu jejich produktů společnosti ESET.

Současná implementace poskytuje přístup ke čtení základních informací o produktu, nainstalovaných funkcích a jejich stavu, statistikám jednotlivých skenerů a protokolům.

Poskytovatel WMI umožňuje použít standardní Windows WMI infrastrukturu a nástroje pro čtení informací o produktu a protokolů.

Poskytovaná data

Všechny WMI třídy související s produktem ESET patří do jmenného prostoru “root\ESET“. Níže naleznete seznam všech tříd, společně s jejich popisem, které jsou aktuálně v produktu implementovány:

Obecné

- 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

Třída ESET_Product

Třída ESET_Product může mít pouze jednu instanci. Vlastnosti této třídy odkazují na základní informace o nainstalovaném produktu ESET:

- ID – identifikátor produktu, například “emsl”
- Name – název produktu, například "ESET Mail Security"
- FullName – úplný název produktu, například "ESET Mail Security for IBM Domino"
- Version – verze produktu, například "6.5.14003.0"
- VirusDBVersion – verze detekčního jádra, například "14533 (20161201)"
- VirusDBLastUpdate – časové razítko poslední úspěšné aktualizace detekčního jádra. Řetězec obsahuje časové razítko datovém formátu WMI, například “20161201095245.000000+060”
- LicenseExpiration – čas do vypršení licence. Řetězec obsahuje časové razítko v datovém formátu WMI
- KernelRunning – boolean hodnota reprezentující, zda ekrn služba na počítači běží, například “TRUE”
- StatusCode – číslo reprezentuje stav ochrany: 0 – Zelená (OK), 1 – Žlutá (Varování), 2 – Červená (Chyba)
- StatusText – popis, pokud není návratová hodnota 0

ESET_Features

Třída ESET_Features může mít více instancí a jejich počet závisí na množství funkcí produktu. Každá instance obsahuje:

- Name – název funkce (jejich seznam je uveden níže)
- Status – stav funkce: 0 - neaktivní, 1 - vypnutá, 2 - zapnutá

Seznam řetězců reprezentující funkce aktuálně nainstalovaného produktu:

- CLIENT_FILE_AV – rezidentní ochrana souborového systému
- CLIENT_WEB_AV – ochrana přístupu na web
- CLIENT_DOC_AV – ochrana dokumentů
- CLIENT_NET_FW – personální firewall
- CLIENT_EMAIL_AV – antivirová e-mailová ochrana
- CLIENT_EMAIL_AS – antispamová ochrana klienta
- SERVER_FILE_AV – rezidentní ochrana souborů na chráněném serveru, například obsah SharePoint databáze v případě ESET Server Security

• SERVER_EMAIL_AV – antivirová e-mailová ochrana na chráněném serveru, například e-mailů na Microsoft Exchange nebo IBM Domino

• SERVER_EMAIL_AS – antispamová e-mailová ochrana na chráněném serveru, například e-mailů na Microsoft Exchange nebo IBM Domino

• SERVER_GATEWAY_AV – antivirová ochrana síťových protokolů na gateway

• SERVER_GATEWAY_AS – antispamová ochrana síťových protokolů na gateway

ESET_Statistics class

Třída ESET_Features může mít více instancí a jejich počet závisí na množství skenerů. Každá instance obsahuje: Každá instance obsahuje:

• Scanner – řetězec reprezentující určitý skener, například “CLIENT_FILE”

• Total – celkový počet zkontrolovaných souborů

• Infected – počet infikovaných souborů

• Cleaned – počet vyléčených souborů

• Timestamp – časové razítko poslední aktualizace statistik. Řetězec obsahuje časové razítko datovém formátu WMI, například “20130118115511.000000+060”

• ResetTime – časové razítko posledního obnovení čítače statistik. Řetězec obsahuje časové razítko datovém formátu WMI, například “20130118115511.000000+060”

Seznam řetězců reprezentující aktuálně rozpoznané skenery:

• CLIENT_FILE

• CLIENT_EMAIL

• CLIENT_WEB

• SERVER_FILE

• SERVER_EMAIL

• SERVER_WEB

ESET_ThreatLog

Třída ESET_ThreatLog class může mít více instancí. Každá reprezentuje konkrétní záznam protokolu “Detekované hrozby”. Každá instance obsahuje:

• ID – unikátní ID záznamu protokolu

• Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)

• LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical,

SecurityWarning-Critical

- Scanner – název skeneru, který zaznamenal tuto událost
- ObjectType – typ objektu, který souvisí s tímto záznamem v protokolu
- ObjectName – název objektu, který souvisí s tímto záznamem v protokolu
- Threat – název hrozby nalezené v detekovaném objektu reprezentovaný ObjectName a ObjectType
- Action – akce provedená po výskytu hrozby
- User – uživatelský účet, pod kterým událost vznikla
- Information – další informace o této události
- Hash – kontrolní součet objektu, který souvisí s tímto záznamem v protokolu

ESET_EventLog

Třída ESET_ThreatLog class může mít více instancí. Každá reprezentuje konkrétní záznam protokolu "Detekované hrozby". Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Module – název modulu, pod který událost vznikla
- Event – popis události
- User – uživatelský účet, pod kterým událost vznikla

ESET_ODFileScanLogs

Třída ESET_ODFileScanLogs může mít více instancí. Každá reprezentuje konkrétní záznam protokolu volitelné kontroly počítače. Tedy jde o ekvivalent záznamů dostupných v hlavním okně programu na záložce Nástroje > Protokoly > Kontrola počítače. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- Targets – kontrolované složky/objekty
- TotalScanned – celkový počet zkontrolovaných souborů
- Infected – počet infikovaných souborů
- Cleaned – počet vyléčených souborů

- Status – stav funkce:

ESET_ODFileScanLogRecords

Třída ESET_ODFileScanLogRecords může mít více instancí. Každá reprezentuje konkrétní záznam instance třídy ESET_ODFileScanLogs. Instance této třídy poskytuje záznamy všech kontrol počítače. Pokud je požadována instance určitého protokolu kontroly, musí být filtrována pouze podle vlastnosti LogID. Každá instance obsahuje:

- LogID – ID protokolu kontroly, do které záznam patří (ID jedné z instancí třídy ESET_ODFileScanLogs)
- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log – aktuální záznam protokolu

ESET_ODServerScanLogs

Třída ESET_ODServerScanLogs může mít více instancí. Každá reprezentuje konkrétní záznam spuštění volitelné kontroly serveru. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- Targets – kontrolované složky/objekty
- TotalScanned – celkový počet zkontrolovaných souborů
- Infected – počet infikovaných souborů
- Cleaned – počet vyléčených souborů
- RuleHits – celkový počet použitých
- Status – stav funkce:

ESET_ODServerScanLogRecords

Třída ESET_ODServerScanLogRecords může mít více instancí. Každá reprezentuje konkrétní záznam instance třídy ESET_ODServerScanLogs class. Instance této třídy poskytuje záznamy všech kontrol počítače. Pokud je požadována instance určitého protokolu kontroly, musí být filtrována pouze podle vlastnosti LogID. Každá instance obsahuje:

- LogID – ID protokolu kontroly, do které záznam patří (ID jedné z instancí třídy ESET_ODFileScanLogs)
- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)

• LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

• Log – aktuální záznam protokolu

ESET_ODServerScanLogs

Třída ESET_ThreatLog class může mít více instancí. Každá reprezentuje konkrétní záznam protokolu “Detekované hrozby”. Každá instance obsahuje:

• ID – unikátní ID záznamu protokolu

• Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)

• LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

• HELODomain – název HELO domény

• IP - Source IP adresa

• Sender – e-mailová adresa odesílatele

• Recipient – e-mailová adresa příjemce

• ProtectionType – použitý typ ochrany

• Action – provedená akce

• Důvod - Důvod k provedení akce

• TimeToAccept – čas, po kterém bylo přijetí e-mailu akceptováno

ESET_HIPSLog

Třída ESET_HIPSLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu “HIPS”. Každá instance obsahuje:

• ID – unikátní ID záznamu protokolu

• Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)

• LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical

• Application – zdrojová aplikace

• Target - Klikněte na nalezený výsledek nebo spuštění potvrďte klávesou of operace

• Action – akce provedená modulem HIPS (například povoleno, zablokováno, ...)

- Rule – název pravidla zodpovědného za provedení akce
- Další pravidla

ESET_URLLog

Třída ESET_URLLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu “Filtrované webové stránky”. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- URL – adresa webové stránky
- Status – informace, co se s URL stalo (například "Zablokováno filtrováním obsahu webu")
- Application – aplikace, která se pokusila přistoupit na danou URL
- User – uživatelský účet, pod kterým běžela daná aplikace

ESET_DevCtrlLog

Třída ESET_DevCtrlLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu “Správy zařízení”. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Device – název zařízení
- User – název uživatelského účtu
- UserSID – SID uživatelského účtu
- Group – název skupiny uživatele
- GroupSID – SID skupiny uživatele
- Status – informace, co se se zařízením stalo (např. "Zápis zablokován")
- DeviceDetails – dodatečné informace týkajících se zařízení
- EventDetails – další informace týkající se této události

ESET_MailServerLog

Třída ESET_MailServerLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu "ochrany poštovního serveru". Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- IPAddr – zdrojová IP adresa
- HELODomain – název HELO domény
- Sender – e-mailová adresa odesílatele
- Recipient – e-mailová adresa příjemce
- Subject – předmět e-mailu
- ProtectionType – typ ochrany, která provedena akci uvedenou v protokolu (antimalware, antispam nebo pravidla).
- Action – provedená akce
- Reason – důvod, proč byla provedena akce součástí uvedenou v ProtectionType.

ESET_HyperVScanLogs

Třída ESET_HyperVScanLogs může mít více instancí. Každá reprezentuje konkrétní Hyper-V kontrolu. Jedná se o ekvivalent záznamu v protokolu "Hyper-V kontroly" v grafickém rozhraní produktu. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- Targets – kontrolovaná cílová stanice/disky/jednotky
- TotalScanned – celkový počet zkontrolovaných souborů
- Infected – počet infikovaných souborů
- Cleaned – počet vyléčených souborů
- Status – stav funkce:

ESET_HyperVScanLogRecords

Třída ESET_HyperVScanLogRecords může mít více instancí. Každá reprezentuje jeden záznam v protokolu instancí třídy ESET_HyperVScanLogs. Instance této třídy poskytují záznamy protokolu všech Hyper-V kontrol. Pokud je požadována instance určitého protokolu kontroly, musí být filtrována pouze podle vlastnosti LogID. Každá

instance obsahuje:

- LogID – ID protokolu kontroly, do které záznam patří (ID jedné z instancí třídy ESET_HyperVScanLogs)
- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log – aktuální záznam protokolu

ESET_NetworkProtectionLog

Třída ESET_NetworkProtectionLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu "Síťová ochrana". Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Event – událost zachycená modulem zajišťujícím ochranu sítě
- Action – provedená akce modulem zajišťujícím ochranu sítě
- Source – adresa zdrojového zařízení
- Target – adresa cílového zařízení
- Protocol – použitý síťový komunikační protokol
- RuleOrWormName – název červa nebo pravidlo související s danou událostí
- Application – aplikace, která inicializovala síťovou komunikaci
- User – uživatelský účet, pod kterým událost vznikla

ESET_SentFilesLog

Třída ESET_SentFilesLog může mít více instancí. Každá reprezentuje konkrétní záznam protokolu "Odeslané soubory". Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical,

SecurityWarning-Critical

- Sha1 – Sha-1 kontrolní součet odeslaného souboru
- File – název odeslaného souboru
- Size – velikost odeslaného souboru
- Category – kategorie odeslaného souboru
- Reason – důvod k odeslání souboru
- SentTo – informace, do jakého cloudového systému společnosti ESET byl soubor odeslán
- User – uživatelský účet, pod kterým událost vznikla

ESET_OneDriveScanLogs

Třída ESET_OneDriveScanLogs může mít více instancí. Každá reprezentuje konkrétní OneDrive kontrolu. Jedná se o ekvivalent záznamu v protokolu "OneDrive kontroly" v grafickém rozhraní produktu. Každá instance obsahuje:

- ID – unikátní ID záznamu protokolu OneDrive kontroly
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- Targets – kontrolované složky/objekty
- TotalScanned – celkový počet zkontrolovaných souborů
- Infected – počet infikovaných souborů
- Cleaned – počet vyléčených souborů
- Status – stav funkce:

ESET_OneDriveScanLogRecords

Třída ESET_OneDriveScanLogRecords může mít více instancí. Každá reprezentuje jeden záznam v protokolu instancí třídy ESET_OneDriveScanLogs. Instance této třídy poskytují záznamy protokolu všech OneDrive kontrol. Pokud je požadována instance určitého protokolu kontroly, musí být filtrována pouze podle vlastnosti LogID. Každá instance obsahuje:

- LogID – ID protokolu kontroly, do níž záznam patří (ID některé z instancí třídy ESET_OneDriveScanLogs)
- ID – unikátní ID záznamu protokolu OneDrive kontroly
- Timestamp – časové razítko vytvoření záznamu (ve WMI formátu/časovém formátu)
- LogLevel – závažnost záznamu reprezentovaný číselným údajem [0-8]. Hodnoty odpovídají těmto úrovním: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- Log – aktuální záznam protokolu

Přístup k poskytovaným datům

Níže uvádíme několik příkladů, jak získat ESET WMI data prostřednictvím příkazového řádku a PowerShellu, které můžete použít z jakéhokoli operačního systému Windows. K WMI třídám můžete přistupovat mnoha způsoby prostřednictvím dalších skriptovacích jazyků a nástrojů.

Příkazový řádek bez skriptů

Příkazový řádek `wmic` lze použít pro přístup k různým předdefinovaným nebo vlastním třídám WMI.

Pro zobrazení informací o nainstalovaném produktu ESET na lokálním počítači použijte příkaz:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Pro zobrazení pouze informace o verzi nainstalovaného produktu ESET na lokálním počítači použijte příkaz:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Pro zobrazení informací o nainstalovaném produktu ESET na vzdáleném s IP adresou počítači použijte příkaz 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Pro zobrazení informací o nainstalovaném produktu ESET na lokálním počítači použijte příkaz:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Pro zobrazení informací o nainstalovaném produktu ESET na vzdáleném s IP adresou počítači použijte příkaz 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
```

Cíle kontroly: ESET konzole pro vzdálenou správu

Pomocí této možnosti získáte do ESET PROTECT seznam cílů (pro volitelnou kontrolu databáze poštovních schránek a Hyper-V kontrolu), a můžete je následně použít při vytváření klientské úlohy na Kontrolu volitelných cílů. Seznam cílů bude v ESET Server Security dostupný pouze v případě, kdy je na serveru společně s ESET PROTECT nainstalován též ESET Management Agent.

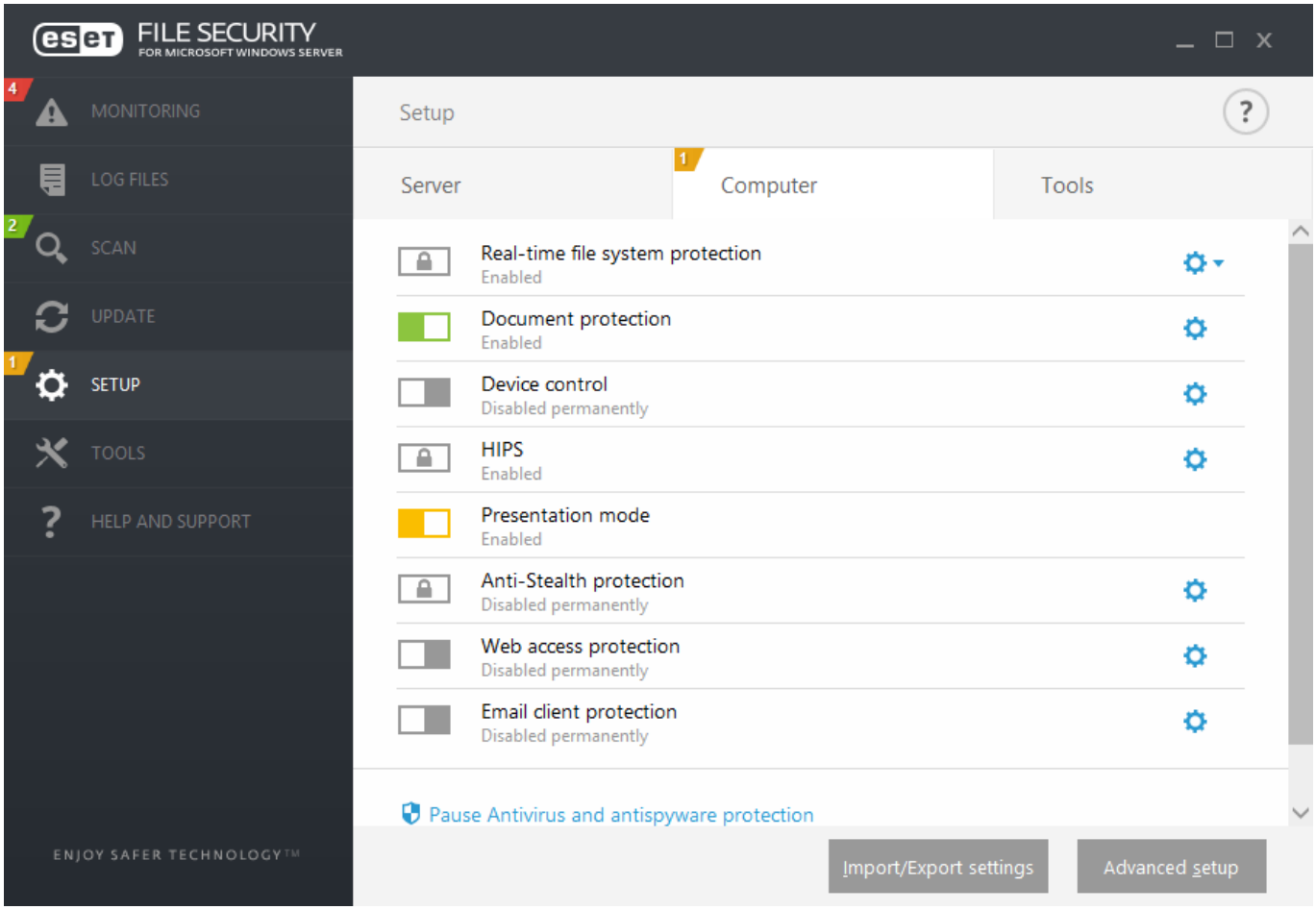
Když povolíte **Generovat seznam cílů**, ESET Server Security vytvoří seznam dostupných cílů kontroly. Tento seznam je generován periodicky s přihlédnutím k **stanovenému intervalu**.

> Prvotní **generování seznamu cílů** kontroly bude trvat polovinu intervalu, ve kterém má ESET PROTECT **replikovat cíle**. Například, pokud máte **interval aktualizace** nastaven na 60 minut, dostupné cíle kontroly v ESET PROTECT budete mít k dispozici již po 30 minutách. Pokud potřebujete získat seznam pomocí ESET PROTECT dříve, nastavte kratší interval aktualizace. Kdykoli jej následně můžete opět prodloužit.

Když ESET PROTECT spouští klientskou úlohu **Kontrola serveru**, bude shromažďovat seznam a budete na daném serveru vyzváni k výběru cílů kontroly pro Hyper-V kontrolu.

Dočasná změna nastavení

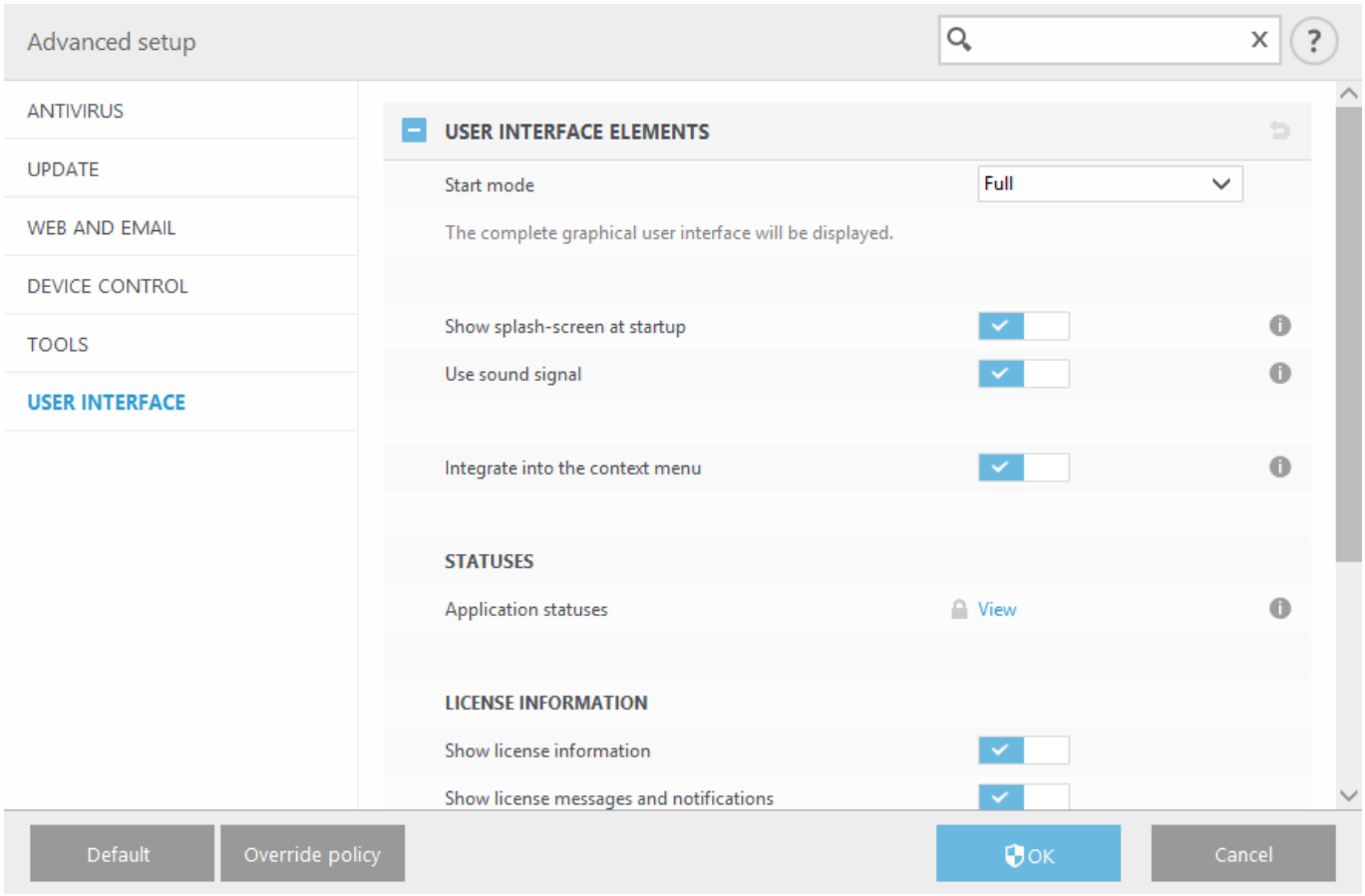
Pokud jsou na ESET Server Security vynuceny politiky ESET PROTECT, zobrazí se na stránce Nastavení ikona zámku místo přepínače zapnout/vypnout a vedle přepínače v okně **Rozšířená nastavení** se také zobrazí ikona zámku.



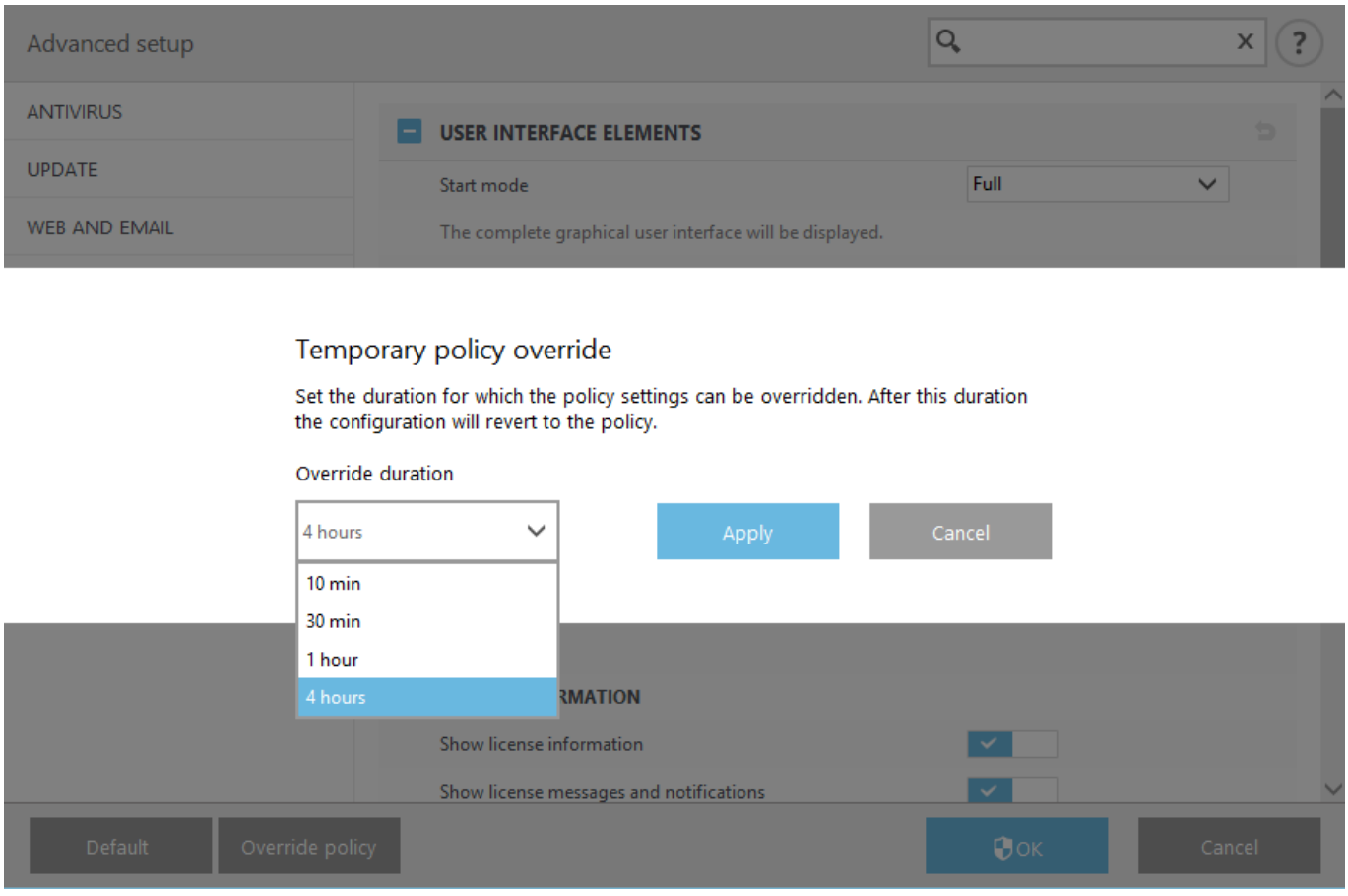
Nastavení vynucená politikou z ESET PROTECT není možné standardně lokálně měnit. V případě, že je potřebujete modifikovat, například při řešení problémů, můžete využít režim dočasné změny nastavení. Aktivaci tohoto režimu pro **dočasnou změnu nastavení** je nutné nejprve povolit prostřednictvím politiky z ESET PROTECT.

Přihlaste se do ESET PROTECT Web Console, přejděte na záložku **Politiky** a vyberte a upravte existující politiku pro ESET Server Security, případně vytvořte novou. V **konfigurační šabloně** přejděte na záložku **Dočasná změna nastavení**. Pomocí přepínače tuto možnost aktivujte a nastavte její parametry včetně způsobu ověření (heslem nebo uživatelským účtem z Active Directory).

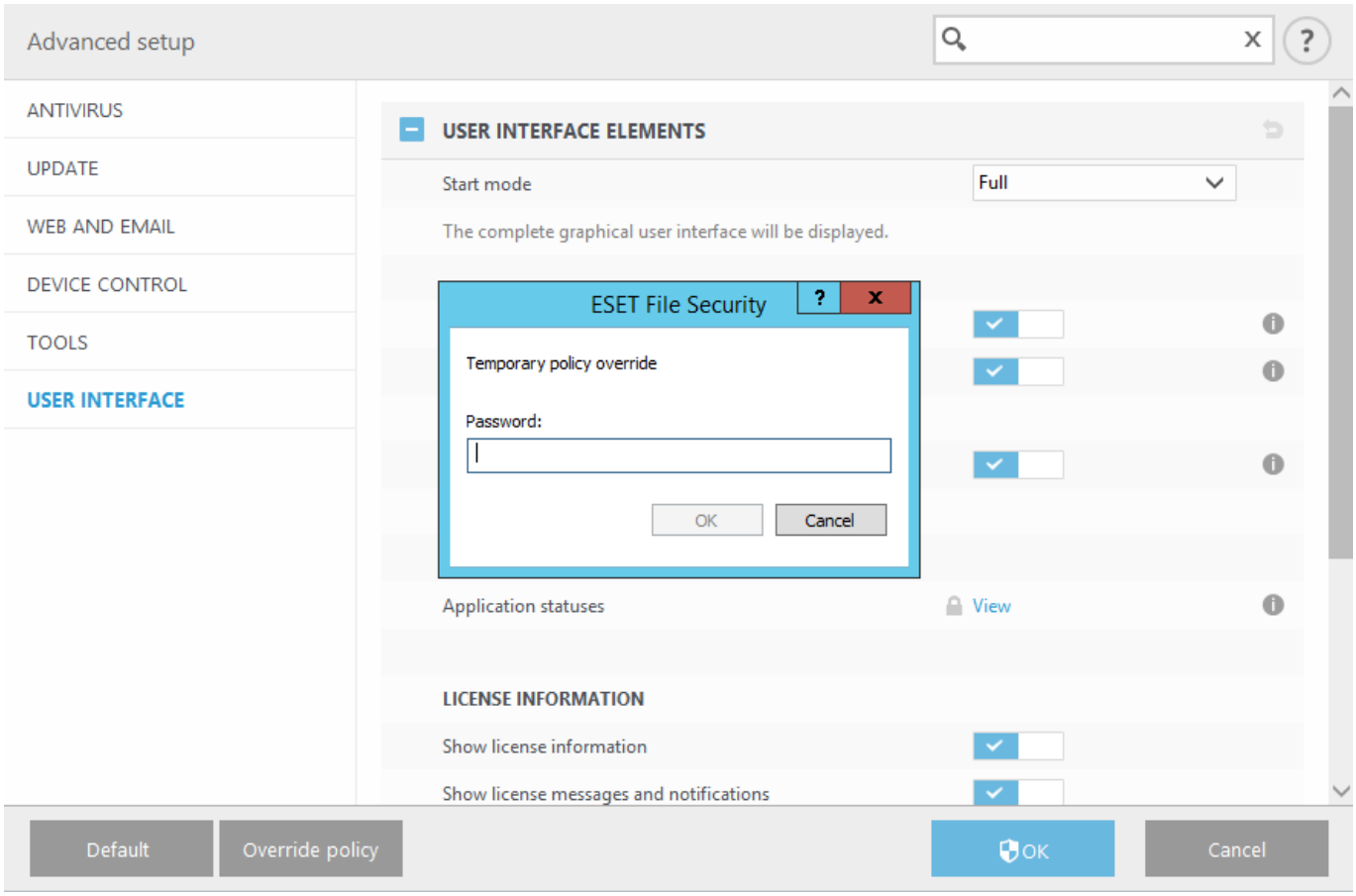
Po úpravě politiky nebo po vynucení nové politiky pro ESET Server Security se v okně **Rozšířená nastavení** zobrazí tlačítko Dočasně změnit nastavení.



Klikněte na toto **tlačítko**, vyberte dobu platnosti změn a klikněte na tlačítko **Použít**.



Pokud jste nastavili ověřování **heslem**, budete vyzváni k jeho zadání.



Po vypršení Dočasné změny nastavení se všechny změny provedené v konfiguraci vrátí zpět k původnímu nastavení politik ESET PROTECT. Před vypršením Dočasné změny nastavení se zobrazí oznámení.

V případě potřeby můžete režim dočasné změny nastavení **kdykoli ručně ukončit** v hlavním okně programu na záložce Přehled nebo v Rozšířeném nastavení.

Protokoly

V této části můžete upravit konfiguraci záznamu dat produktem ESET Server Security.

Filtr protokolování

Standardně jsou aktivní všechny možnosti, a proto se po zapnutí diagnostického režimu začne sbírat velké množství dat. V závislosti na typu řešeného případu doporučujeme deaktivovat sběr z dat z komponent, které s daným problém nesouvisí.

> Diagnostická data se začnou sbírat v případě, kdy pokud zapnete v hlavním okně programu na záložce **Nastavení** > Nástroje možnost **Diagnostické protokolování**. Následně ESET Server Security začne sbírat data z modulů, u kterých jste v této sekci tuto možnost aktivovali.

Pomocí přepínačů můžete zapínat nebo vypínat jednotlivé funkce. Dostupnost jednotlivých možností závisí na nainstalovaných součástech ESET Server Security.

- **Diagnostické protokolování clusteru** – aktivováním této možnosti zapnete diagnostické protokolování ESET clusteru.

Protokoly

V této sekci můžete upravit způsob správy protokolů. To je důležité pro zabránění zaplnění disku protokoly. Ve výchozí konfiguraci je zapnuto automatické mazání starých záznamů, čímž program šetří místo na disku.

Automaticky odstranit staré záznamy

Záznamy starší než zadaný počet dní budou odstraněny.

Odstranit záznamy starší než (dní)

Zadejte počet dní.

Automaticky odstranit staré záznamy, pokud je protokol velký

V případě, že tuto možnost aktivujete, při překročení velikosti definované v poli **Max. velikost protokolu [v MB]** budou staré protokoly odstraněny od doby, než dosáhne hodnoty definované v poli **Velikost optimalizovaného protokolu [v MB]**.

Automaticky zálohovat odstraněné záznamy

Pokud aktivujete tuto možnost, odstraněné záznamy protokolu budou zazálohovány do vámi definované složky a případně zabaleny do ZIP archivu.

Zálohovat diagnostické protokoly

Pokud aktivujete tuto možnost, zálohovány budou také diagnostické protokoly. Tato možnost je standardně vypnutá, a protokoly se nezálohují.

Zálohovat do složky

Vyberte složku, do které chcete zálohovat odstraněné záznamy. V případě potřeby můžete aktivovat ZIP kompresi.

Automaticky optimalizovat protokoly

Tato funkce zajišťuje automatickou defragmentaci protokolů, pokud počet nevyužitých záznamů překročí zadaný poměr v procentech v poli **Při překročení počtu nevyužitých záznamů (v procentech)**. Kliknutím na **Optimalizovat** spustíte ručně defragmentaci protokolů. Defragmentace odstraňuje prázdné záznamy v protokolech, čímž zvyšuje rychlost zpracovávání. Viditelné zlepšení práce s protokoly je po optimalizaci znatelné hlavně především u protokolů s velkým množstvím záznamů.

Zaznamenávat textové protokoly

Pomocí této možnosti aktivujete ukládání protokolů do alternativního formátu.

- **Cílová složka** – složka, do které se uloží protokoly (platné pouze pro **Text**/**CSV**). Každý protokol se ukládá do samostatného souboru (například ve *virlog.txt* naleznete Zachycené hrozby, pokud protokoly ukládáte jako prostý text).
- **Typ** – pokud vybere **Text** jako formát souborů, protokoly budou uloženy do textového souboru; data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené středníkem (**CSV**). Pokud vyberete **Událost**, protokol bude uložen do systémového Protokolu událostí, který si můžete zobrazit v Prohlížeči událostí (dostupném v Ovládacích panelech).
- **Odstranit všechny protokoly** – po kliknutí vymaže všechny protokoly vybrané v rozbalovacím menu **Typ**.

> V rámci rychlého vyřešení problémů vás specialisté technické podpory ESET mohou požádat o zaslání protokolů. Pomocí nástroje ESET Log Collector snadno sesbíráte ze svého počítače potřebná data. Více informací o nástroji ESET Log Collector naleznete v naší Databázi znalostí .

Audit log

Pomocí této možnosti můžete sledovat změny provedené v konfiguraci produktu a jeho stavů ochrany. Vzhledem k tomu, že změna konfigurace produktu může dramaticky ovlivnit fungování produktu, možná budete chtít sledovat změny pro účely auditu. Informace o provedených změnám naleznete v hlavním okně programu na záložce **Protokoly** > Audit log.

Proxy server

Ve velkých lokálních sítích může připojení do internetu zajišťovat tzv. proxy server. V takovém případě musí být správně zadána v nastavení programu. Pokud neprovedete nastavení, program se nebude moci automaticky aktualizovat. V ESET Server Security je nastavení proxy serveru dostupné ve dvou různých sekcích v **Upřesnit nastavení** (**F5**):

1. Otevřete **Rozšířená nastavení** (F5) > **Aktualizace** > **Profily** > **Aktualizace** > **Nastavení připojení** > HTTP Proxy. Toto nastavení je platné pro konkrétní profil aktualizace a je vhodné jej použít, pokud se jedná o přenosný

počítač, který provádí aktualizaci z různých míst.

2. **Rozšířená nastavení** (F5) > **Nástroje** > **Proxy server**. Nastavení proxy serveru na této úrovni definuje globální nastavení proxy serveru pro všechny ESET Server Security. Parametry zde budou používat všechny moduly, které se připojují k internetu.

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

Proxy server vyžaduje autentifikaci

V případě, že komunikace s proxy serverem vyžaduje autentifikaci, aktivujte tuto možnost a zadejte patřičné údaje do polí **Uživatelské jméno** a **Heslo**.

Vyhledat proxy server

Pro automatické získání konfigurace proxy serveru klikněte na tlačítko **Vyhledat**. Konfigurace proxy se tímto přenese z nastavení programu Internet Explorer.

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

Použít přímé spojení, pokud není dostupný proxy server

Pokud má produkt nastaveno využívání HTTP Proxy a ten nebude dostupný, po aktivování této možnosti se produkt zkusí připojit k serverům ESET bez použití proxy.

Oznámení

Upozornění na ploše a bublinové tipy slouží pouze pro zobrazování informací a nenabízejí ani nevyžadují interakci uživatele. Zobrazují se v pravém dolním rohu obrazovky. Pokud nechcete zobrazovat oznámení nevyžadující interakci při běhu aplikací přes celou obrazovku, vyberte možnost Nezobrazovat oznámení při běhu aplikací zobrazených na celou obrazovku. Dále zde naleznete možnosti pro konfiguraci doby zobrazení upozornění a průhlednosti tohoto okna.

Pokud nechcete zobrazovat oznámení nevyžadující interakci při běhu aplikací přes celou obrazovku, vyberte možnost **Nezobrazovat oznámení při běhu aplikací zobrazených na celou obrazovku**.

Zobrazovat upozornění o úspěšné aktualizaci

O úspěšné aktualizaci budete informováni prostřednictvím zobrazení oznámení.

Odesílat oznámení o událostech e-mailem

Pomocí této možnosti aktivujete zasílání oznámení e-mailem.

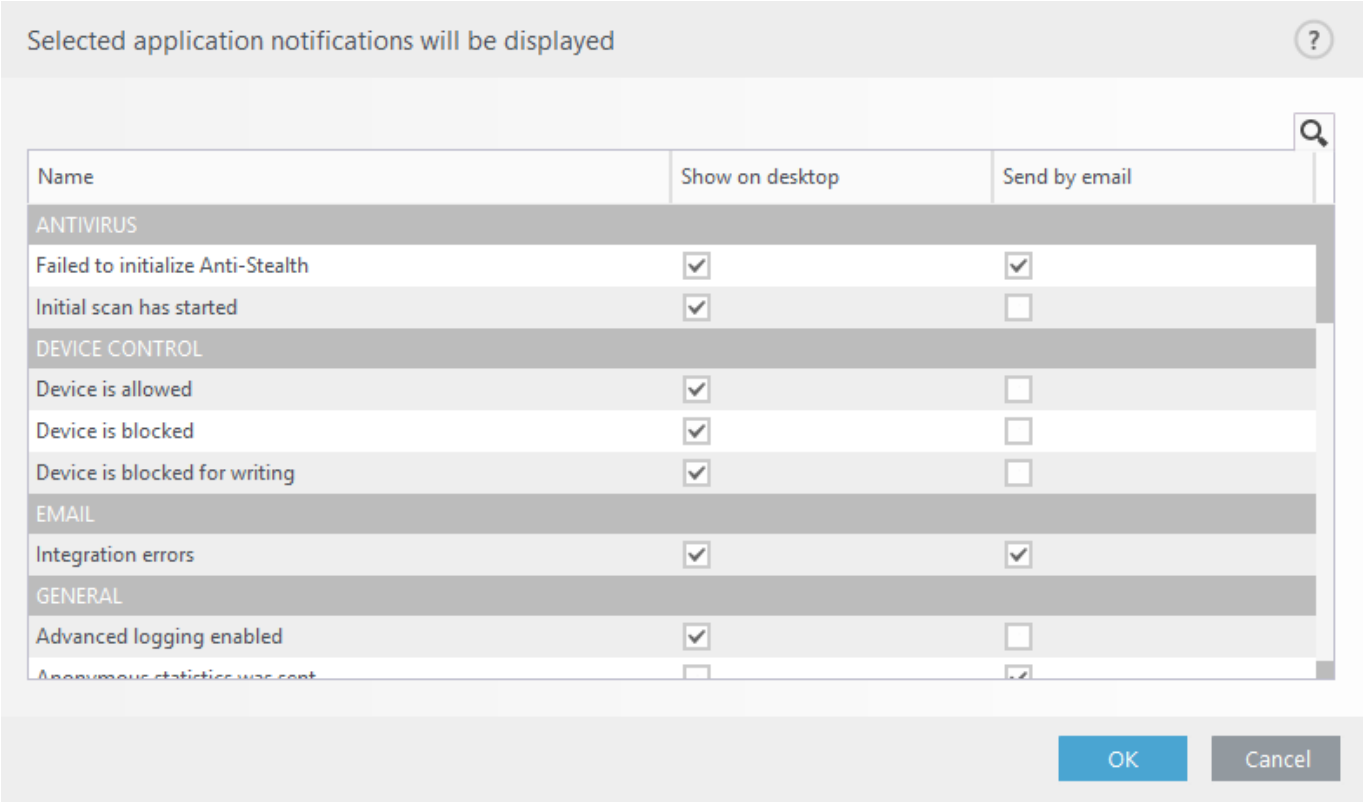
Oznámení aplikace

K zapnutí či vypnutí oznámení aplikace klikněte na Změnit.

Oznámení aplikace

V této části se můžete rozhodnout, zda chcete oznámení produktu ESET Server Security zobrazovat uživateli na Ploše, případně je zasílat e-mailem.

Pro funkční zasílání oznámení e-mailem je nutné v sekci **Obecné** aktivovat možnost **Odesílat oznámení o událostech e-mailem** a následně nakonfigurovat SMTP server.



Oznámení na pracovní ploše

V této sekci můžete konfigurovat výstražná a informační hlášení produktu ESET Server Security, například zobrazování informace o úspěšné aktualizaci. Nastavit můžete **dobu zobrazení** a **průhlednost** v oznamovací oblasti Windows (pouze u systémů, které zobrazování oznámení podporují).

V rozbalovacím menu **Zobrazovat události od úrovně** můžete nastavit bezpečnostní úroveň, od které chcete být informováni. K dispozici jsou následující možnosti:

- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy.
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy.
- **Varování** – obsahují varovné zprávy a kritické chyby.
- **Chyby** – obsahují chyby typu "Chyba při stahování souboru aktualizace" a kritické chyby.
- **Kritické chyby** – obsahují pouze kritické chyby.

Do pole **Ve víceuživatelském prostředí zobrazovat systémová hlášení tomuto uživateli** zadejte jméno uživatele,

který bude dostávat systémová a jiná oznámení v systémech umožňujících připojení více uživatelů současně. Standardně by tímto uživatelem měl být administrátor systému nebo sítě. Tato možnost je vhodná pro terminálové systémy, kdy všechna systémová oznámení budou chodit jen administrátorovi.

Přenést oznámení do popředí – po aktivování této možnosti se okno oznámení přesune do popředí obrazovky a bude dostupné pomocí klávesové zkratky Alt+Tab.

Oznámení e-mailem

ESET Server Security dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti.

ESET Server Security podporuje SMTP servery využívající TLS šifrování.

SMTP server

Adresa SMTP serveru, prostřednictvím kterého budou oznámení a upozornění odesílána. Typicky název vašeho Microsoft Exchange Serveru.

Uživatelské jméno a heslo

V případě, že SMTP server vyžaduje autorizaci, je nutné vyplnit tato pole pro přístup k SMTP serveru.

E-mailová adresa odesílatele

Specifikuje adresu odesílatele, která se použije v hlavičce e-mailové zprávy. Informace, kterou příjemce uvidí v polic **Od**.

E-mailové adresy příjemců

Zadejte e-mailové adresy příjemců, které budou uvedeny v poli Komu.

Povolit TLS

Po aktivování se budou upozornění a oznámení odesílat prostřednictvím TLS spojení.

Nastavení e-mailů

Odesílat události od úrovně

Specifikuje, od které úrovně důležitosti se budou upozornění na události odesílat.

Interval, ve kterém se budou nová upozornění odesílat (v min.)

Interval v minutách, po jehož uplynutí bude odeslán souhrnný e-mail se všemi upozorněními na události, které se v daném intervalu vyskytly. Pokud nastavíte hodnotu na 0, upozornění bude odesláno okamžitě po jeho výskytu.

Odesílat každé upozornění v samostatném e-mailu

Pokud je tato možnost aktivní, příjemce obdrží při výskytu události nové upozornění. Při výskytu velkého množství událostí v krátkém čase obdrží příjemce velké množství e-mailů.

Formát zprávy

Komunikace mezi programem a vzdáleným uživatelem nebo systémovým administrátorem probíhá prostřednictvím e-mailu nebo LAN zpráv (s využitím služby Windows messaging). Výchozí formát událostí je vhodný pro většinu situací. V případě potřeby si jej můžete přizpůsobit.

Formát zprávy o události

Formát zprávy, která se zobrazí na vzdáleném počítači.

Formát zprávy s upozorněním na hrozbu

Upozornění na hrozbu, stejně jako zprávy obsahující oznámení, mají předdefinovaný formát. Měnit jej doporučujeme pouze v ojedinělých případech. Například kdy máte automatizovaný systém na zpracovávání e-mailů.

Proměnné (řetězce mezi %) jsou nahrazovány aktuální informací. K dispozici jsou následující proměnné:

- %TimeStamp% – datum a čas události.
- %Scanner% – modul, který zaznamenal událost.
- %ComputerName% – název počítače, na kterém došlo k události.
- %ProgramName% – program, který způsobil událost.
- %InfectedObject% – název škodlivého souboru, e-mailové zprávy apod.
- %VirusName% – název infekce.
- %ErrorDescription% – popis chyby.

Klíčová slova **%InfectedObject%** a **%VirusName%** se používají pouze v upozorněních na hrozbu. Klíčové slovo **%ErrorDescription%** se používá pouze v informačních upozorněních.

Znaková sada

Z rozbalovacího menu si vyberte požadované kódování. Zpráva bude na základě vybrané sady převedena.

Používat Quoted-printable kódování

E-mailová zpráva bude zakódována do Quoted-printable formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

Přizpůsobení

V této části můžete definovat zprávu, která se zobrazí v patičce vybraných oznámení, a chování oznámení.

Výchozí zpráva oznámení

Výchozí zpráva, které se zobrazí v patičce oznámení.

Hrozby

Nezavírat automaticky upozornění na nalezenou hrozbu

Upozornění na nalezenou hrozbu se zobrazí na obrazovce tak dlouho, dokud jej uživatel nezavře ručně.

Použít výchozí zprávu

Po deaktivování této možnosti se zpřístupní textové pole Zpráva při nalezení hrozby. Vámi definovaný text se následně zobrazí při zablokování hrozby.

Zpráva při nalezení hrozby

Zadejte vlastní zprávu, která se uživateli zobrazí při zablokování hrozby.

Prezentační režim

Prezentační režim je funkce uživatele softwaru, kteří nechtějí být nejen v režimu celé obrazovky rušeni oznámeními a chtějí minimalizovat veškeré nároky na zatížení procesoru. Prezentační režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami produktu ESET Server Security. Zapnutím této funkce zakážete zobrazování všech oznámení a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

Aktivujte možnost Automaticky vypínat prezentační režim a následně definujte interval, po jehož uplynutí se Herní režim automaticky vypne.

Pokud je tato možnost aktivní, Prezentační režim se automaticky aktivuje při spuštění aplikace v režimu celé obrazovky. Zapnutím Prezentačního režimu nebude umožněno zobrazení notifikací či stavů změn vESET Server Security.

Automaticky vypínat Prezentační režim

Pomocí této možnosti můžete definovat interval, po jehož uplynutí se Prezentační režim automaticky vypne.

Diagnostika

Diagnostika poskytuje výpisy ze selhání běhu procesů programu ESET (například *ekrn.exe*). Pokud aplikace selže, vygeneruje se výpis, tzv. dump. Ten může pomoci vývojářům při ladění a opravě různých problémů v ESET Server Security.

Z rozbalovacího menu **Typ výpisu** vyberte jednu z níže uvedených možností:

- **Žádný** – vybráním této možnosti vypnete generování výpisů obsahu paměti.
- **Minimální** – (přednastavený) zaznamená nejmenší sadu užitečných informací, které mohou pomoci identifikovat důvod, proč se aplikace nečekaně zastavila. Tento typ výpisu může být užitečný, pokud jste omezeni volným místem na disku. Nicméně, kvůli omezenému množství zahrnutých informací, chyby, které nebyly způsobeny přímo vláknem běžícím v době problému, nemusí být objeveny analýzou tohoto souboru.
- **Úplný** – zaznamená celý obsah systémové paměti, když se aplikace nečekaně zastaví. Kompletní výpis z paměti může obsahovat data procesů, které běžely v době, kdy byl výpis vytvořen.

Cílová složka

Místo, kam se vygeneruje výpis při pádu.

Otevřít diagnostikou složku

Kliknutím na **Otevřít** se v novém okně *Průzkumníka Windows* zobrazí obsah výše definované složky.

Vytvořit diagnostický výpis

Po kliknutí na **Vytvořit** se do cílové složky vygeneruje soubor s výpisem obsahu paměti.

Rozšířené protokolování

Aktivovat rozšířené protokolování kontroly počítače
Po aktivování této možnosti se do protokolu zaznamenají všechny události, které vznikly při běhu rezidentní ochrany souborového systému nebo volitelné kontrole počítače.
Aktivovat rozšířené protokolování správy zařízení
Po zapnutí se zaznamenají veškeré události související s modulem Správa zařízení. Toto pomůže vývojářům při diagnostice a řešení problémů.
Aktivovat rozšířené protokolování Direct Cloud
Po aktivování této možnosti se do souboru zaznamená veškerá komunikace mezi produktem a servery Direct Cloud.
Aktivovat rozšířené protokolování ochrany dokumentů
Po zapnutí se zaznamenají veškeré události související s modulem Ochrana dokumentů. Toto pomůže vývojářům při diagnostice a řešení problémů.
Aktivovat rozšířené protokolování jádra
Po zapnutí se zaznamenají veškeré události z běhu jádra produktu ESET (`ekrn`). Toto pomůže vývojářům při diagnostice a řešení problémů.
Aktivovat rozšířené protokolování licence
Po zapnutí se zaznamená veškerá komunikace s licenčním serverem.
Zapnout výpis paměti
Po aktivování této možnosti se zaznamenají všechny události, které pomohou vývojářům při diagnostice úniku paměti (memory leaku).
Aktivovat rozšířené protokolování síťové ochrany
Po zapnutí bude do souboru v PCAP formátu zaznamenána veškerá síťová komunikace vyhodnocována síťovou ochranou. Toto pomůže vývojářům při diagnostice a řešení problémů se síťovou ochranou.
Aktivovat rozšířené protokolování operačního systému
Po aktivování se sesbírají informace o operačním systému jako jsou běžící procesy, aktivita CPU a diskové operace. Toto pomůže vývojářům při diagnostice a řešení problémů s chodem programu ve vašem operačním systému. Tato data pomohou vývojářům diagnostikovat a odstranit problémy související s chodem produktu ESET ve vašem operačním systému.
Aktivovat rozšířené protokolování filtrování protokolů
Do budou do souboru v PCAP formátu zaznamenána data zpracovaná filtrováním protokolů. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem filtrování protokolů.
Aktivovat rozšířené protokolování push zpráv
Po aktivování této možnosti se zaznamenají všechny události, které pomohou při diagnostice a řešení problémů souvisejících se zasíláním push zpráv.
Aktivovat rozšířené protokolování rezidentní ochrany souborového systému
Po zapnutí se zaznamenají veškeré události související s modulem Rezidentní ochrana souborového systému. Toto pomůže vývojářům při diagnostice a řešení problémů.
Aktivovat rozšířené protokolování modulu aktualizace
Po zapnutí se zaznamenají všechny události související s procesem aktualizace. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem zajišťujícím aktualizaci.
Umístění protokolů
C:\ProgramData\ESET\ESET Security\Diagnostics

Technická podpora

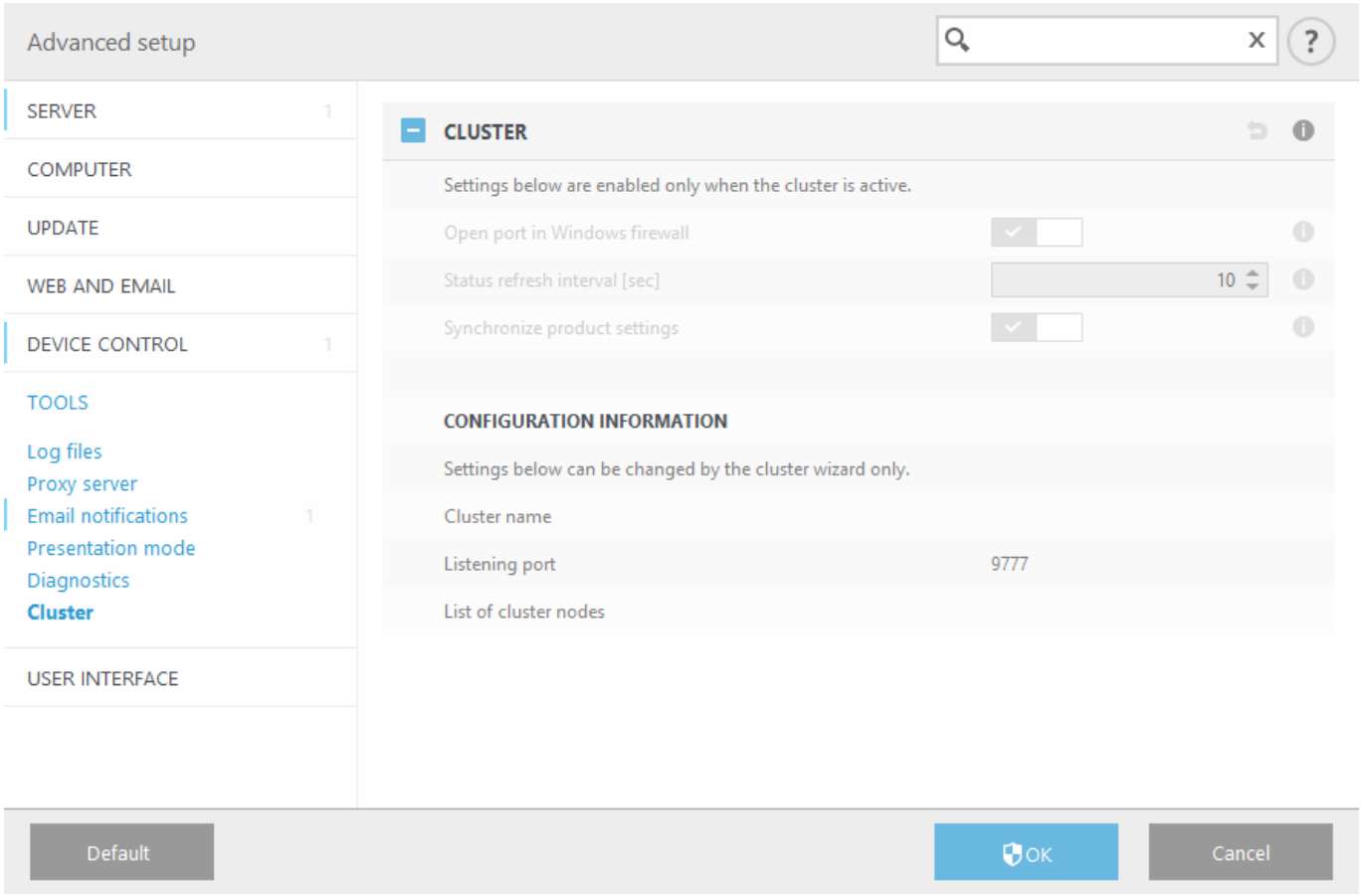
Odeslat data konfigurace systému

Vyberte možnost **Odeslat vždy bez dotázání o povolení k odeslání konfiguračních dat vašeho ESET Server Security technické podpoře nebo klikněte na možnost Dotázat se před odesláním**.

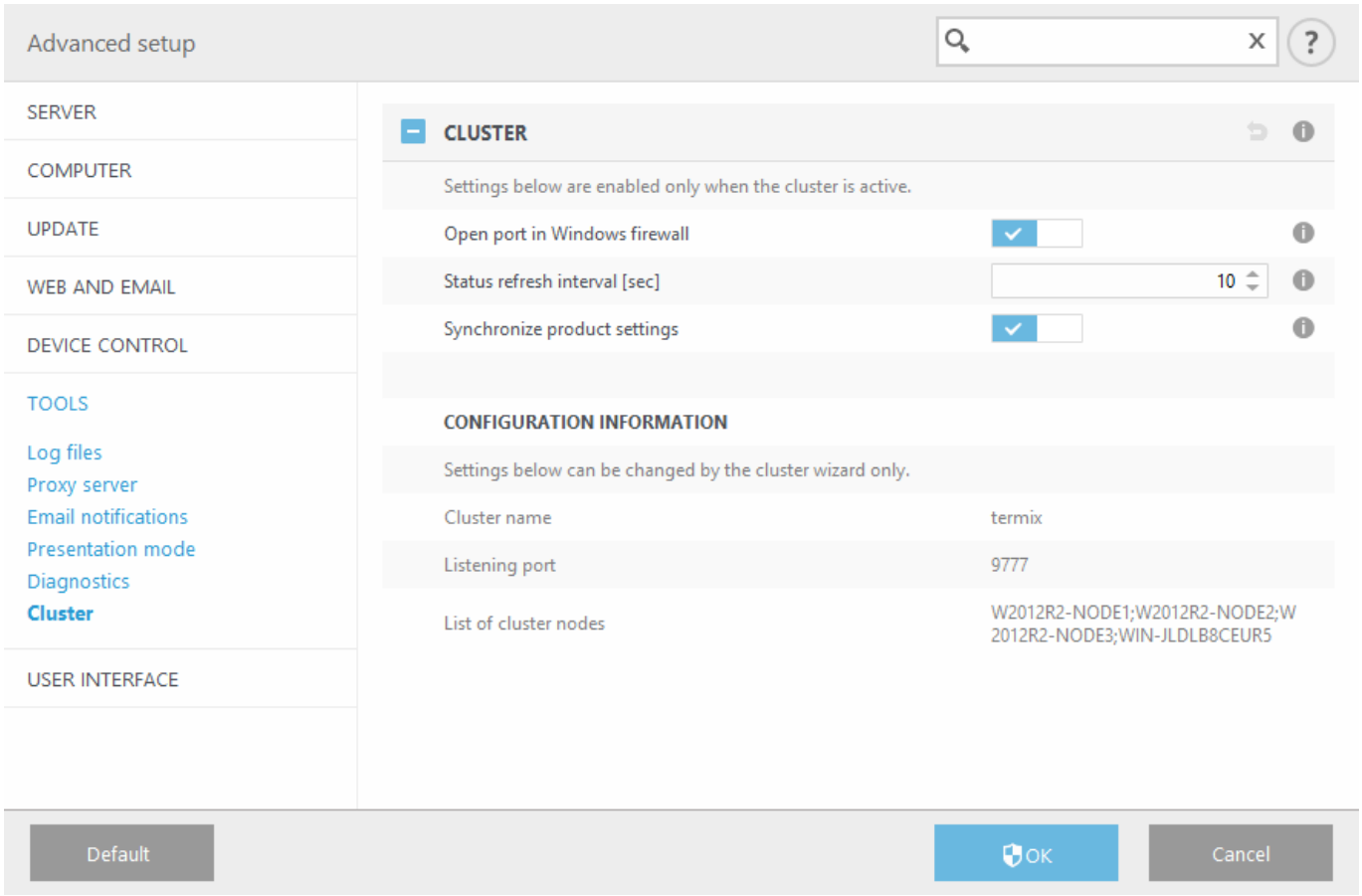
Cluster

Cluster je povolen automaticky, pokud je nakonfigurován ESET Cluster. Kliknutím na ikonu přepínače (např. pokud potřebujete změnit konfiguraci bez ovlivnění ostatních uzlů v clusteru ESET) jej můžete ručně vypnout v okně **Rozšířené nastavení** (F5). Tento přepínač pouze povoluje nebo zakazuje funkci ESET Cluster. Chcete-li nastavit nebo zničit cluster, použijte Průvodce clusterem nebo **Zničit cluster** umístěný v části Nástroje > sekce Cluster v hlavním okně programu.

ESET Cluster není konfigurován a zakázán:



ESET Cluster správně nakonfiguroval své detaily a možnosti:



Uživatelské rozhraní

V sekci Uživatelské rozhraní můžete konfigurovat uživatelské rozhraní (GUI) produktu ESET Server Security. Nejen vzhled rozhraní, ale také množství použitých efektů.

Prvky uživatelského rozhraní

V rozbalovacím menu Režim spuštění jsou k dispozici následující režimy:
• **Úplný** – zobrazí se úplné grafické rozhraní.
• **Terminál** – uživateli se nezobrazí žádné oznámení ani upozornění. Grafické rozhraní může spustit pouze administrátor. Tento režim můžete použít v případě, kdy grafické rozhraní zpomaluj běh počítače nebo způsobuje jiné problémy. Doporučujeme ho aktivovat také na terminálových serverech. Pro více informací o instalaci ESET Server Security na terminálovém serveru přejděte do kapitoly Vypnutí grafického rozhraní na terminálovém serveru

Zobrazit úvodní obrázek při startu
Tuto možnost vypněte, pokud nechcete zobrazovat úvodní obrázek při startu ESET Server Security, například při přihlášení uživatele.

Používat zvuková upozornění
ESET Server Security při důležitých událostech přehrává zvuky, například při výskytu hrozby nebo dokončení kontroly.

Integrovat do kontextového menu
Pokud je tato možnost aktivní, ovládací prvky produktu ESET Server Security se integrují do kontextového menu. Kontextové menu se zobrazuje po kliknutí pravým tlačítkem myši na daný objekt. V tomto menu jsou následně dostupné akce, které je možné na daném objektu provést.

Stavy aplikace
Po kliknutí na Změnit můžete zapnout nebo vypnout zobrazování stavů aplikace v hlavním okně na záložce Přehled Případně můžete pomocí politik v ESET PROTECT konfigurovat stavy aplikace. Mezi sledované stavy aplikace patří také, zda je produkt aktivní, a zda nevypršela platnost licence.

Informace o licenci / Zobrazit informace o licenci
Pokud je tato možnost aktivní, uživateli se zobrazí zprávy a oznámení související s licencí.

Upozornění a informační okna

V této části upravíte způsob upozorňování na detekci hrozeb a systémových oznámení. Tato oznámení si můžete nastavit dle svých potřeb. Pokud se rozhodnete nezobrazovat určitá varování, jejich seznam naleznete v části Vypnout zprávy a stavy. Zde můžete kontrolovat jejich stav, zobrazit více informací nebo znovu povolit jejich zobrazování.

Přístup k nastavení

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu můžete nastavení produktu ochránit heslem.

ESET Shell

Přístupová práva k nastavením produktu, funkcím a datům přes eShell můžete konfigurovat změnou zásad provádění ESET Shell.

Ikona v oznamovací oblasti Windows

Obnovit všechna nastavení v této sekci

Upozornění a informační okna

V této sekci můžete konfigurovat výstražná a informační hlášení produktu ESET Server Security, například zobrazování informace o úspěšné aktualizaci. Nastavit můžete **dobu zobrazení** a **průhlednost** v oznamovací oblasti Windows (pouze u systémů, které zobrazování oznámení podporují).

Zobrazit interaktivní upozornění

Vypnutím této možnosti zakážete produktu ESET Server Security zobrazování oznámení v oznamovací oblasti

Windows.

Seznam interaktivních upozornění

Tuto možnost využijte pro automatizaci. Pokud nechcete zobrazit upozornění a čekat na interakci uživatele, v rámci automatizace deaktivujte možnost **Dotázat se uživatele** a vyberte požadovanou akci, kterou má produkt provést.

Informační okna jsou určena pro zobrazení krátkých zpráv nebo výzev uživateli.

Zavírat informační okna automaticky

Oznámení se zavírají automaticky po uplynutí definovaného intervalu. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

Potvrzovací zprávy

Kliknutím na **Změnit** si zobrazíte dialogové okno se seznamem akcí ESET Server Security, jejichž provedení bude nutné potvrdit. Pomocí zaškrtávacích polí se rozhodněte, na které akce se vás má produkt dotázat.

Přístup k nastavení

Pro zajištění maximálního zabezpečení systému je důležité, aby byl program ESET Server Security správně nastaven. Jakékoli neodborné úpravy mohou mít za následek problémy nebo dokonce ztrátu důležitých dat. Chcete-li se vyhnout neodborným úpravám, můžete mít konfiguraci ESET Server Security chráněnou heslem.

Pokud v ESET Server Security aktivujete ochranu heslem, bude vyžadováno také při pokusu o odinstalování produktu. Bez zadání hesla nebude schopni ESET Server Security standardní cestou odinstalovat.

Chránit nastavení heslem

Zamkne/odemkne nastavení programu. Po kliknutí se zobrazí dialogové okno **Nastavit heslo**.

Nastavit heslo

Pro nastavení nebo změnu klikněte na **Nastavit**. Zadáním nového hesla ochráníte nastavení produktu ESET Server Security a zabráníte neoprávněným změnám v konfiguraci. Při změně stávajícího hesla je nutné jej zadat do pole **Původní heslo**, a následně nové heslo zadat dvakrát do polí **Nové heslo** a **Potvrzení hesla**. Změnu následně potvrdíte kliknutím na tlačítko **OK**. Nastavené heslo bude následně vyžadováno při každé změně nastavení produktu ESET Server Security.

Vyžadovat oprávnění administrátora také pro uživatele s omezeným oprávněním

Pokud přihlášený uživatel nemá administrátorská práva, pak při pokusu o změnu některých nastavení bude po vybrání této možnosti vyžadováno přihlášení administrátora. Taková změna zahrnuje vypnutí modulů ochrany.

V případě, že změníte heslo, a budete chtít prostřednictvím ESET CMD importovat konfiguraci z .xml souboru podepsaného původním heslem, podepište jej nejprve aktuálním heslem. Takto můžete použít konfigurační soubor, který jste si v minulosti exportovali, bez toho, aniž byste museli znovu exportovat konfiguraci produktu ESET Server Security.

ESET Shell

Přístupová práva k nastavením produktu, funkcím a datům přes eShell můžete konfigurovat **změnou zásad provádění ESET Shell**. Výchozí nastavení je **Omezené skriptování**, ale v případě potřeby jej můžete změnit na Zakázáno, Pouze pro čtení nebo Úplný přístup.

Zakázáno

eShell nelze použít pro konfiguraci bezpečnostního produktu ESET. Nastavení konfigurace eShell samotného je povoleno v kontextu ui eshell. Vzhled eShell můžete přizpůsobit, ale nemůžete přistupovat k nastavení produktu či datům.

Pouze pro čtení

eShell můžete v tomto režimu použít jako monitorovací nástroj. V interaktivním i dávkovém režimu máte přístup k nastavení, funkcím a datům, ale nemůžete je měnit.

Omezené skriptování

V interaktivním režimu si můžete zobrazit a měnit všechna nastavení, funkce a data. V dávkovém režimu eShell můžete pouze data číst – nastavení ani žádná data nezměníte. Nicméně pokud použijete podepsané dávkové soubory, můžete nastavení a data měnit.

Úplný přístup

Přístup do všech nastavení je neomezený v interaktivním a dávkovém režimu (při spuštění dávek). V interaktivním režimu si můžete zobrazit a měnit všechna nastavení, funkce a data. Pro aktivaci úplného přístupu eShell je vyžadováno oprávnění administrátora. Pokud je aktivní UAC, je vyžadována elevace oprávnění.

Deaktivace grafického rozhraní na terminálovém serveru

V této kapitole popisujeme, jak deaktivovat grafické rozhraní (GUI) programu ESET Server Security pro uživatele přihlášené na terminálovém serveru.

Za normálních okolností se grafické rozhraní (GUI) ESET Server Security spustí při každém přihlášení uživatele na terminálový server. This is usually undesirable on Terminal Servers. Pokud chcete vypnout GUI pro terminálové relace, můžete tak provést prostřednictvím eShell pomocí příkazu `set ui ui gui-start-mode none`. To přepne grafické rozhraní do módu terminálu. Zde jsou nabídnuty dva režimy grafického rozhraní:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Pro zobrazení aktuálně používaného režimu použijte příkaz `get ui ui gui-start-mode`.

> Pokud máte ESET Server Security nainstalován na Citrix serveru, doporučujeme použít nastavení popsaná v naší Databázi znalostí.

Vypnout zprávy a stavy

Potvrzovací zprávy

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

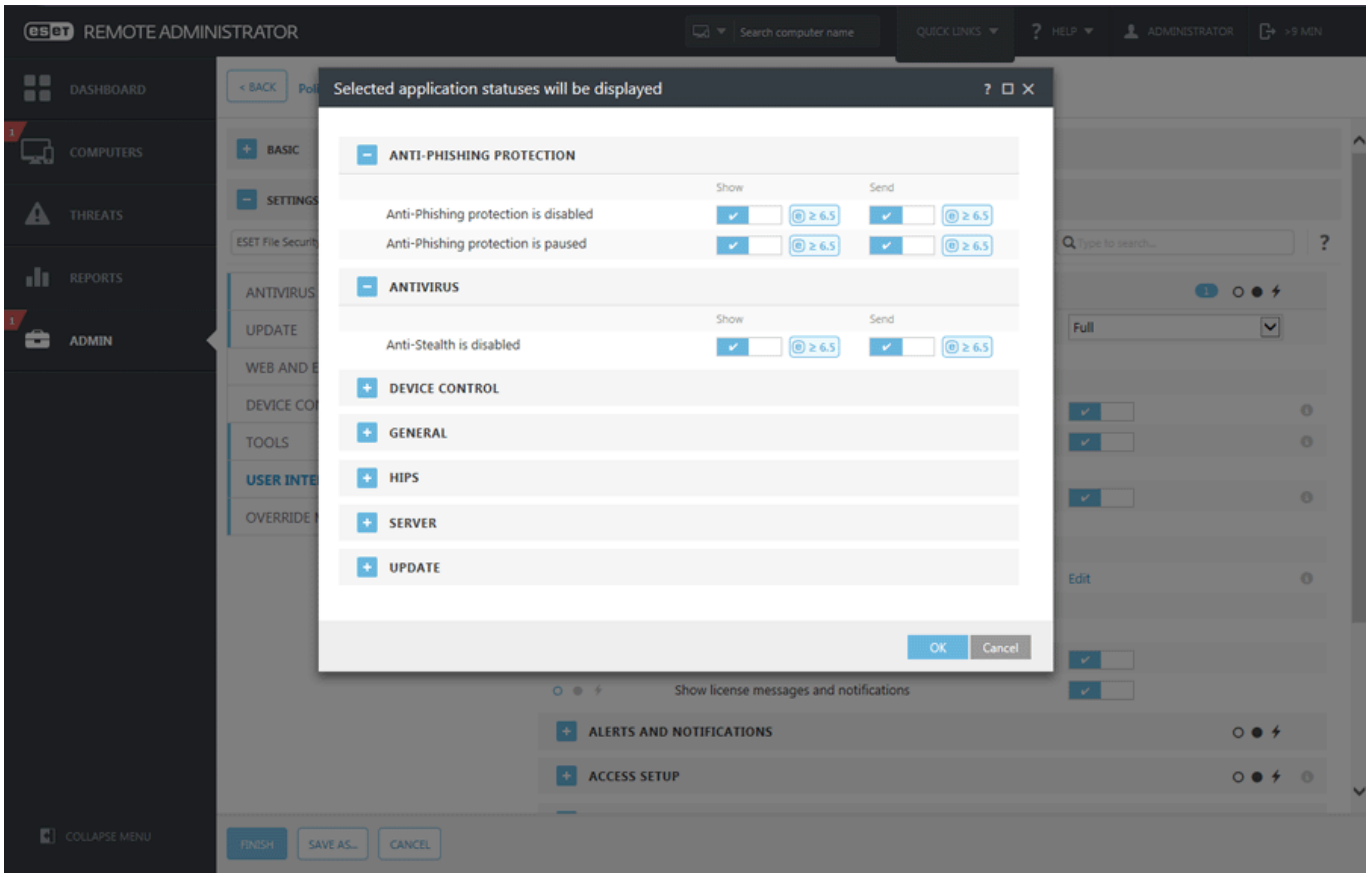
Nastavení stavů aplikace

Pomocí této možnosti můžete zapnout nebo vypnout zobrazování stavů aplikace v sekci Přehled.

Nastavení stavů aplikace

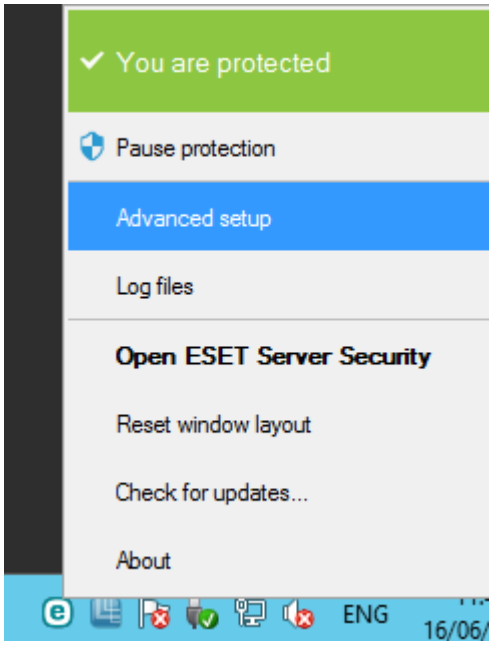
V tomto dialogovém okně můžete aktivovat nebo deaktivovat upozornění na konkrétní stavy aplikace, které se mají zobrazovat v hlavním okně programu v sekci Přehled. Například můžete deaktivovat upozornění pro pozastavenou antivirovou a antispywarovou ochranu nebo zapnutý Prezentační režim. Mezi sledované stavy aplikace patří také, zda je produkt aktivní, a zda nevypršela platnost licence.

Stavy aplikace můžete spravovat pomocí politik v ESET PROTECT. V takovém případě máte v konfigurační šabloně u každé položky možnost **Zobrazit uživateli** a **Odeslat do konzole**. Pokud necháte aktivní pouze možnost Odeslat do konzole, informace se zobrazí výhradně administrátorovi v konzoli pro vzdálenou správu ESET PROTECT. ESET Server Security zobrazí nastavení pomocí ikony zámku. Pro lokální zobrazení uvedené hlášky byste museli použít režim dočasné změny nastavení.



Ikona v oznamovací oblasti Windows

Slouží jako rychlý přístup k často používaným položkám a funkcím služby ESET Server Security. To je k dispozici po kliknutí pravým tlačítkem na ikonu v oznamovací oblasti Windows.



Více informací

Otevře Přehled pro zobrazení aktuálního stavu ochrany a zpráv.

Dočasně vypnout ochranu

Dočasně vypnout ochranu – zobrazí potvrzovací dialogové okno, pomocí kterého vypnete Antivirovou a antispywarovou ochranu, která chrání systém proti škodlivým útokům tím, že kontroluje soubory, e-maily a komunikaci prostřednictvím internetu. Pokud dočasně pozastavíte Antivirovou a antispywarovou ochranu prostřednictvím ikony v oznamovací oblasti Windows, zobrazí se oznámení o **Pozastavení ochrany**. Vypnete tím ochranu před škodlivým kódem po navolenou dobu. Pro trvalé vypnutí ochrany přejděte do sekce **Rozšířená nastavení** (po stisku klávesy F5). Při deaktivaci ochrany buďte opatrní. Váš systém bude vystaven hrozbám.

Rozšířená nastavení

Po kliknutí se zobrazí **Rozšířené nastavení** programu.

Protokoly

Protokoly zachycují všechny podstatné události programu a nabízejí přehled detekovaných hrozeb.

Skrýt ESET Server Security

Kliknutím skryjete všechna okna ESET Server Security.

Obnovit rozmístění oken

Kliknutím obnovíte přednastavenou velikost a pozici okna ESET Server Security na obrazovce

Zkontrolovat aktualizace

Kliknutím spustíte kontrolu dostupnosti nového verze detekčního jádra pro zajištění maximální ochrany před škodlivým kódem.

O programu

Poskytuje informace o systému, instalovaném programu ESET Server Security a všech jeho programovaných modulech. Také zde naleznete datum platnosti licence. Ve spodní části okna se nachází informace o operačním systému a systémových prostředcích.

Obnovit na standardní nastavení

Výchozí hodnoty obnovíte nastavením v **Rozšířeném nastavení**. Na výběr máte ze dvou možností: Můžete vrátit vše do výchozího nastavení nebo vrátit nastavení pouze pro určitou sekci (nastavení v ostatních sekcích zůstane nezměněno).

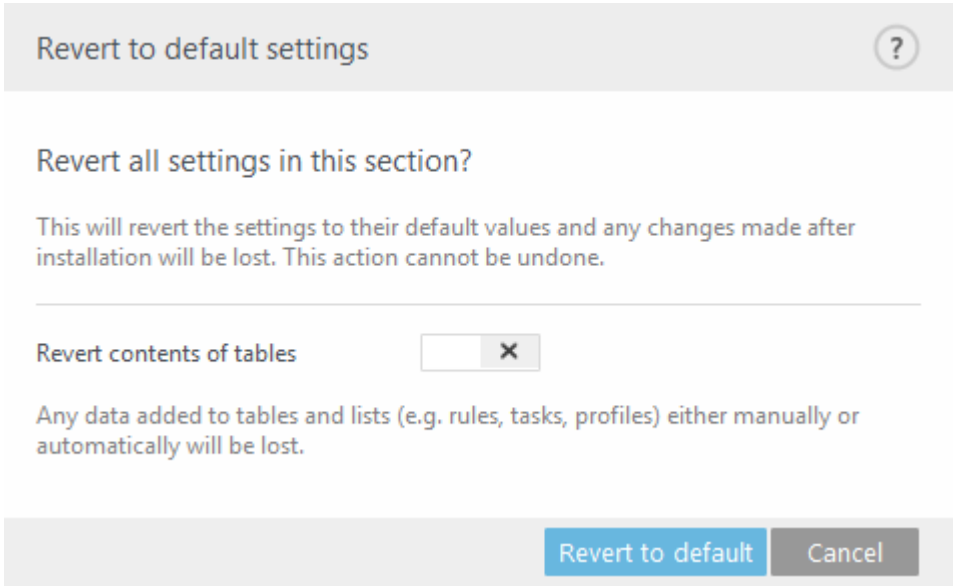
Obnovit všechna nastavení

Veškerá nastavení programu se vrátí do stavu, v jakém byla po instalaci ESET Server Security. Představit si to můžete jako Obnovení do továrního nastavení.

> Mějte na paměti, že po kliknutí na tlačítko **Obnovit na standardní** budou všechna dosavadní nastavení ztracena Tuto akci nelze vrátit zpět.

Obnovit všechna nastavení v této sekci

Obnoví nastavení modulů v dané sekci na výchozí hodnoty. Všechny změny provedené v této sekci budou ztraceny.



Obnovit obsah tabulek

Vybráním této možnosti se odstraní všechna ručně i automaticky přidaná pravidla, úlohy i profily.

Nápověda a podpora

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

Nainstalovaný produkt

Informace o produktu a licenci

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

Nápověda programu

Kliknutím na odkaz zobrazíte online nápovědu programu ESET Server Security.

Databáze znalostí

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

Technická podpora

- Pro vytvoření rozšířených protokolů s informacemi, které pomohou vývojářům s diagnostikou problému, klikněte na možnost Rozšířené protokolování.
- Požádat o podporu – v případě, že nenaleznete řešení problému, můžete kontaktovat přímo specialisty technické podpory.
- Základní informace pro technickou podporu – po kliknutí se zobrazí informace důležité pro technickou podporu jako název produktu, verze, informace o licenci, atp.
- ESET Log Collector – ESET Log Collector je aplikace, která automaticky sesbírá protokoly a informace o systému. Protokoly pomáhají specialistům technické podpory s diagnostikou problému a urychlí přípravu jeho řešení.

Založit požadavek na technickou podporu

Aby mohli specialisté technické podpory rychle a relevantně reagovat na dotazy zákazníků, vyžadují zaslání konfigurace ESET Server Security, detailních informací o systému včetně spuštěných procesů a záznamů v registru – tedy protokolu z nástroje ESET SysInspector. Společnost ESET tato data využívá výhradně při řešení technických problémů s produkty ESET. Možnosti odesílání dat naleznete v **Rozšířeném nastavení** (**F5** v sekci **Nástroje** > **Diagnostika** > **Technická podpora**.

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

Po vyplnění a odeslání webového formuláře se tyto informace automaticky odešlou. Pokud nechcete aby se vás program dotazoval při každém kontaktování technické podpory, vyberte možnost **Vždy odesílat tato data**.

Neodesílat data

Tuto možnost vyberte, pokud nechcete odesílat žádná data. Následně budete přesměrování na webovou stránku technické podpory.

O programu ESET Server Security

V tomto okně naleznete informace o programu ESET Server Security. V horní části se zobrazují informace o operačním systému, systémových prostředcích, aktuálně přihlášeném uživateli, názvu počítače a názvu relace na licenčním portále.

Nainstalované komponenty

Po kliknutí si zobrazíte detailní informace o programových modulech. Informace o modulech můžete zkopírovat do schránky kliknutím na tlačítko **Kopírovat**. To může být užitečné při řešení problému a kontaktování technické podpory společnosti ESET.

Slovník pojmů

Vysvětlení technických pojmů z oblasti počítačových hrozeb a internetové bezpečnosti naleznete v online Slovníku pojmů.

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel”) Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako

i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn

používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro následující funkce Softwaru:

a) **Aktualizace Software**. Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace“), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti“, které jsou k dispozici na webu https://go.eset.com/eol. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

b) **Zasílání infiltrací a informací Poskytovateli.** Software obsahuje funkce, které slouží ke shromažďování vzorků počítačových virů a jiných škodlivých počítačových programů a podezřelých, problematických nebo potenciálně nežádoucích nebo nebezpečných objektů, jako jsou soubory, adresy URL, IP pakety a ethernetové rámce (dále jen "Infiltrace") a jejich následnému odeslání Poskytovateli, mimo jiné včetně informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, a informací o operacích a funkcích Softwaru ("Informace"). Informace a Infiltrace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) o Koncovém uživateli a/nebo jiných uživatelích počítače, na kterém je Software nainstalován, a soubory postižené Infiltracemi, včetně přidružených metadat.

Informace a Infiltrace mohou být shromažďovány následujícími funkcemi Softwaru:

i. Funkce Reputační systém LiveGrid zahrnuje shromažďování a odesílání jednosměrných hodnot hash, které

souvisejí s Infiltracemi, Poskytovateli. Tato funkce je povolena v rámci standardního nastavení Softwaru.

ii. Funkce Systém zpětné vazby LiveGrid zahrnuje shromažďování a odesílání Infiltrací s příslušnými metadaty a Informacemi Poskytovateli. Tuto funkci aktivuje Koncový uživatel během procesu instalace Softwaru.

Poskytovatel bude obdržené Informace a Infiltrace používat pouze pro účely analýzy a zkoumání Infiltrací, zlepšování ověřování pravosti Softwaru a Licence a přijme veškerá vhodná opatření, aby zajistil, že obdržené Infiltrace a Informace zůstanou v bezpečí. Po aktivaci této funkce Softwaru mohou být Infiltrace a Informace shromažďovány a zpracovávány Poskytovatelem, jak je uvedeno v Zásadách ochrany osobních údajů a v příslušných právních předpisech. Tyto funkce můžete kdykoliv deaktivovat.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb

jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí

kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že

by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní

stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

EULAID: EULA-PRODUCT-LG; 3537.0

Zásady ochrany osobních údajů

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvlášť důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v dokumentu Licenční ujednání s koncovým uživatelem, ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané v Licenčním ujednání s koncovým uživatelem („EULA“) a v produktové dokumentaci. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Aktualizace a další statistiky zahrnující informace o procesu instalace a vašem počítači, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako je operační systém, údaje o hardwaru, ID instalace, ID licencí, IP adresa, MAC adresa a nastavení konfigurace produktu.
- Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jako součást reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu.
- Podezřelé vzorky a metadata jako součást systému zpětné vazby ESET LiveGrid®, který umožňuje

společnosti ESET okamžitě reagovat na potřeby našich koncových uživatelů a udržet akceschopnost tváří v tvář nejnovějším hrozbám. Jsme závislí na tom, že nám zasíláte:

- infiltrace, jako jsou potenciální vzorky virů a jiných škodlivých programů, a podezřelé; problematické, potenciálně nežádoucí nebo nebezpečné objekty, jako jsou spustitelné soubory nebo e-mailové zprávy, které jsou nahlášeny koncovým uživatelem jako nevyžádané nebo označené naším produktem; údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- údaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
- Nemáme v úmyslu, aby byly součástí našich systémů nebo aby byly zpracovány pro účely uvedené v těchto Zásadách ochrany osobních údajů.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. Kontaktní informace a údaje obsažené ve vašich požadavcích na podporu mohou být vyžadovány za účelem poskytování podpory. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory.

- Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb.
- Za účelem poskytování podpory mohou být vyžadovány kontaktní informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodejní, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a – pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem

identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úrad na ochranu osobných údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Kontaktní informace

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk