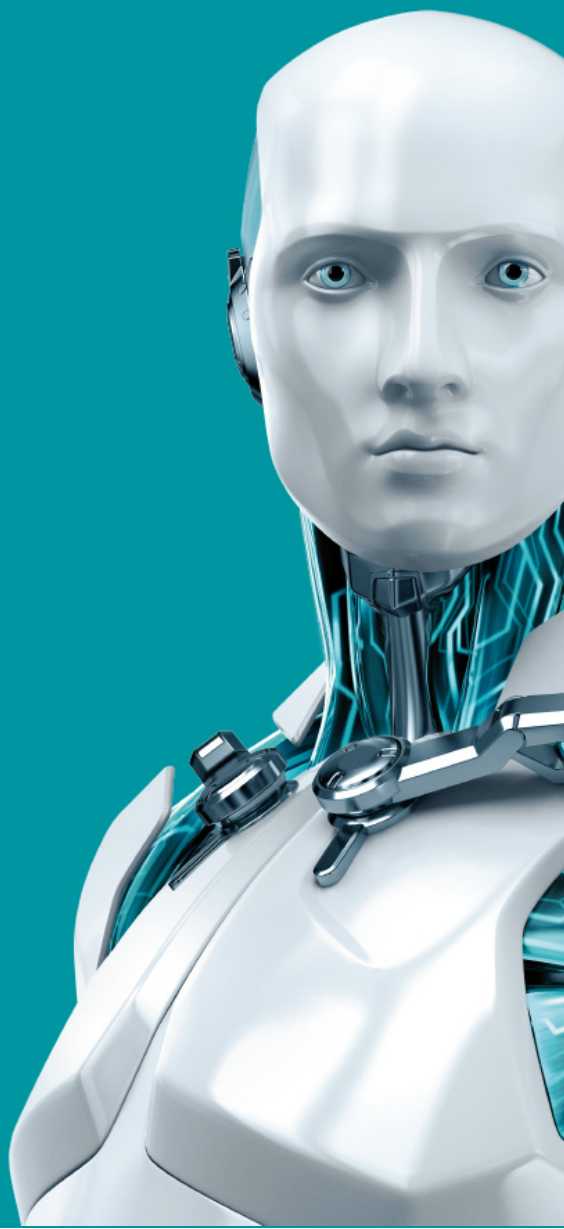
NOD32® ANTIVIRUS

UŽIVATELSKÁ PŘÍRUČKA

(platná pro produkty ve verzi 12.0 a vyšší)

Microsoft® Windows® 10 / 8.1 / 8 / 7 / Vista / Home Server 2011

Klikněte sem pro zobrazení online verze příručky



ENJOY SAFER TECHNOLOGY™

Copyright © 2018 ESET, spol. s r. o.
ESET NOD32 Antivirus byl vyvinut společností ESET, spol. s r. o.
Pro více informací navštivte 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: www.eset.cz/podpora

REV. 10.9.2018

Obsah

1. ESET NOD32 Antivirus.....5
1.1 Co je nového?.....6
1.2 Jaký produkt si mám vybrat?.....7
1.3 Systémové požadavky.....8
1.4 Prevence.....8
2. Instalace.....10
2.1 Live installer.....10
2.2 Offline instalace.....11
2.2.1 Zadání licenčního klíče.....11
2.2.2 Použití správce licencí.....12
2.2.3 Změna instalační složky.....13
2.3 Známé problémy při instalaci.....13
2.4 Aktivace produktu.....13
2.5 Zadání licenčního klíče.....14
2.6 Doporučení produktu ESET přátelům.....15
2.7 Aktualizace na novou verzi.....15
2.8 Kontrola počítače po dokončení instalace.....16
3. Začínáme.....17
3.1 Seznámení s uživatelským prostředím.....17
3.2 Aktualizace.....19
4. Práce s ESET NOD32 Antivirus.....21
4.1 Ochrana počítače.....22
4.1.1 Detekční jádro.....23
4.1.1.1 Rezidentní ochrana souborového systému.....24
4.1.1.1.1 Rozšířená nastavení kontroly.....25
4.1.1.1.2 Úrovně léčení.....25
4.1.1.1.3 Kdy měnit nastavení rezidentní ochrany.....26
4.1.1.1.4 Ověření funkčnosti rezidentní ochrany.....26
4.1.1.1.5 Co dělat, když nefunguje rezidentní ochrana.....26
4.1.1.2 Volitelná kontrola počítače.....26
4.1.1.2.1 Spuštění volitelné kontroly.....28
4.1.1.2.2 Průběh kontroly.....29
4.1.1.2.3 Profily kontroly.....30
4.1.1.2.4 Protokol kontroly.....30
4.1.1.3 Kontrola po startu.....30
4.1.1.3.1 Kontrola souborů spouštěných při startu počítače.....30
4.1.1.4 Kontrola při nečinnosti.....31
4.1.1.5 Výjimky.....31
4.1.1.6 Parametry skenovacího jádra ThreatSense.....32
4.1.1.6.1 Léčení.....35
4.1.1.6.2 Výjimky.....35
4.1.1.7 Nalezena hrozba.....35
4.1.1.8 Ochrana dokumentů.....37
4.1.2 Výměnná média.....38
4.1.3 Správa zařízení.....38
4.1.3.1 Pravidla správy zařízení.....39
4.1.3.2 Vytvoření nového pravidla.....40
4.1.4 HIPS.....41
4.1.4.1 Rozšířená nastavení.....44
4.1.4.2 Interaktivní režim HIPS.....44
4.1.4.3 Detekován potenciální ransomware.....45
4.1.5 Herní režim.....45
4.2 Internetová ochrana.....46
4.2.1 Ochrana přístupu na web.....47
4.2.1.1 Obecné.....47
4.2.1.2 HTTP, HTTPs.....48
4.2.1.3 Správa URL adres.....48
4.2.2 Ochrana poštovních klientů.....49
4.2.2.1 Poštovní klienti.....49
4.2.2.2 Poštovní protokoly.....50
4.2.2.3 Upozornění a události.....51
4.2.2.4 Integrace s poštovními klienty.....52
4.2.2.4.1 Nastavení ochrany poštovních klientů.....52
4.2.2.5 Kontrola protokolu POP3, POP3s.....52
4.2.3 Filtrování protokolů.....53
4.2.3.1 Weboví a poštovní klienti.....53
4.2.3.2 Vyloučené aplikace.....54
4.2.3.3 Vyloučené IP adresy.....55
4.2.3.3.1 Přidání adresy IPv4.....55
4.2.3.3.2 Přidání IPv6 adresy.....55
4.2.3.4 Kontrola protokolu SSL/TLS.....56
4.2.3.4.1 Certifikáty.....57
4.2.3.4.2 Seznam známých certifikátů.....57
4.2.3.4.3 Kontrolovat šifrovanou komunikaci těchto aplikací.....58
4.2.4 Anti-Phishingová ochrana.....58
4.3 Aktualizace programu.....59
4.3.1 Nastavení aktualizace.....62
4.3.1.1 Profily aktualizace.....64
4.3.1.2 Pokročilá nastavení aktualizace.....64
4.3.1.2.1 Režim aktualizace.....64
4.3.1.2.2 Možnosti připojení.....64
4.3.2 Vrátit předchozí aktualizace.....65
4.3.3 Jak vytvořit aktualizační úlohu.....66
4.4 Nástroje.....67
4.4.1 Nástroje produktu ESET NOD32 Antivirus.....67
4.4.1.1 Protokoly.....68
4.4.1.1.1 Protokoly.....69
4.4.1.2 Spuštěné procesy.....70
4.4.1.3 Bezpečnostní přehled.....71
4.4.1.4 Sledování aktivity.....72
4.4.1.5 ESET SysInspector.....73
4.4.1.6 Plánovač.....73
4.4.1.7 Kontrola systému.....75
4.4.1.8 ESET SysRescue.....76
4.4.1.9 Cloudová ochrana.....76
4.4.1.9.1 Podezřelé soubory.....77
4.4.1.10 Karanténa.....78
4.4.1.11 Proxy server.....79

4.4.1.12 Upozornění e-mailem ... 80
4.4.1.12.1 Formát zprávy ... 81
4.4.1.13 Odesílání souborů analýze ... 82
4.4.1.14 Aktualizace operačního systému Windows ... 82
4.4.1.15 ESET CMD ... 83

4.5 Uživatelské rozhraní ... 84
4.5.1 Prvky uživatelského rozhraní ... 84
4.5.2 Upozornění a události ... 85
4.5.2.1 Rozšířená nastavení ... 86
4.5.3 Přístup k nastavení ... 87
4.5.4 Ikona v oznamovací oblasti ... 88

5. Pokročilý uživatel ... 89

5.1 Profily ... 89
5.2 Klávesové zkratky ... 89
5.3 Diagnostika ... 90
5.4 Import a export nastavení ... 90
5.5 ESET SysInspector ... 91
5.5.1 Úvod do programu ESET SysInspector ... 91
5.5.1.1 Spuštění programu ESET SysInspector ... 91
5.5.2 Uživatelské rozhraní a používání aplikace ... 92
5.5.2.1 Ovládací prvky programu ... 92
5.5.2.2 Navigace v programu ESET SysInspector ... 93
5.5.2.2.1 Klávesové zkratky ... 95
5.5.2.3 Porovnávání ... 96
5.5.3 Ovládaní přes příkazový řádek ... 97
5.5.4 Servisní skript ... 97
5.5.4.1 Generování servisního skriptu ... 98
5.5.4.2 Struktura servisního skriptu ... 98
5.5.4.3 Spouštění servisních skriptů ... 101
5.5.5 Často kladené otázky ... 102
5.5.6 ESET SysInspector jako součást ESET NOD32 Antivirus ... 103

5.6 Příkazový řádek ... 103

6. Řešení nejčastějších problémů ... 106

6.1 Jak aktualizovat ESET NOD32 Antivirus? ... 106
6.2 Jak odstranit vir z počítače? ... 106
6.3 Jak vytvořit novou úlohu v Plánovači? ... 107
6.4 Jak naplánovat kontrolu počítače (kontrola každých 24 hodin)? ... 107
6.5 Jak obnovit přístup do rozšířeného nastavení? ... 108

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ThreatSense® přináší vyšší rychlost a přesnější detekci.Výsledkem je inteligentní systém, který neustále kontroluje veškeré dění na počítači na přítomnost škodlivého kódu.

ESET NOD32 Antivirus je komplexní bezpečnostní řešení, které kombinuje maximální ochranu s minimálním dopadem na operační systém. Pokročilé technologie založené na umělé inteligenci jsou schopny proaktivně eliminovat viry, spyware, trojské koně, červy, adware, rootkity a další internetové hrozby, bez dopadu na výkon počítače nebo funkčnost operačního systému.

Funkce a přednosti

Přepracované uživatelské rozhraní	Grafické rozhraní ESET NOD32 Antivirus bylo kompletně přepracováno. Nyní je čistější, přehlednější a intuitivnější. Nově jsme přidali také podporu pro jazyky se zápisem zprava doleva jako je Hebrejština a Arabština. Prostřednictvím online nápovědy získáte vždy nejrelevantnější informace k aktuálně zobrazenému dialogovému oknu a nápověda vám pomůže vyřešit váš problém.
Antivirus a antispyware	Proaktivně detekuje a léčí známé i neznámé viry, červy, trojské koně a rootkity. **Pokročilá heuristika** označí každý dosud neznámý malware, chrání vás před neznámými hrozbami a eliminuje je dříve, než mohou způsobit škodu. **Ochrana přístupu na web** a modul **Anti-Phishing** monitoruje komunikaci mezi internetovým prohlížečem a vzdálenými servery (včetně SSL). **Ochrana poštovních klientů** zajišťuje kontrolu komunikace pomocí POP3(S) a IMAP(S) protokolů.
Pravidelné aktualizace	Pravidelné aktualizace detekčních a programových modulů zajistí maximální ochranu počítače.
ESET LiveGrid®	Můžete zkontrolovat reputaci běžících procesů a souborů přímo v ESET NOD32 Antivirus vůči cloudové databázi.
Kontrola výměnných médií	Automaticky kontroluje všechny USB disky, paměťové karty a CD/DVD. Blokuje výměnná média podle typu, výrobce, velikosti a dalších atributů.
HIPS	Pomocí tohoto modulu si můžete přizpůsobit detailní chování systému pomocí pravidel pro systémový registr, aktivní procesy a programy.
Herní režim	Při hraní her a používání aplikací běžících v režimu celé obrazovky (fullscreen) se nezobrazí upozornění ani vyskakovací okna a program tak uvolní systémové prostředky pro náročné aplikace.

Funkce

Ochrana bankovnictví a online plateb	Dodatečná ochranná vrstva do internetového prohlížeče. Tato vrstva se stará o to, aby vaše osobní data (čísla bankovních účtů, kreditních karet atp.) nebyla v průběhu online transakcí zneužita, resp. nemohly je získat jiné aplikace.
Podpora síťových vzorků	Jedná se o doplněk do ochrany proti botnetu, díky kterému dokážeme rychleji identifikovat a blokovat škodlivou komunikaci pocházející z napadených počítačů nebo na ně směřující.
Inteligentní firewall	Modul firewall kontroluje síťovou komunikaci a chrání počítač před neautorizovaným přístupem.
ESET Antispam	Antispamový modul dokáže filtrovat nevyžádanou poštu (spam), která dnes představuje více než 80 % veškeré e-mailové komunikace.

ESET Anti-Theft	ESET Anti-Theft zvyšuje bezpečnost dat uživatele ve chvíli ztráty nebo odcizení počítače. Po aktivaci této technologie bude monitorována podezřelá aktivita na zařízení. Prostřednictvím webového rozhraní můžete zařízení vzdáleně ovládat a v případě jeho ztráty jej označit jako ztracené. Tím ochráníte data v něm uložená.
Rodičovská kontrola	Pomocí kategorií můžete omezit přístup na definované internetové stránky, například stránky s nevhodným obsahem.
Monitorování domácí sítě	Zobrazí zařízení připojená do vaší sítě a ověří zabezpečení vašeho routeru.
Ochrana webkamery	Monitoruje a blokuje přístup k webkameře, čímž zabrání pokusů o zneužití webkamery ke špionáži.

Pro správnou funkci všech bezpečnostních funkcí ESET NOD32 Antivirus musíte mít platnou licenci. Doporučujeme prodloužit si licenci ESET NOD32 Antivirus v dostatečném předstihu před jejím koncem platnosti.

1.1 Co je nového?

Nová verze programu ESET NOD32 Antivirus přináší tyto nové funkce a vylepšení:

- **Získání protokolů jedním kliknutím** – jedním kliknutím vytvoříte diagnostické protokoly.
- **Unified Extensible Firmware Interface (UEFI) skener** – další úroveň ochrany, která dokáže detekovat a odstranit škodlivý kód, který by se dokázal spustit ještě před startem samotného operačního systému. Pro více informací přejděte do slovníku pojmů.
- **Vyšší výkon, nižší dopad na systém** – nová verze využívá efektivněji systémové prostředky díky čemuž je kontrola souborů ještě rychlejší.
- **Přepracované rozšířené nastavení** – přejmenovali jsme některé části nastavení a přesunuli adekvátním způsobem nastavení ESET LiveGrid® atp.
- **Vylepšena podpora odečítačů odrazovek** – ESET NOD32 Antivirus podporuje nejrozšířenější odečítače obrazovek (JAWS, NVDA, Narrator).
- **Podpora drag and drop pro kontrolu souborů** – pro zkontrolování konkrétních souborů nebo složek je můžete pohodlně přesunout myší do definované části v hlavním okně programu.
- **Doporučení produktu ESET přátelům** – produkt ESET NOD32 Antivirus můžete doporučit členům vaší rodiny a přátelům a získat odměnu.
- ESET NOD32 Antivirus se nově instaluje s minimem modulů. Instalace je díky tomu rychlejší. Po nainstalování a aktivování produktu se stáhnou nejnovější verze ostatních modulů.
- ESET NOD32 Antivirus vás upozorní na možné bezpečnostní riziko, když se připojíte do nezabezpečené nebo slabě zabezpečené bezdrátové sítě.

Pro více informací o nových funkcích ESET NOD32 Antivirus si přečtěte následující článek v ESET Databázi znalostí:
Co je nového v nové verzi produktu ESET pro domácí uživatele?

1.2 Jaký produkt si mám vybrat?

Pro zabezpečení domácích počítačů nabízíme několik produktů. Záleží pouze na vašich požadavcích – zda hledáte výkonné antivirové řešení nebo požadujete komplexní řešení vybavené firewallem a dalšími bezpečnostními nástroji pro ochranu soukromých dat. Vybírat si můžete z následujících produktů:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

Pro zjištění, jaký produkt máte nainstalován, si otevřete hlavní okno programu, a podívejte se do levého horního rohu.

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Antivirus	✔	✔	✔
Antispyware	✔	✔	✔
Exploit Blocker	✔	✔	✔
Ochrana proti útokům prostřednictvím skriptů	✔	✔	✔
Anti-Phishing	✔	✔	✔
Ochrana přístupu na web	✔	✔	✔
HIPS (včetně ochrany proti ransomware)	✔	✔	✔
Antispam		✔	✔
Firewall		✔	✔
Monitorování domácí sítě		✔	✔
Ochrana webkamery		✔	✔
Ochrana proti síťovým útokům		✔	✔
Ochrana proti zapojení do botnetu		✔	✔
Ochrana bankovnictví a online plateb		✔	✔
Rodičovská kontrola		✔	✔
Anti-Theft		✔	✔
Správce hesel			✔
Šifrování dat			✔

1.3 Systémové požadavky

Pro plynulý běh ESET NOD32 Antivirus by váš systém měl splňovat následující požadavky:

Podporované procesory

Intel® a AMD x86-x64

Podporované operační systémy

Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7
Microsoft® Windows® Vista
Microsoft® Windows® Home Server 2011 64-bit

1.4 Prevence

Při používání počítače, zejména při práci s internetem, je potřeba mít neustále na paměti, že žádný antivirový systém nedokáže zcela odstranit riziko nákazy počítače a útoků. Pro zaručení maximální bezpečnosti a pohodlí je potřeba antivir správně používat a dodržovat několik užitečných pravidel:

Pravidelná aktualizace antivirového systému

Podle statistik z ESET LiveGrid® vznikají denně tisíce nových unikátních infiltrací, které se snaží obejít zabezpečení počítačů a přinést svým tvůrcům zisk. Viroví analytici společnosti ESET tyto hrozby denně analyzují a vydávají aktualizace, které zvyšují úroveň ochrany uživatelů antivirového systému. Při nesprávném nastavení aktualizace se účinnost antivirového systému dramaticky snižuje. Podrobnější informace, jak správně nastavit aktualizace produktu, naleznete v kapitole Nastavení aktualizace.

Stahování bezpečnostních záplat

Tvůrci infiltrací s oblibou využívají chyby v často používaných programech, aby zvýšili účinnost šíření škodlivých kódů. Výrobci většiny programů proto pravidelně vydávají bezpečnostní záplaty, které chyby v produktech opravují. Důležité je stáhnout tyto aktualizaci co nejdříve poté, co byly vydány. Mezi takové programy, které jsou aktualizovány pravidelně, můžeme zařadit například operační systém Windows nebo internetový prohlížeč Internet Explorer.

Zálohování důležitých dat

Tvůrci infiltrací většinou neberou ohled na potřeby uživatelů. Infiltrace tak mohou způsobit částečnou nebo úplnou nefunkčnost programů, operačního systému nebo poškození dat, někdy dokonce i záměrně. Pravidelné zálohování citlivých a důležitých dat například na DVD nebo externí disk může výrazně usnadnit a urychlit případnou obnovu po pádu systému.

Pravidelná kontrola počítače

Detekci známých i neznámých virů, červů, trojských koní a rootkitů zajišťuje rezidentní štít souborového systému. To znamená, že při každém přístupu k souboru, dojde k jeho kontrole. Přesto doporučujeme pravidelně spouštět úplnou kontrolu počítače alespoň jednou za měsíc, pro zajištění odstranění infiltrací, které pronikly jinými úrovněmi ochrany v době používání staršího detekčního jádra.

Dodržování základních bezpečnostních pravidel

Jedním z nejužitečnějších a nejúčinnějších bezpečnostních opatření je obezřetnost uživatele. V současnosti vyžaduje většina infiltrací přímé spuštění uživatelem. Proto opatrnost při otevírání souborů vás může ušetřit mnoha problémům a zabránit proniknutí škodlivého kódu do počítače. Zde jsou některé užitečné rady:

- Omezte návštěvy podezřelých stránek, které uživatele bombardují otevíráním oken s reklamními nabídkami apod.
- Dbejte zvýšené opatrnosti při stahování a instalaci volně šiřitelných programů, kodeků apod. Doporučujeme používat pouze ověřené programy a navštěvovat bezpečné internetové stránky.
- Dbejte zvýšené opatrnosti při otevírání příloh e-mailů zvláště u hromadně posílaných zpráv nebo u zpráv od neznámých odesílatelů.
- Nepoužívejte pro běžnou práci na počítači účet s oprávněním Administrátora.

2. Instalace

Instalaci ESET NOD32 Antivirus můžete provést dvěma způsoby.

- Live installer si můžete stáhnout z internetových stránek společnosti ESET. Live installer je univerzální pro všechny jazykové varianty (při instalaci vyberete jazykovou verzi). Po spuštění se automaticky stáhnou všechny potřebné soubory pro instalaci ESET NOD32 Antivirus.

- Offline instalace – tento typ instalace je běžný při instalaci z CD/DVD. Používá soubor *.exe*, který obsahuje všechny instalační soubory, proto je větší než Live installer. Připojení k internetu není potřebné pro dokončení instalace.

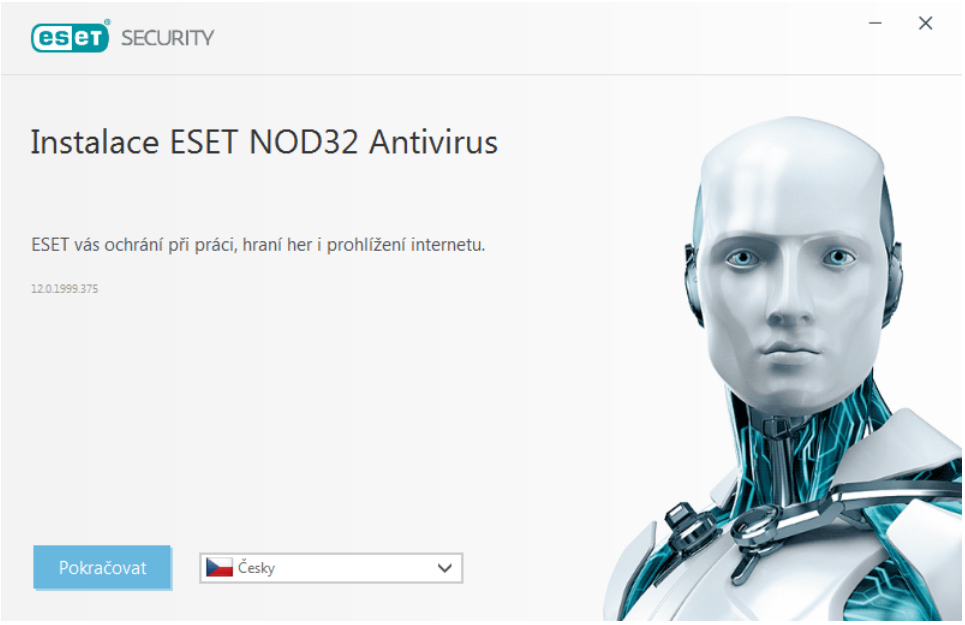
DŮLEŽITÉ:
Před spuštěním instalace ESET NOD32 Antivirus se ujistěte, že na počítači není nainstalován žádný jiný antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě, proto doporučujeme odinstalovat všechny ostatní antivirové programy. V ESET Databázi znalostí naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů.

2.1 Live installer

Po stažení instalačního balíčku *Live installeru*, dvojitým kliknutím pravým tlačítkem myši na stažený soubor spusťte instalaci a postupujte podle pokynů na obrazovce.

DŮLEŽITÉ:
Pro tento způsob instalace musíte být připojeni k internetu.

Důležité:



Z rozbalovacího menu vyberte požadovanou jazykovou verzi a klikněte na tlačítko **Pokračovat**. Následně vyčkejte na stažení potřebných souborů.

Poté, co odsouhlasíte licenční ujednání, budete vyzváni k nastavení technologie **ESET LiveGrid®** a **Detekci potenciálně nechtěných aplikací**. ESET LiveGrid® pomáhá bezprostředně informovat společnost ESET o nových hrozbách a tím chránit zákazníky. Tento systém funguje na principu odeslání podezřelých vzorků do virových laboratoří ESET, kde jsou analyzovány a využívány při sestavování aktualizací detekčního jádra.

Standardně je vybrána možnost **Chci se zapojit do systému včasného varování ESET LiveGrid® (doporučujeme)** a tato funkce bude po instalaci aktivována.

Dalším krokem je nastavení detekce potenciálně nechtěných aplikací. Potenciálně nechtěné aplikace nemusí být nutně škodlivé, ale mohou negativně ovlivnit chování operačního systému. Více informací naleznete v kapitole Potenciálně nechtěné aplikace.

Klikněte na tlačítko **Instalovat** pro spuštění instalačního procesu.

Poznámka:
Pokud máte licenci, která vás opravňuje k instalaci více produktů, nainstalujte si ten, který vyhovuje vašim potřebám. Pro více informací o jednotlivých produktech se podívejte do srovnávací tabulky.

2.2 Offline instalace

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

Z rozbalovacího menu vyberte jazyk, ve kterém chcete jazyk nainstalovat, a klikněte na tlačítko **Pokračovat**.

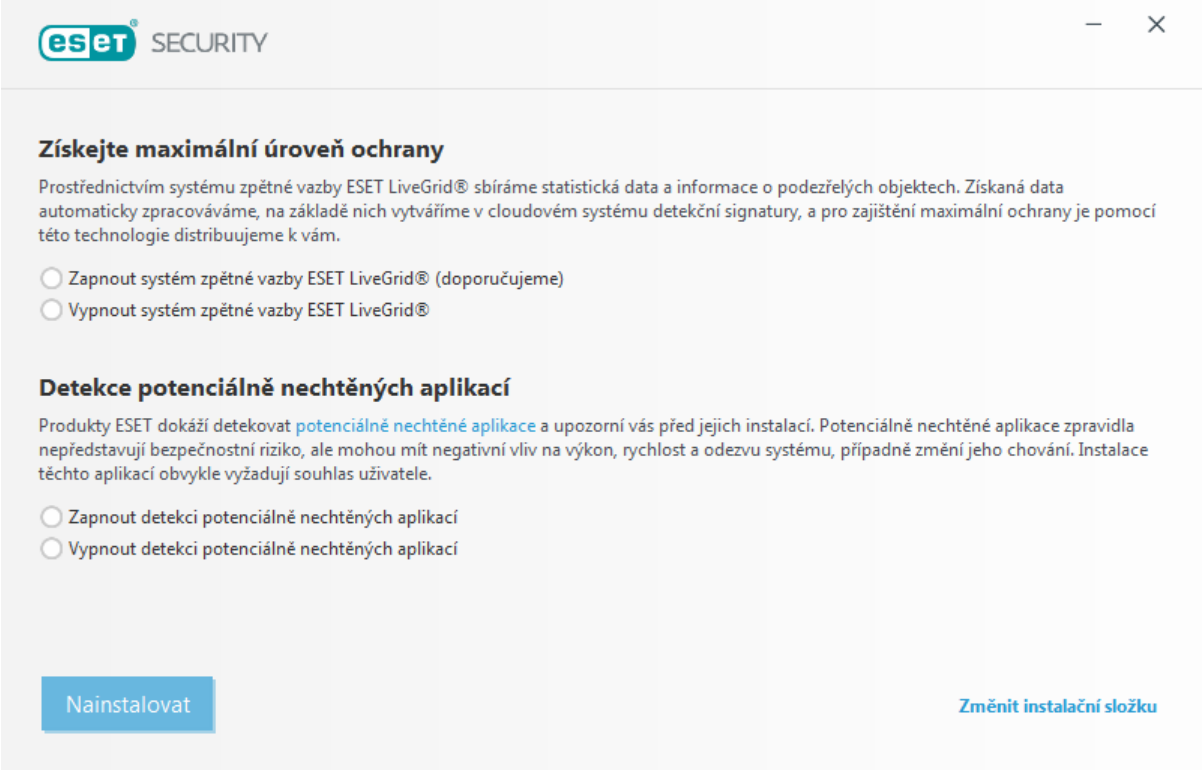
Po odsouhlasení licenčního ujednání budete vyzváni k aktivaci produktu. Aktivovat ho můžete zadáním licenčního klíče nebo prostřednictvím Správce licencí.

Pokud zatím nemáte žádnou licenci, vyberte možnost Zkušební verze nebo kliknout na Zakoupit licenci. Případně klikněte na možnost Přeskočit aktivaci. K aktivaci budete vyzváni po dokončení instalace prvním spuštění programu.

2.2.1 Zadání licenčního klíče

Průvodce do vašeho počítače nainstaluje produkt, který odpovídá zadanému licenčnímu klíči. Pokud máte licenci na více produktů, kliknutím na tlačítko **Změnit produkt** si zobrazte seznam produktů, které si můžete nainstalovat. Následně si vyberte ten, který chcete nainstalovat. Pro více informací o jednotlivých produktech se podívejte do srovnávací tabulky.

Dále klikněte na tlačítko **Pokračovat** a nastavte technologii **ESET LiveGrid®** a **Detekci potenciálně nechtěných aplikací**. ESET LiveGrid® pomáhá bezprostředně informovat společnost ESET o nových hrozbách a tím chránit zákazníky. Tento systém funguje na principu odeslání podezřelých vzorků do virových laboratoří ESET, kde jsou analyzovány a využívány při sestavování detekčního jádra. Potenciálně nechtěné aplikace nemusí být nutně škodlivé, ale mohou negativně ovlivnit chování operačního systému. Více informací naleznete v kapitole Potenciálně nechtěné aplikace ve slovníku pojmů.



Klikněte na tlačítko **Instalovat** pro spuštění instalačního procesu. Po dokončení instalace klikněte na tlačítko **Dokončit**.

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

Pokud máte licenci, která vás opravňuje k instalaci více produktů, nainstalujte si ten, který vyhovuje vašim potřebám. Pro více informací o jednotlivých produktech se podívejte do srovnávací tabulky.

Podrobnější informace, včetně technologie **ESET LiveGrid®** a **detekci potenciálně nechtěných aplikací**, přejděte do kapitoly Live installer.

2.2.2 Použití správce licencí

Po vybrání možnosti **Použít správce licencí** budete vyzváni k zadání přihlašovacích údajů k vašemu my.eset.com účtu. Po zadání údajů a kliknutím na tlačítko **Přihlásit se** se vám zobrazí seznam licencí, které můžete použít pro aktivaci produktu. Vyberte požadovanou licenci a klikněte na tlačítko **Pokračovat**.

Poznámka:
Pokud zatím nemáte my.eset.com účet, klikněte na tlačítko **Vytvořit účet**. V případě, že si nemůžete vzpomenout na heslo, klikněte na možnost **Zapomněl jsem heslo**. Následně budete přesměrování na online portál.

Prostřednictvím ESET Správce licencí můžete spravovat všechny své licence pohodlně z jednoho místa. Na portále uvidíte detaily o licenci, můžete prostřednictvím portálu také prodloužit její platnost, povýšit ji na vyšší produkt nebo rozšířit její počet. Licence na portál nejprve zadejte prostřednictvím licenčního klíče. Následně uvidíte, na kolika zařízeních máte licenci aktivovanou, na kolika počítačích ji ještě můžete použít a informaci o její platnosti. Aktivní instalace aktivované vaší licencí můžete přejmenovat nebo rovnou deaktivovat.

V případě, že budete chtít licenci například povýšit z ESET NOD32 Antivirus na ESET Smart Security Premium, budete po kliknutí na tlačítko **Rozšířit** přesměrováni na online obchod pro dokončení nákupu.

Do správce licencí si můžete přidat všechny své licence, stahovat přímo produkty do svého počítače.

2.2.3 Změna instalační složky

Po vybrání možnosti **Změnit instalační složku** budete vyzváni k výběru umístění instalace. Standardně se program instaluje do složky:

C:\Program Files\ESET\ESET NOD32 Antivirus

Umístění instalace můžete změnit kliknutím na tlačítko **Procházet...** (nedoporučujeme).

V dalším kroku nastavte technologii **ThreatSense** a **Detekci potenciálně nechtěných aplikací**. Více informací naleznete v kapitole Live installer.

Pro zahájení instalace klikněte na tlačítko **Instalovat**.

2.3 Známé problémy při instalaci

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

2.4 Aktivace produktu

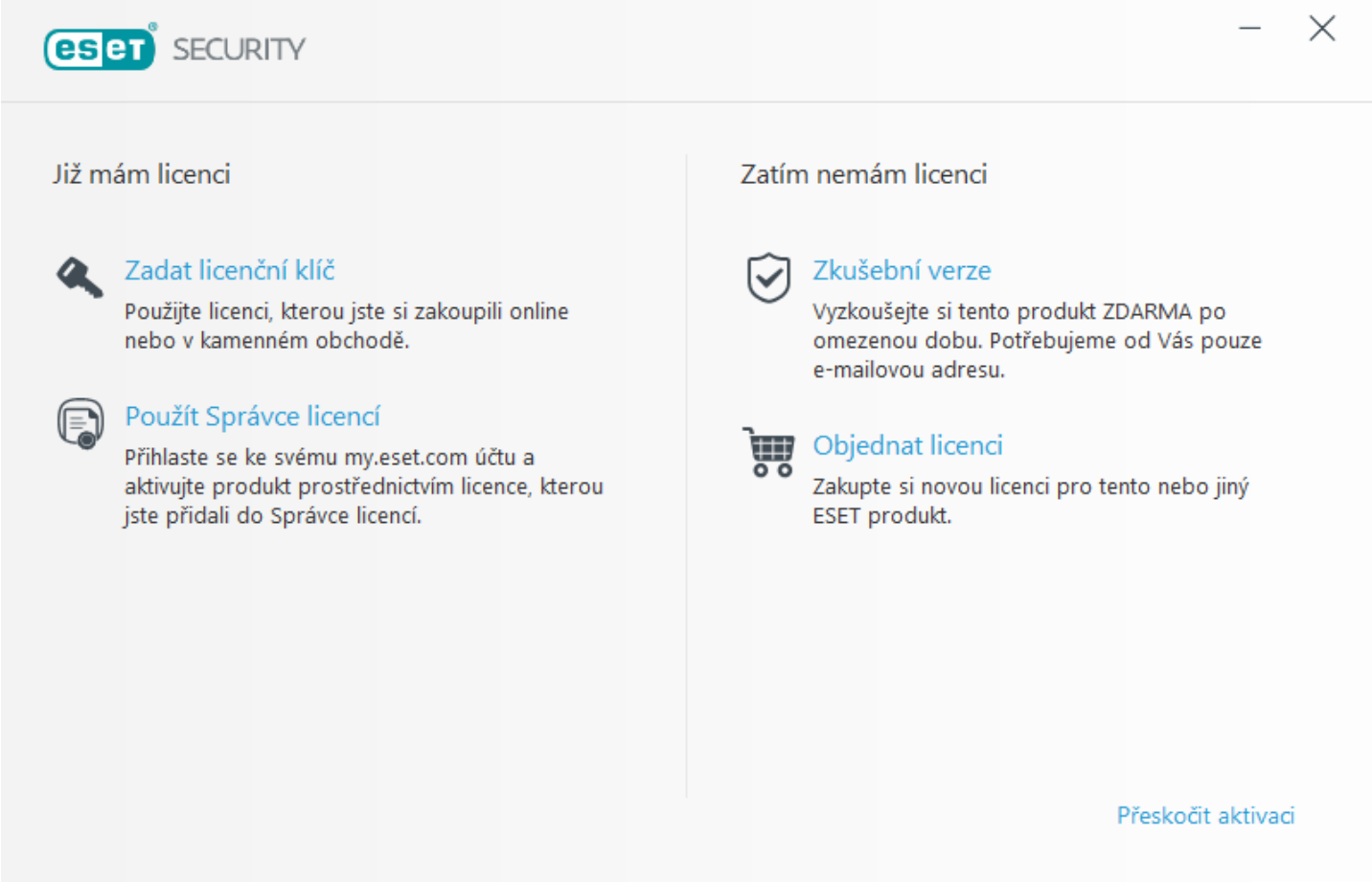
Po dokončení instalace budete vyzváni k aktivaci produktu.

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

Pro aktivaci ESET NOD32 Antivirus klikněte na ikonu v oznamovací oblasti a vyberte možnost **Aktivovat produkt**. Produkt můžete aktivovat také v hlavním okně po kliknutí na záložku **Nápověda a podpora** > **Aktivovat produkt** nebo **Domů** > **Aktivovat produkt**.

K dispozici jsou následující možnosti aktivace:

- **Licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.
- Po vybrání možnosti Použít Správce licencí budete vyzváni k zadání přihlašovacích údajů k vašemu my.eset.com účtu.
- Pokud si chcete produkt ESET NOD32 Antivirus nejprve vyzkoušet, vyberte možnost **Bezplatná zkušební licence**. Následně budete vyzváni k zadání e-mailové adresy, na kterou obdržíte zkušební údaje. Každý zákazník si může zkušební licenci aktivovat pouze jednou.
- Pokud zatím nemáte žádnou licenci, klikněte na možnost **Zakoupit licenci**. Následně budete přesměrování na webové stránky lokálního distributora ESET.



Pokud máte pouze klasické licenční údaje (uživatelské jméno a heslo), klikněte na možnost **Mám uživatelské jméno a heslo, co mám dělat**. Následně budete přesměrováni na online portál, na kterém si můžete licenční údaje přegenerovat a získat nový licenční klíč.

Po aktivaci produktu na záložce **Nápověda a podpora** > **Základní informace pro technickou podporu** naleznete uživatelské jméno/identifikátor licence, které se používá pro identifikaci uživatele při komunikaci s technickou podporou společnosti ESET.

2.5 Zadání licenčního klíče

Pro správný chod programu je důležité, aby byl automaticky aktualizován. To je možné pouze tehdy, pokud jste jej aktivovali.

Pokud jste produkt neaktivovali po dokončení instalace programu, můžete tak učinit nyní. V hlavním okně programu klikněte na záložku **Nápověda a podpora**, v pravé části klikněte na **Aktivovat produkt** a do zobrazeného dialogového okna zadejte licenční údaje, které jste obdrželi při nákupu bezpečnostního produktu ESET.

Licenční klíč zadávejte přesně tak, jak je uvedeno na licenčním certifikátu.

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

POZNÁMKA:
Údaje z licenčního e-mailu doporučujeme zkopírovat (CTRL+C) a vložit do programu (CTRL+V). Při kopírování dejte pozor, abyste navíc nevložili mezeru.

2.6 Doporučení produktu ESET přátelům

Prostřednictvím této verze produktu ESET NOD32 Antivirus můžete získat odměnu za jeho doporučení svým přátelům a členům rodiny – i v případě, kdy používáte zkušební licenci. Za každé doporučení, které úspěšně proměníte v instalaci produktu, získáte vy a druhá strana navíc ochranu počítače na měsíc zdarma.

Doporučení na instalaci produktu je nutné zaslat přímo z programu ESET NOD32 Antivirus. V tabulce níže uvádíme přehled, jaký typ produktu lze, v závislosti na nainstalovaném programu, doporučit.

Nainstalovaný produkt	Produkt k doporučení
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Doporučení produktu

Pro odeslání referral odkazu klikněte v hlavním okně programu ESET NOD32 Antivirus na možnost **Doporučit příteli**. Po kliknutí na možnost **Doporučit prostřednictvím odkazu** vygeneruje produkt unikátní odkaz a zobrazí jej v novém okně. Zobrazený odkaz si zkopírujte a zašlete jej přátelům/členům vaší rodiny. V případě potřeby můžete odkaz sdílet přímo z produktu, na svůj **Google+** kanál, **Facebook**, nebo vašim **Gmail** kontaktům.

Po té, co přítel klikne na vámi zaslaný odkaz, bude přesměrován na webovou stránku, na které si může stáhnout produkt ESET – pokud jej zatím nemá nainstalovaný nebo používá zkušební licenci. Po každém úspěšném použití referral odkazu obdržíte oznámení a platnost vaší licence se prodlouží o další měsíc. Počet úspěšných použití referral odkazů si můžete kdykoli zobrazit po kliknutí na možnost **Doporučit příteli** v hlavním okně produktu.

2.7 Aktualizace na novou verzi

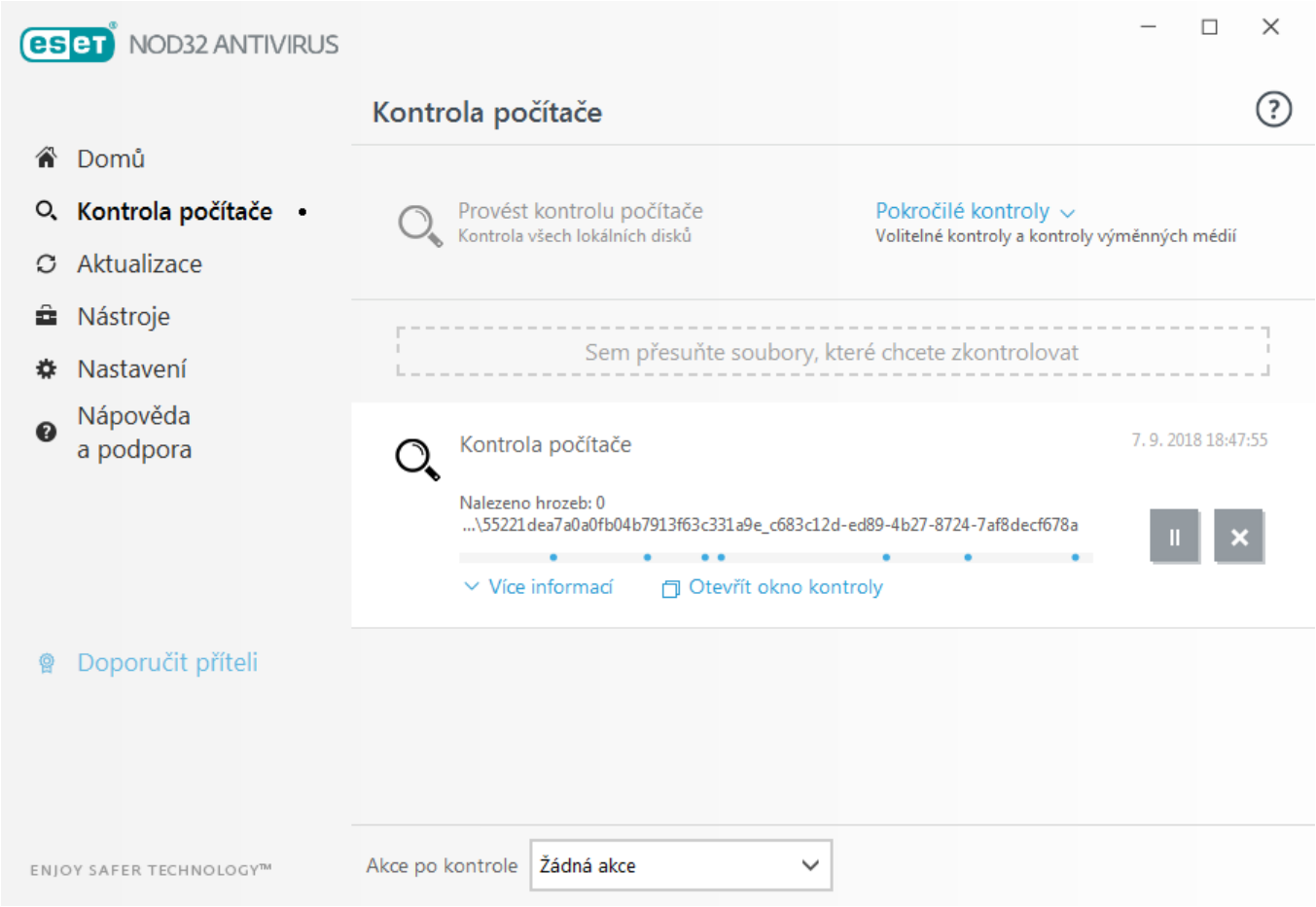
Nové verze produktů opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů. Existuje několik způsobů, jak aktualizovat produkt na novější verzi.

1. Automaticky prostřednictvím aktualizace programu.
   Jelikož se aktualizace programu týká všech uživatelů a může mít významný dopad na systém, je vydávána až po dlouhém období testování na všech operačních systémech v různých konfiguracích. Pokud chcete aktualizovat na nejnovější verzi ihned po jejím vydání, použijte některou z níže uvedených metod.
2. Ručně – v hlavním okně na záložce **Aktualizace** klikněte na **Zkontrolovat aktualizace**.
3. Ručně – stáhněte si z webových stránek společnosti ESET nejnovější verzi a nainstalujte ji přes stávající. V průběhu instalace nové verze dojde k zachování stávající konfigurace programu.

2.8 Kontrola počítače po dokončení instalace

Po nainstalování ESET NOD32 Antivirus a aktualizování detekčních modulů se spustí automatická kontrola počítače.

Kontrolu počítače můžete spustit také kdykoli ručně kliknutím v hlavním okně na záložku **Kontrola počítače** > **Provést kontrolu počítače**. Více informací naleznete v kapitole Kontrola počítače.



3. Začínáme

Tato kapitola poskytuje první seznámení s produktem ESET NOD32 Antivirus a jeho základním nastavení.

3.1 Seznámení s uživatelským prostředím

Hlavní okno produktu ESET NOD32 Antivirus je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

Domů – v přehledné formě poskytuje informace o stavu ochrany ESET NOD32 Antivirus,

Kontrola počítače – umožňuje nastavit a spustit kontrolu počítače nebo výměnných médií. Také můžete zopakovat naposledy provedenou kontrolu.

Aktualizace – zobrazuje informace o aktualizacích detekčních a programových modulů,

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

Nastavení – v této části naleznete možnosti pro aktivaci jednotlivých bezpečnostních prvků z kategorie ochrana počítače, internetová ochrana.

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

Na záložce **Stav ochrany** jsou zobrazeny informace o bezpečnosti a úrovni ochrany počítače.

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

V tomto okně dále naleznete odkazy na často používané funkce ESET NOD32 Antivirus a informace o poslední aktualizaci modulů.

Co dělat, pokud systém nepracuje správně?

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

Červená barva stavu ochrany a informace Není zajištěna maximální ochrana signalizuje kritické problémy. Ochrana vašeho systému tak není zajištěna v plné míře. Možné příčiny jsou:

- **Produkt není aktivován** – ESET NOD32 Antivirus můžete aktivovat kliknutím na záložku **Domů** a vybráním možnosti **Aktivovat plnou verzi** nebo **Zakoupit nyní**.
- **Moduly nejsou aktuální** – tato chyba se zobrazí po několika neúspěšných pokusech o kontaktování aktualizačního serveru z důvodu aktualizace detekčních a programových modulů. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Nejčastějším důvodem neaktivovaný produkt nebo chybně nastavené připojení k internetu.
- **Vypnutá antivirová a antispyware ochrana** – antivir a antispyware ochranu znovu zapněte kliknutím na **Spustit všechny moduly antiviru a antispyware**.
- **Vypršela licence produktu** – v tomto případě ikona ochrany změní barvu na červenou. Program nebude možné od této chvíle aktualizovat. Pro prodloužení licence doporučujeme řídit se instrukcemi zobrazenými v okně s upozorněním.

Žlutá barva stavu ochrany znamená částečné problémy. Například problémy s aktualizací programu nebo blížící se datum vypršení licence.
Možné důvody jsou:

- **Je zapnutý herní režim** – zapnutí Herního režimu představuje potenciální bezpečnostní riziko. Tato funkce

zakáže zobrazování všech oken s upozorněním a pozastaví všechny naplánované úlohy.

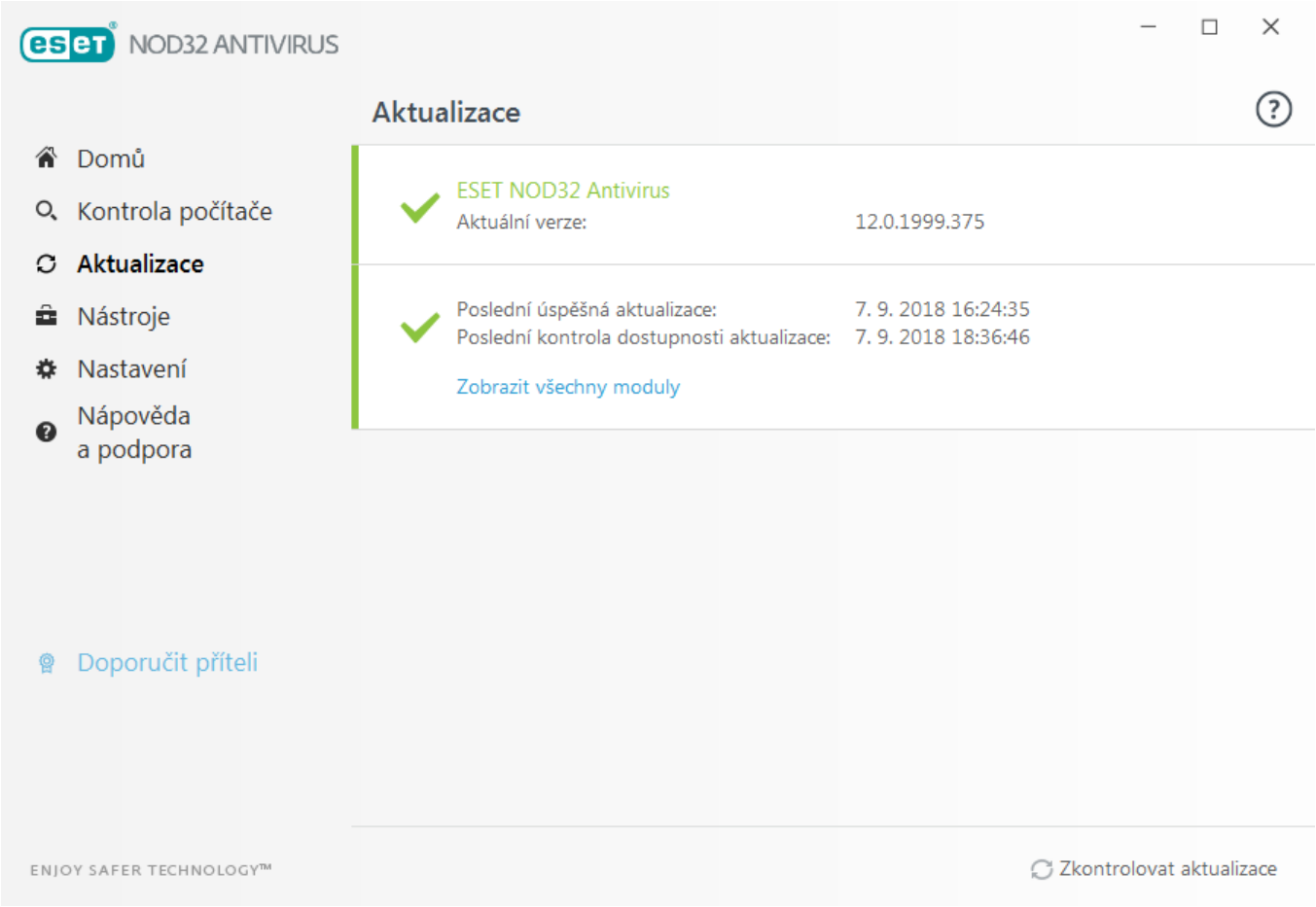
- **Blíží se konec platnosti licence** – v tomto případě ikona ochrany změní barvu na žlutou a zobrazí se varovné hlášení. Poté, co licence vyprší, se program nebude aktualizovat a ikonka ochrany změní barvu na červenou.

V případě, že není možné problém vyřešit, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zobrazte nápovědu nebo přejděte do ESET Databáze znalostí. Pokud i přesto budete potřebovat pomoc, můžete odeslat dotaz na technickou podporu. Specialisté technické podpory ESET reagují rychle a pomáhají při řešení problémů.

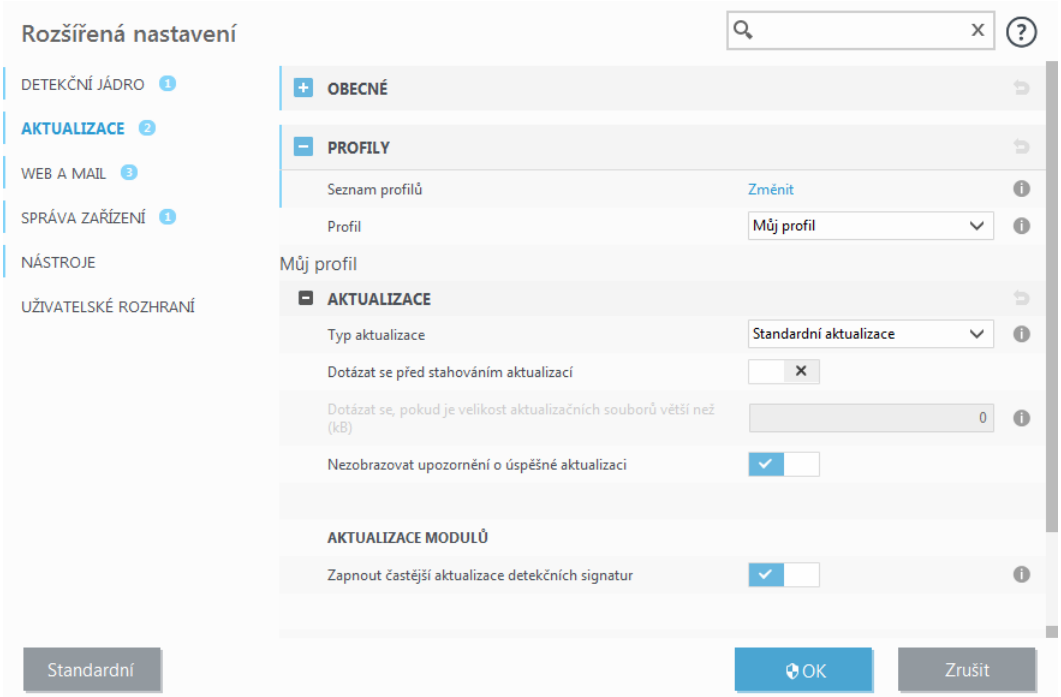
3.2 Aktualizace

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

Pokud jste produkt do této chvíle neaktivovali, budete k tomu vyzváni právě teď.

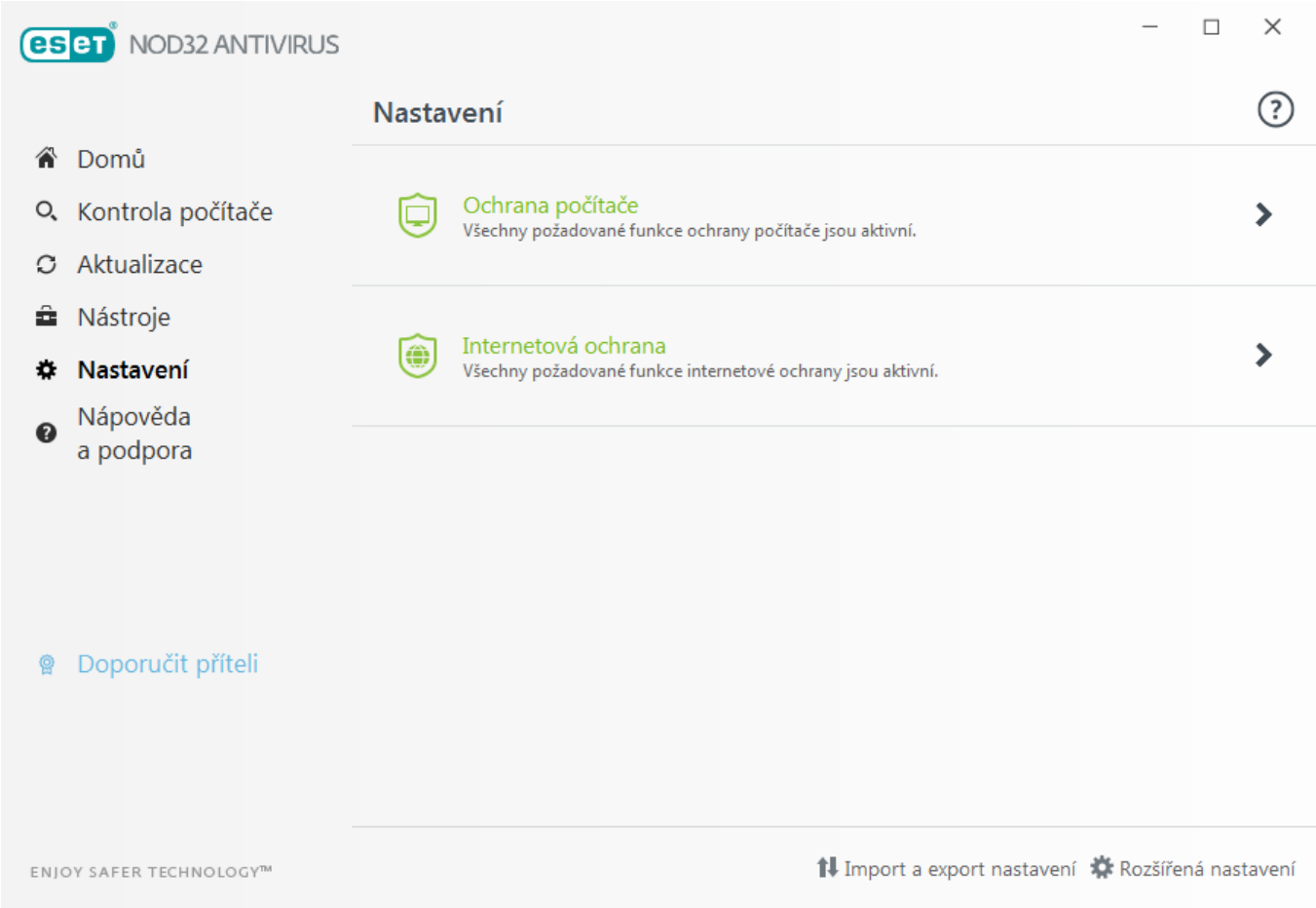


Pro konfiguraci parametrů aktualizace přejděte do rozšířeného nastavení (dostupného po stisknutí **klávesy F5** v hlavním okně programu) na záložku **Aktualizace**. Přistupujete-li do internetu prostřednictvím proxy, je potřeba jej v této části nastavit. V případě problémů s aktualizací, klikněte na tlačítko **Vyprázdnit** pro vyčištění aktualizační cache.


Rozšířená nastavení
DETEKČNÍ JÁDRO 1
AKTUALIZACE 2
WEB A MAIL 3
SPRÁVA ZAŘÍZENÍ 1
NÁSTROJE
UŽIVATELSKÉ ROZHRANÍ
OBECNÉ
PROFILY
Seznam profilů
Změnit
Profil
Můj profil
Můj profil
AKTUALIZACE
Typ aktualizace
Standardní aktualizace
Dotázat se před stahováním aktualizací
Dotázat se, pokud je velikost aktualizačních souborů větší než (kB)
0
Nezobrazovat upozornění o úspěšné aktualizaci
AKTUALIZACE MODULŮ
Zapnout častější aktualizace detekčních signatur
Standardní
OK
Zrušit

4. Práce s ESET NOD32 Antivirus

Na záložce **Nastavení** můžete konfigurovat úroveň ochrany počítače .



Záložka **Nastavení** obsahuje následující sekce:

Ochrana počítače

Internetová ochrana

V sekci **Ochrana počítače** můžete zapnout nebo vypnout následující moduly:

- **Rezidentní ochrana souborového systému** – všechny soubory jsou kontrolovány v momentě, kdy je vytvoříte, otevřete nebo spustíte.
- **Správa zařízení** – pomocí této součásti můžete blokovat přístup k výměnným médiím (CD/DVD/USB...).
- **HIPS** – systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně na základě pravidel předdefinovaných pravidel společností ESET.
- **Herní režim** – po aktivaci herního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. Zároveň hlavní okno změní barvu na oranžovou a upozorní vás na potenciální bezpečnostní riziko.
- **Anti-Stealth ochrana** – detekuje nebezpečné programy jako rootkity, které jsou po svém spuštění neviditelné pro operační systém, a další ochranné mechanismy a aplikace.

V sekci **Internetová ochrana** můžete zapnout nebo vypnout následující moduly:

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

Pro dočasné deaktivování konkrétního modulu klikněte na zelený přepínač . Mějte na paměti, že tím dojde ke snížení úrovně ochrany počítače. Pro znovu zapnutí ochrany vypnutého bezpečnostního modulu klikněte na červený přepínač pro znovu aktivování konkrétního modulu.

POZNÁMKA:
Pokud vypnete výše uvedeným způsobem jednotlivý bezpečnostní modul, automaticky se znovu zapne po restartování počítače.

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

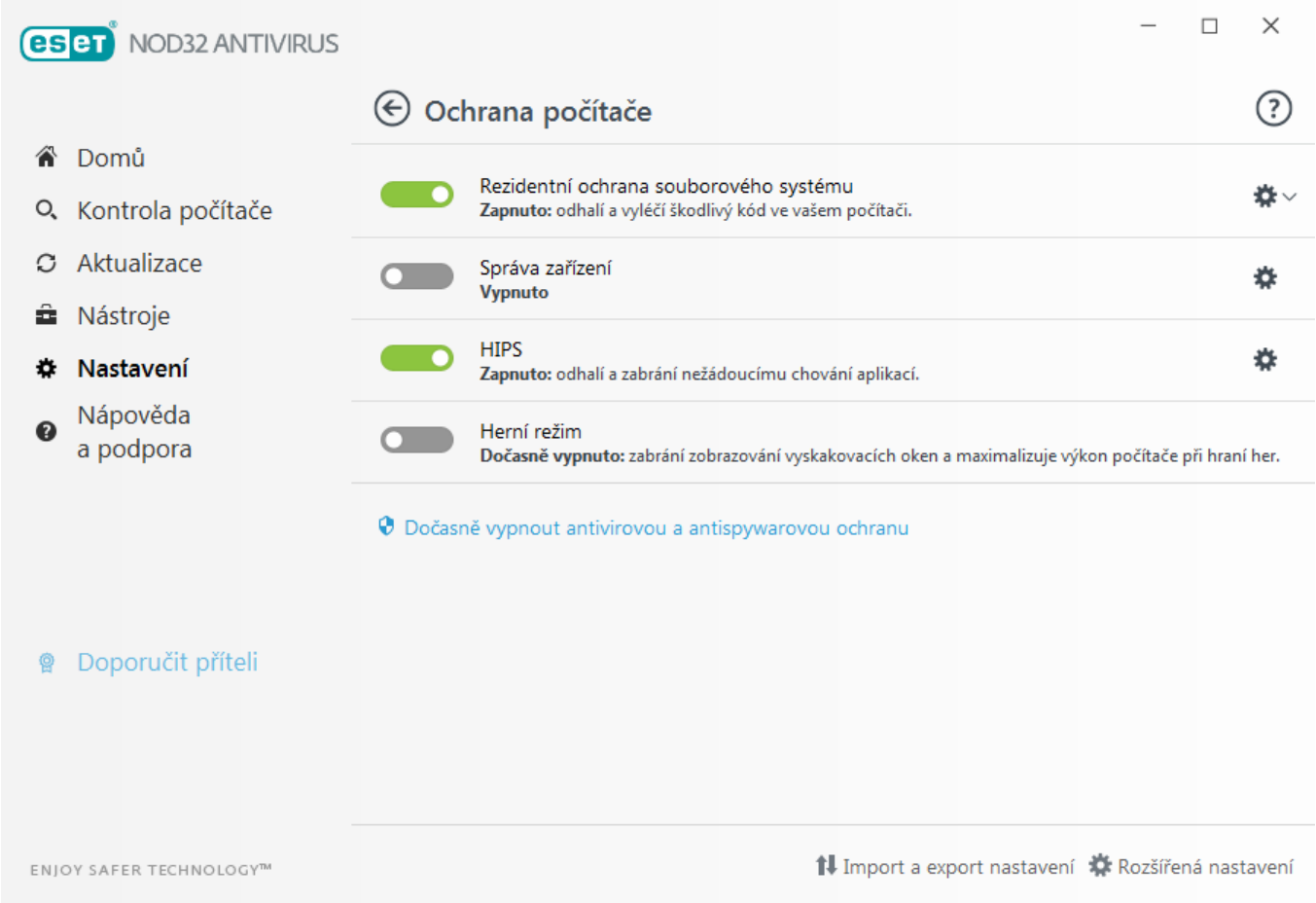
Další možnosti naleznete v dolní části okna. Pro načtení již existující konfigurace z *.xml* konfiguračního souboru nebo pro uložení aktuálního nastavení do souboru klikněte na **Import a export nastavení**. Pro více informací přejděte do kapitoly Import a export nastavení.

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

4.1 Ochrana počítače

V sekci **Nastavení** > **Ochrany počítače** naleznete jednotlivé moduly ochrany počítače Pro dočasné vypnutí jednotlivých modulů použijte přepínač . Mějte na paměti, že tímto můžete snížit úroveň zabezpečení počítače. Detailní nastavení konkrétních modulů se zobrazí po kliknutí na ozubené kolečko .

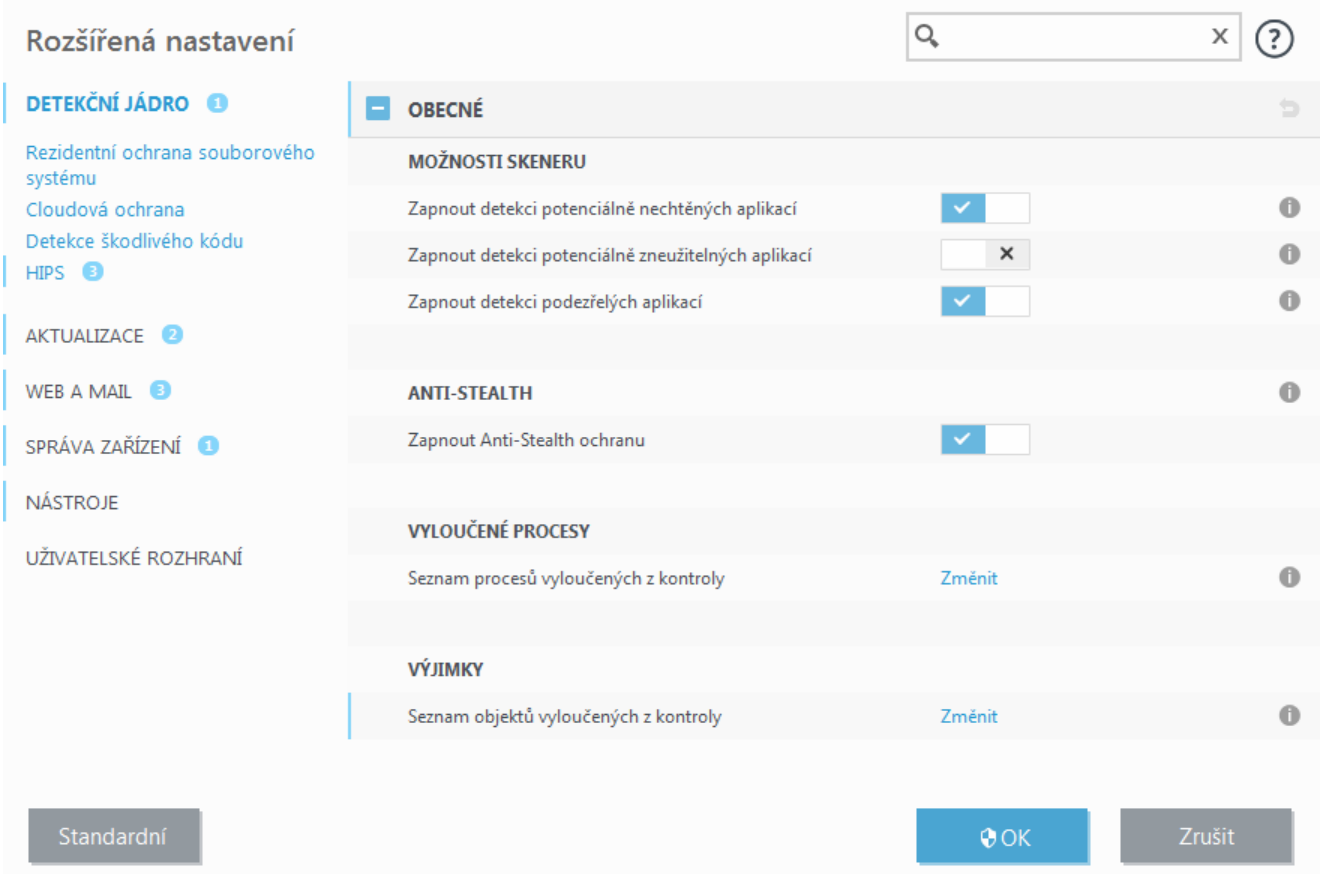
Pro vytvoření výjimek klikněte na ozubené kolečko na řádku rezidentní ochrana souborového systému a vyberte možnost Upravit výjimky....



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

4.1.1 Detekční jádro

Antivirus a antispyware zajišťuje komplexní ochranu před nebezpečnými programy ohrožujícími systém. Zahrnuje kontrolu souborů, e-mailů a internetové komunikace. V případě zjištění škodlivého kódu jej modul Antivir dokáže eliminovat zablokováním, následným vyléčením, odstraněním nebo přesunutím do karantény.



V možnostech kontroly, které jsou společné pro všechny moduly (např. Rezidentní ochrana souborového serveru, Ochrana přístupu na web,...), můžete zapnout nebo vypnout následující detekci:

- **Potenciálně nechtěné aplikace** nemusí být nutně škodlivé, v každém případě však mohou mít negativní dopad na výkon počítače.
  Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- **Potenciálně zneužitelné aplikace** jsou legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti. Příkladem mohou být programy pro vzdálené připojení, aplikace k odšifrování hesel a keyloggery (programy, které zaznamenávají zadané znaky na klávesnici). Tato možnost je standardně vypnuta.
  Více informací o tomto typu aplikací naleznete ve slovníku pojmů.
- **Potenciálně podezřelé aplikace** jsou programy, které používají pro kompresi packery nebo jiné ochranné mechanismy zabraňující detekci. Takové typy ochranných mechanismů jsou velice často zneužívány autory škodlivého kódu.

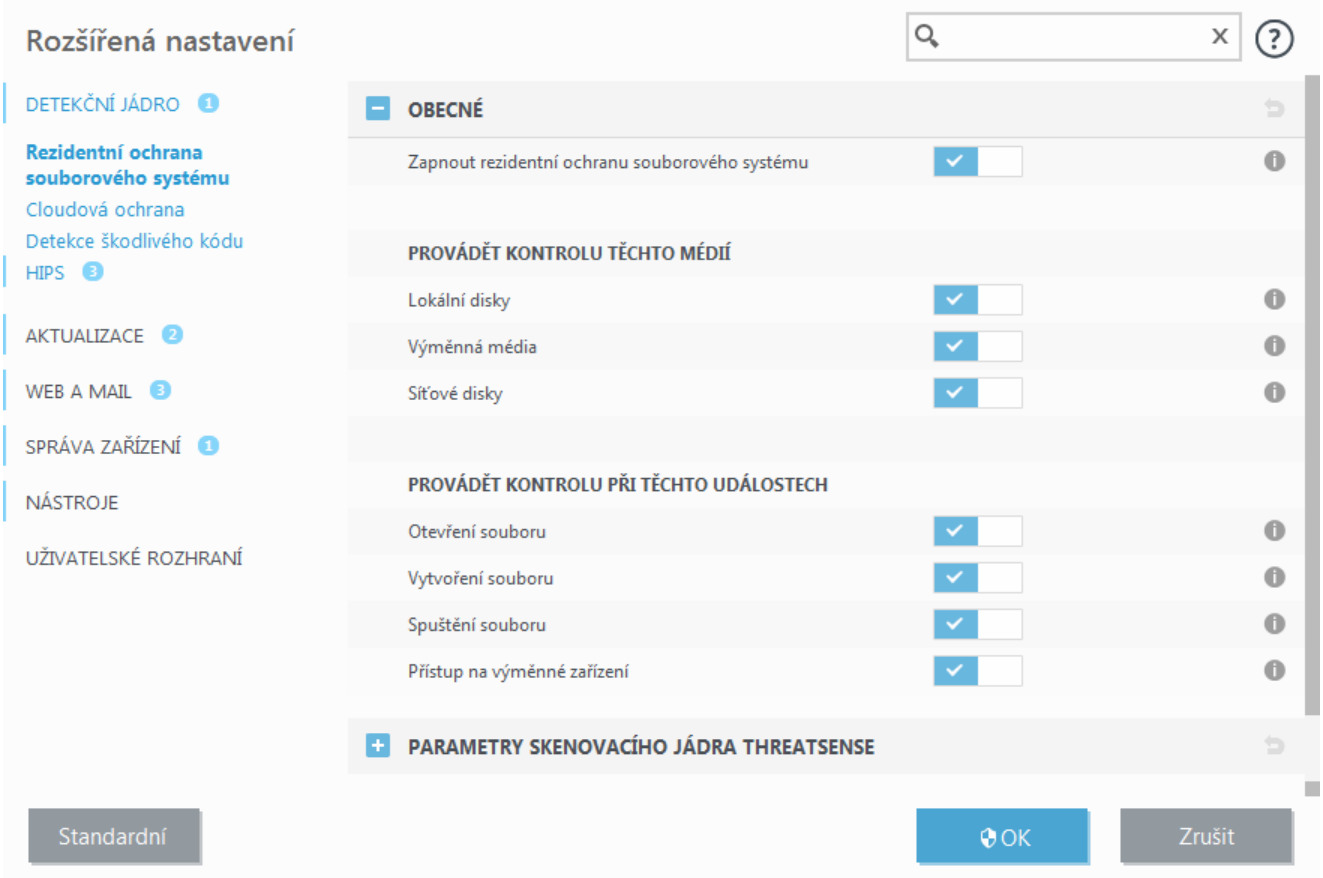
Technologie Anti-Stealth je sofistikovaný systém pro detekci nebezpečných programů například rootkitů, které jsou po svém spuštění neviditelné pro operační systém a bezpečnostní aplikace.

Prostřednictvím **výjimek** můžete vyloučit konkrétní soubory nebo složky z kontroly. Výjimky však doporučujeme vytvářet pouze v ojedinělých případech. Jejich vytvoření může být užitečné například v případě, kdy nechcete kontrolovat velké soubory (databáze, zálohy, ISO soubory atp.), jejichž kontrola zpomaluje systém nebo způsobuje konflikt s jinou aplikací. Pro více informací přejděte do kapitoly výjimky.

Zapnout rozšířenou kontrolu prostřednictvím AMSI – prostřednictvím Microsoft Antimalware Scan Interface bude program Powershell skripty a skripty spouštěné prostřednictvím Windows Script Host (tato funkce je dostupná od Windows 10).

4.1.1.1 Rezidentní ochrana souborového systému

Rezidentní ochrana kontroluje veškeré dění v počítači. Všechny soubory, které se v počítači otevírají, vytvářejí a spouštějí jsou kontrolovány na přítomnost infiltrace. Rezidentní ochrana se spouští automaticky při startu systému.



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 odškrtnutím možnosti **Automatický start rezidentní ochrany souborového systému** v **Rozšířeném nastavení** na záložce **Rezidentní ochrana souborového systému** > **Obecné**.

Kontrola médií

Standardně je nastavena kontrola všech typů médií:

Lokální disky – lokální pevné disky v počítači,
Výměnná média – diskety, CD, DVD, USB klíče, Bluetooth zařízení a další,
Síťové disky – namapované síťové disky.

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

Kontrola při událostech

Standardně jsou soubory kontrolovány při otevírání, spouštění a vytváření. Tato nastavení doporučujeme ponechat pro zajištění maximální možné ochrany počítače:

- **Otevření souboru** – zapne nebo vypne kontrolu souborů při přístupu a otevírání,
- **Vytvoření souboru** – zapne nebo vypne kontrolu vytvářených nebo upravovaných souborů,
- **Spuštění souboru** – zapne nebo vypne kontrolu souborů při jejich spouštění,
- **Přístup k výměnnému médiu** – zapne nebo vypne kontrolu souborů, které přistupují k výměnným zařízením.

Rezidentní ochrana kontroluje všechny typy médií a kontrola je prováděna při různých událostech jako je přístup k souboru. Při kontrole jsou používány detekční metody technologie ThreatSense (ty jsou popsány v kapitole Nastavení skenovacího jádra ThreatSense). Chování rezidentní ochrany 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 při každé aktualizaci detekčních modulů. Toto chování můžete přizpůsobit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje. Pokud chcete možnosti kontroly upravit, otevřete **Rozšířená nastavení** (stisknutím **klávesy F5** v hlavním okně programu), přejděte na záložku **Antivirus** > **Rezidentní ochrana souborového systému**. Dále přejděte na záložku **Parametry skenovacího jádra ThreatSense** > **Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

4.1.1.1.1 Rozšířená nastavení kontroly

Doplňující parametry ThreatSense 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 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 odškrtněte možnost **Standardní nastavení archivů.**

Doplňující parametry ThreatSense pro spouštěné soubory

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

Rozšířená heuristika při spuštění souboru z výměnných médií – rozšířená heuristika emuluje kód aplikace ve virtuálním prostředí a vyhodnotí chování aplikace ještě předtím, než je povoleno aplikaci spuštění z výměnného média.

4.1.1.1.2 Úrovně léčení

Rezidentní ochrana pracuje ve třech režimech léčení (pro jejich zobrazení klikněte na záložku **Rezidentní ochrana souborového systému** > **Parametry skenovacího jádra ThreatSense**).

Neléčit – infikované soubory nebudou automaticky léčeny. Při detekci se zobrazí varovné okno s možností výběru akce, která se má provést. Tato úroveň je navržena pro pokročilé uživatele, kteří vědí, jak postupovat v případě infiltrace.

Standardní úroveň léčení – program se pokusí infikované soubory automaticky léčit, nebo odstranit na základě předdefinované akce (v závislosti na typu infiltrace). Informace o detekci a odstranění infikovaného souboru je zobrazena informační bublinou v pravém dolním rohu obrazovky. Pokud program nedokáže automaticky vybrat správnou akci, zobrazí se okno s možností výběru akce. Možnost výběru akce se zobrazí také v případě, když se předdefinovanou akci nepodaří provést.

Přísné léčení – program vyléčí nebo odstraní všechny infikované soubory. Výjimku tvoří systémové soubory. Pokud je nelze vyléčit, zobrazí se výběr akce, která se má provést.

VAROVÁNÍ:
Při detekci infiltrace v archivu, bude při standardním a přísném léčení odstraněn celý archiv. Při standardním léčení bude archiv odstraněn, pouze pokud obsahuje samotný soubor s infiltrací. Při **přísném léčení** bude archiv odstraněn i v případě, že kromě infiltrace obsahuje další korektní soubory.

4.1.1.1.3 Kdy měnit nastavení rezidentní ochrany

Rezidentní ochrana je klíčovým modulem zabezpečujícím ochranu počítače. Proto je potřeba být při změnách nastavení obezřetný. Rezidentní ochranu doporučujeme měnit pouze ve specifických případech.

Po instalaci ESET NOD32 Antivirus jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Standardní nastavení můžete kdykoliv obnovit kliknutím na tlačítko **Standardní**, které se nachází v okně **Rezidentní ochrana souborového systému** v pravém dolním rohu (**Rozšířená nastavení** > **Detekční jádro** > **Rezidentní ochrana souborového systému**).

4.1.1.1.4 Ověření funkčnosti rezidentní ochrany

Pro ověření, zda je rezidentní ochrana funkční a detekuje viry, je možné použít testovací soubor z webových stránek eicar.com. Jedná se o soubor, který je detekován všemi antivirovými programy a byl vytvořen společností EICAR (European Institute for Computer Antivirus Research) pro testování funkčnosti antivirových programů. Soubor **eicar** je dostupný ke stažení na adrese http://www.eicar.org/download/eicar.com.

4.1.1.1.5 Co dělat, když nefunguje rezidentní ochrana

V této kapitole jsou popsány problémové stavy, které mohou nastat v případě rezidentní ochrany. Je zde také uvedeno jak postupovat při řešení problémů

Rezidentní ochrana je vypnutá

Pokud byla rezidentní ochrana nedopatřením vypnuta uživatelem, je potřeba ji znovu aktivovat. Opětovné zapnutí je možné kliknutím na záložku **Nastavení** v hlavním okně programu a kliknutím na **Ochrana počítače** > **Rezidentní ochrana souborového systému**.

Pokud se rezidentní ochrana nespouští při startu operačního systému, pravděpodobně byla vypnuta možnost **Zapnout rezidentní ochranu souborového systému**. Pro zapnutí této možnosti přejděte do rozšířeného nastavení (dostupného po stisknutí klávesy **F5** v hlavním okně programu) do sekce **Detekční jádro** > **Rezidentní ochrana souborového systému**. V části **Obecné** se ujistěte, že je aktivní možnost **Zapnout rezidentní ochranu souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

Ujistěte se, zda nemáte nainstalován další antivirový program. Mezi dvěma rezidentními ochranami může docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Zapnout rezidentní ochranu souborového systému**, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

4.1.1.2 Volitelná kontrola počítače

Důležitou součástí ESET NOD32 Antivirus je tzv. volitelná kontrola (On-demand), která umožňuje vlastní kontrolu pevných disků, jednotlivých složek a souborů v počítači. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infikované soubory, ale v rámci prevence i průběžně. Hloubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech, aby byly detekovány případné viry, které v době zápisu na disk nebyly zachyceny Rezidentní ochranou souborového systému . Taková situace může nastat, pokud byla rezidentní ochrana v té době vypnutá nebo program neměl aktuální detekční moduly, případně soubor v době zápisu na disk program nebyl vyhodnocen jako vir.

K dispozici jsou dva typy kontroly počítače. Pokud klikněte na možnost **Provést kontrolu počítače**, spustí se rychlá kontrola systému a předdefinovaným nastavení. V případě, že si chcete upravit parametry kontroly, použijte možnost **Volitelná kontrola**, v rámci níž si můžete definovat profil i cíle kontroly.

Provést kontrolu počítače

Tato možnost slouží pro rychlé spuštění kontroly počítače a automaticky léčí nebo odstraňuje infikované soubory a nevyžaduje interakci uživatele. Výhodou této kontroly je snadná obsluha, kdy není nutné cokoli dalšího konfigurovat. V rámci této kontroly se zkontrolují všechny soubory na lokálních jednotkách a hrozby budou automaticky vyléčeny nebo odstraněny. Úroveň léčení je nastavena na standardní úroveň. Více informací o typech léčení se dozvíte v kapitole Léčení.

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

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

Volitelná kontrola

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

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

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

Kontrola výměnných médií

Podobně jako kontrola počítače – spustí rychlou kontrolu výměnných médií (CD/DVD/USB), které 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 kliknutím na **Volitelná kontrola** a vybráním možnosti **Výměnné disky** z rozbalovacího menu **Cíle kontroly**.

Opakovat poslední kontrolu

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

Pomocí rozbalovacího menu **Akce po kontrole** můžete nastavit akci (Žádná akce, Vypnout, Restartovat, Uspat), kterou chcete provést po dokončení kontroly.

Poznámka:
Doporučujeme spouštět kontrolu počítače alespoň jednou za měsíc. Kontrolu je možné nastavit i jako naplánovanou úlohu pomocí **Nástroje** > **Plánovač**.

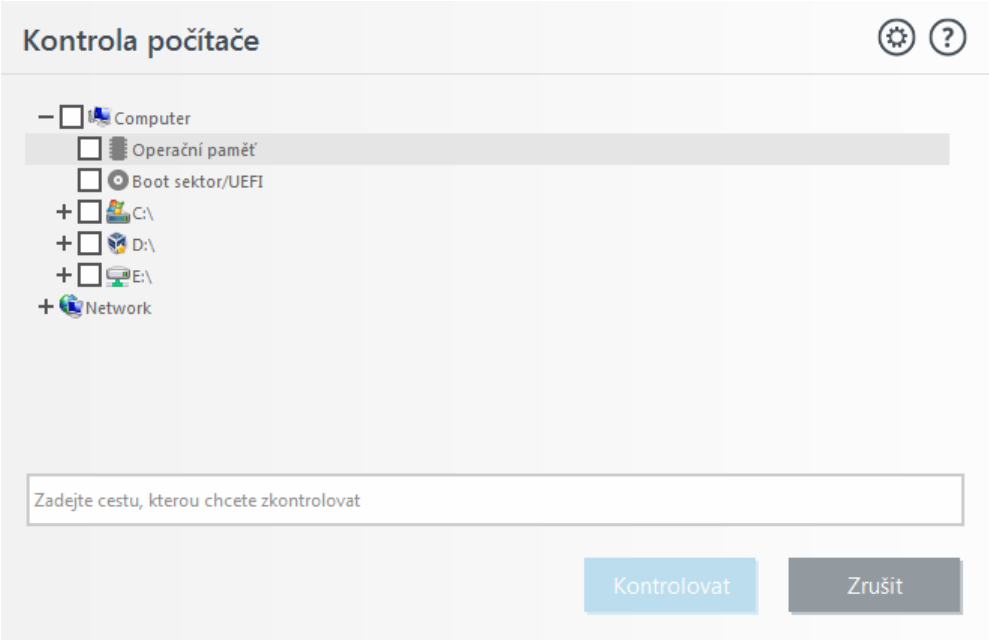
4.1.1.2.1 Spuštění volitelné kontroly

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

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

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

Prázdný řádek pod stromovou strukturou slouží pro rychlý přesun ke zvolenému cíli, nebo k přímému zadání požadovaného cíle. Přímé zadání požadovaného cíle je možné pouze v případě, že není ve stromové struktuře proveden žádný výběr (v rozbalovacím menu **Cíle kontroly** je vybrána možnost **Bez výběru**).



Parametry léčení použitého profilu kontroly můžete změnit v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Volitelná kontrola počítače** > **Parametry skenovacího jádra ThreatSense** > **Léčení**. V případě, že máte zájem pouze o kontrolu souborů bez jejich následného léčení, vyberte možnost **Kontrolovat bez léčení**.

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

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

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

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

Poznámka:
Výsledek kontroly si zobrazíte kliknutím na tlačítko Zobrazit protokol.

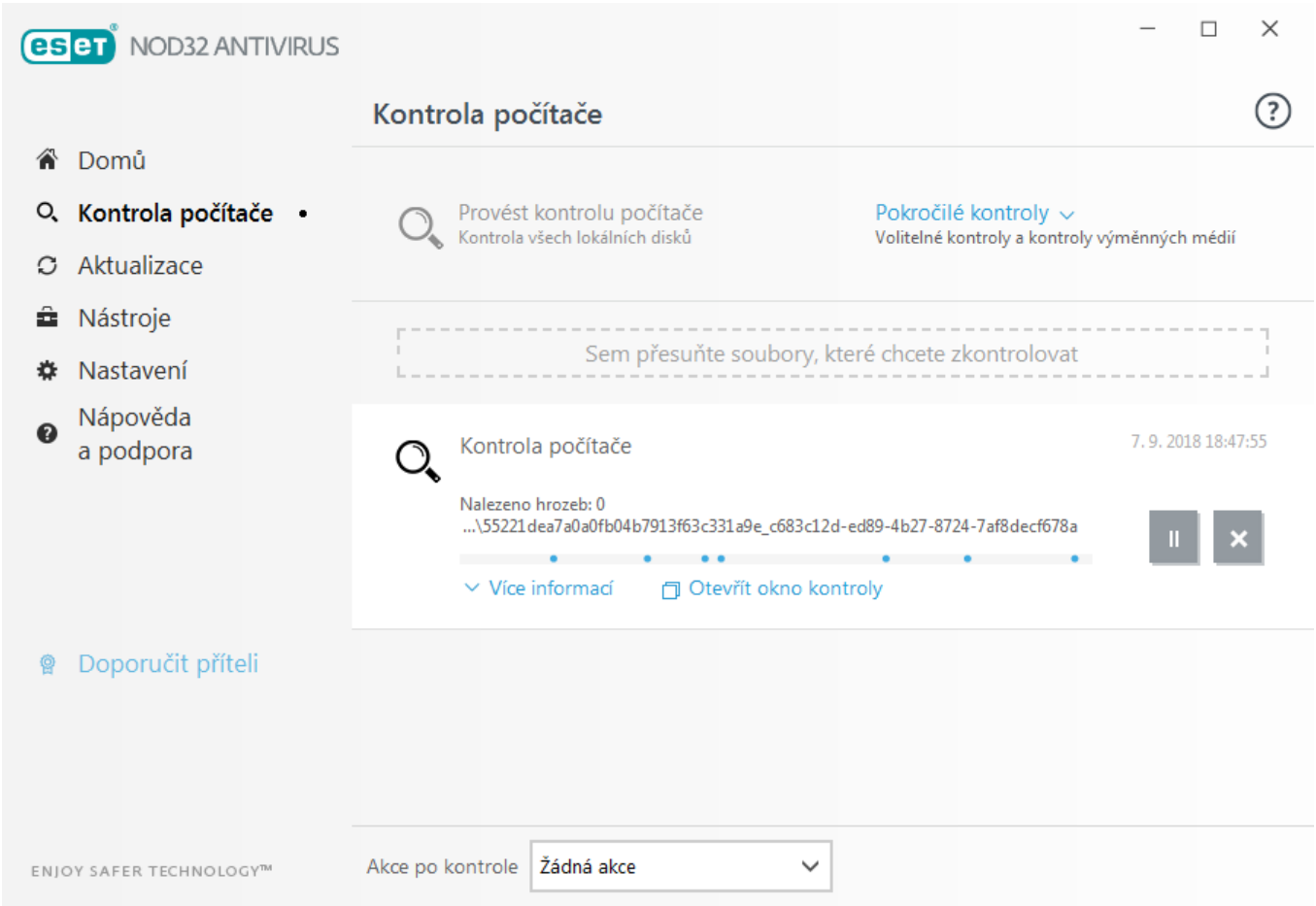
4.1.1.2.2 Průběh kontroly

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

Poznámka:
Je v pořádku, pokud určité typy souborů jako například zaheslovaná data nebo soubory využívané operačním systémem (například *pagefile.sys* a některé soubory protokolů) nemohou být zkontrolovány. Více informací naleznete v Databázi znalostí.

Průběh kontroly – grafická reprezentace procentuálního vyjádření poměru již zkontrolovaných souborů k celkovému množství souborů, které se mají kontrolovat.
Cíl – název právě kontrolovaného souboru a jeho umístění.
Nalezeno hrozeb – celkový počet nalezených hrozeb v průběhu aktuální kontroly.
Pauza – pozastaví právě probíhající kontrolu.
Pokračovat – tato možnost se zobrazí po pozastavení kontroly. Kliknutím na toto tlačítko bude kontrola pokračovat.
Zastavit – přeruší právě probíhající kontrolu.
Rolovat výpis protokolu kontroly – pokud je tato možnost zapnuta, v dialogovém okně protokolu kontroly uvidíte vždy naposledy zkontrolované soubory.

Poznámka:
Pro zobrazení detailních informací klikněte na možnost **Více informací** nebo na **Otevřít okno kontroly**. Kdykoli můžete spustit další kontrolu počítače. Mějte na paměti, že více souběžných kontrol může mít negativní dopad na výkon počítače.



Pomocí možnosti **Akce po kontrole** můžete nastavit akci (Žádná akce, Vypnout, Restartovat, Uspat), kterou chcete provést po dokončení kontroly. Dialog s informací o vypnutí počítače se zobrazí po dobu 1 minuty.

4.1.1.2.3 Profily kontroly

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

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

Příklad:
Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy, potenciální nebezpečné aplikace a přitom požadujete **Přísné léčení**? Vytvořte nový profil kliknutím na tlačítko **Přidat** v Seznamu profilů Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktivní profil** nastavte si parametry kontroly podle potřeby.

4.1.1.2.4 Protokol kontroly

V protokolu kontroly jsou uvedeny následující informace:

- Čas dokončení kontroly
- Doba kontroly
- Počet nalezených hrozeb
- Počet zkontrolovaných objektů
- Informace kontrolovaných discích, složkách a souborech
- Datum a čas kontroly
- Verze použitého detekčního jádra

4.1.1.3 Kontrola po startu

Standardně se provádí během startu počítače a po aktualizaci detekčních 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).

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

4.1.1.3.1 Kontrola souborů spouštěných při startu počítače

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

Rozbalovací menu **Hloubka kontroly** nabízí možnost přizpůsobit množství souborů kontrolovaných při startu. Možnosti kontroly jsou seřazeny vzestupně podle následujících kritérií:

- **Pouze nejčastěji používané soubory** (nejméně kontrolovaných souborů),
- **Často používané soubory**,
- **Běžně používané soubory**,
- **Málo používané soubory**,
- **Všechny registrované soubory** (nejvíce 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** – 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 normální,
- **Nižší** – zatížení systému je nižší,
- **Nejnižší** – zatížení systému je nejnižší,
- **Při nečinnosti** – v momentě, kdy nejsou prováděny žádné jiné činnosti.

4.1.1.4 Kontrola při nečinnosti

Zapnout kontrolu při nečinnosti – aktivováním této možnosti se spustí kontrola počítače, pokud jej uživatel nebude používat.

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**.

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

Kontrola při nečinnosti se může spustit při těchto událostech:

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

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

4.1.1.5 Výjimky

Výjimky umožňují definovat soubory a složky, které nemají být kontrolovány. Pro zajištění kontroly všech objektů na hrozby doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Přesto někdy mohou nastat situace, kdy je nutné objekt vyloučit z kontroly, například u velkých databází, jejichž kontrola by zpomalila počítač nebo aplikací, u kterých dochází ke konfliktu se skenovacím jádrem.

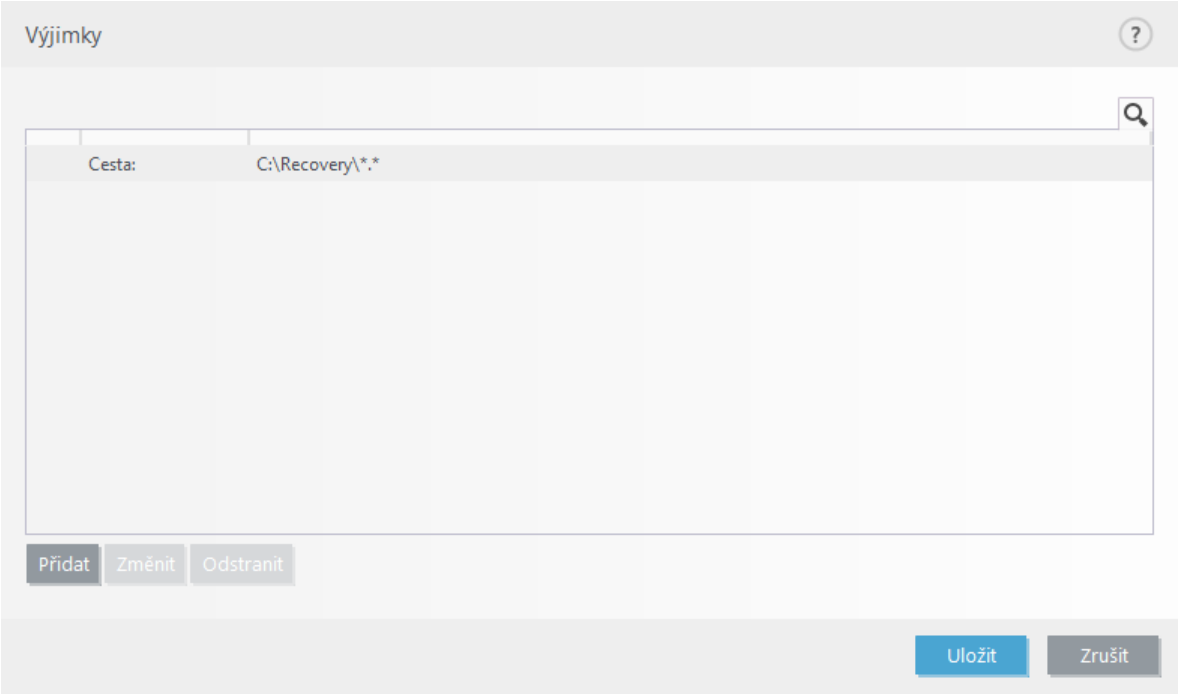
Pro vyloučení objektu z kontroly:

- Klikněte na **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury.

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

Příklady

- Pokud chcete vyloučit ve vybrané složce všechny soubory, zadejte cestu ke složce a použijte masku "*.*".
- Pro vyloučení celé jednotky včetně všech souborů a složek použijte masku "D:*".
- Pokud chcete vyloučit všechny .doc soubory, použijte masku "*.doc".
- Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční, použijte formát "D????. exe". Otazníky zastupují chybějící (neznámé) znaky.



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

Sloupce

Cesta – cesta k vyloučenému souboru nebo složce.

Hrozba – pokud je u vyloučeného souboru uveden i název infiltrace, znamená to, že u souboru je vyloučena pouze detekce této infiltrace. Není však vyloučen soubor jako celek. Pokud by tedy došlo k napadení takto vyloučeného souboru jinou infiltrací, ta bude antivirovým modulem řádně detekována. Tento typ vyloučení je možné použít pouze pro určité typy infiltrací a zadat je můžete pomocí zobrazeného dialogového okna při výskytu hrozby (po kliknutí na **Zobrazit rozšířené nastavení** > **Vyloučit z detekce**), nebo prostřednictvím možnosti **Obnovit a vyloučit z kontroly** z kontextového menu po kliknutí pravým tlačítkem myši na soubor v karanténě (v hlavním okně programu v sekci **Nástroje** > **Karanténa**).

Ovládací prvky

Přidat – přidá objekt na seznam výjimek.

Změnit – upraví existující výjimku.

Odstranit – odstraní výjimku.

4.1.1.6 Parametry skenovacího jádra ThreatSense

ThreatSense je název technologie, kterou tvoří soubor komplexních metod detekce infiltrace. Tato technologie je proaktivní a poskytuje tak ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury, virové signatury), čímž efektivně spojuje jejich výhody. Detekční jádro je schopné kontrolovat několik datových toků paralelně a maximalizovat tak svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně bojovat také s rootkity.

Ve skenovacím jádru 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 ThreatSense** v Rozšířeném nastavení jakéhokoli modulu, který používá ThreatSense technologii (viz níže). Pro různé druhy ochrany se používá různá úroveň nastavení. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému,
- Ochrana dokumentů,
- Ochrana poštovních klientů,
- Ochrana přístupu na web,
- Kontrola počítače.

Parametry ThreatSense jsou optimalizovány speciálně pro každý modul a jejich změna může mít výrazný dopad na výkon systému. Příkladem může být zpomalení systému při povolení kontroly runtime archivů a rozšířené heuristiky pro rezidentní ochranu souborů (standardně jsou kontrolovány pouze nově vytvářené soubory). Proto doporučujeme ponechat původní nastavení ThreatSense pro všechny druhy ochran kromě **Kontroly počítače**.

Kontrolované objekty

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

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

Boot sektory – kontrola přítomnosti boot virů v MBR sektorech disků, kde se nachází tzv. zavaděč operačního systému.

Poštovní soubory – podporovány jsou DBX (Outlook Express) a EML soubory.

Archivy – podporovány jsou formáty ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO, BIN, NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE a jiné.

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

Runtime archivy – runtime archivy se na rozdíl od klasických archivů po spuštění rozbalí v paměti počítače. Kromě podpory tradičních statických archivátorů (UPX, yoda, ASPack, FSG,...) program podporuje díky emulaci kódu i mnoho jiných typů archivátorů.

Možnosti kontroly

V sekci **Možnosti kontroly** můžete vybrat metody, které se použijí pro ověřování přítomnosti infiltrace. Dostupné 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. Nevýhodou je nízká pravděpodobnost falešného poplachu.

Rozšířená heuristika/DNA/Smart vzorky – rozšířená heuristika se skládá z unikátních heuristických algoritmů vyvinutých společností ESET optimalizovaných pro detekci škodlivých kódů napsaných ve vyšších programovacích jazycích. Používání rozšířené heuristiky výrazně zvyšuje detekční schopni produktů ESET. Vzorky zajišťují přesnou detekci virů. S využitím automatického aktualizačního systému mají nové vzorky uživatelé k dispozici do několika hodin od objevení hrozby. Nevýhodou vzorků je detekce pouze známých virů.

Potenciálně nechtěné aplikace – Grayware (neboli PUA – potenciálně nechtěné aplikace) představuje širokou škálu aplikací, které nejsou jednoznačně škodlivé jako viry nebo trojské koně, avšak mohou instalovat nechtěný software, měnit chování vašeho zařízení, provádět neočekávané operace, případně akce bez vědomí uživatele. Další informace naleznete v kapitole Potenciálně nechtěné aplikace ve slovníku pojmů.

Potenciálně zneužitelné aplikace – potenciálně zneužitelné aplikace jsou komerční a legitimní aplikace například pro zobrazení vzdálené pracovní plochy, dešifrování kódů a hesel nebo tzv. keyloggery (programy na monitorování stisknutých kláves). Detekce těchto aplikací je standardně vypnutá.

ESET LiveGrid® – prostřednictvím této reputační technologie jsou kontrolované soubory ověřovány vůči cloudového systému ESET LiveGrid® s cílem dosažení přesnější detekce a zrychlení kontroly.

Léčení

Nastavení léčení ovlivňuje chování virové skeneru. K dispozici jsou 3 úrovně léčení detekovaných infikovaných souborů:

Neléčit – infikované soubory nebudou automaticky léčeny. Při detekci se zobrazí varovné okno s možností výběru akce, která se má provést. Tato úroveň je navržena pro pokročilé uživatele, kteří vědí, jak postupovat v případě infiltrace.

Standardní úroveň léčení – program se pokusí infikované soubory automaticky léčit, nebo odstranit na základě předdefinované akce (v závislosti na typu infiltrace). Informace o detekci a odstranění infikovaného souboru je zobrazena informační bublinou v pravém dolním rohu obrazovky. Pokud program nedokáže automaticky vybrat správnou akci, zobrazí se okno s možností výběru akce. Možnost výběru akce se zobrazí také v případě, když se předdefinovanou akci nepodaří provést.

Přísné léčení – program vyléčí nebo odstraní všechny infikované soubory. Výjimku tvoří systémové soubory. Pokud je nelze vyléčit, zobrazí se výběr akce, která se má provést.

VAROVÁNÍ:
Při detekci infiltrace v archivu, bude při standardním a přísném léčení odstraněn celý archiv. Při standardním léčení bude archiv odstraněn, pouze pokud obsahuje samotný soubor s infiltrací. Při **přísném léčení** bude archiv odstraněn i v případě, že kromě infiltrace obsahuje další korektní soubory.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například *dokument.txt* označuje textový dokument). V této části nastavení ThreatSense nastavíte typy souborů, které chcete vyloučit z kontroly.

Ostatní

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

Kontrolovat alternativní datové proudy (ADS) – alternativní datové proudy (ADS) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho virů je proto využívá jako maskování před případným odhalením.

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

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, do protokolu se zapíší všechny zkontrolované soubory, i když nejsou infikované. Například, při nalezení infiltrace v archivu, se do protokolu zapíší všechny soubory z archivu, i když jsou čisté.

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

Zachovat čas přístupu k souborům – při kontrole souboru nebude změněn čas přístupu, ale bude ponechán původní (vhodné při používání na zálohovacích systémech).

Omezení

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

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota.

Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Standardní hodnota: *neomezeno*.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu objektu. Pokud nastavíte určitou hodnotu, po překročení této hodnoty skončí probíhající antivirová kontrola objektu bez ohledu na to, zda byla dokončena. Objekt může zůstat nezkontrolován. Standardní hodnota: *neomezeno*.

Nastavení archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při antivirové kontrole. Standardní hodnota: *10*.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Standardní hodnota: *neomezeno*.

Poznámka:
Antivirus standardně používá předdefinované hodnoty, které doporučujeme měnit pouze ve zvláštních případech.

4.1.1.6.1 Léčení

Nastavení léčení ovlivňuje chování virové skeneru. K dispozici jsou 3 úrovně léčení detekovaných infikovaných souborů.

4.1.1.6.2 Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například *dokument.txt* označuje textový dokument). V této části nastavení ThreatSense nastavíte, které typy souborů budou kontrolovány.

Standardně jsou kontrolovány všechny soubory. Do seznamu souborů vyloučených z kontroly můžete přidávat libovolné přípony.

Definovat výjimky však doporučujeme pouze v případě potíží s konkrétním programem, který dané typy souborů používá (například .edb, .eml a .tmp pro MS Exchange Server).

Pomocí tlačítka **Přidat** a **Odstranit** můžete povolit nebo zakázat kontrolování vybraných přípon souborů. Pro přidání přípony klikněte na tlačítko **Přidat**, do zobrazeného prázdného pole zadejte příponu a akci potvrďte kliknutím na tlačítko **OK**. Zadat můžete více hodnot oddělené čárkou, středníkem nebo zadejte každou příponu na nový řádek. Vybráním přípony v seznamu a kliknutím na tlačítko **Odstranit** příponu odstraníte ze seznamu. Pro úpravu přípony ji v seznamu vyberte a klikněte na tlačítko **Změnit**.

Pro definování seznamu výjimek použít jako zástupný znak ? (otazník). Otazník (?) reprezentuje jeden znak.

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

4.1.1.7 Nalezena hrozba

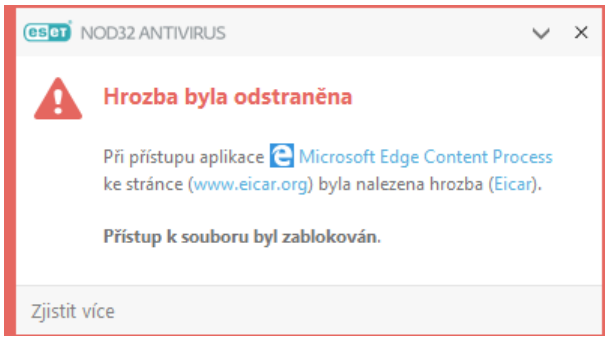
Infiltrace se mohou do počítače dostat z různých zdrojů: z webových stránek, ze sdílených složek, prostřednictvím e-mailu, z výměnných médií (USB klíče, externí disky, CD a DVD, diskety a jiné).

Standardní chování

ESET NOD32 Antivirus dokáže zachytit infiltrace pomocí:

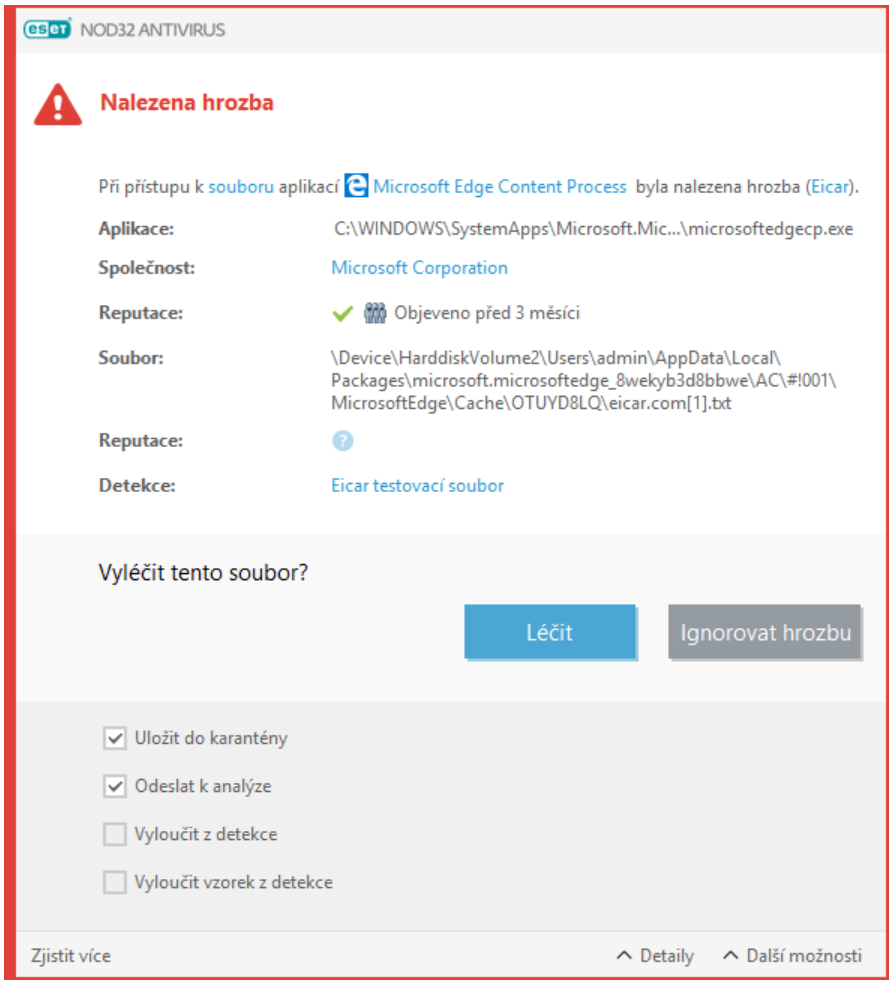
- Rezidentní ochrany souborového systému,
- Ochrany přístupu na web,
- Ochrany poštovních klientů,
- Kontroly počítače.

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



Léčení a mazání

Pokud rezidentní ochrana nemá předdefinovanou akci pro daný typ souboru zobrazí se dialogové okno s výběrem akce. Obvykle jsou dostupné možnosti **Léčit**, **Vymazat** a **Žádná akce**. Výběr možnosti **Žádná akce** nedoporučujeme, protože v tomto případě zůstane infekce nevyléčena. Výjimku tvoří případy, kdy jste si jisti, že je soubor neškodný a byl detekován chybně.



Léčení souboru je možné provést, pokud do zdravého souboru byla zavedena část, která obsahuje škodlivý kód. V tomto případě má smysl pokusit se infikovaný soubor léčit a získat tak původní zdravý soubor. V případě, že infiltrací je soubor, který obsahuje výlučně škodlivý kód, bude odstraněn.

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

Více hrozeb

Pokud infikované soubory nebyly vymazány během kontroly počítače (nebo je Úroveň léčení nastavena na **Neléčit**), zobrazí se dialogové okno s výběrem akce. Vyberte akci, kterou chcete provést (akce se nastavuje individuálně pro každý soubor ze seznamu) a klikněte na **Dokončit**.

Mazání souborů v archivech

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

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

- Otevřete ESET NOD32 Antivirus a přejděte na záložku **Kontrola počítače.**
- Klikněte na **Smart kontrola** (bližší informace naleznete v kapitole Kontrola počítače).
- Po dokončení kontroly se zobrazí protokol, ve kterém je uveden počet zkontrolovaných, infikovaných a vyléčených souborů.

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

4.1.1.8 Ochrana dokumentů

Modul ochrany dokumentů zajišťuje kontrolu dokumentů Microsoft Office před jejich otevřením a také kontroluje automaticky stahované soubory pomocí Internet Explorer, jako například prvky Microsoft ActiveX. Tento modul přidává další bezpečnostní vrstvu do rezidentní ochrany a může být deaktivován pro zvýšení výkonu systému, na kterých neotevíráte velké množství dokumentů Microsoft Office.

Pomocí možnosti **Zapnout ochranu dokumentů** aktivujete systém ochrany dokumentů. Tuto možnost naleznete v **Rozšířeném nastavení** (dostupné po stisknutí klávesy **F5** v hlavním okně programu) v sekci **Detekční jádro** > **Detekce škodlivého kódu** > **Ochrana dokumentů**.

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

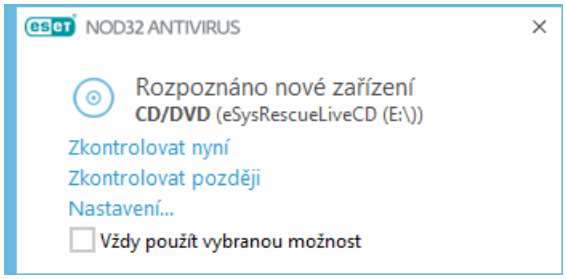
4.1.2 Výměnná média

ESET NOD32 Antivirus dokáže automaticky kontrolovat výměnná média (CD/DVD/USB/...) po jejich připojení/vložení do počítače. Tuto funkci můžete využít pro zvýšení zabezpečení, kdy chcete zabránit uživatelům v připojování médií s infikovaným obsahem.

Akce po vložení výměnného média – vyberte výchozí akci, kterou chcete provést při vložení výměnného média (CD/DVD/USB) do počítače. K dispozici jsou následující akce:

- **Nekontrolovat** – neprovede se žádná akce a nezobrazí se okno s možností výběru akce.
- **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 nastavení výměnných médií.

Kromě toho ESET NOD32 Antivirus disponuje pokročilými funkcemi pro správu zařízení, které vám umožňují definovat pravidla pro zacházení s externími zařízeními. Více informací naleznete v kapitole Správa zařízení.

4.1.3 Správa zařízení

Správa zařízení

Prostřednictvím tohoto modulu dokáže ESET NOD32 Antivirus omezit přístup k výměnných médií (CD/DVD/USB/...). Přístup můžete omezit pouze pro čtení nebo úplně zakázat a pravidla lze aplikovat na konkrétního uživatele nebo celé skupiny uživatelů. Tuto funkci můžete použít v případě, kdy chcete uživatelům například zabránit připojování výměnných médií k počítači.

Podporovaná externí zařízení:

- Datové úložiště (HDD, výměnné USB jednotky),
- CD/DVD,
- USB tiskárna,
- FireWire úložiště,
- Bluetooth zařízení,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port,
- Přenosné zařízení,
- Mikrofon,
- Všechny typy zařízení.

Nastavení správy zařízení můžete upravit v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) > **Správa zařízení**.

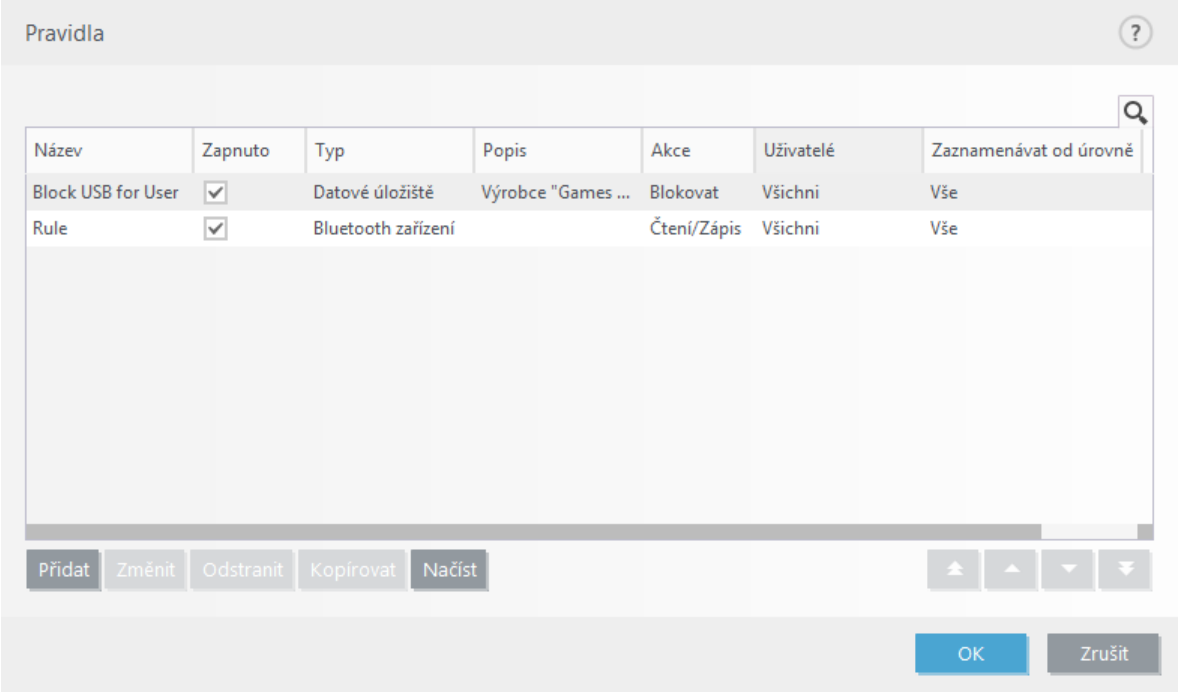
Pomocí přepínače **Integrovat do systému** aktivujete funkci Správa zařízení. Pro provedení změn bude potřeba restartovat počítač. Po aktivaci této funkce se zpřístupní možnost editor pravidel.

Poznámka:
Na každou vytvořenou skupinu zařízení můžete aplikovat rozdílná pravidla. Blokovat všechna neznámá zařízení můžete tak, že si nejprve vytvoříte skupinu důvěryhodných zařízení. Na tuto skupinu aplikujete pravidlo pro čtení a zápis, případně jen pro čtení. Poté vytvořte druhé pravidlo, které bude blokovat přístup k zařízení.

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.

4.1.3.1 Pravidla správy zařízení

Editor pravidel správy zařízení zobrazuje seznam všech existujících pravidel, které umožňují detailní kontrolu nad zařízeními připojovanými k počítači.



Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování.

Pro správu pravidel klikněte na **Přidat** nebo **Změnit**. Stisknutím klávesy **CTRL** a kliknutím můžete vybrat více pravidel najednou a provést hromadné akce. Pomocí zaškrtávacího pole ve sloupci **Zapnuto** dané pravidlo zapnete nebo vypnete. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

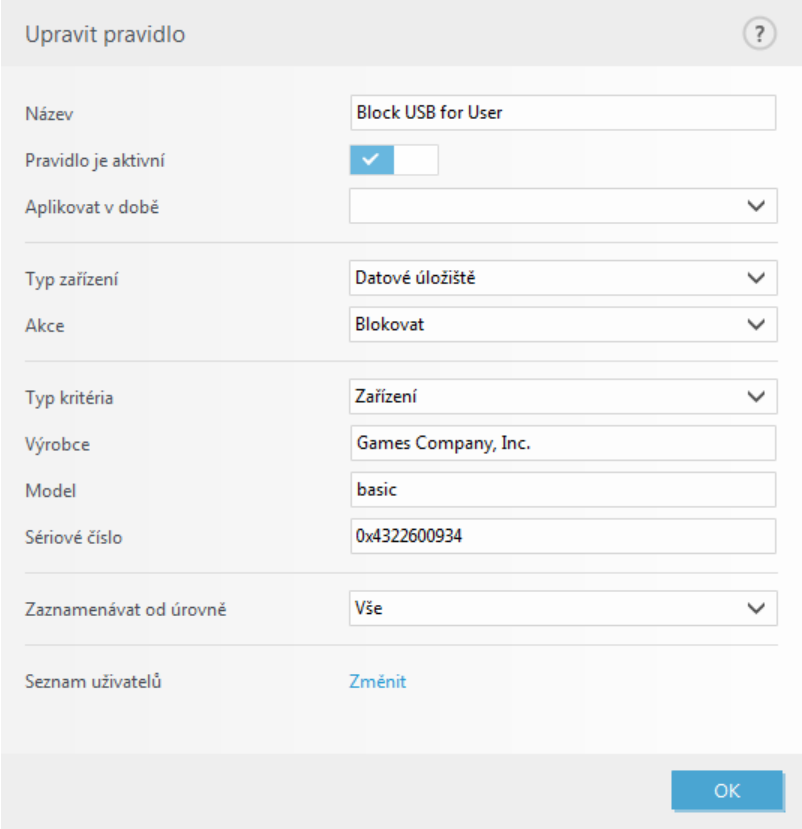
Pravidla jsou vyhodnocována na základě priority. Pravidlo s nejvyšší prioritou je umístěno v seznamu na prvním místě. Pravidla vztažená na URL mají vždy vyšší prioritu než pravidla vztažená na kategorii adres. Například, pravidlo na URL umístěné v seznamu níže, než pravidlo na kategorii, bude vyhodnoceno jako první.

Protokoly si můžete kdykoli prohlédnout v hlavním okně programu ESET NOD32 Antivirus po kliknutí na **Nástroje** > Protokoly.

Do protokolu správy zařízení se zapíší informace o všech připojených zařízeních. Kliknutím na tlačítko **Načíst** se automaticky načtou parametry všech připojených výměnných zařízení připojených k počítači.

4.1.3.2 Vytvoření nového pravidla

V tomto okně můžete definovat akce, které se provedou po připojení daného zařízení k počítači.



Pro lepší přehlednost do pole **Název** zadejte jméno pravidla. Zaškrtnutím možnosti **Pravidlo je aktivní** dané pravidlo povolíte. Pokud ponecháte tuto možnost neaktivní, pravidlo se nebude uplatňovat a můžete jej použít v budoucnu.

Typ zařízení

Z rozbalovacího menu vyberte typ zařízení (diskové úložiště/přenosné zařízení/Bluetooth/FireWire/...). Typy zařízení se přebírají ze systému a můžete si je prohlídnout v systémovém Správci zařízení, který poskytuje informace o zařízeních připojených k počítači. Možnost Optická média představuje data uložená na optických médiích jako jsou CD nebo DVD. 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.

Mějte na paměti, že uvedené akce nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze dvě akce (například akce **Pouze pro čtení** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zakázán).

Typ kritéria – vyberte, zda chcete pravidlo vytvořit pro jednotlivé zařízení nebo skupinu zařízení.

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se 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.

Poznámka:
Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Filtrování parametrů rozlišuje velikost písmen a nepodporuje 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. Protokol naleznete v hlavním okně programu v sekci **Nástroje** > **Protokoly**, kde z rozbalovacího menu vyberte možnost **Správa zařízení**

Zaznamenávat do protokolu

- **Vše** – zaznamenají se všechny události.
- **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.
- **Žádné** – nebudou zaznamenávány žádné události nevytvoří se žádné protokoly.

Pravidla můžete přiřadit konkrétnímu uživateli nebo celé skupině uživatelů pomocí dialogového okna **Seznam uživatelů**.

- **Přidat** – otevře okno **Vybrat typ objektu: Uživatelé nebo Skupiny**, kde můžete vybrat konkrétní uživatele.
- **Vymazat** – odebere vybraného uživatele ze seznamu.

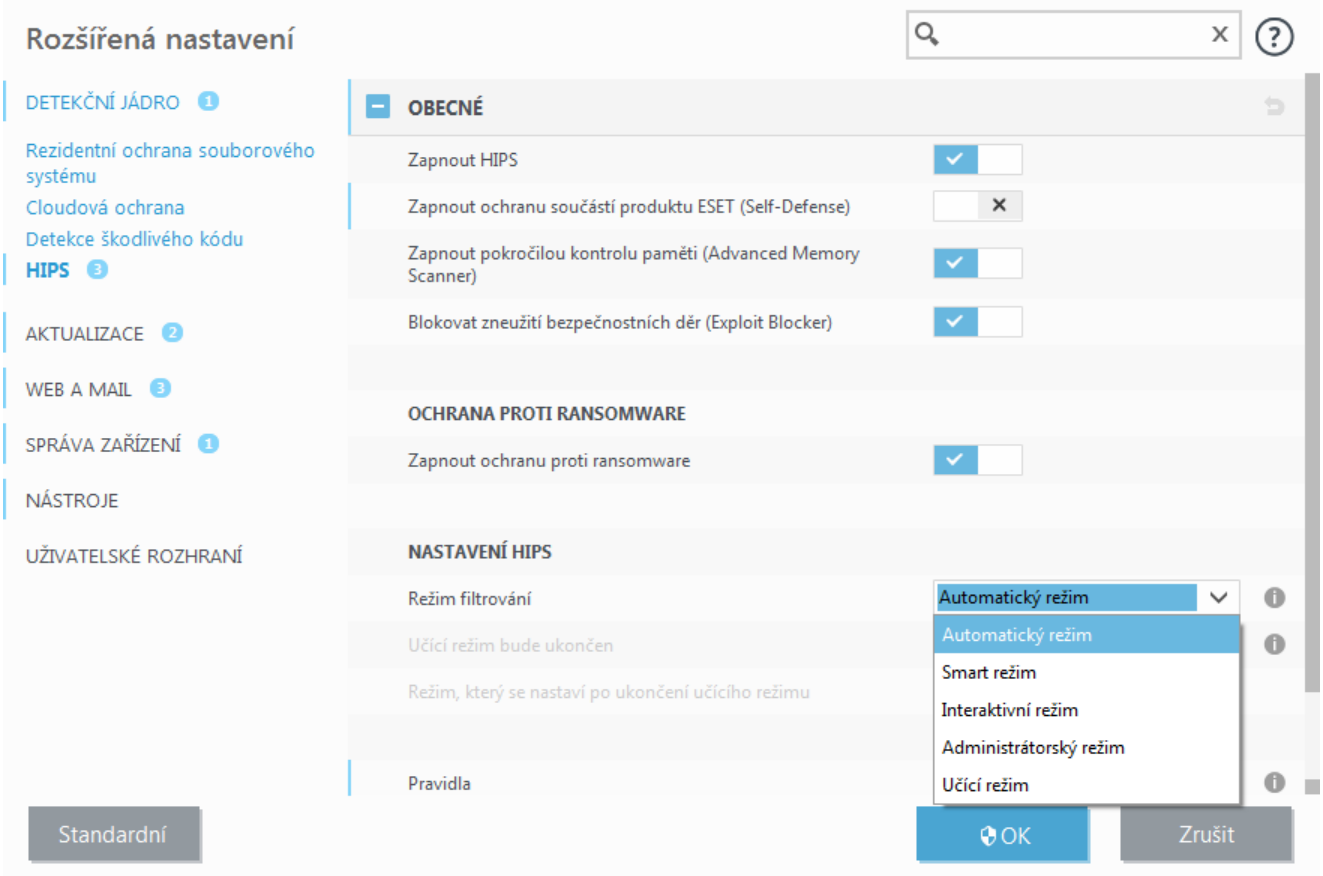
Poznámka:
Mějte na paměti, že není možné omezit všechna zařízení. Například zobrazovací zařízení neposkytují žádné informace o uživateli, pouze vyvolávají akci.

4.1.4 HIPS

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

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

Nastavení HIPS naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5**) na záložce **Detekční jádro** > **HIPS**. Stav ochrany HIPS je zobrazen v hlavním okně ESET NOD32 Antivirus na záložce **Nastavení** v sekci **Ochrana počítače**.



ESET NOD32 Antivirus má vestavěnou technologii *Self-Defense*, která brání škodlivé aplikaci v narušení nebo zablokování antivirové ochrany. *Self-Defense* chrání soubory a klíče v registru, které jsou kritické pro správnou funkci ESET NOD32 Antivirus 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 – pomocí této možnosti aktivujete ochranu jádra produktu pomocí systémových prostředků. Tato možnost je dostupná na Windows 8.1 a 10.

Zapnout pokročilou kontrolu paměti (Advanced Memory Scanner) – tato funkce v kombinaci s blokováním zneužití bezpečnostních děr poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Pro více informací se podívejte do slovníku pojmů.

Blokovat zneužití bezpečnostních děr (Exploit Blocker) – tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, pdf čtečky). Tato funkce je standardně zapnuta. Pro více informací se podívejte do slovník pojmů.

Zapnout ochranu proti ransomware – tato součást představuje další vrstvu do modulu HIPS a je plně funkční pouze s aktivní technologií ESET LiveGrid. Více informací o tomto typu ochrany naleznete ve slovníku pojmů.

HIPS může běžet v jednom z následujících režimů:

Automatický režim – operace budou povoleny s výjimkou předdefinovaných pravidel,

Interaktivní režim – uživatel bude na povolení či zakázání operace dotázán,

Administrátorský režim – operace jsou zablokované s výjimkou definovaných pravidel.

Smart režim – uživatel bude upozorněn pouze na podezřelé operace,

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 **Upozornit na ukončení učícího**

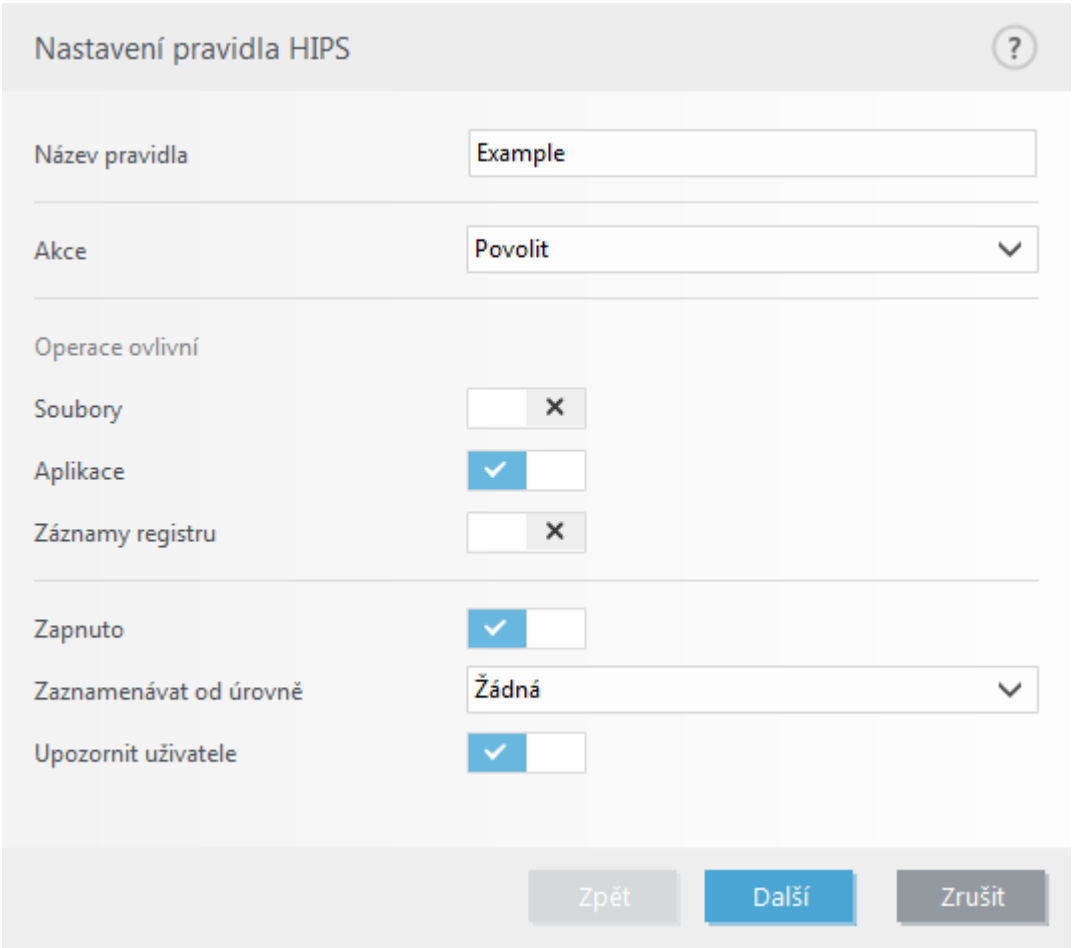
režimu za X dní. Po této nastavené době se učící režim automaticky ukončí. Maximální počet dní je 14. Po uplynutí tohoto času se zobrazí dialog, ve kterém je možné upravovat pravidla a následně musíte vybrat jiný režim systému HIPS.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte režim filtrování, který se automaticky nastaví po ukončení běhu učícího režimu.

Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům firewallu. Kliknutím na **Změnit** vedle položky Pravidla otevřete Editor pravidel systému HIPS, kde můžete pravidla prohlížet, vytvářet nová, upravovat nebo odstranit stávající.

Na následujícím příkladu si ukážeme, jak omezit nežádoucí chování aplikací:

1. Zadejte název pravidla a vyberte akci **Zablokovat** z rozbalovacího menu **Akce**,
2. Vyberte možnost **Upozornit uživatele** pro zobrazení upozornění při každém aplikování pravidla.
3. Vyberte alespoň jednu operaci, pro kterou má pravidlo platit.
4. Přejděte na záložku **Cílové aplikace**. Záložku **Zdrojové aplikace** nechte prázdnou, aby se nové pravidlo uplatnilo pro všechny aplikace, které se pokoušejí vykonat vybrané **Operace** v aplikacích uvedených v části **Nad těmito aplikacemi**,
5. Vyberte operaci **Změnit stav jiné aplikace** (všechny operace jsou popsány v nápovědě produktu, kterou vyvoláte stisknutím **klávesy F1**).
6. Pomocí tlačítka **Přidat...** přidejte jednu nebo více aplikací, které chcete ochránit,
7. Klikněte na **OK** pro uložení nového pravidla.



4.1.4.1 Rozšířená nastavení

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

Automaticky povolené ovladače – vybrané ovladače budou vždy načteny bez ohledu na nastavený režim filtrování, pokud nejsou blokovány uživatelským pravidlem.

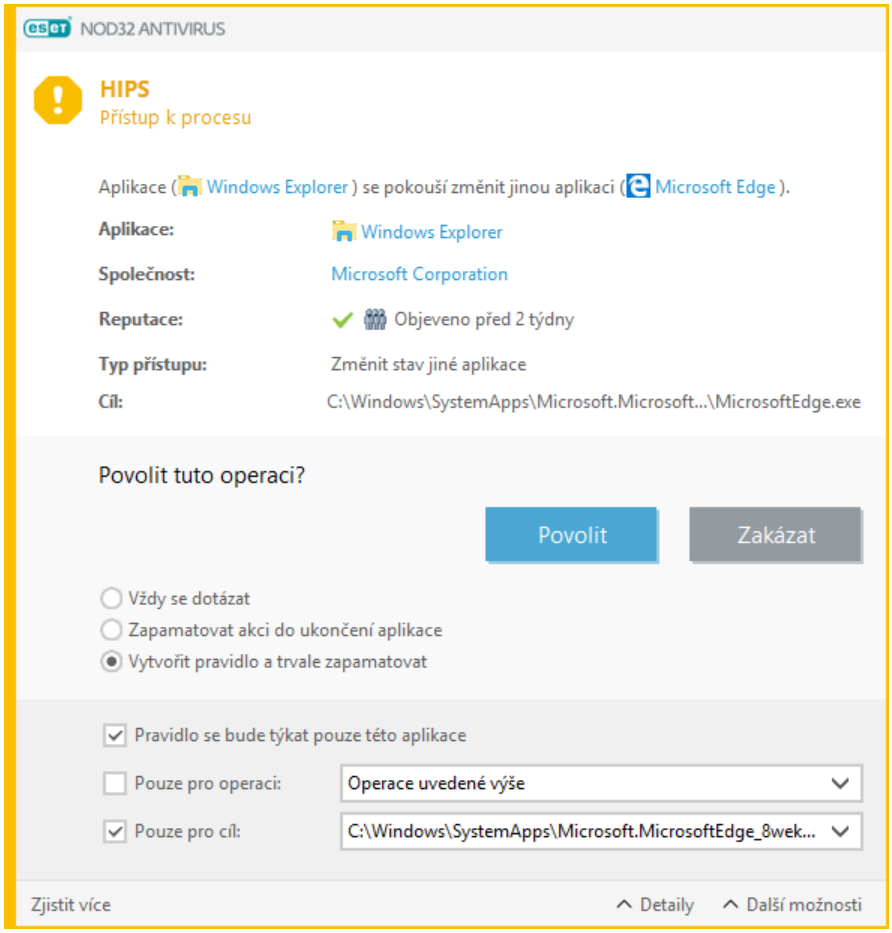
Zapisovat všechny zablokované operace do protokolu – všechny zablokované operace se zapíší do protokolu HIPS.

Upozornit na změny v seznamu aplikací automatický spouštěných při startu – při změně počtu aplikací spouštěných po startu operačního systému se zobrazí oznámení.

Nejaktuálnější verzi této nápovědy naleznete v Databázi znalostí.

4.1.4.2 Interaktivní režim HIPS

Dialogové okno s výběrem akce se zobrazí pokaždé, když je pro událost vybrána akce **Dotázat se**. Umožňuje vybrat, zda chcete operaci **Povolit** nebo **Zakázat**. Pokud nevyberete žádnou akci, použije se standardní pravidlo z již předdefinovaných.

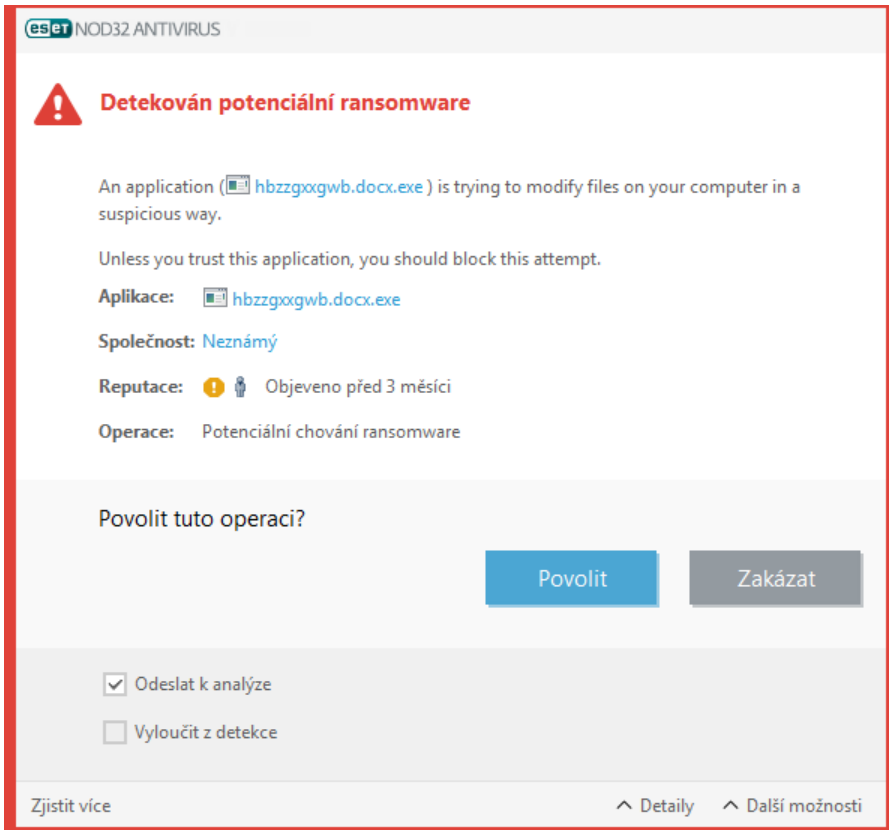


Dialogové okno s výběrem akce umožňuje vytvoření pravidla, které má vlastnosti podle operace, která vyvolala tento dialog. Přesné parametry nového pravidla můžete nastavit po kliknutí na **Zobrazit nastavení**. Takto vytvořená pravidla se vyhodnocují stejně, jako kdyby byla zadána ručně, přesto může být pravidlo vytvořené pomocí dotazu méně specifické. To znamená, že po vytvoření pravidla může stejná operace znovu vyvolat dialogové okno, pokud se parametry z předchozího pravidla nevztahují na tuto situaci.

Aktivovaná možnost **Dočasně si zapamatovat akci pro tento proces** způsobí, že se vybraná akce (**Povolit** nebo **Zakázat**) zapamatuje pro tento proces, a použije se pokaždé, kdyby se pro operaci tohoto procesu měl zobrazit další dotazovací dialog. Tato nastavení jsou jen dočasná, platí pouze do nejbližší změny pravidel, režimu filtrování, aktualizaci modulu HIPS nebo restartu systému.

4.1.4.3 Detekován potenciální ransomware

Toto dialogové okno se zobrazí, pokud ESET NOD32 Antivirus detekuje aplikaci, jejíchž chování je velmi podobné ransomware. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**.



Po kliknutí na možnost **Detaily** můžete odeslat vzorek do virové laboratoře k bližší analýze, případně danou aplikaci vyloučit z detekce.

Důležité:
Pro fungování ochrany proti ransomware je vyžadována aktivní technologie ESET LiveGrid.

4.1.5 Herní režim

Herní režim je funkce navržená pro uživatele, kteří nechtějí být nejen v režimu celé obrazovky rušeni vyskakujícími okny a chtějí minimalizovat veškeré nároky na zatížení procesoru. Herní režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami antiviru. Zapnutím této funkce zakážete zobrazování všech vyskakujících oken a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

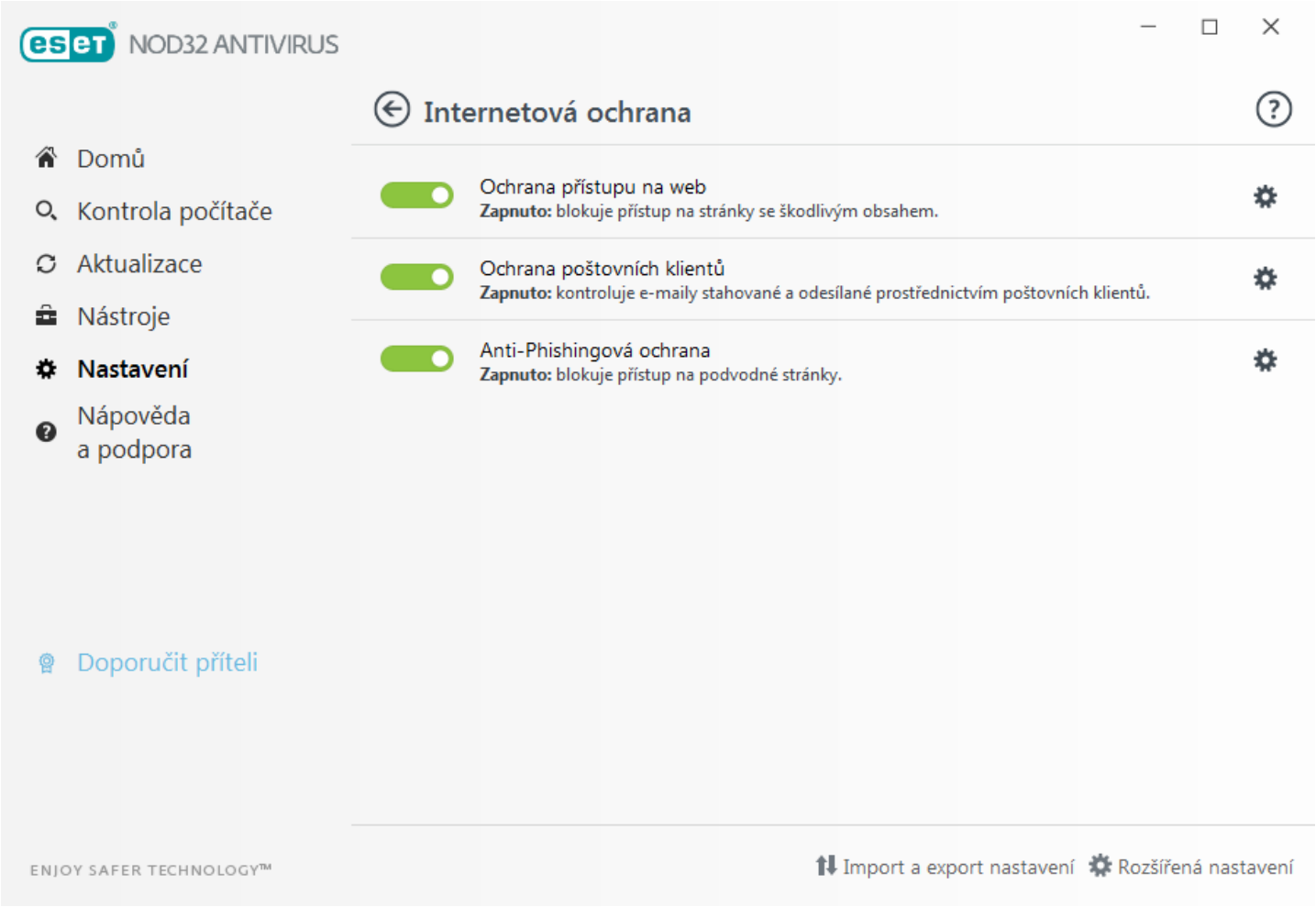
Herní režim můžete zapnout nebo vypnout v hlavním okně na záložce **Nastavení** > **Ochrana počítače** prostřednictvím přepínače resp. . Zapnutí herního režimu může představovat potenciální bezpečnostní riziko, a proto se ikonka ochrany na liště změní na oranžovou a v hlavním okně programu se zobrazí upozornění **Herní režim je zapnutý**.

Vybráním možnosti **Automaticky zapnout Herní režim při zobrazení aplikací na celou obrazovku** se Herní režim automaticky zapne po spuštění aplikace na celou obrazovku a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování Herního režimu po spuštění hry nebo zahájení prezentace a najdete si v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) v sekci **Nástroje** > **Herní režim**.

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

4.2 Internetová ochrana

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



Internetové připojení patří do standardní výbavy osobních počítačů a bohužel se stalo i hlavním médiem pro šíření škodlivého kódu. Proto je velmi důležité věnovat zvýšenou pozornost nastavení ochrany přístupu na web.

Pro zobrazení nastavení webové/e-mailové/anti-phishingové ochrany klikněte na ikonu ozubeného kolečka .

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Pomocí zásuvných modulů do poštovních klientů zajišťuje ESET NOD32 Antivirus kontrolu veškeré komunikace těchto programů (POP3, MAPI, IMAP, HTTP).

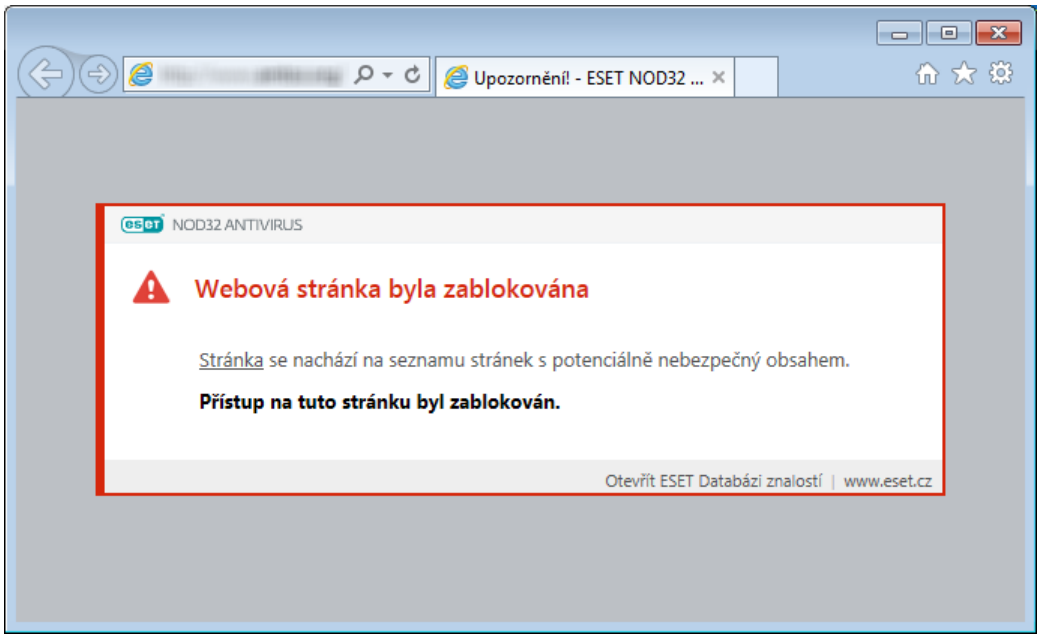
Anti-Phishingová ochrana blokuje webové stránky, na kterých se nachází podvodný obsah. Doporučujeme ponechat anti-phishingovou ochranu zapnutou.

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

4.2.1 Ochrana přístupu na web

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

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



Důrazně doporučujeme mít funkci Ochrana přístupu na web zapnutou. Podrobné možnosti konfigurace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně ESET NOD32 Antivirus) na záložce **Web a mail** > **Ochrana přístupu na web**. Pokud je tato možnost zapnutá, známé stránky se škodlivým obsahem budou blokovány.

Dostupné jsou následující možnosti:

- Webové protokoly – umožňuje konfigurovat monitorování standardních protokolů používaných internetovými prohlížeči,
- Správa URL adres – umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly,
- Parametry skenovacího jádra ThreatSense – nabízí pokročilé nastavení kontroly jako jsou cíle kontroly, metody detekce ochrany přístupu na web apod.

4.2.1.1 Obecné

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

Zapnout rozšířenou kontrolu skriptů v prohlížeči – pokud je tato možnost zapnutá, automaticky budou kontrolovány všechny JavaScriptové programy spouštěné internetovým prohlížečem.

Poznámka:
V rámci zajištění bezpečnosti nedoporučujeme ochranu přístupu na web vypínat. Tuto možnost vypněte pouze při řešení problému, pokud vás k tomu vyzval specialista technické podpory.

4.2.1.2 HTTP, HTTPs

Standardně je ESET NOD32 Antivirus nakonfigurován pro používání norem většiny internetových prohlížečů. Přesto je možné kontrolu HTTP konfigurovat v rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Ochrana přístupu na web** > **HTTP, HTTPs**. Zde můžete kontrolu aktivovat nebo deaktivovat a dále definovat čísla portů, na kterých v systému probíhá HTTP komunikace. Standardně jsou přednastaveny porty 80 (HTTP), 8080 a 3128 (pro proxy server).

ESET NOD32 Antivirus podporuje také kontrolu šifrované komunikace HTTPs. Při této komunikací jsou přenášené údaje mezi serverem a klientem zašifrované. Kontrolována je komunikace šifrovaná pomocí SSL (Secure Socket Layer) nebo TLS (Transport Layer Security). Šifrovanou HTTPs komunikaci je možné filtrovat ve dvou režimech:

Nepoužívat kontrolu protokolu HTTPs – šifrovaná komunikace nebude kontrolována,

Používat kontrolu protokolu HTTPs pro vybrané porty – kontrolována bude pouze komunikace na portech definovaných v sekci Weboví a poštovní klienti a používají porty definované v sekci **Porty používané protokolem HTTPs**. Standardně se kontroluje komunikace na portu 443.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout filtrování protokolu SSL/TLS**.

4.2.1.3 Správa URL adres

Správa URL adres umožňuje 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.

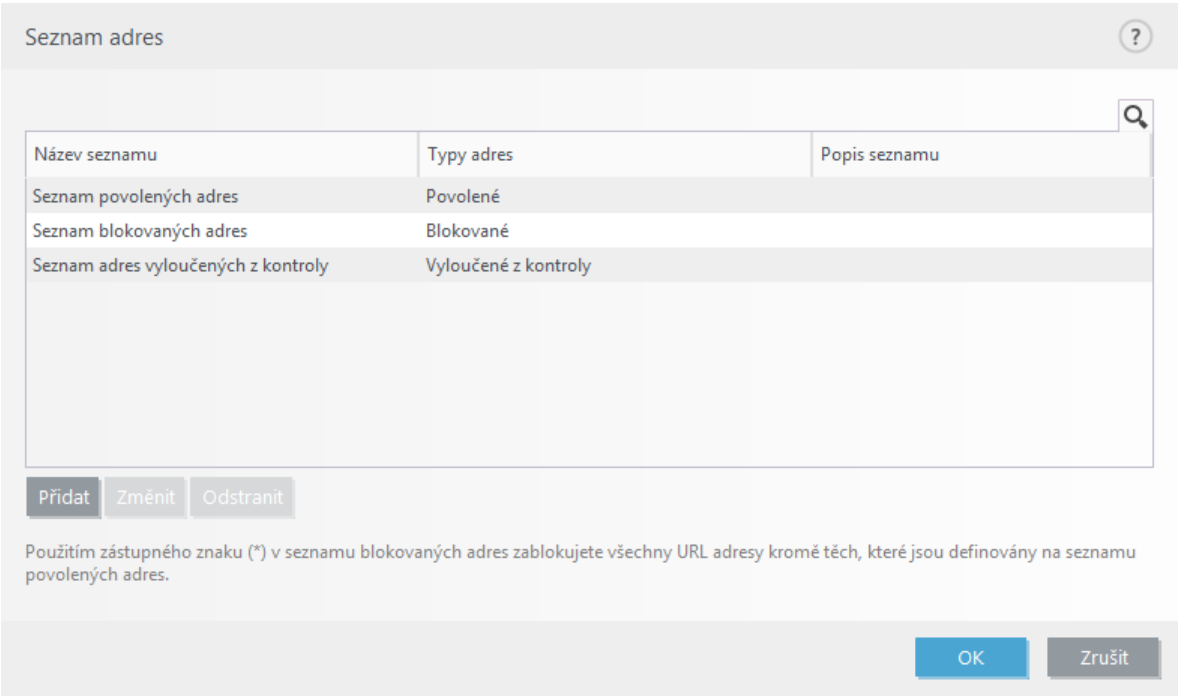
Možnost Zaplnout filtrování protokolu SSL/TLS musí být aktivní, pokud chcete filtrovat HTTPS adresy. V opačném případě by byl zakázán pouze přístup na nešifrovanou verzi webové stránky.

Pro vyloučení konkrétní adresy z kontroly přidejte danou adresou stránky na **Seznam adres vyloučených z kontroly**.

Pokud chcete zablokovat všechny HTTP adresy kromě těch definovaných na **Seznamu povolených adres**, zadejte do seznamu blokovaných adres * (hvězdičku).

V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám a proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu. Pro více informací, jak bezpečně přidat celou doménu včetně jejich subdomén přejděte do kapitoly Přidání masky adresy/domény. Pro aktivování seznamu vyberte možnost **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit zobrazení upozornění zaškrtnutím možnosti **Upozornit při aplikování adresy ze seznamu**.

Poznámka:
Pomocí seznamů adres můžete blokovat také stahování konkrétních typů souborů. Pokud chcete například zablokovat stahování spustitelných souborů z internetu, přidejte do seznamu blokovaných adres masku "**.exe".



Ovládací prvky

Přidat – umožňuje vytvořit nový seznam. To je užitečné, pokud chcete adresy rozdělit do logických skupin. Například jeden seznam blokovaných adres může obsahovat adresy z veřejných blacklistů, a druhý vámi definované adresy. V takovém případě je správa seznamu externích adres mnohem snadnější.

Změnit – upraví existující seznam adres.

Odstranit – odebere existující seznam. Toto platí pouze na ručně vytvořené seznamy, nikoli předdefinované.

4.2.2 Ochrana poštovních klientů

4.2.2.1 Poštovní klienti

Integrace ESET NOD32 Antivirus do poštovních klientů zvyšuje úroveň ochrany před škodlivým kódem obdrženým prostřednictvím e-mailových zpráv. Pokud používáte poštovního klienta, který ESET NOD32 Antivirus podporuje, je vhodné integraci povolit. Při integraci dochází k vložení panelu nástrojů programu ESET NOD32 Antivirus do poštovního klienta (panel nástrojů není dostupný pro nejnovější verze Windows Live Mail), což přispívá k efektivnější kontrole e-mailových zpráv. Konkrétní možnosti integrace naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Ochrana poštovních klientů** > **Poštovní klienti**.

Integrace s poštovními klienty

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 je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Úplný seznam dostupných poštovních klientů a jejich verzí naleznete v ESET Databázi znalostí.

Pokud není nastavena integrace, e-mailová komunikace je stále chráněna modulem ochrany poštovních klientů (POP3, IMAP).

Možnost **Vypnout kontrolu při změně obsahu složek s doručenou poštou** doporučujeme použít v případě, že pociťujete zpomalení při práci s poštovním klientem Microsoft Outlook. Uvedená situace může nastat například, že přijímáte zprávy z úložiště zpráv prostřednictvím Kerio Outlook Connector.

Kontrolovat tyto zprávy

Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta – pokud deaktivujete tuto možnost, kontrolu pošty bude nadále zajišťovat modul filtrování protokolů.
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 přesouvat infikované zprávy.

Opakovat kontrolu po aktualizaci – zapne/vypne opakovanou kontrolu zpráv po aktualizaci detekčních modulů.
Zohlednit výsledky kontroly jiných modulů – zapne/vypne zohlednění výsledku kontroly jiným modulem.

Poznámka:
Doporučujeme ponechat zapnutou **ochranu prostřednictvím doplňku do poštovního klienta** i poštovní **ochranu prostřednictvím modulu filtrování protokolů**.

4.2.2.2 Poštovní protokoly

Protokol POP3 a IMAP je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET NOD32 Antivirus zajišťuje ochranu těchto protokolů na standardních protokolech (POP3 – 110, IMAP – 143) zcela nezávisle na používaném poštovním klientovi.V případě potřeby můžete v nastavení definovat další porty.

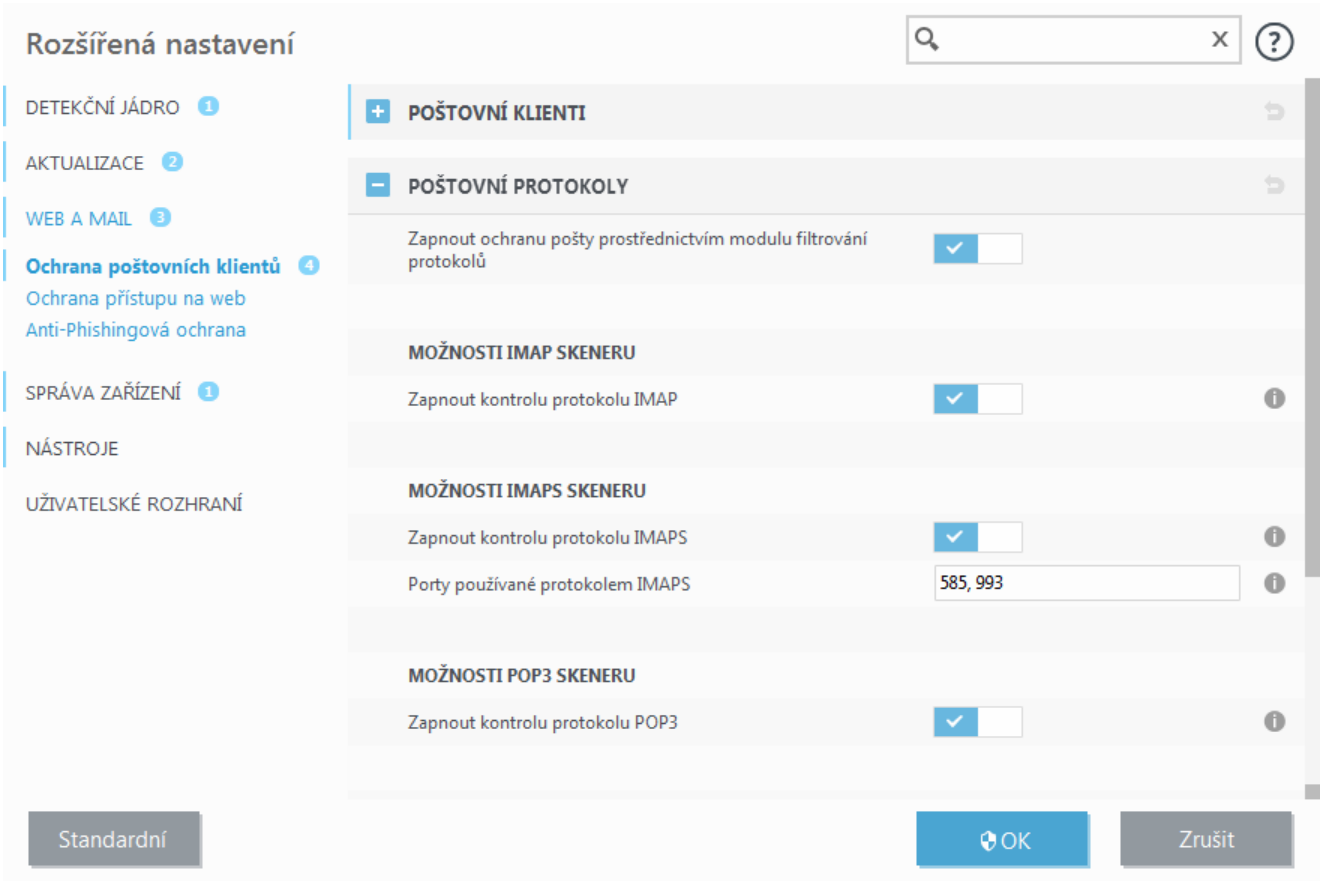
Konfiguraci kontroly protokolu IMAP/IMAPS a POP3/POP3S naleznete v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Ochrana poštovních klientů** > **Poštovní protokoly**. Pro zapnutí tohoto modulu použijte přepínač **Zapnout poštovní ochranu prostřednictvím modulu filtrování protokolů**.

Ve Windows Vista a novějších je komunikace na protokolech IMAP a POP3 automaticky zjišťována a kontrolována na všech portech. Ve Windows XP jsou kontrolovány pouze definované **Porty používané protokolem IMAP/POP3** a aplikace označené jako Weboví a poštovní klienti.

ESET NOD32 Antivirus podporuje kontrolu protokolů IMAPS a POP3S, které používají šifrovaný kanál pro výměnu informací mezi klientem a serverem. ESET NOD32 Antivirus 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.

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 **Filtrování protokolů** > Kontrola protokolu SSL/TLS a aktivujte možnost **Zapnout filtrování protokolu SSL/TLS**.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout filtrování protokolu SSL/TLS**.



4.2.2.3 Upozornění a události

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Pomocí zásuvného doplňku do Microsoft Outlook a dalších e-mailových klientů je zajištěna kontrola veškeré komunikace (POP3, MAPI, IMAP, HTTP). Při kontrole přijímaných zpráv jsou použity veškeré pokročilé metody kontroly obsažené ve skenovacím jádře ThreatSense. Tím je zajištěna detekce nebezpečných programů v přílohách e-mailů ještě před tím, než by vzorek byl součástí detekčního jádra. Kontrola protokolu POP3 a IMAP je nezávislá na používaném poštovním klientovi.

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

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do přijatých a čtených 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 viry. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy. Možná nastavení jsou následující:

- **Nepřidávat do zpráv** – 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. Zároveň zvyšuje důvěryhodnost zprávy a v případě výskytu infiltrace nabízí cenné informace o úrovni hrozby pro příjemce i odesílatele.

Šablona přidávaná do předmětu infikovaných zpráv – upravte tuto šablonu, pokud chcete změnit formát předpony předmětu infikovaného e-mailu. Tato funkce přidá k původnímu předmětu zprávy "Ahoj" předponu "*[virus]*" a výsledný předmět bude: "*[virus] Ahoj*". Proměnná *%VIRUSNAME%* představuje detekovanou hrozbou.

4.2.2.4 Integrace s poštovními klienty

Integrace ESET NOD32 Antivirus s poštovními klienty zvyšuje úroveň aktivní ochrany před škodlivým kódem obsaženým v e-mailových zprávách. V případě, že je daný poštovní klient podporován, je vhodné povolit jeho integraci s ESET NOD32 Antivirus. Při integraci dochází k vložení panelu nástrojů programu ESET NOD32 Antivirus do poštovního klienta, což přispívá k efektivnější kontrole e-mailových zpráv. Konkrétní možnosti integrace jsou dostupné v **Rozšířeném nastavení** (po stisknutí **klávesy F5** v hlavním okně programu) ve větvi **Web a mail** > **Ochrana poštovních klientů** > **Integrace s poštovními klienty**.

V tomto dialogu je možné aktivovat integraci s podporovanými poštovními klienty, kterými v současné verzi jsou Microsoft Outlook, Outlook Express, Windows Mail a Windows Live Mail. Pro kompletní výpis podporovaných klientů a jejich verzí si přečtěte článek v ESET Databázi znalostí.

Možnost **Vypnout kontrolu při změně obsahu složek s doručenou poštou** doporučujeme použít v případě, že pociťujete zpomalení při práci s poštovním klientem Microsoft Outlook. Uvedená situace může nastat například, že přijímáte zprávy z úložiště zpráv prostřednictvím Kerio Outlook Connector.

Pokud není vybrána integrace, e-mailová komunikace bude chráněna modulem ochrany poštovních klientů (POP3, IMAP).

4.2.2.4.1 Nastavení ochrany 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 je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované.

4.2.2.5 Kontrola protokolu POP3, POP3s

Protokol POP3 je nejrozšířenější protokol určený pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET NOD32 Antivirus zajišťuje ochranu tohoto protokolu nezávisle na používaném klientovi.

Modul zajišťující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování ověřte, zda je modul zapnutý. Kontrola protokolu POP3 je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110, v případě potřeby je možné přidat i jiný používaný port. Čísla portů se oddělují čárkou.

Šifrovaná komunikace se standardně nekontroluje. Pro aktivování kontroly šifrované komunikace přejděte do sekce Kontrola protokolu SSL/TLS v Rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu). Následně na záložce **Web a mail** > **Filtrování protokolů** > **SSL** zaškrtněte možnost **Zapnout filtrování protokolu SSL/TLS**.

V této sekci můžete nastavit kontrolu protokolů POP3 a POP3s.

Aktivovat kontrolu protokolu POP3 – zapne sledování poštovní komunikace přes POP3 na přítomnost škodlivého softwaru.

Porty používané protokolem POP3 – nastavení kontrolovaných portů poštovní komunikace přes POP3 (standardně 110).

ESET NOD32 Antivirus také podporuje kontrolu protokolu POP3s. Při této komunikaci jsou přenášeny údaje mezi serverem a klientem přes šifrovaný kanál. ESET NOD32 Antivirus kontroluje komunikaci šifrovanou metodami SSL (Secure Socket Layer) a TLS (Transport Layer Security).

Nepoužívat kontrolu protokolu POP3s – šifrovaná komunikace nebude kontrolována.

Používat kontrolu protokolu POP3s pro vybrané porty – kontrolovaná bude pouze komunikace přes porty definované v nastavení **Porty používané protokolem POP3s.**

Porty používané protokolem POP3S – nastavení kontrolovaných portů poštovní komunikace přes POP3s (standardně 995).

4.2.3 Filtrování protokolů

Antivirová ochrana aplikačních protokolů je prováděna prostřednictvím skenovacího jádra ThreatSense, které obsahuje všechny pokročilé metody detekce škodlivého softwaru. Kontrola pracuje zcela nezávisle na použitém internetovém prohlížeči, nebo poštovním klientovi. Pro kontrolu šifrované komunikace (SSL) přejděte do sekce **Web a mail** > **Kontrola protokolu SSL/TLS**.

Zapnout kontrolu obsahu aplikačních protokolů – pokud tuto možnost vypnete některé, moduly ESET NOD32 Antivirus, které závisí na této funkci (například Ochrana přístupu na web, Ochrana poštovních klientů, Anti-Phishing, Filtrování obsahu webu), nebudou fungovat.

Vyloučené aplikace – umožňuje vyloučit konkrétní aplikaci z filtrování protokolů. To může být užitečné při řešení problémů.

Vyloučené IP adresy – umožňuje vyloučit konkrétní adresu z filtrování protokolů. To může být užitečné při řešení problémů

Internetové prohlížeče a poštovní klienti – Tato možnost je dostupná pouze na operačním systému XP/2003 a umožňuje vybrat aplikace jejichž komunikace bude filtrována, bez ohledu na používaný port.

4.2.3.1 Weboví a poštovní klienti

Poznámka:
Na systémech Windows Vista s nainstalovaným Service Packem 1, Windows 7 a Windows Server 2008 je použit odlišný způsob kontroly komunikace (je využita nová architektura Windows Filtering Platform), než na starších systémech. Z tohoto důvodu není nastavení **Weboví a poštovní klienti** na těchto systémech dostupné.

Bezpečnost při prohlížení webových stránek je vzhledem k velkému množství škodlivého kódu důležitou součástí ochrany počítače. Zranitelnosti prohlížečů a podvodné odkazy dokáží zavést škodlivý kód do systému bez vědomí uživatele. Z tohoto důvodu je v ESET NOD32 Antivirus věnována pozornost bezpečnosti internetových prohlížečů. Každá aplikace, která přistupuje k síti, může být označena jako internetový prohlížeč. Zaškrtávací pole má dva stavy:

- **Prázdné** – komunikace této aplikace se sítí je filtrována pouze podle portů.
- **Označeno fajfkou** – komunikace této aplikace se sítí je filtrována vždy (i v případě, že je nastaven jiný port).

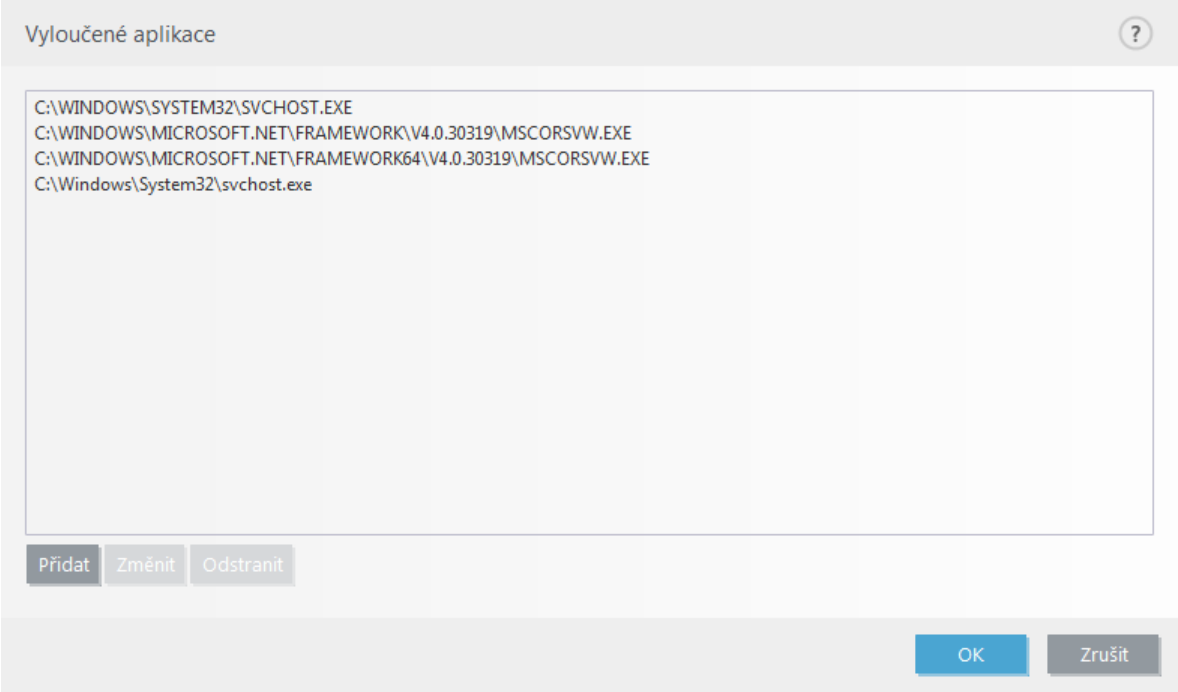
4.2.3.2 Vyloučené aplikace

V tomto dialogovém okně vyberte aplikace, které chcete vyloučit z kontroly filtrování protokolů. HTTP, POP3 a IMAP komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze ve výjimečných případech, například pokud aplikace v důsledku kontroly komunikace nepracuje správně.

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

Změnit – upraví existující aplikaci.

Odstranit – odebere vybranou aplikaci ze seznamu.



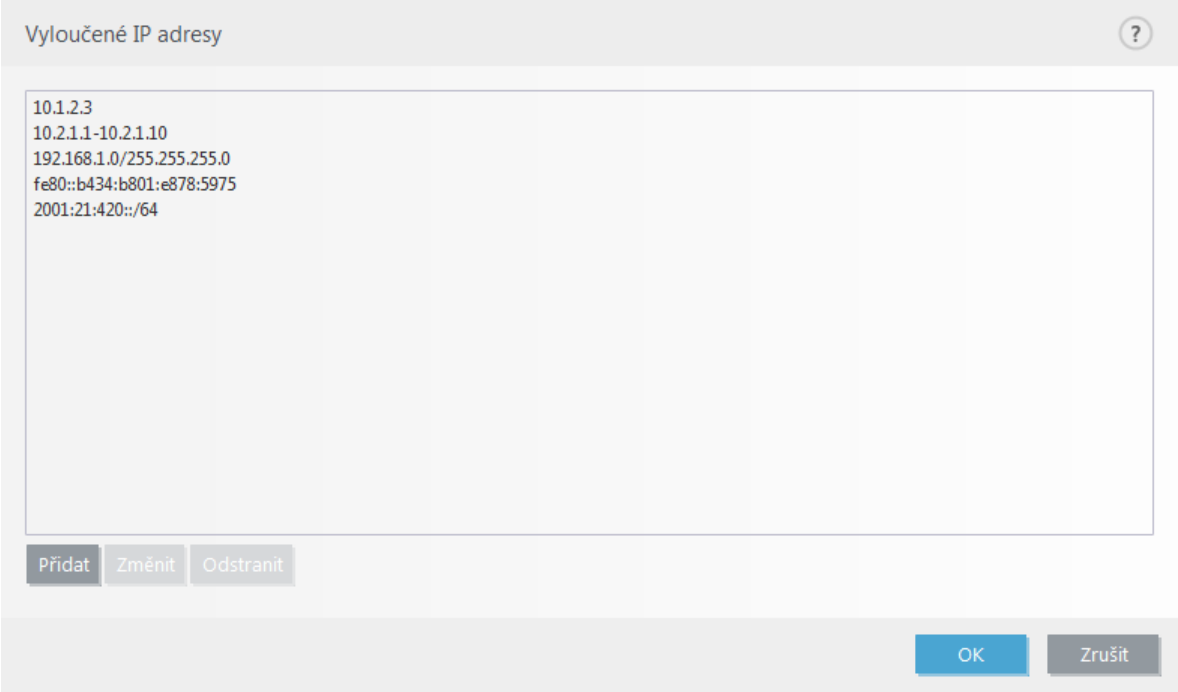
4.2.3.3 Vyloučené IP adresy

IP adresy uvedené v tomto seznamu budou vyloučeny z filtrování protokolů. Oboustranná komunikace protokolů HTTP, POP3 a IMAP z těchto IP adres nebude kontrolována na hrozby. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany, kterou chcete vyloučit z filtrování.

Změnit – upraví existující IP adresu v seznamu.

Odstranit – odebere vybrané IP adresy ze seznamu.



4.2.3.3.1 Přidání adresy IPv4

Umožní přidání IP adresy/rozsahu adres/podsítě vzdáleného zařízení, pro které budou daná pravidla aplikována. Internetový protokol (IP) verze 4 je starší než IPv6, ale v současnosti je stále nejrozšířenější.

Samostatná adresa – slouží pro zadání samostatné adresy počítače, pro který má pravidlo platit (například *192.168.0.10*).

Rozsah adres – vytvoří pravidla pro více počítačů po zadání rozsahu IP adres těchto počítačů, pro které má pravidlo platit (například *192.168.0.1* až *192.168.0.99*).

Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky.

PŘÍKLAD: *255.255.255.0* je maska podsítě pro prefix *192.168.1.0/24*, což znamená rozsah adres od *192.168.1.1* do *192.168.1.254*.

4.2.3.3.2 Přidání IPv6 adresy

Umožní přidání IPv6 adresy/podsítě vzdáleného zařízení, pro které budou daná pravidla aplikována. Tato nejnovější verze Internetového Protokolu (IP) nahrazuje starší verzi 4.

Samostatná adresa – slouží pro zadání samostatné adresy počítače, pro který má pravidlo platit (například *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsíť – umožní zadat podsíť skupiny počítačů pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

4.2.3.4 Kontrola protokolu SSL/TLS

ESET NOD32 Antivirus umožňuje také kontrolu protokolů zapouzdřených v protokolu SSL. Kontrolu můžete přizpůsobit podle toho, zda je certifikát využíván danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL.

Zapnout filtrování kontrolu protokolu SSL/TLS – pokud je tato možnost aktivní, bude se provádět kontrola každé šifrované komunikace pomocí protokolu SSL.

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

Automatický režim – v tomto režimu je kontrolována šifrovaná komunikace vybraných aplikací – webových prohlížečů a poštovních klientů. V případě potřeby můžete kdykoli rozšířit seznam aplikací, jejichž šifrovanou komunikaci chcete kontrolovat.

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 – vyberte tuto možnost, pokud chcete kontrolovat veškerou komunikaci chráněnou protokolem SSL kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru využívající nedůvěryhodný certifikát označený jako důvěryhodný, komunikace bude povolena a přenášený obsah bude filtrován.

Kontrolovat šifrovanou komunikaci těchto aplikací – pomocí této možnosti můžete vytvořit seznam aplikací, u kterých bude komunikace SSL kontrolována.

Seznam známých certifikátů – pomocí této možnosti můžete přidat do programu důvěryhodné certifikáty.

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

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

Kořenový certifikát

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) používají certifikát podepsaný certifikační autoritou (Trusted Root Certification Authorities). Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (tato možnost je nastavena standardně), při navázání šifrované komunikace se zobrazí okno s výběrem akce. Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** 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**.

4.2.3.4.1 Certifikáty

Pro správné fungování kontroly SSL komunikace ve webových prohlížečích a poštovních klientech je potřeba přidat kořenový certifikát společnosti ESET do seznamu známých kořenových certifikátů (vydavatelů). Možnost Přidat kořenový certifikát do známých prohlížečů by měla být zapnuta. 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.

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

Pomocí možnosti **Zakázat komunikaci využívající daný certifikát** vždy zablokujete komunikaci s webovou stránkou využívající nedůvěryhodný certifikát.

Pokud je certifikát neplatný nebo poškozený, znamená to, že certifikátu vypršela platnost nebo nebyl správně podepsán. V tomto případě doporučujeme **zakázat komunikaci využívající daný certifikát**.

4.2.3.4.2 Seznam známých certifikátů

Pomocí **seznamu známých certifikátů** můžete přizpůsobit chování ESET NOD32 Antivirus, při detekci konkrétních SSL certifikátů. V tomto seznamu naleznete certifikáty, pro které jste v Interaktivním režimu nastavili zapamatování vybrané akce. Seznam naleznete v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Web a mail** > **Kontrola protokolu SSL/TLS** > **Seznam známých certifikátů**.

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

Sloupce

Název – název certifikátu.

Vydavatel certifikátu – jméno autora certifikátu.

Předmět certifikátu – identifikace entity asociované s veřejným klíčem uloženým v poli předmět veřejného klíče.

Přístup – pro povolení nebo zablokování komunikace využívající daný certifikát bez ohledu na to, zda je důvěryhodný, vyberte možnost **Povolit** nebo **Blokovat**. V případě možnosti **Automaticky** budou důvěryhodné certifikáty povoleny, a v nedůvěryhodných bude muset uživatel vybrat akci. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Kontrolovat – pro kontrolu nebo ignorování komunikace využívající daný certifikát vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automaticky** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – certifikát můžete přidat ručně ve formátu *.cer*, *.crt* nebo *.pem* a to buď přímo ze souboru nebo externího zdroje po zadání URL.

Změnit – klikněte pro úpravu již existujícího certifikátu.

Odstranit – klikněte pro odebrání vybraného certifikátu.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

4.2.3.4.3 Kontrolovat šifrovanou komunikaci těchto aplikací

Kontrolu šifrované (SSL/TLS) komunikace můžete nastavit rozdílné pro jednotlivé aplikace. Do tohoto seznamu se automaticky přidávají také aplikace, pro které jste v interaktivním režimu nastavili zapamatování vybrané akce. Seznam aplikací naleznete v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Kontrola protokolu SSL/TLS** > **Kontrolovat šifrovanou komunikaci těchto aplikací**.

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

Sloupce

Aplikace – název aplikace.

Akce při kontrole – pro kontrolu nebo ignorování šifrované komunikace konkrétní aplikace vyberte možnost **Kontrolovat** nebo **Ignorovat**. V případě možnosti **Automatická** se bude komunikace kontrolovat v automatickém režimu filtrování a výzva s výběrem akce se uživateli zobrazí v interaktivním režimu. Pokud nastavíte **Dotázat se**, vždy se uživateli zobrazí výzva s výběrem akce.

Ovládací prvky

Přidat – klikněte pro vytvoření výjimky na konkrétní aplikaci.

Změnit – klikněte pro úpravu již existující výjimky na aplikaci.

Odstranit – klikněte pro odebrání vybrané výjimky na aplikaci.

OK/Zrušit – pro uložení změn klikněte na tlačítko **OK**, v opačném případě klikněte na tlačítko **Zrušit**.

4.2.4 Anti-Phishingová ochrana

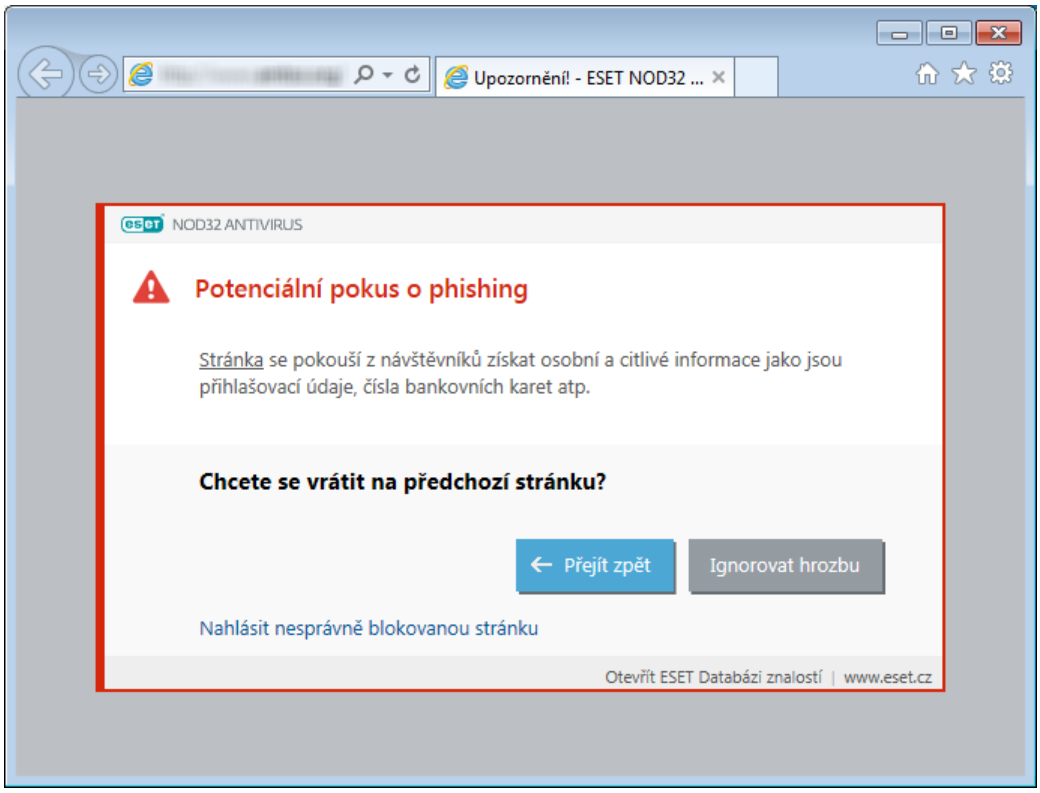
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Nejčastěji je vyžadován přístup k bankovnímu účtu nebo PIN. Více informací naleznete ve slovníku pojmů). ESET NOD32 Antivirus obsahuje anti-phishingovou ochranu, která blokuje internetové stránky s tímto obsahem.

Důrazně doporučujeme aktivovat Anti-Phishingovou ochranu programu ESET NOD32 Antivirus. To provedete v **Rozšířeném nastavení** (dostupném po stisknutím **klávesy F5** v hlavním okně programu) na záložce **Web a mail** > **Anti-Phishing**.

Podrobnější informace o fungování Anti-Phishingové ochrany naleznete v ESET Databázi znalostí.

Přístup na stránky s phishingovým obsahem

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).



Poznámka:
V případě, že budete pokračovat na potenciální phishingovou stránku, na několik hodin se pro ni vytvoří výjimka. Následně bude přístup opět blokován. Pokud chcete trvale povolit přístup na danou stránku, použijte Správce URL adres – v **Rozšířeném nastavení** přejděte na záložku **Web a mail** > **Ochrana přístupu na web** > **Správa URL adres** a upravte **Seznam povolených adres**.

Nahlášení phishingové stránky

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

Poznámka:
Předtím než odešlete stránku do společnosti ESET se ujistěte, že splňuje alespoň jedno z níže uvedených kritérií:
- stránka není detekována jako škodlivá,
- stránka je chybně detekována jako škodlivá. V tomto případě použijte tento odkaz.

Případně můžete odkaz na webovou stránku odeslat 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.)

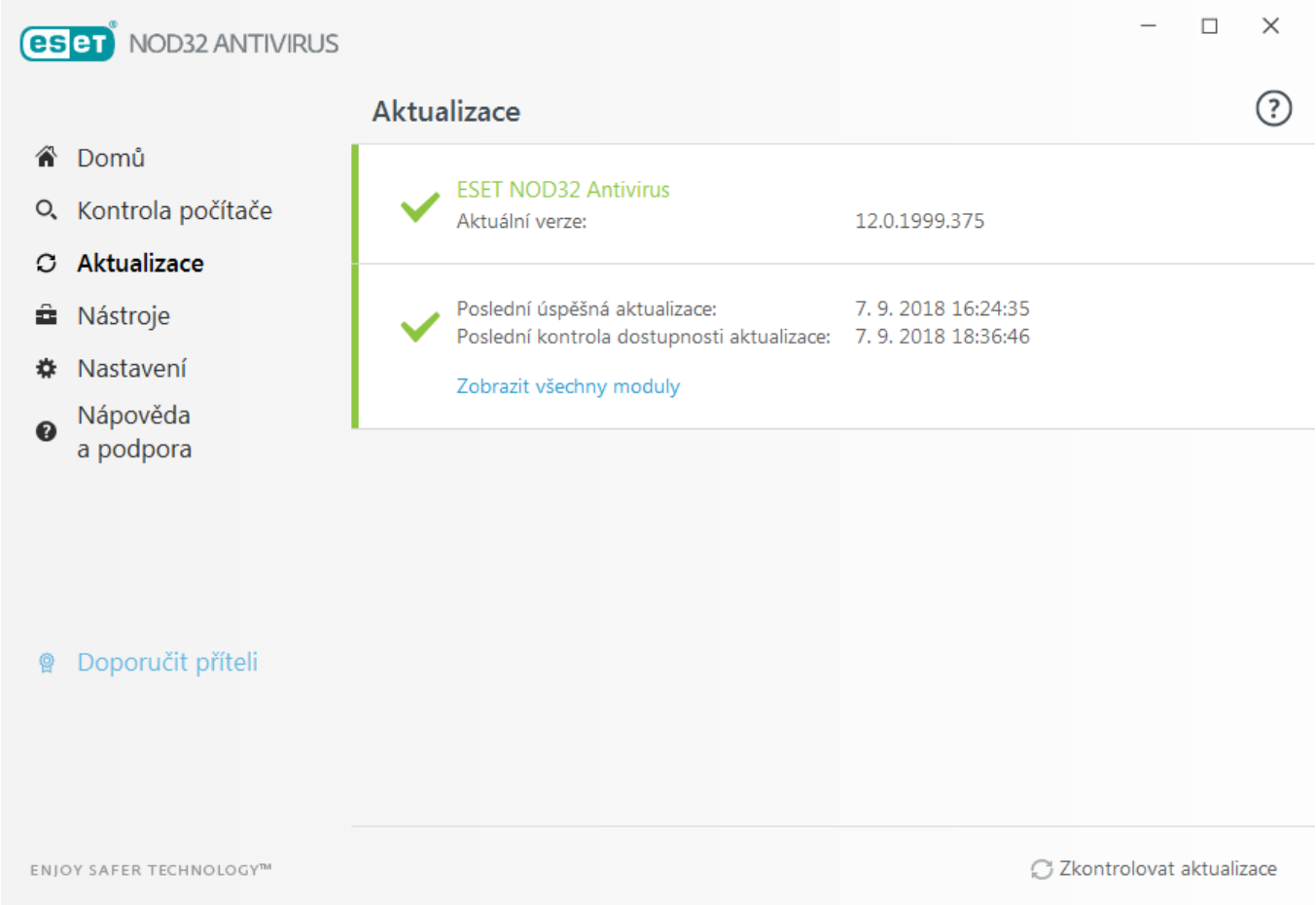
4.3 Aktualizace programu

Pravidelná aktualizace programu ESET NOD32 Antivirus je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program používal nejnovější detekční a programové moduly.

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

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

POZNÁMKA:
Licenční klíč jste obdrželi po nákupu nebo registraci ESET NOD32 Antivirus.



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

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

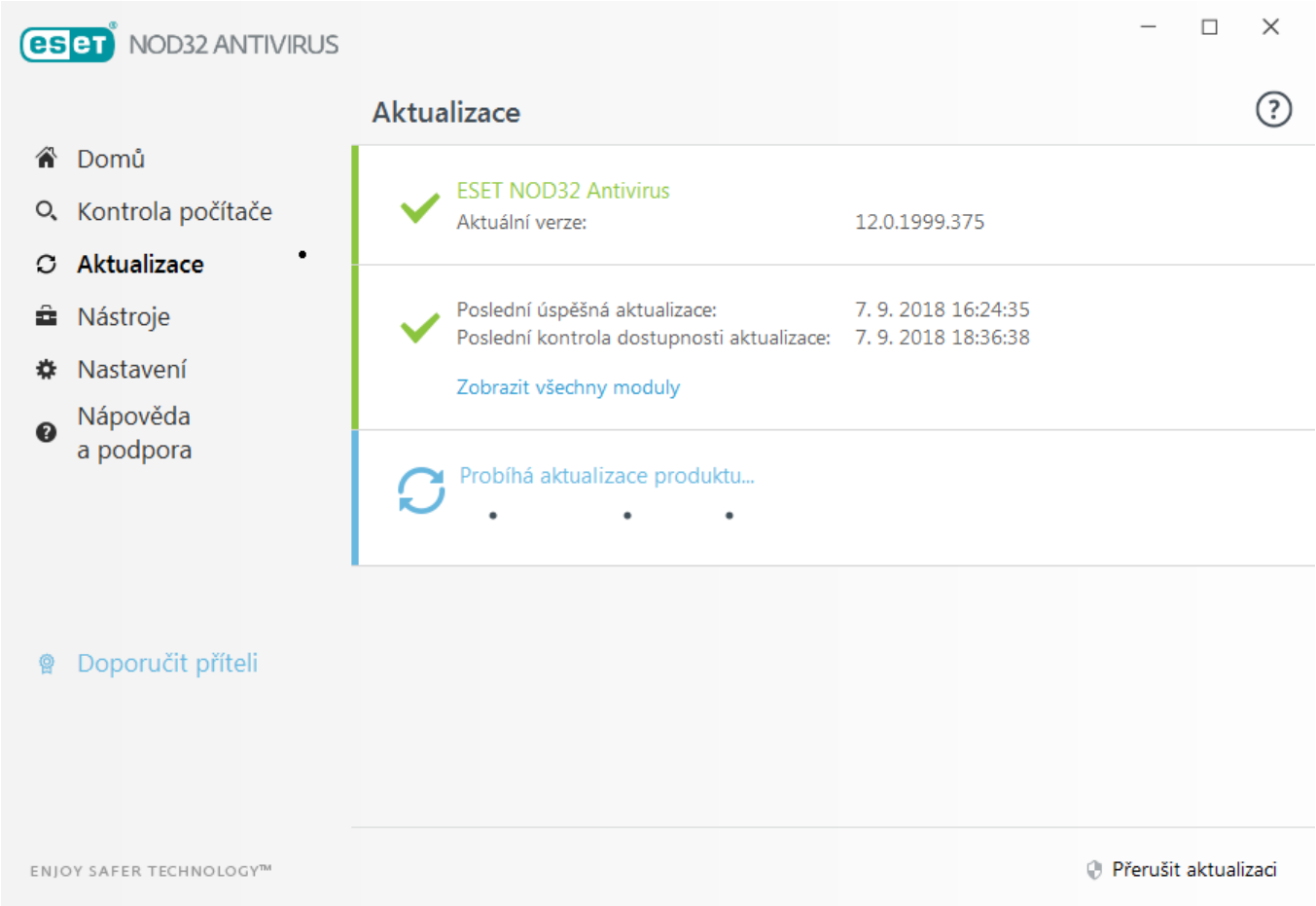
Poslední kontrola dostupnosti aktualizace – zobrazuje datum, kdy se program naposledy připojil k aktualizačním serverům a ověřil, zda není dostupná nová verze modulů.

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

Kliknutím na tlačítko **Zkontrolovat aktualizace** vynutíte ruční ověření dostupnosti detekčních a programových modulů.

Průběh aktualizace

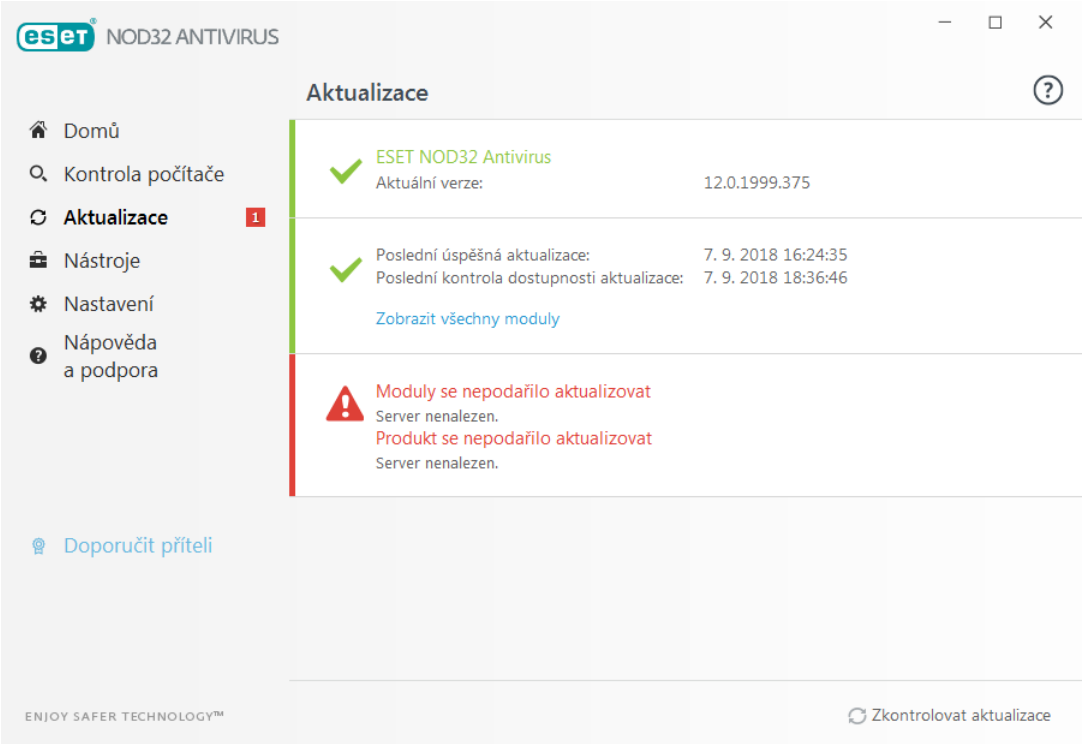
V případě, že jsou na aktualizačních serverech dostupné nové moduly, po kliknutí na tlačítko **Zkontrolovat aktualizace** se spustí proces stahování. Zároveň se zobrazí průběh stahování souboru aktualizace a zbývající čas do konce. Kliknutím na tlačítko **Zrušit aktualizaci** aktualizaci zastavíte.



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

V některých případech se může zobrazit chybová zpráva **Moduly se nepodařilo aktualizovat**, a to z níže uvedených důvodů:

1. **Program není aktivován/Neplatná licence** – v hlavním okně program přejděte na záložku **Nápověda a podpora**, kde klikněte na tlačítko **Změnit licenci**. Poté vyberte způsob aktivace a postupujte podle kroků na obrazovce.
2. **Chyba při stahování souborů aktualizace** – při pokusu o stažení souboru aktualizace došlo k chybě. Chyba může souviset s nesprávným nastavením připojení k internetu. Doporučujeme zkontrolovat připojení k internetu (otevřením jakékoliv webové stránky ve webovém prohlížeči). Rovněž doporučujeme zkontrolovat, zda je počítač připojen k internetu, a ověřit, zda poskytovatel internetu nemá výpadek připojení.



DŮLEŽITÉ:
Po úspěšné aktualizaci programových modulů doporučujeme pro restartovat počítač.

POZNÁMKA:
Pro více informací přejděte do ESET Databáze znalostí.

4.3.1 Nastavení aktualizace

Možnosti aktualizace jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) na záložce **Aktualizace** > **Obecné**. Nastavení aktualizace se skládá ze zadání zdroje aktualizace, tedy z nastavení aktualizačních serverů a autentifikace vůči těmto serverům.

Profil

Aktuálně používaný aktualizační profil se zobrazuje v rozbalovacím menu **Výchozí profil**.

Automatické přepínání profilu – pomocí této možnosti se může profil používaný pro aktualizaci dynamicky měnit v závislosti na síti do níž jste připojeni.

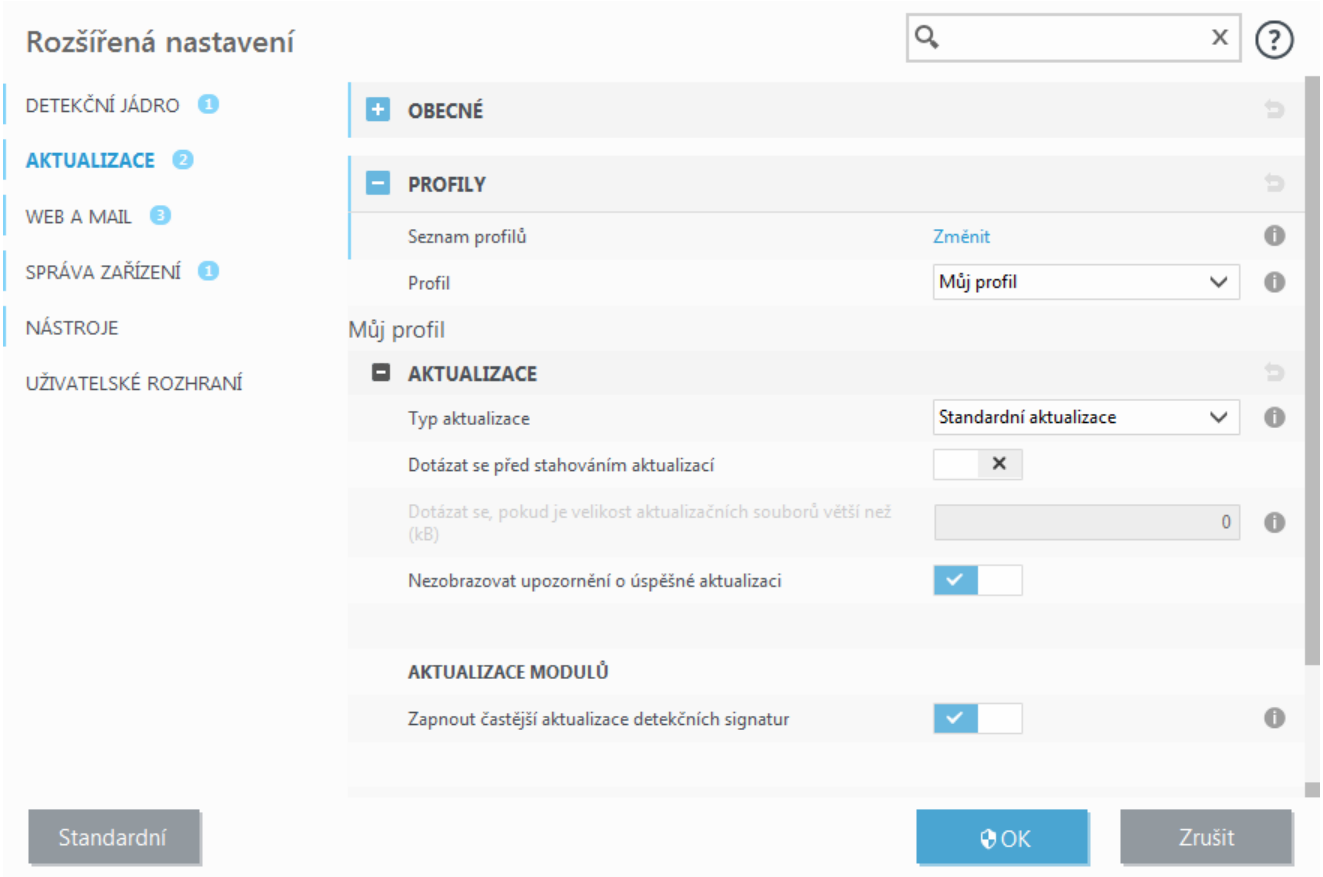
Většinu problémů souvisejících s aktualizací modulů vyřešíte vymazáním aktualizační cache po kliknutí na tlačítko **Vyčistit**.

Záloha modulů

Pokud máte podezření, že nová verze modulů je nestabilní nebo poškozená, můžete se vrátit ke starší verzi modulů a na stanovený časový interval zakázat jejich aktualizaci.

ESET NOD32 Antivirus zálohuje detekční a programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshoty modulů vytvářely, ponechte možnost **Vytvářet zálohu aktualizačních souborů** zaškrtnutou. **Počet vytvářených záloh** určuje počet obrazů předchozích virových databází uložených na lokálním disku počítače.

Pokud kliknete na tlačítko **Vrátit**, vyberte z rozbalovacího menu **Časový interval**, na jak dlouho chcete aktualizaci detekčních a programových modulů pozastavit.



Pro správné fungování aktualizace je nezbytné zadat veškeré aktualizační informace správně. Pokud používáte firewall, ujistěte se, že má produkt ESET povolenou HTTP komunikaci.

Profily

V případě potřeby si můžete vytvořit pro každou situaci samostatný aktualizační profil s rozdílnou konfigurací. To se může hodit například u uživatelů, kteří hodně cestují a připojují se do rozdílných sítí.

Standarně je v rozbalovacím menu **Profil** vybrána **Můj profil**. Pro vytvoření nového nebo úpravu již existujícího klikněte na **Změnit** vedle položky **Seznam profilů**.

Aktualizace

Standardně jsou jako **Typ aktualizace** nastaveny vybrány **Standardní aktualizace**. Tím je zajištěno automatické stahování aktualizací ze serverů společnosti ESET. Pokud je vybrána možnost **Testovací aktualizace**, budou se při aktualizaci stahovat beta verze modulů a virové databáze. V předstihu tak získáte přístup k novějším funkcím, opravám a metodám detekce škodlivého kódu. Protože testovací aktualizace nereprezentují finální kvalitu, neměli byste je instalovat na produkční stroje a pracovní stanice, u který je vyžadována stabilita a dostupnost. Vyberete-li možnost **Opožděné aktualizace**, aktualizace se budou stahovat z aktualizačního severu, na který jsou aktualizace umisťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

Vyberete-li možnost **Dotázat se před stahováním aktualizací**, před stažením nové aktualizace se zobrazí informace, že je dostupná aktualizace. Následně bude nutné stažení aktualizace potvrdit.

V případě, že aktualizační soubor bude větší než definovaná hodnota pomocí možnosti **Dotázat se, pokud je velikost aktualizačního souboru větší než (kB)**, zobrazí informace, zda chcete aktualizaci stáhnout. Tato možnost je vhodná při mobilních připojení, kdy potřebujete šetřit množství přenášených dat.

Nezobrazovat upozornění o úspěšné aktualizaci – vypne zobrazování oznámení v pravém dolním rohu obrazovky. Použití této možnosti je užitečné v případě, kdy na počítači běží aplikace v režimu celé obrazovky. Stejnou akci můžete vynutit aktivováním Herního režimu.

Aktualizace modulů

Zapnout častější aktualizace detekčních signatur – aktivováním této možnosti zkrátíte interval aktualizace. Vypnutí této možnosti negativně ovlivní detekční schopnosti.

Aktualizace programových komponent

Pokud aktivujete možnost **Aktualizovat aplikaci**, program bude pravidelně ověřovat dostupnost nové verze produktu a automaticky novou verzi nainstaluje. Aktualizace na novější verzi zpravidla nevyžaduje interakci uživatele, pouze je nutné restartovat počítače. Na nutnost restartování vás aplikace upozorní.

4.3.1.1 Profily aktualizace

Aktualizační profily můžete použít pro různá nastavení aktualizací. Vytvoření aktualizačních profilů pro aktualizaci má význam především pro mobilní uživatele, kteří si mohou vytvořit alternativní profil pro internetové připojení, které se často mění.

V rozbalovacím menu **Aktualizační profil** se vždy zobrazuje aktuálně používaný profil. Standardně je vybrána možnost **Můj profil**. Nový profil můžete vytvořit po kliknutí na Změnit v sekci **Profily** > **Seznam profilů**, kde zadejte název nového profilu a klikněte na tlačítko **Přidat**.

4.3.1.2 Pokročilá nastavení aktualizace

V pokročilém nastavení aktualizace můžete konfigurovat režim aktualizace a připojení prostřednictvím Proxy serveru.

4.3.1.2.1 Režim aktualizace

V sekci **Režim aktualizace** se nachází nastavení související s pravidelným stahováním detekčních a programových modulů i aktualizací programu na novou verzi. Nové verze programu přidávají nové detekční technologie a případně opravují chyby, které se vyskytly v předchozí verzi. Tyto změny není možné implementovat prostřednictvím standardní aktualizace modulů, proto je nutné provádět aktualizaci programu. Mějte na paměti, že po aktualizaci programu může být vyžadován restart počítače.

V této části jsou dostupné následující možnosti:

Pokud aktivujete možnost **Aktualizovat aplikaci**, program bude pravidelně ověřovat dostupnost nové verze produktu a automaticky novou verzi nainstaluje. Aktualizace na novější verzi zpravidla nevyžaduje interakci uživatele, pouze je nutné restartovat počítače. Na nutnost restartování vás aplikace upozorní.

Vyberete-li možnost **Dotázat se před stahováním aktualizací**, před stažením nové aktualizace se zobrazí informace, že je dostupná aktualizace. Následně bude nutné stažení aktualizace potvrdit.

V případě, že aktualizační soubor bude větší než definovaná hodnota pomocí možnosti **Dotázat se, pokud je velikost aktualizačního souboru větší než (kB)**, zobrazí informace, zda chcete aktualizaci stáhnout. Tato možnost je vhodná při mobilních připojení, kdy potřebujete šetřit množství přenášených dat.

4.3.1.2.2 Možnosti připojení

Pro přístup k nastavení proxy serveru pro daný aktualizační profil přejděte v **Rozšířeném nastavení** (dostupném po stisknutí klávesy **F5** v hlavním okně programu) na záložku **Aktualizace** > **Profily** > **Možnosti připojení**. V rozbalovacím menu **Režim proxy** jsou dostupné následující možnosti:

- **Nepoužívat proxy server**,
- **Připojení prostřednictvím proxy serveru,**
- **Použít globální nastavení proxy serveru.**

Vybráním možnosti **Použít globální nastavení proxy serveru** se použijí veškerá nastavení proxy serveru definovaná v Rozšířeném nastavení na záložce **Nástroje** > **Proxy server**.

Pomocí možnosti **Nepoužívat proxy server** zajistíte, aby se při aktualizaci ESET NOD32 Antivirus nepoužíval proxy server.

Možnost **Spojení pomocí proxy serveru** vyberte v případě, že:

- Pro aktualizaci ESET NOD32 Antivirus potřebujete použít jiné, než globální nastavení proxy serveru definované v Rozšířeném nastavení ve větvi **Nástroje** > **Proxy server**. Pokud vyberte tuto možnost, je potřeba zadat adresu **Proxy serveru**, komunikační **Port** (standardně 3128), případně také **Uživatelské jméno** a **Heslo**,
- Nebylo definováno globální nastavení proxy serveru, ale pro aktualizaci ESET NOD32 Antivirus se má používat proxy,
- Počítač je připojen k internetu pomocí proxy serveru a 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.

Standardně je nastavena možnost **Použít globální nastavení proxy serveru**.

Pokud aktivujete možnost **Použít přímé spojení, pokud není dostupný proxy server**, ESET NOD32 Antivirus automaticky zkusí připojení k aktualizačním serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.

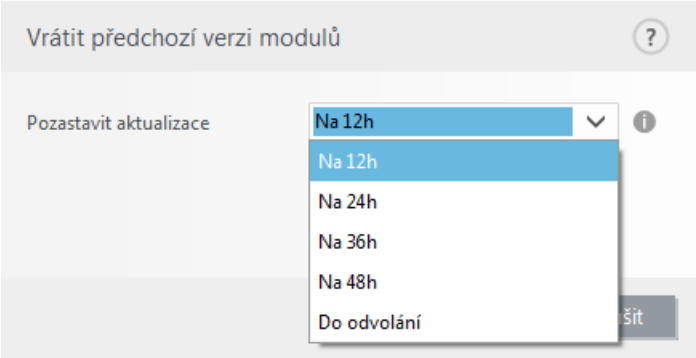
Poznámka:
Autentifikační údaje jako **Uživatelské jméno** a **Heslo** pro proxy server vyplňte pouze v případě, že je proxy server vyžaduje. Mějte na paměti, že se nejedná o údaje, které jste obdrželi při koupi produktu ESET NOD32 Antivirus.

4.3.2 Vrátit předchozí aktualizace

Pokud máte podezření, že nová aktualizace detekčních nebo programových modulů je nestabilní nebo poškozená, můžete vrátit moduly do předchozího stavu a na stanovený časový interval pozastavit aktualizace.

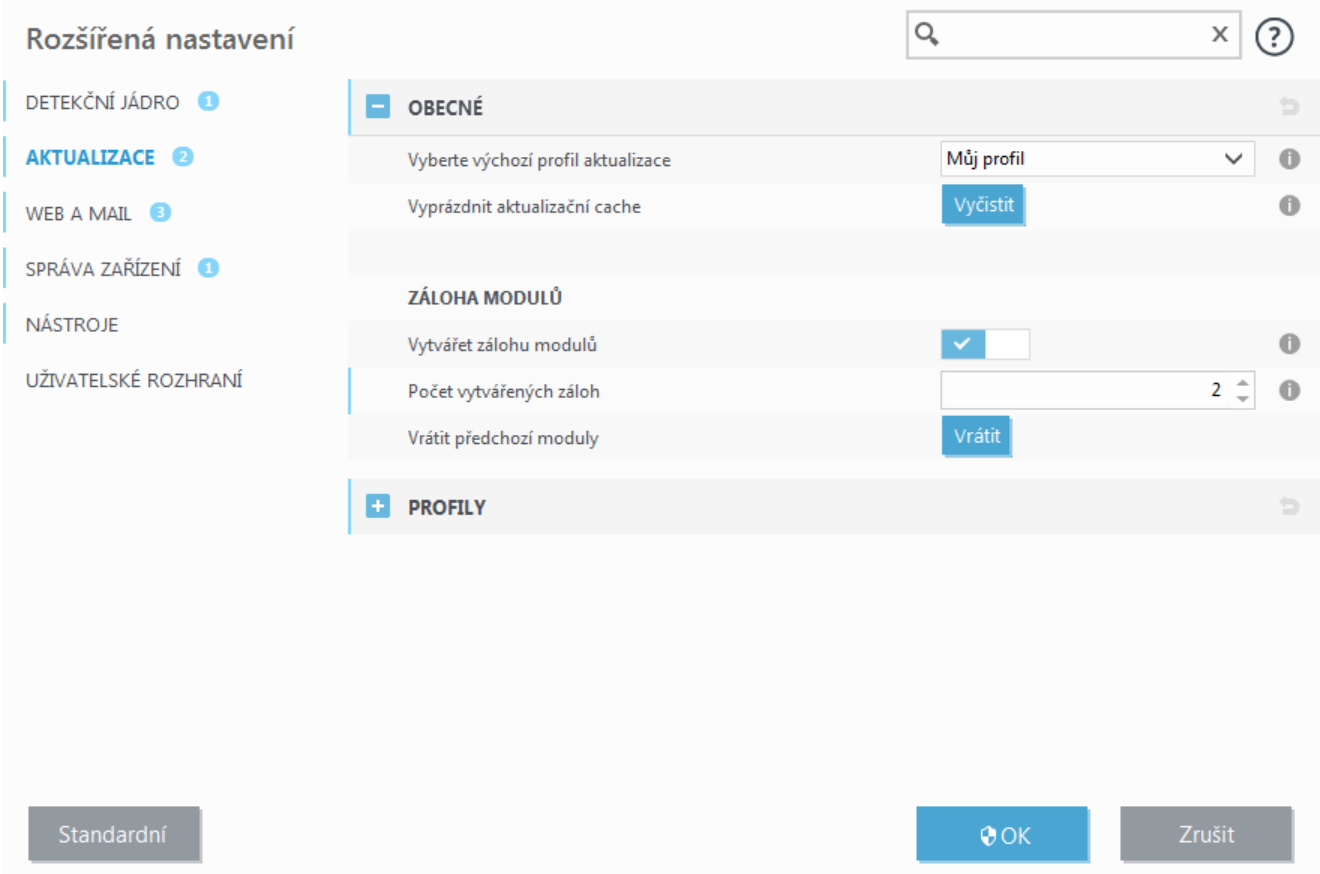
Bezpečnostní produkt ESET zálohuje detekční a jednotlivé programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshoty modulů vytvářely, ponechte aktivní možnost **Vytvářet zálohu aktualizačních souborů**. **Počet záloh vytvářených lokálně** určuje počet obrazů předchozích virových databází uložených na lokálním disku počítače.

Pokud kliknete na tlačítko **Vrátit** (v **Rozšířeném nastavení** (F5) > **Aktualizace** > **Obecné**), vyberte z rozbalovacího menu **Časový interval**, na jak dlouho chcete aktualizaci detekčních 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.

Pro provedení této akce se na stanovenou dobu obnoví nejstarší uložené detekční a programové moduly uložené v počítači a zároveň se text tlačítka změní na **Povolit aktualizace**.



Příklad:
Nejnovější verze detekčního jádra má číslo 9556. Na pevném disku počítače jsou uloženy obrazy detekčního jádra 9555 a 9553. Všimněte si, že verze 9554 není k dispozici, protože počítač byl například delší dobu vypnut, proto byla stažena novější verze modulů. Pokud jste jako **Počet vytvářených záloh** nastavili číslo 2, po navrácení změn se obnoví detekční jádro (i programové moduly) s číslem 9553. Tento proces může chvíli trvat. Pro ověření, zda se vrátily předchozí moduly přejděte v hlavním okně ESET NOD32 Antivirus na záložku Aktualizace.

4.3.3 Jak vytvořit aktualizační úlohu

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

Aktualizaci můžete spouštět jako naplánovanou úlohu. Pro konfiguraci naplánované úlohy klikněte na záložku **Nástroje** > **Plánovač**. Standardně jsou po instalaci ESET NOD32 Antivirus vytvořeny následující aktualizační úlohy:

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

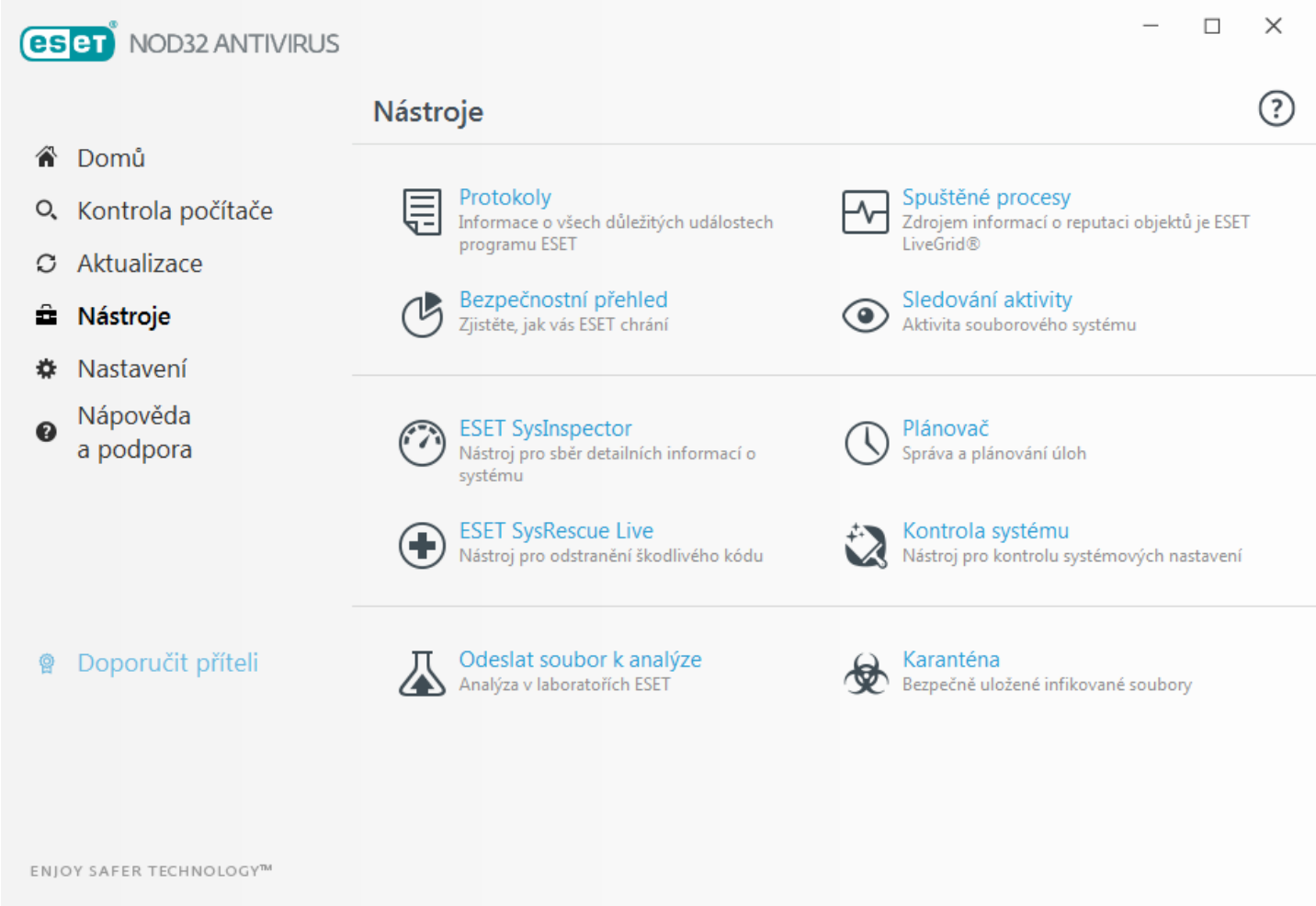
Každou z uvedených aktualizačních úloh můžete upravit podle svých představ. Kromě standardních aktualizačních úloh můžete vytvořit nové aktualizační úlohy s vlastním nastavením. Podrobněji se vytváření a nastavení aktualizačních úloh zabýváme v kapitole Plánovač.

4.4 Nástroje

Záložka **Nástroje** obsahuje součásti, které usnadňují správu programu a nabízejí rozšířené možnosti pro pokročilé uživatele.

4.4.1 Nástroje produktu ESET NOD32 Antivirus

V hlavním menu programu na záložce **Nástroje** naleznete součásti určené pro zkušené uživatele, které vám usnadní správu a diagnostiku programu.



ESET NOD32 Antivirus nabízí následující nástroje:

Protokoly

Bezpečnostní přehled

Sledování aktivity

Spuštěné procesy (tato součást je dostupná, pokud máte aktivní technologii ESET LiveGrid®)

ESET SysInspector

ESET SysRescue Live – přesměruje vás na webové stránky společnosti ESET, kde si můžete stáhnout přímo obraz ESET SysRescue Live nebo nástroj pro vytvoření záchranného CD/USB..

Plánovač

Kontrola systému – pomůže vám obnovit důležitá nastavení systému do doby před jeho infiltrací.

Odeslat soubor k analýze – umožní odeslat podezřelý soubor k analýze do virové laboratoře ESET. Po kliknutí se zobrazí dialogové okno, které je popsané v kapitole Odeslání souboru k analýze.

Karanténa

4.4.1.1 Protokoly

Protokoly obsahují informace o všech důležitých událostech programu, které nastaly a poskytují přehled o detekovaných hrozbách. Protokolování představuje silný nástroj při systémové analýze, odhalování problémů a rizik a v neposlední řadě při hledání řešení. Zaznamenávání probíhá aktivně na pozadí bez jakékoli interakce s uživatelem a zaznamenávají se informace na základě nastavení citlivosti protokolování. Prohlížení textových zpráv a protokolů je možné přímo z prostředí ESET NOD32 Antivirus a stejně tak je tyto protokoly možné archivovat.

Protokoly jsou přístupné v hlavním okně po kliknutí na záložku **Nástroje** > **Protokoly**. Následně z rozbalovacího menu **Protokoly** vyberte požadovaný typ protokolu.

- **Zachycené hrozby** – protokol zachycených infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly ESET NOD32 Antivirus. Informace zahrnují čas detekce, název infiltrace, umístění, provedenou činnost a uživatele přihlášeného v době detekce. Dvojklikem na záznam protokolu otevřete detaily v samostatném okně.
- **Události** – protokol událostí obsahuje informace o všech událostech ESET NOD32 Antivirus a chybách, které se vyskytly. 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.
- **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
- **Filtrované webové stránky** – tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem Ochrana přístupu na web. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.
- **Správa zařízení** – obsahuje záznamy o výměnných médiích nebo zařízeních připojených k počítači. V protokolu se zobrazí pouze zařízení, na která byla aplikována pravidla Správce zařízení. Pokud nebylo na zařízení aplikováno žádné pravidlo, záznam v protokolu se nevytvoří. Pro každé zařízení se zobrazí také informace o typu zařízení, sériové číslo, název výrobce a velikost média (pokud jsou dostupné).

V každé sekci můžete jednotlivé události kopírovat do schránky přímo po označení události a kliknutím na tlačítko **Kopírovat** (nebo pomocí klávesové zkratky **Ctrl + C**). Pro výběr více záznamů stiskněte zároveň klávesu **CTRL** nebo **SHIFT**.

Po kliknutí na přepínač **Filtrování** se zobrazí dialogové okno **Filtrování protokolu**, pomocí kterého můžete definovat kritéria filtrování.

V okně **Protokoly** můžete vyvolat kontextové menu kliknutím pravým tlačítkem myši na konkrétní záznam. Dostupné jsou následující možnosti:

- **Zobrazit** – zobrazí v novém okně všechny záznamy protokolu.
- **Filtrovat záznamy stejného typu** – po aktivovaní tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování,...).
- **Filtrovat.../Hledat...** – po kliknutí se otevře dialogové okno Filtrování protokolu, ve kterém můžete definovat kritéria pro filtrování záznamů.
- **Zapnout filtr** – kliknutím aktivujete filtr. Pokud jste dosud žádný filtr nedefinovali, zobrazí se průvodce jeho vytvořením. Při opětovném kliknutí se automaticky aktivuje naposledy použitý filtr.
- **Zrušit filtr** – vypne filtrování.
- **Kopírovat/Kopírovat vše** – zkopíruje všechny záznamy z daného okna.
- **Odstranit/Odstranit vše** – odstraní vybrané/všechny záznamy – tato akce vyžaduje administrátorská oprávnění.
- **Exportovat...** – uloží vybrané záznamy do .XML formátu.
- **Exportovat vše...** – uloží všechny záznamy do .XML formátu.
- **Najít...** – 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.
- **Rolovat výpis protokolu** – pokud je tato možnost povolena, starší protokoly budou automaticky rolovat a v okně **Protokoly** se zobrazí pouze ty nejnovější.

4.4.1.1.1 Protokoly

Nastavení protokolování produktu ESET NOD32 Antivirus je přístupné z hlavního okna programu. Přejděte na záložku **Nastavení** a klikněte na **Rozšířená nastavení** > **Nástroje** > **Protokoly**. V této sekci můžete upravit způsob správy protokolů. Program dokáže automaticky odstraňovat staré protokoly, čímž šetří místo na disku. V nastavení můžete vybrat následující možnosti:

Zaznamenávat události od úrovně – umožňuje nastavit úroveň, od které se budou zaznamenávat události do protokolu.

- **Diagnostické** – 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 (chyba při startu antivirové ochrany, atd...).

POZNÁMKA: Všechna zablokovaná spojení se do protokolu zapíší při vybrání diagnostické úrovně.

Pomocí možnosti **Automaticky vymazat záznamy starší než (dní)** můžete nastavit po kolika dnech se záznamy mají vymazat.

Automaticky optimalizovat protokoly – zajistí 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 defragmentaci protokolů. Defragmentace odstraňuje prázdné záznamy v protokolech, čímž zvyšuje rychlost zpracovávání. Viditelné zlepšení práce s protokoly je po optimalizaci znatelné hlavně především u protokolů s velkým množstvím záznamů.

Pomocí možnosti **Zaznamenávat textové protokoly** aktivujete ukládání protokolů do odlišeného formátu:

- **Cílová složka** – složka, do které se uloží protokoly (pouze pro Text/CSV). Každý protokol se ukládá do samostatného souboru (například ve *virlog.txt* naleznete **Zachycené hrozby**, pokud protokoly ukládáte jako prostý text).

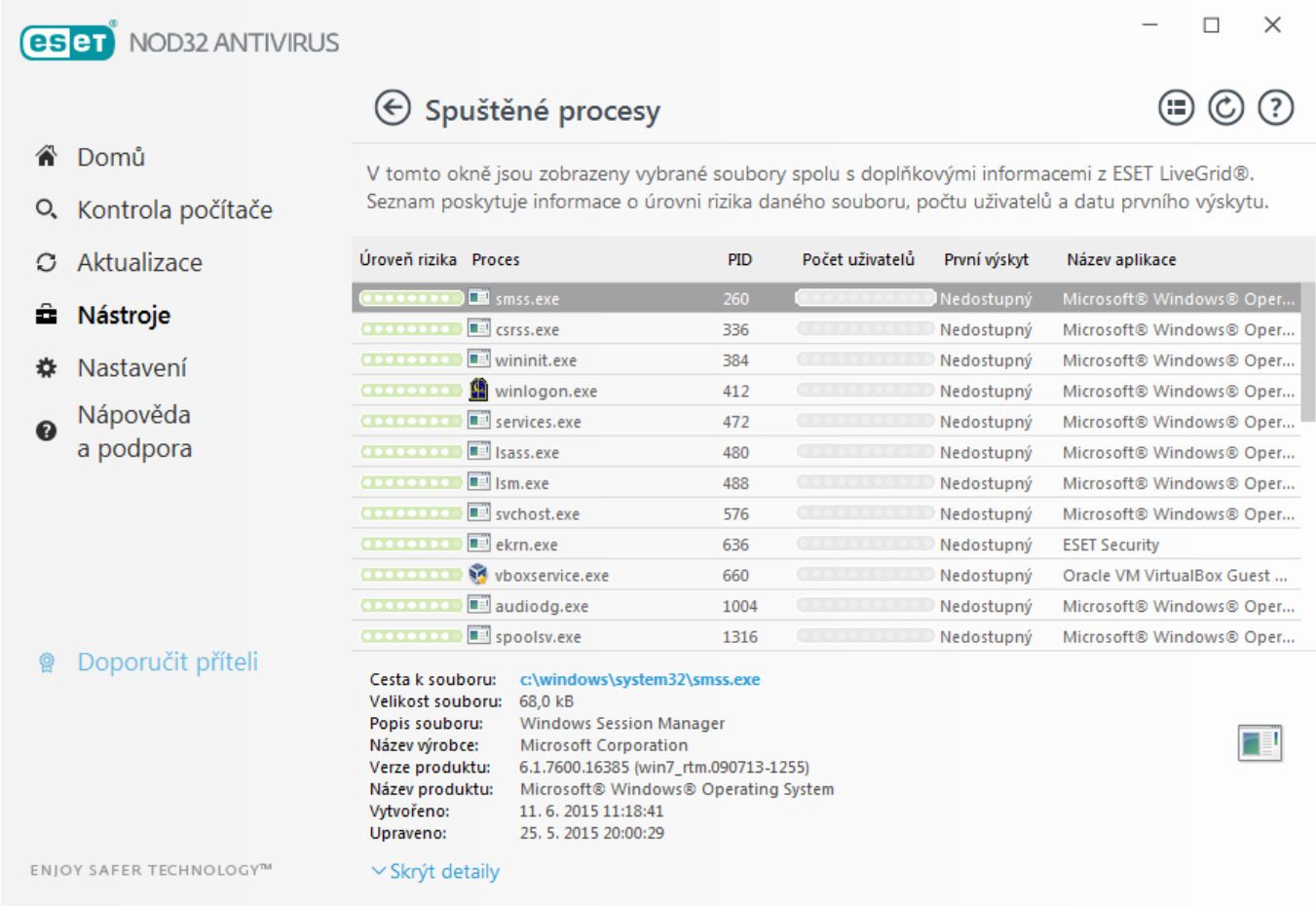
- **Typ** – pokud vybere **Text** jako formát souborů, protokoly budou uloženy do textového souboru; data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené středníkem **CSV**. Pokud vyberete **Událost**, protokol bude uložen do systémového Protokolu událostí, který si můžete zobrazit v Prohlížeči událostí.

Odstranit všechny protokoly – po kliknutí vymaže všechny protokoly vybrané v rozbalovacím menu **Typ**. O úspěšném vymazání protokolů budete informováni.

POZNÁMKA:
Specialisté technické podpory vás mohou požádat o zaslání protokolů, které mohou urychlit řešení vašeho problému. Pomocí nástroje ESET Log Collector snadno získáte diagnostické informace z počítače včetně protokolů. Pro více informací o používání tohoto nástroje navštivte ESET Databázi znalostí.

4.4.1.2 Spuštěné procesy

Tento nástroj zobrazuje spuštěné programy a procesy a umožňuje společnosti ESET získávat informace o nových infiltracích. ESET NOD32 Antivirus poskytuje detailnější informace o spuštěných procesech díky technologii ESET LiveGrid® pro zajištění lepší ochrany uživatelů.



Úroveň rizika – ve většině případů přiřazuje ESET NOD32 Antivirus objektům (souborům, procesům, klíčům registru apod.) úroveň rizika pomocí technologie ESET LiveGrid® na základě heuristických pravidel a kontroly každého objektu na přítomnost škodlivého kódu. Poté na základě těchto výsledků přidělí procesům úroveň rizika od 1 – V pořádku (zelený) až po 9 – Nebezpečný (červený).

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

Proces – název aplikace nebo procesu, který aktuálně běží na počítači. Pro zobrazení všech běžících programů na počítači můžete použít také Správce úloh systému Windows. Správce úloh spustíte kliknutím pravým tlačítkem na Hlavní panel a vybráním možnosti **Spustit správce úloh**, případně pomocí klávesové zkratky **Ctrl** + **Shift** + **Esc**.

PID – ID běžícího procesu v operačním systému Windows.

POZNÁMKA: Aplikace označené jako 1 – V pořádku (zelený) jsou bezpečné a vyloučené z kontroly pro zajištění vyššího výkonu kontroly počítače.

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® .

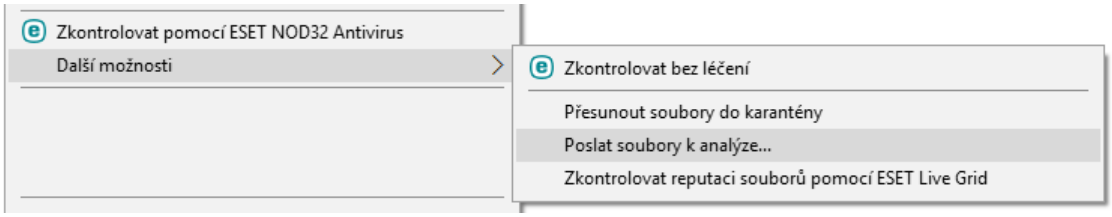
Poznámka:
I v případě, že je aplikace označená jako Neznáma (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete soubor odeslat k analýze do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde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

Název aplikace – název aplikace nebo procesu.

Po kliknutí na konkrétní aplikaci a možnost **Zobrazit detaily** se v dolní části okna 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.

Poznámka:
Reputaci můžete zjistit také pro soubory, které se nechovají jako spuštěné programy/procesy. Na soubor, který chcete zkontrolovat, klikněte pravým tlačítkem myši a ze zobrazeného kontextového menu vyberte **Další možnosti** > **Zkontrolovat reputaci souborů pomocí ESET LiveGrid®**.



4.4.1.3 Bezpečnostní přehled

V této části naleznete statistické údaje o činnosti programu rozdělené do následujících kategorií:

Zablokováno webových stránek – zobrazuje počet zablokovaných webových stránek (blacklisted URL for PUA, phishingu, hacked router, IP r certificate).
Detekované infikované e-mailové objekty – zobrazuje počet detekovaných infikovaných poštovních objektů.
Zablokované webové stránky Rodičovskou kontrolou – zobrazuje počet stránek zablokovaných rodičovskou kontrolou.
Detekovaných PUA – zobrazuje počet detekovaných potenciálně nechtěných aplikací (PUA).
Detekovaných nevyžádaných e-mailů – zobrazuje počet detekovaných spamů.
Zablokované přístupy k webové kameře – zobrazuje počet zablokovaných přístupu k webové kameře.
Chráněné přístupy k internetovému bankovnictví – zobrazuje počet chráněných stránek internetového bankovnictví.
Zkontrolováno dokumentů – zobrazuje počet zkontrolovaných dokumentů.
Zkontrolováno aplikací – zobrazuje počet zkontrolovaných spustitelných objektů.
Zkontrolovány další objekty – zobrazuje počet dalších zkontrolovaných objektů.
Zkontrolovány objekty webových stránek – zobrazuje počet zkontrolovaných objektů webových stránek.
Zkontrolovány poštovní objekty – zobrazuje počet zkontrolovaných poštovních objektů.

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

Pod těmito kategoriemi je zobrazena mapa světa s aktuální virovou situací. Přítomnost virů v dané zemi je reprezentována barvami, kdy tmavší barva představuje vyšší výskyt. Země, ze kterých nemáme žádná data, jsou šedé. Při najetí myší nad konkrétní zemi se zobrazí přesná data. Jednotlivé kontinenty si můžete pomocí ovládacích prvků přiblížit.

Přímo z bezpečnostního přehledu můžete aktivovat také následující funkce:

- Správce hesel
- Šifrování dat
- Rodičovská kontrola
- Anti-Theft

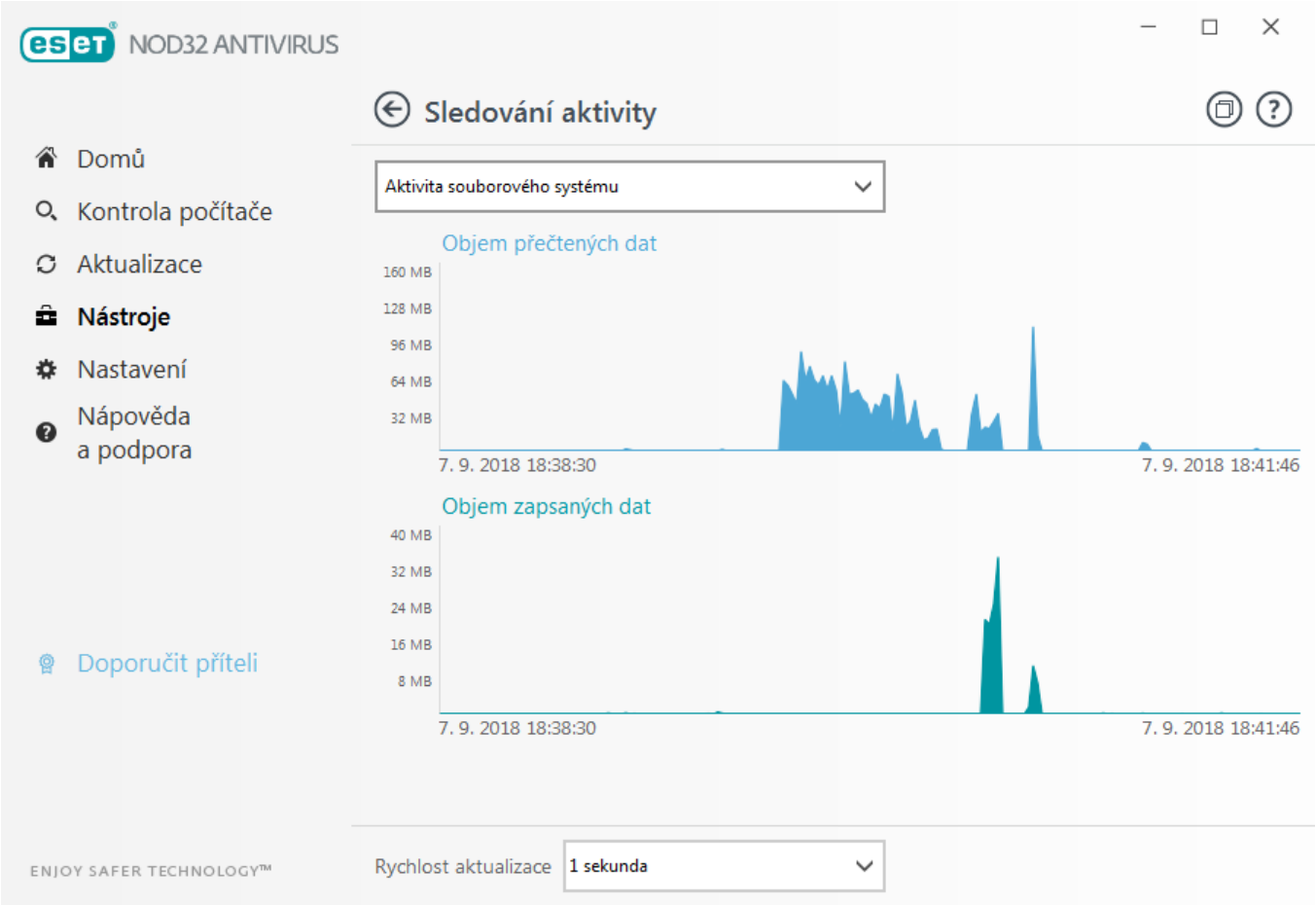
Po aktivování některé z výše uvedených funkcí se již nebude zobrazovat v bezpečnostním přehledu jako nefunkční.

Kliknutím na ozubené kolečko v pravém horním rohu můžete zapnout/vypnout upozornění na bezpečnostní přehled, případně si zobrazit data ze posledních 30 dní, resp. od aktivace produktu. Pokud jste produkt ESET NOD32 Antivirus nainstalovali před méně než 30 dny, zobrazí se pouze data od instalace produktu. Výchozí dobou pro zobrazení dat je 30 dní.

Pomocí možnosti **Vynulovat data** odstraníte všechny statistiky a data z bezpečnostního přehledu. Tuto akci je nutné potvrdit, pokud nemáte definováno jinak v rozšířeném nastavení (dostupném po stisknutí klávesy F5) v sekci **Uživatelské rozhraní** > **Upozornění a události** > **Potvrzovací zprávy**.

4.4.1.4 Sledování aktivity

Pro zjednodušené sledování činnosti systému je na záložce **Nástroje** > **Sledování aktivity** k dispozici grafické rozhraní, které umožňuje v reálném čase sledovat aktivitu souborového systému. Ve spodní části se zobrazuje časová osa, jejíž měřítko můžete změnit pomocí kontextového menu **Krok**.



K dispozici jsou následující rozlišení měřítka:

- **Krok: 1 sekunda** – graf se obnoví každou sekundu a časová osa zobrazuje posledních 10 minut,
- **Krok: 1 minuta (posledních 24 hodin)** – graf se obnoví každou minutu a časová osa zobrazuje posledních 24 hodin,
- **Krok: 1 hodina (poslední měsíc)** – graf se obnoví každou hodinu a zobrazuje poslední měsíc,
- **Krok: 1 hodina (vybraný měsíc...)** – graf se obnoví každou hodinu a zobrazuje vybraný měsíc. Pokud chcete zobrazit data z jiného měsíce, klikněte na tlačítko **Změnit měsíc**.

Vertikální osa grafu probíhající aktivity souborového systému reprezentuje množství přečtených dat (modrá) a zapsaných dat (červená). Obě tyto hodnoty jsou vyčísleny v KB/MB/GB. Pod grafem je zobrazena legenda, která zároveň slouží jako přepínač zobrazovaných hodnot. Po ponechání kurzoru na vybrané položce legendy se v grafu zobrazí pouze tato položka.

4.4.1.5 ESET SysInspector

ESET SysInspector je aplikace, která slouží k získání podrobných informací o systému zahrnující seznam nainstalovaných ovladačů a programů, síťových připojeních a důležitých údajů z registru. Tyto informace mohou být užitečné při zjišťování příčiny podezřelého chování systému ať už vlivem nekompatibility software/hardware nebo infekce škodlivého kódu.

V okně SysInspector se nachází informace o vytvořených protokolech:

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

Dostupné jsou následující akce:

- **Zobrazit** – zobrazí vytvořený záznam. Případně klikněte pravým tlačítkem na vybraný záznam a z kontextového menu vyberte možnost **Zobrazit**.
- **Porovnat** – porovná dva vytvořené záznamy,
- **Přidat** – vytvoří nový záznam. Vyčkejte na dokončení protokolu ESET SysInspector (po dokončení se ve sloupci *Stav* zobrazí **Vytvořeno**),
- **Odstranit** – odebere 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. Vyčkejte na dokončení protokolu ESET SysInspector (po dokončení se ve sloupci *Stav* zobrazí **Vytvořeno**),
- **Odstranit** – odstraní vybraný záznam,
- **Odstranit vše** – vymaže všechny záznamy,
- **Exportovat...** – uloží záznamy do *.XML* souboru nebo do zazipovaného *.XML* souboru.

4.4.1.6 Plánovač

Plánovač spravuje a spouští naplánované úlohy s předem nakonfigurovaným nastavením.

Plánovač je dostupný v hlavním okně programu ESET NOD32 Antivirus na záložce **Nástroje** > **Plánovač**. Plánovač obsahuje přehledný seznam všech naplánovaných úloh, jejich nastavení a vlastností, které se provádějí ve stanovený čas pomocí definovaných profilů.

Plánovač slouží k plánování úloh jako je např. aktualizace modulů, kontrola disku, kontrola souborů spouštěných po startu nebo pravidelná údržba protokolů. Přímo z hlavního okna můžete **Přidat** nebo **Odstranit** úlohu kliknutím na příslušné tlačítko. Kontextové menu, které se otevře po kliknutí pravým tlačítkem myši v okně plánovače, umožňuje následující akce: zobrazení detailních informací o úloze, okamžité provedení úlohy, přidání nové úlohy, úpravu resp. odstranění již existující úlohy. Zaškrtávacím tlačítkem vedle úkolu je možné úlohu deaktivovat.

Standardně **Plánovač** zobrazuje následující naplánované úlohy:

- **Údržba protokolů,**
- **Pravidelná automatická aktualizace,**
- **Automatická aktualizace po modemovém spojení,**
- **Automatická aktualizace po přihlášení uživatele,**
- **Kontrola souborů spouštěných po startu** (při přihlášení uživatele na počítač),
- **Kontrola souborů spouštěných po startu** (při úspěšné aktualizaci detekčních modulů)**.**

Nastavení existujících naplánovaných úloh (a to jak předdefinovaných, tak vlastních) můžete měnit přes kontextové menu kliknutím na možnost **Změnit...**, nebo vybráním požadované úlohy, kterou chcete změnit, a kliknutím na tlačítko **Změnit**.

Přidání nové úlohy

1. Klikněte na tlačítko **Přidat** ve spodní části okna.
2. Zadejte název úlohy.
3. Vyberte požadovaný typ úlohy:
   - **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 detekčních i programových modulů.
4. Pro aktivování úlohy přepněte přepínač do polohy **Zapnuto** (to můžete udělat kdykoli později přímo v seznamu naplánovaných úloh) a po kliknutí na tlačítko **Další** vyberte interval opakování:

- **Jednou** – úloha se provede pouze jednou v naplánovaném čase.
- **Opakovaně** – úloha se bude provádět opakovaně každých x minut.
- **Denně** – úloha se provede každý den ve stanový čas.
- **Týdně** – úloha se bude provádět v určitý den/dny v týdnu ve stanoveném čase.
- **Při události** – úloha se provede při určité situaci.

5. Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii nebo počítače z UPS, aktivujte možnost **Nespouštět úlohu, pokud je počítač napájen z baterie**. Po kliknutí na tlačítko Další zadejte **Čas provedení úlohy**. Pokud nebude možné úlohu v daném čase spustit, nastavte alternativní termín pro spuštění úlohy:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

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

4.4.1.7 Kontrola systému

Tento nástroj vám pomůže obnovit počítač do funkčního a použitelného stavu před jeho infiltrací. Škodlivý kód může v některých případech zakázat přístup k systémovým součástem jako je například Editor registru, Správce úloh nebo Windows Update. Použitím tohoto nástroje obnovíte klíčová nastavení systému na výchozí hodnoty.

Tento nástroj detekuje problém v následujících kategoriích:

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

Tento nástroj:

- se může spustit po detekci hrozby
- můžete spustit ručně (kliknutím na Obnovit)

Prohlédněte si změny, které produkt provedete a v případě potřeby tato nastavení obnovte na výchozí hodnoty kliknutím na tlačítko **Obnovit** nebo **Obnovit vše**.

Poznámka:
Tento nástroj může použít pouze uživatel s administrátorským oprávněním.

4.4.1.8 ESET SysRescue

ESET SysRescue je nástroj, který umožňuje vytvořit bootovatelný disk obsahující produkt ESET Security – tedy ESET NOD32 Antivirus, ESET Internet Security, ESET Smart Security, ESET Smart Security Premium nebo jiný produkt určený pro servery. Hlavní výhodou ESET SysRescue je fakt, že ESET Security běží zcela nezávisle na aktuálně nainstalovaném operačním systému, přičemž má přímý přístup k disku a celému souborovému systému. Díky tomu je takto možné například odstranit infiltraci, kterou nebylo možné vymazat standardním způsobem při spuštěném operačním systému apod.

4.4.1.9 Cloudová ochrana

ESET LiveGrid® (nová generace systému včasného varování ESET ThreatSense.Net) využívá data od uživatelů bezpečnostních produktů ESET z celého světa a zasílá je do virových laboratoří společnosti ESET. Díky podezřelým vzorkům a souvisejícím meta informacím dokážeme prostřednictvím tohoto systému okamžitě reagovat na nejnovější hrozby. Více informací o tomto systému naleznete ve slovníku pojmů.

Uživatelé mají díky tomuto systému možnost ověřit přímo z rozhraní produktu ESET, případně kontextového menu, reputaci souborů a běžících procesů – a získat o těchto objektech další informace. V průběhu instalace <%PN%> máte na výběr ze dvou možností:

- Můžete se rozhodnout, že nechcete zapínat <%ELG%>. Nepřijdete tím o žádnou funkci, ale v některých případech může <%PN%> reagovat na nové hrozby se zpožděním – dokud nedojde k aktualizaci detekčního jádra..
- Můžete <%ELG%> nakonfigurovat pro odesílání anonymních informací o nových hrozbách společně s informací, kde byl soubor detekován. Takový soubor může být odeslán do virové laboratoře společnosti ESET k analyzování, což nám pomůže vylepšit schopnosti detekce škodlivého kódu a zajistí rychlejší vydání aktualizace detekčního jádra.

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

Ve výchozí konfiguraci ESET NOD32 Antivirus odesílá na podrobnou analýzu do virové laboratoře ESET pouze podezřelé soubory. Pokud se infiltrace nachází v souborech s určitými příponami, jako například .doc a .xls, nikdy se neodesílá jejich obsah. Mezi výjimky můžete přidat další přípony souborů, jejichž obsah nechcete odesílat.

Reputační systém ESET LiveGrid® zajišťuje cloudový whitelisting a blacklisting objektů. Jeho konfiguraci naleznete v rozšířeném nastavení (dostupném po stisknutí **klávesy F5** v hlavním okně programu) v sekci **Detekční jádro** > **Cloudová ochrana**.

Zapnout reputační systém <%ESET_LIVE_GRID%> (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_LIVE_GRID%> – 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 – pomocí této možnosti umožníte společnosti ESET získávat z vašeho zařízení informace o nově detekovaných hrozbách zahrnující název hrozby, datum a čas detekce, modul, který hrozbu detekoval a související metadata, verzi produktu, konfiguraci a informace o operačním systému.

Kontaktní e-mail (nepovinný údaj) – zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Prosím, mějte na paměti, že od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.

Odesílání vzorků

Odesílat podezřelé vzorky

Pomocí této možnosti umožníte zasílání vzorků do společnosti ESET k bližší analýze pro zajištění vylepšení detekce.

- **Všechny infikované vzorky**
- **Všechny vzorky kromě dokumentů**
- **Neodesílat**

Odesílat podezřelé vzorky

Podezřelé vzorky považované za hrozby a vzorky s obvyklou charakteristikou nebo chováním budou odesílány k analýze do společnosti ESET.

- **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** – vybráním této možnosti umožníte zasílání částí nebo celých zpráv, včetně příloh, označených jako spam k bližší analýze do společnosti ESET. Tímto krokem přispějete k vylepšení detekce nevyžádaných e-mailů.
- **Dokumenty** – zahrnuje Microsoft Office dokumenty a PDF s aktivním obsahem.

Výjimky – pomocí seznamu výjimek můžete vyloučit složky a konkrétní typy souborů z odeslání k analýze (například soubory obsahující citlivé informace jako dokumenty nebo tabulky). Seznam zobrazených souborů a složek nebude nikdy odeslán do virových laboratoří ESET k další analýze na přítomnost škodlivého kódu. Standardně se neodesílají nejrozšířenější typy souborů (.doc atp.) a v případě potřeby můžete tento seznam kdykoli rozšířit.

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

Maximální velikost vzorku (MB) – definujte maximální velikost vzorku, který může být odeslán.

4.4.1.9.1 Podezřelé soubory

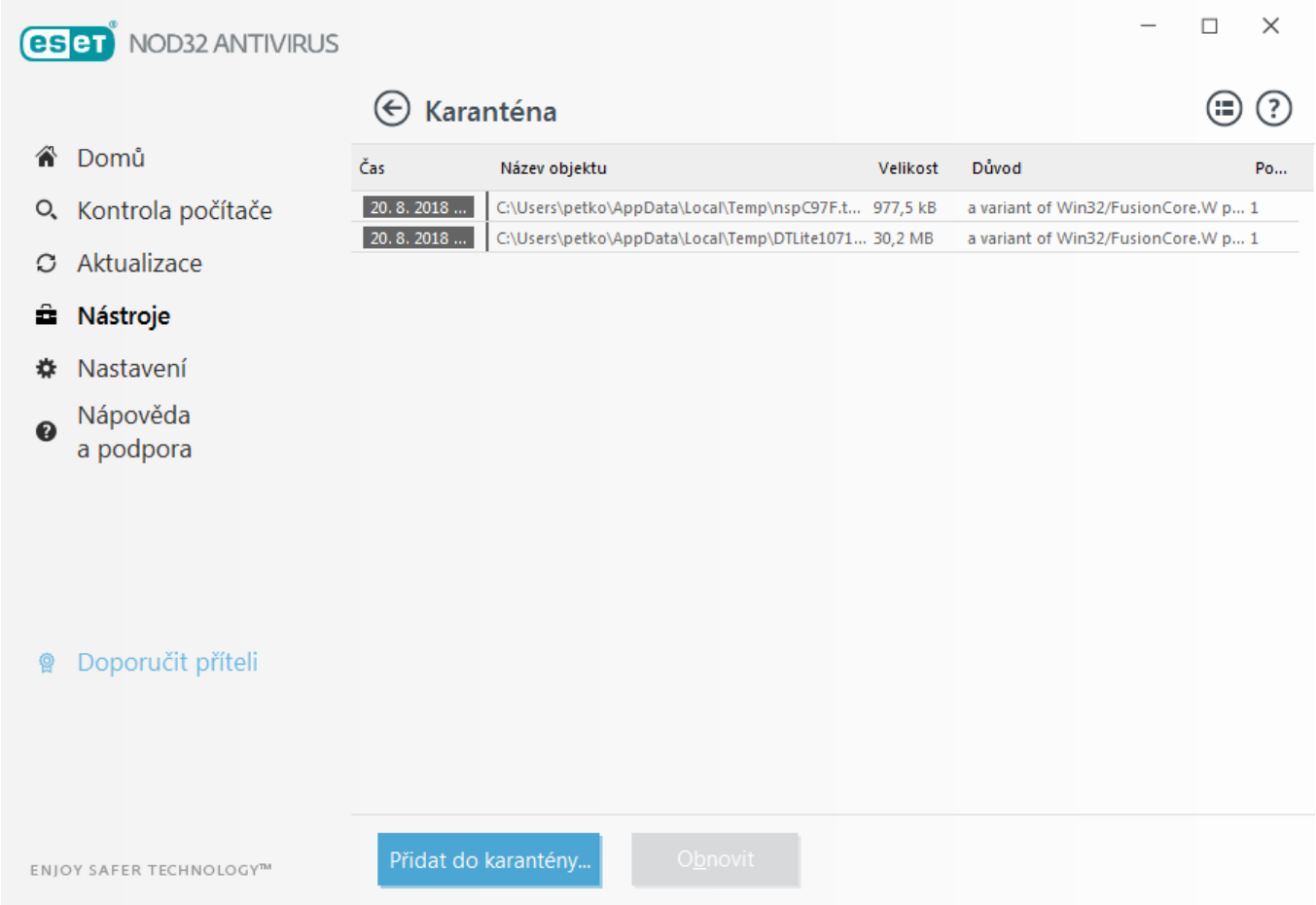
Po kliknutí na **Změnit** na řádku **Výjimky** na záložce ESET LiveGrid® můžete nastavit, jakým způsobem budou podezřelé soubory odesílány do virové laboratoře společnosti ESET.

Pokud naleznete podezřelý soubor, můžete jej odeslat k analýze do naší virové laboratoře. V případě, že jedná o nebezpečnou aplikaci, její detekce bude přidána v některé z nejbližších aktualizací detekčního jádra.

4.4.1.10 Karanténa

Hlavním úkolem karantény je bezpečné uchovávání infikovaných souborů v šifrované podobě. Ve většině případů se může jednat o soubory, které není možné vyléčit, není jisté, zda je bezpečné jejich odstranění, případně se jedná o chybnou detekci antivirové ochrany ESET NOD32 Antivirus.

Do karantény můžete ručně přidat jakýkoli soubor. To je vhodné v případě, kdy podezřelý soubor nebyl detekován antivirovým skenerem. Soubory z karantény můžete zaslat k analýze do virové laboratoře společnosti 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).

Přidání do karantény

ESET NOD32 Antivirus přidává soubory do karantény automaticky při jejich vymazání (pokud jste tuto možnost v okně s upozorněním nezrušili). Pokud uznáte za vhodné, může pomocí tlačítka **Přidat do karantény...** do karantény přidat podezřelý soubor ručně. V takovém případě se však soubor ze svého původního umístění nesmaže. Kromě tlačítka **Přidat do karantény...** lze tuto akci provést kliknutím pravým tlačítkem myši v okně **Karantény** a vybrat možnost **Přidat do karantény...**.

Obnovení z karantény

Soubory uložené v karanténě můžete vrátit do jejich původního umístění, odkud byly vymazány. Slouží k tomu funkce **Obnovit**, která je rovněž přístupná také z kontextového menu po kliknutí pravým tlačítkem myši na daný soubor v karanténě. V kontextovém menu se dále nachází možnost **Obnovit do...**, která dokáže obnovit soubor na jiné místo, než to, ze kterého byl původně smazán. Pokud se jedná o potenciálně nechtěnou aplikace, v takovém případě bude v kontextovém menu dostupná možnost **Obnovit a vyloučit z kontroly**. Pro více informací o tomto typu aplikací přejděte do slovníku pojmů.

Odstranění z karantény – klikněte pravým tlačítkem na objekt v karanténě z kontextového menu vyberte možnost **Odstranit z karantény**. Případně vyberte objekt a stiskněte klávesu **Delete**.

Poznámka:
Pokud program do karantény umístil soubor z důvodu falešného detekce, 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, 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**.

4.4.1.11 Proxy server

Ve velkých lokálních sítích, může připojení do internetu zajišťovat tzv. proxy server. V takovém případě musí být proxy server správně zadán v nastavení programu, jinak by mohlo dojít k potížím se stahováním aktualizací. Nastavení proxy serveru je možné v ESET NOD32 Antivirus definovat na dvou odlišných místech v rámci Rozšířeného nastavení.

V prvním případě můžete konfigurovat proxy server v části **Nástroje** > **Proxy server**. Definování proxy serveru na této úrovni má pro ESET NOD32 Antivirus důsledek globálního nastavení proxy serveru. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

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

V případě, že komunikace s proxy serverem vyžaduje autentifikaci, je potřeba také zaškrtnout pole **Proxy server vyžaduje autorizaci** a zadat patřičné údaje do polí **Uživatelské jméno** a **Heslo**. Pro získání automatického nastavení proxy serveru můžete kliknout na tlačítko **Vyhledat**, tímto se přenese nastavení z programu Internet Explorer.

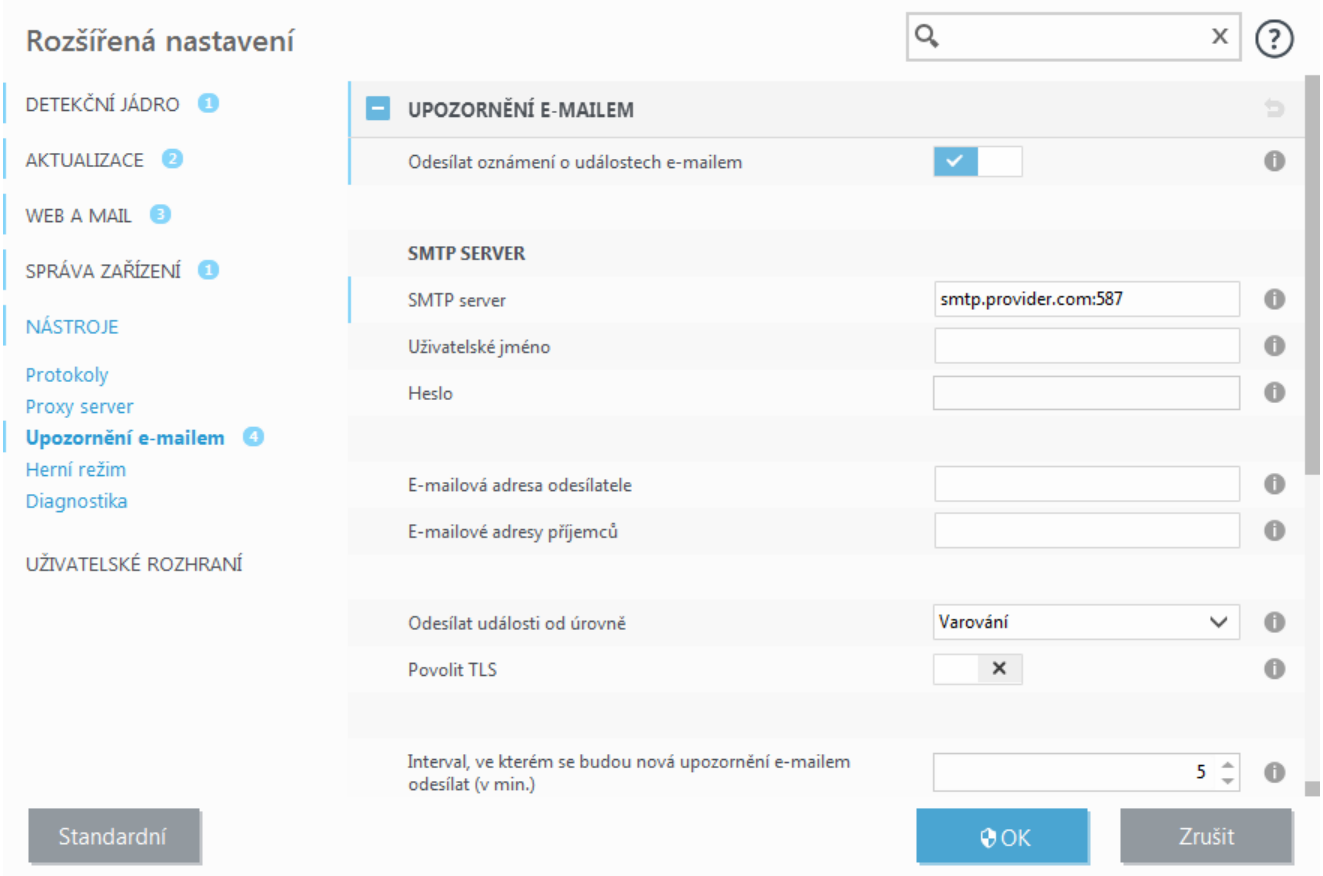
Poznámka:
Tímto způsobem není možné získat autentifikační údaje (uživatelské jméno a heslo). Pokud jsou pro přístup k proxy serveru vyžadovány, musíte je zadat ručně.

Pokud aktivujete možnost **Použít přímé spojení, pokud není dostupný proxy server**, ESET NOD32 Antivirus automaticky zkusí připojení k aktualizačním serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.

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

4.4.1.12 Upozornění e-mailem

ESET NOD32 Antivirus dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pomocí možnosti **E-mailem odesílat oznámení o událostech** aktivujete tuto funkci a zasílání upozornění e-mailem.



POZNÁMKA:
ESET NOD32 Antivirus podporuje SMTP servery využívající TLS šifrování.

SMTP server

SMTP server – adresa SMTP serveru prostřednictvím kterého budou zprávy odesílány (například *smtp.provider.com:587*, pokud nespecifikujete port, použije se výchozí 25).

Uživatelské jméno a **Heslo** – v případě, že SMTP server vyžaduje autorizaci, musíte vyplnit tato pole pro přístup k SMTP.

E-mailová adresa odesílatele – specifikuje adresu odesílatele, která se použije v hlavičce e-mailové zprávy.

E-mailová adresa příjemce – specifikuje adresu příjemce, která se použije v hlavičce e-mailové zprávy.

Odesílat události od úrovně – specifikuje, od které úrovně důležitosti se budou upozornění na události odesílat.

- **Diagnostické** – e-mailem se odešlou diagnostické informace pro řešení problémů a všechny níže uvedené záznamy.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy.
- **Varování** – e-mailem se odešlou upozornění na chyby a varovné zprávy (například Anti-stealth není funkční nebo selhala aktualizace modulů).
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například je nefunkční ochrana dokumentů).
- **Kritické** – e-mailem se odešlou upozornění na kritické stavy aplikace (například je problém s antivirovou ochranou nebo upozornění na infiltraci v systému).

Povolit TLS – umožní odesílání zpráv prostřednictvím zabezpečeného TLS spojení.

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 událostí, 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

Formát zprávy o události – formát zprávy, která se zobrazí na vzdáleném počítači.

Formát zprávy s upozorněním na hrozbu – přednastavený formát zpráv je vhodný pro většinu situací. Měnit jej doporučujeme pouze v ojedinělých případech.

Použít znaky národní abecedy – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250). Pokud ponecháte tuto možnost nezaškrtnutou, zpráva se převede do ASCII 7-bit (v takovém případě se například znak "á" změní na "a" a neznámý symbol bude označen nahrazen otazníkem "?").

Použít Quoted-printable kódování – e-mailová zpráva bude zakódována do Quoted-printable (QP) formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

4.4.1.12.1 Formát zprávy

Můžete definovat formát zpráv, které se odesílají na vzdálené počítače při výskytu dané události.

Upozornění na hrozby a informační oznámení mají přednastavený formát. Měnit jej doporučujeme pouze v ojedinělých případech, například pokud používáte automaticky systém pro zpracovávání e-mailů.

Ve formátu zpráv se nacházejí klíčová slova označená procentem (%), která jsou při vytváření zpráv nahrazena odpovídajícími hodnotami. Dostupná jsou následující klíčová slova:

- **%TimeStamp%** – datum a čas události,
- **%Scanner%** – modul, který zaznamenal událost,
- **%ComputerName%** – název počítače, na kterém došlo k události,
- **%ProgramName%** – program, který způsobil událost,
- **%InfectedObject%** – název škodlivého souboru, e-mailové zprávy apod.,
- **%VirusName%** – název infekce,
- **%Action%** – provedená akce,
- **%ErrorDescription%** – popis chyby.

Klíčová slova **%InfectedObject%** a **%VirusName%** se používají pouze v upozorněních na hrozbu. Klíčové slovo **%ErrorDescription%** se používá pouze v informačních upozorněních.

Použít znaky národní abecedy – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250). Pokud ponecháte tuto možnost nezaškrtnutou, zpráva se převede do ASCII 7-bit (v takovém případě se například znak "á" změní na "a" a neznámý symbol bude označen jako "?").

Použít kódování pro znaky národní abecedy – e-mailová zpráva bude zakódována do Quoted-printable (QP) formátu, který využívá ASCII znaky, čímž se mohou bezchybně přenášet prostřednictvím e-mailu speciální (národní) znaky v 8-bitovém formátu (áéíóú).

4.4.1.13 Odesílání souborů analýze

Existuje možnost zaslání podezřelého souboru k analýze do společnosti ESET. Formulář k této akci naleznete na záložce **Nástroje** > **Odeslat soubor k analýze**. 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.

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

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

Kontaktovat zpět vás budeme pouze v případě, že budeme potřebovat více informací.

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

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

Soubor/Stránka – cesta k souboru nebo URL adresa.

Kontaktní e-mail – na tento e-mail vás budou pracovníci virové laboratoře ESET kontaktovat, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné. Na kontaktní e-mail nebude zaslána žádná odezva, protože denně do společnosti ESET chodí několik desítek tisíc souborů a není možné na každý e-mail reagovat.

4.4.1.14 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 NOD32 Antivirus můžete nastavit, od jaké úrovně chcete být informováni na chybějících systémové aktualizace. Na výběr jsou následující možnosti:

- **Žádné aktualizace** – nebudou nabízeny žádné aktualizace,
- **Volitelné aktualizace** – budou nabízeny aktualizace s nízkou prioritou a všechny následující,
- **Doporučené aktualizace** – budou nabízeny běžné aktualizace a všechny následující,
- **Důležité aktualizace** – budou nabízeny důležité aktualizace a všechny následující,
- **Kritické aktualizace** – budou nabízeny pouze kritické aktualizace.

Kliknutím na tlačítko **OK** uložíte změny. Zobrazení okna dostupných aktualizací proběhne po ověření stavu na aktualizačním serveru. Samotné zobrazení dostupných aktualizací proto nemusí nutně proběhnout ihned po uložení změn.

4.4.1.15 ESET CMD

Prostřednictvím této funkce můžete importovat a exportovat konfiguraci produktu ESET NOD32 Antivirus pomocí příkazového řádku (ecmd.exe). Pokud tuto funkci neaktivujete, konfiguraci programu můžete importovat/exportovat výhradně prostřednictvím grafického rozhraní.

Po aktivování funkce ESET CMD (v **rozšířeném nastavení** v sekci **Nástroje** > **ESET CMD**) si vyberte způsob ověření:

- **Žádný** – pokud vyberete tuto možnost, nebudete vyžadována autentifikace. 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* soubor není podepsán.

Poté co aktivujete funkci ESET CMD, můžete pro importování a exportování konfigurace produktu ESET NOD32 Antivirus používat příkazový řádek. Příkazy můžete pouštět manuálně, případně si operace v rámci automatizace naskriptovat.

DŮLEŽITÉ:
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.

Příklad:
Konfiguraci z nainstalovaného produktu exportujete příkazem:
```
ecmd /getcfg c:\config\settings.xml
```

Konfiguraci do nainstalovaného produktu naimportujete příkazem:
```
ecmd /setcfg c:\config\settings.xml
```

Poznámka:
Rozšířené emcd příkazy je možné používat pouze lokálně.

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 podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`

DŮLEŽITÉ:
Hodnota parametru `/version` závisí na verzi ESET NOD32 Antivirus. Pro starší verze použijte `/version 1`. Pro ESET NOD32 Antivirus ve verzi 11.1 a novější použijte `/version 2`.

5. Zadejte heslo, které jste si nastavili pro přístup do nastavení. Následně bude vaše *.xml* soubor s konfigurací programu podepsán a můžete jej prostřednictvím ESET CMD importovat do jiné instalace <%PN%>.

Příklad:
Konfigurační soubor podepíšete tímto příkazem:
```
xmlsigntool /version 1 c:\config\settings.xml
```

VAROVÁNÍ:

Aktivováním ESET CMD bez nastaveného ověřování představuje bezpečnostní riziko a nedoporučujeme tuto možnost používat v produkčních prostředích. V takovém případě je možné do produktu importovat nepodepsané konfigurace. Pokud dosud nemáte nastaveno heslo pro ochranu produktu, přejděte v rozšířeném nastavení do sekce **Uživatelské rozhraní** > **Přístup k nastavení**.

4.5 Uživatelské rozhraní

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

V části prvky uživatelského rozhraní upravíte vzhled rozhraní a množství použitých efektů.

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

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

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu použijte sekci Přístup k nastavení a nastavte si heslo.

4.5.1 Prvky uživatelského rozhraní

ESET NOD32 Antivirus umožňuje přizpůsobit nastavení pracovního prostředí programu vašim potřebám. Tyto možnosti jsou dostupné v **Rozšířeném nastavení** (dostupném po stisknutí klávesy F5 v hlavním okně programu) na záložce **Uživatelské rozhraní** > **Prvky uživatelského rozhraní**.

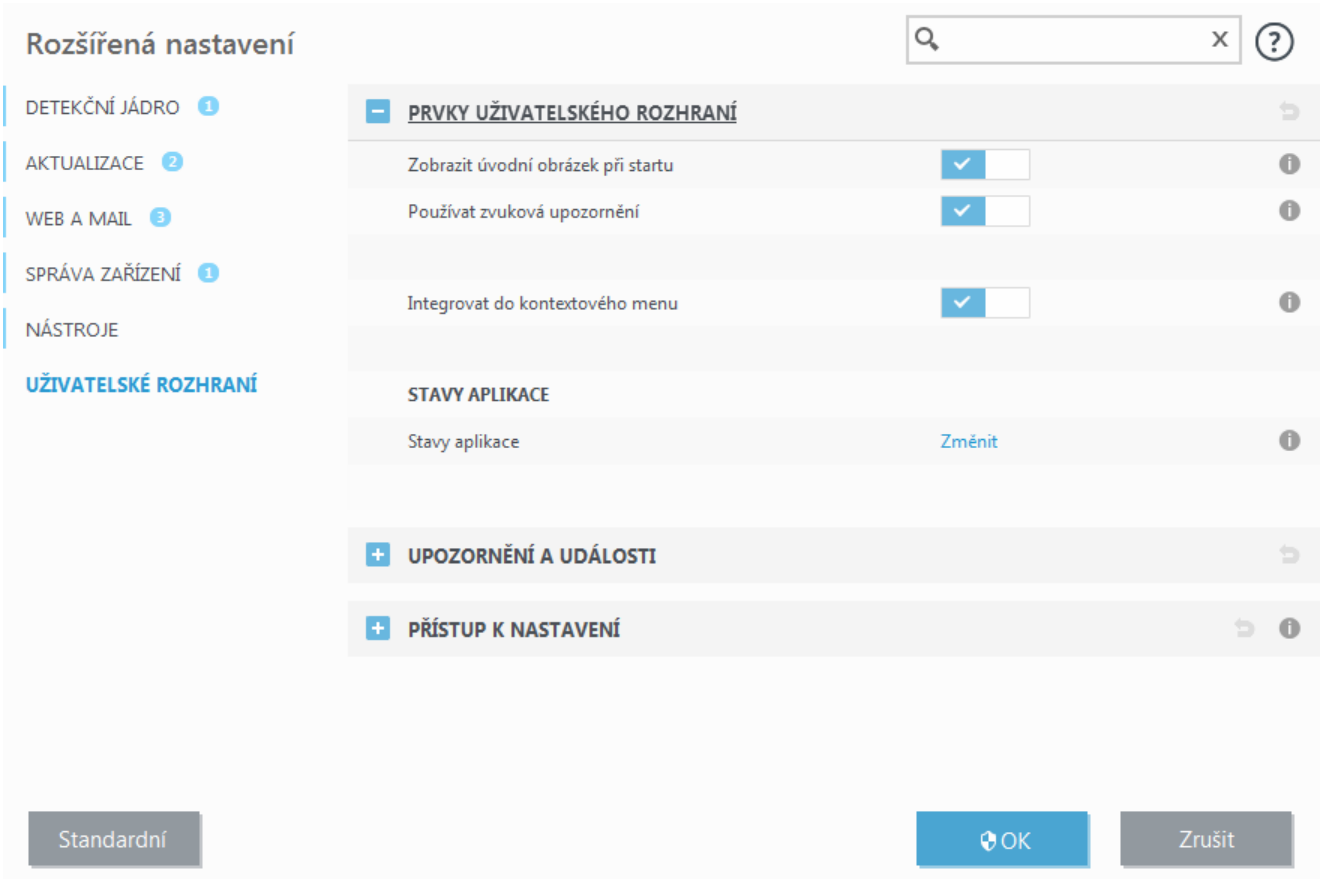
Pomocí možnosti **Zobrazit úvodní obrázek při startu** můžete zapnout nebo vypnout zobrazování úvodního obrázku při spouštění ESET NOD32 Antivirus.

Pokud chcete, aby ESET NOD32 Antivirus přehrával zvuky při důležitých událostech, zaškrtněte možnost **Používat zvuková upozornění**.

Integrovat do kontextového menu – integruje ovládací prvky ESET NOD32 Antivirus do kontextového menu.

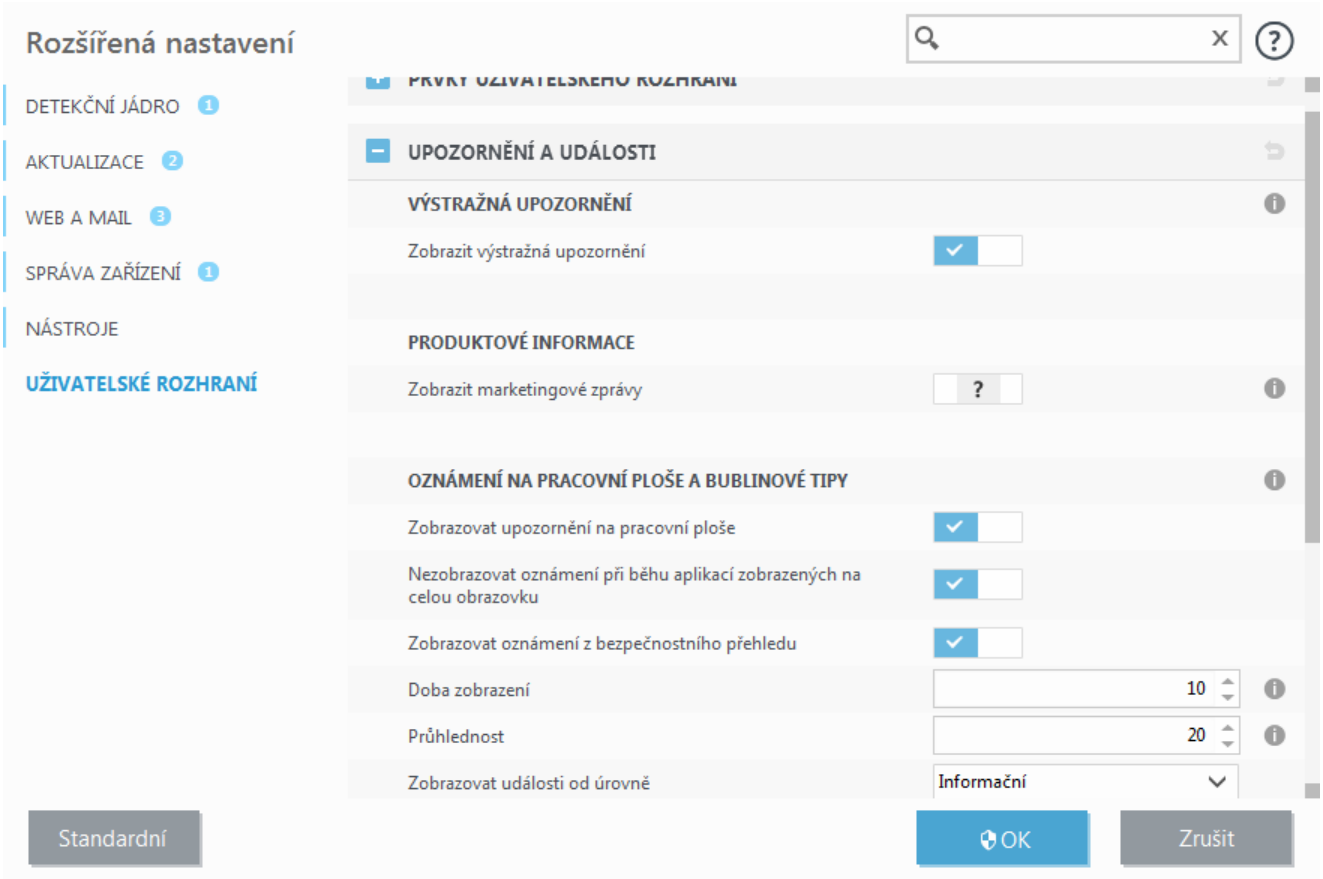
Stavy aplikace

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



4.5.2 Upozornění a události

Okno **Upozornění a události** se nachází v sekci **Uživatelské rozhraní** a umožňuje konfiguraci výstražných a informačních hlášení ESET NOD32 Antivirus, například informace o úspěšné aktualizaci. Nastavit můžete dobu zobrazení a průhlednost bubliny s upozorněním (pouze na systémech, které to podporují).



Výstražná upozornění

Zobrazování všech oken s upozorněním vypnete odškrtnutím možnosti **Zobrazit výstražná upozornění**. Toto doporučujeme nastavit pouze ve specifických situacích. Pro většinu uživatelů doporučujeme ponechat tuto možnost aktivní.

Produktové informace

Zobrazit marketingové zprávy – in-product messaging představuje kanál, prostřednictvím kterého vás můžete informovat o novinkách a ESET akcích. Příjem těchto marketingových informací vyžaduje váš souhlas. Standardně vám žádné zprávy nejsou zasílány a ve výchozím nastavení je u této položky zobrazena ikona otazníku. Pokud chcete dostávat tento druh informací, aktivujte tento přepínač. Vypnutím této možnosti nebudete dostávat žádné marketingové informace.

Oznámení na pracovní ploše

Upozornění na ploše a bublinové tipy slouží pouze pro zobrazování informací a nenabízejí ani nevyžadují interakci uživatele. Zobrazují se v pravém dolním rohu obrazovky. Pro aktivování této možnosti použijte přepínač **Zobrazovat upozornění na pracovní ploše**.

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.

Zobrazit oznámení z bezpečnostního přehledu – pomocí této možnosti zapnete nebo vypnete zobrazování oznámení v bezpečnostního přehledu.

V rozbalovacím menu **Zobrazovat události od úrovně** můžete nastavit bezpečnostní úroveň, od které chcete být na události informováni.

- **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 (chyba při startu antivirové ochrany atp.).

Poslední možností v tomto okně je nastavení příjemce zpráv ve víceuživatelských systémech. Do pole **Ve víceuživatelském prostředí posílat systémová hlášení tomuto uživateli** zadejte jméno uživatele, kterému bude ESET NOD32 Antivirus zobrazovat systémová oznámení. 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.

Informační okna

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

Potvrzovací zprávy – pomocí této možnosti můžete ovlivnit, která dialogové se budou nebo nebudou zobrazovat.

4.5.2.1 Rozšířená nastavení

V rozbalovacím menu **Zobrazovat události od úrovně** můžete nastavit bezpečnostní úroveň, od které chcete být informováni.

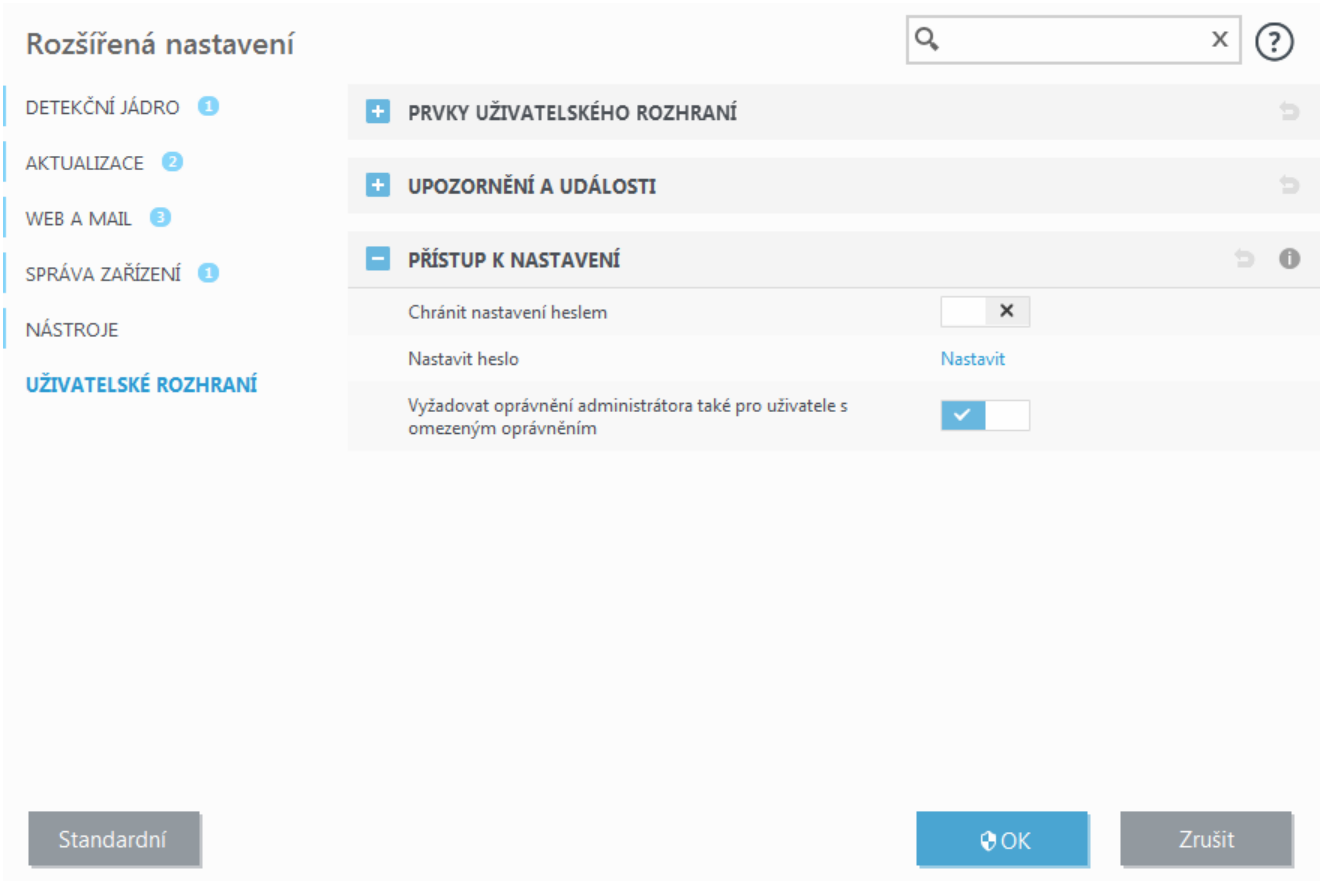
- **Diagnostické** – obsahují informace důležité pro ladění programu a všechny níže uvedené záznamy,
- **Informační** – obsahují informační zprávy, například o úspěšné aktualizaci a všechny níže uvedené záznamy,
- **Varování** – obsahují varovné zprávy a kritické chyby,
- **Chyby** – obsahují chyby typu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

Poslední možností v tomto okně je nastavení příjemce zpráv ve víceuživatelských systémech. Do pole **Ve víceuživatelském prostředí posílat systémová hlášení uživateli** zadejte jméno uživatele, kterému bude ESET NOD32

Antivirus zobrazovat systémová oznámení. 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.

4.5.3 Přístup k nastavení

Správné nastavení ESET NOD32 Antivirus je velmi důležité pro zachování celkové bezpečnosti systému a jeho neoprávněná změna může vést ke snížení stability a ochrany systému. Pro ochranu nastavení heslem přejděte v **Rozšířeném nastavení** (dostupném po stisknutí **klávesy F5** v hlavním okně programu) na záložku **Uživatelské rozhraní** > **Přístup k nastavení**).



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

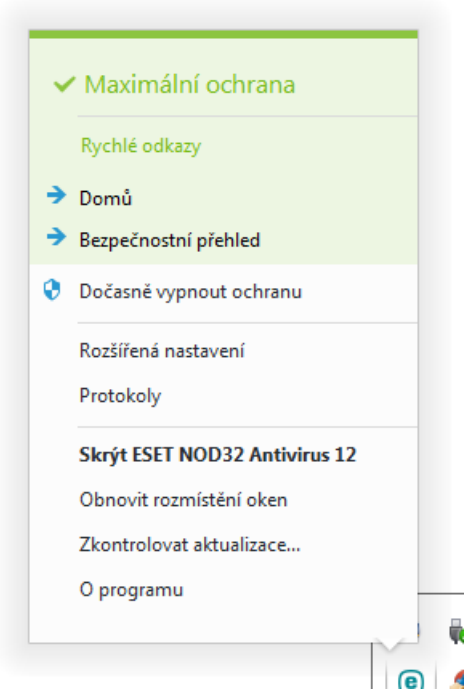
Pro nastavení změnu stávajícího hesla klikněte na **Nastavit heslo**.

> **Poznámka:**
> Po nastavení hesla budete při přístupu do rozšířeného nastavení a odinstalaci produktu vyzváni k zadání tohoto hesla. Pokud heslo zapomenete, klikněte na možnost **Obnovit heslo** a dále zadejte e-mailovou adresu uvedenou při nákupu/registraci licence. Následně na e-mail obdržíte ověřovací kód a návod, jak heslo resetovat. Pro více informací přejděte do kapitoly Jak obnovit heslo do rozšířeného nastavení.

Vyžadovat oprávnění administrátora také pro uživatele s omezeným oprávněním – pokud přihlášený uživatel nemá administrátorská práva, pak při pokusu o změnu některých nastavení bude vyžadováno přihlášení administrátora (podobně jako je tomu ve Windows Vista a vyšších při zapnutém UAC). Taková změna zahrnuje vypnutí modulů ochrany.

4.5.4 Ikona v oznamovací oblasti

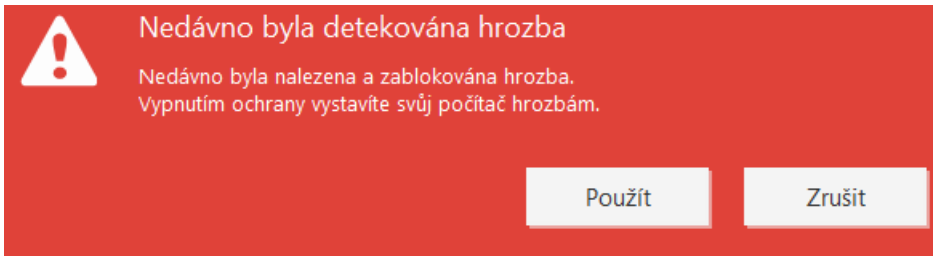
Nejdůležitější možnosti a funkce programu jsou dostupné přímo ze systémové oznamovací oblasti (v pravém dolním rohu obrazovky). Stačí kliknout pravým tlačítkem myši na ikonu programu .



Rychlé odkazy – v této části máte dostupné odkazy pro rychlý přístup k nejdůležitějším součástem programu ESET NOD32 Antivirus.

Dočasně vypnout ochranu – zobrazí potvrzovací dialog, pomocí kterého vypnete Antivirovou a antispywarovou ochranu – ta chrání systém proti škodlivým útokům tím, že kontroluje soubory, e-maily a komunikaci prostřednictvím internetu.

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



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

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

Skrýt ESET NOD32 Antivirus – skryje všechna otevřená okna ESET NOD32 Antivirus.

Obnovit rozmístění oken – obnoví přednastavenou velikost a pozici okna ESET NOD32 Antivirus na obrazovce.

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

O programu – poskytuje informace o systému, instalovaném programu ESET NOD32 Antivirus a všech jeho programovaných modulech. Také zde naleznete datum platnosti licence. Ve spodní části okna se nachází informace o operačním systému a systémových prostředcích.

5. Pokročilý uživatel

5.1 Profily

Správa profilů se v programu ESET NOD32 Antivirus používá na dvou místech – při **Volitelné kontrole počítače** a **Aktualizaci**.

Volitelná kontrola počítače

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

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

Příklad:
Chcete vytvořit vlastní profil kontroly počítače a částečně vám vyhovuje nastavení předdefinovaného profilu **Smart kontrola počítače**, ale nechcete zároveň kontrolovat runtime archivy, potenciální nebezpečné aplikace a přitom požadujete **Přísné léčení**? Vytvořte nový profil kliknutím na tlačítko **Přidat** v Seznamu profilů Následně nově vytvořený profil vyberte z rozbalovacího menu **Aktivní profil** nastavte si parametry kontroly podle potřeby.

Aktualizace

Editor profilů umožňuje vytvořit nové aktualizační profily odlišné od standardního **Můj profil**. Ty se používají pouze v případě, že používáte různé způsoby připojení na aktualizační servery.

Příkladem může být firemní notebook, který se v interní síti aktualizuje z mirroru, ale mimo firemní síť se aktualizace stahují ze serverů společnosti ESET. Pro zajištění funkční aktualizace modulů vytvoříte dva profily, jeden pro firemní síť a druhý pro aktualizaci mimo firemní síť. Po vytvoření profilů je ještě potřeba odpovídajícím způsobem upravit naplánované úlohy na záložce **Nástroje** > **Plánovač**. Jeden profil bude primární, druhý jako sekundární.

Aktualizační profil – aktuálně používaný profil. Pro jeho změnu vyberte jiný z rozbalovacího menu.

Seznam profilů – správa existujících aktualizačních profilů.

5.2 Klávesové zkratky

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

F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Šipka Nahoru/Dolů	pohyb mezi jednotlivými položkami
-	sbalí vybranou část strom pokročilého nastavení
TAB	přesune se na další položku v rámci okna
Esc	zavře aktivní dialogové okno
Ctrl+U	zobrazí dialogové okno se základními informacemi pro technickou podporu, kde mj. najdete identifikátor vaší licence
Ctrl+R	obnoví pozici a velikost okna na výchozí hodnoty

5.3 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 NOD32 Antivirus. Dostupné jsou dva typy výpisů:

- Vyberte možnost **Žádný** pro vypnutí této funkce.
- **Minimální** – zaznamená nejmenší sadu užitečných informací, které mohou pomoci identifikovat důvod, proč se aplikace nečekaně zastavila. Tento typ výpisu může být užitečný, pokud jste omezeni volným místem na disku. Nicméně, kvůli omezenému množství zahrnutých informací, chyby, které nebyly způsobeny přímo vláknem (thread) běžícím v době problému, nemusí být objeveny analýzou tohoto souboru.
- **Úplný** – zaznamená celý obsah systémové paměti, když se aplikace nečekaně zastaví. Kompletní výpis z paměti může obsahovat data procesů, které běžely v době, kdy byl výpis vytvořen.

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

Aktivovat diagnostické protokolování modulu aktualizace – po aktivování této možnosti se do souboru zapíší detailní informace o průběhu aktualizace programu. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem zajišťujícím aktualizaci programu.

Aktivovat diagnostické protokolování licence – po aktivování této možnosti se zaznamená veškerá komunikace produktu s licenčními servery.

Aktivovat diagnostické protokolování antispamového jádra – po aktivování této možnosti se zaznamenají všechny události v průběhu kontroly zpráv. Toto nám pomůže diagnostikovat a odstranit potíže s antispamovým jádrem.

Aktivovat diagnostické 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 (dostupné na Windows 10).

Vytvořené protokoly naleznete ve složce:
C:\ProgramData\ESET\ESET Security\Diagnostics ve Windows Vista a novějších nebo *C:\Documents and Settings\All Users\...* ve starších verzích operačního systému Windows.

Cílová složka – místo, kam se vygeneruje výpis při pádu.

Otevřít cílovou složku – kliknutím na **Otevřít** zobrazíte obsah výše uvedené složky v novém okně *Průzkumníku Windows*.

Vytvořit diagnostický dump – po kliknutí na tlačítko **Vytvořit** se do cílové složky vygeneruje soubor s výpisem obsahu paměti.

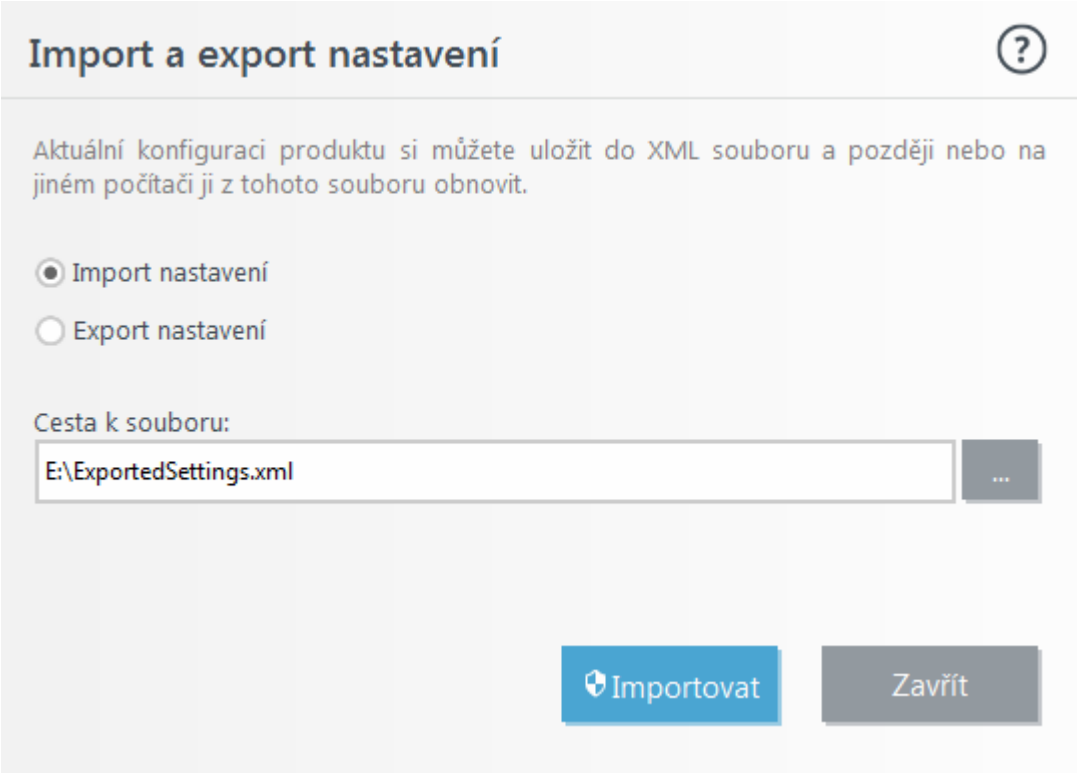
5.4 Import a export nastavení

Na záložce **Nastavení** můžete do programu ESET NOD32 Antivirus importovat nebo z něj naopak exportovat konfiguraci v .xml souboru.

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET NOD32 Antivirus a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích, kdy stačí pouze naimportovat daný .xml soubor.

Import nastavení je velmi jednoduchý. V hlavním okně programu klikněte na záložku **Nastavení** > **Import a export nastavení...**, vyberte možnost **Import nastavení** a kliknutím na tlačítko **...** najděte konfigurační soubor, který chcete importovat.

Export nastavení je velmi podobný importování. V případě, že potřebujete uložit aktuální nastavení ESET NOD32 Antivirus, na záložce **Nastavení** klikněte na odkaz **Import a export nastavení**. Vyberte možnost **Export nastavení**, zadejte **Název souboru** (např. export.xml) a následně vyberte, kam chcete soubor s nastavením uložit.



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

5.5 ESET SysInspector

5.5.1 Úvod do programu ESET SysInspector

ESET SysInspector je aplikace, která důkladně prohlédne počítač a zobrazí získaná data v souhrnném náhledu. Informace jako nainstalované ovladače a aplikace, síťová připojení nebo důležité položky registru Windows mohou pomoci při zjišťování příčiny podezřelého chování systému, ať už kvůli softwarové nebo hardwarové nekompatibilitě či infiltraci škodlivým kódme.

ESET SysInspector můžete spustit dvěma způsoby: Spuštěním přímo z řešení ESET Security nebo stažením samostatné verze (SysInspector.exe) z webových stránek společnosti ESET. Obě verze nabízejí identické funkce a ovládají se stejně. Rozdíl je pouze při zpracovávání výstupů. Samostatná verze exportuje záznam o systému do *.xml* souboru a uloží jej na pevný disk. Zatímco integrovaná verze uloží záznam o systému přímo do záložky **Nástroje** > **ESET SysInspector** (kromě ESET Remote Administrator). Pro více informací se podívejte do sekce ESET SysInspector jako součást ESET NOD32 Antivirus.

Po spuštění ESET SysInspector chvíli vyčkejte na dokončení inspekce počítače. Může to trvat 10 sekund až několik minut v závislosti na hardwarové konfiguraci, operačním systému a počtu nainstalovaných aplikací.

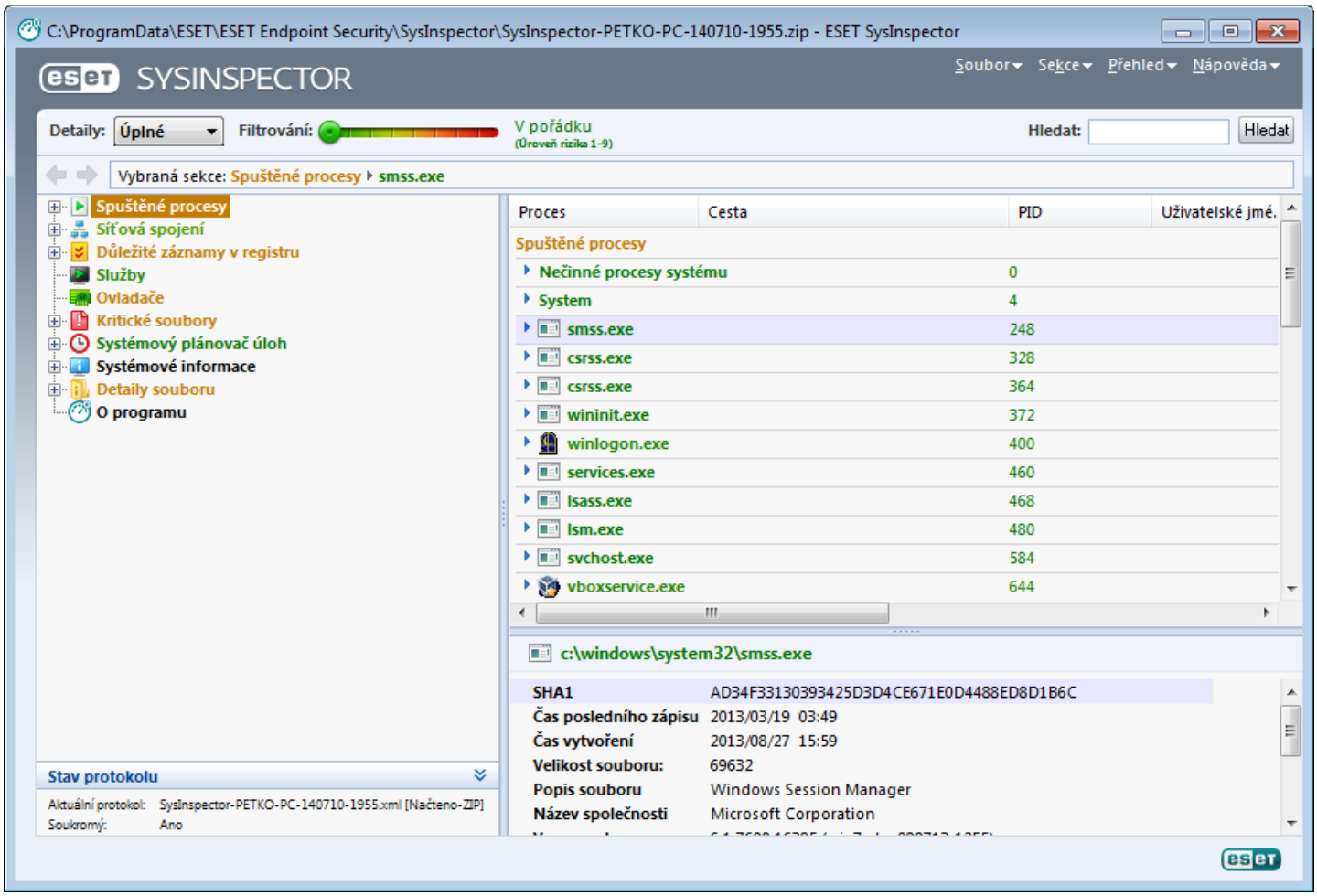
5.5.1.1 Spuštění programu ESET SysInspector

Pro spuštění programu ESET SysInspector klikněte na soubor *SysInspector.exe*, který jste stáhli z webových stránek společnosti ESET. Pokud již máte nainstalováno ESET Security řešení, můžete spustit ESET SysInspector přímo z Nabídky Start kliknutím na **Všechny programy** > **ESET** > **ESET NOD32 Antivirus**).

Následně vyčkejte, dokud aplikace neprovede inspekci systému, což může trvat několik minut.

5.5.2 Uživatelské rozhraní a používání aplikace

Pro snadné používání je hlavní okno rozděleno do čtyř hlavních sekcí – **Ovládání programu** je umístěno v horní části hlavního okna, **Navigační okno** naleznete vlevo a **Okno s popisem** vpravo ve střední části. **Okno s detaily** se nachází v pravé části dole. Sekce **Stav protokolu** zobrazuje základní parametry protokolu (použitý filtr, typ filtru, zda je protokol výsledkem srovnání atd.).



5.5.2.1 Ovládací prvky programu

Tato sekce obsahuje popis všech ovládacích prvků dostupných v programu ESET SysInspector.

Soubor

Kliknutím na **Soubor** můžete uložit současný protokol pro pozdější prozkoumání, nebo otevřít dříve uložený protokol. Pokud chcete protokol zveřejnit, doporučujeme jej vygenerovat jako vhodný **Připravený k odeslání** (CTRL + G). V tomto případě se vynechají citlivé informace (uživatelské jméno, název počítače, oprávnění uživatele, proměnné prostředí atd.).

Poznámka: Uložené protokoly programu ESET SysInspector můžete jednoduše otevřít přetažením .xml souboru do hlavního okna. Tato funkce není z bezpečnostních důvodů dostupná ve Windows Vista.

Sekce

Umožňuje rozbalit nebo zavřít všechny sekce a exportovat vybrané části do Servisního skriptu.

Přehled

Obsahuje funkce pro snadnější navigaci v programu a další funkce, jako například vyhledávání informací online.

Nápověda

Obsahuje informace o aplikaci a dostupných funkcích.

Detaily

Toto nastavení ovlivňuje informace zobrazené v ostatních sekcích hlavního okna. V "Základním" režimu máte přístup k informacím, které se používají k nalezení běžných problémů. Ve "Středním" režimu program zobrazuje i méně používané detaily, zatímco v "Úplném" režimu ESET SysInspector zobrazí všechny informace potřebné k vyřešení specifických problémů.

Filtrování

Slouží k vyhledání podezřelých souborů nebo záznamů v systémovém registru. Nastavením posuvníku můžete filtrovat položky podle jejich úrovně rizika. Pokud je posuvník nastaven co nejvíce vlevo (Úroveň ohrožení 1), jsou zobrazeny všechny položky. Nastavením posuvníku více doprava odfiltrujete všechny položky s menší mírou rizika. Pokud je posuvník nastaven co nejvíce vpravo, program zobrazí pouze známé škodlivé položky.

Všechny položky, které mají úroveň rizika 6 až 9 mohou představovat bezpečnostní riziko. Pokud nepoužíváte bezpečnostní řešení od společnosti ESET a ESET SysInspector detekoval nebezpečné záznamy, doporučujeme zkontrolovat systém pomocí ESET Online Scanner. ESET Online Scanner je služba dostupná zdarma.

POZNÁMKA: Úroveň rizika položky se dá rychle určit porovnáním barvy dané položky s barvou na posuvníku úrovně rizika.

Porovnat

Při porovnávání dvou protokolů můžete zobrazit všechny záznamy, pouze nově přidané nebo naopak odebrané případně nahrazené záznamy.

Hledat

Vyhledávání můžete použít pro rychlé vyhledání celého názvu záznamu nebo pouze jeho části. Výsledky vyhledávání se zobrazí v okně s detaily.

Zpět

Kliknutím na šipku zpět nebo vpřed se můžete vrátit k předchozí zobrazené informaci v okně s detaily. Místo klikání na šipky můžete použít klávesy backspace a mezerník.

Zobrazená sekce

Zobrazuje současnou sekci v navigačním okně.

Důležité: Položky označené červenou barvou jsou neznámé, proto je program označí jako potenciálně nebezpečné. Pokud je některá položka červená, neznamená to, že můžete automaticky daný soubor vymazat. Před samotným vymazáním se ujistěte, že jsou soubory skutečně nebezpečné nebo nepotřebné.

5.5.2.2 Navigace v programu ESET SysInspector

ESET SysInspector rozděluje několik typů informací do několika základních sekcí, které se nazývají uzly. Případně podrobnější informaci získáte rozbalením jednotlivých uzlů a zobrazením poduzlů. Pro rozbalení nebo zavření uzlu, dvakrát poklepejte na název nebo klikněte na ⊞ nebo ⊟ vedle názvu uzlu. Při prohlížení stromové struktury uzlů a poduzlů v navigačním okně více detailů pro každý uzel naleznete v okně s popisem. Pokud prohlížíte položky v okně s popisem, další detaily pro každý typ položky mohou být zobrazeny v okně s detaily.

Následují popisy hlavních uzlů v navigačním okně a související informace v oknech popisem a detaily.

Spuštěné procesy

Tato větev obsahuje informace o aplikacích a procesech, které jsou spuštěny v době generování protokolu. V okně Popis můžete najít další informace pro každý proces, jako které knihovny proces používá a jejich umístění v systému, jméno výrobce aplikace a úroveň rizika daného souboru.

Okno Detaily obsahuje další informace o vybraných položkách v okně Popis, jako například velikost souboru, nebo jeho kontrolní součet.

Poznámka: Operační systém se skládá z několika důležitých komponent jádra systému, které běží nepřetržitě a poskytují základní funkce pro ostatní uživatelské aplikace. V některých případech jsou tyto procesy zobrazeny v protokolu ESET SysInspector s cestou začínající na \??\. Tyto symboly poskytují optimalizaci ještě před spuštěním pro těchto procesů; jsou bezpečné pro systém.

Síťová připojení

Okno Popis obsahuje seznam procesů a aplikací, které komunikují přes síť pomocí protokolu, který je vybrán v navigačním okně (TCP nebo UDP) a také vzdálenou adresu, kam se daná aplikace připojuje. Také můžete zkontrolovat IP adresy DNS serverů.

Okno Detaily obsahuje další informace o vybraných položkách v okně Popis, jako například velikost souboru, nebo jeho kontrolní součet.

Důležité záznamy v registru

Obsahuje seznam vybraných položek registru Windows, které často souvisí s různými problémy, například ty, které definují programy spouštěny po startu, browser helper objects (BHO) atd.

V okně Popis můžete zjistit, které soubory souvisí s konkrétními položkami v registru. Další informace se zobrazí v okně Detaily.

Služby

Okno Popis obsahuje seznam souborů, které jsou zaregistrovány jako služby systému Windows. Můžete si zkontrolovat, jakým způsobem se služba spouští společně se specifickými parametry souboru v okně s Detaily.

Ovladače

Seznam instalovaných ovladačů v systému.

Kritické soubory

V okně Popis se zobrazí kritické soubory spojené s operačním systémem Microsoft Windows.

Systémový plánovač úloh

Obsahuje seznam úloh naplánovaných pomocí Plánovače úloh Windows.

Systémové informace

Obsahuje detailní informace o hardwaru a softwaru společně s informacemi o nastavených globálních proměnných, uživatelských právech a systémových protokolech událostí.

Detaily souboru

Seznam důležitých systémových souborů a souborů ve složce Program Files. Další informace specifické pro soubory naleznete v oknech Popis a Detaily.

O programu

Informace o programu ESET SysInspector a seznam modulů programu.

5.5.2.2.1 Klávesové zkratky

Klávesové zkratky, které můžete použít při práci s programem ESET SysInspector.

Soubor

Ctrl+O	otevře existující protokol
Ctrl+S	uloží vytvořený protokol

Analýza systému

Ctrl+G	vytvoří standardní záznam o počítači
Ctrl+H	vytvoří záznam o počítači, který může obsahovat citlivé informace

Filtrování položek

1, O	v pořádku, jsou zobrazeny položky s úrovní rizika 1-9
2	v pořádku, jsou zobrazeny položky s úrovní rizika 2-9
3	v pořádku, jsou zobrazeny položky s úrovní rizika 3-9
4, U	neznámé, jsou zobrazeny položky s úrovní rizika 4-9
5	neznámé, jsou zobrazeny položky s úrovní rizika 5-9
6	neznámé, jsou zobrazeny položky s úrovní rizika 6-9
7, B	nebezpečné, jsou zobrazeny položky s úrovní rizika 7-9
8	nebezpečné, jsou zobrazeny položky s úrovní rizika 8-9
9	nebezpečné, jsou zobrazeny položky s úrovní rizika 9
-	snižuje úroveň rizika
+	zvyšuje úroveň rizika
Ctrl+9	režim filtrování, stejná úroveň nebo vyšší
Ctrl+0	režim filtrování, pouze stejná úroveň

Zobrazit

Ctrl+5	zobrazit podle výrobce, všichni výrobci
Ctrl+6	zobrazit podle výrobce, pouze Microsoft
Ctrl+7	zobrazit podle výrobce, všichni ostatní výrobci
Ctrl+3	zobrazí úplné detaily
Ctrl+2	zobrazí střední detaily
Ctrl+1	základní zobrazení
BackSpace	krok zpět
Mezerník	krok vpřed
Ctrl+W	rozbalí stromovou strukturu
Ctrl+Q	sbalí stromovou strukturu

Další

Ctrl+T	přejde na původní umístění položky po vyjmutí ve výsledcích vyhledávání
Ctrl+P	zobrazí základní informace o položce
Ctrl+A	zobrazí úplné informace o položce
Ctrl+C	zkopíruje stromovou větev aktuální položky
Ctrl+X	zkopíruje všechny položky
Ctrl+B	vyhledá informace o vybrané položce na internetu
Ctrl+L	otevře složku, kde se nachází vybraný soubor
Ctrl+R	otevře odpovídající záznam v Editoru registru
Ctrl+Z	zkopíruje cestu k souboru (pokud označena položka souvisí se souborem)
Ctrl+F	přepne se do vyhledávacího pole
Ctrl+D	zavře výsledky vyhledávání
Ctrl+E	spustí servisní skript

Porovnání

Ctrl+Alt+O	otevře protokol k porovnání
Ctrl+Alt+R	zruší porovnání
Ctrl+Alt+1	zobrazí všechny položky
Ctrl+Alt+2	zobrazí pouze přidané položky, tedy položky, které jsou přítomny v aktuálním protokolu
Ctrl+Alt+3	zobrazí pouze odebrané položky, tedy položky, které jsou přítomny v předchozím protokolu
Ctrl+Alt+4	zobrazí pouze nahrazené položky (včetně souborů)
Ctrl+Alt+5	zobrazí pouze rozdíly mezi protokoly
Ctrl+Alt+C	zobrazí porovnání
Ctrl+Alt+N	otevře aktuální protokol
Ctrl+Alt+P	otevře předchozí protokol

Různé

F1	zobrazí nápovědu
Alt+F4	zavře program
Alt+Shift+F4	zavře program bez dotazu
Ctrl+I	statistiky protokolu

5.5.2.3 Porovnávání

Funkce porovnání umožňuje porovnat dva stávající protokoly. Výstupem této funkce je sada záznamů, které nejsou společné pro oba protokoly. To je vhodné ve chvíli, kdy chcete sledovat změny v systému a užitečné také při detekci škodlivého programu.

Po spuštění programu ESET SysInspector se vytvoří nový protokol a zobrazí v novém okně. Pro otevření již existujícího protokolu použijte menu **Soubor** > **Otevřít protokol**. V hlavním okně programu se vždy zobrazí zároveň pouze jeden protokol.

Pokud porovnáváte dva protokoly, princip spočívá v tom, že porovnáváte právě aktivní protokol s protokolem uloženým v souboru. Pro porovnání protokolů klikněte na **Soubor** > **Porovnat protokoly** a vyberte **Vybrat soubor**. Vybraný protokol bude porovnán s aktivním v hlavním okně programu. Výsledný tzv. srovnávací protokol zobrazí pouze rozdíly mezi těmito dvěma protokoly.

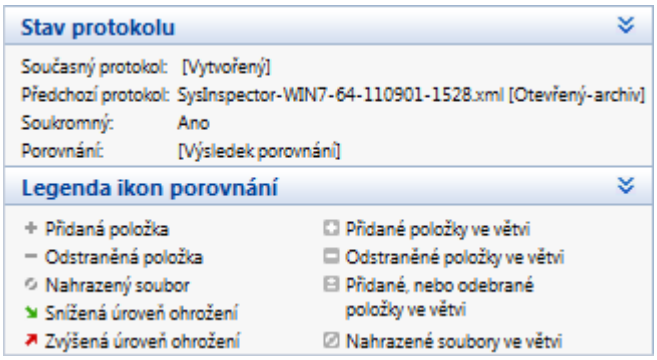
POZNÁMKA: V případě, že porovnáváte dva protokoly, kliknutím na **Soubor** > **Uložit protokol** uložíte oba soubory jako ZIP archiv. Pokud později tento archiv otevřete, protokoly v něm obsažené, budou automaticky porovnány.

Vedle zobrazených položek ESET SysInspector zobrazuje symboly identifikující rozdíly mezi porovnávanými protokoly.

Význam jednotlivých symbolů:

- + nová hodnota, nebyla přítomna v předchozím protokolu
- sekce se stromovou strukturou obsahuje nové hodnoty
- – odebraná hodnota, přítomna pouze v předchozím protokolu
- sekce se stromovou strukturou obsahuje odebrané hodnoty
- hodnota/soubor byly změněny
- sekce se stromovou strukturou obsahuje změněné hodnoty/soubory
- úroveň rizika klesla/byla vyšší v předchozím protokolu
- úroveň rizika vzrostla/byla nižší v předchozím protokolu

Vysvětlující sekce v levém dolním rohu popisuje všechny symboly a také zobrazuje názvy protokolů, které jsou porovnávány.



Kterýkoli srovnávací protokol může být uložen do souboru a kdykoliv později otevřen.

Příklad

Vygenerujte a uložte protokol, který zaznamená původní informace o systému do souboru puvodni.xml. Poté, co budou provedeny změny v systému otevřete ESET SysInspector a vygenerujte nový protokol, který uložte do souboru aktualni.xml.

Pro zjištění změn mezi těmito dvěma protokoly klikněte na **Soubor** > **Porovnat protokoly**. Program vytvoří srovnávací protokol a zobrazí rozdíly mezi protokoly.

Stejného výsledku dosáhnete, pokud zadáte následující příkaz do příkazového řádku:

SysIsnpector.exe aktualni.xml puvodni.xml

5.5.3 Ovládaní přes příkazový řádek

ESET SysInspector podporuje generování protokolů z příkazového řádku za použití následujících parametrů:

/gen	vygeneruje protokol přímo z příkazové řádky bez spuštění grafického rozhraní
/privacy	vygeneruje protokol bez citlivých informací
/zip	uloží výsledný protokol přímo na disk v zip archivu
/silent	tento parametr potlačí zobrazení ukazatele průběhu při generování protokolu
/blank	spustí ESET SysInspector bez vytvoření/načtení protokolu

Příklady

Použití:
`Sysinspector.exe [puvodni.xml] [/gen=novy.xml] [/privacy] [/zip] [srovnani.xml]`

Pro zobrazení specifického protokolu v prohlížeči použijte: *SysInspector.exe .\protokol.xml*
Pro vygenerování protokolu použijte: *SysInspector.exe /gen=.\novyprotokol.xml*
Pro vygenerování protokolu bez citlivých informací použijte: *SysInspector.exe /gen=.\novyprotokol.zip /privacy /zip*
Pro porovnání dvou protokolů použijte: *SysInspector.exe "novy.xml" "puvodni.xml"*

POZNÁMKA: Pokud název souboru nebo složky obsahuje mezeru, měl by být zadán s uvozovkami.

5.5.4 Servisní skript

Servisní skript je nástroj, který umožňuje pomocí ESET SysInspector odstranit nežádoucí objekty ze systému.

Servisní skript umožňuje exportovat celý ESET SysInspector protokol, nebo pouze vybrané části. Po exportování můžete označit nežádoucí objekty, které chcete odstranit. Poté stačí upravený protokol spustit a dojde k odstranění označených objektů.

Servisní skript je určen pokročilým uživatelům s předchozími zkušenostmi v diagnostice systémových problémů. Neodborné zásahy mohou vést k poškození operačního systému.

Příklad

Pokud máte podezření, že je počítač napaden virem, který není detekován antivirovým programem, pokračujte podle následujících kroků:

1. Spusťte ESET SysInspector a vygenerujte nový protokol o systému.
2. Vyberte první položku v sekci nalevo (ve stromové struktuře), stiskněte klávesu **Shift** a vyberte poslední položku pro označení všech položek.
3. Klikněte pravým tlačítkem myši na označené objekty a vyberte z kontextového menu možnost **Exportovat vybrané sekce do Servisního skriptu**.
4. Vybrané objekty budou vyexportovány do nového souboru.
5. Toto je nejdůležitější krok v celém procesu: otevřete uložený soubor v Poznámkovém bloku a změňte atribut - na + u všech objektů, které chcete odstranit. Ujistěte se, že jste neoznačili žádné objekty, které jsou nezbytné pro správné fungování systému.
6. Spusťte ESET SysInspector, klikněte na **Soubor** > **Spustit servisní skript** a zadejte cestu k upravenému skriptu.
7. Klikněte na **OK** pro spuštění skriptu.

5.5.4.1 Generování servisního skriptu

Pro vygenerování skriptu, klikněte pravým tlačítkem myši na libovolnou položku ve stromové struktuře (v levé části) v hlavním okně programu ESET SysInspector. Z kontextového menu vyberte možnost **Exportovat všechny sekce do Servisního skriptu** nebo **Exportovat vybrané sekce do Servisního skriptu**.

POZNÁMKA: Není možné exportovat servisní skript, pokud se porovnávají dva protokoly.

5.5.4.2 Struktura servisního skriptu

V prvním řádku hlavičky skriptu se nacházejí informace o verzi enginu (ev), verzi grafického rozhraní (gv) a verzi protokolu (lv). Tato data můžete použít při hledání možných změn v .xml souboru, které generuje skript a zamezit veškerým nesrovnalostem během provádění skriptu. Tato část skriptu by neměla být modifikována.

Zbytek souboru je rozdělen do sekcí, ve kterých můžete jednotlivé položky modifikovat (označit ty, které budou zpracovány skriptem). Položky ke zpracování označíte tak, že zaměníte znak "-" před položkou za znak "+". Jednotlivé sekce ve skriptu jsou odděleny prázdným řádkem. Každá sekce má číslo a nadpis.

01) Running processes

Tato sekce obsahuje seznam všech běžících procesů v systému. Každý proces je identifikován svou UNC cestou a následně kontrolním součtem CRC16 mezi hvězdičkami (*).

Příklad:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

V tomto příkladu byl vybrán proces module32.exe (označen znakem "+"); proces bude ukončen při spuštění skriptu.

02) Loaded modules

Tato sekce obsahuje seznam aktuálně použitých systémových modulů.

Příklad:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

V tomto příkladu byl modul khbekhb.dll označen znakem "+". Když se skript spustí, rozpozná procesy, které používají tento specifický modul a ukončí je.

03) TCP connections

Tato sekce obsahuje informace o existujících TCP spojeních.

Příklad:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445
(microsoft-ds), owner: System
[...]
```

Když se skript spustí, najde vlastníka socketu v označených TCP spojeních a zastaví tento socket, čímž uvolní systémové prostředky.

04) UDP endpoints

Tato sekce obsahuje informace o stávajících koncových bodech UDP.

Příklad:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Když se skript spustí, izoluje vlastníka socketu v označených koncových bodech UDP a zastaví tento socket.

05) DNS server entries

Tato sekce obsahuje informace o současné konfiguraci DNS serverů.

Příklad:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Označené záznamy DNS budou odstraněny.

06) Important registry entries

Tato sekce obsahuje informace o důležitých záznamech v registru Windows.

Příklad:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:
\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Označené hodnoty budou po spuštění skriptu vymazány, redukovány na 0 bajtové hodnoty, nebo vynulovány na základních hodnoty. Akce, která se provede po spuštění skriptu, závisí na kategorii dané položky a hodnotě klíče v konkrétní větvi registru.

07) Services

Tato sekce obsahuje seznam služeb zaregistrovaných v systému.

Příklad:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe,
state: Running, startup: Automatic
- Name: Application Experience Service, exe path: c:
\windows\system32\aelupsvc.dll, state: Running, startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:
\windows\system32\alg.exe, state: Stopped, startup: Manual
[...]
```

Označené služby a služby na nich závislé budou po spuštění skriptu zastaveny a odinstalovány.

08) Drivers

Tato sekce obsahuje seznam nainstalovaných ovladačů.

Příklad:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys,
state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:
\windows\system32\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Po spuštění skriptu budou vybrané ovladače odregistrovány ze systému a následně odstraněny.

09) Critical files

Tato sekce obsahuje informace o souborech, které jsou kritické pro správné fungování operačního systému.

Příklad:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Vybrané položky budou odstraněny nebo vynulovány na své původní hodnoty.

10) Scheduled tasks

Tato sekce obsahuje informace o naplánovaných úlohách.

Příklad:

```
10) Scheduled tasks
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe
- c:\windows\syswow64\macromed\flash\flashplayerupdateservice.exe
- c:\users\admin\appdata\local\google\update\googleupdate.exe /c
- c:
\users\admin\appdata\local\google\update\googleupdate.exe /ua /installsource
- %windir%\system32\appidpolicyconverter.exe
- %windir%\system32\appidcertstorecheck.exe
- aitagent
[...]
```

5.5.4.3 Spouštění servisních skriptů

Označte všechny požadované položky, poté skript uložte a zavřete. Spusťte změněný skript přímo z hlavního okna programu ESET SysInspector vybráním možnosti **Spustit servisní skript** z menu **Soubor**. Když otevřete skript, program zobrazí následující upozornění: **Opravdu chcete spustit Servisní skript "%Scriptname%"?** Po potvrzení této akce se může objevit další upozornění s informací, že servisní skript, který se pokoušíte spustit, nebyl podepsán. Klikněte na **Spustit** pro spuštění skriptu.

Zobrazí se dialogové okno s informací o úspěšném provedení skriptu.

Pokud byl skript zpracován pouze z části, objeví se dialogové okno s následující zprávou: **Servisní skript byl spuštěn pouze částečně. Chcete zobrazit chybové hlášení?** Klikněte na **Ano** pro zobrazení úplného chybového protokolu se seznamem operací, které nebyly provedeny.

Pokud nebyl skript rozpoznán, zobrazí se dialogové okno s následující zprávou: **Vybraný Servisní skript není podepsán. Spuštění nepodepsaných a neznámých skriptů může vážně poškodit vaše data v počítači. Jste si jisti, že chcete Spustit skript a provést akci?** Toto může být způsobeno nesrovnalostmi ve skriptu (poškozená hlavička, poškozený nadpis sekce, chybějící prázdný řádek mezi dvěma sekcemi atd.). V takovém případě znovu otevřete servisní skript a opravte chyby nebo vytvořte skript nový.

5.5.5 Často kladené otázky

Potřebuje ke svému běhu ESET SysInspector oprávnění Administrátora?

ESET SysInspector nepotřebuje pro spuštění oprávnění Administrátora, ale některé informace, které sbírá, jsou přístupné pouze pro administrátorský účet. Spuštění programu jako Standardní uživatel nebo Uživatel s omezeným oprávněním bude mít za následek shromáždění méně informací o operačním prostředí.

Vytváří ESET SysInspector soubor s protokolem?

ESET SysInspector dokáže vytvořit soubor s protokolem o konfiguraci počítače. Pro uložení souboru klikněte v hlavním menu na **Soubor** > **Uložit protokol**. Protokoly jsou ukládány v XML formátu, standardně do složky *%uživatel%\Dokumenty* s názvem souboru podle konvence "SysInspector-%NÁZEVPOČÍTAČE%-RRMMDD-HHMM.XML". Umístění a název protokolu můžete před uložením změnit, pokud si to přejete.

Jak si prohlédnu protokol ESET SysInspector?

Pro zobrazení protokolu, který vytvořil ESET SysInspector, spusťte program a klikněte v hlavním menu na **Soubor** > **Načíst protokol**. Můžete také soubor přetáhnout do okna programu ESET SysInspector. Pokud si potřebujete často prohlížet protokoly programu ESET SysInspector, doporučujeme vytvořit na Ploše zástupce souboru *SysInspector.exe*; poté můžete protokoly prohlížet pouhým přetažením souboru na vytvořeného zástupce. Z bezpečnostních důvodů nemusí Windows Vista/7 povolit přetahování souboru mezi okny, která mají různá bezpečnostní práva.

Je k dispozici specifikace formátu souboru s protokolem? Co SDK?

V současnosti není k dispozici ani specifikace, ani SDK, protože program je stále ve vývoji. Poté, co bude program uvolněn, můžeme tyto informace poskytnout na základě zpětné vazby a požadavků uživatelů.

Jak ESET SysInspector vyhodnotí riziko, které představuje konkrétní objekt?

Většinou ESET SysInspector přiřadí úroveň rizika objektům (soubory, procesy, klíče v registru atd.) použitím série heuristických pravidel, kterými ověří charakteristiku každého objektu, a poté zváží potenciál pro škodlivou činnost. Na základě této heuristiky se objektu přiřadí úroveň rizika od 1 - V pořádku (zelená) do 9 - Nebezpečné (červená). V levém navigačním okně jsou jednotlivé sekce zabarvené barvou podle objektu s nejvyšší úrovní rizika, který se v nich nachází.

Znamená úroveň rizika "6 - Neznámé (červená)," že je objekt nebezpečný?

Odhad programu ESET SysInspector nezaručuje, že je objekt škodlivý – toto rozhodnutí by měl udělat bezpečnostní expert.ESET SysInspector je navržen pro poskytnutí rychlého souhrnu, na které objekty se má bezpečnostní expert zaměřit pro podrobnější zkoumání neobvyklého chování.

Proč se ESET SysInspector po spuštění připojuje k internetu?

Jako mnoho jiných aplikací, také ESET SysInspector je podepsán digitálním certifikátem, aby bylo možné zaručit, že software byl vydán společností ESET a nebyl modifikován. Pro ověření daného certifikátu operační systém kontaktuje certifikační autoritu pro ověření identity vydavatele softwaru. Toto je normální chování pro všechny digitálně podepsané programy pod operačním systémem Microsoft Windows.

Co je technologie Anti-Stealth ?

Technologie Anti-Stealth poskytuje efektivní detekci rootkitů.

Pokud je systém napaden škodlivým kódem, který se chová jako rootkit, uživatel může být vystaven riziku poškození, ztráty nebo odcizení dat. Bez speciálních anti-rootkit nástrojů je téměř nemožné detekovat rootkity.

Proč jsou někdy soubory označené jako "Podepsal Microsoft" a zároveň mají jiné "Jméno společnosti"?

Při pokusu identifikovat digitální podpis spustitelného souboru SysInspector nejdříve hledá digitální podpis vložený v souboru. Pokud jej najde, pro ověření se použije tato identifikace. Na druhé straně, pokud soubor neobsahuje digitální podpis, ESI začne hledat příslušný CAT soubor (Security Catalog - *%systemroot%\system32\CatRoot*), který obsahuje informace o zpracovávaném spustitelném souboru. V případě, že se najde patřičný CAT soubor, digitální podpis toho CAT souboru se použije při ověřovacím procesu spustitelného souboru.

Toto je důvod, proč jsou někdy soubory označené jako "Podepsal Microsoft" a zároveň mají jiné "Jméno společnosti."

5.5.6 ESET SysInspector jako součást ESET NOD32 Antivirus

ESET SysInspector můžete také otevřít přímo v ESET NOD32 Antivirus kliknutím na záložku **Nástroje** > **ESET SysInspector**. Okno správy ESET SysInspector je velmi podobné protokolům a plánovači úloh. Všechny operace – vytvoření, prohlížení, porovnávání, odstranění a export protokolu – jsou dostupné pomocí jednoho nebo dvou kliknutí myší.

Okno ESET SysInspector obsahuje základní informace o vytvořených záznamech jako je čas vytvoření, krátký komentář, jméno uživatele a stav.

Pro porovnání, vytvoření nebo odstranění protokolu použijte příslušná tlačítka umístěná v dolní části okna ESET SysInspector. Tyto možnosti jsou také dostupné z kontextového menu, které dále obsahuje možnost **Zobrazit**. Pro exportování vybraných protokolů klikněte pravým tlačítkem myši a vyberte možnost **Exportovat...**.

Podrobný popis funkcí:

- **Porovnat** – umožňuje porovnat dva existující protokoly. To je vhodné, pokud potřebujete identifikovat změny ve stávajícím a předchozím protokolu. Pro tuto možnost musíte ze seznamu vybrat 2 záznamy.
- **Přidat...** – vytvoří nový záznam. Před vytvořením musíte zadat krátký komentář o záznamu. Pro zjištění průběhu vytváření protokolu se podívejte do sloupce **Stav**. Všechny vytvořené protokoly mají stav **Vytvořeno**.
- **Odstranit/Odstranit vše** – odstraní záznamy ze seznamu.
- **Exportovat...** – uloží protokol do XML souboru (také jako zip archiv).

5.6 Příkazový řádek

Antivirový modul ESET NOD32 Antivirus můžete spustit pomocí příkazového řádku – ručně (příkazem "ecls") nebo dávkovým souborem typu "bat". Použití ESET skenovacího modulu z příkazového řádku:

```
ecls [MOŽNOSTI..] SOUBORY..
```

Při spouštění kontroly na vyžádání přes příkazový řádek můžete použít několik parametrů a přepínačů:

Možnosti

/base-dir=SLOŽKA	načíst moduly ze SLOŽKY
/quar-dir=SLOŽKA	soubory ulož do karantény - SLOŽKY
/exclude=MASKA	vyloučí soubory odpovídající MASCE z kontroly
/subdir	zahrnout podsložky (standardně)
/no-subdir	nezahrnovat podsložky
/max-subdir-level=ÚROVEŇ	podsložky zkontrolovat pouze do hloubky ÚROVNĚ (standardně 0 = neomezeně)
/symlink	následovat symbolické odkazy (standardně)
/no-symlink	přeskočit symbolické odkazy
/ads	kontrolovat ADS (standardně)
/no-ads	nekontrolovat ADS
/log-file=SOUBOR	zapisovat výstup do SOUBORU
/log-rewrite	přepisovat výstupní soubor (standardně se přidá na konec současného)
/log-console	zapisovat výstup na konzoli

/no-log-console	nezapisovat výstup na konzoli
/log-all	vypsat i čisté soubory
/no-log-all	nevypisovat čisté soubory (standardně)
/aind	zobrazit indikátor aktivity
/auto	automaticky zkontrolovat a vyléčit všechny lokální disky

Možnosti skeneru

/files	kontrolovat soubory (standardně)
/no-files	nekontrolovat soubory
/memory	kontrolovat paměť
/boots	kontrolovat zaváděcí sektory
/no-boots	nekontrolovat zaváděcí sektory (standardně)
/arch	kontrolovat archivy (standardně)
/no-arch	nekontrolovat archivy
/max-obj-size=VELIKOST	kontrolovat pouze soubory menší než VELIKOST megabajtů (standardně 0 = neomezené)
/max-arch-level=ÚROVEŇ	archivy kontrolovat do hloubky ÚROVNĚ
/scan-timeout=LIMIT	archivy kontrolovat nejdéle LIMIT sekund
/max-arch-size=VELIKOST	kontrolovat pouze soubory v archivech menší než VELIKOST megabajtů (standardně 0 = neomezené)
/max-sfx-size=VELIKOST	kontrolovat pouze soubory v samorozbalovacích archivech menší než VELIKOST megabajtů (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 archivy (standardně)
/no-rtp	nekontrolovat runtime archivy
/adware	kontrolovat adware aplikace (standardně)
/no-adware	nekontrolovat adware aplikace
/unsafe	kontrolovat zneužitelné aplikace
/no-unsafe	nekontrolovat zneužitelné aplikace (standardně)
/unwanted	kontrolovat nechtěné aplikace
/no-unwanted	nekontrolovat nechtěné aplikace (standardně)
/pattern	použít vzorky (standardně)
/no-pattern	nepoužívat vzorky
/heur	zapnout heuristiku (standardně)
/no-heur	vypnout heuristiku
/adv-heur	zapnout rozšířenou heuristiku (standardně)
/no-adv-heur	vypnout rozšířenou heuristiku
/ext=PŘÍPONY	kontrolovat pouze dvojtečkou oddělené PŘÍPONY
/ext-exclude=PŘÍPONY	vyloučit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=REŽIM	použít REŽIM léčení infikovaných objektů: none, standard (výchozí), strict, rigorous, delete
/quarantine	uložit infikované soubory (při léčení) do karantény (kromě vykonání AKCE)
/no-quarantine	neukládat infikované soubory do karantény

Všeobecné volby

/help	zobrazit tuto pomůcku a skončit
/version	zobrazit informaci o verzi a skončit
/preserve-time	zachovat čas přístupu k souborům

Návratové hodnoty

0	nenalezena žádná infekce
1	infekce nalezena a odstraněna
10	některé soubory nemohly být zkontrolovány (mohou obsahovat infekci)
50	nalezena infekce
100	chyba

Poznámka:
Návratové hodnoty větší než 100 znamenají, že soubor nebyl zkontrolován a může být infikován.

6. Řešení nejčastějších problémů

Tato kapitola obsahuje některé z nejčastěji se vyskytujících otázek a problémů, se kterými se můžete setkat. Klikněte na název kapitoly pro zobrazení řešení problému.

Jak aktualizovat ESET NOD32 Antivirus?
Jak aktivovat ESET NOD32 Antivirus?
Jak odstranit vir z počítače?
Jak vytvořit novou úlohu v Plánovači?
Jak naplánovat kontrolu počítače (kontrola každých 24 hodin)?

Pokud není váš problém zahrnut v seznamu výše, zkuste v nápovědě ESET NOD32 Antivirus vyhledat řešení podle klíčového slova nebo fráze, která popisuje váš problém. Pokud nenaleznete řešení vašeho problému v nápovědě, navštivte pravidelně aktualizovanou ESET Databázi znalostí. Níže naleznete odkazy na nejnavštěvovanější články v databázi.

Při aktivaci produktu ESET došlo k chybě. Co to znamená?
Jak aktivovat program ESET?
Jak odinstalovat nebo přeinstalovat program ESET?
Instalace programu ESET skončila předčasně
Co musím udělat po obnovení licence? (Domácí uživatelé)
Co se stane, pokud změním e-mailovou adresu?
Jak spustit Windows v Nouzovém režimu nebo Nouzovém režimu se sítí

Pokud je to nutné, můžete se obrátit přímo na naše pracovníky technické podpory. Kontaktní formulář naleznete přímo v programu na záložce **Nápověda a podpora**.

6.1 Jak aktualizovat ESET NOD32 Antivirus?

Aktualizaci ESET NOD32 Antivirus můžete provádět ručně nebo automaticky. Pro zahájení aktualizace klikněte v hlavním okně programu na tlačítko **Zkontrolovat aktualizace** na záložce **Aktualizace**.

Po nainstalování programu se standardně vytvoří naplánovaná úloha, která spouští automatickou aktualizaci každou hodinu. Pokud chcete změnit tento interval, přejděte na záložku **Nástroje** > **Plánovač** (pro více informací týkajících se Plánovače klikněte sem).

6.2 Jak odstranit vir z počítače?

Pokud jeví počítač známky infekce, tzn. je pomalejší, zamrzá apod. doporučujeme postupovat podle následujících kroků:

1. V hlavním okně programu klikněte na záložku **Kontrola počítače**,
2. Klikněte na možnost **Smart kontrola** pro zahájení kontroly počítače,
3. Po ukončení kontroly prověřte protokol zkontrolovaných, infikovaných a vyléčených souborů,
4. Pokud chcete zkontrolovat pouze určité části počítače, vyberte možnost **Volitelná kontrola** a ručně vyberte cíle kontroly.

Pro více informací přejděte do Databáze znalostí.

6.3 Jak vytvořit novou úlohu v Plánovači?

Pro vytvoření nové úlohy v Plánovači přejděte v hlavním okně programu na záložku **Nástroje** > **Plánovač** a klikněte na tlačítko **Přidat** v dolní části okna nebo z kontextového menu dostupného po kliknutím pravým tlačítkem myši. K dispozici jsou následující typy úloh:

- **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 detekčních a programových modulů.

Mezi nejčastěji používané naplánované úlohy patří **Aktualizace**, proto si podrobněji popíšeme přidání nové aktualizační úlohy.

Po zobrazení nabídky naplánovaných úloh vyberte z rozbalovacího menu položku **Aktualizace**. Zadejte název úlohy. a klikněte na tlačítko **Další**. Dále nastavte pravidelnost opakování úlohy. K dispozici jsou možnosti: **Jednou**, **Opakovaně**, **Denně, Týdně**, **Při události**. Možnost **Nespouštět úlohu, pokud je počítač napájen z baterie** je dobré použít, pokud přenosný počítač není zapojen do elektrické sítě a chcete v tomto čase minimalizovat jeho systémové prostředky. Dále je potřeba definovat akci, která se provede v případě, že ve stanoveném termínu nebude možné úlohu spustit. K dispozici jsou následující možnosti:

- **Při dalším naplánovaném termínu**
- **Jakmile to bude možné**
- **Okamžitě, pokud od posledního provedení uplynul stanovený interval** (definovaný v poli **Čas od posledního spuštění**)

V dalším kroku se zobrazí souhrnné informace o přidávané naplánované úloze. Akci dokončete kliknutím na tlačítko **Dokončit.**

V zobrazeném dialogovém okně vybrat profil, který se použije pro aktualizaci. Vybrat můžete primární a alternativní profil, který se použije v případě, že úlohu nebude možné provést pomocí primárního profilu. Kliknutím na tlačítko **Dokončit** se vytvořená naplánovaná úloha přidá do seznamu naplánovaných úloh.

6.4 Jak naplánovat kontrolu počítače (kontrola každých 24 hodin)?

Pro naplánování standardní úlohy přejděte v hlavním okně programu na záložku **Nástroje** > **Plánovač**. Níže je popsán stručný návod, jak vytvořit úlohu, která bude kontrolovat lokální disky každých 24 hodin. Více informací naleznete v Databázi znalostí.

Pro naplánovaní úlohy postupujte následovně:

1. Klikněte na tlačítko **Přidat** v hlavním okně **Plánovače**,
2. V rozbalovacím menu vyberte možnost **Kontrola počítače**,
3. Zadejte název úlohy a klikněte na možnost **Opakovaně**,
4. Interval provedení úlohy zadejte 24 hodin (1440 minut),
5. Vyberte akci, která se provede v případě neprovedení úlohy ve stanoveném čase,
6. Zkontrolujte všechna nastavení úlohy v seznamu a klikněte na **Dokončit**,
7. V rozbalovacím menu **Cíle kontroly** vyberte lokální disky,
8. Klikněte na **Nastavit** pro dokončení.

6.5 Jak obnovit přístup do rozšířeného nastavení?

Pokud jste si aktivovali ochranu heslem pro zabránění neoprávněným změnám v konfiguraci produktu a nyní jste heslo zapomněli, při pokusu o přístup do rozšířeného nastavení klikněte na možnost **Obnovit heslo**. Následně zadejte e-mailovou adresu, kterou jste uvedli při nákupu/registraci licence. Na tuto adresu vám zašleme ověřovací kód společně s návodem na reset hesla. Daný kód zadejte do zobrazeného dialogového pole a nastavte si nové heslo. Ověřovací kód je platný 7 dní.

Zapomenuté heslo si můžete obnovit také **prostřednictvím vašeho my.eset.com účtu**. Tuto možnost můžete využít pouze v případě, kdy máte licence přidanou do ESET Správce licencí.

V případě, že si nepamatujete e-mailovou adresu, klikněte na možnost **Neznám moji e-mailovou adresu**. Následně budete přesměrování na webový formulář pro kontaktování technické podpory.

Vygenerovat kód pro technickou podporu – pomocí této možnosti vygenerujete kód, který poskytněte specialistům technické podpory. Následně vyberte možnost **Mám ověřovací kód** a do zobrazeného dialogového pole zadejte kód, který jste obdrželi od specialistů technické podpory, a nastavte si nové heslo. Ověřovací kód je platný 7 dní.

Pro více informací přejděte do ESET Databáze znalostí.