

ESET NOD32 Antivirus

Uživatelská příručka

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

Copyright ©2024 ESET, spol. s r.o.

ESET NOD32 Antivirus byl vyvinut společností ESET, spol. s r.o.

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

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

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

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

REV. 2024-04-12

1 ESET NOD32 Antivirus	1
1.1 Co je nového?	2
1.2 Jaký mám produkt?	2
1.3 Systémové požadavky	3
1.3 Zastaralá verze Microsoft Windows	4
1.4 Prevence	5
1.5 Návod programu	6
2 Instalace	7
2.1 Online instalační balíček	7
2.2 Offline instalace	9
2.3 Aktivace produktu	10
2.3 Zadání licenčního klíče během aktivace	11
2.3 Použití účtu ESET HOME	11
2.3 Aktivace zkušební licence	12
2.3 Bezplatný licenční klíč na produkt ESET	13
2.3 Neúspěšná aktivace – běžné scénáře	14
2.3 Stav licence	14
2.3 Neúspěšná aktivace z důvodu nadužívání licence	15
2.3 Povýšení licence	16
2.3 Povýšení produktu	17
2.3 Ponižení licence	18
2.3 Ponižení produktu	18
2.4 Poradce při potížích s instalací	19
2.5 Prvotní kontrola počítače po dokončení instalace	19
2.6 Aktualizace na novou verzi	20
2.6 Automatická aktualizace starších produktů	21
2.6 Nainstaluje se ESET NOD32 Antivirus	21
2.6 Přejít na jinou produktovou řadu	21
2.6 Registrace	21
2.6 Průběh aktivace	22
2.6 Úspěšná aktivace	22
3 Začínáme	22
3.1 Ikona v oznamovací oblasti	22
3.2 Klávesové zkratky	23
3.3 Profily	23
3.4 Aktualizace	24
4 Práce s ESET NOD32 Antivirus	26
4.1 Přehled	27
4.2 Kontrola počítače	30
4.2 Spuštění volitelné kontroly	32
4.2 Průběh kontroly	34
4.2 Protokol kontroly počítače	36
4.3 Aktualizace	38
4.3 Dialogové okno – Vyžadován restart	40
4.3 Jak vytvořit aktualizací úlohu?	41
4.4 Nástroje	41
4.4 Protokoly	42
4.4 Filtrování protokolů	44
4.4 Spuštěné procesy	46
4.4 Bezpečnostní přehled	47

4.4 ESET SysInspector	49
4.4 Plánovač	49
4.4 Možnosti naplánované kontroly	51
4.4 Informace o naplánované úloze	52
4.4 Detaily úlohy	53
4.4 Provedení úlohy	53
4.4 Provedení úlohy – Jednou	53
4.4 Provedení úlohy – Denně	53
4.4 Provedení úlohy – Týdně	54
4.4 Provedení úlohy – Při události	54
4.4 Neprovedení úlohy	54
4.4 Detaily úlohy – Aktualizace	55
4.4 Detaily úlohy – Spuštění aplikace	55
4.4 Kontrola systému	55
4.4 Karanténa	56
4.4 Odeslání vzorku k analýze	59
4.4 Podezřelý soubor	60
4.4 Podezřelá stránka	60
4.4 Falešně detekovaný soubor	60
4.4 Falešně detekovaná stránka	61
4.4 Ostatní	61
4.5 Nastavení	61
4.5 Ochrana počítače	62
4.5 Nalezena infiltrace	63
4.5 Internetová ochrana	66
4.5 Anti-Phishingová ochrana	67
4.5 Import a export nastavení	68
4.6 Nápopověda a podpora	69
4.6 O programu ESET NOD32 Antivirus	70
4.6 ESET Novinky	71
4.6 Odeslat konfiguraci systému	72
4.6 Technická podpora	72
4.7 Účet ESET HOME	73
4.7 Připojení k ESET HOME	74
4.7 Přihlášení do ESET HOME	75
4.7 Neúspěšné přihlášení – běžné chyby	76
4.7 Přidání zařízení v ESET HOME	77
5 Rozšířená nastavení	77
5.1 Detekční jádro	78
5.1 Výjimky	79
5.1 Výkonnostní výjimky	79
5.1 Přidání a úprava výkonnostních výjimek	80
5.1 Formát výjimky podle cesty	82
5.1 Detekční výjimky	82
5.1 Přidání a úprava detekčních výjimek	84
5.1 Průvodce vytvořením detekční výjimky	85
5.1 Rozšířená nastavení detekčního jádra	86
5.1 Kontrola síťové komunikace	86
5.1 Cloudová ochrana	86
5.1 Filtr výjimek pro cloudovou ochranu	89
5.1 Detekce škodlivého kódu	89

5.1 Profily kontroly	90
5.1 Cíle kontroly	90
5.1 Kontrola při nečinnosti	91
5.1 Detekce stavu nečinnosti	92
5.1 Kontrola po startu	92
5.1 Automatická kontrola souborů spouštěných při startu počítače	92
5.1 Výměnná média	93
5.1 Ochrana dokumentů	94
5.1 HIPS – Host Intrusion Prevention System	94
5.1 HIPS výjimky	97
5.1 Rozšířená nastavení HIPS	97
5.1 Ovladače, jejichž načtení je vždy povoleno	97
5.1 Interaktivní režim HIPS	98
5.1 Detekován potenciální ransomware	99
5.1 Správa HIPS pravidel	100
5.1 Úprava pravidla HIPS	101
5.1 Přidat cestu k aplikaci/registru pro HIPS	104
5.2 Aktualizace	104
5.2 Obnovení předchozí verze modulů	106
5.2 Interval pro obnovení předchozí verze modulů	108
5.2 Aktualizace produktu	108
5.2 Možnosti připojení	108
5.3 Ochrany	109
5.3 Rezidentní ochrana souborového systému	112
5.3 Vyloučené procesy	114
5.3 Přidání a úprava výjimek pro procesy	115
5.3 Kdy měnit nastavení rezidentní ochrany	115
5.3 Ověření funkčnosti rezidentní ochrany	115
5.3 Co dělat, když nefunguje rezidentní ochrana	116
5.3 SSL/TLS	116
5.3 Pravidla pro kontrolu aplikací	118
5.3 Pravidla pro certifikáty	119
5.3 Šifrovaná síťová komunikace	120
5.3 Ochrana poštovních klientů	120
5.3 Ochrana transportu zpráv	121
5.3 Vyloučené aplikace	122
5.3 Vyloučené IP adresy	123
5.3 Ochrana poštovní schránky	124
5.3 Integrace	125
5.3 Panel nástrojů v MS Outlook	125
5.3 Potvrzovací dialog	126
5.3 Opakovaná kontrola zpráv	126
5.3 Reakce	126
5.3 ThreatSense	127
5.3 Ochrana přístupu na web	130
5.3 Vyloučené aplikace	132
5.3 Vyloučené IP adresy	133
5.3 Správa seznamu URL adres	134
5.3 Seznam adres	135
5.3 Vytvoření nového seznamu URL adres	136
5.3 Jak přidat masku URL?	137

5.3 Kontrola HTTP(S) komunikace	138
5.3 ThreatSense	138
5.3 Správa zařízení	141
5.3 Editor pravidel ve správě zařízení	142
5.3 Detekovaná zařízení	143
5.3 Vytvoření nového pravidla	144
5.3 Skupiny zařízení	146
5.3 ThreatSense	147
5.3 Úrovně léčení	151
5.3 Přípony souborů vyloučených z kontroly	151
5.3 Doplňující parametry skenovacího jádra ThreatSense	152
5.4 Nástroje	152
5.4 Aktualizace operačního systému Windows	153
5.4 Dialogové okno – Aktualizace systému	153
5.4 Informace o aktualizacích	153
5.4 ESET CMD	153
5.4 Protokoly	155
5.4 Herní režim	156
5.4 Diagnostika	157
5.4 Technická podpora	158
5.5 Připojení	158
5.6 Uživatelské rozhraní	159
5.6 Prvky uživatelského rozhraní	160
5.6 Přístup k nastavení	161
5.6 Heslo pro přístup do Rozšířeného nastavení	162
5.6 Podpora odcítačů obrazovky	162
5.7 Oznámení	163
5.7 Dialogová okna – Stavby aplikace	164
5.7 Oznámení na pracovní ploše	164
5.7 Seznam oznámení na pracovní ploše	165
5.7 Interaktivní upozornění	167
5.7 Potvrzovací zprávy	168
5.7 Přeposílání	169
5.8 Nastavení ochrany soukromí	172
5.8 Obnovit všechna nastavení na standardní	172
5.8 Obnovit všechna nastavení v této sekci na standardní	173
5.8 Chyba během ukládání nastavení	173
5.9 Skener příkazového řádku	173
6 Řešení nejčastějších problémů	176
6.1 Jak aktualizovat ESET NOD32 Antivirus?	177
6.2 Jak odstranit vir z počítače?	177
6.3 Jak vytvořit novou úlohu v Plánovači?	177
6.4 Jak naplánovat každý týden kontrolu počítače?	178
6.5 Jak obnovit přístup do rozšířeného nastavení?	179
6.6 Jak deaktivovat produkt prostřednictvím portálu ESET HOME?	179
6.6 Produkt je deaktivovaný, zařízení je odpojené	180
6.6 Produkt není aktivován	180
7 Program zvyšování spokojenosti zákazníků	180
8 Licenční ujednání s koncovým uživatelem	181
9 Zásady ochrany osobních údajů	192

ESSENTIAL SECURITY

ESET NOD32 Antivirus

ESET NOD32 Antivirus představuje nový přístup k integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ESET LiveGrid® rychle a přesně zajišťuje bezpečnost vašeho zařízení. 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	Uživatelské rozhraní produktu bylo kompletně přepracováno. Nyní je čistější, přehlednější a intuitivnější. Upravili jsme textaci oznámení zobrazených uživateli a přidali také podporu pro jazyky se zápisem zprava doleva, jako je Hebrejščina a Arabština. Prostřednictvím online nápovědy, integrované do produktu, získáte vždy nejaktuálnější informace ke konkrétním zobrazeným oknům v programu ESET NOD32 Antivirus.
Tmavý režim	Rozšíření pro zapnutí tmavého zobrazení uživatelského rozhraní. Preferované barevné schéma si můžete zvolit v prvcích uživatelského rozhraní .
Antivirus a antispyware	Proaktivně detekuje a léčí známé i neznámé viry, červy, trojské koně a rootkity. Pokročilá heuristika označí každý dosud neznámý škodlivý kód, chrání vás před neznámými hrozbami a eliminuje je dříve, než mohou způsobit škodu. Ochrana přístupu na web a modul Anti-Phishing monitorují 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 detekční jádra (dříve známé jako "virové databáze") a programových modulů zajistí maximální ochranu počítače.
ESET LiveGrid® (založen na cloudové technologii)	Můžete zkontrolovat reputaci spuštěných procesů a souborů přímo v ESET NOD32 Antivirus vůči cloudové databázi.
Správa zařízení	Produkt automaticky kontroluje všechny USB disky, paměťové karty a CD/DVD. Dále dokáže blokovat výměnná média podle typu, výrobce, velikosti a dalších atributů.
HIPS	Pomocí tohoto modulu si můžete přizpůsobit detailní chování systému a jeho bezpečnost pomocí pravidel pro systémový registr, aktivní procesy a programy.
Herní režim	Při hraní her a používání aplikací běžících v režimu celé obrazovky (fullscreen) se nezobrazí upozornění ani vyskakovací okna a program tak uvolní systémové prostředky hry a pro náročné aplikace.

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

Co je nového?

Co je nového v ESET NOD32 Antivirus verze 16.2

Intel® Threat Detection Technology

Hardwarová technologie odhalující ransomware, který se pokouší vyhnout se detekci v paměti. Její integrace zvyšuje ochranu proti ransomware a nemá negativní vliv na výkon systému. Viz [podporované procesory](#).

Tmavý režim

Tato funkce umožňuje kromě světlého barevného schématu uživatelského rozhraní ESET NOD32 Antivirus zvolit schéma tmavé, případně barevné schéma dle systému. Barevné schéma lze přepínat v pravém horním rohu [hlavního okna programu](#).

Operační systém Windows verze 7, 8 a 8.1 už není podporovaný.

ESET NOD32 Antivirus 16.2 je podporovaný pouze v systému Windows 10 a 11. Více informací naleznete v kapitole [Zastaralá verze Microsoft Windows](#).

Přepracovaná Rozšířená nastavení

[Rozšířená nastavení](#) byla přepracována a jednotlivá nastavení jsou nyní seskupena s ohledem na větší pohodlí uživatele.



Pro vypnutí oznámení **Co je nového** přejděte do [Rozšířených nastavení](#) a v sekci **Oznámení > Oznámení na pracovní ploše**. Na řádce **Oznámení na pracovní ploše** klikněte na **Změnit**. V zobrazeném dialogovém okně **Oznámení aplikace** odklikněte zaškrtačkové pole na řádce **Zobrazit oznámení Co je nového**. Více informací naleznete v [samostatné kapitole](#).



Podrobný seznam změn v ESET NOD32 Antivirus naleznete v [seznamu změn ESET NOD32 Antivirus](#).

Jaký mám produkt?

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

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

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

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detekční jádro	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓
Exploit Blocker	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓
Anti-Phishing	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Strážce sítě		✓	✓
Ochrana webkamery		✓	✓
Ochrana proti síťovým útokům		✓	✓
Ochrana proti zapojení do botnetu		✓	✓
Ochrana bankovníctví a online plateb		✓	✓
Rodičovská kontrola		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

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

Systémové požadavky

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

Podporované procesory

Intel nebo AMD procesor, 32-bit (x86) s instrukční sadou SSE2 nebo 64-bit (x64), 1 GHz a rychlejší
ARM64 procesor, 1 GHz a rychlejší

Podporované operační systémy

Microsoft® Windows® 11

Microsoft® Windows® 10



Nejnovější verze ESET NOD32 Antivirus vyžaduje operační systém Windows 10 nebo Windows 11. Pokud nemůžete aktualizovat systém Windows, [nainstalujte si ESET NOD32 Antivirus ve verzi 16.0](#). Další informace naleznete v [online příručce k ESET NOD32 Antivirus ve verzi 16.0](#).



Vždy se snažte udržovat svůj operační systém aktualizovaný.

Požadavky funkcí produktu ESET NOD32 Antivirus

V tabulce níže naleznete přehled systémových požadavků konkrétních funkcí produktu ESET NOD32 Antivirus:

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

Ostatní

Pro aktivaci ESET NOD32 Antivirus a získání aktualizací pro jeho správnou funkci je vyžadováno internetové připojení.

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

Zastaralá verze Microsoft Windows

Problém

- Pokoušíte se nainstalovat nejnovější verzi ESET NOD32 Antivirus na zařízeních s Windows 7, Windows 8 (8.1) nebo Windows Home Server 2011
- ESET NOD32 Antivirus při instalaci zobrazí chybu **Zastaralý operační systém**

Detaily

Nejnovější verze ESET NOD32 Antivirus vyžaduje operační systém Windows 10 nebo Windows 11.

Řešení

K dispozici jsou následující možnosti:

Přejít na Windows 10 nebo Windows 11

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

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

Instalace ESET NOD32 Antivirus verze 16.0

Pokud nemůžete aktualizovat systém Windows, [nainstalujte si ESET NOD32 Antivirus ve verzi 16.0](#). Další informace naleznete v [online příručce k ESET NOD32 Antivirus ve verzi 16.0](#).

Prevence

Při používání počítače, zejména při práci s internetem, je potřeba mít neustále na paměti, že žádný antivirový systém nedokáže zcela odstranit riziko [detekcí](#) a [vzdálených útoků](#). Pro zajištění maximální bezpečnosti a pohodlí je potřeba antivirové řešení správně používat a dodržovat několik užitečných pravidel:

Pravidelná aktualizace antivirového systému

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

Stáhněte si aktualizace co nejdříve poté, co byly vydány.

Autoři škodlivého softwaru často využívají různé slabiny systému, aby zvýšili efektivitu šíření škodlivého kódu. Výrobci většiny programů proto pravidelně vydávají bezpečnostní záplaty, které chyby v produktech opravují a snižují tak riziko potenciální nákazy. Je důležité stáhnout aktualizace zabezpečení co nejdříve po jejich vydání. Microsoft Windows a webové prohlížeče, jako např. Internet Explorer, jsou dva příklady programů, pro které jsou vydány aktualizace zabezpečení v pravidelném rozvrhu.

Zálohování důležitých dat

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

Pravidelná kontrola počítače

Detekci známých i neznámých virů, červů, trojských koní a rootkitů zajišťuje rezidentní ochrana souborového systému. To znamená, že při každém přístupu k souboru, dojde k jeho kontrole. Přesto vám doporučujeme, abyste prováděli ruční kontrolu počítače alespoň jednou měsíčně, protože signatury malwaru se mohou lišit. Aktualizace detekčního jádra probíhá denně.

Dodržování základních bezpečnostních pravidel

Neužitečnější a neúčinnější pravidlo ze všech – vždy buďte opatrní. V dnešní době je provedení a distribuce mnoha infiltrací závislé na prvním zásahu ze strany uživatele. Pokud budete při otevírání nových souborů opatrní, ušetříte si čas, který byste jinak trávili léčením počítače od škodlivého kódu. Několik užitečných rad:

- Omezte návštěvy podezřelých stránek, které uživatele bombardují otevíráním oken s reklamními nabídkami apod.

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

Nápověda programu

Vítejte v uživatelském manuálu ESET NOD32 Antivirus. Věříme, že informace obsažené v této nápovědě vás seznámí s produktem a pomohou vám zabezpečit počítač.

Jak začít

Před použitím ESET NOD32 Antivirus vám doporučujeme seznámit se s různými [typy infiltrací](#) a [útoků na dálku](#), se kterými se můžete setkat. O nových funkcích v ESET NOD32 Antivirus si můžete přečíst v [samostatné kapitole](#).

Začněte kapitolou [Instalace ESET NOD32 Antivirus](#). Pokud již máte ESET NOD32 Antivirus nainstalovaný, přečtěte si kapitolu [Práce s ESET NOD32 Antivirus](#).

Jak používat nápovědu programu ESET NOD32 Antivirus

Témata Online nápovědy jsou rozdělena do několika kapitol a podkapitol. Pokud si s konkrétní částí produktu ESET NOD32 Antivirus nevíte rady, stiskněte funkční klávesu **F1** a zobrazí se vám nápověda.

Online nápověda umožňuje vyhledávání prostřednictvím klíčových slov nebo pomocí slovních spojení. Rozdíl mezi těmito dvěma typy vyhledávání je ten, že klíčová slova se váží ke stránkám nápovědy logicky, přičemž samotné klíčové slovo se vůbec v textu nemusí vyskytovat. Vyhledávání pomocí slov a slovních spojení naopak najde všechny stránky nápovědy, na kterých se hledaná slova nachází přímo v textu.

Připravili jsme také průvodce, který vám pomůže se základním nastavením ESET NOD32 Antivirus. Používáme rovněž jednotnou sadu symbolů na zvýraznění částí kapitol, které jsou zvláště důležité, případně by neměly uniknout vaší pozornosti.



Poznámka je krátký výtah informace. Ačkoli ji můžete vynechat, poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.



Tato část vyžaduje vaši pozornost a doporučujeme ji nevynechat. Obvykle obsahuje nekritické, avšak důležité informace.



Takto označená informace vyžaduje vaši plnou pozornost. Varování jsou umístěna tak, aby vás včas varovala a zároveň vám pomohla vyvarovat se chybám, které by mohly mít negativní následky. Prosím, důkladně si přečtěte text ohraničený tímto označením, protože se týká velmi citlivých systémových nastavení nebo upozorňuje na možná rizika.



Příklad popisující uživatelský scénář nebo praktickou ukázkou pro pochopení fungování nebo používání dané funkce.

Konvence	Význam
Tučné písmo	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.

Konvence	Význam
<i>Kurzíva</i>	Zástupné znaky pro informace, které máte zadat. Například název souboru nebo cesta k souboru znamená, že máte zadat skutečnou cestu nebo název souboru.
Courier New	Příklady kódů nebo příkazů
Hypertextový odkaz	Poskytuje rychlý přístup do odkazovaných kapitol nebo externích zdrojů. Hypertextové odkazy jsou zvýrazněny modře a mohou být podtržené.
<i>%ProgramFiles%</i>	Systémová složka operačního systému Windows, do které se standardně instalují programy a další součásti systému.

Online příručka je primárním zdrojem nápovědy. V případě funkčního připojení k internetu se automaticky zobrazí nejnovější verze Online nápovědy.

Instalace

Instalaci ESET NOD32 Antivirus můžete na svém počítači provést dvěma způsoby. Způsoby instalace se mohou lišit v závislosti na zemi a způsobu vydání:

- [Live installer](#) si můžete stáhnout z internetových stránek společnosti ESET, případně jej naleznete na zakoupeném CD/DVD. Instalační balíček je univerzální pro všechny jazykové varianty (při instalaci vyberete jazykovou verzi). Jedná se o malý soubor. Další potřebné soubory pro instalaci ESET NOD32 Antivirus se stáhnou automaticky z internetu.
- [Offline instalační balíček](#) – jedná se o .exe soubor, který obsahuje všechny soubory potřebné pro instalaci. Proto je větší než Live installer a nevyžaduje připojení k internetu.



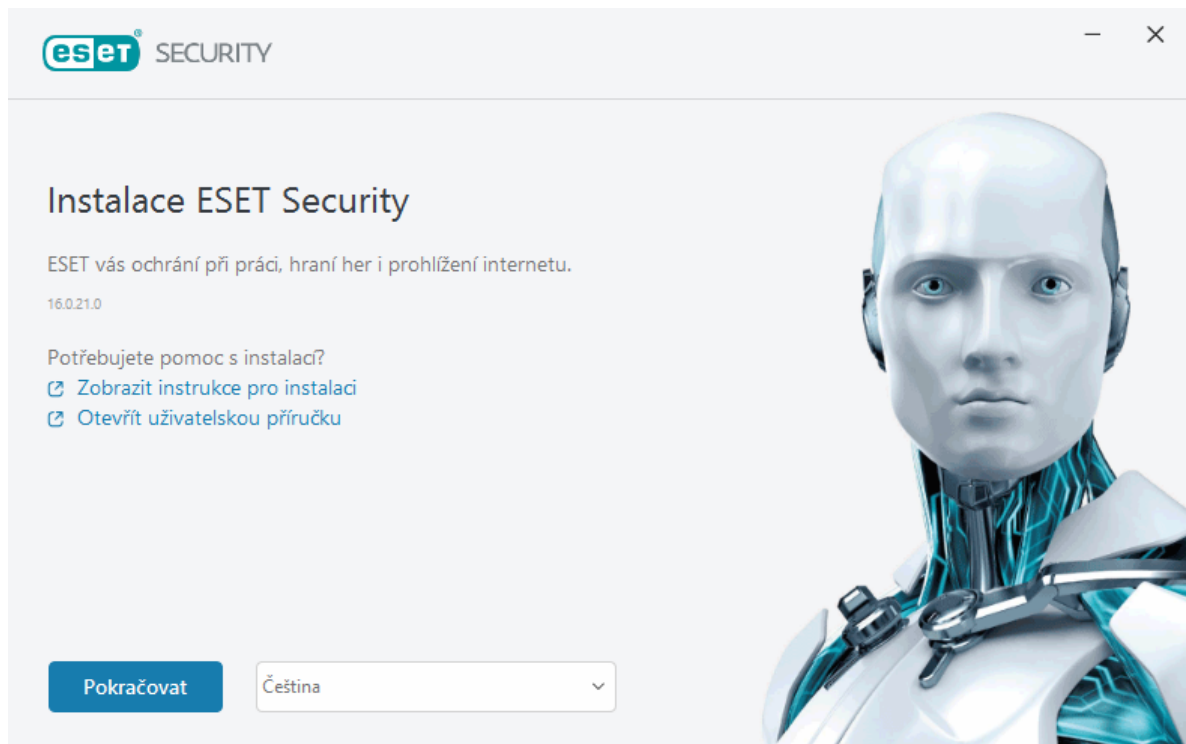
Před spuštěním instalace ESET NOD32 Antivirus se ujistěte, že na počítači není nainstalován žádný jiný antivirový program. Současný běh dvou a více antivirových programů na jednom počítači může vést k vzájemné nekompatibilitě. Proto doporučujeme odinstalovat všechny ostatní antivirové programy. V [ESET Databázi znalostí](#) naleznete nástroje pro odinstalaci nejrozšířenějších antivirových programů (dostupný v angličtině a několika dalších jazycích).

Online instalační balíček

Po stažení [Online instalačního balíčku Live installer](#), dvakrát klikněte na instalační soubor a postupujte krok za krokem podle pokynů v Průvodci instalací.



Tento způsob instalace vyžaduje připojení k internetu.



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

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

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

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

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

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


4. Pokud budete pokračovat bez připojení k účtu ESET HOME, zvolte si [možnost aktivace](#). Pokud již máte v počítači nainstalovanou starší verzi programu, licenční údaje se převezmou automaticky.

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

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

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


 [Poradce při potížích s instalací.](#)

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

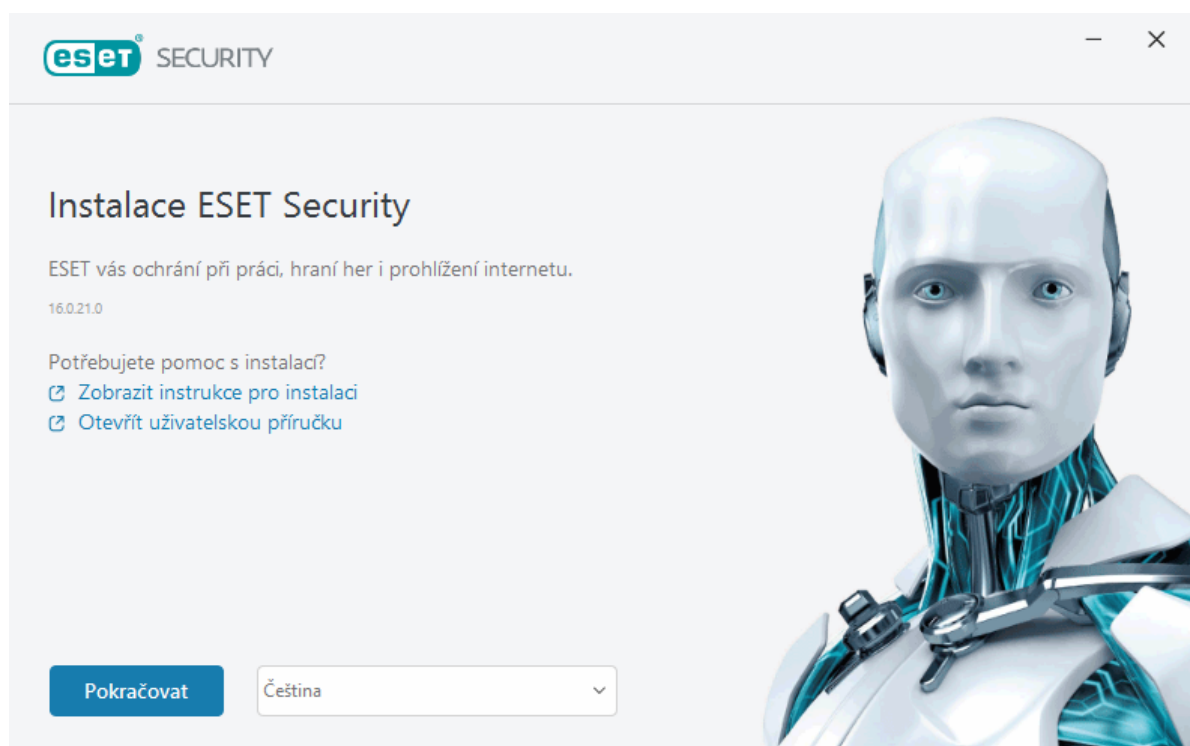
Offline instalace

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


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

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

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



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

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

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

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

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

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

4. Dále klikněte na **Přeskočit aktivaci**. Aby byl produkt ESET NOD32 Antivirus funkční, je nutné jej po dokončení instalace aktivovat. Pro jeho [aktivaci](#) je vyžadováno připojení k internetu.

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

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

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

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

Aktivace produktu

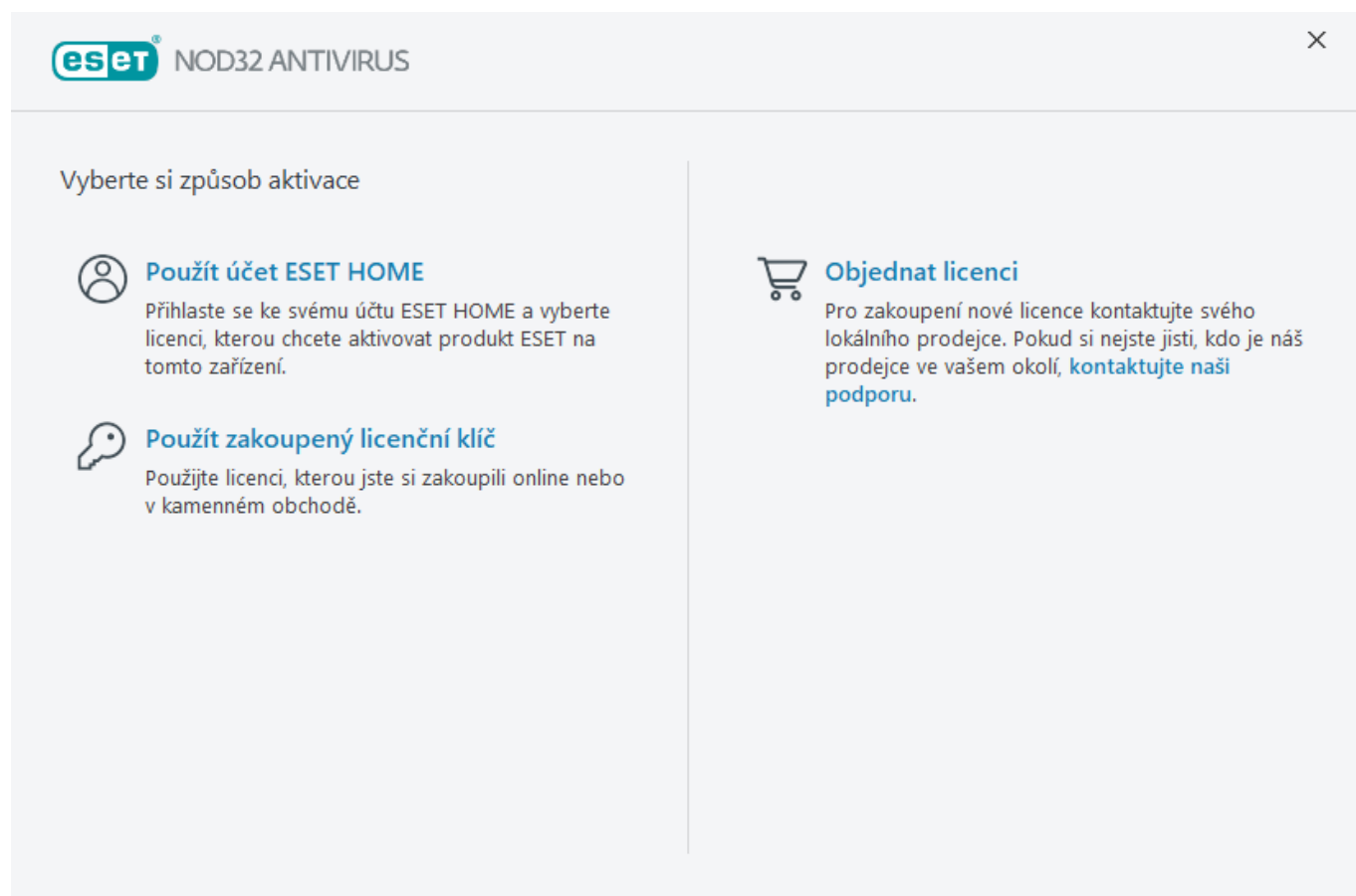
Produkt můžete aktivovat několika způsoby. Dostupnost jednotlivých metod závisí na zemi a způsobu distribuce (CD/DVD, webové stránky společnosti ESET, apod.):

- Pokud jste si zakoupili krabicovou verzi, případně jste obdrželi licenční údaje e-mailem, vyberte možnost **Použít zakoupený licenční klíč**. Pro úspěšnou aktivaci produktu je nutné licenční klíč zadat přesně tak, jak jste jej obdrželi. Licenční klíč je unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX nebo XXXX-XXXXXXXX, který slouží pro identifikaci vlastníka licence a aktivaci produktu. Licenční klíč se zpravidla nachází uvnitř nebo na zadní straně krabice.
- Po vybrání možnosti [Použít účet ESET HOME](#) budete vyzváni k zadání přihlašovacích údajů ke svému účtu ESET HOME.
- Pokud si chcete produkt ESET NOD32 Antivirus nejprve vyzkoušet, vyberte možnost [Zkušební verze](#). Následně budete vyzváni k výběru země a zadání e-mailové adresy, ke které budete mít zkušební verzi ESET NOD32 Antivirus vázanou. Po dokončení dojde k automatické aktivaci zkušební licence. Každý zákazník si může zkušební licenci aktivovat pouze jednou.
- Pokud zatím nemáte žádnou licenci, klikněte na možnost **Objednat licenci**. Následně budete přesměrováni na webové stránky lokálního distributora ESET. Licence ESET domácích produktů pro Windows [nejsou zdarma](#).

Kdykoli můžete licenci v produktu změnit. Pro přeaktivaci produktu jinou licencí přejděte v [hlavním okně programu](#) na záložku **Nápověda a podpora** a klikněte na tlačítko **Změnit licenci**. Na této obrazovce zároveň naleznete veřejné ID licence, které se používá pro identifikaci uživatele při komunikaci s technickou podporou

společnosti ESET.

 [Neúspěšná aktivace?](#)



Zadání licenčního klíče během aktivace

Pro správný chod bezpečnostního produktu ESET NOD32 Antivirus je důležité, aby byl automaticky aktualizován.

Licenční klíč zadávejte přesně tak, jak je napsaný. Licenční klíč je unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.


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

Pokud po dokončení instalace ne zadáte licenční klíč, produkt nebude aktivovaný. Pro aktivaci produktu ESET NOD32 Antivirus přejděte v [hlavním okně programu](#) na záložku **Nápověda a podpora** a klikněte na tlačítko **Aktivovat**.


Licence ESET domácích produktů pro Windows [nejsou zdarma](#).


Použití účtu ESET HOME


Pro zobrazení a správu licencí, včetně jimi aktivovaných zařízení, připojte zařízení k [ESET HOME](#). Prostřednictvím portálu můžete prodloužit platnost licence nebo zobrazit její detailní informace. V portálu nebo mobilní aplikaci ESET HOME můžete přidat všechny své licence, stahovat produkty přímo do svých zařízení, kontrolovat stavy zabezpečení svých zařízení nebo sdílet licence prostřednictvím e-mailu. Více informací naleznete v [Online](#)


 NOD32 ANTIVIRUS


Přihlášení k účtu ESET HOME

 Přihlásit se pomocí Google

 Přihlásit se pomocí Apple

 Naskenovat QR kód




 HOME

E-mailová adresa

Heslo

[Zapomněli jste heslo?](#)

 Přihlásit se

Zrušit

Nemáte účet? [Vytvořte si jej!](#)

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

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



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

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

2. Zadejte **Název zařízení**, pod kterým bude zobrazené v portálu ESET HOME a klikněte na možnost **Pokračovat**.
3. Vyberte si licenci, kterou chcete produkt aktivovat, případně klikněte na možnost [přidat novou licenci](#). Klikněte na tlačítko **Pokračovat** a dokončete aktivaci produktu ESET NOD32 Antivirus.

Aktivace zkušební licence

Pro aktivaci zkušební licence ESET NOD32 Antivirus zadejte platnou adresu do pole **E-mailová adresa** a **Potvrdit e-mailovou adresu**. Po aktivaci vám budou vygenerovány licenční údaje vyžadované pro aktualizaci produktu a tyto údaje zašleme na zadanou adresu. Adresa bude také použita pro oznámení před ukončením platnosti licence a pro další komunikaci se společností ESET. Zkušební licence může být aktivovaná pouze jednou.

Z rozbalovacího menu **Země** vyberte zemi pro registraci produktu ESET NOD32 Antivirus u lokálního distributora, který vám bude poskytovat technickou podporu.

Bezplatný licenční klíč na produkt ESET

Placená licence ESET NOD32 Antivirus není zdarma.

Licenční klíč ESET je unikátní sekvence písmen a číslic oddělených pomlčkou poskytovaná společností ESET v souladu s [Licenčním ujednáním s koncovým uživatelem](#) a slouží k legální aktivaci produktu ESET NOD32 Antivirus. Každý koncový uživatel je oprávněn používat licenční klíč pouze v rozsahu, v jakém má právo používat ESET NOD32 Antivirus – na základě počtu licencí udělených společností ESET. Licenční klíč je považován za důvěrný a není možné jej sdílet, ovšem [prostřednictvím portálu ESET HOME můžete sdílet jednotky své licence](#).

Na internetu můžete nalézt velké množství webových stránek, které vám zaručeně poskytnou licenční klíč ESET "zdarma", ale pamatujte:

- Kliknutím na reklamu "bezplatná ESET licence" může dojít ke kompromitaci vašeho počítače nebo zařízení a riskujete jeho napadení škodlivým kódem. Malware se může šířit prostřednictvím neoficiálního obsahu internetu (např. z různých fór nebo videí), z webových stránek slibujících zisk finančního obnosu na základě jejich navštívení apod. Jsou to běžné postupy, jak obelhat uživatele.
- Společnost ESET je schopna deaktivovat pirátské licence a také tak provádí.
- Aktivace produktu pirátskou licencí není v souladu s [Licenčním ujednáním s koncovým uživatelem](#), které přijímáte instalací ESET NOD32 Antivirus.
- Licenci na produkty ESET kupujte výhradně prostřednictvím oficiálních kanálů, například na webových stránkách www.eset.com, u distributorů a prodejců ESET. Nikdy nenakupujte licence na neoficiálních webových stránkách, jako je eBay, nebo sdílené licence poskytnuté třetí stranou.
- [Stažení](#) ESET NOD32 Antivirus je bezplatné, ovšem v průběhu instalace je vyžadována aktivace platným licenčním klíčem (produkt si můžete stáhnout a nainstalovat, nicméně bez aktivace nebude fungovat).
- Nesdílejte nikdy své licenční údaje prostřednictvím internetu nebo sociálních médií. Mohly by být rozšířeny a zneužity ve váš neprospěch.

Jak rozpoznat pirátskou licenci ESET, a jak ji nahlásit, se dovíte v [Databázi znalostí](#).

Pokud jste se dosud nerozhodli, že si zakoupíte bezpečnostní produkt ESET, můžete zatím využít zkušební verzi:

1. [Aktivujte ESET NOD32 Antivirus bezplatnou zkušební licencí](#)
2. [Zapojte se do ESET Beta programu](#)
3. Pokud používáte zařízení s operačním systémem Android, [nainstalujte si ESET Mobile Security](#). Jedná se o freemium.

Pro získání slevy / prodloužení licence si přečtěte článek: [Rozšíření a prodloužení licence na produkt ESET](#).

Neúspěšná aktivace – běžné scénáře

Nejčastější problémy s aktivací ESET NOD32 Antivirus mohou být:

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

Ověřte si, zda jste zadali správný licenční klíč, a pokuste se provést aktivaci znovu. Zkuste aktivovat ESET NOD32 Antivirus znovu. Jestliže pro aktivaci používáte účet ESET HOME, přečtěte si kapitolu Online nápovědy ESET HOME [Licence a jejich správa](#).

i Pokud se zobrazí konkrétní chyba (například Pozastavená licence nebo Nadužitá licence), postupujte podle pokynů v části [Stav licence a její odebrání](#).

Pokud se vám stále nedaří produkt ESET NOD32 Antivirus aktivovat, náš [ESET průvodce aktivací](#) vám poskytne odpovědi na nejčastější dotazy, aktivační chyby a problémy společně s informacemi týkajícími se licencování produktu.

Stav licence

Vaše licence může být různých stavech. Stav své licence můžete zjistit v [ESET HOME](#). Pokud chcete přidat svou licenci v účtu ESET HOME, přečtěte si [Přidání licence](#).

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

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

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

Popisy a doporučená řešení různých stavů licence naleznete v tabulce níže:

Stav licence	Popis	Řešení
Aktivní	Licence je platná a není nutná vaše součinnost. ESET NOD32 Antivirus lze licenci aktivovat a údaje o licenci najdete následně v hlavním okně programu > Nápověda a podpora .	
Nadužívána	Tato licence je používána na více zařízeních, než je povoleno. Zobrazí se chyba aktivace.	Pro vyřešení problému si prostudujte kapitolu: Neúspěšná aktivace z důvodu nadužívání licence .

Stav licence	Popis	Řešení
Pozastavena	Vaše licence byla pozastavena z důvodu problému s platbou. Chcete-li licenci používat, zkontrolujte prostřednictvím účtu ESET HOME, zda jsou platební údaje aktuální, nebo se obraťte na prodejce licence. Oznámení o této chybě se vám zobrazí během aktivace produktu nebo v hlavním okně programu .	Nainstalovaný produkt – pokud máte účet ESET HOME, klikněte v oznámení zobrazeném v hlavním okně programu na možnost Spravovat moji licenci v ESET HOME a zkontrolujte své platební údaje. Jinak kontaktujte prodejce vaší licence. Chyba při aktivaci – pokud máte účet ESET HOME, klikněte v oznámení zobrazeném v hlavním okně programu na možnost Přejít na ESET HOME a zkontrolujte své platební údaje. Jinak kontaktujte prodejce vaší licence.
Vypršela	Platnost vaší licence vypršela a tuto licenci nemůžete použít k aktivaci stránky ESET NOD32 Antivirus. Oznámení o této chybě se vám zobrazí během aktivace produktu nebo v hlavním okně programu . Pokud již nainstalovali ESET NOD32 Antivirus, vaše zařízení není chráněno a aktualizováno.	Nainstalovaný produkt – v oznámení zobrazeném v hlavním okně programu klikněte na položku Prodloužit licenci a postupujte podle pokynů v kapitole Jak zakoupit prodloužení licence , nebo klikněte na tlačítko Aktivovat produkt a vyberte způsob aktivace produktu . Chyba při aktivaci – v oznámení zobrazeném v hlavním okně programu klikněte na položku Prodloužit licenci a postupujte podle pokynů v kapitole Jak zakoupit prodloužení licence , nebo klikněte na tlačítko Aktivovat produkt a vyberte způsob aktivace produktu .
Zrušena	Vaše licence byla zrušena společností ESET nebo prodejcem licence.	Pokud se zobrazí chyba: Zrušení licence v hlavním okně programu nebo během aktivace, ale vaše licence by měla fungovat správně, kontaktujte svého prodejce licence.

Neúspěšná aktivace z důvodu nadužívání licence

Problém

- Vaše licence může být nadužívána nebo je zneužitá
- Neúspěšná aktivace z důvodu nadužívání licence

Řešení

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

Pokud jste vlastníky licence a nebyli jste požádáni o e-mailovou adresu:

1. Ke správě své licence ESET si otevřete ve webový prohlížeč a přejděte na adresu <https://home.eset.com>. Přejděte do sekce ESET License Manager, kde odstraňte již nepoužívaná zařízení, případně licenci deaktivujte na zařízeních, na kterých ji nechcete používat. Pro více informací si přečtěte článek [Co dělat v případě, kdy je licence nadužívána?](#)
2. Jak rozpoznat pirátskou licenci ESET a jak ji nahlásit, se dozvíte v článku [Databáze znalostí](#).
3. Pokud si nejste jisti, klikněte na tlačítko **Zpět** a použijte odkaz [Technická podpora společnosti ESET](#).

Pokud nejste její vlastníkem, kontaktujte vlastníka s informací, že produkt ESET nelze aktivovat licenci z důvodu jejího nadužívání. Vlastník může vyřešit problém na portálu [ESET HOME](#).

Pokud jste požádáni o potvrzení e-mailové adresy (pouze v některých případech), zadejte tu, kterou jste použili při nákupu a aktivaci ESET NOD32 Antivirus.

Povýšení licence

Tato možnost se zobrazí v případě, kdy byl produkt ESET aktivovaný vaší licencí změněn. Licenci můžete použít k aktivaci produktu s vyšším množstvím bezpečnostních funkcí. Pokud neprovedete žádnou akci, ESET NOD32 Antivirus zobrazí se okno **Změna na produkt s vyšším množstvím bezpečnostních funkcí**.

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

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

Pro pozdější změnu produktu si prostudujte článek [Jak změnit domácí produkt bez odinstalace původního](#)? Pro více informací o licencích ESET přejděte do článku [Nejčastější dotazy k licencování produktů](#) (článek nemusí být dostupný ve všech jazycích).

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detekční jádro	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓
Exploit Blocker	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓
Anti-Phishing	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Strážce sítě		✓	✓
Ochrana webkamery		✓	✓
Ochrana proti síťovým útokům		✓	✓
Ochrana proti zapojení do botnetu		✓	✓
Ochrana bankovníctví a online plateb		✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Rodičovská kontrola		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Povýšení produktu

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

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

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detekční jádro	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓
Exploit Blocker	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓
Anti-Phishing	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Strážce sítě		✓	✓
Ochrana webkamery		✓	✓
Ochrana proti síťovým útokům		✓	✓
Ochrana proti zapojení do botnetu		✓	✓
Ochrana bankovníctví a online plateb		✓	✓
Rodičovská kontrola		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Ponížení licence

Tato možnost se zobrazí v případě, kdy byl produkt ESET aktivovaný vaší licencí změněn. Licenci můžete použít k aktivaci produktu s menším množstvím bezpečnostních funkcí. Aby nedošlo ke ztrátě ochrany, byl produkt automaticky změněn.

Pro více informací o licencích ESET přejděte do článku [Nejčastější dotazy k licencování produktů](#) (článek nemusí být dostupný ve všech jazycích).

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detekční jádro	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓
Exploit Blocker	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓
Anti-Phishing	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Strážce sítě		✓	✓
Ochrana webkamery		✓	✓
Ochrana proti síťovým útokům		✓	✓
Ochrana proti zapojení do botnetu		✓	✓
Ochrana bankovníctví a online plateb		✓	✓
Rodičovská kontrola		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Ponížení produktu

Produkt, který jste právě nainstalovali, má více bezpečnostních funkcí než ten, který se chystáte aktivovat.

V níže uvedené tabulce uvádíme rozdíly mezi jednotlivými produkty.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Detekční jádro	✓	✓	✓
Pokročilé strojové učení	✓	✓	✓

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Exploit Blocker	✓	✓	✓
Ochrana proti skriptovým útokům	✓	✓	✓
Anti-Phishing	✓	✓	✓
Ochrana přístupu na web	✓	✓	✓
HIPS (včetně ochrany proti ransomware)	✓	✓	✓
Antispam		✓	✓
Firewall		✓	✓
Strážce sítě		✓	✓
Ochrana webkamery		✓	✓
Ochrana proti síťovým útokům		✓	✓
Ochrana proti zapojení do botnetu		✓	✓
Ochrana bankovníctví a online plateb		✓	✓
Rodičovská kontrola		✓	✓
Anti-Theft		✓	✓
Password Manager			✓
ESET Secure Data			✓
ESET LiveGuard			✓

Poradce při potížích s instalací

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

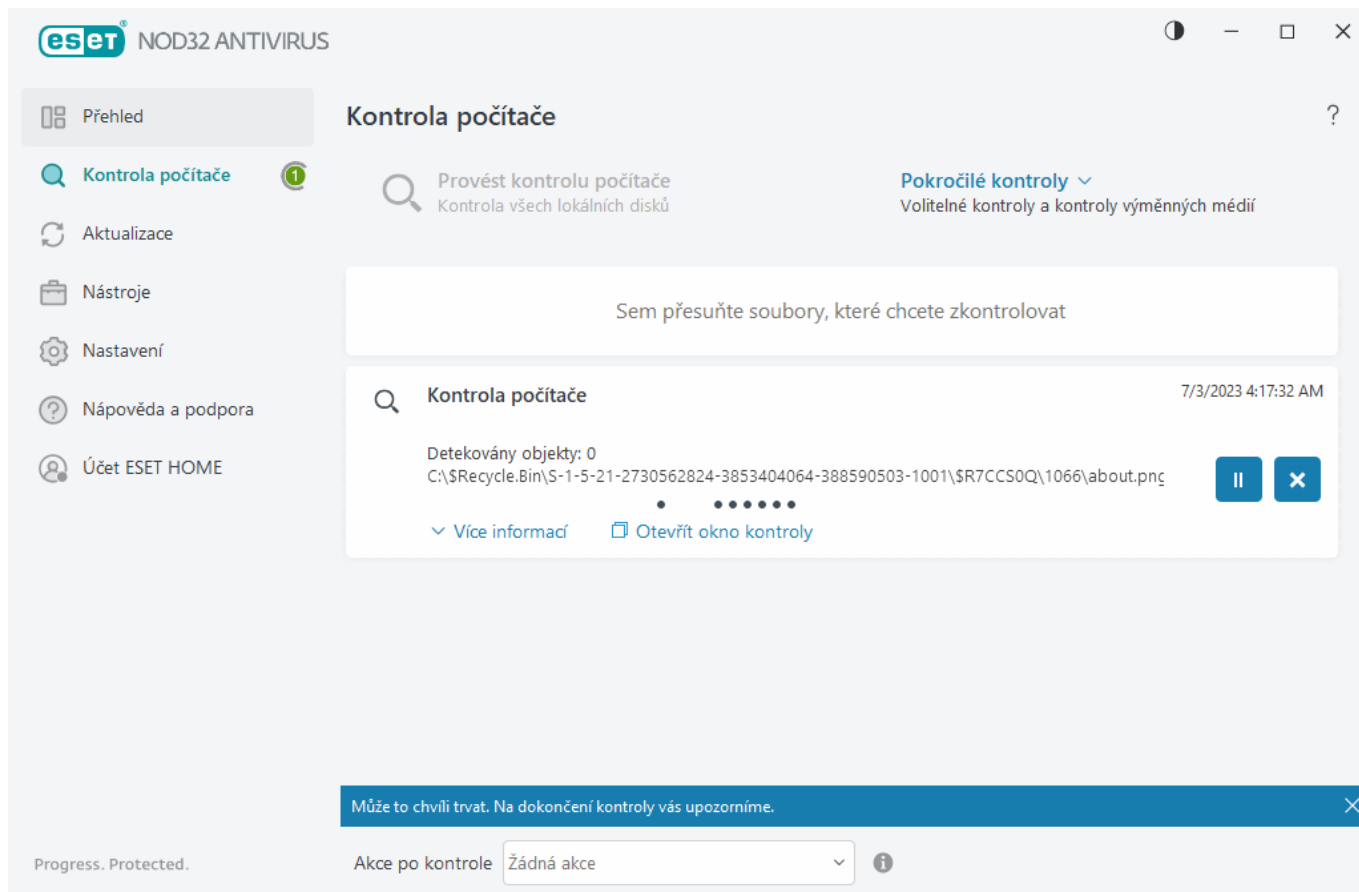
Pro spuštění klikněte na **Spustit Poradce při potížích**. Po dokončení postupujte podle doporučeného řešení.

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

Prvotní kontrola počítače po dokončení instalace

Po nainstalování ESET NOD32 Antivirus a aktualizování detekčních modulů se spustí automatická kontrola počítače zajišťující ochranu před škodlivým kódem.

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



Aktualizace na novou verzi

Nové verze ESET NOD32 Antivirus opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů. Existuje několik způsobů, jak aktualizovat produkt na novější verzi:

1. Automaticky prostřednictvím aktualizace programu.

Jelikož se aktualizace programu týká všech uživatelů a může mít významný dopad na systém, je vydávána až po dlouhém období testování na všech operačních systémech v různých konfiguracích. Pokud chcete aktualizovat na nejnovější verzi ihned po jejím vydání, použijte některou z níže uvedených metod.

Ujistěte se, že jste povolili **Aktualizace programových funkcí** v [Rozšířených nastaveních](#) > **Aktualizace** > **Profily** > **Aktualizace**.

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

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


Další informace a ilustrované návody:

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

Automatická aktualizace starších produktů

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

[Známé problémy při instalaci](#)

 Každá nová verze produktu ESET opravuje chyby a vylepšuje funkce. Stávající zákazníci s platnou licencí mohou svůj produkt ESET aktualizovat na nejnovější verze zcela zdarma.

Pro dokončení instalace postupujte podle následujících kroků:

1. Klikněte na tlačítko **Přijmout a pokračovat** pro souhlas s [Licenčním ujednáním s koncovým uživatelem](#) a [Zásadami ochrany osobních údajů](#). Pokud nesouhlasíte s Licenčním ujednáním s koncovým uživatelem, klikněte na tlačítko **Odinstalovat**. Upozorňujeme, že tím ovšem není možný návrat k předešlé verzi produktu.
2. Klikněte na tlačítko **Přijmout vše a pokračovat** pro aktivování [systému zpětné vazby ESET LiveGrid®](#) a zapojení se do [Programu zvyšování spokojenosti zákazníků](#). Pokud se nechcete obou uvedených systémů účastnit, klikněte na tlačítko **Pokračovat**.
3. Po aktivaci produktu ESET licenčním klíčem se zobrazí nová část Přehled. Pokud program nenalezne vaše licenční údaje, pokračujte aktivací zkušební licence. Jestliže licence použitá v předchozím produktu není platná, [aktivujte produkt vámi zakoupenou licencí](#).
4. Pro úplné dokončení instalace je vyžadován restart.

Nainstaluje se ESET NOD32 Antivirus

Toto dialogové okno lze zobrazit:

- Během instalačního procesu – pro instalaci klikněte na **Pokračovat**.
- Při změně licence ESET NOD32 Antivirus – pro její změnu a aktivaci klikněte na **Aktivovat**.

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

Přechod na jinou produktovou řadu

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

Registrace

Zaregistrujte svoji licenci vyplnění povinných polí a akci dokončete kliknutím na tlačítko Aktivovat. Pole označená jako povinná je nutné vyplnit. Tyto informace budou odeslány do společnosti ESET a slouží výhradně pro identifikaci vaší licence.

Průběh aktivace

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

Úspěšná aktivace

Proces aktivace byl dokončen.


Do několika sekund se spustí aktualizace modulů. Následně se bude produkt ESET NOD32 Antivirus aktualizovat automaticky.

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

Začínáme

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

Ikona v oznamovací oblasti

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

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



Vypnout antivirovou a antispywarovou ochranu?

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

Vypnout na 10 minut



Použít

Zrušit

Rozšířená nastavení – otevře [Rozšířená nastavení](#) ESET NOD32 Antivirus. Pro otevření Rozšířených nastavení z [hlavního okna programu](#) stiskněte funkční klávesu F5 nebo klikněte na **Nastavení > Rozšířená nastavení**.

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

Otevřít ESET NOD32 Antivirus – otevře [hlavní okno programu](#) ESET NOD32 Antivirus.

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

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

Zkontrolovat aktualizace – spustí aktualizaci modulu nebo produktu. Tímto krokem získáte nejnovější aktualizace produktu. ESET NOD32 Antivirus kontroluje aktualizace automaticky několikrát denně.

[O programu](#) – poskytuje informace o instalovaném programu ESET NOD32 Antivirus a všech jeho programovaných modulech. Také zde naleznete informace o operačním systému a systémových prostředcích.

Klávesové zkratky

Pro rychlejší navigaci v produktu ESET NOD32 Antivirus můžete použít také následující klávesové zkratky:

Klávesové zkratky	Akce
F1	otevře nápovědu
F5	otevře Rozšířená nastavení
Šipka nahoru / šipka dolů	přesun v položkách rozbalovací nabídky
TAB	přesun na následující ovládací prvek v uživatelském rozhraní
Shift+TAB	přesun na předchozí ovládací prvek v uživatelském rozhraní
ESC	zavře zobrazené dialogové okno
Ctrl+U	zobrazí dialogové okno se základními informacemi pro technickou podporu ESET, kde mj. najdete identifikátor své licence a informace o počítači
Ctrl+R	obnoví pozici a velikost okna na výchozí hodnoty
ALT + šipka vlevo	přesun zpět
ALT + šipka vpravo	přesun vpřed
ALT+Home	přesun na úvodní obrazovku

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

Profily

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

Kontrola počítače

K dispozici jsou čtyři předdefinované profily kontroly ESET NOD32 Antivirus:

- **Smart kontrola počítače:** toto je výchozí profil pokročilé kontroly. Profil Smart kontrola počítače využívá technologii Smart optimalizace, pro vyloučení souborů, které byly při předchozí kontrole označeny jako čisté, a nedošlo u nich od té doby ke změně. Tím se zkracuje doba kontroly při současném minimálním dopadu na zabezpečení systému.
- **Kontrola z kontextového menu:** Volitelnou kontrolu libovolného souboru můžete spustit z kontextového menu. Profil kontroly z kontextového menu umožňuje nastavit konfiguraci kontroly při jejím využití.
- **Hlubková kontrola počítače:** Profil hlubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.

- **Kontrola počítače:** Toto je výchozí profil používaný při standardní kontrole počítače.

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

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

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

Aktualizace

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

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

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

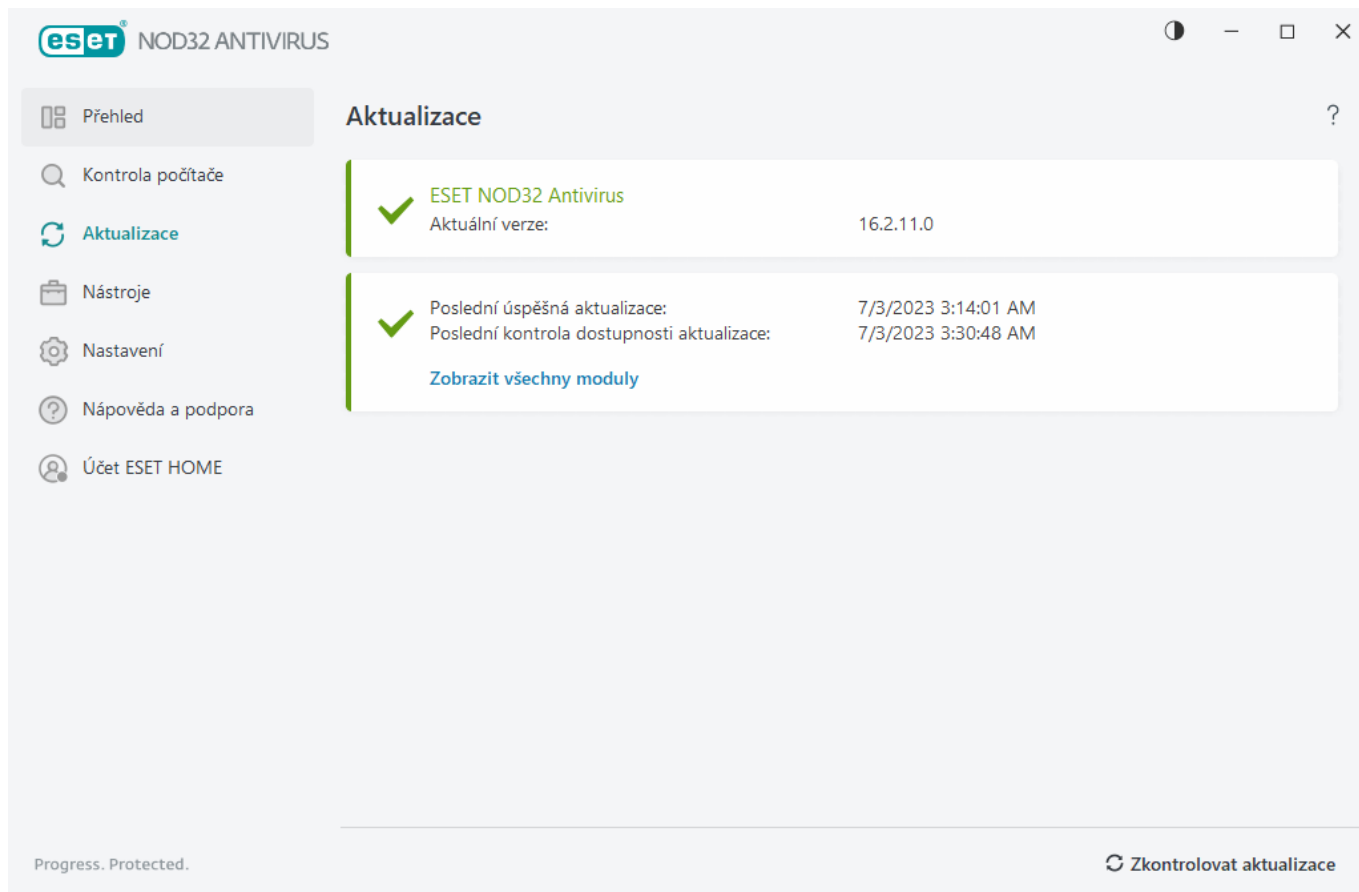
Seznam profilů – správa existujících aktualizací profilů.

Aktualizace

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

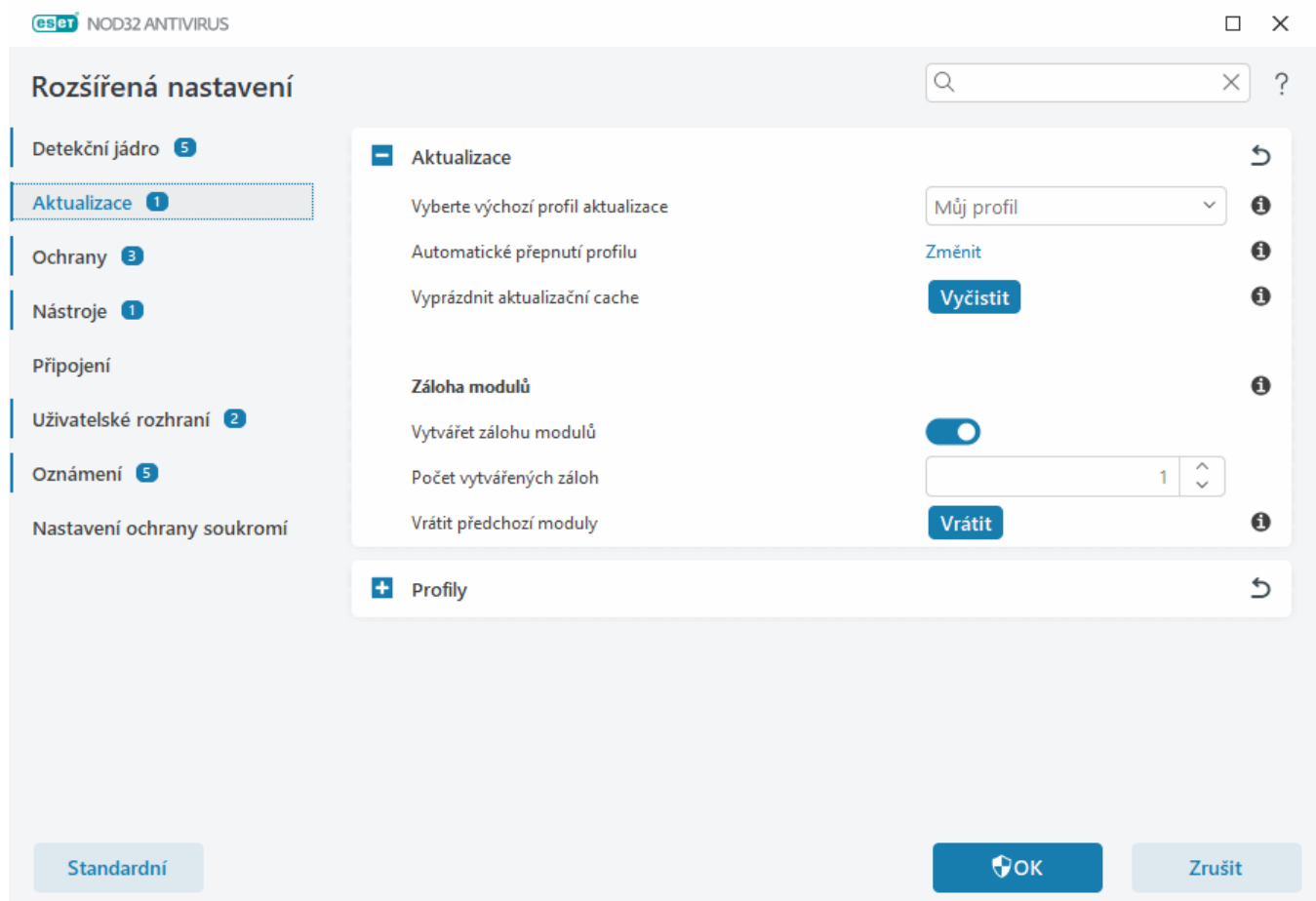
Informace o aktuálním stavu aktualizace jsou zobrazovány na záložce **Aktualizace** v [hlavním okně programu](#). Naleznete zde informaci o datu a čase poslední úspěšné aktualizace, zda jsou moduly aktuální, případně jestli není potřeba program aktualizovat.

Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na tlačítko **Zkontrolovat aktualizace**.



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

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



Práce s ESET NOD32 Antivirus

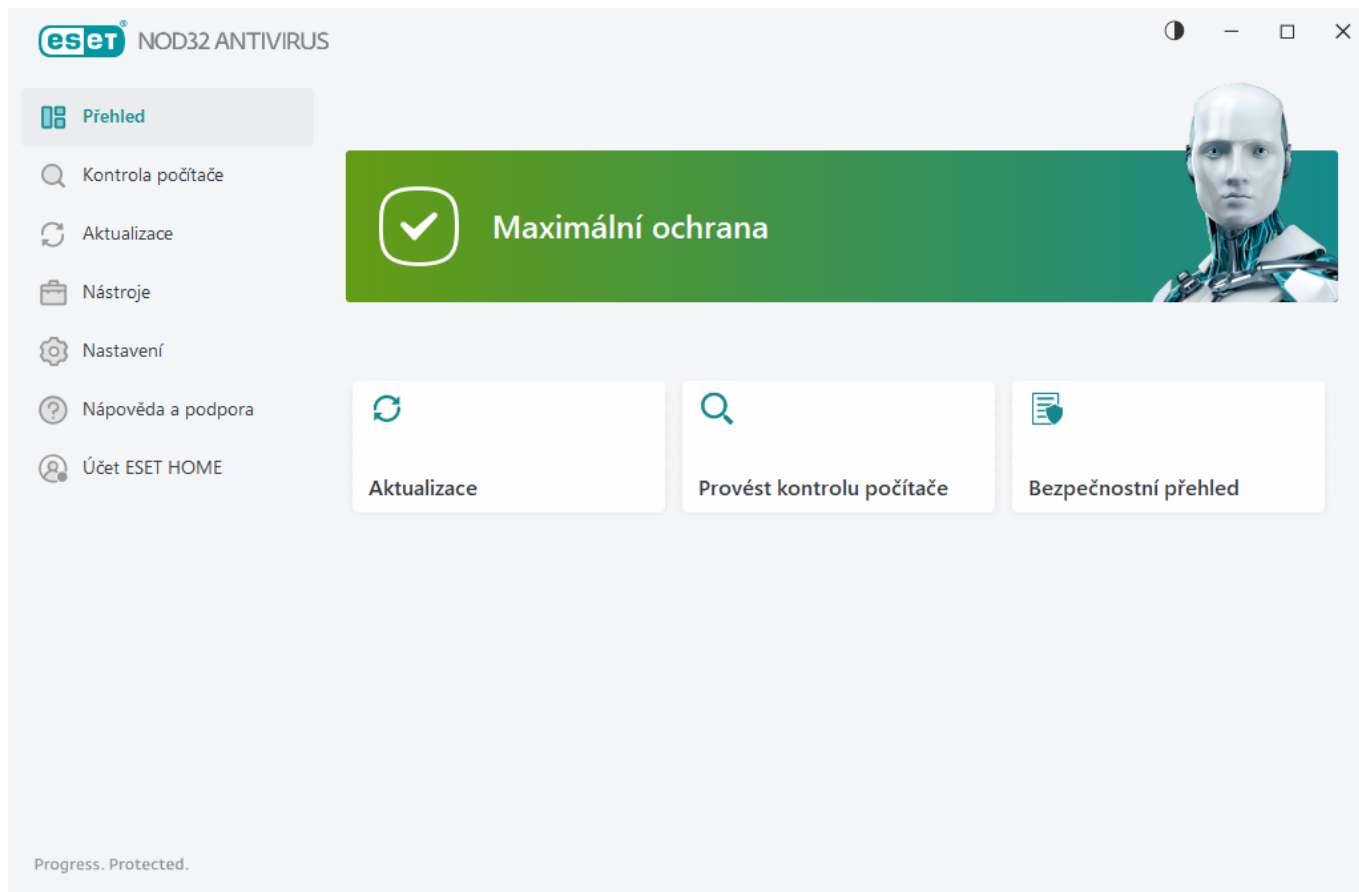
Hlavní okno programu ESET NOD32 Antivirus je rozděleno na dvě hlavní části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Názorné ukázky

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

V pravém horním rohu hlavního okna programu si můžete navolit barevný režim, ve kterém se vám bude zobrazovat uživatelské rozhraní ESET NOD32 Antivirus. Klikněte na ikonu pro **barevné schéma** (ikona se mění podle aktuálně vybraného barevného schématu) vedle ikony pro **minimalizaci** a z rozbalovacího menu vyberte barevný režim:

- **Stejný jako barva systému** – rozhraní ESET NOD32 Antivirus se zobrazí ve stejném barevném schématu, jako uživatelské rozhraní vašeho operačního systému.
- **Tmavý** – ESET NOD32 Antivirus bude zobrazen v tmavém režimu.
- **Světlý** – ESET NOD32 Antivirus bude zobrazen ve světlém režimu.



Položky hlavního menu:

[Přehled](#) – poskytuje informace o událostech a stavu ochrany ESET NOD32 Antivirus.

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

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

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

[Nastavení](#) – umožňují konfiguraci ochranných funkcí ESET NOD32 Antivirus (Ochrana počítače a Internetová ochrana) a přístup k [Rozšířeným nastavením](#).

[Nápověda a podpora](#) – Zobrazuje informace o vaší licenci, nainstalovaném produktu ESET a odkazy na [Online nápovědu](#), [Databázi znalostí](#) a [Technickou podporu](#).

[Účet ESET HOME](#) – v této části můžete [připojit zařízení ke svému účtu ESET HOME](#) nebo zkontrolovat stav připojení k účtu. Použijte [ESET HOME](#) pro zobrazení a správu aktivovaných licencí a zařízení ESET.

Přehled

V části **Přehled** se zobrazují informace o aktuální ochraně počítače spolu s rychlými odkazy na bezpečnostní funkce ESET NOD32 Antivirus.

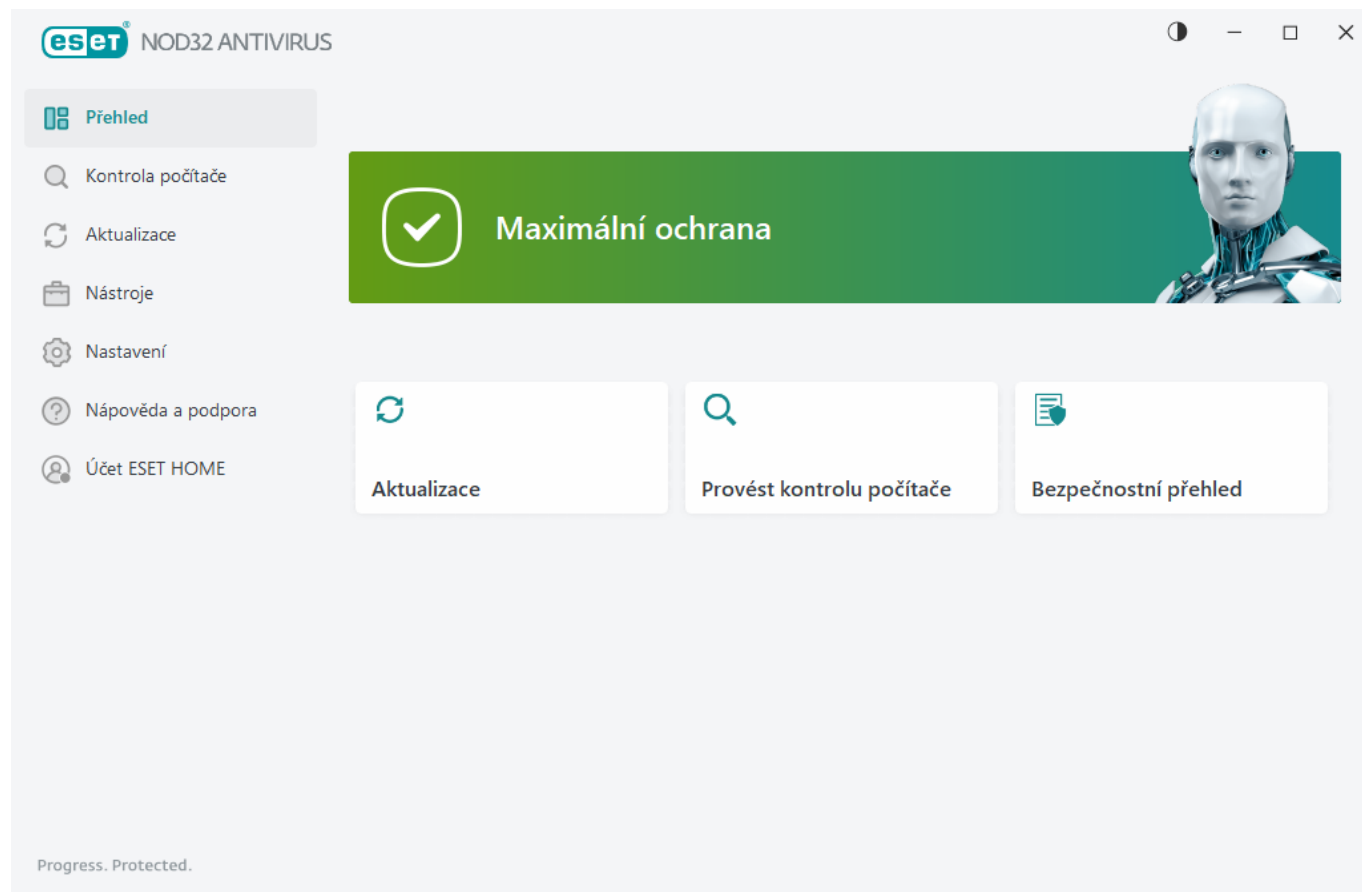
V okně **Přehled** se zobrazují [oznámení](#) s podrobnými informacemi a doporučenými řešeními událostí v ESET NOD32 Antivirus, pro zapnutí dalších funkcí nebo zajištění maximální ochrany. Pokud je oznámení více, kliknutím

na **více oznámení** je všechny rozbalíte.

Aktualizovat – otevře sekci [Aktualizace](#) a zkontroluje, zda nejsou k dispozici aktualizace.

Provést kontrolu počítače – otevře sekci [Kontrola počítače](#) a spustí [standardní kontrolu počítače](#).

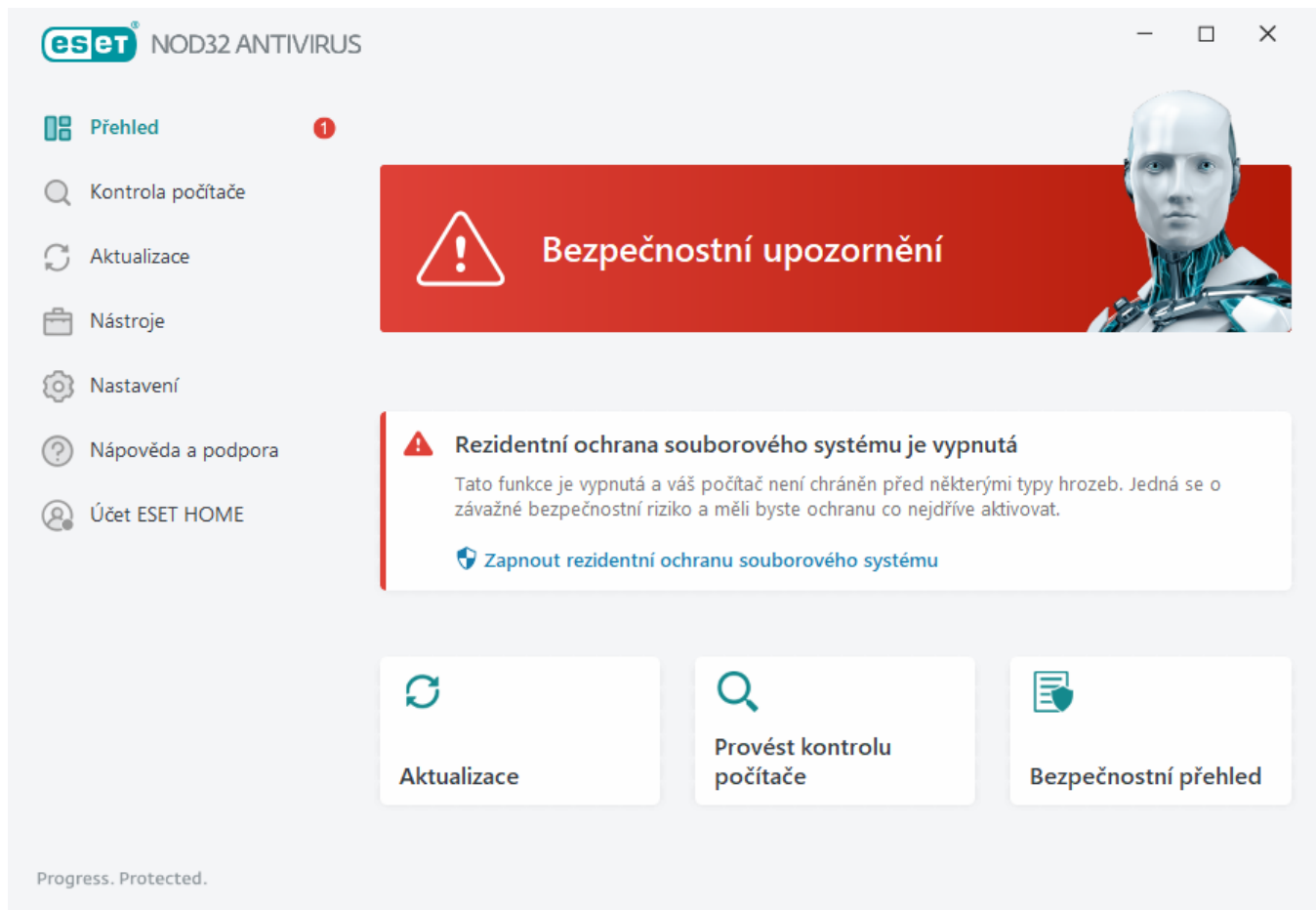
Bezpečnostní přehled – otevře sekci [Bezpečnostní přehled](#).



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

Co dělat, pokud systém nepracuje správně?

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



Červená barva stavu a informace **Bezpečnostní upozornění** signalizují kritické problémy. Ochrana vašeho systému není zajištěna v plné míře. Možné příčiny jsou:

- **Produkt není aktivován** nebo **Platnost licence vypršela** – ikona ochrany změnila barvu na červenou. Program nebude možné od této chvíle aktualizovat. Přečtěte si v okně s upozorněním, jak licenci prodloužit.
- **Detekční jádro není aktuální** – tato chyba se zobrazí po neúspěšném kontaktování serveru při pokusu o aktualizaci detekčního jádra. V takovém případě doporučujeme zkontrolovat nastavení aktualizací. Mezi nejčastější důvody patří nesprávně zadaná [ověřovací data](#) nebo nesprávně nastavené [připojení k internetu](#).
- **Rezidentní ochrana souborového systému je dočasně vypnutá** – rezidentní ochrana byla vypnuta uživatelem. Váš počítač není chráněn před hrozbami. Pro opětovné zapnutí Rezidentní ochrany souborového systému klikněte na **Zapnout rezidentní ochranu**.
- **Antivirová a antispywarová ochrana je vypnutá** – ochranu zapněte kliknutím na **Zapnout antivirovou a antispywarovou ochranu**.



Žlutá barva stavu ochrany znamená částečné problémy. Bývají to například problémy s aktualizací programu nebo blížící se datum vypršení licence.

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

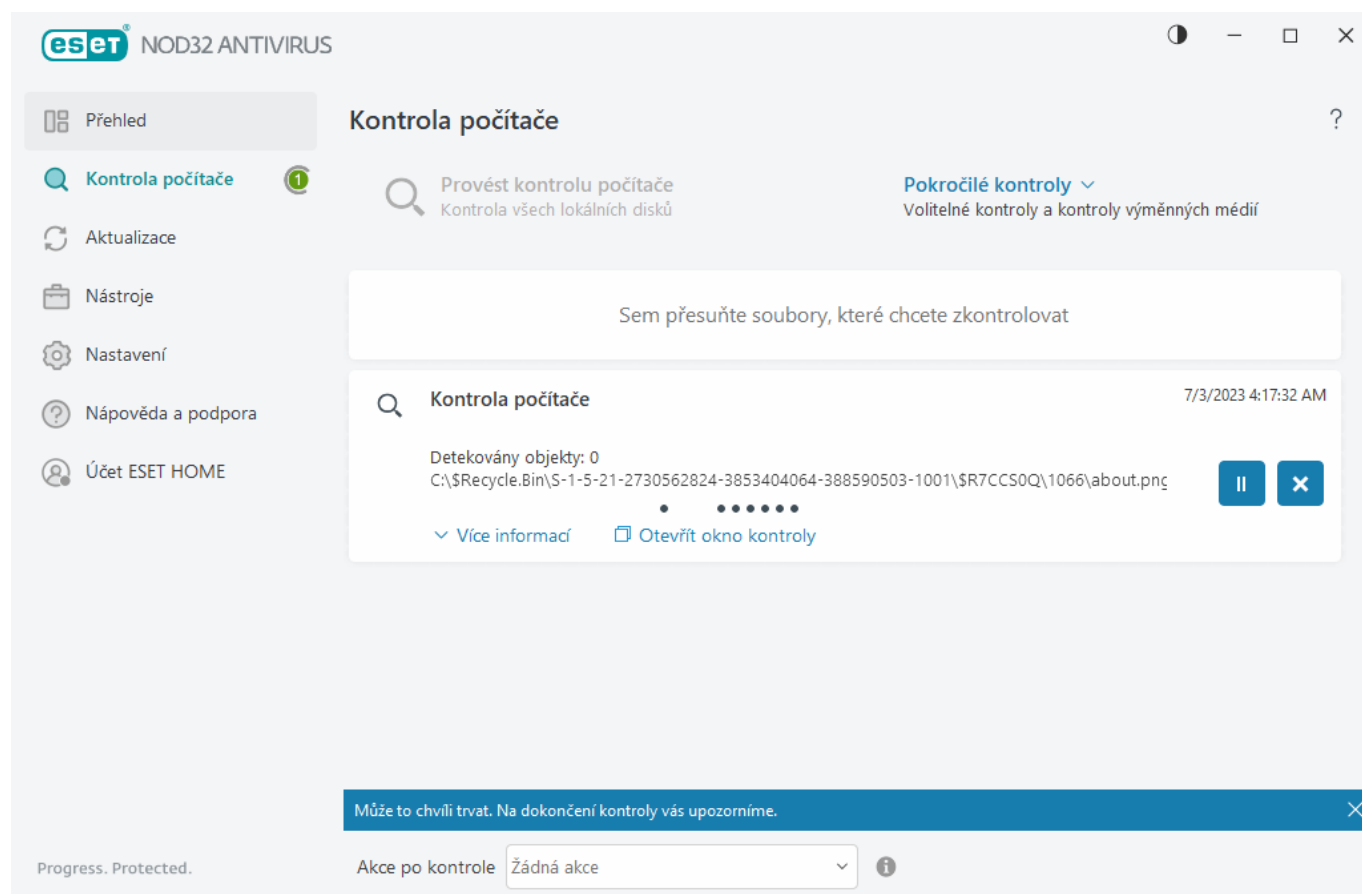
- **Herní režim je zapnutý** – zapnutí [Herního režimu](#) představuje potenciální bezpečnostní riziko. Povolením této funkce zakážete všechna okna s oznámeními nebo upozorněními a zastavíte všechny naplánované úlohy.
- **Blíží se konec platnosti licence / Platnost vaší licence dnes vyprší** – ikona produktu vedle

systémových hodin bude označena žlutou ikonou stavu ochrany s vykřičníkem. Poté, co licence vyprší, se program přestane aktualizovat a ikona ochrany změní barvu na červenou.

V případě, že není možné problém vyřešit, klikněte v hlavním okně programu na záložku **Nápověda a podpora** a zobrazte nápovědu nebo přejděte do [ESET Databáze znalostí](#). Pokud i přesto budete potřebovat pomoc, pošlete dotaz na technickou podporu. Specialisté technické podpory ESET vám odpoví v co nejkratším možném čase a pomohou vám s řešením problému.

Kontrola počítače

Důležitou součástí antivirového řešení je volitelná kontrola. Díky ní si spustíte vlastní kontrolu jednotlivých složek a souborů v počítači. Z bezpečnostního hlediska je žádoucí, aby kontrola počítače byla spouštěna nejen při podezření na infikované soubory, ale v rámci prevence i průběžně. Hlubkovou kontrolu pevného disku doporučujeme provádět v určitých časových intervalech, aby byl detekován případný malware, který v době zápisu na disk nebyl zachycen [Rezidentní ochranou souborového systému](#). Taková situace může nastat, pokud byla rezidentní ochrana v té době vypnutá nebo program neměl aktuální detekční moduly, případně soubor v době zápisu na disk program nebyl vyhodnocen jako vir.



K dispozici jsou dva typy **kontroly počítače**. Pokud klikněte na možnost **Provést kontrolu počítače**, spustí se rychlá kontrola systému bez nutnosti specifikovat parametry kontroly. **Volitelná kontrola** (po kliknutí na Pokročilé kontroly), umožňuje vybrat předdefinované profily kontroly, které jsou navrženy tak, aby cílily na konkrétní místa a také vybraly konkrétní cíle kontroly.

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

i Ve výchozím stavu se ESET NOD32 Antivirus pokusí automaticky vyléčit nebo smazat objekty, které detekoval během kontroly počítače. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Instrukce pro změnu úrovně léčení společně s jejich detailním popisem máme uveden v kapitole [Úroveň léčení](#). Výsledky provedených kontrol naleznete v [Protokolech](#).

Provést kontrolu počítače

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

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

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

Volitelná kontrola

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

Kontrola výměnných médií

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

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

Opakovat poslední kontrolu

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

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

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

potřeba pro dokončení léčení detekovaných hrozeb.

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



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

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



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

Spuštění volitelné kontroly

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

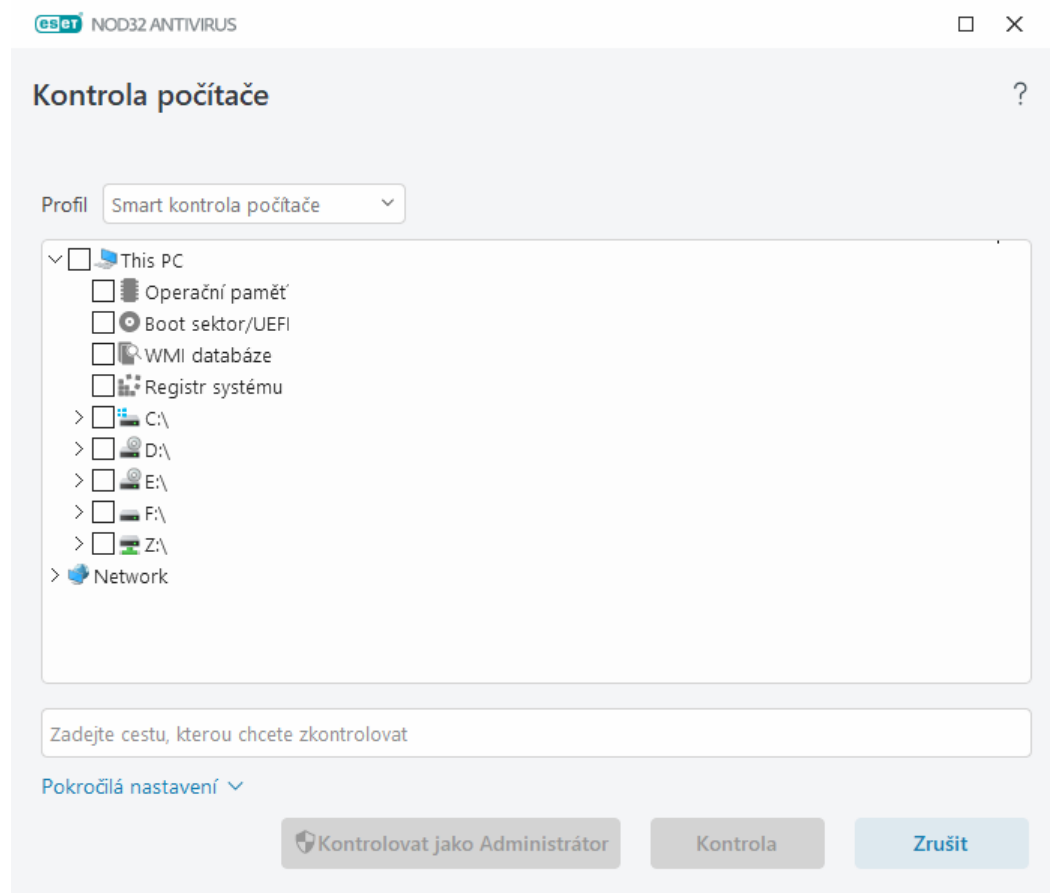
Pomocí rozbalovacího menu **Profil** si můžete vybrat jeden z předdefinovaných profilů kontroly. Výchozím profilem je **Smart kontrola počítače**. Dále jsou dostupné tři předdefinované profily pojmenované **Hlubková kontrola počítače**, **Kontrola z kontextového menu** a **Kontrola počítače**. Navzájem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

Další cíle kontroly si můžete vybrat ve stromové struktuře.

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

Pro rychlý přesun k požadovanému cíli kontroly (souboru nebo složce), zadejte jeho cestu do textového pole zobrazeném pod stromovou strukturou. Mějte na paměti, že se v cestě rozlišuje velikost písmen. Použitím zaškrtnutí pole ve stromové struktuře přidáte daný cíl do seznamu cílů, které se mají kontrolovat.

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



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

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

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

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

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

Průběh kontroly

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



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



Jak naplánovat každý týden kontrolu počítače?

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

Průběh kontroly – ukazatel průběhu zobrazuje stav probíhající kontroly.

Cíl – název právě kontrolovaného souboru a jeho umístění.

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

Kliknutím na Více informací se zobrazí následující informace:

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

Ikona pozastavení – přeruší kontrolu.

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

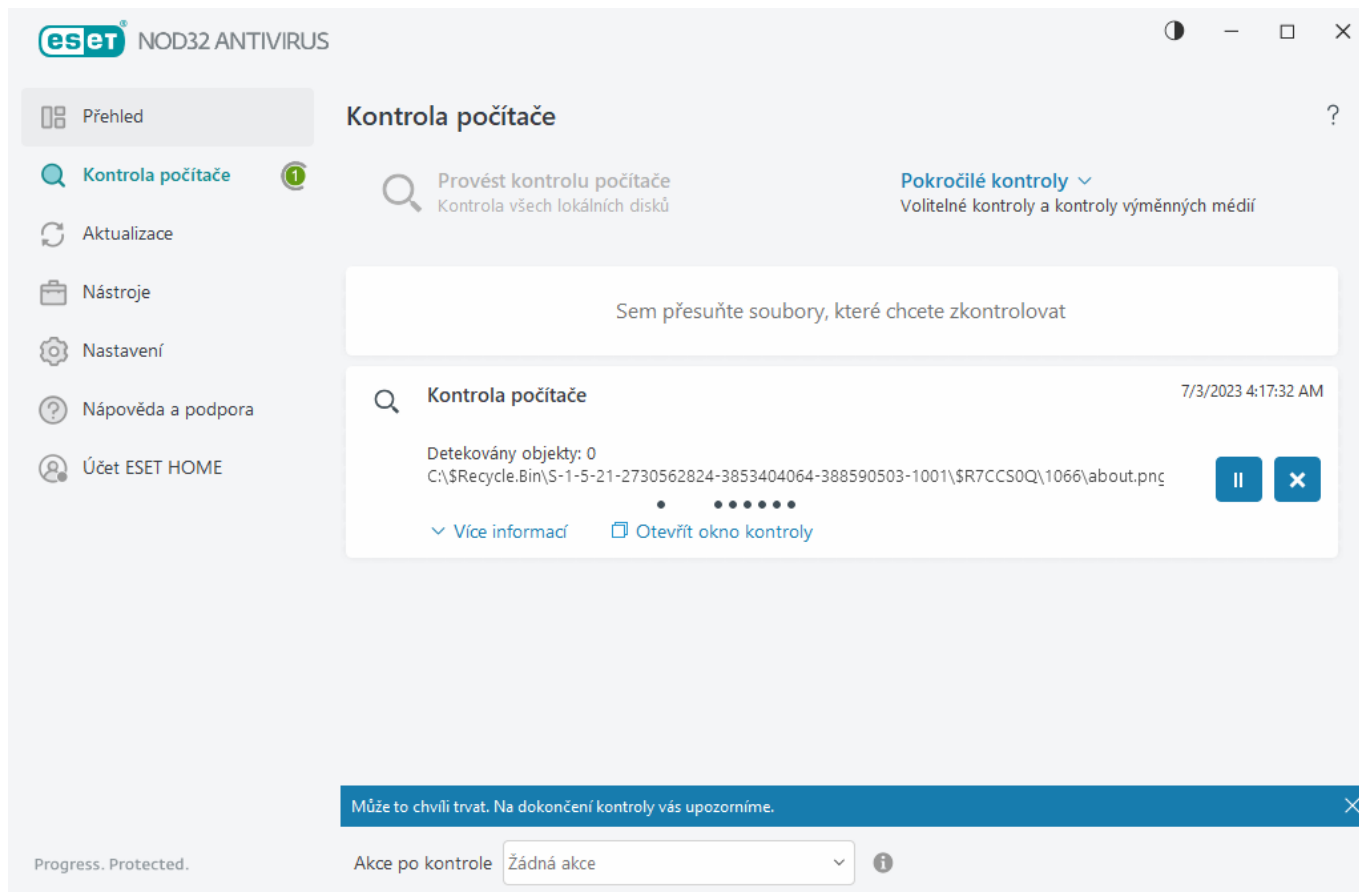
Ikona Stop – ukončí kontrolu.

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

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



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



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

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



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

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

Protokol kontroly počítače

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

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



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

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

Kontrola počítače



Protokol kontroly

Verze detekčního jádra: 27508 (20230703)

Datum: 7/3/2023 Čas: 4:17:32 AM

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

User: DESKTOP-ILTJID9\User

Kontrola přerušena uživatelem.

Počet kontrolovaných objektů: 6860

Počet detekcí: 0

Čas ukončení: 4:17:44 AM Celkový čas kontroly: 12 sek (00:00:12)

☐ Filtrování

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

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

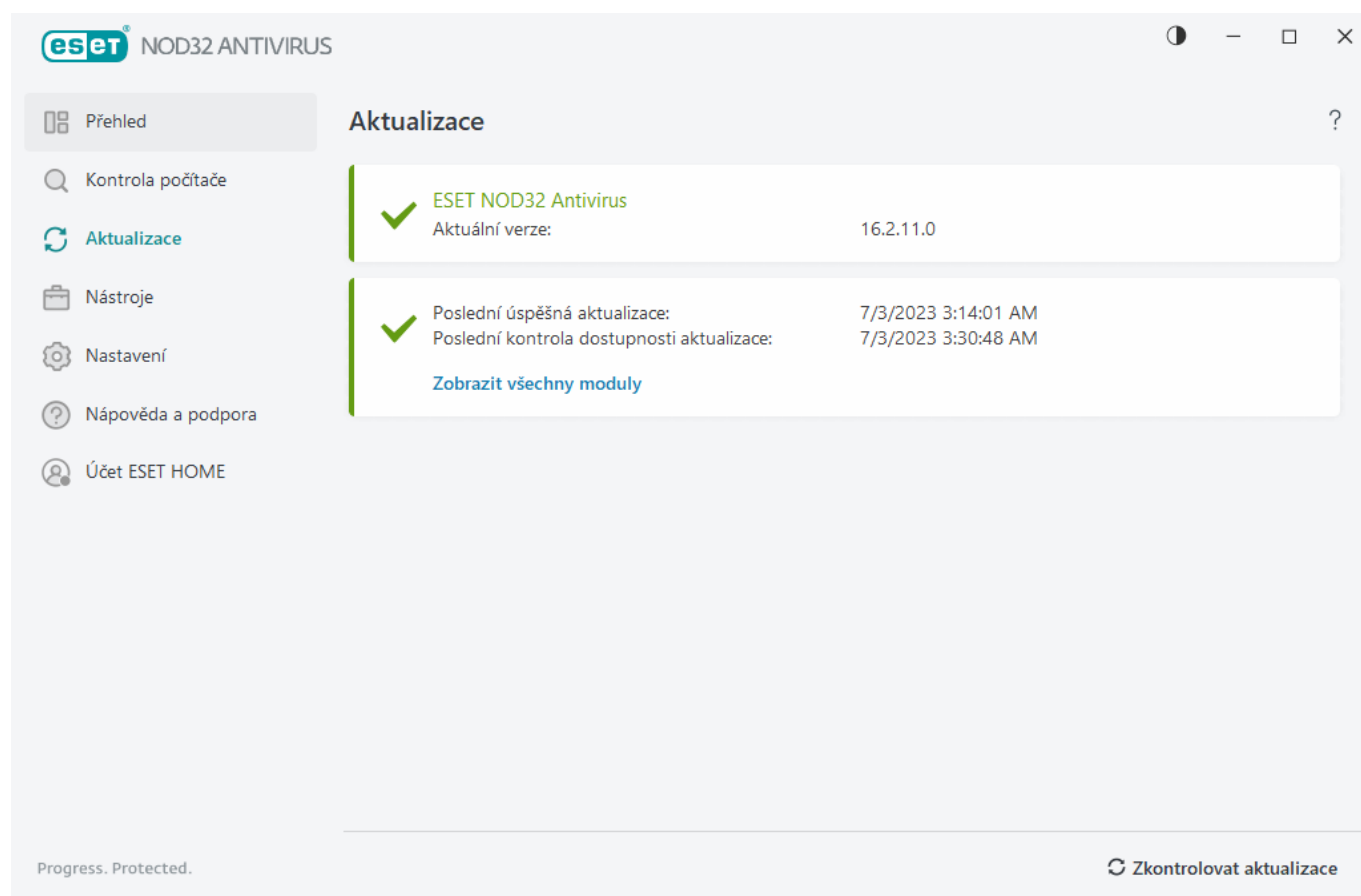
Akce	Použití
Filtrovat stejné záznamy	Aktivuje filtrování protokolu. V protokolu se následně zobrazí pouze záznamy stejného typu, odpovídající aktuálně vybranému záznamu.
Filtr	Tato možnost otevře okno Filtrování protokolu a umožňuje definovat kritéria pro konkrétní položky protokolu. Klávesová zkratka: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

Aktualizace

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

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

Aktualizace se kontrolují, stahují a instalují automaticky, jejich dostupnost můžete ověřit kdykoli kliknutím na tlačítko **Zkontrolovat aktualizace**. Pravidelná aktualizace modulů a komponent je důležitým aspektem pro zachování plné ochrany před škodlivým kódem. Věnujte prosím pozornost konfiguraci a práci modulů. Pro příjem automatických aktualizací je třeba produkt aktivovat pomocí licenčního klíče. Pokud jste tak neučinili během instalace, je nutné [aktivovat ESET NOD32 Antivirus](#), abyste získali přístup k aktualizacím serverům společnosti ESET. Licenční klíč jste obdrželi po nákupu nebo registraci ESET NOD32 Antivirus.



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

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

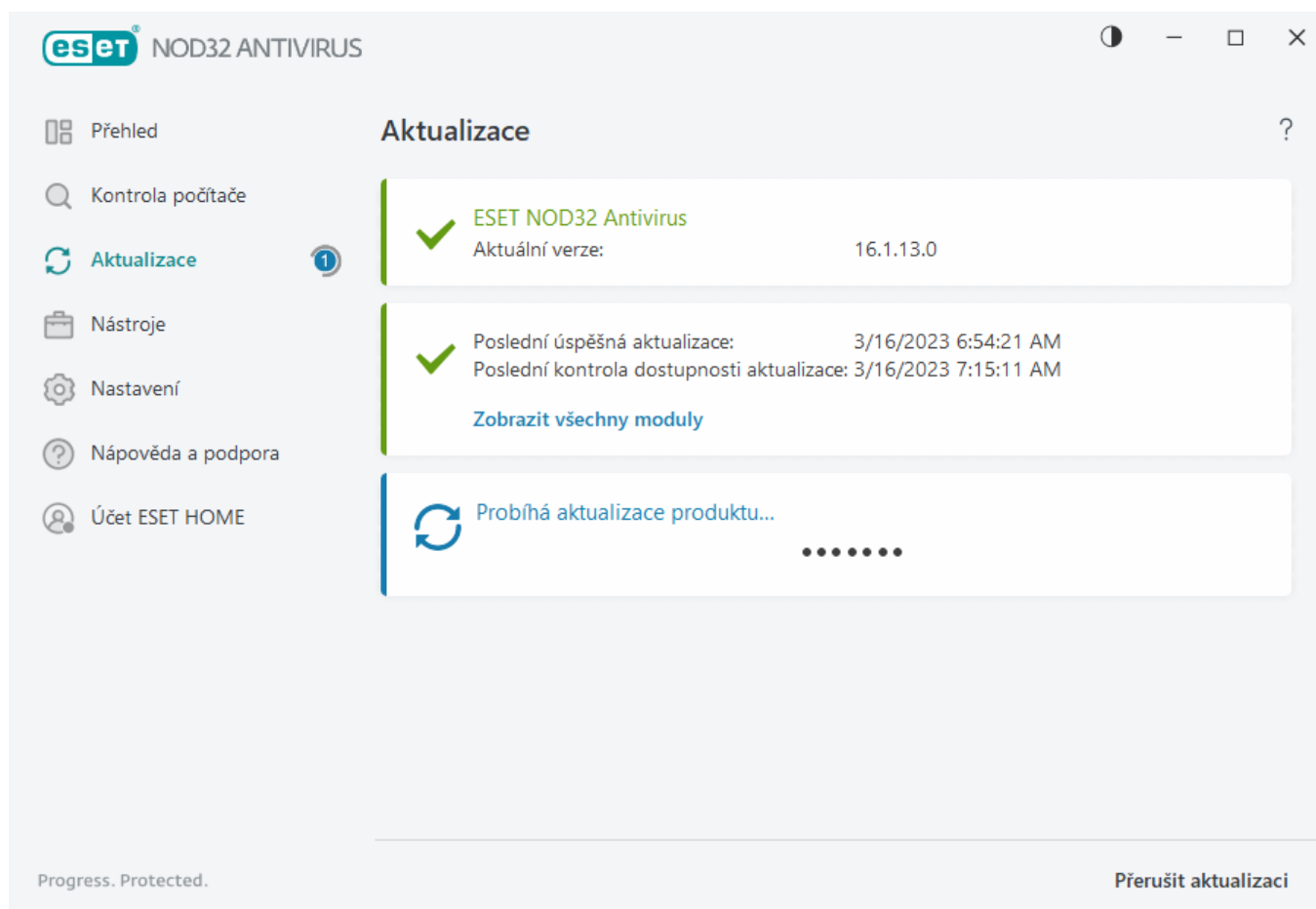
Poslední kontrola dostupnosti aktualizace – zobrazuje datum, kdy se program naposledy připojil k aktualizacím serverům a ověřil, zda není dostupná nová verze modulů.

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

Kliknutím na **Zkontrolovat aktualizace** zkontrolujte, zda máte nejnovější verzi ESET NOD32 Antivirus.

Průběh stahování

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



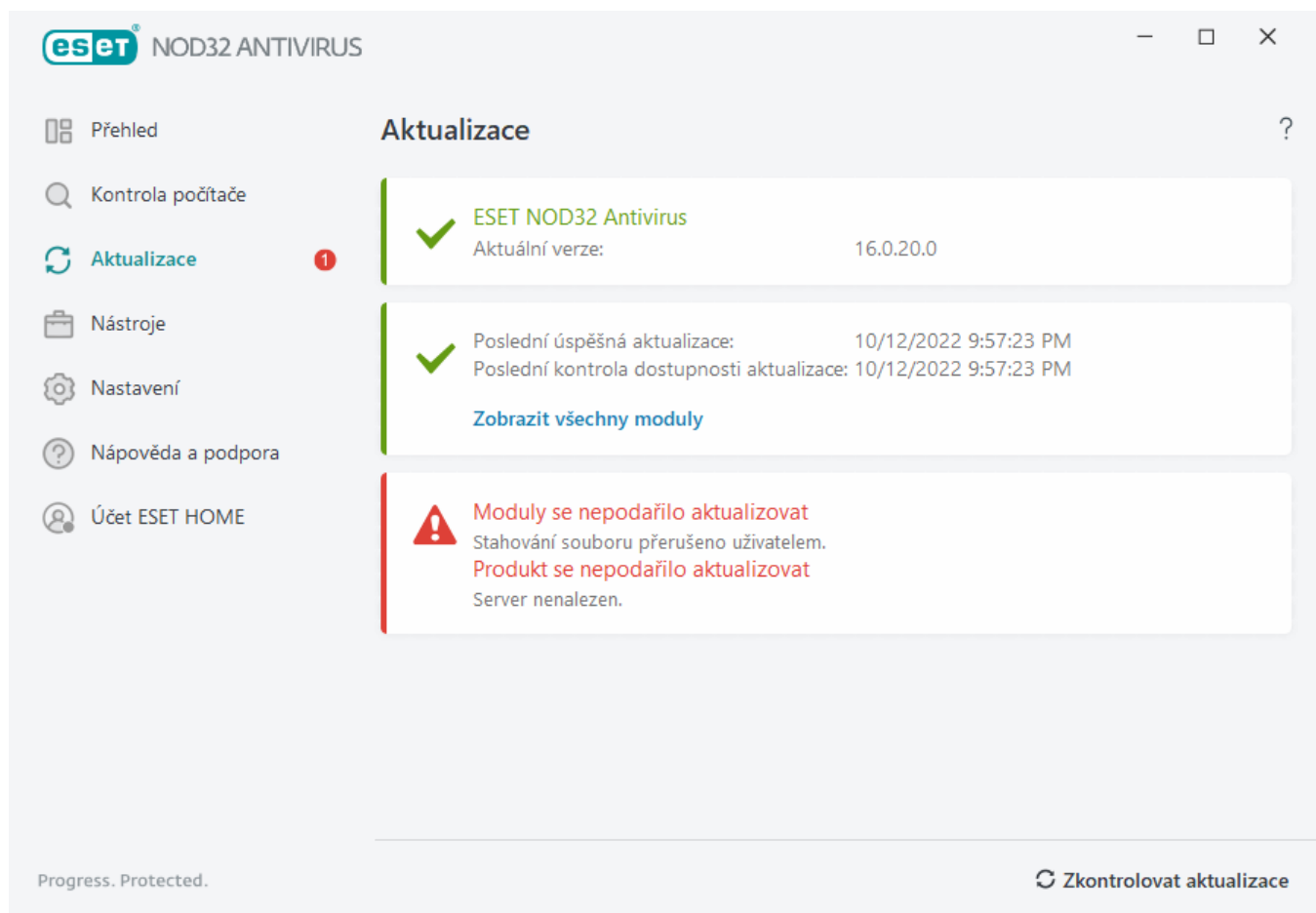
Za normálních okolností, při pravidelné a úspěšné stahování aktualizací, se v okně **Aktualizace** zobrazuje zelená fajfka. Pokud tomu tak není, program nepoužívá aktuální detekční moduly, čímž se zvyšuje riziko infiltrace. V takovém případě doporučujeme co nejdříve moduly aktualizovat.

Poslední úspěšná aktualizace

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

1. **Neplatná licence** – licence, kterou jste použili k aktivaci produktu, je neplatná nebo vypršela její platnost. V [hlavním okně programu](#) přejděte na záložku **Návod a podpora**, klikněte na **Změnit licenci** a aktivujte produkt.
2. **Při pokusu o stažení souboru aktualizace došlo k chybě** – to může být způsobeno nesprávným [nastavením připojení](#). Doporučujeme, abyste vyzkoušeli připojení k internetu (otevřením jakékoli webové stránky ve

webovém prohlížeči). Pokud se stránka nenačte, děje se tak v situaci, kdy počítač připojen k internetu není nebo má problémy s připojením. Rovněž doporučujeme zkontrolovat, zda je počítač připojen k internetu, a ověřit, zda poskytovatel internetu nemá výpadek připojení.



! Po úspěšné aktualizaci ESET NOD32 Antivirus musíte restartovat vaše zařízení, aby se programové moduly aktualizovaly správně. Toto není vyloženě nutné po aktualizaci programových modulů.

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

Dialogové okno – Vyžadován restart

Po aktualizaci ESET NOD32 Antivirus na novou verzi je vyžadován restart počítače. Nové verze ESET NOD32 Antivirus opravují známé chyby a přidávají nové funkce, které není možné distribuovat v rámci automatické aktualizace programových modulů.

Novou verzi ESET NOD32 Antivirus lze získat v [závislosti na nastavení aktualizace](#) automaticky nebo ručně [stažením a nainstalováním nejnovější verze](#) přes stávající.

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

Jak vytvořit aktualizací úlohu?

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

Aktualizaci můžete také spouštět jako naplánovanou úlohu. Pro vytvoření naplánované úlohy klikněte v hlavním okně programu na záložku **Nástroje > Plánovač**. Ve výchozím nastavení jsou v ESET NOD32 Antivirus aktivovány následující aktualizací úlohy:

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

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

Nástroje

Nabídka **Nástroje** obsahuje funkce, které nabízejí dodatečná zabezpečení a pomáhají zjednodušit správu ESET NOD32 Antivirus. K dispozici jsou následující nástroje:



[Protokoly](#)



[Spuštěné procesy](#) (pokud je ESET LiveGrid® v ESET NOD32 Antivirus zapnut)



[Bezpečnostní přehled](#)



[ESET SysInspector](#)



[Plánovač](#)



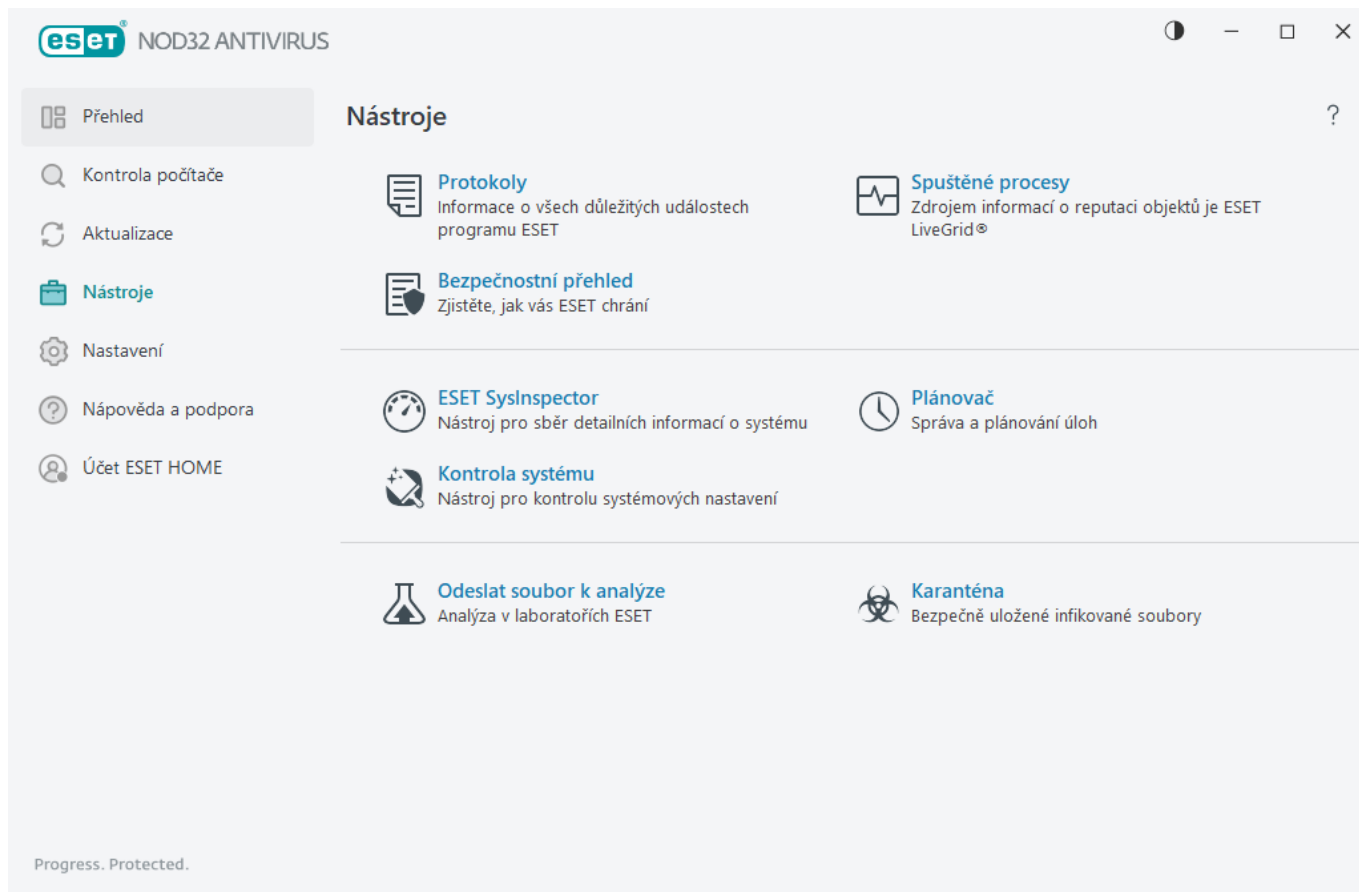
[Kontrola systému](#)



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

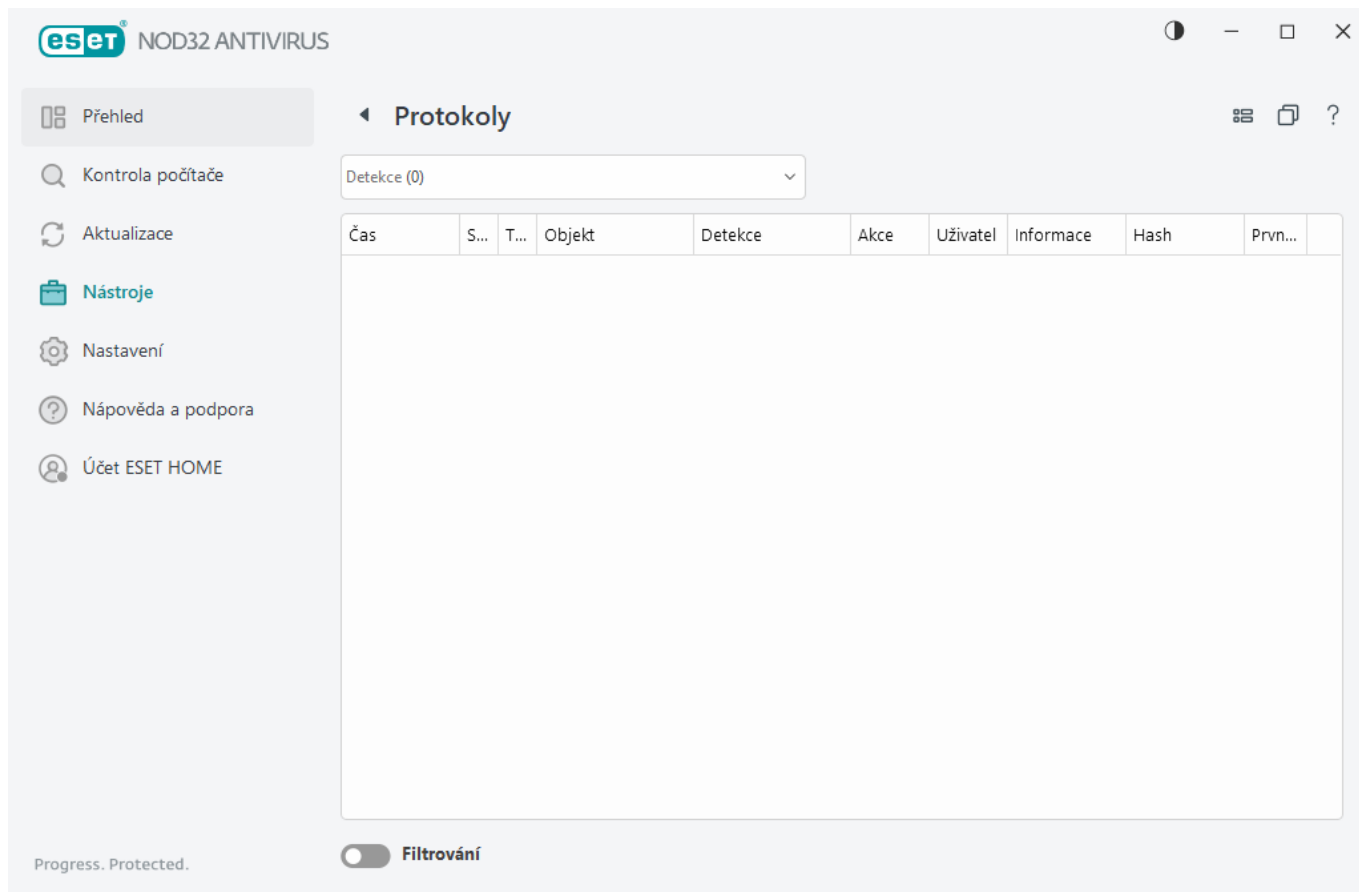


[Karanténa](#)



Protokoly

Do protokolů se zaznamenávají všechny důležité události programu, stejně tak v nich naleznete informace o detekovaných hrozbách. Záznamy v protokolech jsou důležitým zdrojem pro systémové analýzy, detekci hrozeb a řešení problémů. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové informace a protokoly si můžete prohlédnout i archivovat přímo v prostředí ESET NOD32 Antivirus.




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

- **Detekce** – protokol zachycených detekcí a infiltrací poskytuje detailní informace týkající se infiltrací zachycených moduly programu ESET NOD32 Antivirus. Informace v protokolu zahrnují čas detekce, skener, typ objektu, objekt, název detekce, uživatele přihlášeného v době detekce, informace o události, hash a první výskyt. Nevyléčené infiltrace jsou vždy označeny červeně na světle červeném pozadí. Vyléčené infiltrace jsou vždy označeny žlutě na bílém pozadí. Neléčené potenciálně nechtěné nebo zneužitelné aplikace jsou označeny žlutě na bílém pozadí.
- **Události** – protokol událostí obsahuje informace o všech událostech ESET NOD32 Antivirus a chybách, které se vyskytly. Protokol událostí obsahuje informace o událostech a chybách, ke kterým v programu došlo. Informace jsou určené systémovým administrátorům a uživatelům pro vyřešení problémů. Právě zde nejčastěji naleznete informace, které vám pomohou vyřešit problém vyskytující se v programu.
- **Kontrola počítače** – výsledky každé kontroly počítače se zobrazují v tomto okně. Každý řádek náleží samostatné kontrole. Dvojklikem na záznam si [zobrazíte detaily vybrané kontroly](#).
- **HIPS** – protokoly obsahují záznamy konkrétních [HIPS](#) 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, pokud chcete zobrazit seznam webových stránek, které byly zablokovány [Ochranou přístupu na web](#). Protokol obsahuje informace o čase, URL adrese, uživateli a aplikaci, která se chtěla na konkrétní 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 + Shift**). Pro výběr více záznamů podržte zároveň klávesu **CTRL** nebo **SHIFT** a proveďte výběr zájmových položek.

Po kliknutí na přepínač  **Filtrování** se zobrazí dialogové okno [Filtrování protokolu](#), pomocí kterého můžete definovat kritéria filtrování.

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

- **Zobrazit** – po kliknutí si všechny záznamy protokolu zobrazíte v novém okně.
- **Filtrovat záznamy stejného typu** – po aktivování tohoto filtru se zobrazí pouze záznamy stejného typu (diagnostické, varování,...).
- **Filtrovat...** – po kliknutí se otevře dialogové okno [Filtrování protokolu](#), ve kterém můžete definovat kritéria pro filtrování záznamů.
- **Zapnout filtr** – kliknutím aktivujete filtr. Pokud jste dosud žádný filtr nedefinovali, zobrazí se průvodce jeho vytvořením. Při opětovném kliknutí se automaticky aktivuje naposledy použitý filtr.
- **Zrušit filtr** – kliknutím vypnete filtrování.
- **Kopírovat/Kopírovat vše** – zkopíruje vybrané/všechny záznamy z daného okna.
- **Kopírovat buňku** – zkopíruje obsah buňky, na kterou jste v tabulce protokolů klikli pravým tlačítkem myši.
- **Odstranit/Odstranit vše** – odstraní vybrané nebo všechny zobrazené záznamy. Tato akce vyžaduje administrátorská oprávnění.
- **Exportovat.../Exportovat vše** – po kliknutí uložíte vybrané záznamy do souboru v XML formátu.
- **Hledat.../Hledat další.../Hledat předchozí...** – po kliknutí můžete definovat kritéria pro konkrétní záznamy pomocí Filtrování protokolu.
- **Popis detekce** – po kliknutí budete přesměrováni do ESET Encyklopedie hrozeb, kde naleznete informace o jednotlivých hrozbách.
- **Vytvořit výjimku** – kliknutím spustíte [průvodce vytvořením detekční výjimky](#) (tato možnost není dostupná pro objekty detekované jako malware).

Filtrování protokolů

Pro definování kritérií filtrování v hlavním okně programu na záložce Nástroje > **Protokoly** klikněte na tlačítko  **Filtrování**.

Díky funkci filtrování protokolů se snadněji zorientujete v zobrazených záznamech, a to zejména v situaci, kdy je záznamů více. Takový zúžený počet záznamů oceníte, pokud hledáte konkrétní typ události, stav nebo určité časové období. Záznamy protokolu lze filtrovat pomocí výběru určitých hodnot ve vyhledávání. Ve výsledcích se

následně zobrazí hodnoty, které jsou pro nastavená kritéria relevantní.

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

Hledat text

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

Hledat ve sloupcích

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

Typy záznamů

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

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informační** – jedná se o informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíše kritické chyby, chybová a varovná hlášení.
- **Chyby** – kromě kritických varování se zaznamenají chyby typu "Chyba při stahování souboru aktualizace".
- **Kritické chyby** – zobrazí se pouze kritické chyby (chyba při startu antivirové ochrany)

Časové období

Definujte časové období, za které chcete zobrazit výsledky:

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

Hledat pouze celá slova

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

Rozlišovat velká a malá písmena

Tuto možnost zapněte, pokud chcete při vyhledávání rozlišovat velikost písmen. Po dokončení konfigurace filtru pro vyhledávání v protokolu klikněte na tlačítko **OK**, případně **Najít** pro zahájení vyhledávání. Protokol se prohledává ze shora dolů a začíná se na aktuální pozici (zvýrazněném záznamu). Vyhledávání se zastaví na prvním vyhovujícím záznamu. Pro zobrazení dalšího výsledku vyhledávání stiskněte klávesu **F3**, případně v kontextovém menu vyberte možnost **Najít** a upravte parametry vyhledávání.

Spuštěné procesy

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

eSet NOD32 ANTIVIRUS

Spuštěné procesy

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

Úroveň rizi...	Proces	PID	Počet uživatelů	První výskyt	Název aplikace
Safe	smss.exe	372	1	před 2 lety	Microsoft® Windows® Op...
Safe	csrss.exe	476	1	před 2 lety	Microsoft® Windows® Op...
Safe	wininit.exe	556	1	před 6 měsíci	Microsoft® Windows® Op...
Safe	winlogon.exe	656	1	před měsícem	Microsoft® Windows® Op...
Safe	services.exe	696	1	před 3 měsíci	Microsoft® Windows® Op...
Safe	lsass.exe	708	1	před 6 měsíci	Microsoft® Windows® Op...
Safe	svchost.exe	832	1	před rokem	Microsoft® Windows® Op...
Safe	fontdrvhost.exe	852	1	před 3 měsíci	Microsoft® Windows® Op...
Safe	dwm.exe	484	1	před 2 lety	Microsoft® Windows® Op...
Safe	efwd.exe	1676	1	před 3 dny	ESET Security
Suspicious	vboxservice.exe	1724	1	před 2 lety	Oracle VM VirtualBox Guest...
Safe	wudfhost.exe	1740	1	před 6 měsíci	Microsoft® Windows® Op...
Safe	spoolsv.exe	2888	1	před 3 měsíci	Microsoft® Windows® Op...
Suspicious	akvcamassistant.exe	2152	1	před 2 lety	AkVCamAssistant
Safe	sihost.exe	3780	1	před 2 lety	Microsoft® Windows® Op...
Safe	taskhostw.exe	1496	1	před 6 měsíci	Microsoft® Windows® Op...
Safe	googleupdate.exe	2440	1	před 2 lety	Google Update
Safe	ctfmon.exe	1780	1	před 2 lety	Microsoft® Windows® Op...
Safe	explorer.exe	4044	1	před měsícem	Microsoft® Windows® Op...
Safe	startmenuexperiencehost.exe	5456	1	před rokem	

Progress. Protected.

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).

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

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

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

Počet uživatelů – počet uživatelů, kteří používají danou aplikaci. Tyto informace se shromažďují pomocí technologie ESET LiveGrid®.

První výskyt – doba, kdy byl proces poprvé objeven pomocí technologie ESET LiveGrid®.

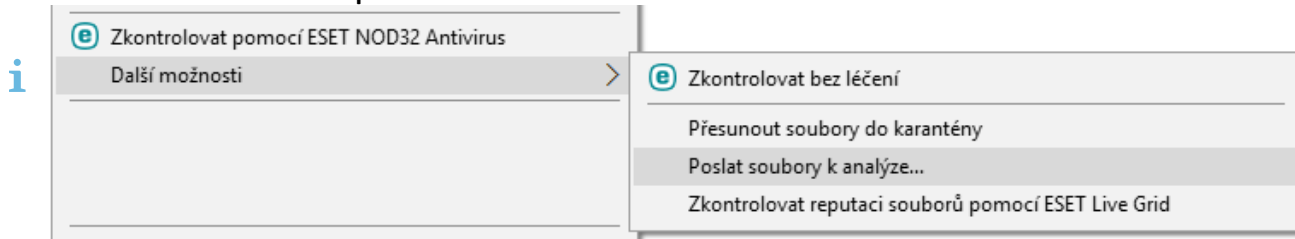
i V případě, že je aplikace označená jako Neznámá (oranžová), nemusí to nutně znamenat, že obsahuje škodlivý kód. Obvykle se jedná o novou aplikaci. Pokud si nejste jisti, zda je tomu opravdu tak, můžete [soubor odeslat k analýze](#) do virové laboratoře společnosti ESET. Pokud se potvrdí, že jde o aplikaci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

Název aplikace – název aplikace nebo procesu.

Po kliknutí na konkrétní aplikaci si zobrazíte následující informace:

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

Úroveň rizika můžete zjistit také pro soubory, které se nechovají jako spuštěné programy/procesy. Na soubor, který chcete zkontrolovat, klikněte pravým tlačítkem myši a ze zobrazeného kontextového menu vyberte **Další možnosti > Zkontrolovat reputaci souboru**.



Bezpečnostní přehled


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

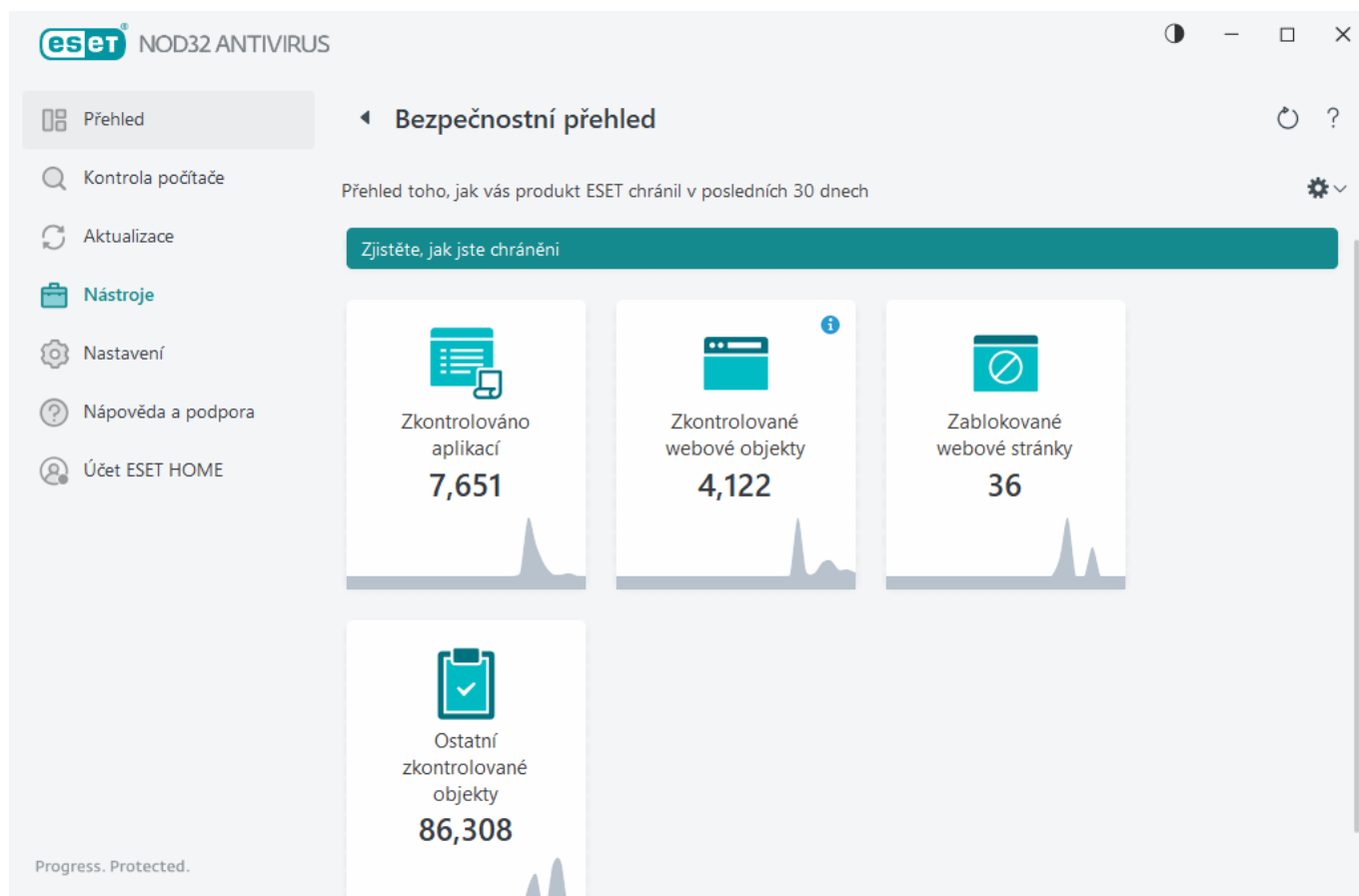
- **Zablokováno webových stránek** – zobrazuje počet zablokovaných webových stránek (zablokováno na základě PUA, výskytu phishingu, hacknutého routeru, IP adresy nebo certifikátu).
- **Detekované infikované e-mailové objekty** – zobrazuje počet detekovaných infikovaných poštovních [objektů](#).
- **Detekované PUA** – zobrazuje počet detekovaných [potenciálně nechtěných aplikací](#) (PUA).

- **Zkontrolováno dokumentů** – zobrazuje počet zkontrolovaných dokumentů.
- **Zkontrolováno aplikací** – zobrazuje počet zkontrolovaných spustitelných objektů.
- **Ostatní zkontrolované objekty** – zobrazuje počet dalších zkontrolovaných objektů.
- **Zkontrolované objekty webových stránek** – zobrazuje počet zkontrolovaných objektů webových stránek.
- **Zkontrolované poštovní objekty** – zobrazuje počet zkontrolovaných poštovních objektů.

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

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

Kliknutím na ozubené kolečko  v pravém horním rohu můžete **zapnout/vypnout upozornění na bezpečnostní přehled**, případně si zobrazit data za posledních 30 dní, resp. od aktivace produktu. Pokud jste produkt ESET 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 toto nemáte v **Rozšířených nastaveních** (dostupných po stisknutí klávesy F5) definováno jinak v části [Oznámení](#) > **Interaktivní upozornění** > **Potvrzovací zprávy** > **Změnit**.

ESET SysInspector

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

V okně ESET SysInspector se nachází informace o vytvořených protokolech:

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

Dostupné jsou následující akce:

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

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

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

Plánovač

Plánovač spravuje a spouští naplánované úlohy s předem nakonfigurovaným nastavením.

Plánovač je dostupný v [hlavním okně programu](#) ESET NOD32 Antivirus na záložce **Nástroje > Plánovač**. Plánovač obsahuje seznam všech naplánovaných úloh a jejich nastavení jako je datum a čas provedení, použitý profil kontroly atp.

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

Standardně **Plánovač** zobrazuje následující naplánované úlohy:

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

Pro úpravu existujících (a to jak předdefinovaných, tak vlastních) úloh použijte kontextové menu, ve kterém vyberte možnost **Změnit...**, případně po vybrání požadované úlohy klikněte na tlačítko **Změnit**.

eset NOD32 ANTIVIRUS

Plánovač

Úloha	Podmínka spuštění	Příští spuštění	Naposledy spuštěna
<input checked="" type="checkbox"/> Údržba protokolů	Úloha bude proveden...	7/4/2023 2:00:00 AM	7/3/2023 2:00:44 AM
<input checked="" type="checkbox"/> Aktualizace	Úloha bude proveden...	7/3/2023 4:22:01 AM	7/3/2023 3:22:01 AM
<input checked="" type="checkbox"/> Aktualizace	Vytáčené připojení k in...	Při události	
<input type="checkbox"/> Aktualizace	Přihlášení uživatele (p...	Při události	
<input checked="" type="checkbox"/> Kontrola souborů spouštěných při startu	Přihlášení uživatele Úl...	Při události	7/3/2023 4:14:00 AM
<input checked="" type="checkbox"/> Kontrola souborů spouštěných při startu	Úspěšná aktualizace m...	Při události	7/3/2023 4:16:36 AM

Progress. Protected.

Přidat **Změnit** **Vymazat** **Standardní**

Přidání nové úlohy

1. Klikněte na tlačítko **Přidat** ve spodní části okna.
2. Zadejte název úlohy.

3. Vyberte požadovaný typ úlohy:

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

4. Pro aktivování úlohy přepněte přepínač do polohy **Zapnuto** (to můžete udělat kdykoli později přímo v seznamu naplánovaných úloh) a po kliknutí na tlačítko **Další** vyberte interval opakování:

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

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

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

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

Možnosti naplánované kontroly

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

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

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

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

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



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

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

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

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

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

Informace o naplánované úloze

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

Detaily úlohy

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

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

Provedení úlohy

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

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

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

Provedení úlohy – Jednou

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

Provedení úlohy – Denně

Úloha bude provedena každý den ve stanovený čas.

Provedení úlohy – Týdně

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

Provedení úlohy – Při události

Úloha bude provedena při jedné z následujících událostí:

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

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

Neprovedení úlohy

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

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

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

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

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

Detaily úlohy – Aktualizace

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

Detaily úlohy – Spuštění aplikace

Pomocí tohoto typu úlohy si můžete naplánovat spuštění externí aplikace.

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

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

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

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

Kontrola systému

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

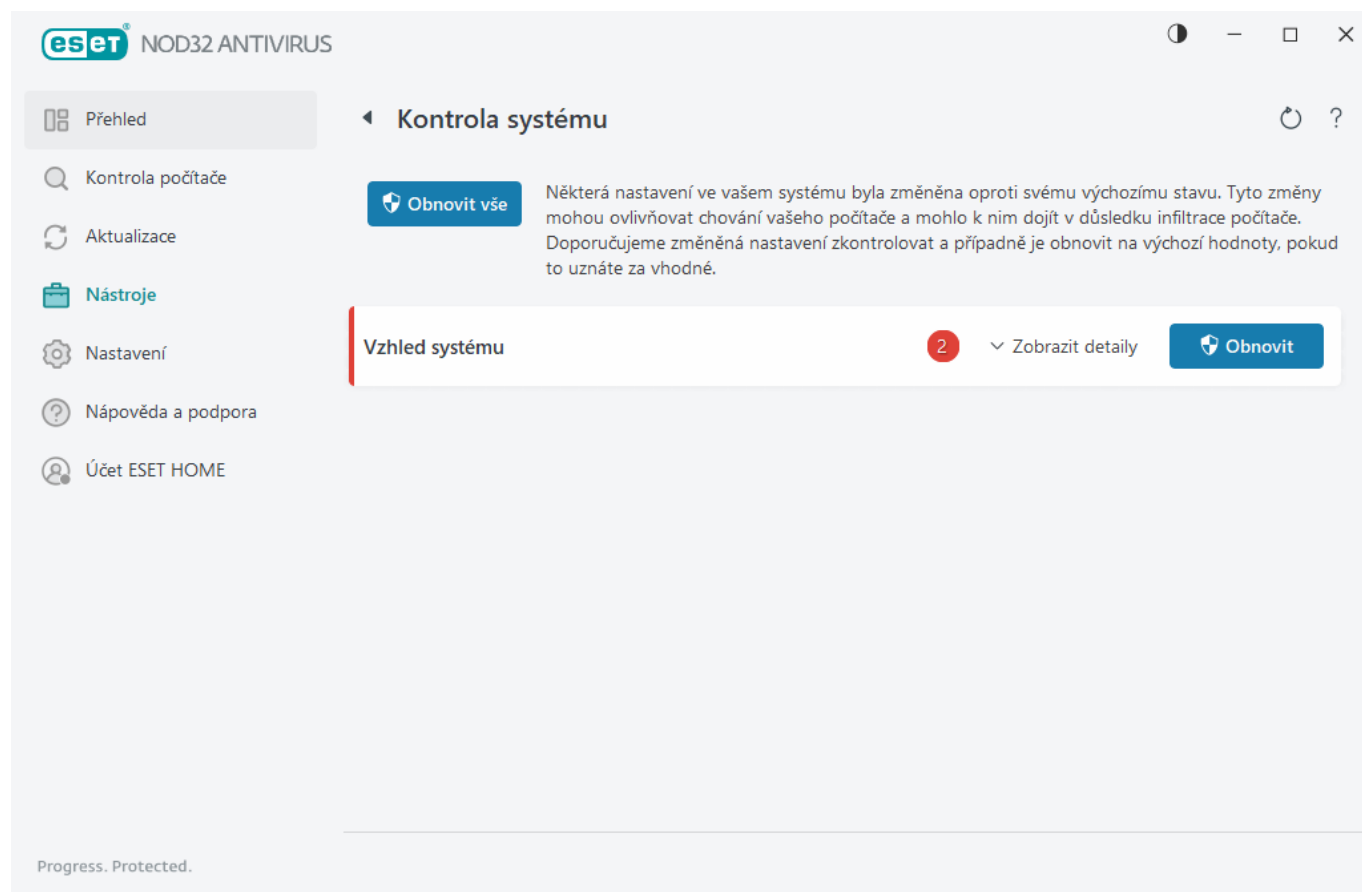
Použitím tohoto nástroje obnovíte klíčová nastavení systému na výchozí hodnoty:

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

Kontrola systému se může spustit:

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

Zkontrolujte změny a případně obnovte nastavení.



i Tento nástroj může použít pouze uživatel s administrátorským oprávněním.

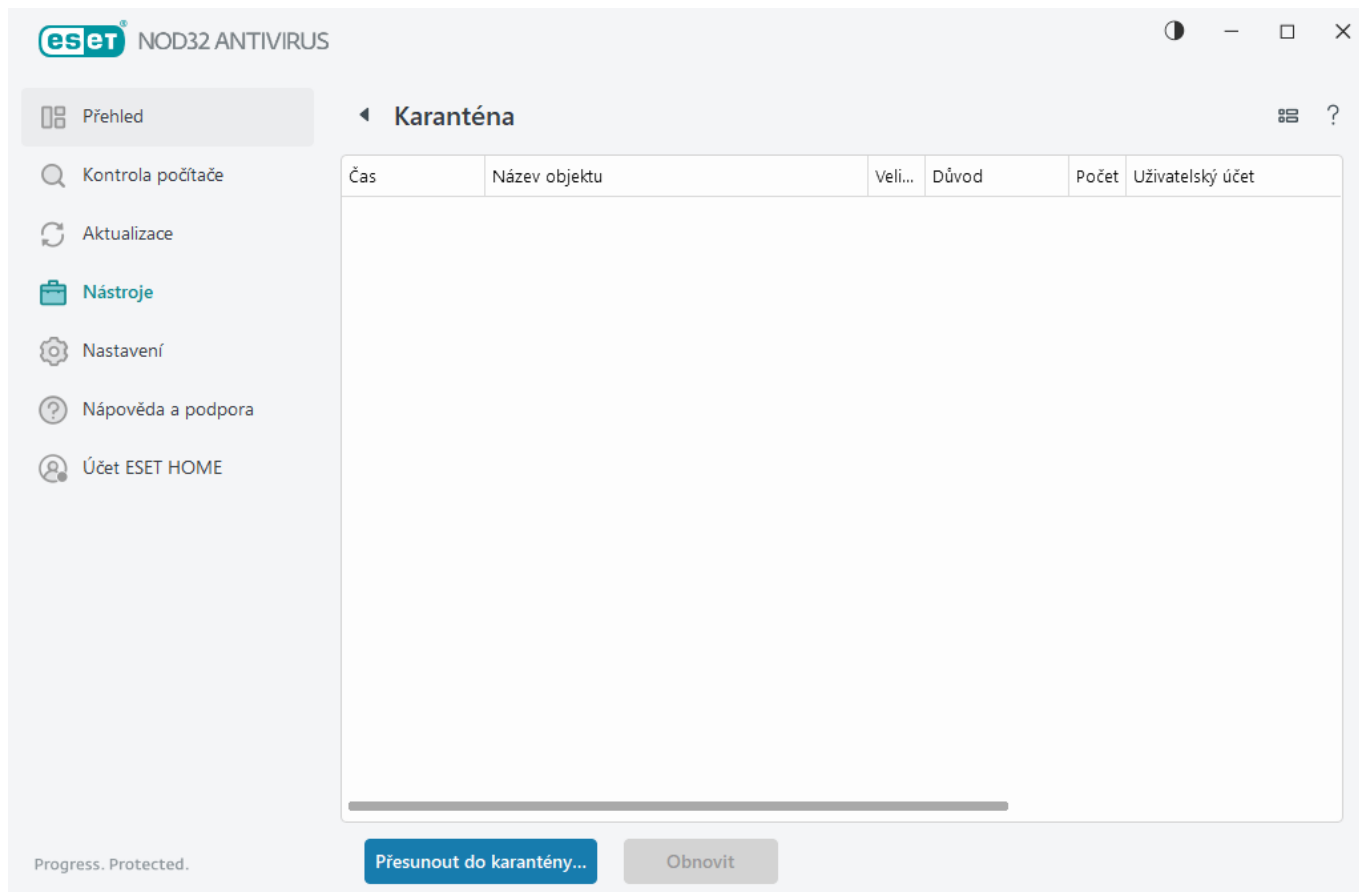
Karanténa

Hlavní funkcí karantény je bezpečně uschovat nahlášené objekty (jako je malware, infikované soubory nebo potenciálně nechtěné aplikace).

Karanténa je dostupná v [hlavním okně programu](#) ESET NOD32 Antivirus na záložce **Nástroje > Karanténa**.

Soubory uložené v karanténě si můžete prohlédnout v přehledné tabulce včetně informací o:

- datu a čase přidání souboru do karantény,
- cesty k původnímu umístění souboru,
- jeho velikosti v bajtech,
- důvodu proč byl přidán do karantény (např. objekt přidán uživatelem),
- a počtu detekcí. (např. duplikovanou detekcí stejného souboru, nebo pokud se jedná o archiv obsahující více infiltrací).



Vložení objektu do karantény

ESET NOD32 Antivirus automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nezrušili v [okně s upozorněním](#)).

Soubory mohou být umístěny do karantény, pokud:

- a.nemohou být léčeny,
- b.pokud není bezpečné a doporučené jejich odstranění,
- c.pokud byly ESET NOD32 Antivirus falešně detekovány,
- d.nebo pokud soubor vykazuje podezřelou aktivitu, ale není detekován [Ochranami](#).

Pro uložení souboru do karantény máte několik možností:

- a.Přetáhněte ji způsobem Drag and drop (nakliknout na soubor levým tlačítkem myši, podržet levé tlačítko, přesunout do zvýrazněné oblasti a tlačítko pustit). Po přesunutí souboru se okno aplikace přesune do popředí.
- b.Klikněte na soubor pravým tlačítkem myši a v zobrazeném kontextovém menu vyberte možnost **Rozšířená nastavení > Přesunout soubor do karantény**.
- c.V hlavním menu programu přejděte do sekce **Karanténa** a klikněte na tlačítko **Přesunout do karantény...**
- d.Využít můžete rovněž kontextové menu – klikněte pravým tlačítkem v okně **Karantény** a vyberte možnost **Přesunout do karantény...**

Obnovení z karantény

Soubory v karanténě lze vrátit do původního umístění:

- K tomuto účelu použijte funkci **Obnovit**, která je k dispozici v místní nabídce kliknutím pravým tlačítkem myši na daný soubor v karanténě.
- Pokud je soubor označen jako [potenciálně nechtěná aplikace](#), je povolena možnost **Obnovit a vyloučit z kontroly**. Viz také kapitolu [Výjimky](#).
- V kontextovém menu se dále nachází možnost **Obnovit do...**, pomocí které můžete obnovit soubor na jiné místo než to, ze kterého byl původně smazán.
- Funkce obnovení není dostupná například pro soubory umístěné ve sdílené síťové složce pro čtení.

Odstranění z karantény

Klikněte pravým tlačítkem na objekt v karanténě a vyberte možnost **Odstranit z karantény**, případně vyberte objekt a stiskněte na klávesnici klávesu **Delete**. Rovněž můžete vybrat více položek a smazat je najednou. Smazané objekty budou trvale odstraněny z karantény a vašeho počítače.

Odeslání souboru z karantény k analýze

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

Popis detekce...

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

Názorné ukázky

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

- [Obnovení objektu z karantény v ESET NOD32 Antivirus](#)
- [Odstranění objektu z karantény v ESET NOD32 Antivirus](#)
- [Program ESET mě upozornil na detekci. Co mám dělat?](#)

Soubor se nepodařilo přesunout do karantény

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

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

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

přesunout do karantény.

Odeslání vzorku k analýze

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

Před odesláním vzorku do společnosti ESET

Vzorky zasílejte pouze v případě, kdy splňuje jedno z následujících kritérií:



- Soubor není produktem ESET detekován
- Vzorek je detekován nesprávně jako hrozba
- Mějte na paměti, že osobní soubory nepřijímáme jako vzorky (neprovádíme jejich kontrolu za uživatele)
- Nezapomeňte vyplnit předmět a přiložte maximální možné množství informací o daném vzorku (jak jste se k němu dostali, odkud jste obdrželi odkaz, screenshot apod.)

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

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

V zobrazeném dialogovém **okně pro odeslání vzorku** vyberte z rozbalovacího menu **Důvod odeslání vzorku** možnost, která nejlépe vystihuje danou situaci:

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

Soubor/Stránka – cesta k souboru nebo URL adresa.

Kontaktní e-mail – na tento e-mail vás budou pracovníci virové laboratoře ESET kontaktovat, pokud budou potřebovat více informací. Zadání e-mailu je nepovinné. V takovém případě vyberte možnost **Odeslat anonymně**.

Pravděpodobně neobdržíte žádnou zpětnou vazbu



Na zadanou e-mailovou adresu vás budou pracovníci virové laboratoře ESET kontaktovat pouze v případě, kdy budou potřebovat více informací. Denně do společnosti ESET chodí několik desítek tisíc souborů, a není možné na každý e-mail reagovat.

Pokud se ukáže, že se jedná o nebezpečnou aplikaci nebo webovou stránku, její detekce bude přidána v některé z nejbližších aktualizací.

Podezřelý soubor

Pozorované projevy a příznaky infekce – uveďte prosím, co nejdetailnější popis chování souboru v systému pro přesnější analýzu souboru.

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

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

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

Podezřelá stránka

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

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

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

Falešně detekovaný soubor

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

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

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

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

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

i První tři parametry jsou povinné z důvodu lepší identifikace legitimní aplikace. Poskytnutím doplňujících informací pomůžete významnou měrou při identifikaci a zpracování vzorků.

Falešně detekovaná stránka

Při odesílání stránky, která je falešně detekována jako infikovaná, scam nebo phishing, ale ve skutečnosti není, vyžadujeme zadání dalších informací. Falešný poplach (False positive, zkráceně FP) může nastat, když struktury souboru mají stejné charakteristiky jako vzorky obsažené v detekčním jádru. Poskytnutím těchto informací pomůžete vylepšit antivirové a anti-phishingové jádro.

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

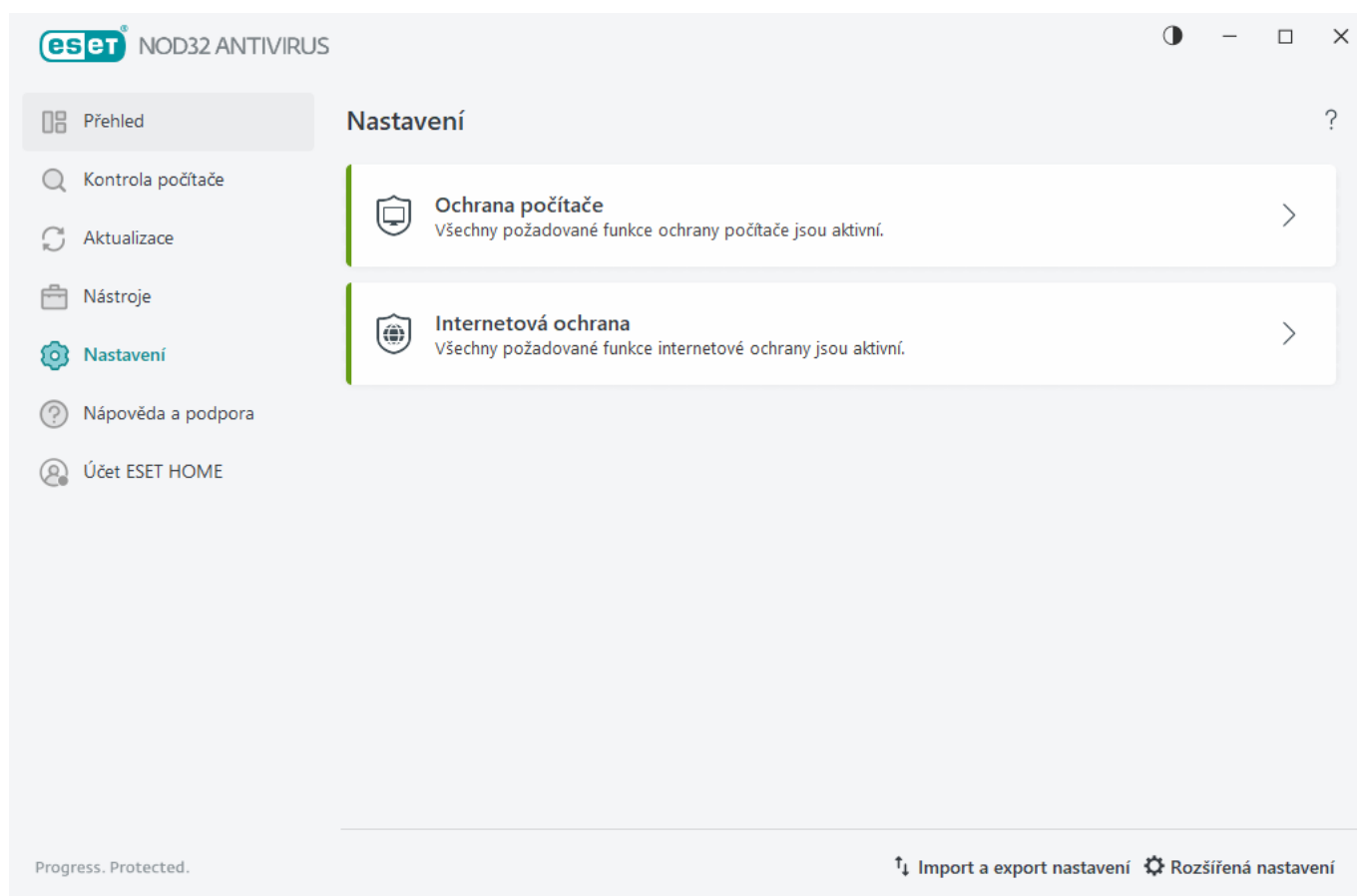
Ostatní

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

Důvod odesílání souboru – uveďte prosím důvod odeslání souboru a co nejpřesnější popis souboru.

Nastavení

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



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

 [Ochrana počítače](#)



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

Ochrana počítače

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

- [Rezidentní ochrana souborového systému](#) – všechny soubory jsou kontrolovány v momentu, kdy je vytvoříte, otevřete nebo spustíte.
- [Správa zařízení](#) – pomocí této součásti můžete uživatelům nastavovat, kontrolovat nebo blokovat přístupy k výměnným médiím (CD/DVD/USB aj.).
- [Host Intrusion Prevention System \(HIPS\)](#) – systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně na základě pravidel.
- [Herní režim](#) – po aktivaci Herního režimu vás ESET nebude obtěžovat bublinovými upozorněními a sníží zátěž na CPU. Obdržíte varovnou zprávu o potenciální bezpečnostní hrozbě a hlavní okno se zbarví do oranžova.

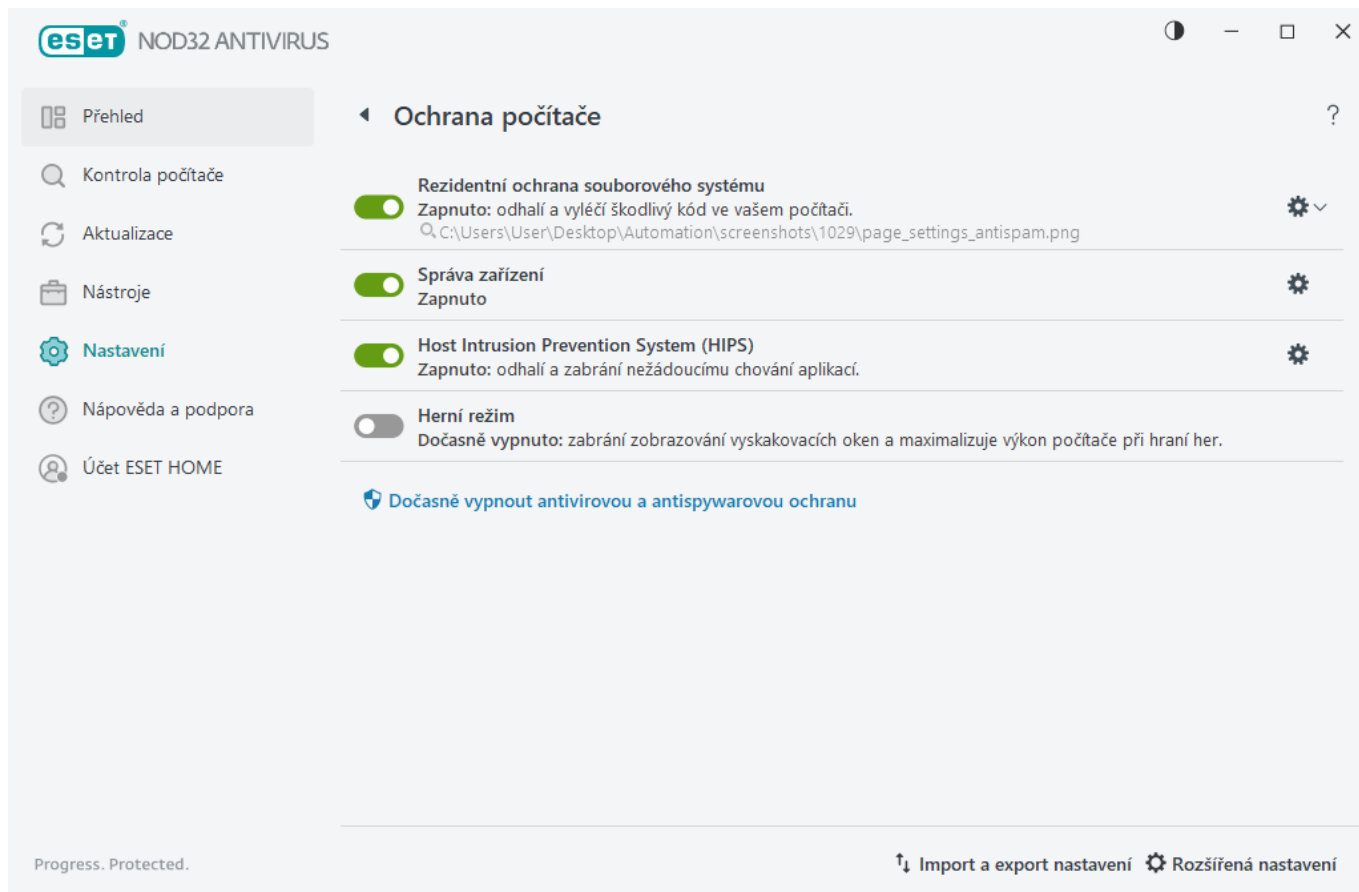
Chcete-li pozastavit nebo vypnout některé moduly ochrany, klikněte na ikonu

Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.

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

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

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



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

Nalezena infiltrace

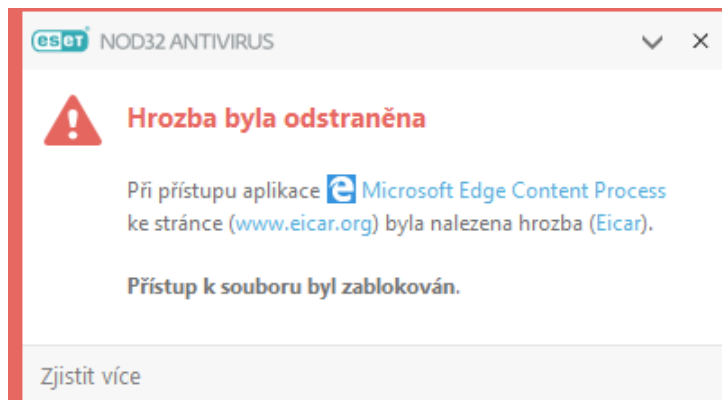
Infiltrace se mohou do počítače dostat z různých zdrojů: z [webových stránek](#), ze sdílených složek, prostřednictvím e-mailu, z [výměnných médií](#) (USB, externí disků, CD a DVD jiných).

Standardní chování

ESET NOD32 Antivirus dokáže zachytit infiltrace pomocí:

- [Rezidentní ochrany souborového systému](#),
- [Ochrana přístupu na web](#)
- [Ochrany poštovních klientů](#),
- [Volitelné kontroly počítače](#).

Každý z těchto modulů používá standardní úroveň léčení. Program se pokusí soubor vyléčit a přesunout do [Karantény](#), nebo přeruší spojení. Oznámení se zobrazují v pravé dolní části obrazovky. Pro více informací o detekovaných/vyléčených objektech přejděte do kapitoly [Protokoly](#). Pro více informací o jednotlivých úrovních léčení a jejich chování si prosím přečtěte kapitolu [Úrovně léčení](#).



Kontrola počítače na výskyt infikovaných souborů

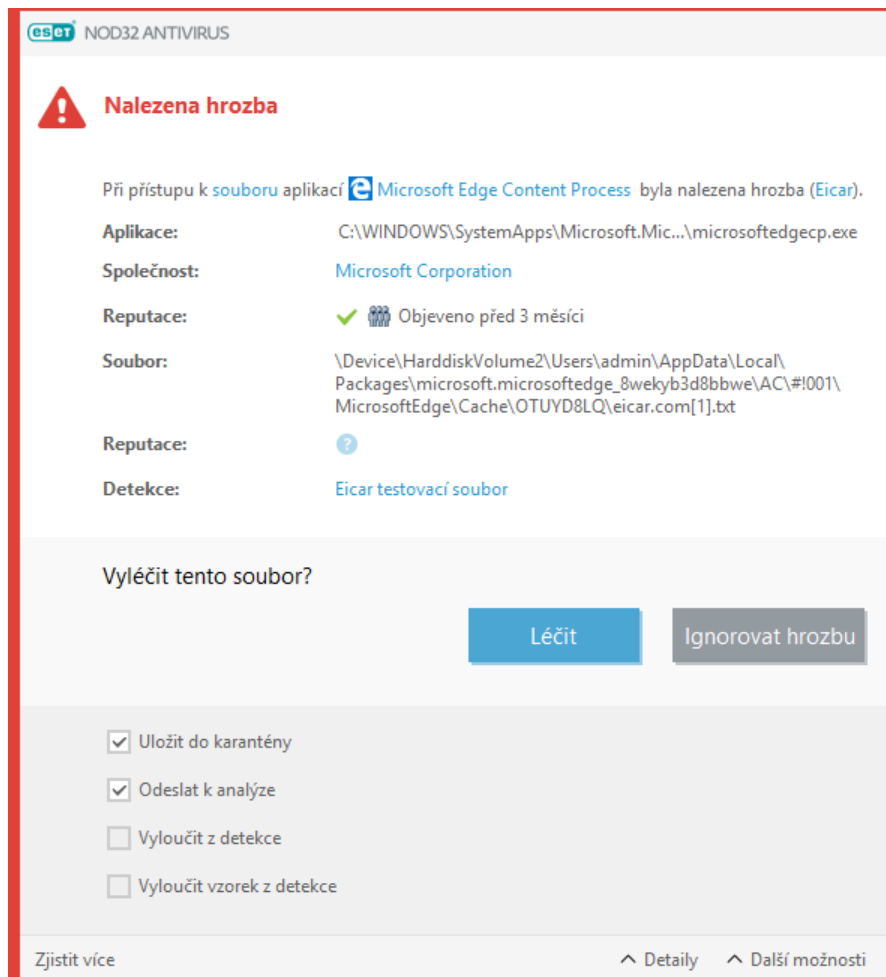
Pokud se váš počítač chová podezřele nebo máte podezření, že je infikován (zamrzá, je pomalý atp.), postupujte podle následujících kroků:

1. Otevřete ESET NOD32 Antivirus a přejděte na záložku **Kontrola počítače**.
2. Klikněte na **Provést kontrolu počítače** (bližší informace naleznete v kapitole [Kontrola počítače](#)).
3. Po dokončení kontroly, zkontrolujte zobrazený protokol.

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

Léčení a mazání

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



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

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

Obnovení z karantény

Karanténa je dostupná v [hlavním okně programu](#) ESET NOD32 Antivirus na záložce **Nástroje > Karanténa**.

Soubory v karanténě lze vrátit do původního umístění:

- K tomuto účelu použijte funkci **Obnovit**, která je k dispozici v místní nabídce kliknutím pravým tlačítkem myši na daný soubor v karanténě.
- Pokud je soubor označen jako [potenciálně nechtěná aplikace](#), je povolena možnost **Obnovit a vyloučit z kontroly**. Viz také kapitolu [Výjimky](#).
- V kontextovém menu se dále nachází možnost **Obnovit do...**, pomocí které můžete obnovit soubor na jiné místo než to, ze kterého byl původně smazán.
- Funkce obnovení není dostupná například pro soubory umístěné ve sdílené síťové složce pro čtení.

Více hrozeb


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


Mazání souborů v archivech

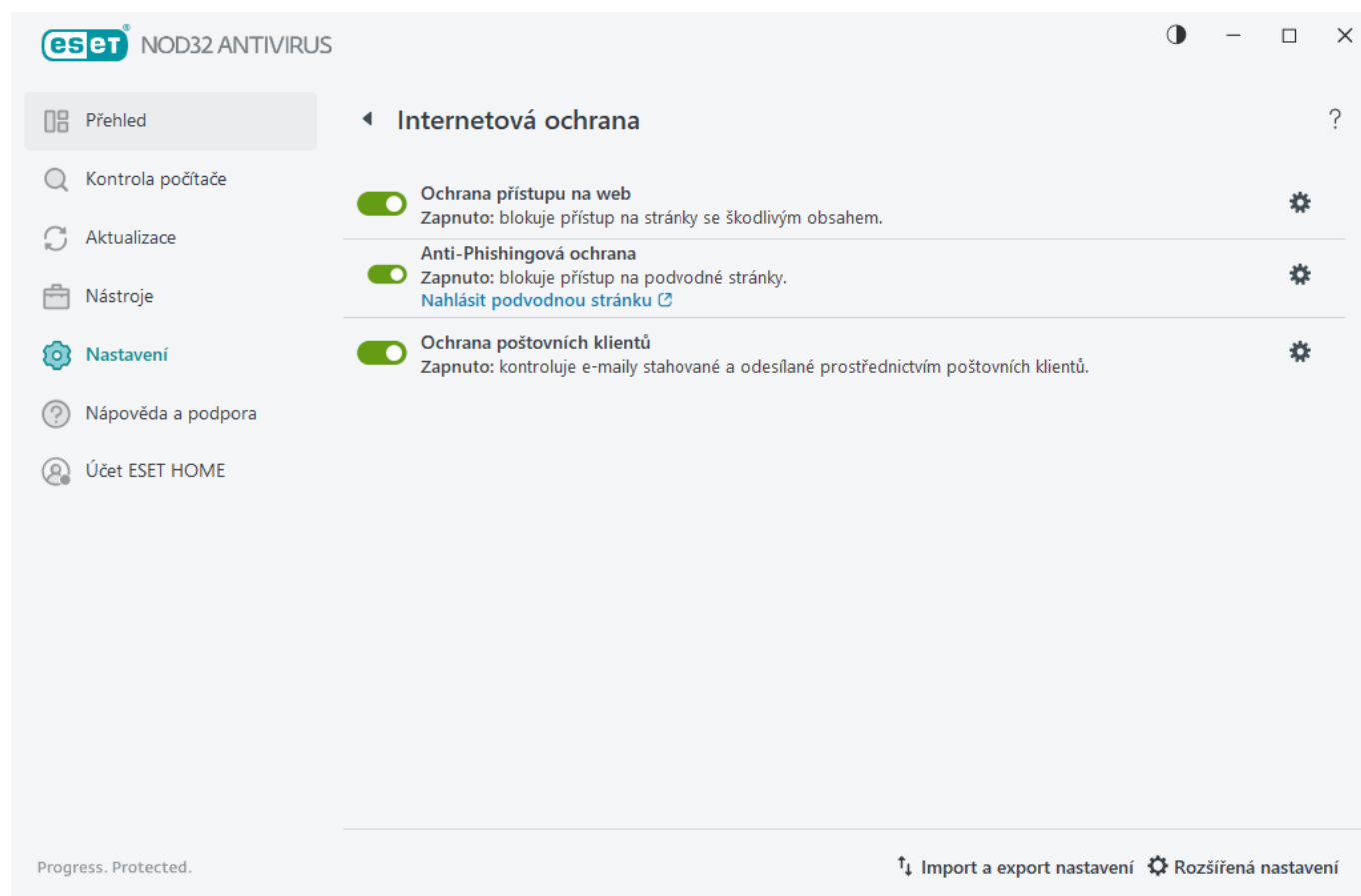
Pokud je zjištěna infiltrace uvnitř archivu, bude archiv při standardní úrovni léčení odstraněn pouze v případě, že obsahuje pouze infikovaný soubor. Archiv nebude vymazán, pokud kromě infiltrace obsahuje také nezávadné soubory. Opatrnost je potřeba dodržovat při nastavení přísné úrovně léčení, kdy v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

Internetová ochrana

Internetové připojení se stalo u počítačů standardem. Bohužel i pro šíření škodlivého kódu. Otevřete [hlavní okno programu](#) > **Nastavení** > **Internetová ochrana** a nakonfigurujte funkce na ESET NOD32 Antivirus, které zvyšují internetovou ochranu.

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

 Vypnutí modulů ochrany snižuje úroveň zabezpečení počítače.



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

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

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

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



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

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

[Ochrana poštovních klientů](#) zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3(S) a IMAP(S). Pomocí zásuvných modulů do/z poštovních klientů zajišťuje ESET NOD32 Antivirus kontrolu veškeré komunikace.

Anti-Phishingová ochrana

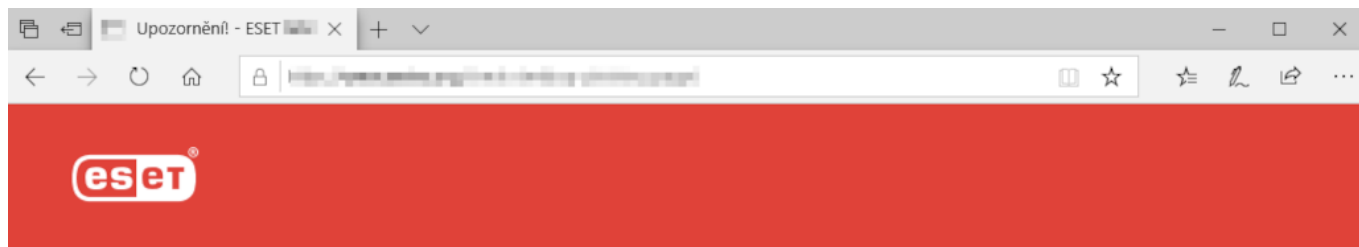
Termín phishing definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Cílem útočníků využívajících phishing je získání citlivých dat, jako jsou čísla bankovních účtů, PIN kódy a další. Více informací naleznete v [glosáři](#). ESET NOD32 Antivirus obsahuje anti-phishingovou ochranu, která blokuje internetové stránky s tímto obsahem.

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

Podrobnější informace o fungování Anti-Phishingové ochrany ESET NOD32 Antivirus naleznete v [ESET Databázi znalostí](#).

Přístup na stránky s phishingovým obsahem

Při přístupu na stránku se škodlivým obsahem se v internetovém prohlížeči zobrazí níže uvedené upozornění. Pokud přesto chcete stránku otevřít, klikněte na tlačítko **Ignorovat hrozbu** (nedoporučujeme).



Potenciální pokus o phishing

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

Chcete se vrátit na předchozí stránku?

Přejít zpět

Ignorovat hrozbu

[Nahlásit nesprávně blokovanou stránku](#)

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



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

Nahlásit podvodnou stránku

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

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

Import a export nastavení

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

Názorné ukázky

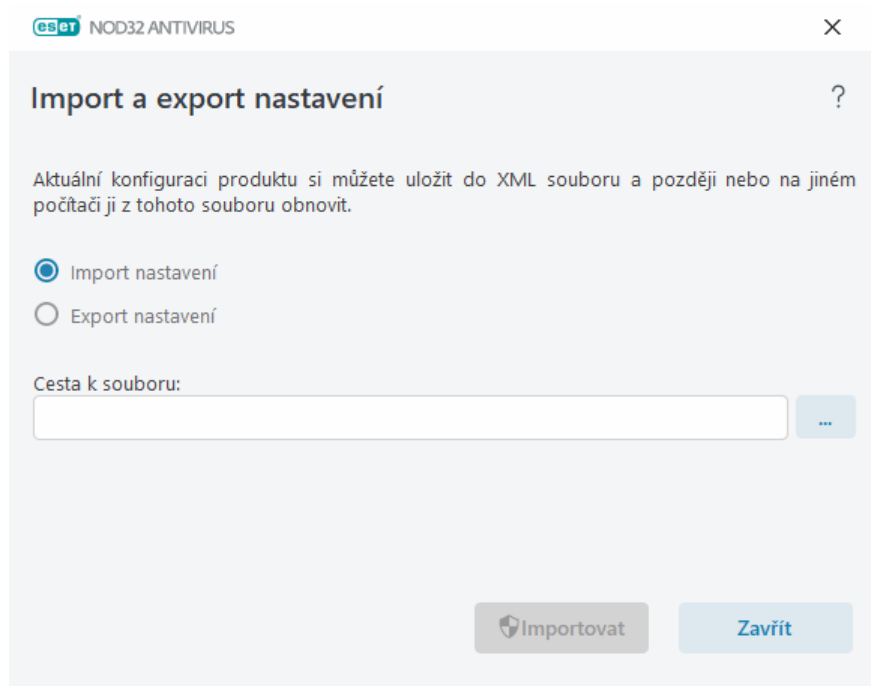
i Pokud se chcete podívat na názornou ukázkou, klikněte na návod ESET Databáze znalostí [Jak importovat nebo exportovat nastavení bezpečnostního produktu ESET pomocí konfiguračního souboru .xml](#) (článek nemusí být dostupný ve všech jazycích).

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

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

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

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



Nápověda a podpora

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

Licence

- [Průvodce řešením problémů s licencí](#) – po kliknutí si zobrazíte nejčastější problémy týkající se aktivace nebo změny licence společně s jejich řešením.
- [Změnit licenci](#) – po kliknutí se zobrazí dialogové okno, pomocí kterého můžete produkt aktivovat. Pokud je

zařízení [připojené k ESET HOME](#), automaticky se zobrazí seznam licencí, které jsou v daném ESET HOME účtu dostupné, případně můžete produkt aktivovat jinou licencí.

Nainstalovaný produkt

- [Co je nového](#) – po kliknutí na odkaz se otevře okno s informacemi o nových a vylepšených funkcích.
- [O programu ESET NOD32 Antivirus](#) – kliknutím si zobrazíte souhrnné informace o vámi nainstalovaném programu ESET NOD32 Antivirus.
- [Průvodce řešením problémů s produktem](#) – kliknutím na tento odkaz naleznete řešení nejčastějších problémů.
- **Změnit produkt** – kliknutím na toto tlačítko si můžete nainstalovat [jiný produkt ESET NOD32 Antivirus](#), který vaše licence umožňuje.



Otevřít nápovědu – kliknutím na odkaz si zobrazíte nápovědu k programu ESET NOD32 Antivirus.



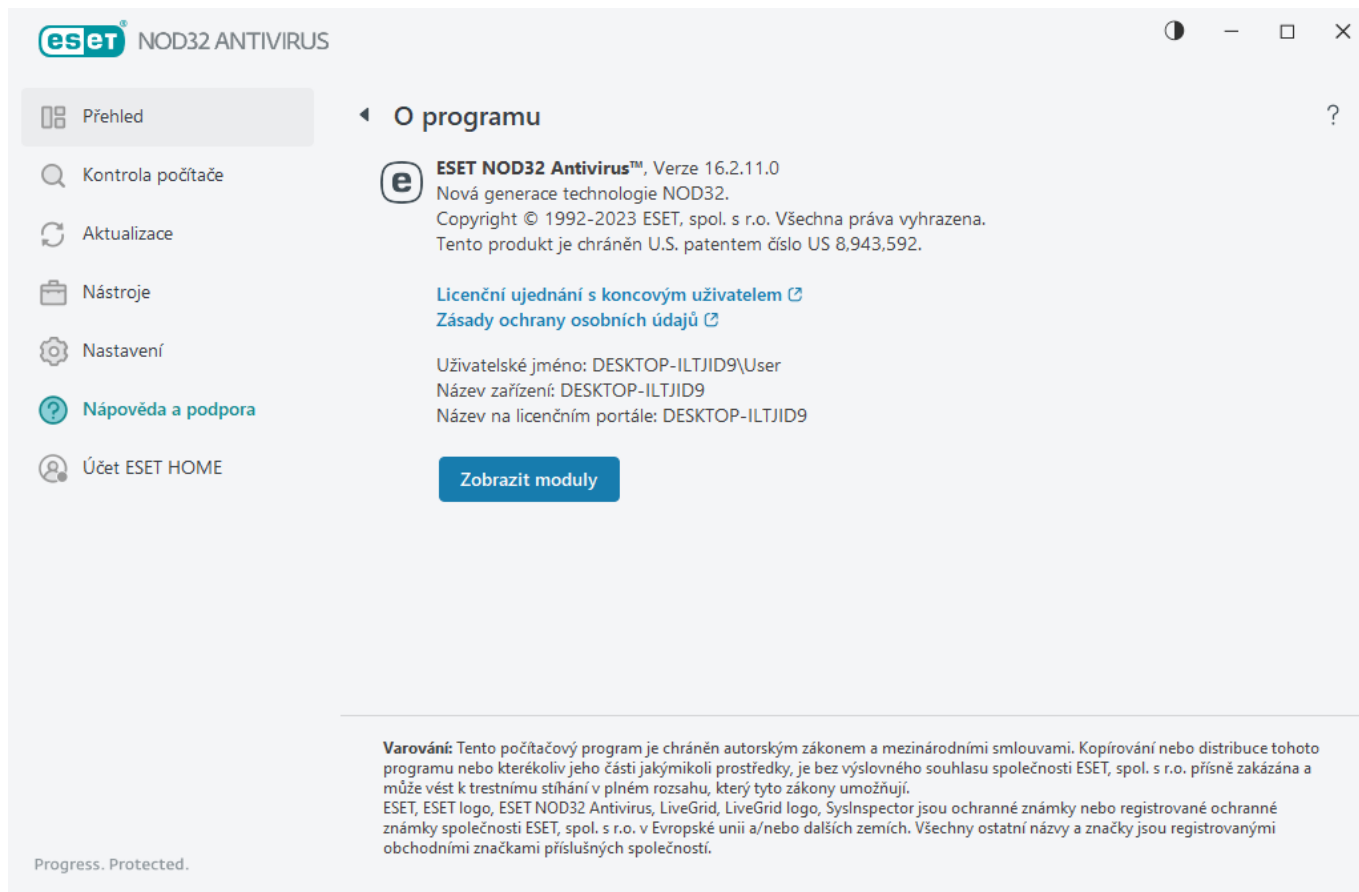
[Technická podpora](#)



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

O programu ESET NOD32 Antivirus

Toto okno zobrazuje informace o verzi ESET NOD32 Antivirus a o vašem počítači.



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

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

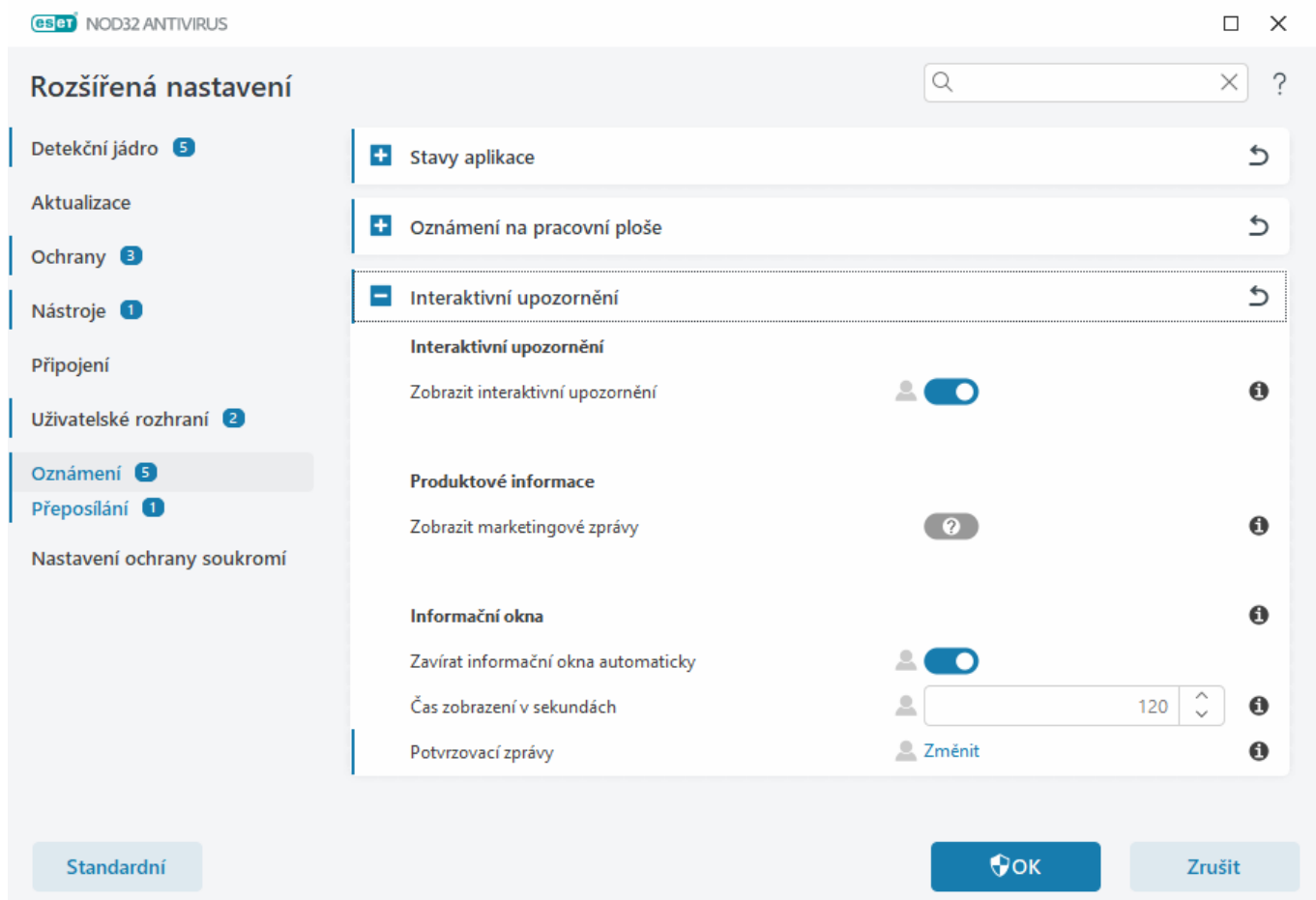
ESET Novinky

V této části ESET NOD32 Antivirus vás budeme informovat o novinkách a výhodných akcích produktů ESET.

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

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

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



Odeslat konfiguraci systému

Aby mohli specialisté technické podpory rychle a relevantně reagovat na dotazy zákazníků, vyžadují zaslání konfigurace produktu ESET NOD32 Antivirus, detailních informací o systému včetně spuštěných procesů a záznamů v registru – tedy protokolu z nástroje [ESET SysInspector](#). Společnost ESET použije tyto údaje pouze pro poskytnutí technické pomoci zákazníkovi.

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

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



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

Technická podpora

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

Kontaktovat Technickou podporu

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

Získání informací pro technickou podporu

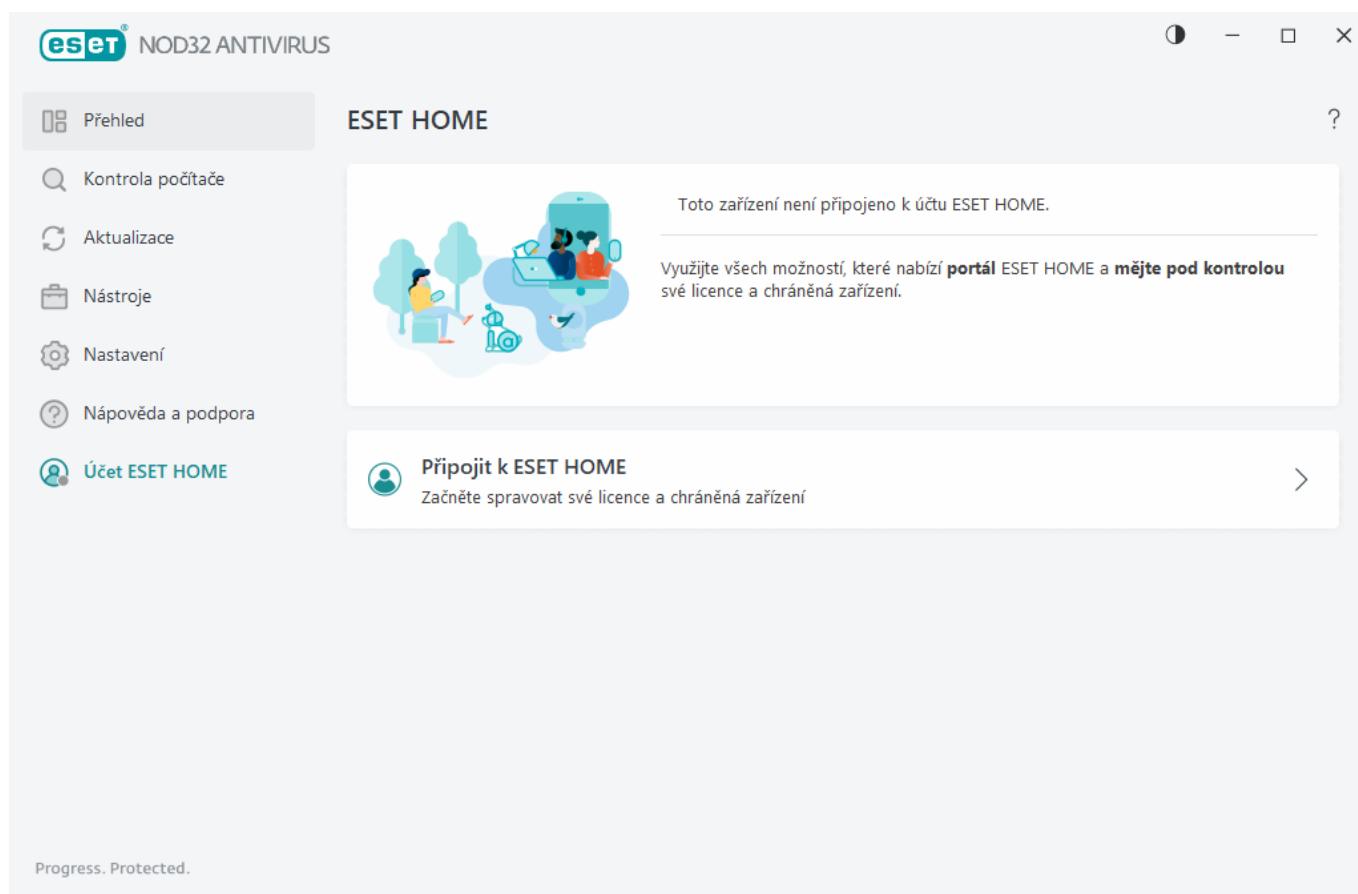
Základní informace pro technickou podporu – tuto možnost použijte, pokud po vás specialisté technické podpory vyžadují informace o vašem počítači (informace o licenci, verzi produktu, operačním systému, atp.)

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

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

Účet ESET HOME

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



Toto zařízení není připojeno k účtu ESET HOME.

Pro [připojení zařízení ke svému účtu ESET HOME](#) z důvodu správy licencí a chráněných zařízení klikněte na [Připojit k ESET HOME](#). Prostřednictvím portálu můžete prodloužit platnost licence nebo zobrazit její detailní informace. V portálu nebo mobilní aplikaci ESET HOME můžete přidat všechny své licence, stahovat produkty přímo do svých zařízení, kontrolovat stavy zabezpečení svých zařízení nebo sdílet licence prostřednictvím e-mailu. Více informací naleznete v [Online nápovědě ESET HOME](#).

Toto zařízení je připojeno k účtu ESET HOME

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

Účet ESET HOME – jméno vašeho účtu ESET HOME.

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

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

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

Připojení k ESET HOME

Pro zobrazení a správu licencí, včetně jimi aktivovaných zařízení, připojte zařízení k [ESET HOME](#). Prostřednictvím portálu můžete prodloužit platnost licence nebo zobrazit její detailní informace. V portálu nebo mobilní aplikaci ESET HOME můžete přidat všechny své licence, stahovat produkty přímo do svých zařízení, kontrolovat stavy zabezpečení svých zařízení nebo sdílet licence prostřednictvím e-mailu. Více informací naleznete v [Online nápovědě ESET HOME](#).

Přihlášení k účtu ESET HOME



Přihlásit se pomocí Google



Přihlásit se pomocí Apple



Naskenovat QR kód



eset HOME

E-mailová adresa



Heslo



[Zapomněli jste heslo?](#)



Přihlásit se

Zrušit

Nemáte účet? [Vytvořte si jej!](#)

Pro připojení zařízení ke svému ESET HOME účtu:

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



Pokud máte na zařízení nainstalovaný ESET NOD32 Antivirus a je aktivovaný licenci, kterou jste přidali do účtu ESET HOME, ovšem zařízení ještě není k účtu ESET HOME připojené, můžete jej připojit. Více informací, jak ESET NOD32 Antivirus připojit, si prostudujte v kapitole produktové příručky [Přihlášení ke svému účtu ESET HOME](#) a [Přidání zařízení v ESET HOME](#).

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



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

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

3. Zadejte **Název zařízení** a klikněte na možnost **Pokračovat**.
4. Po úspěšném připojení se zobrazí okno s podrobnostmi. Klikněte na **Hotovo**.

Přihlášení do ESET HOME

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

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



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

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

[Neúspěšné přihlášení – běžné chyby.](#)

Neúspěšné přihlášení – běžné chyby

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

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

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

Uživatelské jméno a heslo nesouhlasí

Chybně zadané přihlašovací údaje. Klikněte na **Zpět**, zadejte správné heslo a ujistěte se, že zadaná e-mailová adresa je správná. Pokud se stále nemůžete přihlásit, klikněte na **Zpět** a dále vyberte možnost **Zapomněl jsem heslo**, abyste mohli obnovit své heslo a postupujte podle pokynů na obrazovce. Případně si prostudujte v příručce k portálu ESET HOME kapitolu [Zapomněli jste heslo k účtu ESET HOME](#).

Nepodporovaný způsob přihlášení k vašemu účtu

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

Nesprávné heslo

K této chybě může dojít, pokud je váš ESET NOD32 Antivirus již připojen k ESET HOME a provádíte změny, které vyžadují přihlášení (například deaktivace Anti-Theft) a zadané heslo neodpovídá přihlašovacím údajům k vašemu účtu. Po kliknutí na **Zpět** zadejte správné heslo. Pokud se stále nemůžete přihlásit, klikněte na **Zpět** a dále vyberte možnost **Zapomněl jsem heslo**, abyste mohli obnovit své heslo a postupujte podle pokynů na obrazovce. Případně si prostudujte v příručce k portálu ESET HOME kapitolu [Zapomněli jste heslo k účtu ESET HOME](#).

Přidání zařízení v ESET HOME

Pokud máte na zařízení nainstalovaný ESET NOD32 Antivirus a je aktivovaný licenci, kterou jste přidali do účtu ESET HOME, ovšem zařízení ještě nemáte ke svému účtu ESET HOME připojené, můžete jej k ESET HOME připojit:

1. [Odešlete do zařízení žádost o připojení](#).
2. V ESET NOD32 Antivirus se zobrazí dialogové okno **Připojte toto zařízení k účtu ESET HOME** a názvem tohoto účtu. Kliknutím na **Povolit** se zařízení k účtu připojí.

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

Rozšířená nastavení

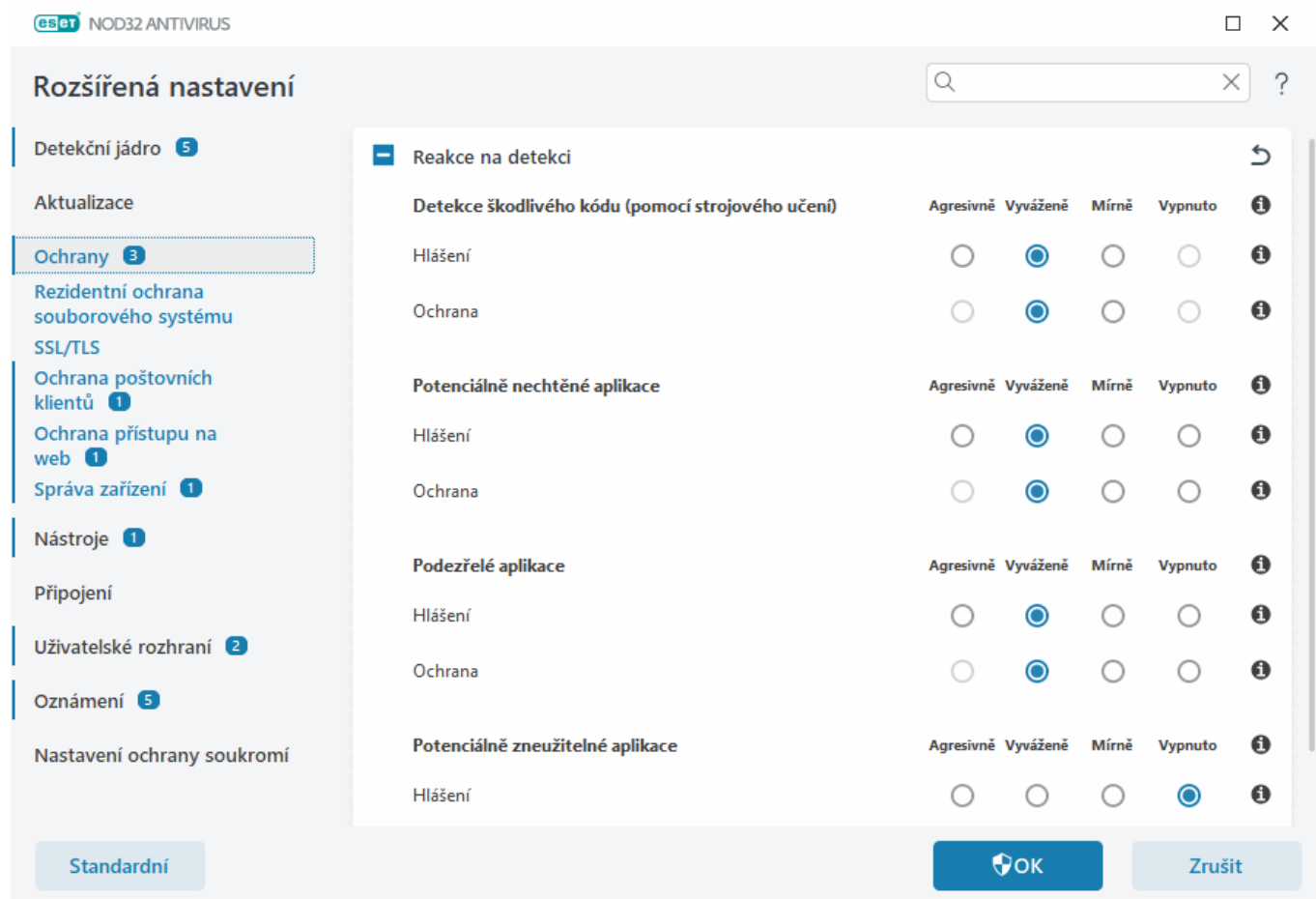
Rozšířená nastavení umožňují podrobné nastavení ESET NOD32 Antivirus podle vašich potřeb.

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

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

V rozšířeném nastavení můžete provádět následující nastavení:

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



Detekční jádro

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

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

- [Kontrola síťové komunikace](#)

Výjimky

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

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

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

Nezaměňujte mezi sebou jednotlivé typy výjimek:

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

Výkonnostní výjimky

Prostřednictvím výkonnostních výjimek můžete vyloučit soubory nebo složky z kontroly.

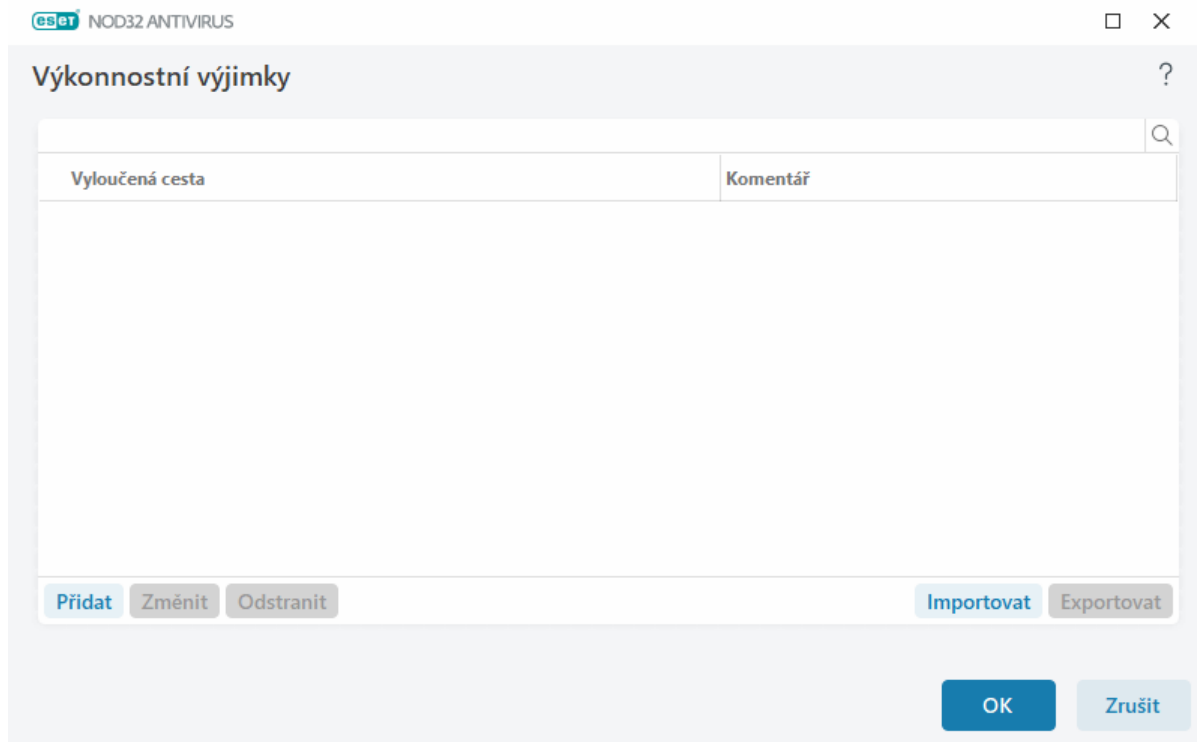
Pro zajištění kontroly všech objektů na výskyt hrozeb doporučujeme výjimky vytvářet pouze v nevyhnutelných případech. Příkladem, kdy je nutné vyloučit objekt z kontroly (například velké databázové soubory), je situace, kdy v průběhu kontroly dochází ke zpomalení počítače nebo konfliktu s právě používanou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

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



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

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



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

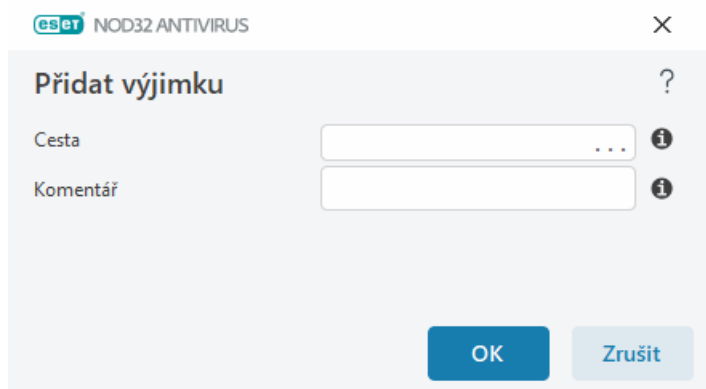
Ovládací prvky

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

Přidání a úprava výkonnostních výjimek

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

i Cestu můžete zadat ručně nebo ji vybrat pomocí Průzkumníka. Pro vybrání cesty klikněte na symbol ... v poli **Cesta**. Pro více informací se podívejte do části [příklady formátů výjimek](#).



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

Formát výjimky

- Pokud chcete vyloučit ve vybrané složce všechny soubory a podsložky, zadejte cestu ke složce a použijte masku *
- Pokud chcete vyloučit všechny .doc soubory, použijte masku *.doc
- Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční písmeno (řekněme "D"), použijte následující formát: D????.exe (otazníky nahrazují chybějící a neznámé znaky)

✓ Příklady:

- C:\Tools* – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce včetně jejich podložek.
- C:\Tools*. * – se bude chovat stejně jako C:\Tools*
- C:\Tools – v tomto případě nedojde k vyloučení složky Tools. Z pohledu skeneru může Tools představovat rovněž název souboru.
- C:\Tools*.dat – tímto vyloučíte všechny .dat nacházející se ve složce Tools.
- C:\Tools\sg.dat – vyloučí konkrétní soubor v přesně definované cestě.

Systémové proměnné ve výjimkách

Při vytváření výjimek můžete použít systémové proměnné jako %PROGRAMFILES%.

- Pro vyloučení složky Program Files pomocí této systémové proměnné použijte cestu %PROGRAMFILES%* (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty).
- Pokud chcete vyloučit všechny soubory z podsložky %PROGRAMFILES%, použijte cestu %PROGRAMFILES%\vyloučená_složka*

✓ [Rozbalte seznam podporovaných systémových proměnných](#)

Při definování výjimky podle cesty můžete použít následující proměnné:



- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Systémové proměnné specifické pro uživatele (jako %TEMP% nebo %USERPROFILE%) nebo proměnné prostředí (jako %PATH%) nejsou podporovány.

Zástupné znaky uprostřed cesty nejsou podporované



Důrazně nedoporučujeme používání zástupných znaků uprostřed cesty (například C:\Tools*\Data\file.dat), pokud to nevyžaduje infrastruktura systému.

V případě [detekčních výjimek](#) neexistují žádná omezení pro použití zástupných znaků uprostřed cesty.

Pořadí výjimek



- Pro výjimky nelze nastavovat prioritu pomocí tlačítek nahoru/dolů.
- Když skener použije první platné pravidlo, druhé platné pravidlo nebude vyhodnoceno.
- Čím méně pravidel, tím lepší je výkon kontroly.
- Vyhněte se vytváření souběžných pravidel.

Formát výjimky podle cesty

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

Formát výjimky

- Pokud chcete vyloučit ve vybrané složce všechny soubory a podsložky, zadejte cestu ke složce a použijte masku *
- Pokud chcete vyloučit všechny .doc soubory, použijte masku *.doc
- Pokud se název spustitelného souboru skládá z určitého počtu znaků, ale nevíte jakých, přesto znáte počáteční písmeno (řekněme "D"), použijte následující formát:
D?????.exe (otazníky nahrazují chybějící a neznámé znaky)

✓ Příklady:

- C:\Tools* – cesta musí končit zpětným lomítkem (\) a hvězdičkou (*), která indikuje, že mají být vyloučeny všechny soubory v dané složce včetně jejich podložek.
- C:\Tools*. – se bude chovat stejně jako C:\Tools*
- C:\Tools – v tomto případě nedojde k vyloučení složky Tools. Z pohledu skeneru může Tools představovat rovněž název souboru.
- C:\Tools*.dat – tímto vyloučíte všechny .dat nacházející se ve složce Tools.
- C:\Tools\sg.dat – vyloučí konkrétní soubor v přesně definované cestě.

Systémové proměnné ve výjimkách

Při vytváření výjimek můžete použít systémové proměnné jako %PROGRAMFILES%.

- Pro vyloučení složky Program Files pomocí této systémové proměnné použijte cestu %PROGRAMFILES%* (nezapomeňte při definování výjimky přidat zpětné lomítko na konci cesty).
- Pokud chcete vyloučit všechny soubory z podsložky %PROGRAMFILES%, použijte cestu %PROGRAMFILES%\vyloučená_složka*

✓ [Rozbalte seznam podporovaných systémových proměnných](#)

Při definování výjimky podle cesty můžete použít následující proměnné:

✓

- %ALLUSERSPROFILE%
- %COMMONPROGRAMFILES%
- %COMMONPROGRAMFILES(X86)%
- %COMSPEC%
- %PROGRAMFILES%
- %PROGRAMFILES(X86)%
- %SystemDrive%
- %SystemRoot%
- %WINDIR%
- %PUBLIC%

Systémové proměnné specifické pro uživatele (jako %TEMP% nebo %USERPROFILE%) nebo proměnné prostředí (jako %PATH%) nejsou podporovány.

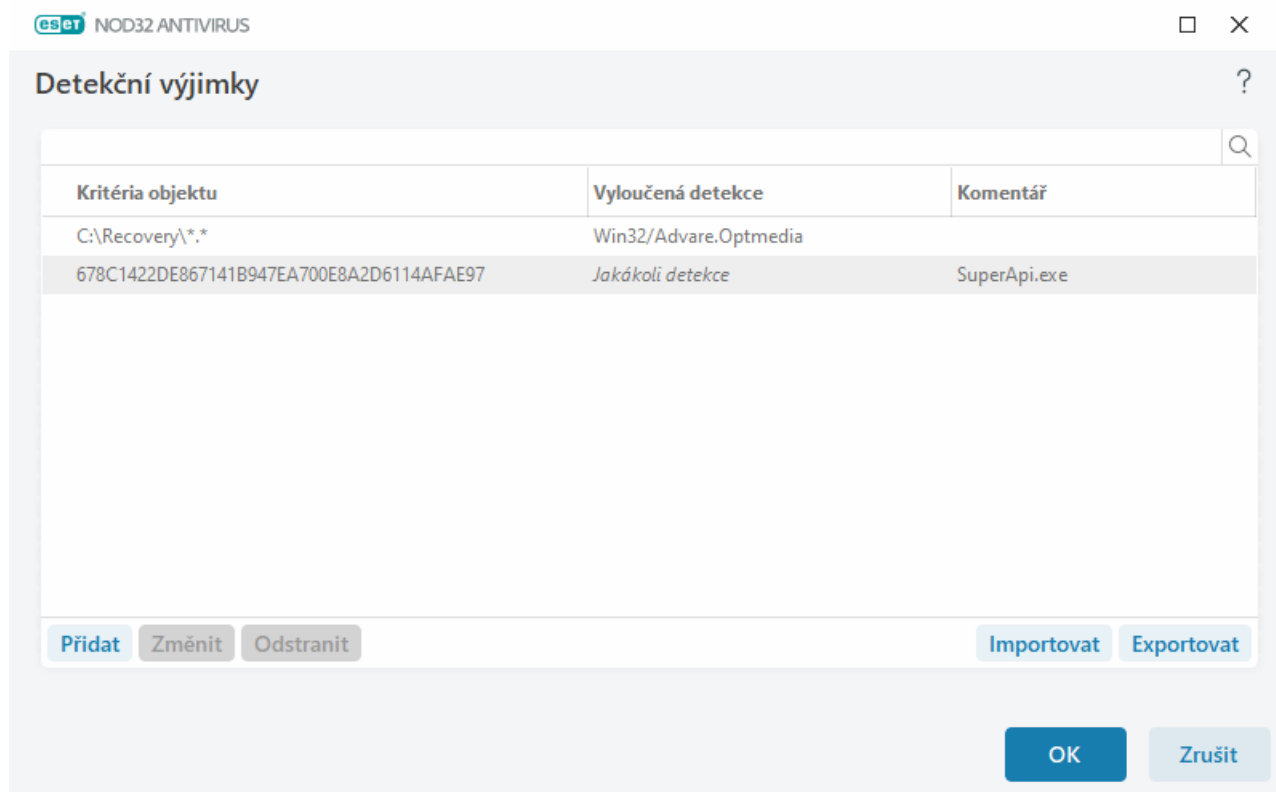
Detekční výjimky

Prostřednictvím detekčních výjimek můžete zabránit detekci objektů tím, že je budete filtrovat na základě názvu detekce, cesty k objektu nebo kontrolního součtu.

Jak detekční výjimky fungují?

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

Například podle prvního řádku dle obrázku níže bude z detekčního jádra vyloučen objekt detekovaný jako Win32/Adware.Optmedia, a může se nacházet v umístění *C:\Recovery\file.exe*. Dle druhého řádku bude soubor s uvedeným SHA-1 kontrolním součtem vyloučen bez ohledu na název detekce.



Chcete-li zajistit, aby byly všechny objekty kontrolovány na možný výskyt hrozeb, doporučujeme výjimky vytvářet pouze v nezbytných případech.

Přidání souborů a složek do seznamu výjimek z kontroly provedete v [Rozšířených nastaveních](#) > **Detekční jádro** > **Výjimky** > **Detekční výjimky** > **Změnit**.

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

Pro [vyloučení objektu](#) (na základě názvu detekce nebo kontrolního součtu klikněte na tlačítko **Přidat**).

Výjimku pro [potenciálně nechtěné aplikace](#) a [potenciálně zneužitelné aplikace](#) na základě jejich názvu můžete vytvořit rovněž následujícím způsobem:

- V dialogovém okně s upozorněním na detekci klikněte na **Zobrazit rozšířená nastavení** a vyberte možnost **Vyloučit z detekce**.
- V kontextové menu nad konkrétním záznamem v protokolu detekcí použijte [Průvodce vytvořením detekční výjimky](#).
- V hlavním okně programu na záložce **Nástroje** > **Karanténa** klikněte pravým tlačítkem myši na soubor v karanténě a z kontextového menu vyberte možnost **Obnovit a vyloučit z kontroly**.

Kritéria objektu detekční výjimky

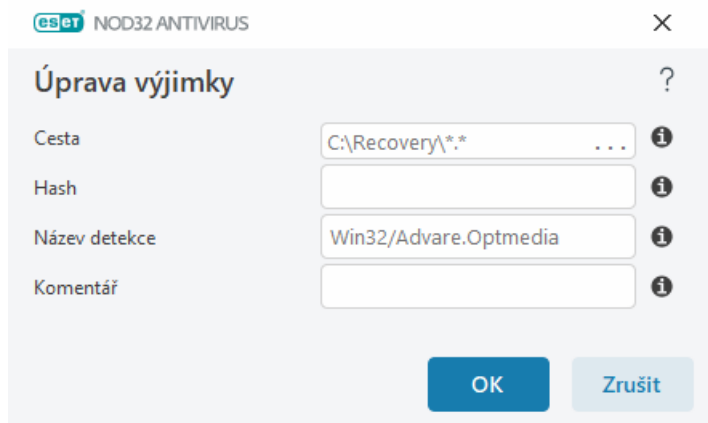
- **Cesta** – pomocí této možnosti můžete omezit, v případě potřeby, výjimku jen na konkrétní umístění.
- **Název detekce** – pokud je u vyloučeného souboru uveden i název [detekce](#), znamená to, že je soubor vyloučen pro danou detekci, nikoli celý. Pokud však bude soubor infikován později jiným malwarem, bude detekován.
- **Has** – pomocí této možnosti vyloučíte konkrétní objekt na základě jeho specifického SHA-1 kontrolního součtu bez ohledu na jeho umístění, název nebo příponu.

Přidání a úprava detekčních výjimek

Vyloučení detekce

Je nutné uvést platný název ESET detekce. Informace o platném názvu detekce naleznete na záložce [Protokoly](#), kdy z rozbalovacího menu vyberte možnost **Detekce**. Tento typ detekce je vhodné využít v případě, kdy ESET NOD32 Antivirus objekt [nesprávně označil za škodlivý](#) (false positive). Protože výjimky pro skutečné infiltrace představují velké riziko, při jejich vytváření zvažte, zda není vhodné vytvořit výjimku pouze na konkrétní soubor nebo umístění, ve kterém k detekci došlo (k tomu využijte tlačítko ... v poli **Cesta**). Případně výjimku vytvořte pouze dočasně. Výjimky je možné vytvářet také pro [potenciálně nechtěné aplikace](#), potenciálně zneužitelné aplikace a podezřelé aplikace.

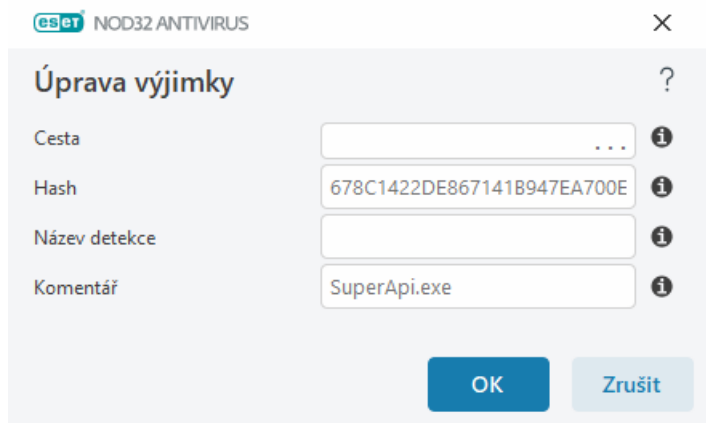
Další informace naleznete v kapitole [Formát výjimky podle cesty](#).



Další informace naleznete v níže uvedeném [příkladu na vyloučení detekce](#).

Vyloučit hash

Pomocí této možnosti vyloučí konkrétní objekt na základě jeho specifického SHA-1 kontrolního součtu bez ohledu na jeho umístění, název nebo příponu.



Výjimky na základě názvu detekce

Pro vyloučení konkrétní detekce na základě názvu zadejte její platný název:
Win32/Adware.Optmedia

- ✓ Můžete také použít následující formát, pokud vyloučíte detekci z okna výstrahy ESET NOD32 Antivirus:
- @NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
 - @NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
 - @NAME=Win32/Bagle.D@TYPE=worm

Ovládací prvky

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

Průvodce vytvořením detekční výjimky

Detekční výjimku můžete vytvořit také přímo z [Protokolu](#) (tato možnost není dostupná nad objekty, které byly označeny jako malware):

1. V [hlavním okně programu](#) přejděte na záložku **Nástroje > Protokoly**.
2. Z rozbalovacího menu vyberte možnost **Detekce** a následně klikněte pravým tlačítkem na zobrazený záznam.
3. Vyberte možnost **Vytvořit výjimku**.

Pro změnu **Kritéria výjimky** klikněte na tlačítko **Změnit kritéria**.

- **Konkrétní soubory** – pomocí této možnosti vyloučíte konkrétní soubor podle jeho SHA-1 kontrolního součtu.
- **Detekce** – vyloučí soubor podle názvu detekce.
- **Cesta + Detekce** – pomocí této možnosti vyloučíte v konkrétním souboru (například `file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe`) definovanou detekci.

Na základě typu detekce je vždy předvybrána doporučená možnost.

Volitelně můžete přidat **Komentář**, pokračujte kliknutím na tlačítko **Vytvořit výjimku**.

Rozšířená nastavení detekčního jádra

Zapnout rozšířenou kontrolu prostřednictvím AMSI – pokud zapnete tuto možnost v Rozšířených nastaveních > Detekční jádro > Další možnosti, bude nástroj Antimalware Scan Interface (AMSI) kontrolovat skripty PowerShellu, skripty spouštěné programem Windows Script Host a data kontrolovaná pomocí AMSI SDK.

Kontrola síťové komunikace

Kontrola síťové komunikace poskytuje ochranu před malwarem pro aplikační protokoly, která integruje několik pokročilých technik kontroly škodlivého kódu. Kontrola síťové komunikace automaticky kontroluje protokoly HTTP(S), POP3(S) a IMAP(S) bez ohledu na internetový prohlížeč nebo e-mailového klienta. Kontrolu síťové komunikace můžete zapnout nebo vypnout v [Rozšířených nastaveních](#) > **Detekční jádro** > **Kontrola síťové komunikace**.

Zapnout kontrolu síťové komunikace – pokud tuto možnost vypnete, protokoly HTTP(S), POP3(S) a IMAP(S) se nebudou kontrolovat. Všimněte si, že následující funkce ESET NOD32 Antivirus vyžadují zapnutou Kontrolu síťové komunikace:

- [Ochrana přístupu na web](#)
- [SSL/TLS](#)
- [Anti-Phishingová ochrana](#)
- [Ochrany poštovních klientů](#),

Cloudová ochrana

ESET LiveGrid® (nová generace systému včasného varování ESET ThreatSense.Net) využívá data od uživatelů bezpečnostních produktů ESET z celého světa a zasílá je do virových laboratoří společnosti ESET. Díky podezřelým vzorkům a souvisejícím metadatům dokážeme prostřednictvím ESET LiveGrid® okamžitě reagovat na nejnovější hrozby.

K dispozici jsou následující možnosti:

Zapnout reputační systém ESET LiveGrid®

Reputační systém ESET LiveGrid® porovnává soubory v cloudu oproti neškodnému nebo škodlivému chování souborů.


Díky tomuto systému máte možnost ověřit přímo z rozhraní produktu ESET, případně kontextového menu, spolehlivost souborů a [spuštěných procesů](#) a získat o těchto objektech další informace ze systému ESET LiveGrid®.

Zapnout systém zpětné vazby ESET LiveGrid®

Reputační systém ESET LiveGrid® a systém zpětné vazby ESET LiveGrid® shromažďuje z vašeho počítače pouze informace, které se týkají nové infiltrace. To může zahrnovat:



- Vzorek nebo kopii souboru, ve kterém se hrozba objevila
- Cesty k umístění souboru
- Název souboru
- Datum a čas
- Způsob, jakým se hrozba dostala do počítače
- Informace o stavu zabezpečení počítače

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

 Více informací o zasílaných datech naleznete v dokumentu [Zásady ochrany osobních údajů](#).

Můžete se rozhodnout ESET LiveGrid® nezapínat

Nepřijde vám o žádnou funkci, ale v některých případech může ESET NOD32 Antivirus reagovat na nové hrozby se zpožděním, než kdyby byl ESET LiveGrid® aktivní. Pokud jste měli zapnutý ESET LiveGrid® a nyní jste jej vypnuli, může se stát, že v počítači jsou již připraveny datové balíčky k odeslání. Tyto balíčky se ještě odešlou při nejbližší příležitosti. Po vypnutí systému se již nové balíčky vytvářet nebudou.

 Více informací o technologii ESET LiveGrid® naleznete ve [slovníku pojmů](#).
 [Názorné ukázky](#), jak zapnout nebo vypnout ESET LiveGrid® v produktu ESET NOD32 Antivirus máme k dispozici v Databázi znalostí v angličtině a několika dalších jazycích.

Konfigurace cloudové ochrany v Rozšířeném nastavení produktu

Chcete-li získat přístup k nastavení pro ESET LiveGrid®, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Cloudová ochrana**.

- **Zapnout reputační systém ESET LiveGrid® (doporučeno)** – reputační systém ESET LiveGrid® zvyšuje účinnost anti-malwarových řešení ESET ověřováním souborů vůči cloudové databázi povolených a zakázaných souborů.
- **Zapnout systém zpětné vazby ESET LiveGrid®** – po aktivování se budou do laboratoří ESET k analýze odesílat relevantní data (popsáno níže v sekci **Odesílání vzorků**) spolu se statistikami a hlášeními o pádech.
- **Odesílat informace o pádech a diagnostická data** – po aktivování ESET LiveGrid® se budou odesílat diagnostická data, jako jsou informace o pádech a výpisy obsahu paměti jednotlivých modulů.

Doporučujeme ponechat tuto funkci zapnutou, abyste pomohli firmě ESET diagnostikovat problémy, vylepšovat produkty a zajistit lepší ochranu uživatelů.

- **Odesílat anonymní statistiky** – tímto umožníte společnosti ESET shromažďovat informace o nově detekovaných hrozbách, jako je název hrozby, datum a čas detekce, metoda detekce a přidružená metadata, verze produktu a konfigurace včetně informací o vašem systému.
- **Kontaktní e-mail (nepovinný údaj)** – zadaný kontaktní e-mail se odešle společně s podezřelým souborem a v případě potřeby může být použit pro vyžádání dalších informací. Od společnosti ESET neobdržíte žádnou informaci o zaslaném vzorku, pokud nejsou vyžadovány podrobnější informace k jeho analyzování.

Odesílání vzorků

Ruční odesílání vzorků – umožňuje z kontextového menu, [Karantény](#) nebo z části [Nástroje > Další nástroje](#) odesílat soubor k analýze do společnosti ESET.

Automatické odesílání detekovaných vzorků

Vyberte, jaké druhy vzorků budete odesílat společnosti ESET k analýze a k vylepšení budoucí detekce (výchozí maximální velikost vzorku je 64 MB). K dispozici jsou následující možnosti:

- **Všechny detekované vzorky** – Všechny [objekty](#) detekované [Detekčním jádrem](#) (včetně potenciálně nechtěných aplikací, pokud jsou v nastavení skeneru povoleny).
- **Všechny vzorky kromě dokumentů** – všechny detekované objekty kromě **Dokumentů** (viz níže).
- **Neodesílat** – Detekované objekty nebudou společnosti ESET odeslány.

Automatické odesílání podezřelých souborů

Tyto vzorky budou rovněž poslány společnosti ESET i v případě, že nebudou detekovány detekčním jádrem. Například vzorky, které se vyhnuly detekci těsně, nebo je některý z [modulů ochrany](#) ESET NOD32 Antivirus považuje za podezřelé, případně vykazují nejasné chování (výchozí maximální velikost vzorku je 64 MB).

- **Spustitelné soubory** – zahrnuje následující typy souborů: .exe, .dll, .sys.
- **Archivy** – zahrnuje následující typy souborů: .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skripty** – zahrnuje následující typy souborů: .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Ostatní** – zahrnuje následující typy souborů: .jar, .reg, .msi, .sfw, .lnk.
- **Pravděpodobný spam** – vybráním této možnosti umožníte zasílání částí nebo celých zpráv, včetně příloh, označených jako spam, k bližší analýze do společnosti ESET. Tímto krokem přispějete k vylepšení globální detekce nevyžádaných e-mailů, a získáte tím, nejen vy, v budoucnu lepší detekci spamu.
- **Dokumenty** – zahrnují dokumenty Microsoft Office nebo PDF s aktivním obsahem i bez.

✓ [Zobrazit seznam všech dotčených typů dokumentů](#)

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

Výjimky

Pomocí [filtru výjimek](#) můžete vyloučit složky a konkrétní typy souborů z odeslání k analýze (například soubory obsahující citlivé informace jako dokumenty nebo tabulky). Soubory uvedené na seznamu nebudou nikdy odeslány do laboratoří ESET k analýze, i pokud by se v nich nacházel škodlivý kód. Standardně jsou vyloučeny nejrozšířenější typy souborů (.doc, atp.). Do seznamu výjimek můžete přidat vlastní typy souborů.

✓ Chcete-li vyloučit soubory stažené z webu `download.domain.com`, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Cloudová ochrana** > **Odesílání vzorků** a klikněte na **Změnit** vedle položky **Výjimka**. Na řádku **Výjimky** klikněte na **Změnit** a v zobrazeném dialogovém okně a definujte výjimku následovně: `.download.domena.cz`.

Maximální velikost vzorku (MB) – určuje maximální velikost automaticky odesílaných vzorků (1-64 MB).

Filtr výjimek pro cloudovou ochranu

Pomocí seznamu výjimek můžete zabránit v odesílání konkrétních typů souborů nebo obsahu složek k analýze. Soubory uvedené na seznamu nebudou nikdy odeslány do laboratoří ESET k analýze, i pokud by se v nich nacházel škodlivý kód. Standardně se neodesílají nejrozšířenější typy souborů (.doc, atp.).

i Tuto funkci můžete využít pro vyloučení souborů, které by mohly obsahovat důvěryhodné informace – například dokumenty nebo tabulky.

✓ Pro vyloučení souborů stažených z adresy `download.domena.cz` přejděte v [Rozšířených nastaveních](#) do sekce **Detekční jádro** > **Cloudová ochrana** > **Odesílání vzorků**. Na řádku **Výjimky** klikněte na **Změnit** a v zobrazeném dialogovém okně definujte výjimku následovně: `*download.domena.cz*`.

Detekce škodlivého kódu

Sekce **Detekce škodlivého kódu** je přístupná z [Rozšířeného nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** a umožňuje konfigurovat parametry pro profily kontroly.

Volitelná kontrola

Profil kontroly – určuje název profilu, jehož nastavení se použijí při volitelné kontrole počítače. Nový profil můžete vytvořit po kliknutí na tlačítko **Změnit** na řádku **Seznam profilů**. Další podrobnosti naleznete v kapitole [Profily kontroly](#).

Po výběru profilu kontroly můžete nakonfigurovat následující možnosti:

Cíle kontroly – pokud chcete zkontrolovat konkrétní cíl nebo skupinu cílů, klikněte na **Změnit** vedle položky **Cíle kontroly** a vyberte možnost ze stromové struktury složek. Další podrobnosti naleznete v kapitole [Cíle kontroly](#).

Volitelná ochrana s využitím strojového učení – pro každý profil kontroly můžete nakonfigurovat úroveň hlášení

a ochrany. Ve výchozím nastavení mají profily kontroly stejné nastavení, jaké je nastaveno v části [Rezidentní ochrana souborového systému](#). Pro konfiguraci vlastních hlášení a úrovní ochrany přepínačem deaktivujte možnost **Použít nastavení rezidentní ochrany**. Podrobné vysvětlení úrovní hlášení a ochrany naleznete v kapitole [Ochrany](#).

ThreatSense – možnosti rozšířeného nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Profily kontroly

K dispozici jsou čtyři předdefinované profily kontroly ESET NOD32 Antivirus:

- **Smart kontrola počítače:** toto je výchozí profil pokročilé kontroly. Profil Smart kontrola počítače využívá technologii Smart optimalizace, pro vyloučení souborů, které byly při předchozí kontrole označeny jako čisté, a nedošlo u nich od té doby ke změně. Tím se zkracuje doba kontroly při současném minimálním dopadu na zabezpečení systému.
- **Kontrola z kontextového menu:** Volitelnou kontrolu libovolného souboru můžete spustit z kontextového menu. Profil kontroly z kontextového menu umožňuje nastavit konfiguraci kontroly při jejím využití.
- **Hlubková kontrola počítače:** Profil hloubkové kontroly ve výchozím nastavení nepoužívá smart optimalizaci, takže použitím tohoto profilu nejsou vyloučeny z kontroly žádné soubory.
- **Kontrola počítače:** Toto je výchozí profil používaný při standardní kontrole počítače.

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

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

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

Cíle kontroly

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

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

- **Vlastní výběr** – zruší výběr cílů.

Další cíle kontroly si můžete vybrat ve stromové struktuře.

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

Pro rychlý přesun k požadovanému cíli kontroly (souboru nebo složce), zadejte jeho cestu do textového pole zobrazeném pod stromovou strukturou. Mějte na paměti, že se v cestě rozlišuje velikost písmen. Použitím zaškrtnutí pole ve stromové struktuře přidáte daný cíl do seznamu cílů, které se mají kontrolovat.

Kontrola při nečinnosti

Kontrolu při nečinnosti můžete nastavit v [Rozšířených nastaveních](#) v sekci **Detekční jádro > Detekce škodlivého kódu > Kontrola při nečinnosti**.

Kontrola při nečinnosti

Aktivujte tuto funkci pomocí přepínače vedle položky **Zapnout kontrolu při nečinnosti**. Tichá kontrola všech lokálních disků v počítači se spouští v případě, že je počítač ve stavu nečinnosti.

Standardně se kontrola při nečinnosti nespouští, pokud je počítač (notebook) napájen z baterie. Toto nastavení můžete zrušit aktivací přepínače vedle položky **Spustit také při napájení počítače z baterie** v [Rozšířených nastaveních](#).

V [Rozšířených nastaveních](#) přepínačem aktivujte možnost **Zapisovat do protokolu**, pokud chcete průběh kontroly zapisovat do sekce [Protokoly](#) (v [hlavním okně programu](#) klikněte na **Nástroje > Protokoly** a z rozbalovacího menu **Detekce** vyberte možnost **Kontrola počítače**).

Detekce stavu nečinnosti

Více informací o možnostech definování akce, při které se spustí kontrola, naleznete v kapitole [Detekce stavu nečinnosti](#).

ThreatSense – možnosti Rozšířeného nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Detekce stavu nečinnosti

Nastavení Detekce stavu nečinnosti můžete konfigurovat v části [Rozšířená nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Kontrola při nečinnosti** > **Detekce stavu nečinnosti**. Tato nastavení určují spouštění [Kontroly při nečinnosti](#):

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

Pomocí přepínačů určete stav, při kterém chcete provádět kontrolu počítače.

Kontrola po startu

Standardně se kontrola souborů zaváděných při startu počítače do operační paměti provádí během startu počítače a po aktualizaci detekčního jádra. Tato kontrola závisí na nastavení úloh v [Plánovači](#).

Možnosti nastavení kontroly souborů zaváděných při startu počítače jsou součástí naplánované úlohy **Kontrola souborů spouštěných po startu**. Chcete-li upravit toto nastavení, přejděte na **Nástroje** > **Plánovač** > klikněte na **Kontrola souborů spouštěných po startu** a následně na tlačítko **Změnit**. V posledním kroku se zobrazí okno [Kontrola souborů spouštěných po startu počítače](#). Více informací o tvorbě a správě úloh Plánovače naleznete v kapitole [Vytvoření nové úlohy](#).

ThreatSense – možnosti rozšířeného nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

Automatická kontrola souborů spouštěných při startu počítače

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

Pomocí rozbalovacího menu **Cíle kontroly** můžete upravit množství souborů, které se má kontrolovat. Seznam souborů, získaný na základě sofistikovaného algoritmu, je seřazen vzestupně podle následujících kritérií:

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

Mezi tyto možnosti patří také tyto dvě:

- **Soubory zaváděné před přihlášením uživatele** – zahrnuje soubory z míst, ke kterým může být přístupováno bez toho, aby byl uživatel přihlášen (typicky všechny položky po spuštění jako jsou služby, browser helper objects, winlogon oznámení, záznamy plánovače Windows, známé dll atd.).
- **Soubory zaváděné po přihlášení uživatele** – zahrnuje soubory z míst, ke kterým může být přístupováno až po přihlášení uživatele (typicky soubory, které jsou spouštěny pro daného uživatele, nejčastěji umístěné v `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`).

Seznamy souborů určených ke kontrole jsou určeny výše uvedenými skupinami. Pokud zvolíte nižší hloubku kontroly pro soubory spouštěných při startu, nebudou kontrolovány po otevření nebo spuštění.

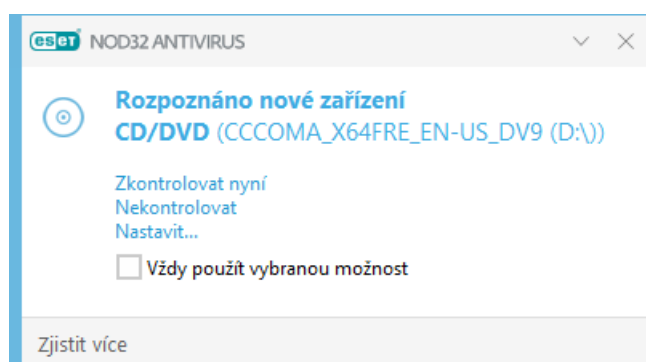
Priorita kontroly – definujte úroveň priority, při které se spustí kontrola počítače:

- **Při nečinnosti** – úloha se spustí pouze při nečinnosti systému,
- **Nižší** – zatížení systému je nižší,
- **Nejnižší** – zatížení systému je nejnižší,
- **Normální** – zatížení systému je běžné.

Výměnná média

ESET NOD32 Antivirus dokáže automaticky kontrolovat výměnná média (CD/DVD/USB/...) po jejich vložení/připojení do počítače. Tuto funkci můžete využít, pokud jako správce počítače chcete zabránit uživatelům v používání škodlivého obsahu na výměnných médiích.

Pokud je vloženo výměnné médium a v [Rozšířených nastaveních](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média** je nastavena možnost **Zobrazit možnosti kontroly**, objeví se následující dialogové okno:



Možnosti tohoto dialogu:

- **Zkontrolovat nyní** – spustí se ruční kontrola výměnného média.
- **Nekontrolovat** – po vybrání této možnosti se výměnné médium nekontroluje.
- **Nastavení** – otevře [Rozšířená nastavení](#).
- **Vždy použít vybranou možnost** – pokud vyberete toto pole, při příštím připojení výměnného média se provede stejná akce.

Kromě toho Správa zařízení ESET NOD32 Antivirus disponuje pokročilými funkcemi, které vám umožňují definovat

pravidla pro zacházení s externími zařízeními připojovanými k vašemu počítači. Více informací naleznete v kapitole [Správa zařízení](#).

K přístupu do nastavení kontroly výměnných médií otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Výměnná média**.

Akce po vložení vyměnitelného média – Vyberte výchozí akci, která bude provedena po vložení vyměnitelného média do počítače (CD/DVD/USB). Po vložení výměnného média do počítače vyberte požadovanou akci:


- **Nekontrolovat** – neprovede se žádná akce a upozornění **Nalezeno nové nařízení** se nezobrazí.
- **Automaticky zkontrolovat médium** – po vložení média se automaticky spustí kontrola jeho obsahu.
- **Zobrazit možnosti kontroly** – otevře možnost **Nastavení výměnných médií**.

Ochrana dokumentů

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

Pro zapnutí této možnosti přejděte do [Rozšířeného nastavení](#) > **Detekční jádro** > **Detekce škodlivého kódu** > **Ochrana dokumentů** a klikněte na přepínač vedle **Zapnout ochranu dokumentů**.

ThreatSense – možnosti rozšířeného nastavení, například přípony souborů, které chcete kontrolovat, a použité metody detekce. Další informace naleznete v kapitole [ThreatSense](#).

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

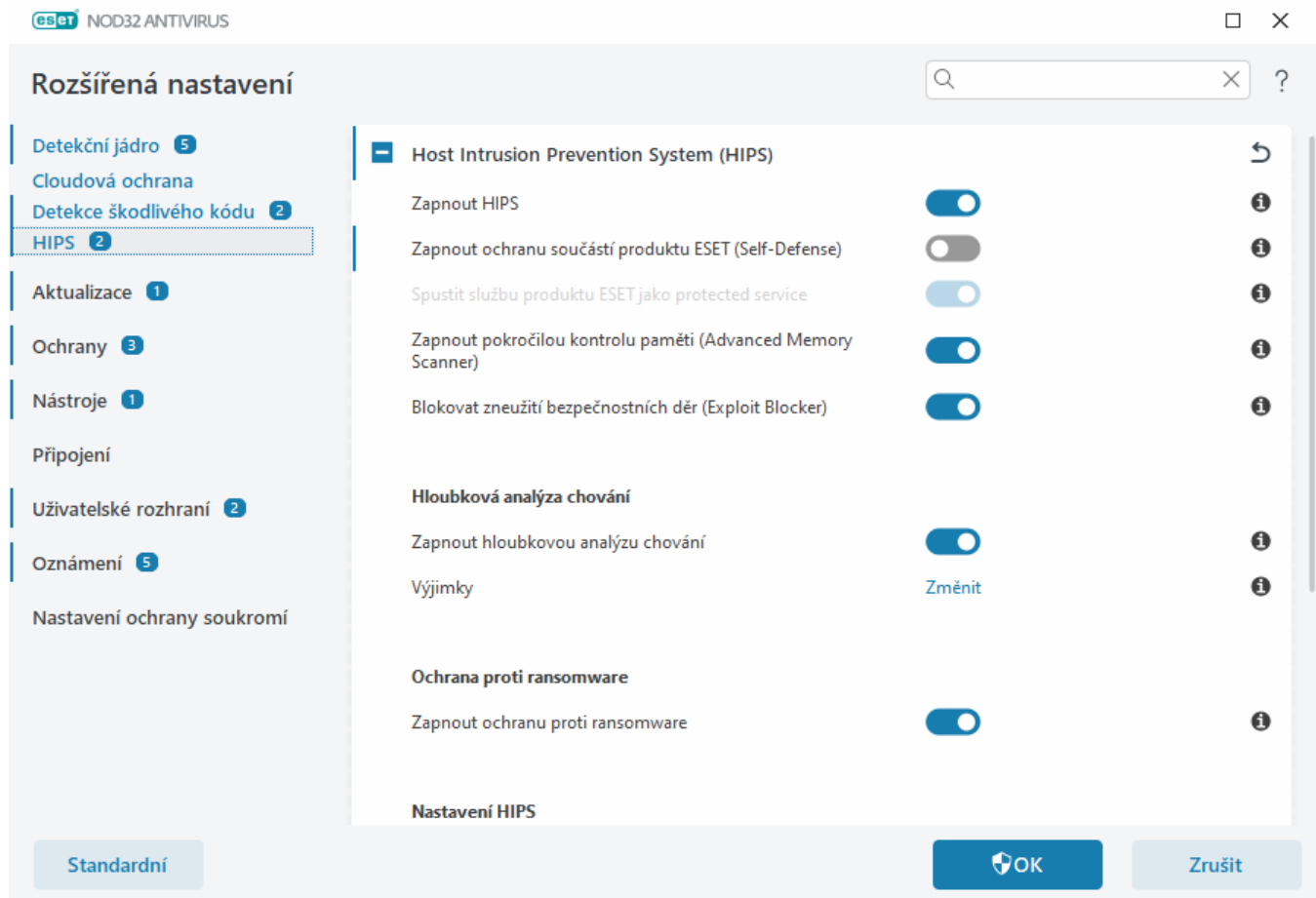
HIPS – Host Intrusion Prevention System



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

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

Systém HIPS můžete nastavit v [Rozšířených nastaveních](#) > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)**. Stav modulu HIPS je zobrazen v [hlavním okně programu](#) ESET NOD32 Antivirus > **Nastavení** > **Ochrana počítače**.



Host Intrusion Prevention System (HIPS)

Zapnout HIPS – HIPS je v ESET NOD32 Antivirus standardně zapnutý. Jeho vypnutím zakážete běh dalších součástí HIPS jako je například Exploit Blocker.

Zapnout ochranu součástí produktu ESET (Self-Defense) – ESET NOD32 Antivirus obsahuje vestavěnou technologii **Self-Defense**, která brání škodlivé aplikaci v narušení nebo zablokování antivirové ochrany. Self-Defense chrání soubory a klíče v registru, které jsou kritické pro správnou funkci produktu ESET a neumožňuje potenciálnímu škodlivému software přístup k těmto záznamům a procesům a jejich úpravu.

Spustit službu produktu ESET jako protected service – pomocí této možnosti zapnete ochranu služby ESET (ekrn.exe). Pokud je možnost zapnutá, služba je spuštěná jako chráněný proces ve Windows a slouží tak pro boj se škodlivým kódem.

Zapnout pokročilou kontrolu paměti (Advanced Memory Scanner) – tato funkce v kombinaci s blokováním zneužití bezpečnostních děr (Exploit Blocker) poskytuje účinnou ochranu proti škodlivému kódu, který využívá obfuskaci a šifrování pro zabránění detekce. Tato funkce je standardně zapnuta. Více informací o tomto typu ochrany naleznete ve [slovníku pojmů](#).

Blokovat zneužití bezpečnostních děr (Exploit Blocker) – tato funkce poskytuje další bezpečnostní vrstvu a chrání známé aplikace se zranitelnými bezpečnostními dírami (například webové prohlížeče, e-mailové klienty, PDF čtečky a komponenty Microsoft Office). Tato funkce je standardně zapnuta. Více informací o této vrstvě ochrany naleznete ve [slovníku pojmů](#).

Hloubková analýza chování

Hloubková analýza chování je další vrstvou ochrany funkce HIPS. Toto rozšíření analyzuje chování běžících programů a varuje vás, jestliže jejich chování bude pro váš počítač škodlivé.

[HIPS výjimky Hloubkové analýzy chování](#) umožňují vyloučit procesy z kontroly. Pro zajištění všech kontrol na možné hrozby doporučujeme vytvářet vyloučení pouze v případě, že je absolutně nezbytné.

Ochrana proti ransomware

Zapnout ochranu proti ransomware – tato součást představuje další vrstvu funkce HIPS. Pro správnou funkci ochrany proti ransomware je třeba mít zapnutý Reputační systém ESET LiveGrid®. Více informací o tomto typu ochrany naleznete ve [slovníku pojmů](#).

Zapnout Intel® Threat Detection Technology – technologie pomáhá odhalovat útoky ransomwaru využitím unikátní telemetrie z procesoru Intel. Zvyšuje účinnost detekce, snižuje počet falešných poplachů a rozšiřuje možnosti zachycení pokročilých technik na obcházení detekce v paměti zařízení. Viz [podporované procesory](#).

Nastavení HIPS

HIPS může běžet v jednom z následujících **režimů**:

Režim filtrování	Popis
Automatický režim	Operace budou povoleny s výjimkou blokových na základě předdefinovaných pravidel, které váš systém chrání.
Smart režim	Uživatel bude upozorněn pouze na velmi podezřelé události.
Interaktivní režim	Uživatel bude na povolení operace dotázán.
Administrátorský režim	Blokuje každé spojení, pro které neexistuje povolující pravidlo.
Učící režim	Operace jsou povoleny a po každé operaci je vytvořeno pravidlo. Pravidla vytvořená v tomto režimu jsou viditelná v editoru Pravidla HIPS , ale jejich priorita je nižší než priorita pravidel vytvořených ručně nebo pravidel vytvářených v automatickém režimu. Vyberete-li v rozbalovací nabídce Režim filtrování možnost Učící režim , zpřístupní se nastavení Učící režim bude ukončen . Vyberte časové období (max. 14 dní), pro které bude učící režim aktivní. Po uplynutí zadaného období budete vyzváni k úpravě pravidel vytvořených pomocí HIPS v učícím režimu. Můžete také zvolit jiný režim filtrování nebo odložit rozhodnutí a pokračovat v používání režimu učení.

Po ukončení učícího režimu nastavit režim – pomocí této možnosti vyberte režim filtrování, který se automaticky nastaví po ukončení běhu učícího režimu. Pokud vyberete možnost **Dotázat se uživatele**, pro změnu režimu filtrování modulu HIPS bude vyžadováno oprávnění administrátora.

Systém HIPS monitoruje události uvnitř operačního systému a reaguje na ně podle pravidel, která jsou strukturou podobná pravidlům firewallu. Kliknutím na **Změnit** vedle položky **Pravidla** otevřete editor **Pravidla HIPS**. Zde můžete pravidla prohlížet, vytvářet nová, upravovat nebo odstranit stávající. Více detailů o vytváření pravidel a operacích HIPS naleznete v kapitole [Úprava pravidla HIPS](#).

HIPS výjimky

Prostřednictvím výjimek můžete vyloučit procesy z HIPS Hlubkové analýzy chování.

Chcete-li upravit výjimky pro HIPS, otevřete [Rozšířená nastavení](#) > **Detekční jádro** > **HIPS** > **Host Intrusion Prevention System (HIPS)** > **Výjimky** > **Změnit**.

i Nezaměňujte tuto funkci s možností pro [vyloučení přípon souborů](#) z kontroly, tvorbu [detekčních výjimek](#), [výkonnostních výjimek](#), [vyloučených procesů](#).

Pro vyloučení objektu z kontroly klikněte na tlačítko **Přidat** a zadejte cestu k objektu nebo ji vyberte ručně ze stromové struktury. Existující výjimky můžete upravovat, případně odstranit.

Rozšířená nastavení HIPS

Následující možnosti jsou užitečné pro ladění a analýzu chování aplikací:

[Automaticky povolené ovladače](#) – seznam ovladačů, které budou vždy načteny, bez ohledu na nastavený režim filtrování, pokud nejsou blokovány uživatelským pravidlem.

Zapisovat všechny zablokované operace do protokolu – všechny zablokované operace se zapíší do protokolu HIPS. Tuto možnost aktivujte výhradně na výzvu specialisty technické podpory ESET. Mějte na paměti, že se následně začne generovat velké množství dat a může dojít ke zpomalení počítače.

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

Ovladače, jejichž načtení je vždy povoleno

Vybrané ovladače budou vždy načteny bez ohledu na nastavený režim filtrování modulu HIPS, pokud nejsou blokovány uživatelským pravidlem.

Přidat – přidá nový ovladač.

Změnit – upraví parametry vybraného ovladače.

Odstranit – Odstranit ovladač ze seznamu.

Reset – obnoví seznam na výchozí hodnoty.

i Po kliknutí na tlačítko **Obnovit** vymažete všechny ovladače, které jste přidali ručně. V seznamu zůstanou pouze systémové ovladače.

i Po instalaci je seznam ovladačů prázdný. ESET NOD32 Antivirus je časem automaticky doplní.

Interaktivní režim HIPS

Přímo z okna HIPS oznámení můžete vytvořit pravidlo na základě akce, které modul HIPS detekoval, a definovat podmínky, za kterých bude tato operace povolena nebo blokována.

Pravidla vytvořená z oznámení jsou ekvivalentní ručně vytvořeným. Pravidlo vytvořené z oznámení může být však méně specifické, než pravidlo vytvořené prostřednictvím editoru pravidel. To znamená, že po vytvoření pravidla prostřednictvím editoru může stejná operace vyvolat zobrazení oznámení. Pro více informací si nastudujte [prioritu HIPS pravidel](#).

Pokud je jako výchozí akce pro pravidlo nastavena možnost **Vždy se dotázat**, dialogové okno se zobrazí při každé aktivaci pravidla. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**. Pokud v danou chvíli akci nevyberete, nová akce se vybere na základě pravidel.

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

Vybráním možnosti **Vytvořit pravidlo a trvale zapamatovat** vytvoříte nové HIPS pravidlo, kterým můžete následně modifikovat prostřednictvím [Editoru HIPS pravidel](#) (ke změně pravidel je vyžadováno oprávnění administrátora).

Kliknutím na **Detaily** v dolní části okna zjistíte, jaká aplikace operaci vyvolala, jakou má soubor reputaci, případně na jaký typ akce (povolit, blokovat) jste byli dotázáni.

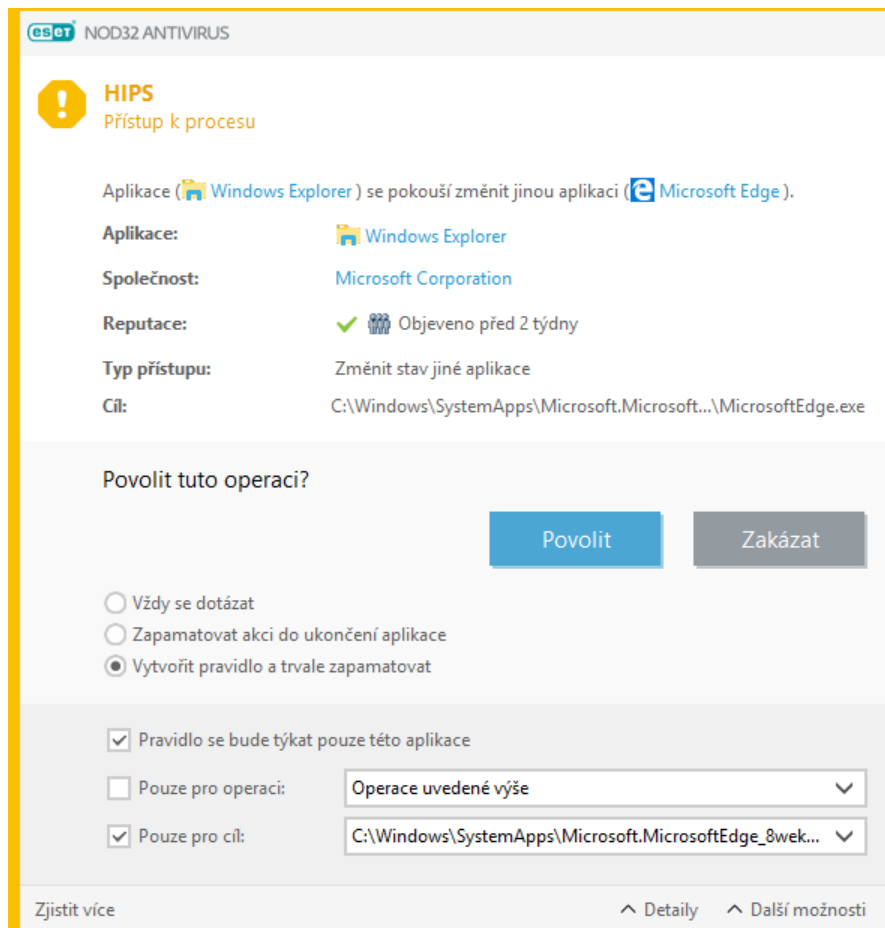
Nastavení detailních parametrů si zpřístupníte kliknutím na **Rozšířená nastavení**. Níže uvedené možnosti jsou dostupné v případě, kdy vyberete možnost **Vytvořit pravidlo a trvale zapamatovat**.

- **Vytvořit pravidlo platné pouze pro tuto aplikaci** – pokud tuto možnost zrušíte, pravidlo bude platné pro všechny zdrojové aplikace.
- **Pouze pro operaci** – vyberte operaci se souborem/aplikace/registrem. [Pro více informací se podívejte na popis všech HIPS operací](#).
- **Pouze pro cíl** – vyberte, zda bude pravidlo platné pro soubor/aplikaci/registr.

Již nechcete zobrazovat HIPS oznámení?

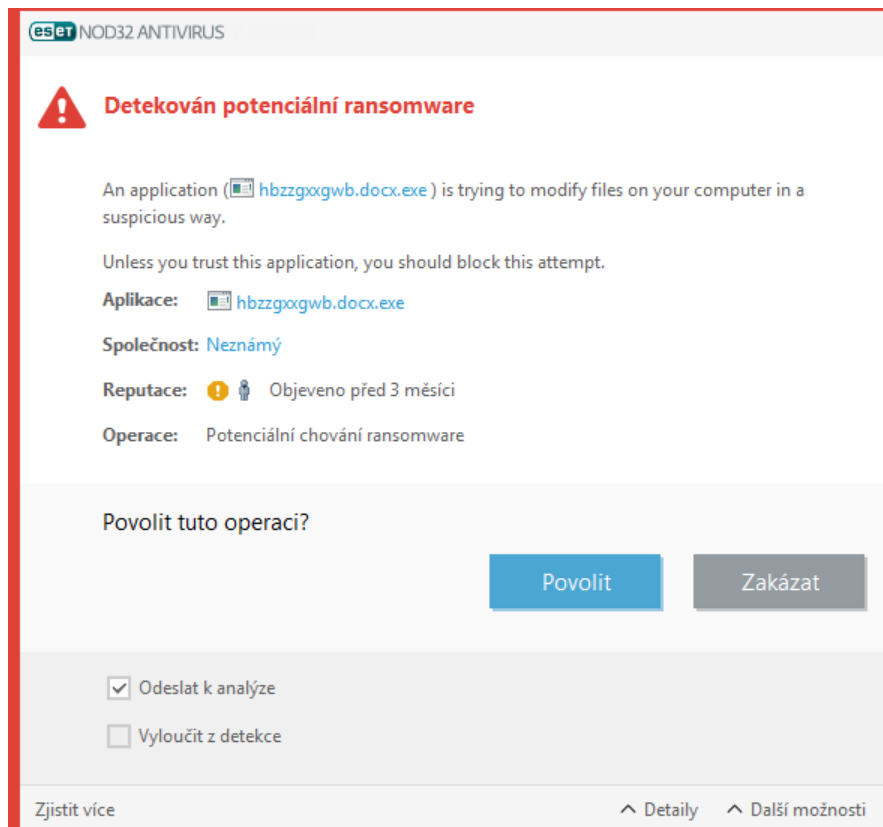


Pro ukončení zobrazování oznámení přepněte režim filtrování na **Automaticky** v [Rozšířených nastaveních](#) > **Detekční jádro > HIPS > Host Intrusion Prevention System (HIPS)**.



Detekován potenciální ransomware

Toto dialogové okno se zobrazí, pokud je detekována aplikace, jejíž chování je velmi podobné ransomware. Následně se rozhodněte, zda další běh aplikace chcete **povolit** nebo **zablokovat**.



Prostřednictvím tohoto dialogového okna můžete **odeslat vzorek do virové laboratoře k bližší analýze**, případně danou aplikaci **vyloučit z detekce**. Po kliknutí na možnost **Detaily** si zobrazíte konkrétní parametry detekce.

! Pro fungování [ochrany proti ransomware](#) je vyžadována aktivní technologie ESET LiveGrid®.

Správa HIPS pravidel

V tomto dialogovém okně naleznete uživatelsky a automaticky vytvořená pravidla modulu HIPS. Více informací o vytváření HIPS pravidel naleznete v kapitole [Úprava pravidla HIPS](#). Podívejte se rovněž do kapitoly [Obecné principy HIPS](#).

Sloupce

Pravidlo – uživatelský nebo automaticky zadaný název pravidla.

Zapnuto – deaktivujte tuto možnost, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Zdroje – pravidlo se uplatní, pouze pokud událost vyvolají dané aplikace.

Cíle – pravidlo se použije, pouze pokud se operace týká daného cíle (souboru, aplikace nebo záznamu v registru).

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do [protokolu HIPS](#).

Oznámit – pokud je spuštěna událost, zobrazí se v pravém dolním rohu obrazovky oznámení.

Ovládací prvky

Přidat – kliknutím vytvoříte nové pravidlo.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odstraníte vybraný záznam.

Priorita pravidel HIPS

Neexistují žádné možnosti nastavení priority pravidel HIPS pomocí tlačítek nahoru/dolů.

- Všechna pravidla mají stejnou prioritu
- Specifičtější pravidla mají vyšší prioritu (například pravidlo pro konkrétní aplikaci je nadřazeno pravidlu platnému pro všechny aplikace)
- Interně HIPS obsahuje několik předdefinovaných pravidel s nejvyšší prioritou, která nemůžete ovlivnit (například nemůžete přepsat Self-Defense pravidla)
- Vámi vytvořená pravidla, která mohou způsobit zamrznutí systému, se nebudou aplikovat (budou mít nejnižší prioritu)

Úprava pravidla HIPS

Nejprve si prosím přečtěte kapitolu [Správa HIPS pravidel](#).

Název pravidla – uživatelský nebo automaticky zadaný název pravidla.

Akce – pravidlo specifikuje (právě jednu) akci – **Povolit**, **Zablokovat**, **Dotázat se** – která se má provést, pokud jsou všechny podmínky splněny.

Operace ovlivní – vyberte typ operace, pro kterou má být pravidlo platné. Konkrétní pravidlo je možné použít pouze pro jeden typ operace nad vybraným cílem.

Zapnuto – deaktivujte tuto možnost pomocí přepínače, pokud chcete ponechat pravidlo v seznamu, ale nepoužívat ho.

Zapsat do protokolu – pokud aktivujete tuto možnost, při aplikování pravidla se informace zapíše do [protokolu HIPS](#).

Upozornit uživatele – při výskytu události se v pravém dolním rohu obrazovky zobrazí oznámení.

Pravidlo se skládá z částí, které definují podmínky, za kterých se pravidlo uplatní.

Zdrojové aplikace – pravidlo se uplatní, pouze pokud událost vyvolají **definované aplikace**. Pro vybrání **konkrétní aplikace** klikněte v rozbalovacím menu na **Přidat** a vyberte jednotlivé soubory nebo klikněte na možnost **Všechny aplikace** pro výběr všech.

Cílové soubory – pravidlo se uplatní pouze v případě, kdy operace náleží cíli. Pro vybrání **konkrétních souborů** klikněte v rozbalovacím menu na možnost **Přidat** a vyberte jednotlivé soubory nebo složky nebo klikněte na

Všechny soubory pro výběr všech.

Aplikace – pravidlo se uplatní, pouze pokud se operace provádí nad definovanými aplikacemi. Pro vybrání **konkrétní aplikace** klikněte v rozbalovacím menu na **Přidat** a vyberte jednotlivé soubory nebo složky nebo klikněte na možnost **Všechny aplikace** pro výběr všech.

Záznamy registru – pravidlo se uplatní, pouze pokud se operace provádí nad definovanými záznamy v registru. Pro vybrání konkrétních záznamů klikněte na tlačítko **Přidat** zadejte je ručně, případně po kliknutí na **Otevřít Editor registru** můžete přímo vybrat jednotlivé klíče z registru. Pro monitorování celého registru vyberte z rozbalovacího menu možnost **Všechny záznamy**.



Některé operace zvláštních pravidel předdefinovaných systémem HIPS nemohou být zablokovány a standardně jsou povoleny. HIPS nemonitoruje všechny systémové operace. HIPS monitoruje operace, které mohou být považovány za nebezpečné.

Popis důležitých operací:

Operace se soubory

- **Vymazat soubor** – aplikace žádá o povolení vymazat cílový soubor.
- **Zápis do souboru** – aplikace žádá o povolení zapisovat do cílového souboru.
- **Přímý přístup na disk** – aplikace se snaží číst nebo zapisovat na disk nestandardním způsobem, který obchází běžné procedury Windows. Výsledkem může být změna souboru bez použití příslušného pravidla. Tato operace může být způsobena škodlivým kódem, který se snaží vyhnout se detekci, zálohovacím programem, který kopíruje celý obsah pevného disku nebo správcem oddílů který reorganizuje diskové oddíly.
- **Nainstalovat globální hook** – volání funkce SetWindowsHookEx z MSDN knihovny pomocí dané aplikace.
- **Načíst ovladač** – instalace a načítání ovladače do systému.

Operace aplikace

- **Ladění jiné aplikace** – připojení debuggeru k procesu. Při debuggingu můžete sledovat a měnit chování aplikace a přistupovat k jejím datům.
- **Zachytávat události jiné aplikace** – zdrojová aplikace se pokouší zachytit události cílové aplikace (například pokud se keylogger snaží zachytit aktivitu webového prohlížeče).
- **Ukončit/přerušit jinou aplikaci** – pozastavení, obnovení nebo ukončení procesu (může být vyvoláno přímo ze Správce úloh nebo ze záložky Procesy).
- **Spustit novou aplikaci** – spuštění nové aplikace nebo procesu.
- **Změnit stav jiné aplikace** – zdrojová aplikace se pokouší zapisovat do paměti cílové aplikace, případně se snaží spustit kód pod jejím jménem. Tato funkce je užitečná pro ochranu důležité aplikace, pokud ji nastavíte jako cílovou aplikaci v pravidle, které blokuje tyto operace.

Operace se záznamy registru

- **Úprava nastavení spuštění** – všechny změny v nastavení, definující, které aplikace budou spouštěny při startu operačního systému Windows. Zobrazíte je například vyhledáním klíče Run v Editoru registru Windows.
- **Vymazání z registru** – vymazání klíče nebo hodnoty.
- **Přejmenování klíče registru** – přejmenování konkrétního klíče.
- **Úprava registru** – vytvoření nové hodnoty nebo změna existujících hodnot. Přesouvání dat v rámci datové struktury. Nastavení uživatelských nebo skupinových práv pro dané klíče registru.

Při zápisu cíle můžete použít zástupné znaky s jistými omezeními. Místo specifikování klíče můžete použít v cestě k registru * (hvězdičku) ve významu "libovolný jeden klíč". Například `HKEY_USERS*\software` může znamenat `HKEY_USER\default\software`, ale ne `HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\default\software`.
i `HKEY_LOCAL_MACHINE\system\ControlSet*` není platná cesta ke klíči registru. Cesta registru ukončená * má speciální význam, znamená "tento klíč nebo libovolný podklíč libovolně hluboko". U souborových cílů se dá používat hvězdička pouze tímto způsobem. U vyhodnocování platí, že vždy se hledá nejprve cíl, který popisuje danou cestu přesně, a až poté cíl, který ji popisuje zástupným znakem (*).

! Pokud vytvoříte příliš obecné pravidlo, program vás na to upozorní.

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

1. Zadejte název pravidla a z rozbalovacího menu **Akce** vyberte **Blokovat** (nebo **Dotázat se**, pokud se chcete při výskytu akce rozhodnout později).
2. Přepínačem aktivujte možnost **Upozornit uživatele** pro zobrazení oznámení při každém aplikování pravidla.
3. V části **Operace ovlivní** vyberte [alespoň jednu operaci](#), pro kterou má pravidlo platit.
4. Pokračujte kliknutím na tlačítko **Další**.
5. V dialogovém okně **Zdrojové aplikace** vyberte možnost **Konkrétní aplikace**. Tím zajistíte, že vámi vytvářené pravidlo bude platné pouze pro konkrétní aplikace.
6. Klikněte na tlačítko **Přidat a ...**. Výběr cesty k aplikaci potvrďte kliknutím na tlačítko **OK**. V případě potřeby přidejte více aplikací.
Příklad: `C:\Program Files (x86)\Untrusted application\application.exe`
7. Jako operaci vyberte **Zápis do souboru**.
8. V dalším kroku vyberte z rozbalovacího menu **Všechny soubory**. Tím zablokuje jakýkoli pokus definovaných aplikací o zápis do libovolného souboru.
9. Vytvoření nového pravidla potvrdíte kliknutím na tlačítko **OK**.

Nastavení pravidla HIPS



Název pravidla

Bez názvu

Akce

Povolit

Operace ovlivní

Cílové soubory



Aplikace



Záznamy registru



Zapnuto



Zaznamenávat od úrovně

Žádná

Upozornit uživatele



Zpět

Další

Zrušit

Přidat cestu k aplikaci/registru pro HIPS

Kliknutím na ... vyberte cestu k aplikaci. Pokud vyberete složku, všechny aplikace v této složce budou zahrnuty do daného pravidla.

Kliknutím na **Otevřít Editor registru** spustíte Editor registru Windows (regedit). Během přidávání zadejte správnou cestu do pole **Hodnota**.

Příklad cesty k souboru nebo v registru:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Aktualizace

Možnosti nastavení aktualizace jsou k dispozici v [Rozšířených nastaveních](#) > **Aktualizace**. Tato sekce vám poskytne informace o aktualizacích serverech a datech pro tyto servery.

Aktualizace

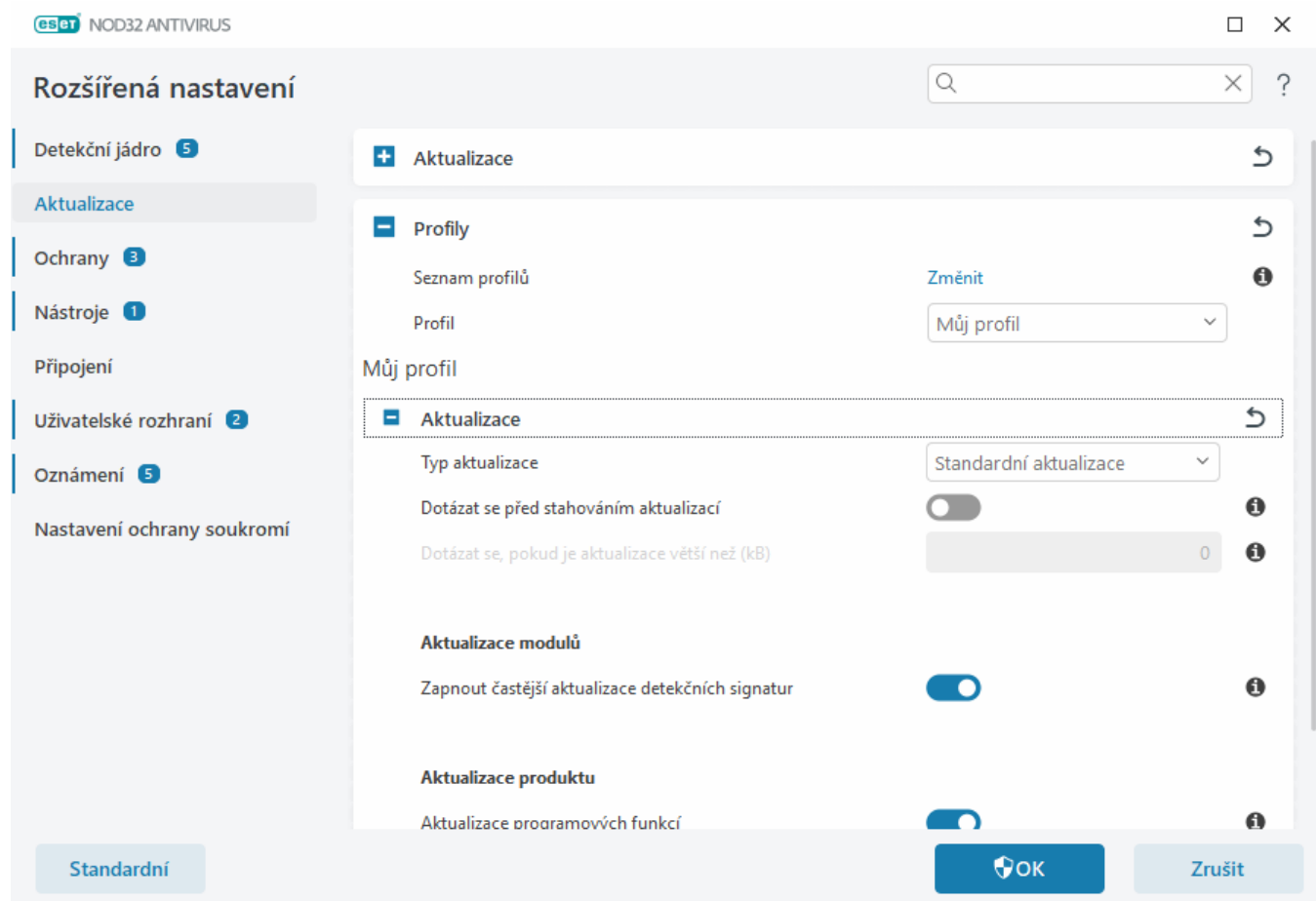
Aktuálně používaný aktualizací profil se zobrazuje v rozbalovacím menu **Vyberte výchozí profil aktualizace**.

Pro vytvoření nového profilu přejděte do kapitoly [Profily aktualizace](#).

Pokud se při pokusu o stažení aktualizací detekčního jádra nebo modulu vyskytnou potíže, klikněte na **Vyčistit** vedle položky **Vyprázdnit aktualizací cache** a vymažte dočasné soubory aktualizací.

Záloha modulů

Pokud máte podezření, že nová verze detekčního jádra je nestabilní nebo poškozená, můžete se [vrátit ke starší verzi](#) modulů a na stanovený časový interval zakázat její aktualizaci.



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

Profily

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

V rozbalovacím menu **Aktuální profil** se vždy zobrazuje aktuálně vybraný profil. Standardně je vybrán profil s názvem **Můj profil**. Pro vytvoření nového klikněte na **Změnit** vedle položky **Seznam profilů**, následně klikněte na tlačítko **Přidat** a zadejte **Název profilu**.

Aktualizace

Jako **Typ aktualizace** je ve výchozím nastavení vybrána možnost **Standardní aktualizace**. Tím je zajištěno automatické stahování aktualizací ze serverů společnosti ESET. **Předběžné aktualizace** jsou aktualizace, které prošly důkladným interním testováním a budou brzy dostupné široké veřejnosti. Při vybrání této možnosti získáte v předstihu přístup k novějším opravám a metodám detekce škodlivého kódu. Protože předběžné aktualizace nereprezentují finální kvalitu, neměli byste je instalovat na produkční stroje a pracovní stanice, u kterých je vyžadována stabilita a dostupnost.

Dotázat se před stahováním aktualizací – zapne zobrazování oznámení, ve kterém lze zvolit, zda aktualizaci chcete přijmout nebo odmítnout.

Dotázat se, pokud je aktualizace větší než (kB) – program zobrazí potvrzovací dialog, pokud je velikost souboru aktualizace větší než zadaná hodnota. Pokud je velikost aktualizacího souboru nastavena na 0 kB, program zobrazí potvrzovací dialog vždy.

Aktualizace modulů

Zapnout častější aktualizace detekčních signatur – zapnutím této možnosti se budou detekční signatury aktualizovat v kratších intervalech. Deaktivace tohoto nastavení může mít negativní dopad na rychlost detekce.

Aktualizace produktu

Aktualizace programových funkcí – automaticky instaluje nové verze ESET NOD32 Antivirus.

Možnosti připojení

Jak používat proxy server ke stahování aktualizací si prostudujte v kapitole [Možnosti připojení](#).

Obnovení předchozí verze modulů

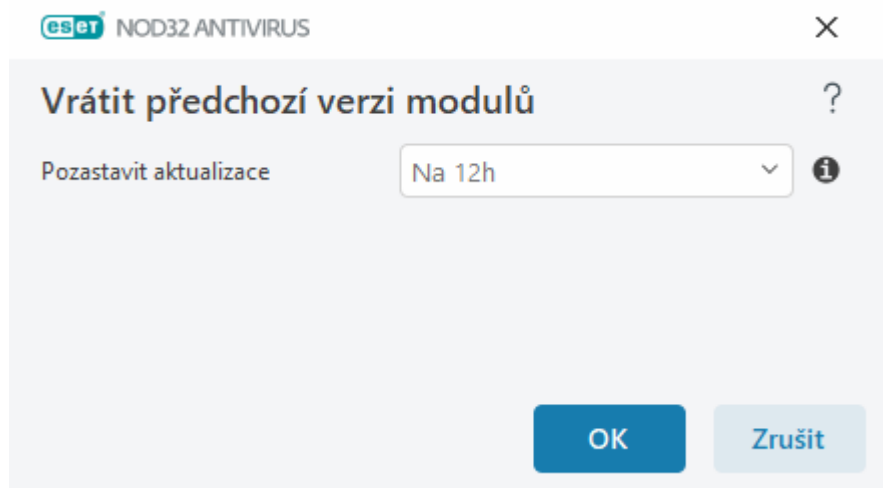
Pokud máte podezření, že nová verze detekčního jádra je nestabilní nebo poškozená, můžete se vrátit ke starší verzi a na stanovený časový interval zakázat jejich aktualizaci. Případně můžete povolit dříve zakázané aktualizace, pokud jste je odložili na neomezeně dlouhou dobu.

ESET NOD32 Antivirus zálohuje detekční jádro a programové moduly pro případ, že by bylo potřeba se vrátit ke starší verzi. Aby se obrazy, tzv. snapshoty modulů, vytvářely, ponechte možnost **Vytvářet zálohu modulů** aktivní. Po jejím **zapnutí** se první záloha (snapshot) vytvoří v průběhu příští aktualizace. Další záloha se následně vytvoří po uplynutí 48 hodin. **Počet vytvářených záloh** určuje počet obrazů detekčního jádra uložených na lokálním disku počítače.



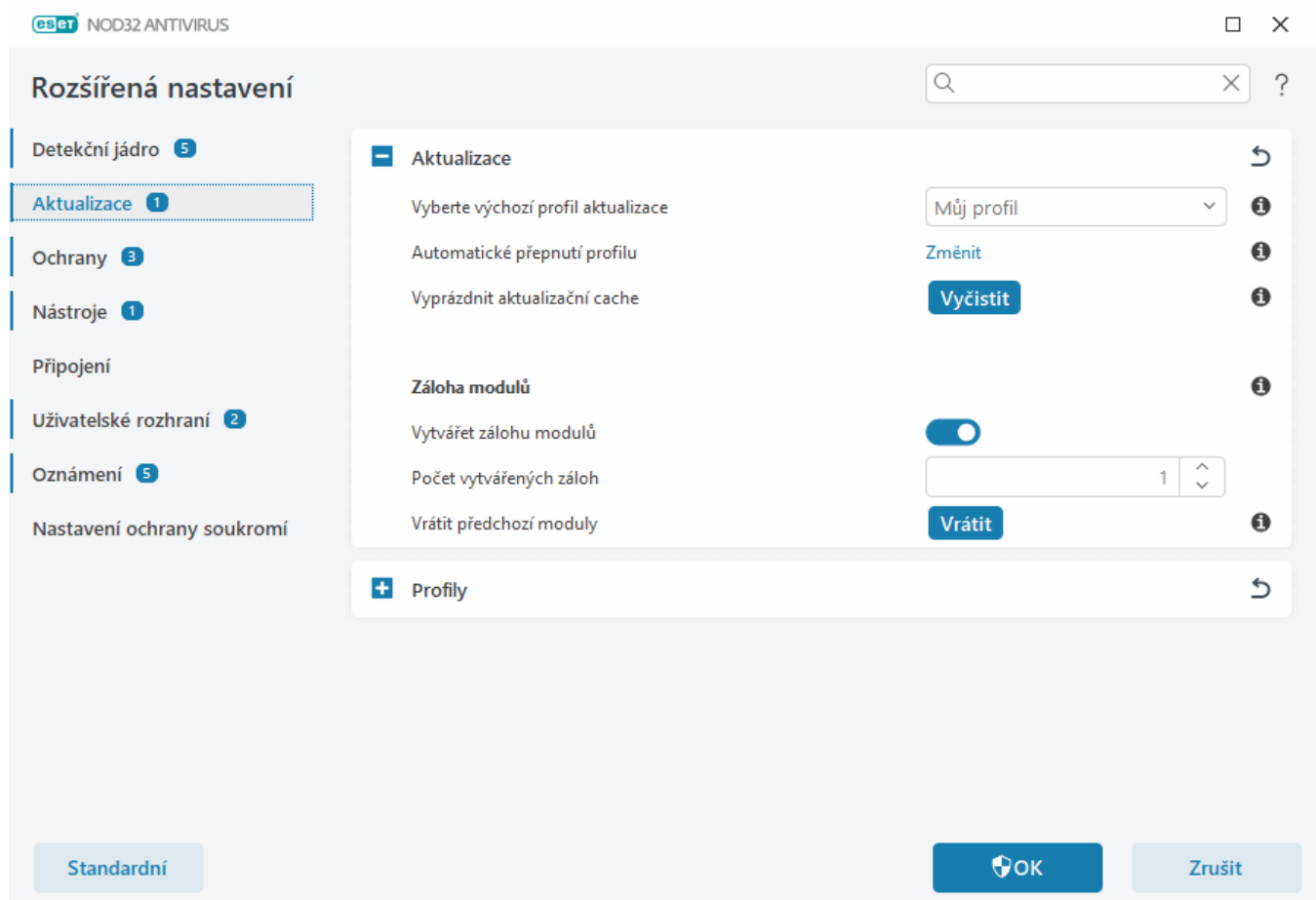
Při dosažení maximálního počtu vytvářených záloh (například tří), dojde každých 48 hodin k nahrazení nejstarší zálohy novou. ESET NOD32 Antivirus se při obnovení předchozí verze detekčního jádra a programových modulů vrátí vždy k nejstarší verzi.

Pokud kliknete na tlačítko **Vrátit v Rozšířených nastaveních** > **Aktualizace** > **Aktualizace** vyberte z rozbalovacího menu **Časový interval**, na jak dlouho chcete aktualizaci detekčního jádra a programových modulů pozastavit.



Možnost **Do odvolání** vyberte v případě, kdy chcete aktualizaci modulů obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

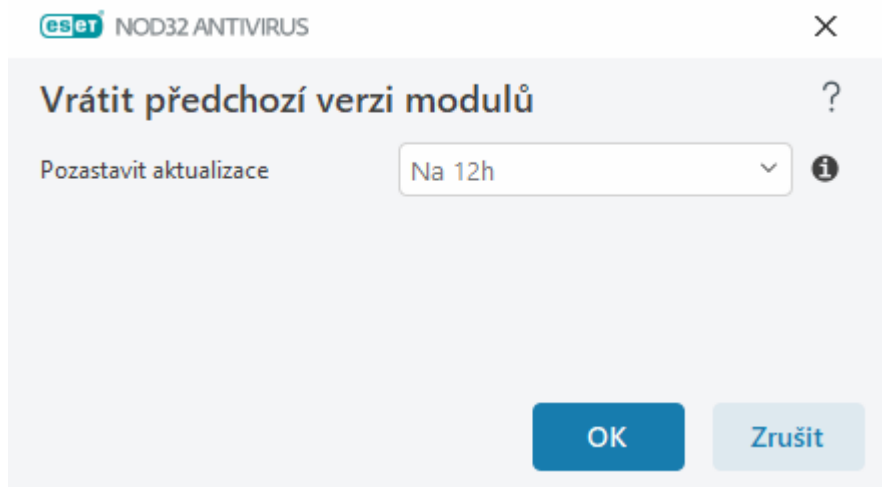
Po obnovení předchozí verze modulů se tlačítko **Vrátit** změní, a bude sloužit pro akci **Povolit aktualizace**. Aktualizace se přeruší na dobu definovanou v dialogovém okně **Pozastavit aktualizace na**. Ze zálohy se obnoví nejstarší verze detekčního jádra a programových modulů uložená v souborovém systému počítače.



Nejnovější verze detekčního jádra má číslo 22700. Na pevném disku počítače jsou uloženy obrazy detekčního jádra 22698 a 22696. Všimněte si, že verze 22697 není k dispozici. Počítač byl totiž delší dobu vypnutý, proto byla stažena novější verze modulů. Pokud jste jako **Počet vytvářených záloh** nastavili číslo 2, po **navrácení změn** se obnoví detekční jádro (i programové moduly) s číslem 22696. Tento proces může chvíli trvat. Pro ověření, zda došlo k obnovení starší verze přejděte v hlavním okně programu na záložku [Aktualizace](#).

Interval pro obnovení předchozí verze modulů

Pokud kliknete na tlačítko **Vrátit** v [Rozšířených nastaveních](#) > **Aktualizace** > **Aktualizace** vyberte z rozbalovacího menu **Časový interval**, na jak dlouho chcete aktualizaci detekčního jádra a programových modulů pozastavit.



Možnost **Do odvolání** vyberte v případě, kdy chcete aktualizaci modulů obnovit ručně. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Aktualizace produktu

V části **Aktualizace produktu** můžete povolit automatickou instalaci nových funkcí produktu ve chvíli, kdy jsou dostupné.

Aktualizace programových funkcí přináší nové funkce, nebo upravují již existující z předchozích verzí. Aktualizace může probíhat automaticky bez interakce uživatele, nebo po jejím odsouhlasení. Po instalaci aktualizace programové funkce může být zapotřebí restart počítače.

Aktualizace programových funkcí – pokud je tato možnost aktivní, bude docházet k automatické aktualizaci funkcí produktu.

Možnosti připojení

Chcete-li získat přístup k možnostem nastavení proxy serveru pro konkrétní profil aktualizace, otevřete [Rozšířená nastavení](#) > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení**. V rozbalovacím menu **Režim proxy** jsou dostupné následující možnosti:

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

Vybráním možnosti **Použít globální nastavení proxy serveru** se použijí veškerá [nastavení proxy serveru](#) definovaná v [Rozšířených nastaveních](#) > **Připojení** > **Proxy server**.

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

Možnost **Připojení prostřednictvím proxy serveru** vyberte v případě, že:

- Pro aktualizaci ESET NOD32 Antivirus se používá jiný proxy server než ten, který je definován v [Rozšířených nastaveních](#) > **Připojení**. Při takové konfiguraci definujte nový proxy server zadáním jeho adresy do pole **Proxy server**, komunikačního portu (standardně 3128), **uživatelského jména** a **hesla** pro přístup k proxy serveru, je-li to potřeba.
- Nastavení proxy serveru není nastaveno globálně, ale ESET NOD32 Antivirus se připojí k proxy serveru z důvodu aktualizace.
- Počítač je připojen k internetu pomocí proxy serveru. Nastavení bylo v průběhu instalace programu převzato z Internet Exploreru, ale v průběhu času došlo ke změně nastavení proxy serveru (například z důvodu přechodu k jinému poskytovateli 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**, PRODUCTNAME automaticky zkusí připojení k aktualizacím serverům ESET bez použití proxy. Tuto možnost je vhodné nastavit mobilním uživatelům.



Uživatelské jméno a Heslo v této části jsou pro proxy server specifické. Tato pole vyplňte pouze v případě, kdy jsou vyžadovány údaje pro přístup k proxy serveru. Stává se tak v situaci, kdy pro přístup k internetu prostřednictvím proxy serveru je nutné zadat heslo.

Ochrany

Ochrany chrání systém před útoky škodlivého kódu tím, že kontroluje komunikaci se soubory, e-maily a internetem. Například pokud je detekován objekt klasifikovaný jako malware, zahájí se akce pro vyřešení situace. Škodlivý kód může být zablokován a následně léčen, odstraněn nebo přesunut do karantény.

Chcete-li podrobně nakonfigurovat ochrany, otevřete [Rozšířená nastavení](#) > **Ochrany**.



Změny v Ochránách by měl provádět pouze zkušený uživatel. Chybnou úpravou nastavení se může snížit úroveň ochrany.

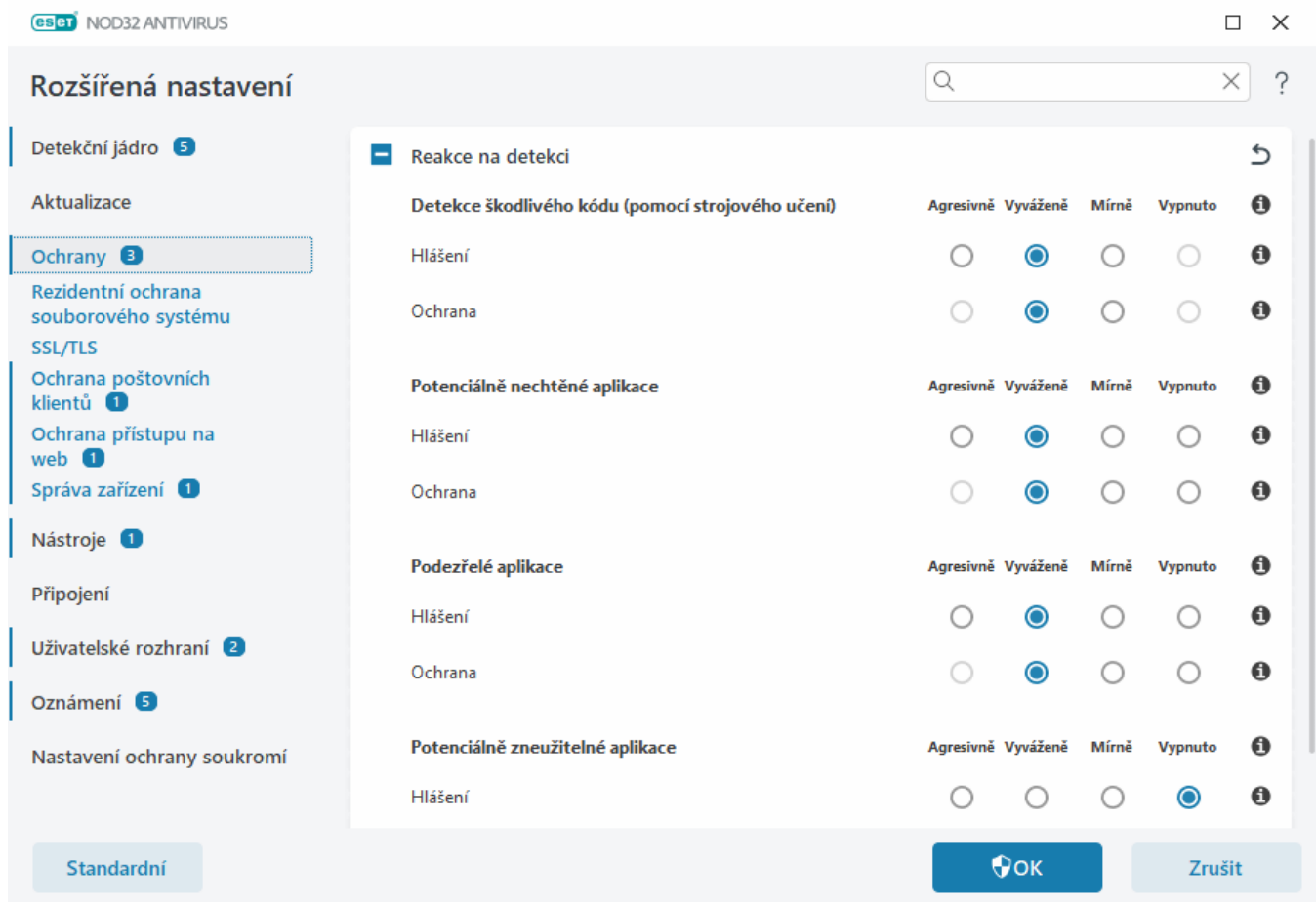
V této kapitole naleznete:

- [Reakce na detekci](#)
- [Nastavení hlášení](#)
- [Nastavení ochrany](#)

Reakce na detekci

Reakce na detekci umožňují nastavit úroveň hlášení a ochrany pro následující kategorie:

- **Detekce škodlivého kódu (pomocí strojového učení)** – počítačový virus je část škodlivého kódu, která je připojena k existujícím souborům v počítači. Termín "virus" bývá často vykládán nesprávně. Vhodnějším výrazem je "malware" (škodlivý software). Detekce malwaru zajišťuje modul detekčního jádra v kombinaci s komponentou strojového učení. Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).
- **Potenciálně nechtěné aplikace** – grayware (neboli PUA – potentially unwanted application) představují širokou škálu aplikací, které nejsou jednoznačně škodlivé jako viry nebo trojské koně. Mohou však instalovat nechtěný software, měnit chování vašeho zařízení, provádět neočekávané operace, případně akce bez vědomí uživatele. Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).
- Mezi **potenciálně podezřelé aplikace** řadíme rovněž programy, které jsou komprimovány pomocí [packerů](#) nebo protektorů. Tuto metodu často využívají tvůrci škodlivého kódu, aby se vyhnuli detekci ze strany antiviru.
- **Potenciálně zneužitelné aplikace** – legitimní komerční aplikace, které mohou být zneužity ke škodlivé činnosti. Příkladem mohou být programy pro vzdálené připojení, aplikace k odšifrování hesel a keyloggery (programy, které zaznamenávají uživatelem zadané znaky na klávesnici). Více informací o tomto typu aplikací naleznete ve [slovníku pojmů](#).



Vylepšená ochrana

- i** Pokročilé strojové učení je nyní funguje jako pokročilá vrstva ochrany a vylepšuje tak detekci. Pro více informací o tomto typu ochranu se podívejte do [slovníku pojmů](#).

Nastavení hlášení

Při výskytu detekce (například při objevení hrozby klasifikované jako malware) se informace zapíše do [Detekčního protokolu](#) a může se zobrazit [Oznámení na pracovní ploše](#) (pokud je to v produktu ESET NOD32 Antivirus povoleno).

Práh (úroveň) hlášení můžete konfigurovat jednotlivě pro každou kategorii (dále jen "KATEGORIE"):

1. Detekce škodlivého kódu
2. Potenciálně nechtěné aplikace
3. Potenciálně zneužitelné aplikace
4. Podezřelé aplikace

Hlášení zajišťuje detekční jádro včetně komponenty strojového učení. Pro hlášení můžete nastavit vyšší práh, než je aktuální úroveň [ochrany](#). Tato nastavení nemají vliv na blokování, [léčení](#) nebo odstraňování [objektů](#).

Před změnou prahu (úrovně) pro danou KATEGORII si přečtěte níže uvedené informace:

Práh	Vysvětlení
Agresivně	Hlášení z dané KATEGORIE je nakonfigurováno na nejvyšší citlivost. Hlášeno bude větší množství detekcí. V agresivním nastavení může docházet k chybné identifikaci některých objektů patřících do KATEGORIE.
Vyváženě	Hlášení z dané KATEGORIE je nakonfigurováno jako vyvážené. Toto nastavení je optimalizováno s ohledem na výkon, přesnost detekce a množství falešných poplachů.
Mírně	Hlášení z dané KATEGORIE je nakonfigurováno tak, aby se minimalizoval počet falešných poplachů při zachování dostatečné úrovně zabezpečení. Objekty budou hlášeny pouze v případě vysoké pravděpodobnosti a shody chování odpovídající KATEGORII.
Vypnuto	Hlášení pro danou KATEGORII není aktivní a detekce tohoto typu nebudou zachytávány, hlášeny ani léčeny. V důsledku tohoto nastavení bude vypnuta ochrana před tímto typem detekce. V rámci hlášení malware není k dispozici možnost Vypnuto. Tato hodnota je výchozí pro potenciálně zneužitelné aplikace.

✓ [Dostupnost modulů ochrany produktu ESET NOD32 Antivirus](#)

Níže uvádíme dostupnost jednotlivých prahů KATEGORIÍ (zapnuto nebo vypnuto) v modulech ochrany:

	Agresivně	Vyváženě	Mírně	Vypnuto*
Modul pokročilého strojového učení	✓ (agresivní režim)	✓ (konzervativní režim)	X	X
Modul detekčního jádra	✓	✓	✓	X
Ostatní moduly ochrany	✓	✓	✓	X

** Nedoporučeno.

✓ [Jak zjistím verzi produktu, programových modulů a data sestavení?](#)

1. V hlavním okně programu klikněte na **Nápověda a podpora > O programu ESET NOD32 Antivirus**.
2. V zobrazeném dialogovém okně **O programu** se na prvním řádku zobrazuje číslo verze vámi používaného produktu ESET.
3. Pro zobrazení informací o jednotlivých modulech klikněte na tlačítko **Nainstalované programové komponenty**.

Důležité poznámky

Při konfiguraci vhodných prahů ve svém prostředí vezměte v potaz následující informace:

- Možnost **Vyváženě** je doporučena pro většinu situací.
- Čím vyšší práh nastavíte, tím vyšší bude počet detekcí. Zároveň se zvedne pravděpodobnost výskytu falešně detekovaných objektů.
- Z pohledu reálného světa není možné zaručit 100% úspěšnost detekce, stejně tak nulovou pravděpodobnost, že bude čistý objekt označen jako malware.
- Pro zajištění maximální rovnováhy mezi výkonem, přesností detekce a počtem falešně detekovaných objektů [udržuje ESET NOD32 Antivirus a jeho moduly aktuální](#).

Nastavení ochrany

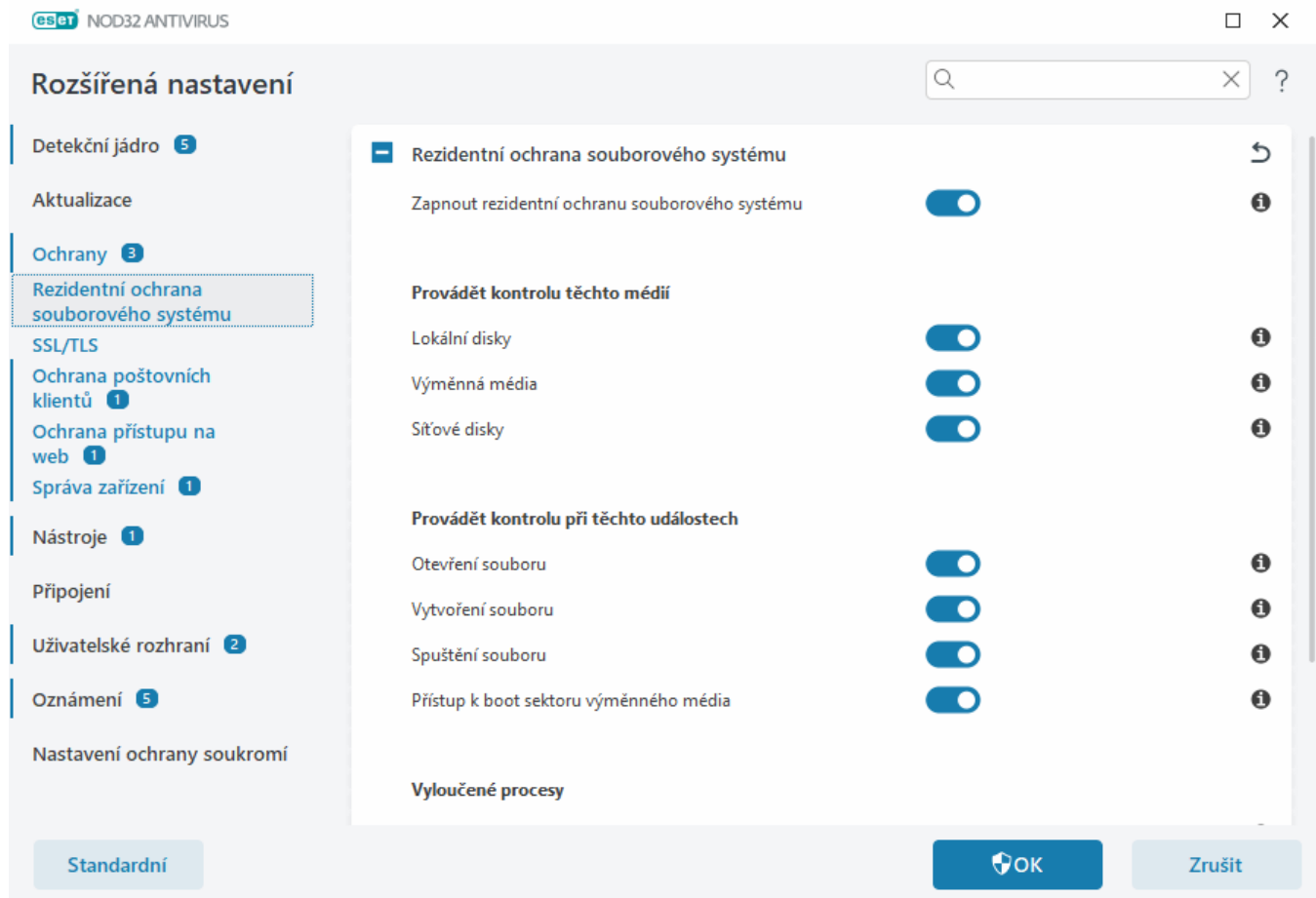
Pokud je detekovaný objekt klasifikován jako KATEGORIE, program jej zablokuje, a následně [vyléčí](#), odstraní nebo přesune do [karantény](#).

Před změnou prahu (úrovně) pro danou KATEGORII si přečtěte níže uvedené informace:

Práh	Vysvětlení
Agresivně	Detekce zachycené s úrovní Agresivně (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení). Toto nastavení je doporučeno, pokud na všech koncových zařízeních proběhla kontrola s agresivním nastavením a chybně detekované objekty jste přidali do detekčních výjimek.
Vyváženě	Detekce zachycené s úrovní Vyváženě (nebo nižší) jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Mírně	Detekce zachycené s úrovní Opatrně jsou blokovány a automaticky se provádí definovaná akce (například léčení).
Vypnuto	Toto nastavení je užitečné pro identifikaci a vytvoření výjimek na falešně detekované objekty. V rámci ochrany před malwarem není k dispozici možnost Vypnuto. Tato hodnota je výchozí pro potenciálně zneužitelné aplikace.

Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému vyhledává škodlivý kód ve všech souborech v systému, které se otevírají, vytvářejí nebo spouštějí.



Standardně se rezidentní ochrana spustí vždy při startu operačního systému. Nedoporučujeme vypínat **Zapnout rezidentní ochranu souborového systému** v [Rozšířených nastaveních](#) > **Ochrany** > **Rezidentní ochrana souborového systému** > **Rezidentní ochrana souborového systému**.

Kontrola médií

Standardně je nastavena kontrola všech typů médií:

- **Lokální disky** – kontroluje všechny systémové a lokální pevné disky (například `C:\`, `D:\`).
- **Výměnná média** – kontroluje CD, DVD, USB úložiště, paměťové karty, atp.
- **Síťové disky** – kontroluje všechny namapované síťové jednotky (například kdy pod písmenem `H:` máte `\\store04`), stejně tak síťová umístění přímo (například `\\store08`).

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

Kontrola při událostech

Standardně jsou kontrolovány všechny soubory, jakmile jsou otevřené, vytvořené nebo spuštěné. Tato nastavení doporučujeme ponechat pro zajištění maximální možné ochrany počítače:

- **Otevření souboru** – zapne/vypne kontrolu otevíraných souborů.
- **Vytvoření souboru** – zapne/vypne kontrolu vytvářených nebo modifikovaných souborů.

- **Spuštění souboru** – zapne/vypne kontrolu spouštěných souborů.
- **Přístup na boot sektor výměnného zařízení** – pokud obsahuje vložené výměnné médium boot sektor, po připojení média do zařízení dojde automaticky ke kontrole sektoru. Tato možnost nezapíná kontrolu souborů na výměnných médiích. Nastavení kontroly na výměnných médiích se nachází v části **Provádět kontrolu těchto médií > Výměnná média**. Aby kontrola boot sektoru výměnných médií fungovala správně, ponechte v ThreatSense zapnutou funkci **Boot sektory/UEFI**.

Vyloučené procesy

Viz [Vyloučené procesy](#).

ThreatSense

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí jako je přístup k souboru. Při kontrole jsou používány detekční metody technologie **ThreatSense** (ty jsou popsány v kapitole [Nastavení skenovacího jádra ThreatSense](#)). Chování rezidentní ochrany souborového systému lze nakonfigurovat tak, aby se s nově vytvořenými soubory zacházelo jinak než s existujícími soubory. Například, pro nově vytvářené soubory můžete nastavit hlubší úroveň kontroly.

Pro zajištění minimálních systémových nároků, nejsou již dříve kontrolované soubory znovu kontrolovány (pokud nebyly změněny). Soubory jsou opět kontrolovány pouze po každé aktualizaci detekčních modulů. Toto chování můžete přizpůsobit pomocí **Smart optimalizace**. Pokud je tato funkce zakázána, všechny soubory jsou kontrolovány vždy, když se k nim přistupuje. Chcete-li toto nastavení upravit, otevřete [Rozšířená nastavení > Ochrany > Rezidentní ochrana souborového systému](#). Klikněte na **ThreatSense > Ostatní** a aktivujte nebo vypněte možnost **Používat Smart optimalizaci**.

Rezidentní ochrana souborového systému také umožňuje konfigurovat [Další parametry ThreatSense](#).

Vyloučené procesy

Pomocí této funkce vyloučíte z Rezidentní ochrany souborového systému činnost konkrétních procesů. V případě obnovy dedikovaných serverů (aplikačních, souborových atd.) ze zálohy do funkčního stavu hraje kritickou roli čas. Při navýšení rychlosti zálohování, zajištění integrity dat a dostupnosti služeb jsou některá zálohovací řešení technicky v konfliktu s antivirovou ochranou souborového systému. Jediným řešením pro zabránění konfliktu bývá deaktivace anti-malware řešení. Vyloučením činnosti konkrétních procesů (například zálohovacího agenta) z kontroly je veškerá jejich činnost ignorována a považována za důvěryhodnou, čímž je minimalizován vliv na celý průběh operace (například zálohování). Při vytváření výjimek však buďte obezřetní. Při přístupu zálohovacího agenta k infikovanému souboru nedojde k detekci a hlášení hrozby. Z tohoto důvodu je možné výjimky vytvářet pouze z rezidentní ochrany souborového systému.



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

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

Spustitelné soubory můžete přidat do seznamu vyloučených procesů v [Rozšířených nastaveních > Ochrany > Rezidentní ochrana souborového systému > Rezidentní ochrana souborového systému > Vyloučené procesy](#).

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

- ✓ Kliknutím na **Změnit** si otevřete správce **Výjimek**, kde pomocí tlačítka **Přidat** a použitím průzkumníka vyberete spustitelný soubor (například *Backup-tool.exe*), který chcete vyloučit z kontroly. Po přidání .exe souboru na seznam výjimek přestane ESET NOD32 Antivirus monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

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

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

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

Přidání a úprava výjimek pro procesy

Kliknutím na tlačítko **Přidat** můžete v tomto dialogovém okně vytvořit v detekčním jádře výjimku na činnost procesu. Prostřednictvím těchto výjimek můžete minimalizovat možné konflikty a zvýšit výkon vyloučených aplikací, což povede ke zvýšení celkového výkonu operačního systému a jeho stabilitě. Výjimky na proces/aplikaci je možné vytvářet na spustitelné soubory (.exe).


- ✓ Kliknutím na ... vyberte cestu k aplikaci (například *C:\Program Files\Firefox\Firefox.exe*). Nezadávejte název aplikace. Po přidání .exe souboru na seznam výjimek přestane ESET NOD32 Antivirus monitorovat aktivity tohoto procesu a nebude kontrolovat souborové operace prováděné tímto procesem.

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

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

Kdy měnit nastavení rezidentní ochrany

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

Po instalaci ESET NOD32 Antivirus jsou veškerá nastavení optimalizována pro zajištění maximální bezpečnosti systému. Chcete-li obnovit výchozí nastavení, klikněte na  vedle položky v **Rozšířených nastaveních** > **Ochrany** > **Reakce na detekci**.

Ověření funkčnosti rezidentní ochrany

Pro ověření, zda je rezidentní ochrana funkční a detekuje malware, je možné použít bezpečný testovací soubor z webových stránek *www.eicar.com*. Jedná se o soubor, který je detekován všemi antivirovými programy. Byl

vytvořen společností EICAR (European Institute for Computer Antivirus Research) pro testování funkčnosti antivirových programů.

Soubor eicar je dostupný na adrese <http://www.eicar.org/download/eicar.com>.

Po zadání této URL adresy do prohlížeče by se měla objevit zpráva, že hrozba byla odstraněna.

Co dělat, když nefunguje rezidentní ochrana

V této části popisujeme problémové stavy, které mohou nastat při běhu rezidentní ochrany. Je zde také uvedeno jak postupovat při jejich řešení.

Rezidentní ochrana je vypnutá

Pokud uživatel nechtěně zakáže rezidentní ochranu, měli byste funkci znovu aktivovat. Opětovné zapnutí je možné v hlavním okně programu na záložce **Nastavení** po kliknutí na **Ochrana počítače > Rezidentní ochrana souborového systému**.

Pokud se rezidentní ochrana nespouští při startu operačního systému, pravděpodobně byla vypnuta možnost **Zapnout rezidentní ochranu souborového systému**. Chcete-li se ujistit, že je tato možnost povolena, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

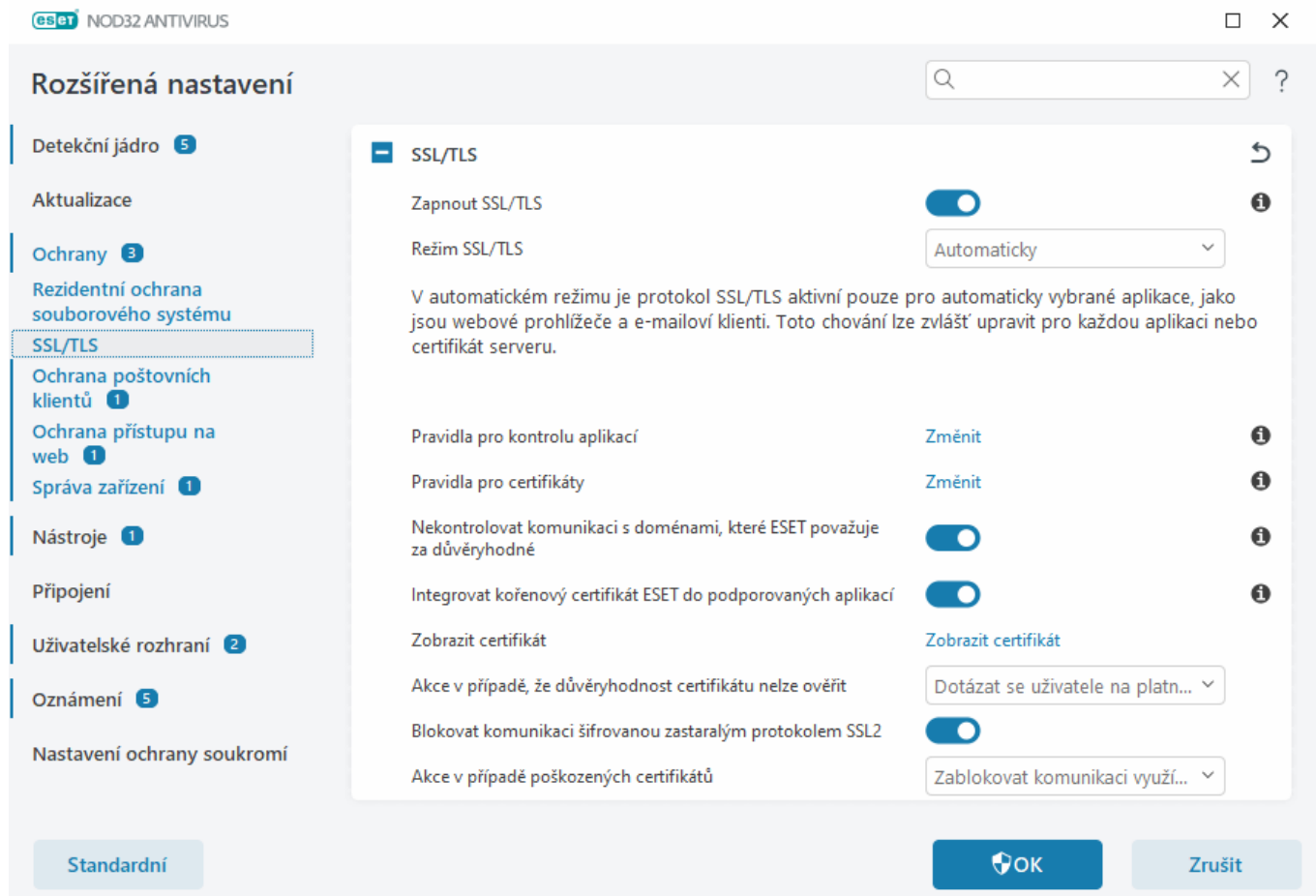
Ujistěte se, zda nemáte nainstalovaný další bezpečnostní program. Pokud jsou na zařízení nainstalované dva bezpečnostními programy, může mezi nimi docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému ani po aktivování možnosti **Zapnout rezidentní ochranu souborového systému**, zřejmě dochází ke konfliktu s jiným programem. Pokud chcete problém vyřešit, [vytvořte ESET SysInspector protokol a odešlete jej k analýze technické podpoře ESET](#).

SSL/TLS

ESET NOD32 Antivirus může kontrolovat komunikační hrozby, které používají SSL protokol. Filtrování můžete přizpůsobit podle toho, zda je certifikát využívaný danou SSL komunikací důvěryhodný, neznámý, nebo je zařazen na seznamu certifikátů, pro které se nebude vykonávat kontrola obsahu v protokolu SSL. Chcete-li upravit nastavení SSL/TLS, otevřete [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS**.



Zapněte SSL/TLS – jestliže je vypnuto, ESET NOD32 Antivirus nebude kontrolovat komunikaci přes SSL/TLS.

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

Režim filtrování	Popis
Automaticky	Výchozí režim, ve kterém je kontrolována pouze komunikace vybraných aplikací, jako jsou webové prohlížeče a poštovní klienti. Můžete jej přepsat výběrem aplikací, u kterých se komunikace kontroluje.
Interaktivní	Při přístupu k nové stránce zabezpečené protokolem SSL (s neznámým certifikátem) se zobrazí dialogové okno s výběrem akce. V tomto režimu můžete vytvořit seznam SSL certifikátů / aplikací, které chcete vyloučit z kontroly.
Administrátorský režim	Tuto možnost vyberte, pokud chcete kontrolovat veškerou komunikaci zabezpečenou protokolem SSL kromě komunikace chráněné certifikáty vyloučených z kontroly. Při navázání komunikace využívající zatím neznámý certifikát, který je důvěryhodně podepsán, nebudete upozorněni a komunikace bude automaticky filtrována. Při přístupu k serveru s nedůvěryhodným certifikátem označeným jako důvěryhodný (je v seznamu důvěryhodných certifikátů) je komunikace se serverem povolena a obsah komunikačního kanálu je filtrován.

Pravidla pro kontrolu aplikací – umožňují přizpůsobit chování ESET NOD32 Antivirus pro konkrétní aplikace.

Pravidla pro certifikáty – umožňují přizpůsobit chování ESET NOD32 Antivirus pro konkrétní SSL certifikáty.

Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné – pokud je tato volba povolena, bude komunikace s důvěryhodnými doménami vyloučena z kontroly. Vestavěný seznam povolených adres spravovaný společností ESET určuje důvěryhodnost domény.

Integrovat kořenový certifikát ESET do podporovaných aplikací – aby SSL komunikace správně fungovala ve vašich prohlížečích a e-mailových klientech, je nezbytné, aby byl kořenový certifikát společnosti ESET přidán do seznamu známých kořenových certifikátů (vydavatelů). Pokud je tato možnost zapnutá, ESET NOD32 Antivirus automaticky přidá certifikát ESET SSL Filter CA do známých prohlížečů ve vašem počítači (např. do prohlížeče Opera). Do prohlížečů využívajících systémové úložiště kořenových certifikátů se certifikát přidá automaticky. Např. Firefox je automaticky nastaven tak, aby důvěřoval kořenovým autoritám nacházejícím se v systémovém úložišti certifikátů.

V případě nepodporovaných prohlížečů certifikát exportujte pomocí tlačítka **Zobrazit certifikát > Detaily > Kopírovat do souboru** a následně jej ručně importujte do prohlížeče.

Akce v případě, že důvěryhodnost certifikátu nelze ověřit – v některých případech nelze certifikát webové stránky ověřit pomocí TRCA (Trusted Root Certification Authorities), například vypršela platnost certifikátu, certifikát není důvěryhodný, certifikát není platný pro danou doménu nebo podpis, který lze zpracovat, ale nepodepisuje správně. Legitimní webové stránky vždy používají důvěryhodné certifikáty. Pokud je neposkytují, může to znamenat, že útočník dešifruje vaši komunikaci nebo že webové stránky mají technické potíže.

Pokud vyberete možnost **Dotázat se uživatele na platnost certifikátu** (ve výchozím nastavení je vybrána), při navázání šifrované komunikace se zobrazí okno s výběrem akce. V zobrazeném dialogovém okně pro výběr akce můžete certifikát označit jako důvěryhodný nebo vyloučený. Pokud se certifikát nenachází v TRCA, okno bude červené. V opačném případě bude okno zelené.

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

Blokovat komunikaci šifrovanou zastaralým protokolem SSL2 – komunikace pomocí starší verze protokolu SSL bude automaticky blokována.

Akce v případě poškozených certifikátů – poškozený certifikát znamená, že certifikát používá formát, který ESET NOD32 Antivirus nerozpoznává, nebo byl přijat poškozený (například přepsaný náhodnými daty). V tomto případě doporučujeme ponechat zvolenou možnost **Zakázat komunikaci využívající daný certifikát**. Pokud vyberete **Dotázat se uživatele na platnost certifikátů**, uživatel bude vyzván k výběru akce po navázání šifrované komunikace.

Názorné příklady

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

- [Upozornění na certifikát v produktu ESET](#)
- [Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"](#)

Pravidla pro kontrolu aplikací

Pomocí **Pravidel pro kontrolu aplikací** můžete přizpůsobit chování ESET NOD32 Antivirus u konkrétních aplikací a zapamatovat si vybrané akce, pokud je **Režim filtrování protokolu SSL/TLS** nastaven v **Interaktivním režimu**. Seznam lze zobrazit a upravit v části [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS** > **Pravidla pro kontrolu aplikací** > **Změnit**.

Okno **Pravidla pro kontrolu aplikací** se skládá z:

Sloupce

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

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

Ovládací prvky

Přidat – kliknutím přidáte filtrovanou aplikaci.

Změnit – vyberte aplikaci, kterou chcete konfigurovat a klikněte na tlačítko **Změnit**.

Odstranit – vyberte aplikaci, kterou chcete odstranit a klikněte na tlačítko **Odstranit**.

Importovat/Exportovat – seznam aplikací můžete importovat ze souboru, případně si jej a uložit pro budoucí použití.

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

Pravidla pro certifikáty

Pravidla pro certifikáty lze použít k přizpůsobení chování ESET NOD32 Antivirus pro konkrétní certifikáty SSL a k zapamatování akcí zvolených v režimu **SSL/TLS** v **interaktivním režimu**. Seznam lze zobrazit a upravit v části [Rozšířená nastavení](#) > **Ochrany** > **SSL/TLS** > **Pravidla pro certifikáty** > **Změnit**.

Okno **Pravidla pro certifikáty** se skládá z:

Sloupce

Název – název certifikátu.

Vydavatel certifikátu – jméno autora certifikátu.

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

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

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

Ovládací prvky

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

Změnit – vyberte certifikát, který chcete konfigurovat a klikněte na **Změnit**.

Odstranit – vyberte certifikát, který chcete smazat a klikněte na tlačítko **Odstranit**.

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

Šifrovaná síťová komunikace

Pokud je váš systém nakonfigurován tak, aby kontroloval SSL/TLS, zobrazí se dialogové okno s výzvou k výběru akce ve dvou situacích:

Webová stránka používá neověřený nebo neplatný certifikát a ESET NOD32 Antivirus je nakonfigurován tak, aby se dotázal uživatele (standardně je tato možnost aktivní pro neověřené certifikáty, nikoli neplatné), zda chcete komunikaci **Povolit** nebo **Zakázat**. Pokud se certifikát nenachází v Trusted Root Certification Authorities store (TRCA), je považován za nedůvěryhodný.

Za druhé, pokud je **režim SSL/TLS** nastaven na **Interaktivní**, zobrazí se u každé webové stránky dialogové okno s dotazem, zda se má komunikace **Kontrolovat** nebo **Ignorovat**. Některé aplikace ověřují, že jejich SSL nikdo nemodifikuje ani nekontroluje, v takových případech musí ESET NOD32 Antivirus tuto komunikaci **ignorovat**, aby aplikace fungovala.

Názorné příklady

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



- [Upozornění na certifikát v produktu ESET](#)
- [Při přístupu na webovou stránku se zobrazí informace: "Šifrovaná síťová komunikace: nedůvěryhodný certifikát"](#)

V obou případech je dostupná možnost pro zapamatování vybrané akce. Zapamatované akce jsou uloženy v [Pravidlech pro certifikáty](#).

Ochrana poštovních klientů

Chcete-li nastavit Ochranu poštovních klientů, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** a vyberte jednu z následujících možností:

- [Ochrana transportu zpráv](#)
- [Ochrana poštovní schránky](#)
- [ThreatSense](#)

Ochrana transportu zpráv

POP3(S) a IMAP(S) jsou nejrozšířenější protokoly určené pro příjem e-mailové komunikace prostřednictvím poštovního klienta. Internet Message Access Protocol (IMAP) je další internetový protokol pro získávání pošty. IMAP má oproti POP3 několik výhod, například více klientů se může současně připojit ke stejné poštovní schránce a udržovat informace o stavu zprávy (např. zda byla zpráva přečtena, zda na ni bylo odpovězeno nebo byla odstraněna. Modul ochrany poskytující tuto kontrolu je automaticky zaveden při spuštění systému a je pak aktivní v paměti.

ESET NOD32 Antivirus poskytuje ochranu těchto protokolů bez ohledu na použitého e-mailového klienta a bez nutnosti změny konfigurace e-mailového klienta. Ve výchozím nastavení se kontroluje veškerá komunikace využívající protokoly POP3 a IMAP, bez ohledu na výchozí čísla portů POP3 / IMAP.

Protokol MAPI není kontrolován. Komunikace s Microsoft Exchange serverem však může být kontrolována po [integrování modulu](#) do e-mailového klienta, jako je Microsoft Outlook.

i ESET NOD32 Antivirus rovněž podporuje kontrolu protokolů IMAPS (585, 993) a POP3S (995), 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). Šifrovaná komunikace se standardně nekontroluje. Chcete-li zobrazit nastavení skeneru, otevřete [Rozšířená nastavení](#) > **Ochrany** > [SSL/TLS](#).

Chcete-li nakonfigurovat ochranu přenosu pošty, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana transportu zpráv**.

Povolit ochranu transportu zpráv – pokud je tato ochrana povolena, bude ESET NOD32 Antivirus kontrolovat poštovní komunikaci.

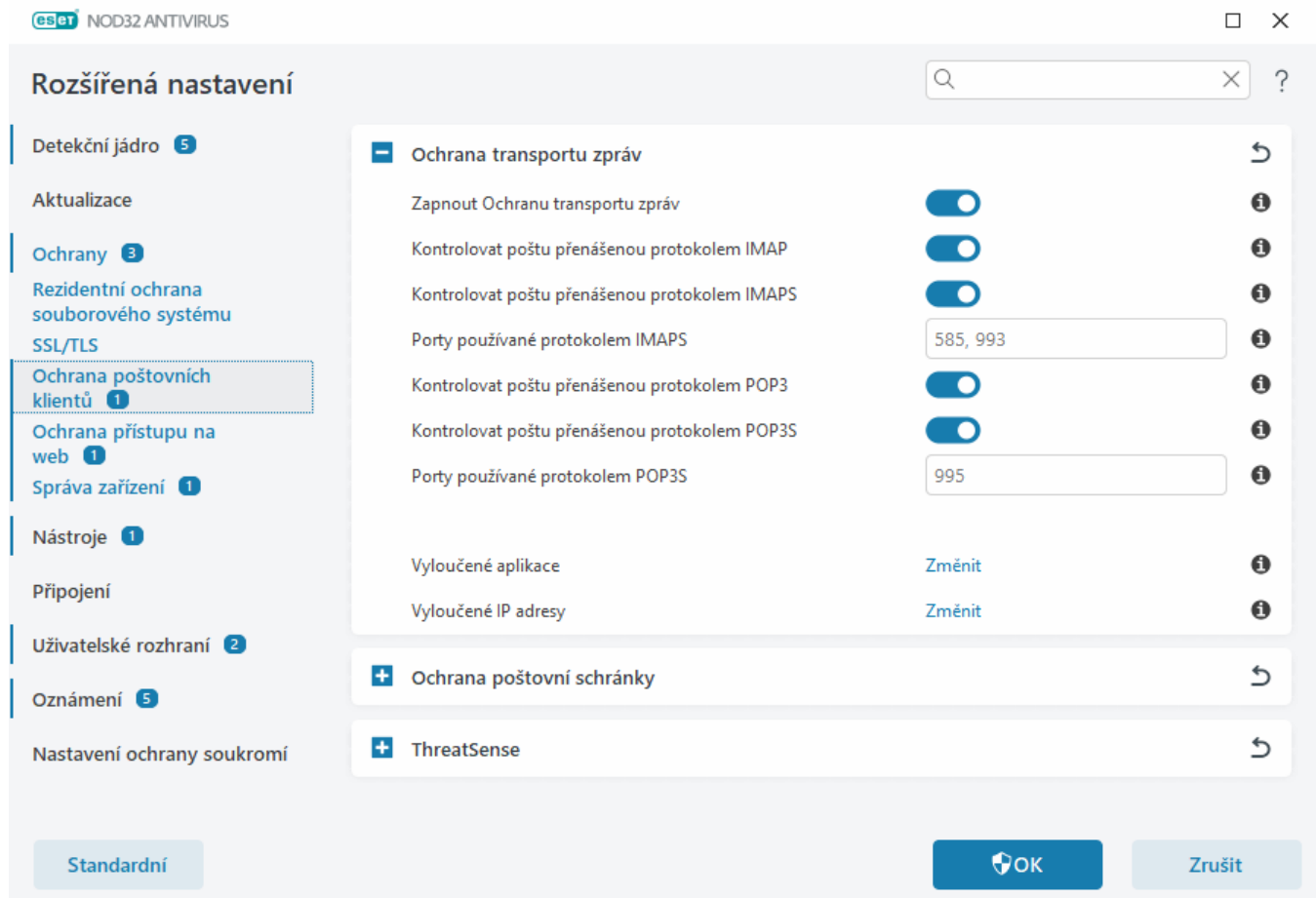
Kliknutím na přepínač vedle následujících možností můžete zvolit, které protokoly pro přenos pošty budou kontrolovány (ve výchozím nastavení je povolena kontrola všech protokolů):

- **Kontrolovat poštu přenášenou protokolem IMAP**
- **Kontrolovat poštu přenášenou protokolem IMAPS**
- **Kontrolovat poštu přenášenou protokolem POP3**
- **Kontrolovat poštu přenášenou protokolem POP3S**

Ve výchozím nastavení bude ESET NOD32 Antivirus kontrolovat komunikaci na standardních portech IMAPS a POP3S. Chcete-li přidat vlastní porty pro protokoly IMAPS a POP3S, zadejte je do textového pole vedle **Porty používané protokolem IMAPS** nebo **Porty používané protokolem POP3S**. Více čísel portů je třeba oddělit čárkou.

[Vyloučené aplikace](#) – umožňuje neprovádět Ochranu poštovního transportu u zvolených aplikací. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

[Vyloučené IP adresy](#) – umožňuje neprovádět u konkrétních adres kontrolu pomocí Ochrany transportu zpráv. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



Vyloučené aplikace

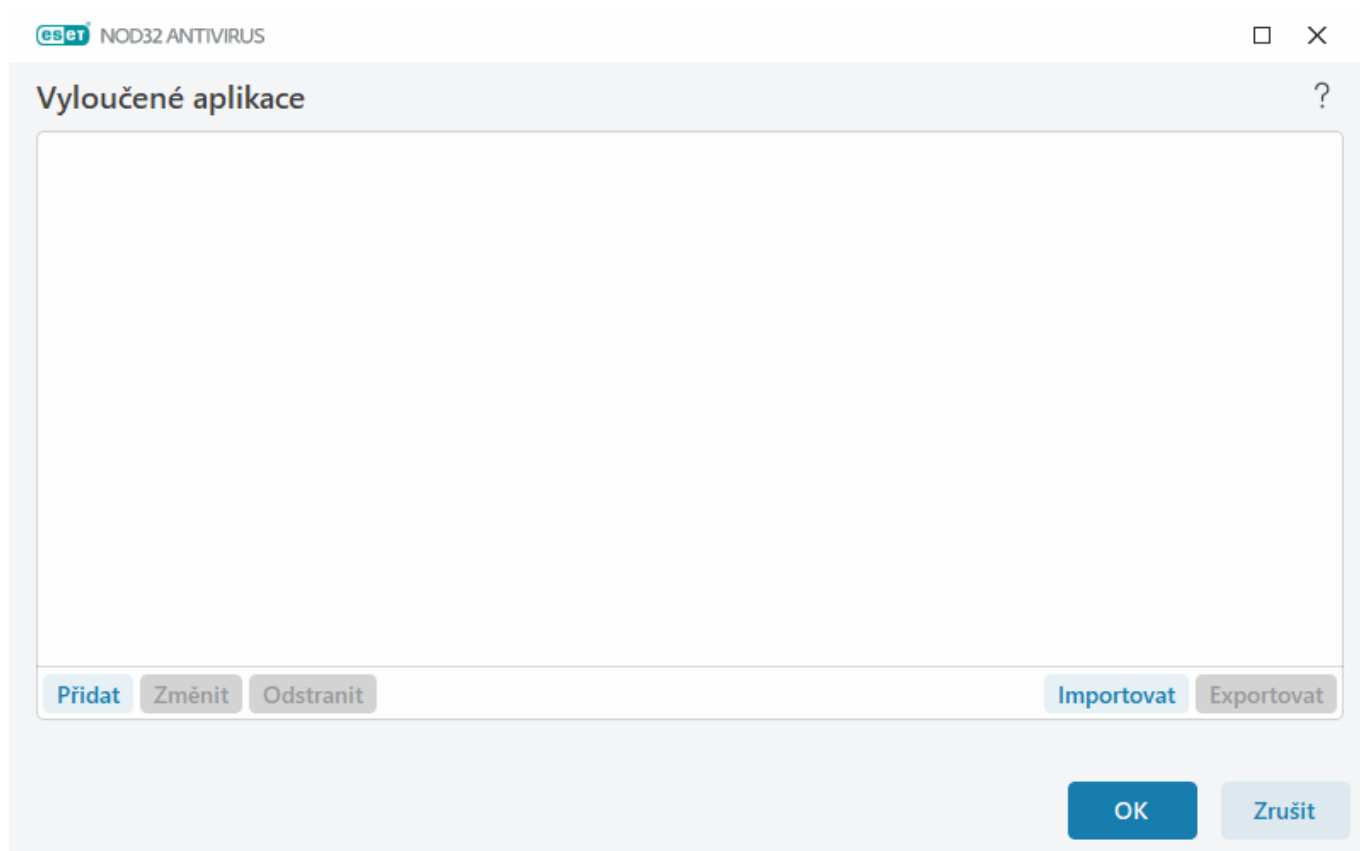
Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu.

HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na ... a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany.

Upravit – klikněte pro změnu vybrané IP adresy.

Odstranit – kliknutím odstraníte vybrané IP adresy ze seznamu.

Vyloučené IP adresy



--	--

Přidat

Změnit

Odstranit

Importovat

Exportovat

OK

Zrušit

Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).**Rozsah adres** – umožní zadat počáteční a koncovou IP adresu pro rozsah IP několika zařízení (například *192.168.0.1-192.168.0.99*).✓ **Podsít** – umožní zadat podsít skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsít 192.168.1.0. Chcete-li vyloučit celou podsít, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).**Podsít** – podsít skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Ochrana poštovní schránky

Integrace ESET NOD32 Antivirus s poštovní schránkou zvyšuje úroveň ochrany před škodlivým kódem v e-mailových zprávách.

Chcete-li nakonfigurovat ochranu poštovní schránky, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky**.

Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta – Vypnutím se deaktivuje ochrana zajišťovaná doplňkem v e-mailových klientech.

Vyberte e-maily pro kontrolu:

- Příchozí zprávy
- Odchozí zprávy
- Čtené zprávy

- Změněná zpráva

i Doporučujeme, abyste možnost **Zapnout poštovní ochranu prostřednictvím doplňku do poštovního klienta** měli zapnutou. I když integrace není zapnuta nebo je nefunkční, ochrana e-mailová komunikace je stále zajišťována prostřednictvím modulu [Ochrana transportu zpráv](#) (IMAP/IMAPS a POP3/POP3S).

Optimalizovat zpracování příloh – při vypnutí této možnosti budou všechny přílohy kontrolovány okamžitě. Může tím dojít ke zpomalení výkonu e-mailového klienta.

Integrace – umožňuje integrovat Ochranu poštovní schránky do e-mailového klienta. Další informace naleznete v kapitole [Integrace](#).

Reakce – umožňuje přizpůsobit zpracování nevyžádaných zpráv. Další informace naleznete v kapitole [Reakce](#).

Integrace

Integrace ESET 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, což přispívá k efektivnější kontrole e-mailových zpráv. Chcete-li upravit nastavení integrace, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Integrace**.

Povolit integraci s Microsoft Outlook – [Microsoft Outlook](#) je v současné době jediným podporovaným e-mailovým klientem. Poštovní ochrana je zajišťována pomocí doplňku. Hlavní výhodou doplňku je nezávislost na použitém protokolu. Pokud jsou zprávy šifrovány, virový skener je dostává ke kontrole již dešifrované. Úplný seznam podporovaných poštovních klientů a jejich verzí naleznete v [ESET Databázi znalostí](#) (článek nemusí být dostupný ve všech jazycích).

Pokročilé zpracování poštovními klienty – zpracovává další [Outlook Messaging API \(MAPI\) události](#): Objekt upraven (`fnevObjectModified`) a Objekt vytvořen (`fnevObjectCreated`). Tuto možnost vypněte, pokud pozorujete propad výkonu při práci s vaším poštovním klientem.

Panel nástrojů v MS Outlook

Ochrana Microsoft Outlook pracuje jako zásuvný modul (plug-in). Po instalaci ESET NOD32 Antivirus se do aplikace Microsoft Outlook přidá tento panel nástrojů s možnostmi antivirové ochrany :

ESET NOD32 Antivirus – dvojitým kliknutím na ikonu otevřete hlavní okno programu ESET NOD32 Antivirus.

Znovu zkontrolovat zprávy – umožní ruční spuštění kontroly e-mailů. V této části můžete vybrat zprávy, které budou zkontrolovány. Tím můžete aktivovat opakovanou kontrolu přijatého e-mailu. Další informace naleznete v kapitole [Ochrana poštovní schránky](#).

Nastavení skeneru – zobrazí možnosti nastavení [Ochrany poštovní schránky](#).

Potvrzovací dialog

Dialog s možností potvrzení nebo zamítnutí dané akce slouží pro ověření, že chcete akci opravdu provést. Předejdete tím také akcím, jejichž provedení jste nastavili nedoplněním.

Zároveň můžete tato upozornění vyžadující potvrzení zcela vypnout.

Opakovaná kontrola zpráv

Na panelu nástrojů produktu ESET NOD32 Antivirus integrovaném v poštovním klientovi máte k dispozici možnosti pro kontrolu zpráv. Dostupné jsou dvě možnosti kontroly:

Všechny zprávy v aktuální složce – zkontrolují se všechny zprávy ve složce, která je aktuálně zobrazena.

Pouze označené zprávy – zkontrolují se pouze zprávy, které jste vybrali ručně.

Možnost **Kontrolovat zprávy, které již byly překontrolovány** zajistí nové zkontrolování zpráv, které již byly v minulosti zkontrolovány.

Reakce

Na základě výsledků kontroly zpráv může ESET NOD32 Antivirus zkontrolované zprávy přesunout nebo přidat vlastní text do předmětu. Tato nastavení můžete nakonfigurovat v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana poštovních klientů** > **Ochrana poštovní schránky** > **Reakce**.

Pokud zpráva obsahuje detekci, ve výchozím nastavení se ji ESET NOD32 Antivirus pokusí vyléčit. Pokud zprávu nelze vyléčit, můžete zvolit **Akce, pokud není možné objekt vyléčit**:

- **Žádná akce** – program upozorní na zprávy s infikovanými přílohami, avšak neprovede žádnou akci.
- **Odstranit zprávu** – program upozorní na infikované přílohy a odstraní celou zprávu.
- **Přesunout zprávu do složky s odstraněnými zprávami** – program bude přesouvat infikované zprávy do složky s vymazanými zprávami.
- **Přesunout zprávu do složky** (výchozí akce) – program bude přesouvat infikované zprávy do vybrané složky.

Složka – definujte vlastní složku, do které přesouvat infikované zprávy.

Do kontrolovaných zpráv je možné přidávat podpis s informacemi o výsledku kontroly. Textové upozornění můžete **Přidávat do příchozích a čtených zpráv** nebo **Přidávat do odchozích zpráv**. Samozřejmě, na tyto podpisy se nelze zcela spoléhat, protože nemusí být doplněny do problematických HTML zpráv a také mohou být zfalšovány malwarem. Přidávání podpisu můžete nastavit zvlášť pro přijaté a čtené zprávy a zvlášť pro odesílané zprávy nebo pro oboje. K dispozici jsou následující možnosti:

- **Nikdy** – program nebude přidávat podpisy,
- **Při výskytu detekce** – pouze zprávy obsahující škodlivý software budou označeny jako zkontrolované (výchozí).

- **Přidávat do všech kontrolovaných zpráv** – program bude přidávat zprávy do všech kontrolovaných e-mailů.

Modifikovat předmět příchozích a čtených zpráv / Modifikovat předmět odchozích zpráv – povolením této možnosti přidáte do zprávy vlastní text zadaný níže.

Šablona přidávaná do předmětu infikovaných zpráv – upravte tuto šablonu, pokud chcete změnit formát předpony předmětu infikovaného e-mailu. Tato funkce přidá k původnímu předmětu zprávy "Ahoj" předponu "[detekce %DETECTIONNAME%]". Proměnná %DETECTIONNAME% představuje detekovanou hrozbou.

ThreatSense

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

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

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

Kontrolované objekty

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

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

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do [slovníku pojmů](#).

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

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

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

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

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

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

Léčení

Nastavení léčení ovlivňuje chování ESET NOD32 Antivirus během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET NOD32 Antivirus

Úroveň léčení	Popis
Vždy vyřešit infekci	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých ojedinělých případech vyléčit (např. u systémových souborů), bude detekovaný objekt ponechán v původním umístění.

Úroveň léčení	Popis
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučeno pro většinu případů.
Vždy se dotázat uživatele	V průběhu léčení objektů se uživateli zobrazí interaktivní okno, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Tato úroveň je určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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

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

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do [protokolu](#) zapíše všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnutí Smart optimalizaci je použito neoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

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

Omezení

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

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena.

V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány.

Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a **Maximální velikost souboru v archivu** (nedoporučuje se z důvodu možných bezpečnostních rizik).

Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: **3 GB**.

i Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Ochrana přístupu na web

Ochrana přístupu na web umožňuje konfigurovat pokročilá nastavení modulu [Internetová ochrana](#). V [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana přístupu na web** > **Ochrana přístupu na web** jsou k dispozici následující možnosti:

Zapnout ochranu přístupu na web – pokud je tato možnost vypnutá, nefunguje Ochrana přístupu na web ani [Anti-Phishingová ochrana](#).

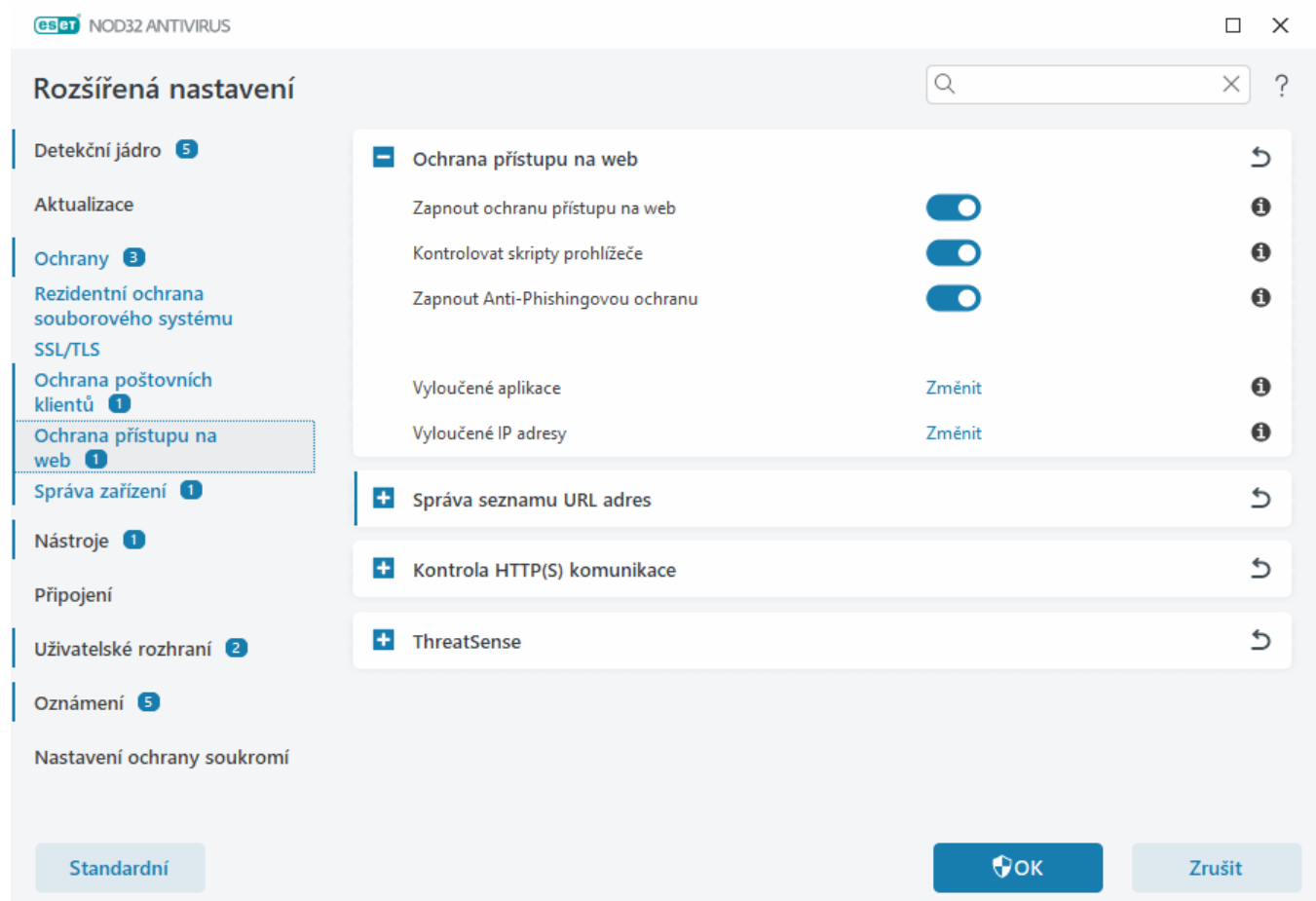
i Důrazně doporučujeme ponechat Ochranu přístupu na web zapnutou a nevylučovat žádné aplikace ani IP adresy ve výchozím nastavení.

Kontrolovat skripty prohlížeče – pokud je tato funkce povolena, detekční jádro zkontroluje všechny JavaScript programy spouštěné webovými prohlížeči.

Zapnout Anti-Phishingovou ochranu – pokud je povolena, jsou phishingové webové stránky blokovány. Pro více informací přejděte do kapitoly [Anti-Phishingová ochrana](#).

Vyloučené aplikace – umožňuje vyloučit konkrétní aplikace z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.

[Vyloučené IP adresy](#) – umožňuje vyloučit konkrétní IP adresy z kontroly prováděné Ochranou přístupu na web. To může být užitečné, jestliže Ochrana přístupu na web způsobuje problémy s kompatibilitou.



Při přístupu na blokovanou stránku se v internetovém prohlížeči zobrazí níže uvedená zpráva:



Nalezena hrozba

Stránka obsahuje potenciálně nebezpečný obsah.

Hrozba: HTML/ScrInject.B trojský kůň

Přístup na tuto stránku byl zablokován. Váš počítač je v bezpečí.

[Otevřít ESET Databázi znalostí](#) | www.eset.cz

Názorné ukázky



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

- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Jak zablokovat přístup na webovou stránku prostřednictvím produktu ESET NOD32 Antivirus](#)

Vyloučené aplikace

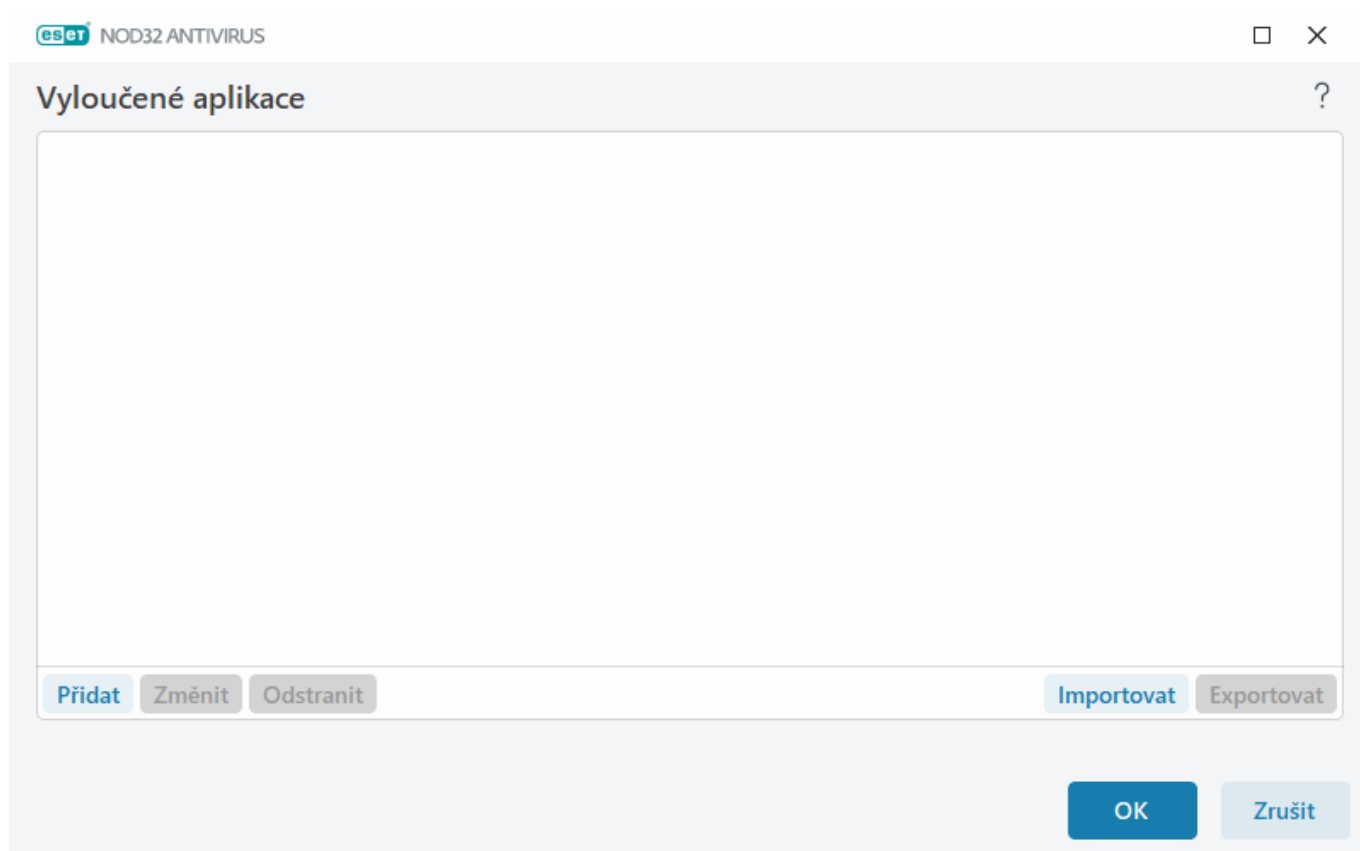
Chcete-li neprovádět kontrolu komunikace pro konkrétní aplikace, přidejte je do seznamu.

HTTP(S)/POP3(S)/IMAP(S) komunikace vybraných aplikací nebude kontrolována na přítomnost hrozeb. Tuto možnost doporučujeme použít pouze u aplikací, které nefungují správně při kontrole jejich komunikace.

Spuštěné aplikace a služby zde budou k dispozici automaticky po kliknutí na **Přidat**. Klikněte na ... a přejděte na aplikaci, do kterou chcete vyloučit.

Změnit – kliknutím upravíte vybraný záznam.

Odstranit – kliknutím odeberete vybraný záznam ze seznamu.



Vyloučené IP adresy

IP adresy uvedené v tomto seznamu se nebudou kontrolovat. To znamená, že komunikace prostřednictvím protokolů HTTP(S), POP3(S) a IMAP(S) z/do zvolených IP adres nebude kontrolována na přítomnost hrozeb. Doporučujeme používat tuto možnost pouze v případě důvěryhodných IP adres.

Přidat – klikněte pro přidání IP adresy/rozsahu adres/podsítě vzdálené strany.

Upravit – klikněte pro změnu vybrané IP adresy.

Odstranit – kliknutím odstraníte vybrané IP adresy ze seznamu.

Vyloučené IP adresy



--	--

Přidat

Změnit

Odstranit

Importovat

Exportovat

OK

Zrušit

Příklady IP adres

Přidání IPv4 adresy:

Samostatná adresa – přidá IP adresu jednotlivého zařízení (například *192.168.0.10*).**Rozsah adres** – umožní zadat počáteční a koncovou IP adresu pro rozsah IP několika zařízení (například *192.168.0.1-192.168.0.99*).✓ **Podsít** – umožní zadat podsít skupiny počítačů pomocí IP adresy a masky. Například 255.255.255.0 je síťová maska pro podsít 192.168.1.0. Chcete-li vyloučit celou podsít, zadejte *192.168.1.0/24*.

Přidání IPv6 adresy:

Samostatná adresa – umožní zadat IP adresu konkrétního zařízení (například *2001:718:1c01:16:214:22ff:fec9:ca5*).**Podsít** – podsít skupiny počítačů můžete definovat pomocí IP adresy a masky (například *2002:c0a8:6301:1::1/64*).

Správa seznamu URL adres

Správa seznamu URL adres v [Rozšířených nastaveních](#) > **Ochrany** > **Ochrana přístupu na web** umožňuje zadat HTTP adresy, které se mají blokovat, povolit nebo vyloučit z kontroly obsahu webu.

Pokud chcete filtrovat kromě HTTP adres kontrolovat také HTTPS adresy, musí být zapnutý protokol [SSL/TLS](#). V opačném případě by byl zakázán pouze přístup na nešifrovanou HTTPS verzi webové stránky.

Webové stránky zařazené na **Seznamu blokových adres** nebudou dostupné, na rozdíl od adres uvedených na **Seznamu povolených adres**. Webové stránky zařazené na **Seznamu adres vyloučených z kontroly obsahu** nebudou kontrolovány na přítomnost škodlivého kódu.

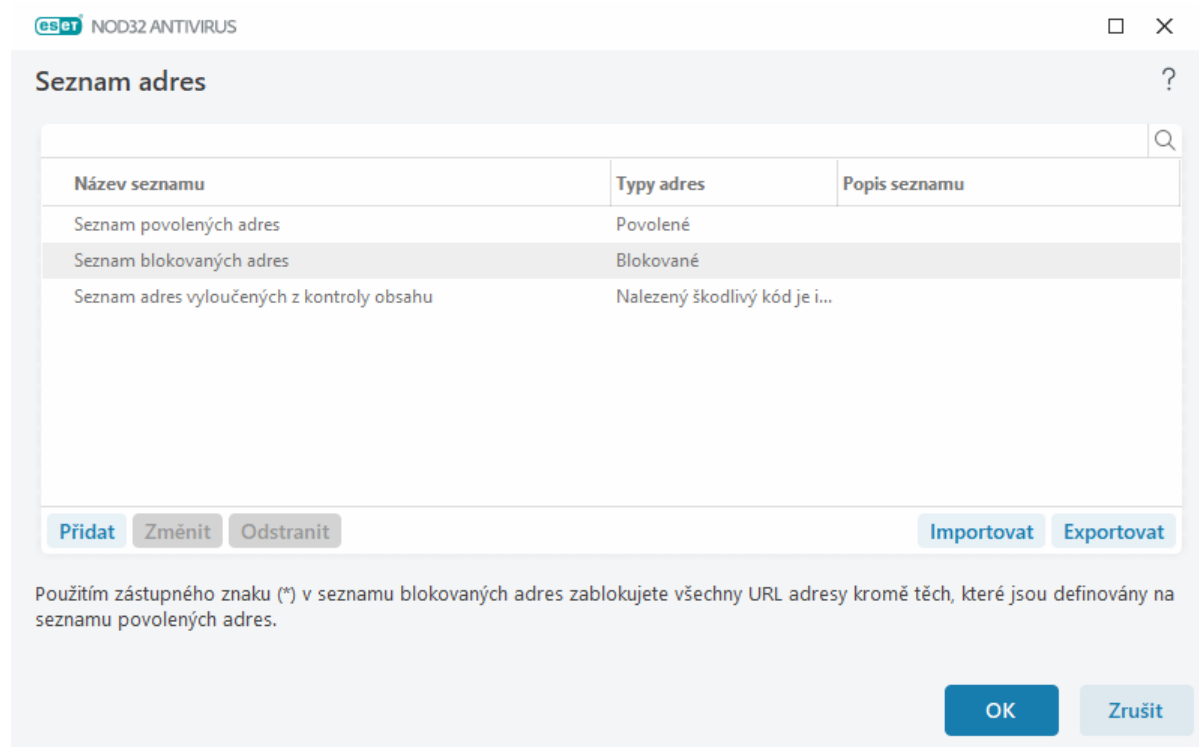
Pokud chcete zablokovat všechny HTTP adresy kromě těch definovaných na **Seznamu povolených adres**, zadejte do již definovaného **Seznamu blokových adres** * (hvězdičku).

V seznamech můžete používat speciální znaky * (hvězdička) a ? (otazník). Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Adresy vyloučené z kontroly se nekontrolují na přítomnost hrozeb, proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Je potřeba dbát opatrnosti při

používání speciálních znaků v tomto seznamu. Pro více informací, jak bezpečně přidat celou doménu včetně jejích subdomén, přejděte do kapitoly [Přidání masky adresy/domény](#). Pro aktivování seznamu vyberte možnost **Seznam je aktivní**. Při aplikování adresy ze seznamu je možné nastavit zobrazení upozornění zaškrtnutím možnosti **Upozornit při aplikování adresy ze seznamu**.

Adresy důvěryhodné pro ESET

i Pokud je povolena možnost **Nekontrolovat komunikaci s doménami, které ESET považuje za důvěryhodné**, nebudou tyto domény ovlivněny vámi vytvořeným seznamem URL adres.



Ovládací prvky

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

Změnit – kliknutím upravíte existující seznam adres. Tuto možnost použijte pro přidání nebo odebrání adres ze seznamu.

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

Seznam adres

V této části můžete zadat seznamy HTTP(S) adres, které budou blokovány, povoleny nebo vyloučeny z kontroly.

Standardně jsou k dispozici tři seznamy:

- **Seznam adres vyloučených z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na škodlivý kód.

- **Seznam povolených adres** – pokud do seznamu blokových adres vložíte hvězdičku (*), bude uživateli povolen přístup pouze na adresy uvedené v tomto seznamu. Přístup na tyto adresy bude povolen i v případě, že se zároveň nachází na seznamu blokových adres.
- **Seznam blokových adres** – na adresy uvedené v tomto seznamu nebude povolen přístup, pokud se zároveň nenachází na seznamu povolených adres.

Pro vytvoření nového seznamu klikněte na tlačítko **Přidat**. Pro odebrání seznamu klikněte na tlačítko **Odstranit**.

Seznam adres

Název seznamu	Typy adres	Popis seznamu
Seznam povolených adres	Povolené	
Seznam blokových adres	Blokované	
Seznam adres vyloučených z kontroly obsahu	Nalezený škodlivý kód je i...	

Přidat Změnit Odstranit Importovat Exportovat

Použitím zástupného znaku (*) v seznamu blokových adres zablokuje všechny URL adresy kromě těch, které jsou definovány na seznamu povolených adres.

OK Zrušit

Názorné ukázky



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

- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Blokovat webovou stránku za použití produktů ESET pro domácnosti](#)

Další informace naleznete v části [Správa seznamu URL adres](#).

Vytvoření nového seznamu URL adres

V tomto dialogovém okně můžete vytvořit nový [seznam adres/masek](#), které budou blokovány, povoleny, nebo vyloučeny z kontroly.

Při vytváření nového seznamu jsou dostupné následující možnosti:

Typ seznamu adres – k dispozici jsou tři typy předdefinovaných seznamů:

- **Vyloučené z kontroly obsahu** – adresy uvedené v tomto seznamu nebudou kontrolovány na přítomnost škodlivého kódu.
- **Blokované** – na adresy v tomto seznamu nebude povolen přístup.
- **Povolené** – pokud do seznamu blokových adres vložíte hvězdičku (*), bude uživateli povolen přístup

pouze na adresy uvedené v tomto seznamu. Přístup na tyto adresy bude povolen i v případě, že se zároveň nachází na seznamu blokových adres.

Název seznamu – zadejte název nového seznamu. Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.

Popis seznamu – zadejte krátký popis pro nově vytvářený seznam (nepovinné). Pole bude šedivé, pokud upravujete některý z předdefinovaných seznamů.

Pro aktivaci seznamu vyberte možnost **Seznam je aktivní**. Pokud chcete být upozorněni při přístupu k adrese uvedené na seznamu, aktivujte možnost **Upozornit při přístupu na adresy ze seznamu**. V takovém případě se zobrazí oznámení o tom, že přistupujete na webovou stránku zařazenou na seznam například blokových nebo povolených stránek. V oznámení se zobrazí název seznamu obsahujícího zadanou webovou stránku.

Zaznamenávat od úrovně – informace o konkrétním seznamu používaném při přístupu na webové stránky lze zapisovat do [souborů protokolu](#).

Ovládací prvky

Přidat – kliknutím přidáte na seznam novou URL adresu (pro hromadné přidání více hodnot použijte oddělovač).

Změnit – kliknutím upravíte existující záznam. Tato možnost je dostupná pouze nad hodnotami, které jste **přidali** ručně.

Odstranit – kliknutím odstraníte záznam ze seznamu. Tato možnost je dostupná pouze nad hodnotami, které jste **přidali** ručně.

Importovat – kliknutím můžete naimportovat adresy ze souboru (kdy je každá hodnota na novém řádku a jde například o *.txt v UTF-8 kódování).

Jak přidat masku URL?

Před zadáním požadované masky adresy/domény se seznamte s instrukcemi.

ESET NOD32 Antivirus umožňuje zablokovat přístup na specifické stránky a dokáže zabránit internetovému prohlížeči v zobrazení jejich obsahu. Dále umožňuje specifikovat adresy, které mají být vyloučeny z kontroly. Pokud neznáte celý název vzdáleného serveru, nebo chcete specifikovat celou skupinu vzdálených serverů, můžete použít tzv. masky. V tomto případě jsou povoleny speciální znaky ? a * přičemž:

- znak ? nahrazuje libovolný symbol,
- znak * nahrazuje libovolný textový řetězec.

Například *.c?m bude platit pro všechny adresy, jejichž poslední část adresy začíná znakem c, končí znakem m a uprostřed se nachází libovolný znak (.com, .cam apod.).

Pokud použijete "*" na začátku názvu domény, bude sekvence vyhodnocena odlišně. Zprvu, zástupný znak hvězdičky ("*") v tomto případě nenahrazuje lomítko ("/"). To proto, aby se například maska *.domena.cz nevyhodnocovala jako adresa <http://jakakolidomena.cz/cesta#.domena.com> (jako přípona může být připojena k jakékoli URL adrese bez toho, že by došlo k zablokování stahování). Za druhé, v tomto zvláštním případě odpovídá "*" také prázdnému řetězci. Jedna maska tak může zahrnovat celou doménu, včetně jejích subdomén. Například

maska *.domena.cz platí také pro adresu <http://domena.cz>. Použití masky *.domena.cz ovšem není správné, protože za daných okolností můžete být použita také pro adresu <http://jinadomena.cz>.

Kontrola HTTP(S) komunikace

Ve výchozím nastavení je aplikace ESET NOD32 Antivirus nakonfigurována tak, aby kontrolovala HTTP a HTTPS komunikaci, kterou používají internetové prohlížeče a další aplikace. Kontrolu komunikace byste měli zakázat pouze v případě, že máte problémy se softwarem třetí strany a chcete zjistit, zda tento problém způsobuje ESET NOD32 Antivirus.

Zapnout kontrolu HTTP komunikace – HTTP komunikace je vždy kontrolována na všech portech pro všechny aplikace.

Zapnout kontrolu HTTPS komunikace – HTTPS komunikace používá k přenosu informací mezi serverem a klientem šifrovaný kanál. ESET NOD32 Antivirus kontroluje komunikaci pomocí protokolů SSL (Secure Socket Layer) a TLS (Transport Layer Security). Program bude kontrolovat pouze komunikaci na portech definovaných v části **Porty používané protokolem HTTPS** bez ohledu na verzi operačního systému (k předdefinovaným portům 443 a 0-65535 můžete přidat další).

ThreatSense

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

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web

- Kontrola počítače

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

Kontrolované objekty

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

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

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do [slovníku pojmů](#).

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

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

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

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

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

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

Léčení

Nastavení léčení ovlivňuje chování ESET NOD32 Antivirus během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET NOD32 Antivirus

Úroveň léčení	Popis
Vždy vyřešit infekci	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých ojedinělých případech vyléčit (např. u systémových souborů), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučeno pro většinu případů.
Vždy se dotázat uživatele	V průběhu léčení objektů se uživateli zobrazí interaktivní okno, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Tato úroveň je určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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

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

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do [protokolu](#) zapíše všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnutí Smart optimalizaci je použito neoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

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

Omezení

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

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena.

V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány.


Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik).

Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: **3 GB**.

 Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Správa zařízení

ESET NOD32 Antivirus automaticky kontroluje zařízení (CD/DVD/USB/atd). Můžete blokovat nebo upravovat rozšířené filtry nebo oprávnění a umožnit uživateli přístup k danému zařízení a práci s ním. Tuto funkci můžete použít v případě, že chcete uživatelům zabránit v připojování výměnných médií k počítači.

Podporovaná externí zařízení:

- Datové úložiště (HDD, USB výměnné jednotky),
- CD/DVD,
- USB tiskárna,
- FireWire úložiště,

- Zařízení Bluetooth,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port,
- Přenosná zařízení (zařízení napájená baterií, jako jsou přehrávače médií, chytré telefony, zařízení plug-and-play, atd.)
- Všechny typy zařízení.

Nastavení správy zařízení můžete upravit v [Rozšířených nastaveních](#) > **Ochrany** > **Správa zařízení**.

Přepínačem aktivujete **Povolit ovládání zařízení**, a povolte tak funkci Správa zařízení v ESET NOD32 Antivirus. Aby se tato změna projevila, musíte restartovat počítač. Po zapnutí správy zařízení se zpřístupní odkaz **Pravidla**, prostřednictvím kterého si otevřete [editor pravidel](#).

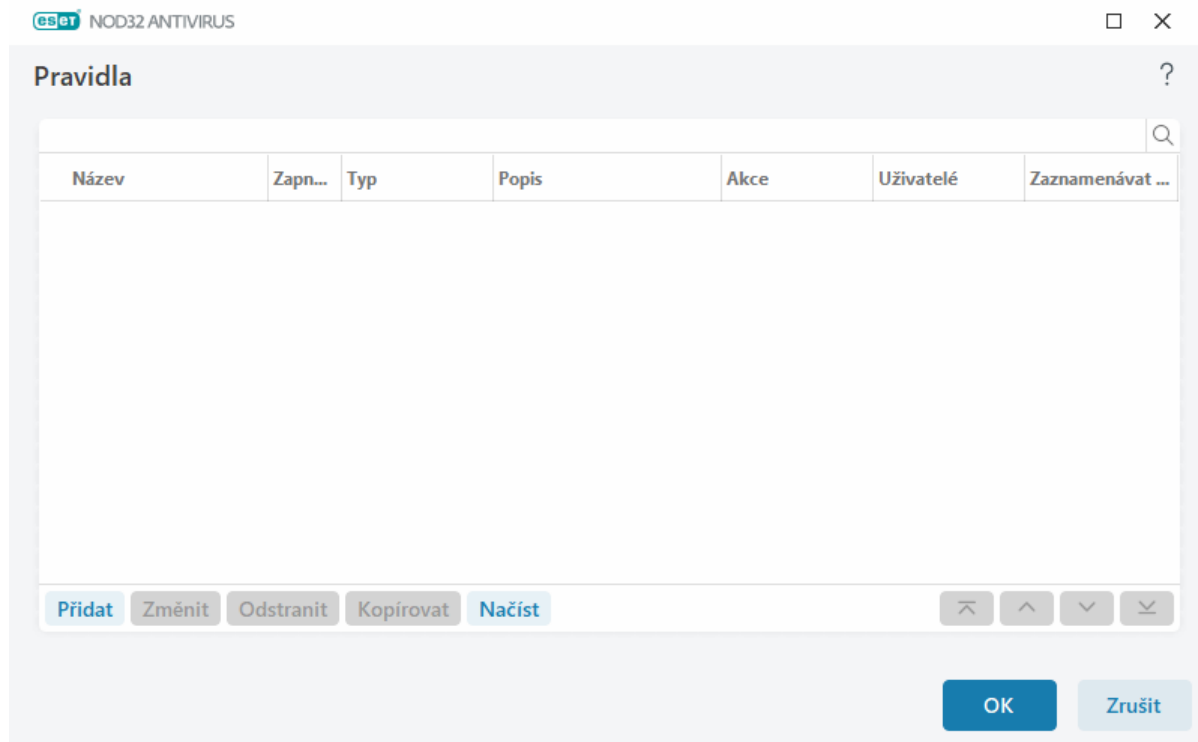


Můžete vytvořit různé skupiny zařízení, na které se budou vztahovat různá pravidla. Vytvořte si skupinu zařízení, na kterou se bude aplikovat pravidlo pro **Povolení** nebo **Blokování zápisu**. Poté vytvořte druhé pravidlo, které bude blokovat přístup.

Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování, zobrazí se informační okno a přístup k zařízení bude odepřen.

Editor pravidel ve správě zařízení

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

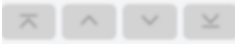


Konkrétní zařízení můžete povolit nebo zakázat pro vybraného uživatele nebo skupinu uživatelů na základě parametrů zařízení, které definujete v konfiguraci pravidla. Seznam pravidel obsahuje popis, tedy název pravidla, typ externích zařízení, akci, která se má provést po připojení k počítači a úroveň protokolování. Více si přečtete v kapitole [Pravidla správy zařízení](#).

Pro správu pravidel klikněte na tlačítko **Přidat** nebo **Změnit**. Kliknutím na tlačítko **Kopírovat** vytvoříte nové pravidlo s identickými parametry. XML řetězce zobrazené při kliknutí na pravidlo si můžete zkopírovat do schránky. To usnadní systémovým administrátorům export/import těchto dat a jejich opětovné použití.

Stisknutím klávesy **CTRL** a kliknutím můžete vybrat více pravidel najednou a provést hromadné akce, jako je jejich odstranění nebo posunutí dolů nebo vzhůru. **Zapnuto** – zaškrtnutím povolujete/zakazujete aplikaci pravidla. To může být vhodné v případě, kdy nechcete pravidlo vymazat, ale ponechat si jej pro případné použití v budoucnu.

Kliknutím na tlačítko **Načíst** se automaticky načtou parametry všech připojených výměnných zařízení připojených k počítači.

Pravidla jsou seřazena dle priority, tedy pravidlo s nejvyšší prioritou je umístěno nahoře. Pořadí pravidel můžete upravit pomocí tlačítek  **Nahoru/Výše/Dolů/Níže**.


Záznamy protokolu lze zobrazit v [hlavním okně programu](#) > **Nástroje** > [Protokoly](#).

Do [protokolu správy zařízení](#) se запиšou informace o všech připojených zařízeních.

Detekovaná zařízení

Kliknutím na tlačítko **Načíst** se zobrazí informace o všech aktuálně připojených zařízeních, jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné).

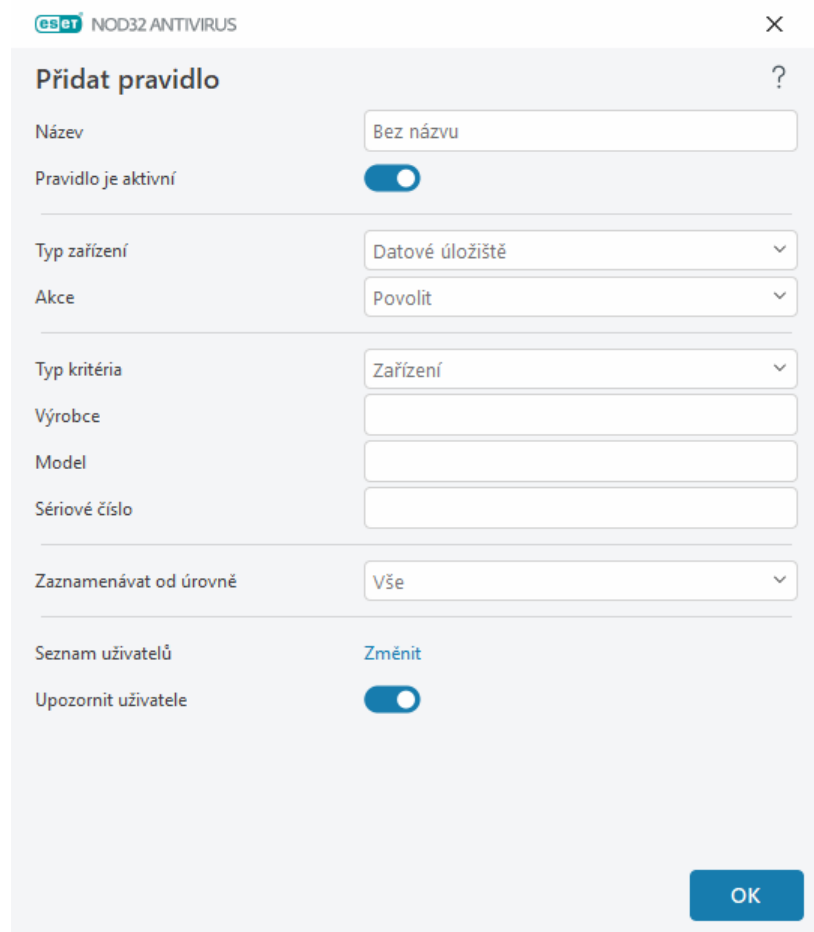
Po vybrání konkrétního zařízení a kliknutí na tlačítko **OK** se zobrazí [dialogové okno pro vytvoření nového pravidla](#) s již předdefinovanými hodnotami (zobrazené hodnoty můžete dle potřeby upravit).

Zařízení v režimu nízké spotřeby (režim spánku) jsou označena vykřičníkem . V takovém případě pro zaktivnění tlačítka **OK**, a dokončení vytvoření pravidla pro dané zařízení, proveďte následující kroky:

- Odpojte a znovu připojte zařízení.
- Použijte zařízení (například spusťte aplikaci Kamera ve Windows a probudte webovou kameru).

Vytvoření nového pravidla

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



Pro snadnější identifikaci do pole **Název** zadejte jméno pravidla. Kliknutím na přepínač vedle **Pravidlo je aktivní** dané pravidlo zakážete nebo povolíte; to může být užitečné, pokud nechcete pravidlo trvale odstranit.

Typ zařízení

Z rozbalovacího menu vyberte typ zařízení (diskové úložiště/přenosné zařízení/Bluetooth/FireWire/...). Typy zařízení se přebírají ze systému a můžete si je zobrazit v systémovém Správci zařízení, který poskytuje informace o zařízeních připojených k počítači. Úložná média zahrnuje externí disky nebo čtečky paměťových karet připojených pomocí USB nebo FireWire. Čtečky čipových karet zahrnují čtečky karet s integrovanými elektronickými obvody jako jsou SIM karty nebo přístupové karty. Příkladem zobrazovacích zařízení jsou fotoaparáty a kamery, které neposkytují informace o uživateli, pouze vyvolávají akce. To znamená, že tato zařízení mohou být blokována pouze globálně.

Akce

Přístup na zařízení, která neslouží pro ukládání dat, může být pouze povolen nebo zakázán. Oproti tomu úložným zařízením můžete nastavit následující práva:

- **Povolit** – plný přístup k zařízení,
- **Blokovat** – přístup k zařízení bude zakázán,
- **Blokovat zápis** – uživatel může pouze číst soubory na daném zařízení, ale ne zapisovat.
- **Upozornit** – při každém připojení zařízení se uživateli zobrazí upozornění, že byl přístup na zařízení povolen/zakázán a zároveň se informace zapíše do protokolu. K zapamatování zařízení nedochází. Při opětovném připojení stejného zařízení dojde k zobrazení oznámení.

Mějte na paměti, že uvedené akce (povolení) nemusí být dostupné u všech zařízení. Pokud se jedná o úložné zařízení, zobrazí se všechny. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

Typ kritéria

Vyberte, zda chcete pravidlo vytvořit pro jednotlivé **zařízení** nebo **skupinu zařízení**.

Pro přizpůsobení pravidel vztažených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.

i Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.

i Tip: Pro získání parametrů zařízení, pro které chcete vytvořit pravidlo, připojte zařízení k počítači a podívejte se do [protokolu správy zařízení](#).

Zaznamenávat do protokolu

ESET NOD32 Antivirus ukládá důležité události do protokolu, který je možné prohlížet přímo v hlavním okně. Protokoly naleznete v sekci **Nástroje > Protokoly** po vybrání možnosti **Správa zařízení** z rozbalovacího menu.

- **Vše** – zaznamenají se všechny události.
- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů,
- **Informační** – zaznamenány budou informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíše kritické chyby a varovná hlášení.

- **Žádné** – nebudou zaznamenávány žádné události, nevytvoří se žádné protokoly.

Seznam uživatelů

Pravidla přiřadíte konkrétnímu uživateli nebo celé skupině kliknutím na **Změnit** na řádku **Seznam uživatelů**.

- **Přidat** – otevře okno **Vybrat typ objektu: Uživatelé nebo Skupiny**, kde můžete vybrat konkrétní uživatele.
- **Odstranit** – odebere vybraného uživatele z filtru.

Omezení v seznamu uživatelů

Seznam uživatelů není možné definovat v pravidlech platných pro níže uvedené [Typy zařízení](#):



- USB tiskárna,
- Bluetooth zařízení,
- Čtečka čipových karet,
- Obrazové zařízení,
- Modem,
- LPT/COM port.

Upozornit uživatele – Pokud do počítače vložíte externí zařízení, na které se použije pravidlo o blokování a zobrazí se okno s oznámením.

Skupiny zařízení



Zařízení připojená k počítači mohou představovat bezpečnostní riziko.

Dialogové okno skupin zařízení je rozděleno na dvě části. V levé části se nachází seznam vytvořených skupin a v pravé části se zobrazují zařízení, která patří do dané skupiny. Pokud si chcete zobrazit v pravém okně zařízení, vyberte vlevo konkrétní skupinu zařízení.

Jakmile máte vybranou konkrétní skupinu, po kliknutí na příslušné tlačítko můžete zařízení do skupiny přidat nebo odstranit. Další možností přidání je import zařízení ze souboru. V neposlední řadě si kliknutím na tlačítko **Načíst** můžete zobrazit seznam všech zařízení připojených k počítači. Následně se vám zobrazí dialogové okno **Detekovaná zařízení**. Vyberte zařízení ze seznamu a přidejte je do skupiny kliknutím na tlačítko **OK**.

Ovládací prvky

Přidat – vytvoří novou skupinu nebo přidá zařízení do již existující skupiny, s ohledem na to, zda jste klikli na stejnojmenné tlačítko v levé nebo pravé části okna.

Změnit – umožní změnit skupinu zařízení a parametry zařízení.

Odstranit – vymaže vybranou skupinu nebo konkrétní zařízení.

Importovat – pomocí této možnosti importujte seznam zařízení z textového souboru. Soubor musí splňovat následující formát:

- Každé zařízení je uvedeno na samostatné řádce.
- **Výrobce, Model a Sériové číslo** pro každé zařízení musí být odděleno čárkou.

✓ Příklad obsahu textového souboru:
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101

Exportovat – pomocí této možnosti exportujete seznam zařízení do souboru.

Kliknutím na tlačítko **Načíst** se zobrazí informace o všech aktuálně připojených zařízeních, jako je typ zařízení, výrobce, model a sériové číslo (pokud je dostupné).

Přidat zařízení

Kliknutím na tlačítko **Přidat** přidáte nové zařízení do existujícího seznamu zařízení. Pro přizpůsobení pravidel vztahených pouze na konkrétní zařízení můžete použít další parametry. V parametrech se rozlišuje velikost písmen a zástupné znaky (*, ?):

- **Výrobce** – filtruje podle názvu výrobce nebo ID,
- **Model** – filtruje podle názvu zařízení,
- **Sériové číslo** – filtruje podle sériového čísla, které zpravidla externí zařízení mají. V případě CD/DVD se jedná o sériové číslo média, nikoli mechaniky.
- **Popis** – váš vlastní popis zařízení pro zjednodušení orientace v seznamu.

i Pokud ponecháte výše uvedené údaje prázdné, pravidlo bude tyto hodnoty ignorovat. Parametry filtrování ve všech textových polích rozlišují velikost písmen a zástupné znaky (*, ?): Otazník (?) reprezentuje jeden znak, zatímco hvězdička (*) reprezentuje celý řetězec znaků.

Kliknutím na tlačítko **OK** uložíte změny. Klikněte na tlačítko **Zrušit** pro zavření dialogového okna **Skupiny zařízení** bez uložení změn.

i Po vytvoření skupiny zařízení je třeba pro ni [přidat nové pravidlo](#) a zvolit akci, která se má provést.

Mějte na paměti, že uvedené akce (povolení) nemusí být dostupné u všech zařízení. Pokud se jedná o úložiště, zobrazí se všechny možnosti. V případě zařízení, která neslouží pro ukládání dat, jsou dostupné pouze tři akce (například akce **Blokovat zápis** není dostupná pro Bluetooth zařízení, přístup k nim může být pouze povolen, zablokován nebo můžete nechat zobrazit upozornění).

ThreatSense

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

Mezi parametry skenovacího jádra ThreatSense, které můžete konfigurovat, patří následující možnosti:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,

- Úrovně léčení.

K nastavení se dostanete kliknutím na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli modul, který používá technologii ThreatSense (viz níže). Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. ThreatSense je možné konfigurovat individuálně pro následující moduly:

- Rezidentní ochrana souborového systému
- Kontrola při nečinnosti
- Kontrola po startu
- Ochrana dokumentů
- Ochrana poštovních klientů
- Ochrana přístupu na web
- Kontrola počítače

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

Kontrolované objekty

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

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

Boot sektory/UEFI – kontrola přítomnosti škodlivého kódu v hlavním spouštěcím záznamu disků (MBR). Pro více informací o UEFI přejděte do [slovníku pojmů](#).

Poštovní soubory – Program podporuje následující rozšíření: DBX (Outlook Express) a EML.

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

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

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

Možnosti kontroly

Vyberte metody, které se použijí během kontroly na přítomnost infiltrace. K dispozici jsou následující možnosti:

Heuristika – heuristika je algoritmus, který analyzuje (nežádoucí) aktivity programů. Předností této technologie je schopnost zjištění škodlivého softwaru, který v předešlé verzi modulu detekčního jádra nebyl obsažen, nebo jím nebyl ošetřen. Nevýhodou je možný výskyt falešných poplachů.

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

Léčení

Nastavení léčení ovlivňuje chování ESET NOD32 Antivirus během léčení objektů. K dispozici jsou 4 úrovně léčení detekovaných infikovaných souborů:

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET NOD32 Antivirus

Úroveň léčení	Popis
Vždy vyřešit infekci	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých ojedinělých případech vyléčit (např. u systémových souborů), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučeno pro většinu případů.
Vždy se dotázat uživatele	V průběhu léčení objektů se uživateli zobrazí interaktivní okno, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Tato úroveň je určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Výjimky

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které se mají kontrolovat.

Ostatní

Při konfiguraci parametrů jádra ThreatSense pro volitelnou kontrolu počítače jsou k dispozici také následující možnosti v části **Ostatní**:

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

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

Zapisovat všechny objekty do protokolu – pokud je tato možnost aktivní, v případě samorozbalovacích archivů se do [protokolu](#) zapíší všechny zkontrolované soubory, i když nejsou infikované. Mějte na paměti, že to může způsobit výrazné nárůst velikosti protokolu.

Používat Smart optimalizaci – při zapnuté Smart optimalizaci je použito neoptimálnější nastavení pro zajištění maximální efektivity kontroly při současném zachování vysoké rychlosti. Každý modul ochrany kontroluje objekty inteligentně a používá odlišné metody, které aplikuje na specifické typy souborů. Pokud je Smart optimalizace vypnuta, použije se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých ochranných modulů.

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

Omezení

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

Nastavení objektů

Maximální velikost objektu – umožňuje definovat maximální hodnotu velikosti objektu, který bude kontrolován. Daný modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Tyto hodnoty doporučujeme měnit pouze pokročilým uživatelům, kteří chtějí velké objekty vyloučit z kontroly. Výchozí hodnota: **neomezeno**.

Maximální čas kontroly objektu (v sekundách) – definuje maximální povolený čas na kontrolu kontejnerových objektů (jako archivy RAR/ZIP nebo e-maily s vícero přílohami). Toto nastavení se nevztahuje na samostatné soubory. Pokud jako uživatel nastavíte konkrétní hodnotu a určený čas vyprší, probíhající kontrola kontejnerového objektu se krátce na to zastaví, a to bez ohledu, zda byla dokončena.

V případě archivu s velkými soubory se kontrola zastaví až poté, co je extrahován soubor z archivu (například když uživatelská proměnná jsou 3 sekundy, ale extrakce souboru trvá 5 sekund). Po uplynutí této doby nebudou zbývající soubory v archivu kontrolovány.


Chcete-li omezit dobu kontroly včetně větších archivů, použijte nastavení **Maximální velikost objektu** a Maximální velikost souboru v archivu (nedoporučuje se z důvodu možných bezpečnostních rizik).

Výchozí hodnota: **neomezeno**.

Nastavení kontroly archivů

Úroveň vnoření archivů – specifikuje maximální úroveň vnoření do archivu při kontrole archivu. Výchozí hodnota: 10.

Maximální velikost souboru v archivu – specifikuje maximální velikost rozbaleného souboru v archivu, který je kontrolován. Maximální hodnota: **3 GB**.

 Nedoporučujeme měnit přednastavené hodnoty, protože většinou není pro tuto změnu důvod.

Úrovně léčení

Chcete-li změnit nastavení úrovně léčení pro určitý ochranný modul, rozbalte položku **ThreatSense** (například **Rezidentní ochrana souborového systému**) a poté z rozbalovacího menu vyberte **Úroveň léčení**.

ThreatSense má následující úrovně řešení (tj. čištění).

Řešení infekce v ESET NOD32 Antivirus

Úroveň léčení	Popis
Vždy vyřešit infekci	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých ojedinělých případech vyléčit (např. u systémových souborů), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak ponechat	V tomto režimu se program pokusí vyléčit detekované objekty bez zásahu uživatele. Pokud nelze detekci v některých případech vyléčit (např. v případě systémových souborů nebo archivů s neinfikovanými i infikovanými soubory zároveň), bude detekovaný objekt ponechán v původním umístění.
Pokud je to bezpečné, vyřešit infekci, jinak se dotázat	V tomto režimu se program pokusí vyléčit detekované objekty. Pokud není možné v některých případech akci provést, uživateli se zobrazí interaktivní upozornění, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Toto nastavení je doporučeno pro většinu případů.
Vždy se dotázat uživatele	V průběhu léčení objektů se uživateli zobrazí interaktivní okno, ve kterém musí vybrat požadovanou akci (např. odstranění nebo ignorování detekce). Tato úroveň je určena zkušeným uživatelům, kteří vědí, jaké kroky podniknout v případě výskytu detekce.

Přípony souborů vyloučených z kontroly

Přípony vyloučených souborů jsou součástí [ThreatSense](#). Chcete-li nakonfigurovat přípony vyloučených souborů, klikněte na **ThreatSense** v [Rozšířených nastaveních](#) pro jakýkoli [modul, který používá technologii ThreatSense](#).

Přípona je část názvu souboru oddělená tečkou. Přípona určuje typ a obsah souboru (například dokument.txt označuje textový dokument). V této části nastavení ThreatSense můžete definovat typy souborů, které chcete kontrolovat.



Nezaměňujte tuto funkci s možností pro [vyloučení procesů](#), tvorbu [HIPS výjimek](#) nebo [vyloučení souborů/složek](#).

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

Definovat výjimky je někdy nezbytné, jestliže jsou kontrolovány soubory s určitým rozšířením a kontrola by mohla mít negativní vliv na běh programu. Může být vhodné vyloučit např. `.edb`, `.eml` a `.tmp` pro MS Exchange Server).



Pro přidání přípony klikněte na tlačítko **Přidat**. Do zobrazeného prázdného pole zadejte příponu (například `tmp`) a akci potvrďte kliknutím na tlačítko **OK**. Zadat můžete **více hodnot** oddělené čárkou, středníkem nebo zadejte každou příponu na nový řádek (například po vybrání možnosti **Středník** můžete zadat `edb; eml ; tmp`).
Při definování seznamu výjimek můžete použít jako zástupný znak `?` (otazník). Otazník reprezentuje jeden znak (například `?db`).



Chcete-li v operačním systému Windows zobrazit příponu souboru (pokud existuje), musíte zaškrtnout políčko **Přípony názvů souborů** v **Průzkumníku Windows > Zobrazit**.

Doplňující parametry ThreatSense

Chcete-li upravit tato nastavení, otevřete [Rozšířená nastavení](#) > **Ochrany** > **Rezidentní ochrana souborového systému** > **Další parametry ThreatSense**.

Doplňující parametry ThreatSense pro nově vytvořený nebo upravený soubor

Pravděpodobnost napadení nově vytvořených nebo upravených souborů je vyšší než u existujících souborů. To je důvod, proč program tyto soubory kontroluje s doplňujícími parametry. Společně s kontrolou založenou na porovnávání vzorků je využívána rozšířená heuristika ESET NOD32 Antivirus, čímž se výrazně zvyšuje úroveň detekce, i když škodlivý kód ještě není znám před vydáním aktualizace detekčního jádra.

Kromě nově vytvářených souborů se kontrolují také **Samorozbalovací soubory** (.sfx) a **Runtime packery** (interně komprimované spustitelné soubory). Standardně jsou archivy kontrolovány do 10 úrovně vnoření bez ohledu na jejich velikost. Pro změnu nastavení kontroly archivů deaktivujte pomocí přepínače možnost **Standardní nastavení kontroly archivů**.

Doplňující parametry ThreatSense pro spouštěné soubory

Rozšířená heuristika pro spouštěné soubory – [rozšířená heuristika](#) se pro spouštěné soubory používá standardně. Pokud je zapnutá, důrazně doporučujeme ponechat zapnutou také [Smart optimalizaci](#) a [ESET LiveGrid®](#) pro snížení dopadu na výkon systému.

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

Nástroje

V [Rozšířených nastaveních](#) > **Nástroje** můžete nakonfigurovat pokročilá nastavení funkcí, které nabízejí dodatečné zabezpečení a pomáhají zjednodušit správu ESET NOD32 Antivirus.

- [Aktualizace operačního systému Windows](#)
- [ESET CMD](#)
- [Protokoly](#)
- [Herní režim](#)
- [Diagnostika](#)

Aktualizace operačního systému Windows

Aktualizace operačního systému Windows představují důležitou součást pro zajištění ochrany uživatelů před zneužitím bezpečnostních děr a tím pádem možným infikováním systému. Z tohoto důvodu je nezbytné, abyste aktualizace systému Microsoft Windows instalovali, jakmile budou k dispozici. ESET NOD32 Antivirus vás upozorní na chybějící aktualizace podle úrovně, kterou jste zadali v [Rozšířených nastaveních](#) > **Nástroje**. K dispozici jsou následující možnosti:

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

Dialogové okno – Aktualizace systému

Pokud jsou připravené aktualizace pro váš operační systém, [hlavním okně programu](#) na záložce **Přehled** se zobrazí související oznámení. Po kliknutí na možnost **Více informací** se zobrazí dialogové okno s přehledem dostupných aktualizací.

V tomto dialogovém okně naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Řazeny jsou dle názvu a vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Dvojklikem na konkrétní aktualizaci si zobrazíte podrobné [informace o dané aktualizaci](#).

Kliknutím na možnost **Spustit aktualizaci systému** stáhnete a nainstalujete všechny uvedené aktualizace operačního systému.

Informace o aktualizacích

V dialogovém okně Aktualizace systému naleznete přehled dostupných aktualizací, které je možné stáhnout a nainstalovat. Vpravo od aktualizací jsou zobrazeny informace o jejich prioritě.

Tlačítkem **Spustit aktualizace systému** zahájíte stahování a instalaci aktualizací operačního systému.

Po kliknutí pravým tlačítkem myši na danou aktualizaci a vybrání možnosti **Zobrazit informace** se zobrazí podrobné informace o aktualizaci.

ESET CMD

Jedná se o funkci, která povolí používání pokročilých cmd příkazů. Díky tomu můžete exportovat a importovat nastavení prostřednictvím příkazového řádku (cmd.exe). Až dosud bylo možné exportovat nastavení pomocí [GUI](#). Export konfigurace ESET NOD32 Antivirus můžete provést do souboru formátu *.xml*.

Po zapnutí funkce ESET CMD (v **Rozšířeném nastavení** v sekci **Nástroje > ESET CMD**) pomocí přepínače do polohy zapnuto si vyberte způsob ověření:

- **Žádný** – pokud vyberete tuto možnost, nebude vyžadováno ověření. Tuto možnost nedoporučujeme, protože představuje potenciální bezpečnostní riziko. V takovém případě totiž bude možné importovat nepodepsané konfigurace.
- **Heslo pro přístup do rozšířeného nastavení** – pro ověření se použije heslo, které chrání přístup do nastavení produktu. Před importováním konfigurace již musí být definováno heslo pro [přístup do nastavení](#). Konfigurace se neimportuje pokud nemáte nastavenou ochranu heslem, heslo nesouhlasí nebo importovaný .xml soubor není podepsán.

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



Pro použití ecmd příkazů musíte mít oprávnění administrátora, resp. je třeba je **spustit jako administrátor**. V opačném případě se zobrazí chyba **Error executing command**. Při exportování konfigurace musí cílová složka existovat. Export je možný i v případě, kdy je funkce ESET CMD v produktu vypnutá.



Konfiguraci z nainstalovaného produktu exportujete příkazem:

```
ecmd /getcfg c:\config\settings.xml
```

Konfiguraci do nainstalovaného produktu nainportujete příkazem:

```
ecmd /setcfg c:\config\settings.xml
```



Pokročilé ecmd příkazy je možné používat pouze lokálně.

Jak podepsat .xml/ konfigurační soubor:

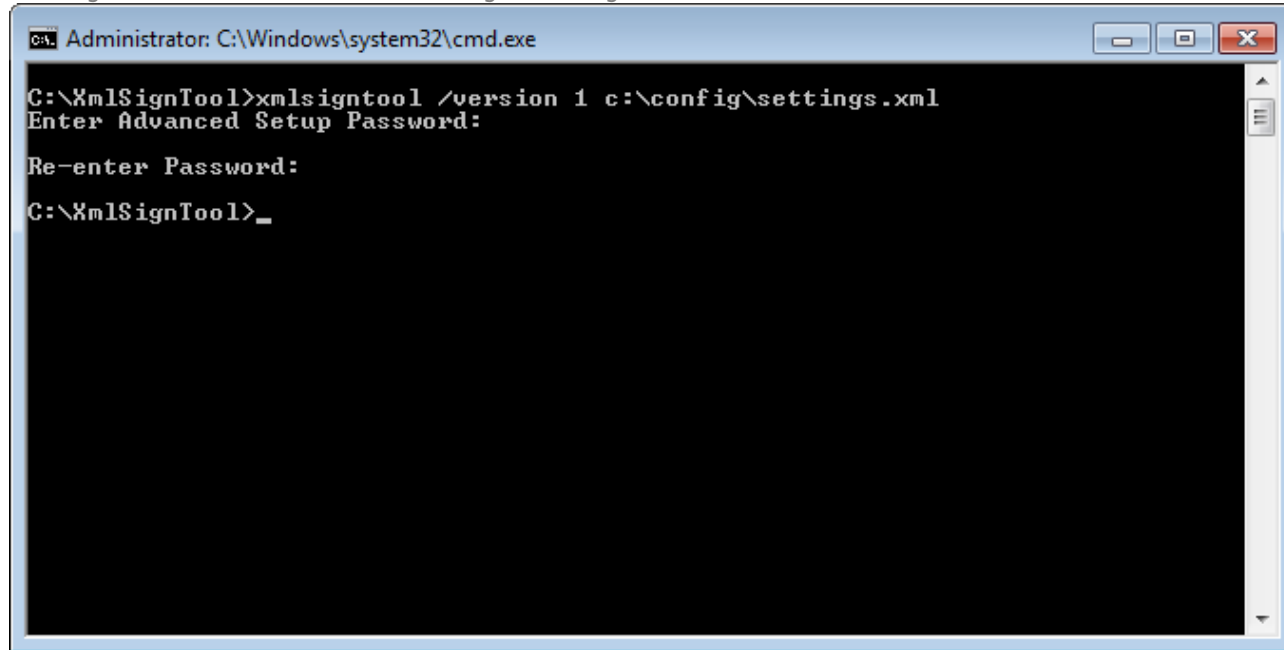
1. Z webových stránek společnosti ESET si stáhněte nástroj [XmlSignTool](#).
2. Příkazový řádek **Spusťte jako administrátor** (cmd).
3. Přejděte do složky se staženým nástrojem `xmlsigntool.exe`.
4. Konfigurační příkaz .xml/ podepište tímto příkazem: `xmlsigntool /version 1|2 <xml_file_path>`



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

5. Na výzvu nástroje XmlSignTool zadejte a znovu zadejte [heslo pro Rozšířená nastavení](#). Následně bude váš .xml/ soubor s konfigurací programu podepsán a můžete jej prostřednictvím ESET CMD importovat do jiné instalace ESET NOD32 Antivirus.

Příkaz pro podepsání konfiguračního souboru:
xmldsigntool /version 2 c:\config\settings.xml



V případě, že změníte heslo pro [přístup do nastavení](#) a budete chtít prostřednictvím ESET CMD importovat konfiguraci z .xml/souboru podepsaného původním heslem, podepište jej nejprve aktuálním heslem. Tímto budete moci využít starší konfigurační soubor, aniž byste jej museli před importem exportovat z jiné běžící instalace ESET NOD32 Antivirus.



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**.

Protokoly

Konfiguraci protokolování ESET NOD32 Antivirus najdete v [Rozšířených nastaveních](#) > **Nástroje** > **Protokoly**. V této sekci můžete upravit způsob správy protokolů. Program dokáže automaticky odstraňovat staré protokoly, čímž šetří místo na disku. V nastavení můžete vybrat následující možnosti:

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

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informační** – jedná se o informační zprávy, například o úspěšné aktualizaci, a všechny záznamy s vyšší závažností.
- **Varování** – do protokolu se zapíše kritické chyby, chybová a varovná hlášení.
- **Chyby** – kromě kritických varování se zaznamenají chyby typu "Chyba při stahování souboru aktualizace".
- **Kritické chyby** – zaznamenají se pouze kritické chyby (chyba při spuštění antivirové ochrany, atd.).

i Všechna zablokovaná spojení se do protokolu zapíše při vybrání diagnostické úrovně.

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

Automaticky optimalizovat protokoly – pokud aktivujete tuto možnost, protokoly budou automaticky defragmentovány po dosažení mezní hranice definované v poli **Při překročení počtu nevyužitých záznamů (v procentech)**.

Kliknutím na **Optimalizovat** spustíte defragmentaci protokolů. Optimalizace odstraňuje prázdné záznamy v protokolech, čímž zvyšuje rychlost zpracovávání. Viditelné zlepšení práce s protokoly je po optimalizaci znatelné hlavně především u protokolů s velkým množstvím záznamů.



Pomocí možnosti **Zaznamenávat textové protokoly** aktivujete ukládání [protokolů](#) do odlišného formátu:

- **Cílová složka** – složka, do které se uloží protokoly (pouze pro Text/CSV). Každý protokol se ukládá do samostatného souboru (např. **detekce** naleznete v virlog.txt, pokud protokoly ukládáte jako prostý text).
- **Typ** – pokud vyberete **Text** jako formát souborů, protokoly budou uloženy do textového souboru, data budou oddělena tabulátorem. Stejný princip platí pro soubory oddělené čárkou **CSV**. Pokud vyberete **Událost**, protokol bude uložen do systémového Protokolu událostí, který si můžete zobrazit v Prohlížeči událostí.
- **Odstranit všechny protokoly** – po kliknutí vymaže všechny protokoly vybrané v rozbalovacím menu **Typ**. O úspěšném vymazání protokolů budete informováni.

i V rámci rychlého vyřešení problémů vás specialisté technické podpory ESET mohou požádat o zaslání protokolů. Pomocí nástroje ESET Log Collector snadno získáte diagnostické informace z počítače včetně protokolů. Pro více informací o používání ESET Log Collector navštivte [ESET Databázi znalostí](#).

Herní režim

Herní režim je funkce navržená pro uživatele, kteří vyžadují nepřetržité používání softwaru, nechťejí být rušeni okny s oznámeními nebo upozorněními a chtějí minimalizovat používání CPU. Herní režim oceníte v průběhu prezentací, kdy nechcete být rušeni aktivitami antiviru. Zapnutím této funkce zakážete zobrazování všech vyskakujících oken a všechny úlohy plánovače budou zastaveny. Samotná ochrana běží dál v pozadí, ale nevyžaduje žádné zásahy uživatele.

Herní režim můžete zapnout nebo vypnout v [hlavním okně programu](#) na záložce **Nastavení** > **Ochrana počítače** pomocí přepínače , resp.  na řádku **Herní režim**. Zapnutý herní režim představuje potenciální bezpečnostní riziko, proto se ikona stav ochrany na hlavní liště změní na oranžovou barvu a zobrazí se související upozornění. V [hlavním okně programu](#) se zobrazí oranžové upozornění, že **Herní režim je zapnutý**.

Vybráním možnosti **Automaticky zapnout herní režim při zobrazení aplikací na celou obrazovku** se herní režim při takovém zobrazení automaticky zapne a po jejím ukončení se vypne. Tato možnost je užitečná pro okamžité aktivování herního režimu po spuštění hry nebo zahájení prezentace a najdete si v [Rozšířených nastaveních](#) (dostupném po stisknutí klávesy v hlavním okně programu) v sekci **Nástroje** > **Herní režim**.

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

Diagnostika

Diagnostika poskytuje výpisy ze selhání běhu procesů programu ESET (například ekrn). Pokud aplikace spadne, vygeneruje se výpis, tzv. dump. Ten může pomoci vývojářům při ladění a opravě různých problémů v ESET NOD32 Antivirus.

Z rozbalovacího menu **Typ výpisu** vyberte jednu z níže uvedených možností:

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

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

Otevřete složku diagnostiky – klikněte na **Otevřít** k zobrazení obsahu výše uvedené složky v novém okně *Průzkumníku Windows*.

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

Rozšířené protokolování

Aktivovat rozšířené protokolování marketingových zpráv – po zapnutí se budou zaznamenávat všechny události související s marketingovými zprávami v rámci produktu.

Aktivovat rozšířené protokolování skeneru – po zapnutí se do protokolu zaznamenají všechny události, které vznikly při volitelné kontrole počítače.

Aktivovat diagnostické protokolování správy zařízení – po aktivování této možnosti se do souboru zapíše detailní informace z běhu správy zařízení. Toto nám pomůže diagnostikovat a odstranit potíže se správou zařízení.

Aktivovat rozšířené protokolování Direct Cloud – po aktivování této možnosti se do souboru zapíše detailní informace z běhu ESET LiveGrid®. Toto pomůže vývojářům při diagnostice a řešení problémů s ESET LiveGrid®.

Aktivovat rozšířené protokolování ochrany dokumentů – po zapnutí se zaznamenají veškeré události související s modulem Ochrana dokumentů. Toto pomůže vývojářům při diagnostice a řešení problémů.

Aktivovat rozšířené protokolování ochrany poštovních klientů – po aktivování této možnosti se do souboru zapíše detailní informace z běhu ochrany poštovních klientů a jejího doplňku. Toto pomůže vývojářům při diagnostice a řešení problémů s touto součástí programu.

Aktivovat rozšířené protokolování jádra – po zapnutí se zaznamenají všechny události, které se vyskytují v jádře ESET (ekrn).

Aktivovat rozšířené protokolování licence – po aktivování této možnosti se zaznamená veškerá komunikace

produktu s licenčními servery (ESET License Manager).

Aktivovat výpis paměti – po aktivování této možnosti se zaznamenají všechny události, které pomohou vývojářům při diagnostice úniku dat z paměti (memory leaku).

Aktivovat rozšířené protokolování kontroly síťové komunikace – zaznamenávání všech dat procházejících kontrolou síťové komunikace do souboru ve formátu PCAP, který pomůže vývojářům při diagnostice a řešení problémů souvisejících s kontrolou síťového provozu.

Aktivovat rozšířené protokolování operačního systému – po aktivování se sesbírají dodatečné informace o operačním systému jako jsou běžící procesy, aktivita CPU a diskové operace. Toto pomůže vývojářům při diagnostice a řešení problémů s chodem programu ve vašem operačním systému.

Aktivovat rozšířené protokolování push zpráv – po zapnutí se zaznamenají všechny události, ke kterým dojde během odesílání push zpráv.

Aktivovat rozšířené protokolování rezidentní ochrany souborového systému – po aktivování této možnosti se do protokolu zaznamenají všechny události, které vznikly při běhu rezidentní ochrany souborového systému.

Aktivovat rozšířené protokolování modulu aktualizace – po aktivování této možnosti se do souboru zapíše všechny události, ke kterým dojde během procesu aktualizace. Toto pomůže vývojářům při diagnostice a řešení problémů s modulem zajišťujícím aktualizaci programu.

Protokoly se nachází ve složce `C:\ProgramData\ESET\ESET Security\Diagnostics\`.

Technická podpora

Pokud zakládáte z ESET NOD32 Antivirus požadavek na [Technickou podporu ESET](#), můžete zjednodušit práci našim expertům odesláním konfiguračních dat systému. Z rozbalovací nabídky **Odeslat konfiguraci systému** zvolte možnost **Odeslat vždy** pro automatické odeslání dat nebo **Dotázat se před odesláním**, pokud chcete mít před založením požadavku možnost volby.

Připojení

V určitých sítích může proxy server zprostředkovávat komunikaci mezi vaším zařízením a internetem. Pokud používáte proxy server, je třeba provést následující nastavení. V opačném případě se ESET NOD32 Antivirus a jeho moduly nemohou automaticky aktualizovat. V ESET NOD32 Antivirus je nastavení proxy serveru k dispozici ve dvou různých sekcích v [Rozšířených nastaveních](#).

V prvním případě můžete nastavení serveru konfigurovat v části [Rozšířená nastavení](#) > **Připojení** > **Proxy server**. Tato nastavení specifikují globální nastavení proxy serveru a tyto parametry se použijí pro jakýkoliv modul ESET NOD32 Antivirus. Nastavení budou používat všechny moduly vyžadující přístup k internetu.

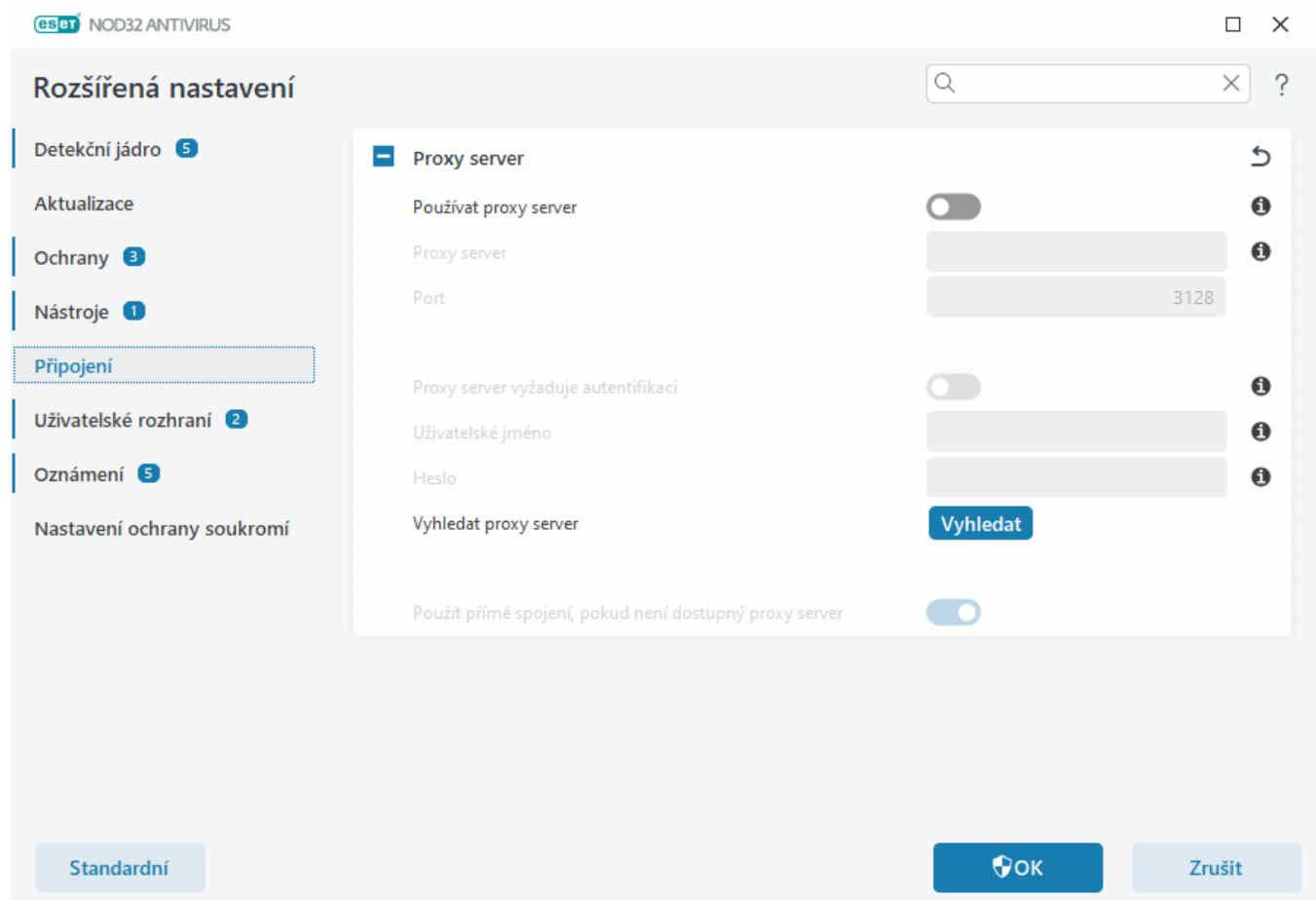
Chcete-li zadat globální nastavení proxy serveru, povolte možnost **Používat proxy server** a zadejte adresu **proxy serveru** spolu s číslem **portu** proxy serveru.

Pokud komunikace s proxy serverem vyžaduje ověření, vyberte možnost **Proxy server vyžaduje ověření** a do příslušných polí zadejte platné **uživatelské jméno** a **heslo**. Klepnutím na **Vyhledat proxy server** se automaticky zjistí a vyplní nastavení proxy serveru. ESET NOD32 Antivirus zkopíruje parametry zadané v možnostech internetu pro Internet Explorer nebo Google Chrome.

i V nastavení **proxy serveru** musíte ručně zadat své uživatelské jméno a heslo.

Použít přímé spojení, pokud není dostupný proxy server – pokud máte nastaveno, že se má ESET NOD32 Antivirus připojovat k serverům ESET prostřednictvím proxy, po aktivování této možnosti se produkt pokusí navázat spojení bez použití proxy.

Nastavení proxy serveru lze provést také v [Rozšířených nastaveních](#) > **Aktualizace** > **Profily** > **Aktualizace** > **Možnosti připojení** výběrem možnosti **Připojení prostřednictvím proxy serveru** v rozbalovací nabídce **Režim proxy**. Tato konfigurace platí pouze pro aktualizace a doporučuje se pro notebooky, které přijímají aktualizace modulů ze vzdálených umístění. Další informace naleznete v kapitole [Pokročilé nastavení aktualizace](#).



Uživatelské rozhraní

Chcete-li nakonfigurovat chování grafického uživatelského rozhraní (GUI) programu, otevřete [Rozšířená nastavení](#) > **Uživatelské rozhraní**.

V části [prvky uživatelského rozhraní](#) můžete přizpůsobit vzhled rozhraní a množství použitých efektů.

Pro zajištění maximální bezpečnosti a zabránění nežádoucím změnám v nastavení programu, stejně tak jeho odinstalaci, si v sekci [Přístup k nastavení](#) nastavte heslo.

i Možnosti pro změnu chování systémových oznámení, upozornění na detekce a stavů aplikace naleznete v sekci [Oznámení](#).

Prvky uživatelského rozhraní

Uživatelské rozhraní ESET NOD32 Antivirus si můžete přizpůsobit svým potřebám. Tyto možnosti jsou dostupné v [Rozšířených nastaveních](#) v sekci **Uživatelské rozhraní > Prvky uživatelského rozhraní**.

Barevný režim – v této části zvolte barevné schéma, ve kterém se bude uživatelské rozhraní ESET NOD32 Antivirus zobrazovat:

- **Stejný jako barva systému** – rozhraní ESET NOD32 Antivirus se zobrazí ve stejném barevném schématu, jako uživatelské rozhraní vašeho operačního systému.
- **Tmavý** – ESET NOD32 Antivirus bude zobrazen v tmavém režimu.
- **Světlý** – ESET NOD32 Antivirus bude zobrazen ve světlém režimu.

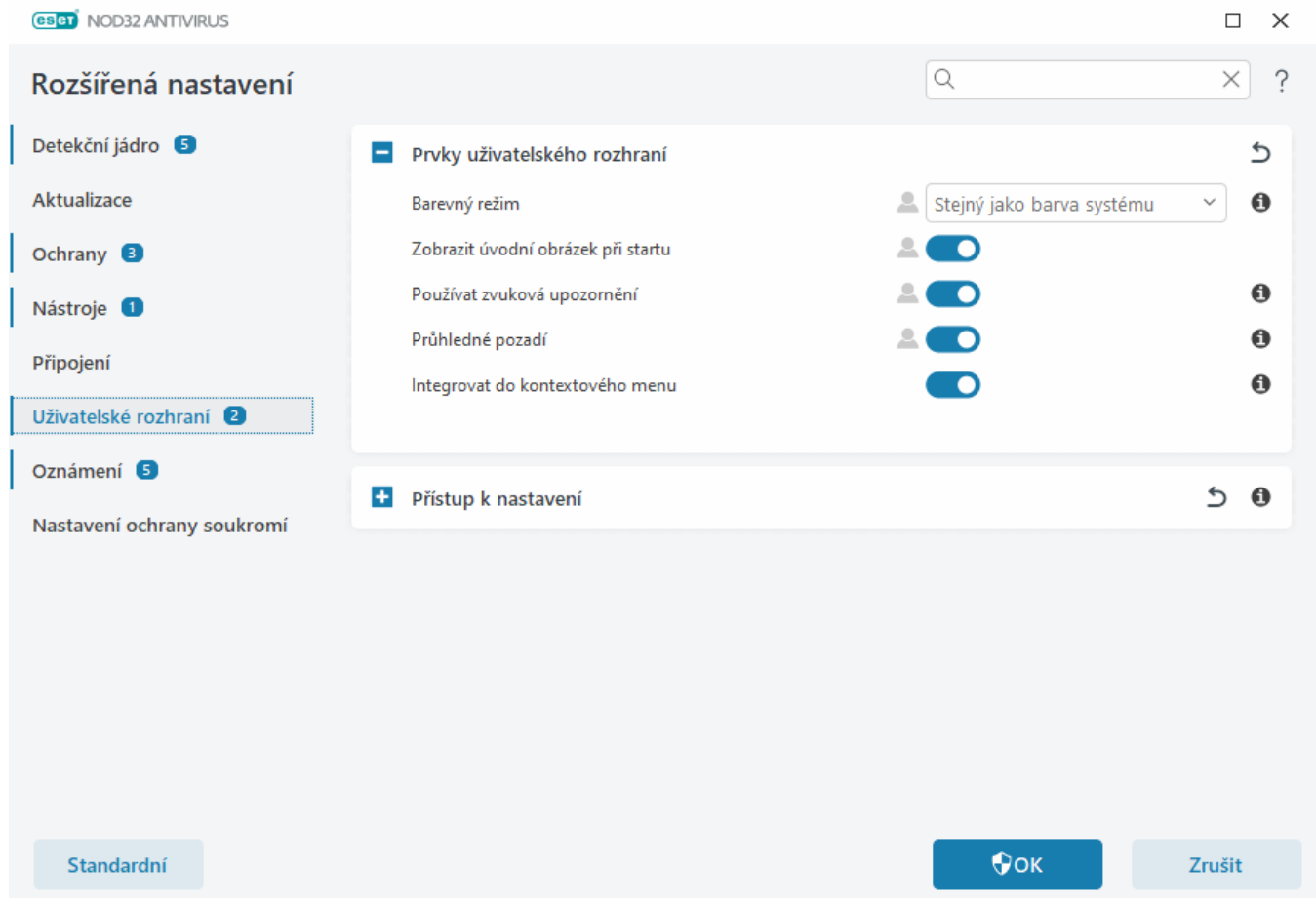
i V pravém horním rohu [hlavního okna programu](#) si můžete navolit barevný režim, ve kterém se vám bude zobrazovat uživatelské rozhraní ESET NOD32 Antivirus.

Zobrazit úvodní obrázek při startu – po zapnutí se bude obrázek ESET NOD32 Antivirus zobrazovat na krátkou dobu po startu systému a následném prvním přihlášení k uživatelskému účtu Windows.

Používat zvuková upozornění – po zapnutí bude program přehrávat zvuky při důležitých událostech (například při detekci hrozby či dokončené kontrole)

Průhledné pozadí – pomocí této možnosti si zapnete efekt průhledného pozadí [hlavního okna programu](#). Průhledné pozadí je k dispozici pouze u nejnovější verze systému Windows (RS4 a novější).

Integrovat do kontextového menu – pomocí této možnosti integrujete ovládací prvky programu ESET NOD32 Antivirus do kontextového menu.



Přístup k nastavení

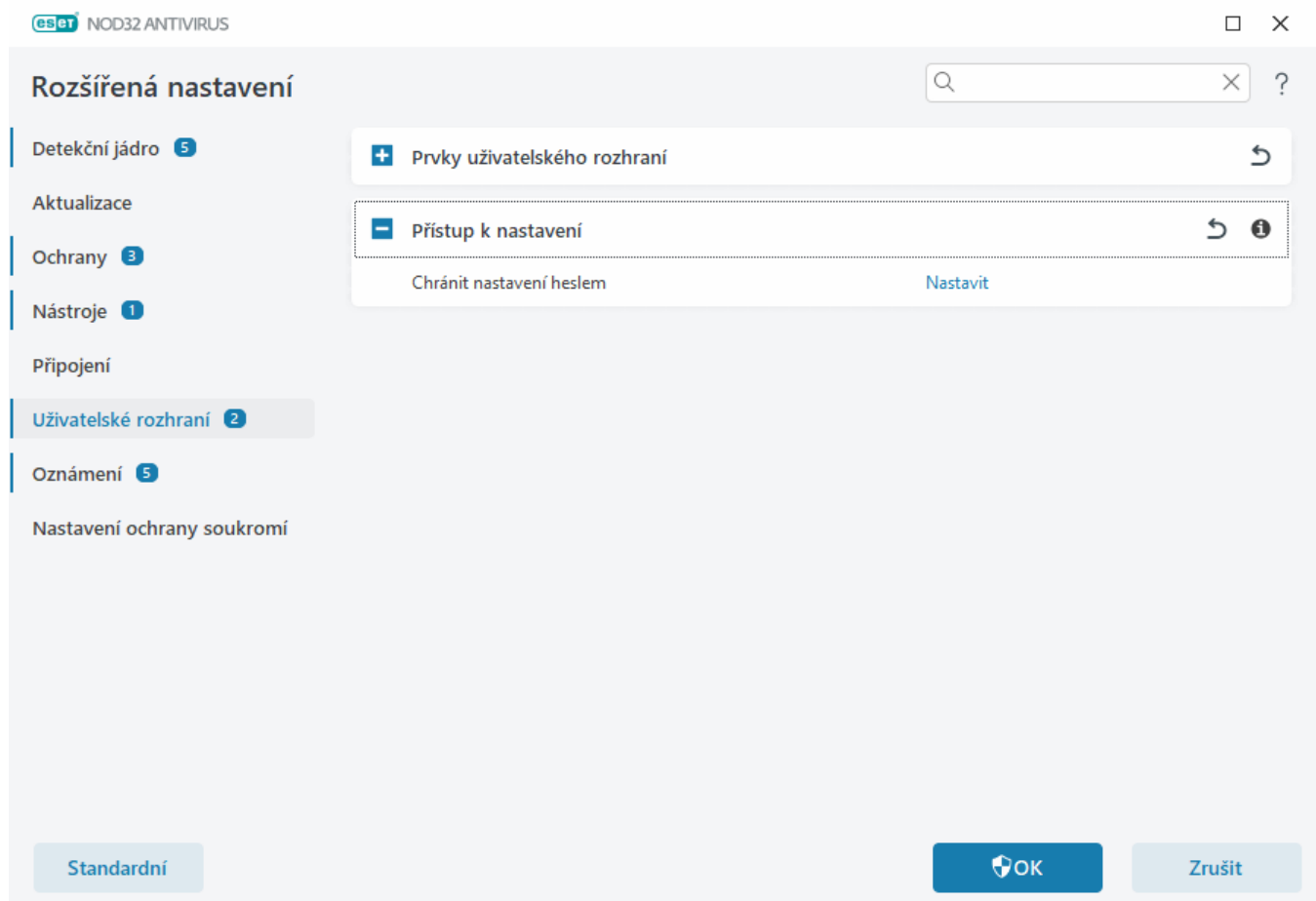
Správné nastavení ESET NOD32 Antivirus je velmi důležité pro celkové zabezpečení systému. Neoprávněná změna může vést ke snížení stability a ochrany. Prevencí proti neoprávněným změnám v ESET NOD32 Antivirus je možnost nastavení hesla. Nastavení přístupu lze konfigurovat v [Rozšířených nastaveních](#) > **Uživatelské rozhraní** > **Přístup k nastavení**.

Heslo jako prvek zabezpečení proti neoprávněnému nastavení ESET NOD32 Antivirus nebo odinstalaci nastavte, případně změňte kliknutím na **Nastavit** vedle položky **Chránit nastavení heslem**.

- i** Pokud chcete přejít do chráněného zobrazení Rozšířených nastavení, zobrazí se okno pro zadání hesla. Pokud zapomenete nebo ztratíte své heslo, klikněte na **Obnovit heslo** a zadejte e-mailovou adresu, na kterou máte registrovanou licenci, případně adresu k vašemu účtu ESET HOME, dle zvolené možnosti. Na tuto adresu vám ESET zašle ověřovací kód společně s návodem na reset hesla.
- [Jak obnovit přístup do rozšířeného nastavení?](#)

Pro změnu hesla klikněte na **Změnit heslo** vedle položky **Chránit nastavení heslem**.

Pro odstranění hesla klikněte na **Odstranit** vedle položky **Chránit nastavení heslem**.



Heslo pro přístup do Rozšířeného nastavení

Rozšířená nastavení ESET NOD32 Antivirus doporučujeme ochránit před neoprávněnými změnami heslem. Heslo zadejte do polí **Nové heslo** a **Potvrzení hesla**. Klikněte na tlačítko **OK**.

Při změně stávajícího hesla:

1. Staré heslo zadejte do pole **Původní heslo**.
2. Nové heslo zadejte dvakrát do polí **Nové heslo** a **Potvrzení hesla**.
3. Klikněte na tlačítko **OK**.

Nastavené heslo bude následně vyžadováno k přístupu do Rozšířených nastavení.

Pokud heslo zapomenete, prostudujte si článek: [Co dělat, pokud zapomenete heslo do nastavení programu ESET](#)

Pokud jste ztratili licenční klíč a potřebujete ověřit datum platnosti nebo jiné informace týkající se vaší licence k produktu ESET NOD32 Antivirus, postupujte podle kroků na stránce [Ztratili jste licenční údaje k produktu ESET?](#)

Podpora odečítačů obrazovky

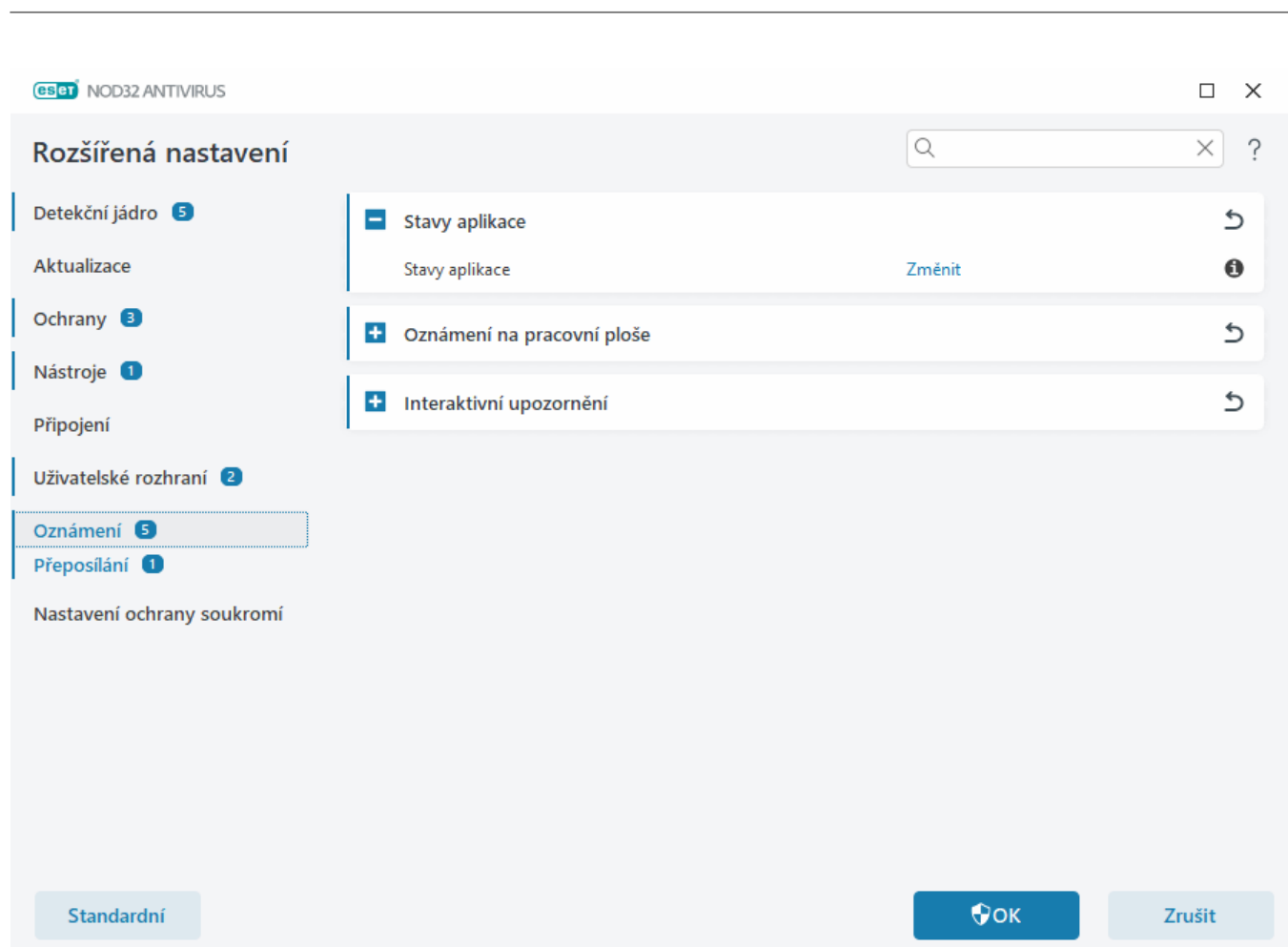
ESET NOD32 Antivirus lze použít společně s odečítači obrazovky, aby se mohli uživatelé ESET se zrakovým hendikepem lépe orientovat v produktu nebo konfigurovat nastavení. Podporovány jsou odečítače obrazovky (JAWS, NVDA, Narrator).

Pro kontrolu, zda má software odečítače obrazovky správný přístup k uživatelskému rozhraní ESET NOD32 Antivirus, si přečtěte návod v [Databázi znalostí](#).

Oznámení

Chcete-li spravovat oznámení ESET NOD32 Antivirus, otevřete [Rozšířená nastavení](#) > **Oznámení**. V této části můžete konfigurovat následující typy oznámení:

- Stav aplikace – jedná se o oznámení, která se zobrazují v [hlavním okně programu](#) > **Přehled**.
- [Oznámení na pracovní ploše](#) – malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami).
- [Interaktivní upozornění](#) – výstražná upozornění a informační okna, která vyžadují interakci uživatele.
- [Přeposílání](#) (e-mailová oznámení) – oznámení se zasílají e-mailem na konkrétní adresy.



– Stav aplikace

Stav aplikace – po kliknutí na **Změnit** se můžete rozhodnout, jaké stavy aplikace chcete zobrazovat v [hlavním okně programu](#) > v části **Přehled**.

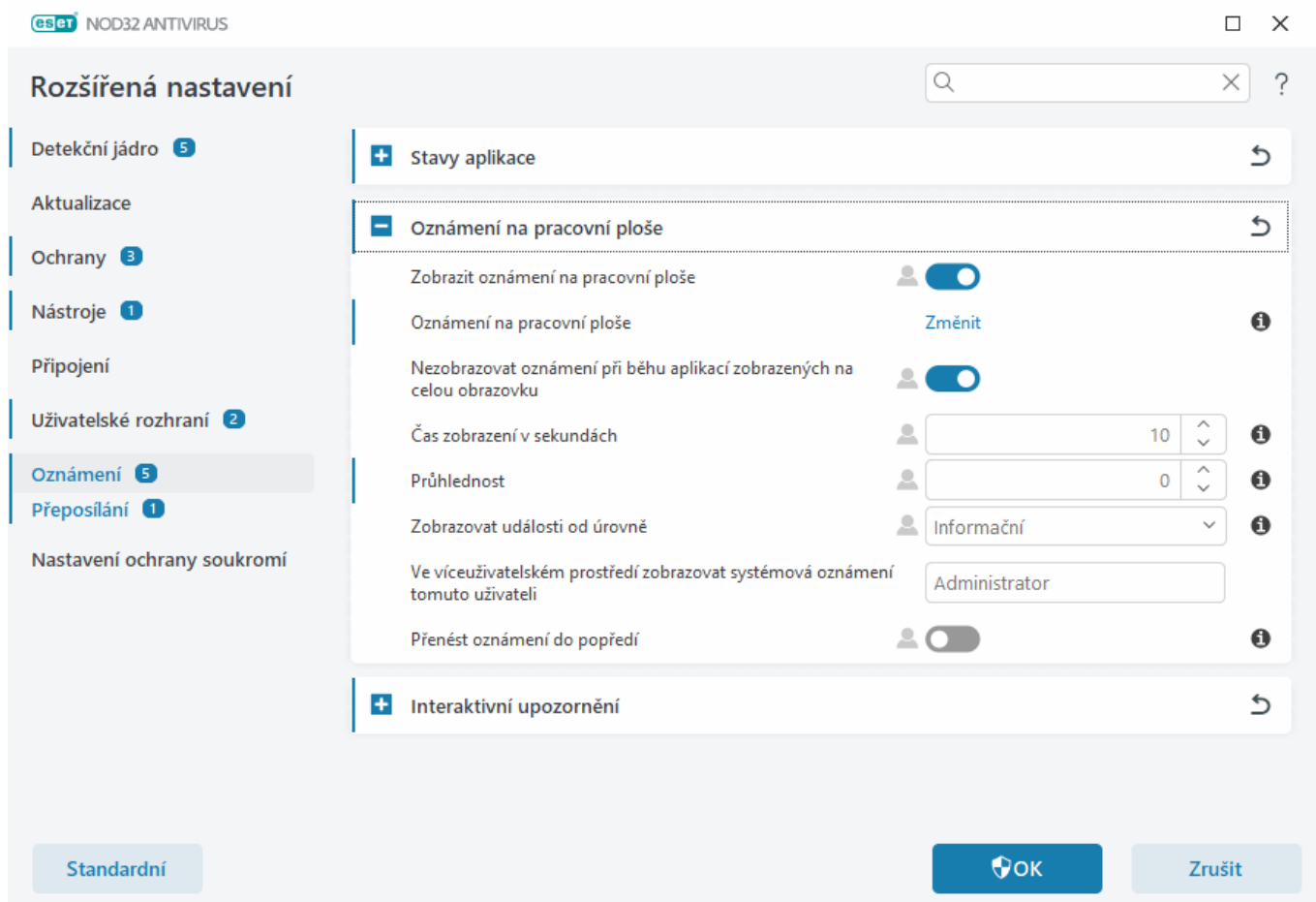
Dialogová okna – Stavy aplikace

V tomto dialogovém okně můžete aktivovat nebo deaktivovat upozornění na konkrétní stavy aplikace. Například můžete deaktivovat upozornění pro pozastavenou antivirovou a antispywarovou ochranu nebo zapnutý Herní režim.

Mezi sledované stavy aplikace patří také, zda je produkt aktivován, a jestli nevypršela platnost licence.

Oznámení na pracovní ploše

Oznámení na pracovní ploše jsou malá informační okna zobrazovaná v oznamovací oblasti Windows (nad hodinami). Ve výchozím nastavení se zobrazí po dobu 10 sekund a následně pomalu zmizí. Oznámení zahrnují informace o provedených aktualizacích, nově připojených zařízeních, dokončených kontrolách nebo nalezených hrozbách.



Zobrazovat oznámení na pracovní ploše – tuto možnost doporučujeme ponechat aktivní, aby vás produkt mohl informovat o nových událostech.

Oznámení aplikace – klikněte na **Změnit** a následně si vyberte [oznámení](#), která chcete nebo nechcete zobrazovat.

Nezobrazovat oznámení při běhu aplikací zobrazených na celou obrazovku – pomocí této možnosti potlačíte zobrazení všech oznámení v režimu celé obrazovky, která nevyžadují interakci.

Čas v sekundách – nastavte dobu viditelnosti oznámení. Hodnota musí být mezi 3 a 30 sekundami.

Průhlednost – nastavte průhlednost zobrazeného oznámení v procentech. Podporovaný rozsah je od 0 (neprůhledné) do 80 (velmi průhledné).

Zobrazovat události od úrovně – nastavit úroveň závažnosti oznámení, od které chcete být informováni. V rozbalovací nabídce vyberte následující možnosti:

O Diagnostické – zobrazuje informace pro řešení problémů a všechny níže uvedené záznamy.

O Informativní – zobrazuje informativní zprávy o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy.

O Varování – zobrazuje varování, upozornění na chyby a kritické chyby (například, selhala aktualizace modulů).

O Chyby – zobrazuje chyby (například nefunkční ochrana dokumentů).

O Kritická – zobrazuje kritické chyby (například problém s antivirovou ochranou nebo upozornění na infiltraci v systému).

Ve víceuživatelském prostředí posílat systémová hlášení tomuto uživateli – nastavte uživatelský účet počítače, který bude dostávat oznámení na pracovní ploše. Pokud například nepoužíváte administrátorský účet, zadejte název toho účtu, který má být o nových událostech v produktu informovaný. Definovat je možné pouze jeden uživatelský účet.

Přenést oznámení do popředí – po aktivování této možnosti se okno oznámení přesune do popředí obrazovky a bude dostupné pomocí klávesové zkratky **ALT + TAB**.

Seznam oznámení na pracovní ploše

Kdykoli se můžete rozhodnout, jaká oznámení produktu chcete zobrazovat na pracovní ploše (v pravém dolním rohu obrazovky). Otevřete si [Rozšířená nastavení](#) > **Oznámení** > **Oznámení na pracovní ploše**. Na řádku **Oznámení na pracovní ploše** klikněte na **Změnit** a následně v zobrazeném dialogovém okně jednotlivá oznámení zapněte pomocí zaškrtnutí pole ve sloupci **Zobrazit na ploše**.

Vyberte oznámení, která chcete zobrazovat na pracovní ploše



Název	Zobrazit na ploše
AKTUALIZACE	
Detekční jádro bylo úspěšně aktualizováno	<input type="checkbox"/>
Je připravena aktualizace aplikace	<input checked="" type="checkbox"/>
Moduly byly úspěšně aktualizovány	<input type="checkbox"/>
OBECNÉ	
Soubor byl odeslán k analýze	<input type="checkbox"/>
Zobrazit oznámení Co je nového	<input checked="" type="checkbox"/>
Zobrazovat oznámení z bezpečnostního přehledu	<input type="checkbox"/>

OK

Zrušit

Obecné

Zobrazovat oznámení z bezpečnostního přehledu - po zapnutí vás produkt upozorní na nově dostupný [bezpečnostní přehled](#).

Zobrazit oznámení Co je nového – vypnutím skryjete oznámení o všech nových a vylepšených funkcích nejnovější verze produktu.

Soubor byl odeslán k analýze – po jejím aktivování se zobrazí oznámení pokaždé, když produkt ESET NOD32 Antivirus zašlete soubor k analýze do virových laboratoří společnosti ESET.

Síťová ochrana

Upozornění na nezabezpečenou Wi-Fi – při pokusu o připojení k síti Wi-Fi se slabým nebo žádným heslem obdržíte upozornění.

Aktualizace

Je připravena aktualizace aplikace – po jejím aktivování budete upozorněni na dostupnou aktualizaci produktu ESET NOD32 Antivirus připravenou k nainstalování.

Detekční jádro bylo úspěšně aktualizováno – po zapnutí produkt zobrazí oznámení po každé aktualizaci detekčního jádra a programových modulů.

Moduly byly úspěšně aktualizovány – po zapnutí produkt zobrazí oznámení po každé aktualizaci programových komponent.

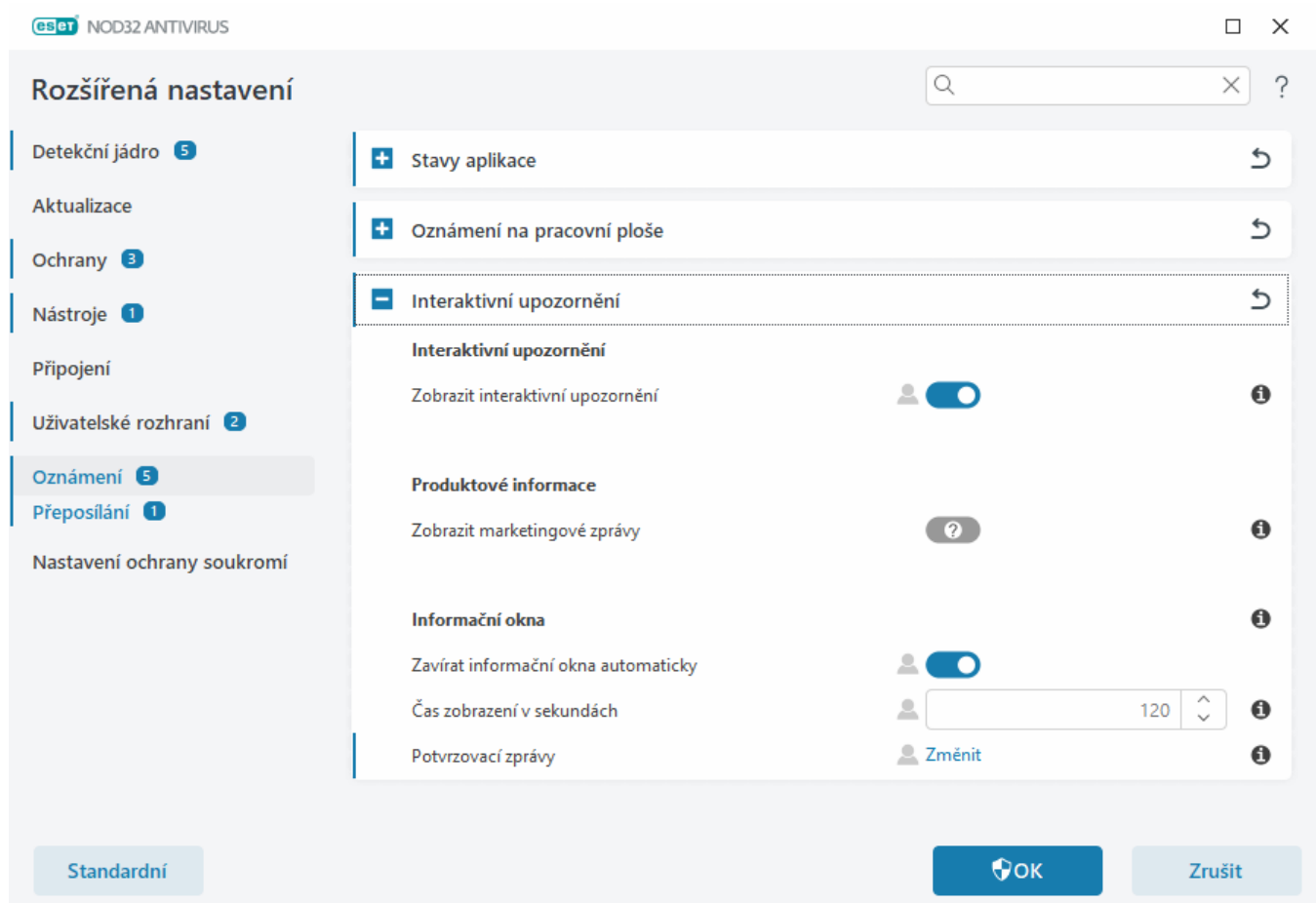
Obecná nastavení oznámení na ploše (například jak dlouho se má zpráva zobrazovat nebo minimální slovní rozsah zobrazovaných událostí) naleznete v části [Oznámení na ploše](#) v [Rozšířených nastaveních](#) > **Oznámení**.

Interaktivní upozornění

Hledáte informace o běžných upozorněních a oznámeních?

- [Nalezena hrozba](#)
- [Přístup na adresu byl zablokován](#)
- [Produkt není aktivován](#)
- [Změna na produkt s vyšším množstvím bezpečnostních funkcí](#)
- [Změna na produkt s nižším množstvím bezpečnostních funkcí](#)
- [Je dostupná aktualizace](#)
- [Informace o aktualizaci nejsou konzistentní](#)
- [Řešení problémů pro chybové hlášení "Moduly se nepodařilo aktualizovat"](#)
- [Řešení problémů s aktualizací modulů](#)
- [Certifikát webové stránky byl zamítnut](#)

V **Rozšířených nastaveních** v sekci [Oznámení](#) > **Interaktivní upozornění** můžete nastavit, jak se má ESET NOD32 Antivirus zachovat, pokud bude při detekci vyžadovat interakci uživatele (například při pokusu o přístup na potenciálně phishingovou stránku), stejně tak způsob zobrazování informačních oken.



Interaktivní upozornění

Vypnutí možnosti **Zobrazit interaktivní upozornění** skryje všechna dialogová okna s upozorněními, včetně informací ve webových prohlížečích. Tuto možnost je vhodné vypnout pouze v určitých situacích. Doporučujeme ponechat tuto možnost zapnutou.

Produktové informace

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

Informační okna

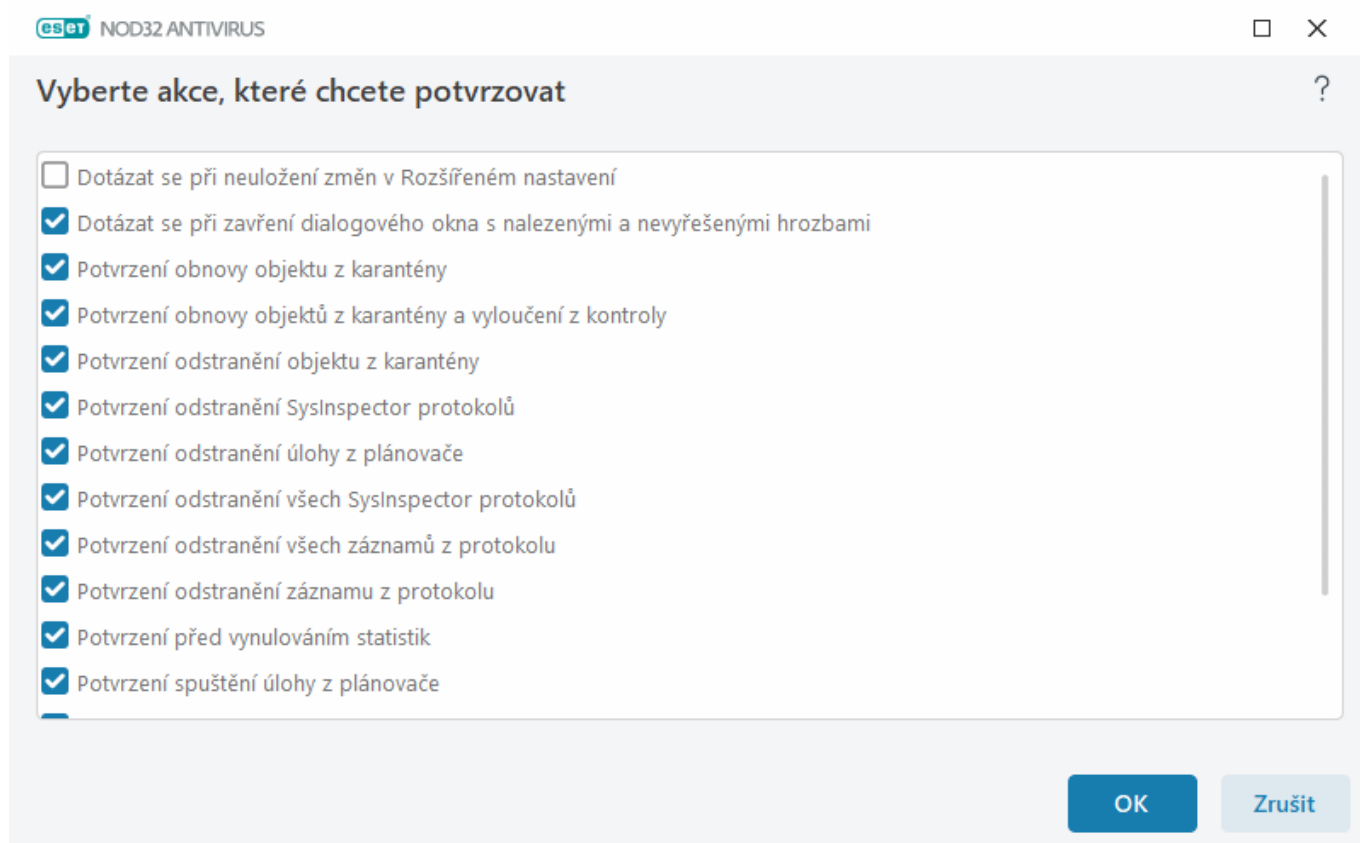
Dobu zobrazení informačních oken nastavíte pomocí možnosti **Zavírat informační okna automaticky**. Po uplynutí nastaveného času se okno s upozorněním zavře, pokud jej dříve nezavřete ručně.

Čas v sekundách – nastavte dobu viditelnosti oznámení. Hodnota musí být mezi 10 a 999 sekundami.

Potvrzovací zprávy – pomocí této možnosti můžete spravovat [seznam potvrzovacích zpráv](#), jejichž zobrazování chcete povolit nebo zakázat.

Potvrzovací zprávy

Chcete-li upravit potvrzovací zprávy, otevřete [Rozšířená nastavení](#) > **Oznámení** > **Interaktivní upozornění** a klikněte na **Upravit** vedle položky **Potvrzovací zprávy**.



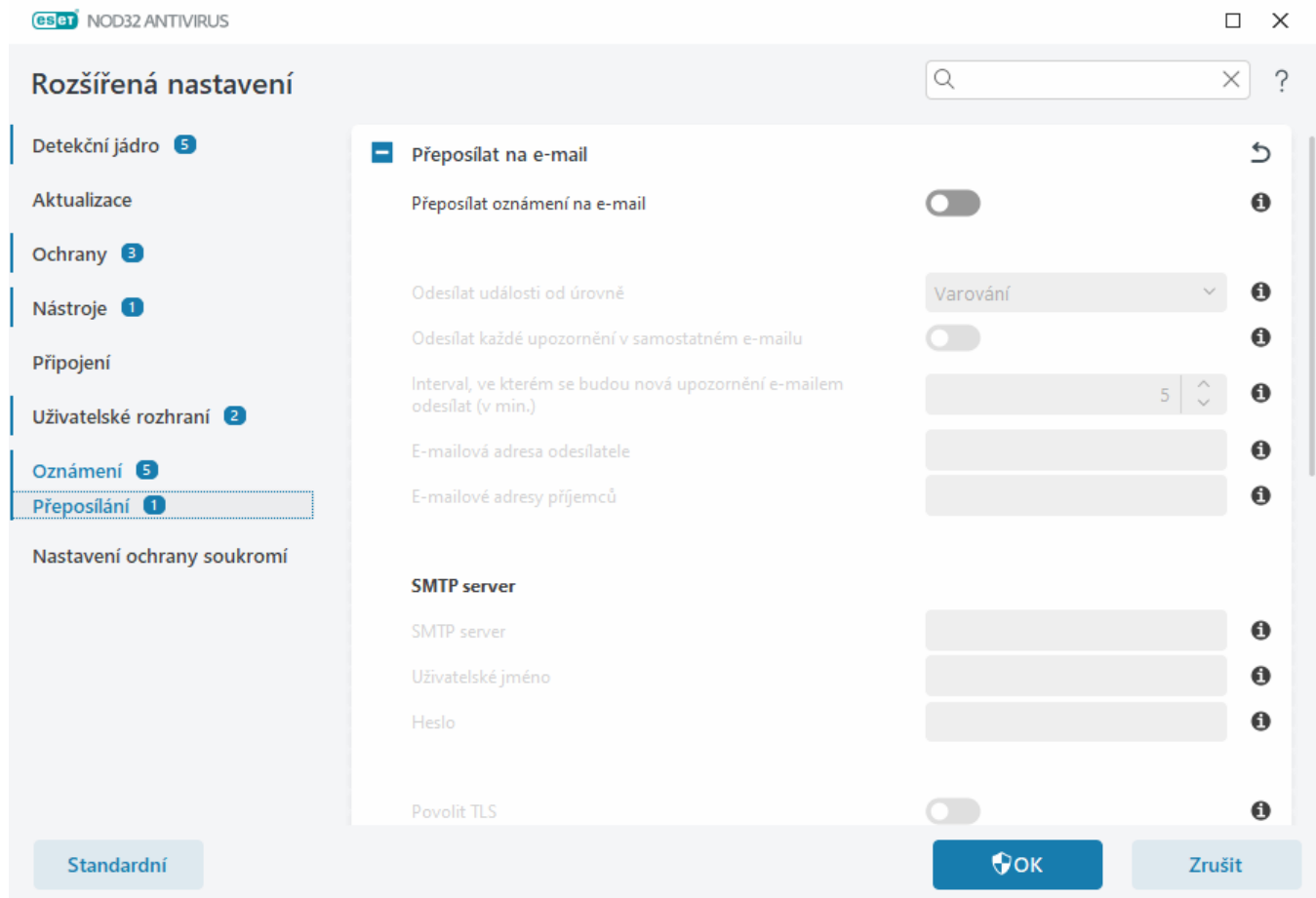
V tomto dialogovém okně můžete upravit zobrazování potvrzovacích zpráv, které ESET NOD32 Antivirus zobrazí před provedením akce. Pro jejich aktivaci nebo deaktivaci použijte zaškrtačací pole na daném řádku.

Pro více informací o konkrétní funkci související s potvrzovacími zprávami klikněte na odkaz:

- [Potvrzení odstranění ESET SysInspector protokolů](#)
- [Potvrzení odstranění všech ESET SysInspector protokolů](#)
- [Potvrzení odstranění objektu z karantény](#)
- Dotázat se při neuložení změn v Rozšířeném nastavení
- [Dotázat se při zavření dialogového okna s nalezenými a nevyřešenými hrozbami](#)
- [Potvrzení odstranění záznamu z protokolu](#)
- [Potvrzení odstranění úlohy z plánovače](#)
- [Potvrzení odstranění všech záznamů z protokolu](#)
- [Potvrzení před vynulováním statistik](#)
- [Potvrzení obnovení objektu z karantény](#)
- [Potvrzení obnovení objektů z karantény a vyloučení z kontroly](#)
- [Potvrzení spuštění úlohy z plánovače](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovních klientů Outlook Express a Windows Mail](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Windows Mail](#)
- [Zobrazit potvrzovací dialog produktu pro integraci doplňku do poštovního klienta Microsoft Outlook](#)

Přeposílání

ESET NOD32 Antivirus dokáže odesílat e-maily při výskytu události s nastavenou úrovní důležitosti. Pro aktivování zaslání upozornění e-mailem otevřete [Rozšířená nastavení](#) > **Oznámení** > **Přeposílání** a zapněte možnost **Přeposílat oznámení na e-mail**.



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

- **Diagnostické** – do protokolu se zapíše diagnostické informace pro řešení problémů a všechny záznamy s vyšší závažností.
- **Informativní** – e-mailem se odešlou informace o nestandardních síťových událostech, informace o úspěšné aktualizaci modulů a všechny níže uvedené záznamy,
- **Varování** – do protokolu se zapíše kritické chyby, chybová a varovná hlášení (například, aktualizace se nezdařila).
- **Chyby** – e-mailem se odešlou upozornění na chybové stavy aplikace (například nefunkční ochrana dokumentů),
- **Kritické chyby** – obsahují pouze kritické chyby (chyba při startu antivirové ochrany nebo infiltraci v systému),

Odesílat každé upozornění v samostatném e-mailu – pokud je tato možnost aktivní, příjemce obdrží při výskytu události nové upozornění. Při výskytu velkého množství událostí v krátkém čase obdrží příjemce velké množství e-mailů.


Interval, ve kterém se budou nová upozornění odesílat (v min.) – interval v minutách, po jehož uplynutí bude odeslán souhrnný e-mail se všemi upozorněními na události, které se v daném intervalu vyskytly. Pokud nastavíte hodnotu na 0, upozornění bude odesláno okamžitě po jeho výskytu.

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

E-mailová adresa příjemce – specifikuje adresu příjemce, která se použije v hlavičce e-mailové zprávy. Podporováno je více hodnot. Jako oddělovač použijte středník.

SMTP server

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

 ESET NOD32 Antivirus podporují SMTP servery s TLS šifrováním.

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

Povolit TLS – po aktivování této možnosti se budou oznámení a bezpečnostní upozornění zasílat šifrovaně prostřednictvím TLS.

Otestovat konfiguraci SMTP – Pomocí tohoto tlačítka odešlete testovací e-mail na e-mailovou adresu příjemce. Je třeba, abyste před odesláním vyplnili údaje, jako SMTP server, uživatelské jméno, heslo, adresa odesílatele a adresa příjemce.

Formát zprávy

Komunikace mezi programem a vzdáleným uživatelem nebo systémovým administrátorem probíhá prostřednictvím e-mailu nebo LAN zpráv (s využitím služby Windows messaging). Standardně je aktivní možnost **Použít výchozí formát zprávy**, který je vhodný pro většinu situací. V případě potřeby si jej můžete přizpůsobit svým požadavkům.

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

Formát zprávy s upozorněním na hrozbu – přednastavený formát zpráv je vhodný pro většinu situací. Měnit jej doporučujeme pouze v ojedinělých případech. V některých případech (například pokud máte systém pro automatické zpracování zpráv), může být potřeba změnit formát zprávy.

Znaková sada – převede e-mailovou zprávu do ANSI kódování, které je nastaveno v regionálním nastavení systému Windows (např. windows-1250, Unicode (UTF-8), ACSII 7-bit nebo (ISO-2022-JP)). To znamená, že se například znak "á" změní na "a", a neznámý symbol bude nahrazen otázníkem ("?").

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

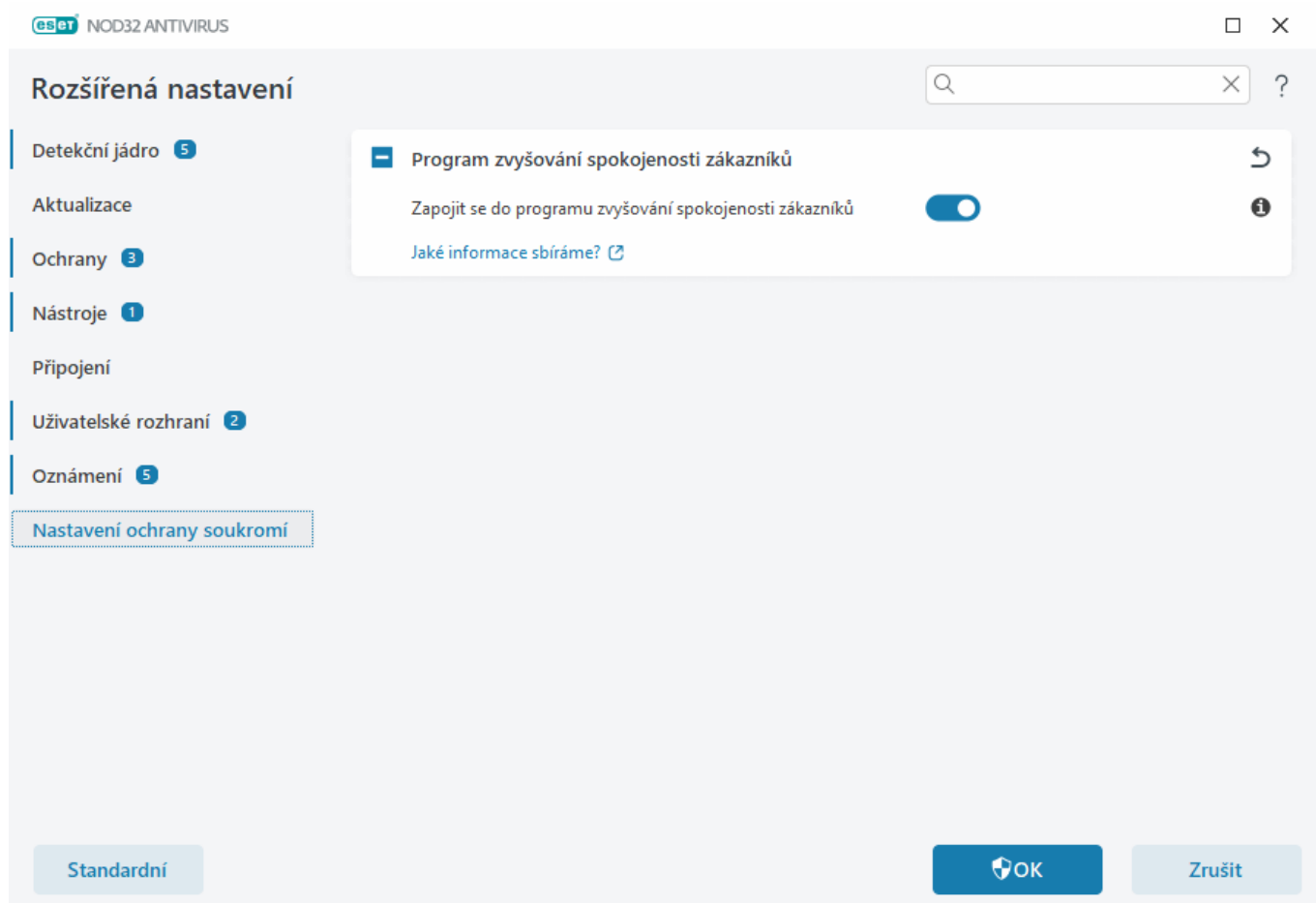
- **%TimeStamp%** – datum a čas události,
- **%Scanner%** – modul, který zaznamenal událost,
- **%ComputerName%** – název počítače, na kterém došlo k události,
- **%ProgramName%** – program, který způsobil událost,
- **%InfectedObject%** – název škodlivého souboru, e-mailové zprávy, apod.,

- **%VirusName%** – název infekce,
- **%Action%** – provedená akce,
- **%ErrorDescription%** – popis chyby.

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

Nastavení ochrany soukromí

Otevřete [Rozšířená nastavení](#) > **Nastavení soukromí**.



Program zvyšování spokojenosti zákazníků

Aktivací pomocí přepínače se můžete **Zapojit do programu zvyšování spokojenosti zákazníků**. Zapojením do programu poskytnete společnosti ESET anonymní informace související s používáním našich produktů. Shromážděné údaje nám pomohou zlepšit produkty. Informace nebudou sdíleny se třetími stranami. [Jaké informace sbíráme?](#)

Obnovit všechna nastavení na standardní

Kliknutím na **Standardní** v [Rozšířených nastaveních](#) vrátíte zpět všechna nastavení aplikace pro všechny moduly. Tím zajistíte, že se nastavení vrátí do stavu, v jakém byla po nové instalaci.

Dále se můžete podívat do kapitoly [Import a export nastavení](#).

Obnovit všechna nastavení v této sekci na standardní

Kliknutím na ikonu šipky ↩ obnovíte všechna nastavení v dané sekci na výchozí hodnoty definované společností ESET.

Prosím, mějte na paměti, že po kliknutí na tlačítko **Obnovit na standardní** budou všechny dosavadní změny ztraceny.

Obnovit obsah tabulek – po aktivování této možnosti se odstraní všechna ručně i automaticky přidaná pravidla, úlohy i profily.

Dále se můžete podívat do kapitoly [Import a export nastavení](#).

Chyba během ukládání nastavení

Tato chyba značí, že nastavení nebylo správně uloženo z důvodu chyby.

To obvykle znamená, že uživatel, který se pokoušel modifikovat nastavení programu:

- nemá dostatečná přístupová oprávnění nebo nemá nezbytná oprávnění operačního systému pro úpravu konfiguračních souborů a záznamů v registru systému.
> Pro provedení požadovaných změn se musí přihlásit administrátor systému.
- aktivoval učicí režim modulu HIPS nebo firewallu, a pokouší se provádět změny v jejich nastavení.
> Pro uložení nastavení a zabránění konfliktu ukončete Rozšířeném nastavení bez uložení změn, a zkuste změny provést znovu.

Druhou nejčastější příčinou bývá nekonzistentnost produktu, který nepracuje správně z důvodu svého poškození, a proto je nutné jej přeinstalovat.

Skener příkazového řádku

Modul antivirové ochrany produktu ESET NOD32 Antivirus můžete spustit pomocí příkazového řádku – ručně (příkazem "ecls") nebo dávkovým souborem typu "bat".

Použití ESET skeneru z příkazového řádku:

```
ecls [MOŽNOSTI..] SOUBORY..
```

Při spouštění volitelné kontroly prostřednictvím příkazového řádku můžete použít několik parametrů a přepínačů:

Možnosti

/base-dir=SLOŽKA	načíst moduly ze SLOŽKY
/quar-dir=SLOŽKA	SLOŽKA s karanténou
/exclude=MASKA	vyloučí soubory odpovídající MASCE z kontroly

/subdir	kontrolovat podsložky (standardně)
/no-subdir	nekontrolovat podsložky
/max-subdir-level=ÚROVEŇ	podsložky kontrolovat pouze do definované ÚROVNĚ vnoření
/symlink	následovat symbolické odkazy (standardně)
/no-symlink	přeskočit symbolické odkazy
/ads	kontrolovat ADS (standardně)
/no-ads	nekontrolovat ADS
/log-file=Soubor	zapisovat výstup do Souboru
/log-rewrite	přepisovat protokol (standardně se záznamy přidávají na konec souboru)
/log-console	zapisovat výstup do konzole (standardně)
/no-log-console	nezapisovat výstup do konzole
/log-all	zaznamenat do protokolu také čisté soubory
/no-log-all	nezaznamenávat do protokolu čisté soubory (standardně)
/aind	zobrazit průběh aktivity
/auto	automaticky zkontrolovat a vyléčit všechny lokální disky

Možnosti skeneru

/files	kontrolovat soubory (standardně)
/no-files	nekontrolovat soubory
/memory	kontrolovat paměť
/boots	kontrolovat boot sektory
/no-boots	nekontrolovat boot sektory (standardně)
/arch	kontrolovat archivy (standardně)
/no-arch	nekontrolovat archivy
/max-obj-size=VELIKOST	kontrolovat pouze soubory menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/max-arch-level=ÚROVEŇ	archivy kontrolovat do definované ÚROVNĚ vnoření
/scan-timeout=LIMIT	archivy kontrolovat nejdéle po definovaný LIMIT v sekundách
/max-arch-size=VELIKOST	kontrolovat pouze soubory v archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/max-sfx-size=VELIKOST	kontrolovat pouze soubory v samorozbalovacích archivech menší než VELIKOST v megabajtech (standardně 0 = neomezené)
/mail	kontrolovat poštovní soubory (standardně)
/no-mail	nekontrolovat poštovní soubory
/mailbox	kontrolovat poštovní schránky (standardně)
/no-mailbox	nekontrolovat poštovní schránky
/sfx	kontrolovat samorozbalovací archivy (standardně)
/no-sfx	nekontrolovat samorozbalovací archivy
/rtp	kontrolovat runtime packery (standardně)
/no-rtp	nekontrolovat runtime packery

/unsafe	detekovat potenciálně zneužitelné aplikace
/no-unsafe	nedetekovat potenciálně zneužitelné aplikace (standardně)
/unwanted	detekovat potenciálně nechtěné aplikace
/no-unwanted	nedetekovat potenciálně nechtěné aplikace (standardně)
/suspicious	detekovat podezřelé aplikace (standardně)
/no-suspicious	nedetekovat podezřelé aplikace
/pattern	používat signatury (standardně)
/no-pattern	nepoužívat signatury
/heur	zapnout heuristiku (standardně)
/no-heur	vypnout heuristiku
/adv-heur	zapnout rozšířenou heuristiku (standardně)
/no-adv-heur	vypnout rozšířenou heuristiku
/ext-exclude=PŘÍPONY	vyločit z kontroly dvojtečkou oddělené PŘÍPONY
/clean-mode=REŽIM	<p>použít REŽIM léčení infikovaných objektů</p> <p>K dispozici jsou následující možnosti:</p> <ul style="list-style-type: none"> • none (standardně) – automaticky se nevyléčí žádné objekty. • standard – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit. • strict – ecls.exe se pokusí infikované objekty automaticky vyléčit nebo odstranit bez interakce uživatele (nebudete dotázáni na vymazání souboru). • rigorous – ecls.exe automaticky odstraní soubor bez pokusu o jeho vyléčení. • delete – ecls.exe automaticky odstraní soubor bez pokusu o jeho vyléčení, ale neodstraní se důležité systémové soubory Windows.
/quarantine	uložit infikované soubory (při léčení) do karantény (doplňková akce při léčení souborů)
/no-quarantine	neukládat infikované soubory do karantény

Všeobecné možnosti

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

Návratové hodnoty

0	nenalezeny žádné hrozby
1	hrozba nalezena a vyléčena
10	některé soubory nemohly být zkontrolovány (mohou obsahovat hrozby)
50	nalezena hrozba
100	chyba



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

Řešení nejčastějších problémů

V této kapitole naleznete vybrané nejčastěji se vyskytující otázky a problémy, se kterými se můžete setkat. Klikněte na název kapitoly pro zobrazení řešení problému.

- [Jak aktualizovat ESET NOD32 Antivirus?](#)
- [ESET NOD32 Antivirus detekoval hrozbu](#)
- [Jak odstranit vir z počítače?](#)
- [Jak vytvořit novou úlohu v Plánovači?](#)
- [Jak naplánovat kontrolu \(týdně\)?](#)
- [Jak obnovit přístup do rozšířeného nastavení?](#)
- [Jak deaktivovat produkt prostřednictvím portálu ESET HOME?](#)

Pokud není váš problém uveden v seznamu výše, zkuste v nápovědě k produktu ESET NOD32 Antivirus vyhledat řešení podle klíčového slova nebo fráze, která popisuje váš problém.

Pokud nenaleznete řešení vašeho problému v nápovědě k produktu ESET NOD32 Antivirus, navštivte pravidelně aktualizovanou [Databázi znalostí](#). Níže naleznete odkazy na nejnavštěvovanější články v Databázi znalostí:

- [Jak prodloužit platnost licence](#)
- [Při aktivaci produktu ESET došlo k chybě. Co to znamená?](#)
- [Aktivace produktu ESET pro domácnosti pomocí licenčního klíče](#) (tento článek nemusí být dostupný ve všech jazycích)
- [Jak odinstalovat nebo přinstalovat program ESET?](#)
- [Instalace programu ESET skončila předčasně](#)
- [Co musím udělat po obnovení licence? \(Domácí uživatelé\)](#)
- [Co se stane, pokud změním e-mailovou adresu?](#)
- [Jak mohu přenést produkt ESET do nového počítače?](#)
- [Jak spustit Windows v Nouzovém režimu nebo Nouzovém režimu se sítí](#)
- [Vytvoření výjimky na bezpečnou stránku tak, aby ji neblokovala ochrana přístupu na web](#)
- [Povolit odečítačům obrazovky přístup k uživatelskému rozhraní produktu ESET](#)

Pokud je to nutné, můžete se obrátit přímo na naše pracovníky [technické podpory](#).

Jak aktualizovat ESET NOD32 Antivirus?

Aktualizaci produktu ESET NOD32 Antivirus můžete provádět ručně nebo automaticky. Pro zahájení aktualizace přejděte v [hlavním okně programu](#) na záložku **Aktualizace** a klikněte na možnost **Zkontrolovat aktualizace**.

Po nainstalování programu se standardně vytvoří naplánovaná úloha, která spouští automatickou aktualizaci každou hodinu. Pro změnu délky nastaveného intervalu klikněte na **Nástroje** > [Plánovač](#).

Jak odstranit vir z počítače?

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

1. V [hlavním okně programu](#) klikněte na záložku **Kontrola počítače**.
2. Klikněte na možnost **Provést kontrolu počítače** pro zahájení jeho kontroly.
3. Po dokončení kontroly si zobrazte její protokol. Zaměřte se především na počet zkontrolovaných, infikovaných a vyléčených souborů.
4. Pokud chcete zkontrolovat pouze vybranou část disku, klikněte na **Volitelná kontrola** a vyberte cíle, které chcete ověřit na přítomnost virů.

Pro podrobnější informace navštivte pravidelně aktualizovanou [ESET Databázi znalostí](#) (článek nemusí být dostupný ve všech jazycích).

Jak vytvořit novou úlohu v Plánovači?

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

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

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

V rozbalovacím menu **naplánovaná úloha** vyberte možnost **Aktualizace**. Zadejte **Název úlohy** a klikněte na tlačítko **Další**. Dále nastavte pravidelnost opakování úlohy. K dispozici jsou následující možnosti: **Jednou, Opakovaně, Denně, Týdně, Při události**. Pokud chcete minimalizovat dopad na systémové zdroje při běhu notebooku na baterii nebo počítače z UPS, zapněte možnost **Nespouštět úlohu, pokud je počítač napájen z baterie**. Po kliknutí na tlačítko **Další** zadejte čas **Provedení úlohy**. Dále je potřeba definovat akci, která se provede v případě, že ve stanoveném termínu nebude možné úlohu spustit. K dispozici jsou následující možnosti:

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

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

Následně se zobrazí dialogové okno. V něm vyberte profil, který se použije pro naplánovanou úlohu. Nastavte primární a sekundární profil. Sekundární profil se použije v případě, kdy nebude možné provést úlohu pomocí primárního profilu. Kliknutím na tlačítko **Dokončit** se vytvořená naplánovaná úloha přidá do seznamu naplánovaných úloh.

Jak naplánovat každý týden kontrolu počítače?

Pro naplánování standardní úlohy přejděte v [hlavním okně programu](#) na záložku **Nástroje > Plánovač**. Níže je popsán stručný návod, jak vytvořit úlohu, která bude kontrolovat lokální disky každých týden. Přečtěte si detailní postup v naší [Databázi znalostí](#).

Pro naplánování úlohy postupujte následovně:

1. Klikněte na tlačítko **Přidat** v hlavním okně Plánovače.
2. Zadejte název úlohy a z rozbalovací nabídky **Typ úlohy** vyberte možnost **Volitelná kontrola počítače**.
3. Vyberte možnost **Týdně**.
4. Vyberte datum a čas, kdy chcete úlohu spustit.
5. Vyberte akci, která se provede v případě neprovedení úlohy ve stanoveném čase (například **Jakmile je to možné**). Tím zajistíte spuštění úlohy, pokud byl počítač vypnutý.
6. Zkontrolujte všechna nastavení úlohy v seznamu a klikněte na **Dokončit**.
7. V rozbalovacím menu **Cíle kontroly** vyberte **Lokální disky**.
8. Kliknutím na tlačítko **Dokončit** potvrdíte její naplánování.

Jak obnovit přístup do rozšířeného nastavení?

Pokud chcete přejít do chráněného zobrazení Rozšířených nastavení, zobrazí se okno pro zadání hesla. Pokud heslo zapomenete nebo ztratíte, klikněte na **Obnovit heslo**. Následně zadejte e-mailovou adresu, kterou jste uvedli při nákupu/registraci licence. Na tuto adresu vám zašleme ověřovací kód. Daný kód zadejte do zobrazeného dialogového pole a nastavte si nové heslo. Ověřovací kód je platný 7 dní.

Obnovit heslo pomocí účtu ESET HOME – tuto možnost využijte v případě, kdy máte licenci, kterou jste aktivovali produkt ESET, přidanou v portálu ESET HOME. Zadejte e-mailovou adresu, kterou se k účtu [ESET HOME](#) přihlašujete.

V případě, že si nepamatujete e-mailovou adresu nebo máte potíže s obnovou hesla, klikněte na možnost **Kontaktovat Technickou podporu**. Následně budete přesměrováni na webový formulář pro kontaktování technické podpory.

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

Více informací naleznete v článku ESET databáze znalostí [Obnovení hesla chránícího přístup do nastavení v domácích produktech pro Windows](#) (článek nemusí být dostupný ve všech jazycích).

Jak deaktivovat produkt prostřednictvím portálu ESET HOME?

Produkt není aktivován

Tato chybová zpráva se zobrazí v případě, že vlastník licence deaktivoval váš ESET NOD32 Antivirus prostřednictvím portálu ESET HOME, případně již nesdílí licenci s vaším účtem ESET HOME. Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET NOD32 Antivirus.
- Kontaktujte případně vlastníka licence s informací, že je váš ESET NOD32 Antivirus deaktivovaný nebo že s vámi již licenci nesdílí. Vlastník licence může problém vyřešit prostřednictvím [portálu ESET HOME](#).

Produkt je deaktivovaný, zařízení je odpojené

Tato chybová zpráva se zobrazí v případě, že bylo [zařízení odebráno ze správcovského portálu ESET HOME](#). Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET NOD32 Antivirus.
- Kontaktujte případně vlastníka licence s informací, že je váš ESET NOD32 Antivirus deaktivovaný a zařízení odpojené od ESET HOME.
- Pokud jste vlastníky licence, ale nejste si změn vědomi, zkontrolujte si [v portálu ESET HOME Informační](#)

[kanál o aktivitách](#). Pokud jste zaznamenali podezřelou aktivitu, [změňte si heslo pro přístup do účtu ESET HOME](#) a [kontaktujte Technickou podporu ESET](#).

Produkt je deaktivovaný, zařízení je odpojené

Tato chybová zpráva se zobrazí v případě, že bylo [zařízení odebráno ze správcovského portálu ESET HOME](#). Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET NOD32 Antivirus.
- Kontaktujte případně vlastníka licence s informací, že je váš ESET NOD32 Antivirus deaktivovaný a zařízení odpojené od ESET HOME.
- Pokud jste vlastníky licence, ale nejste si změn vědomi, zkontrolujte si [v portálu ESET HOME Informační kanál o aktivitách](#). Pokud jste zaznamenali podezřelou aktivitu, [změňte si heslo pro přístup do účtu ESET HOME](#) a [kontaktujte Technickou podporu ESET](#).

Produkt není aktivován

Tato chybová zpráva se zobrazí v případě, že vlastník licence deaktivoval váš ESET NOD32 Antivirus prostřednictvím portálu ESET HOME, případně již nesdílí licenci s vaším účtem ESET HOME. Pro vyřešení problému:

- Klikněte na **Aktivovat** a využijte jeden ze [způsobů aktivace](#) ESET NOD32 Antivirus.
- Kontaktujte případně vlastníka licence s informací, že je váš ESET NOD32 Antivirus deaktivovaný nebo že s vámi již licenci nesdílí. Vlastník licence může problém vyřešit prostřednictvím [portálu ESET HOME](#).

Program zvyšování spokojenosti zákazníků

Zapojením se do programu zvyšování spokojenosti zákazníků poskytnete společnosti ESET anonymní informace související s používáním našich produktů. Bližší informace o zpracování dat máme popsány v zásadách ochrany osobních údajů.

Váš souhlas

Účast v programu je dobrovolná a vychází z vašeho souhlasu. Po zapojení se do programu je účast pasivní a nevyžaduje z vaší strany žádné další akce. Své rozhodnutí můžete kdykoli změnit a účast v programu zrušit v nastavení produktu. Tím nám zabráníte v dalším zpracování anonymních dat.

Své rozhodnutí můžete kdykoli změnit a účast v programu zrušit v nastavení produktu.

- [Změna nastavení Programu zvyšování spokojenosti zákazníků v produktech pro domácnosti na platformě Windows](#)

Jaké informace sbíráme?

Data o interakci s produktem

Tyto informace nám pomohou zjistit, jak naše produkty používáte. Díky tomu například víme, jaké funkce používáte nejčastěji, jaké uživatelské nastavení měníte, a kolik času v produktu trávíte.

Data o zařízení

Tyto informace sbíráme za účelem, abychom zjistili, kde a na jakých zařízeních naše produkty používáte. Typicky se jedná o model zařízení, zemi, verzi a název operačního systému.

Diagnostická data o chybách

Sbíráme rovněž informace o chybách a pádech produktu. Příklad: jaká chyba se vyskytla a co jí předcházelo.

Proč tyto informace sbíráme?

Tyto anonymní informace nám pomohou vylepšit naše produkty – pro vás, naše uživatele. To nám pomůže vyvíjet relevantní, snadno ovladatelné a co nejméně problémové produkty, jak jen to bude v našich silách.

Kdo tyto informace spravuje?

Společnost ESET, spol. s r. o. je výhradním správcem dat získaných v rámci tohoto Programu. Tyto informace nejsou sdíleny s třetími stranami.

Licenční ujednání s koncovým uživatelem

Platné od 19. října 2021.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtete níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBU POUŽITÍM SOFTWARE VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ [ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ](#).**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 („ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou („Vy“ anebo „Koncový uživatel“) Vás opravňuje k používání Software definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Software vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned

klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. Software. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. Instalace, počítač a licenční klíč. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsán v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. Licence. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání.** Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí.** Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícero uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělována. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělovány pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícero počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence.** Vaše právo používat Software je časově omezené.

e) **OEM Software.** Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence.** Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejci či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. Funkce sběru dat a požadavky na připojení k internetu. Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro následující funkce Softwaru:

a) **Aktualizace Software.** Poskytovatel je oprávněn vydávat aktualizace nebo upgrade Softwaru („Aktualizace“), avšak není povinen Aktualizace poskytovat. Tato funkce je při standardním nastavení Softwaru zapnutá, proto se Aktualizace nainstalují automaticky, kromě případů, kdy Koncový uživatel automatickou instalaci Aktualizací zakázal. Pro poskytování aktualizací je vyžadováno ověření pravosti Licence včetně informací o počítači anebo platformě, na které je Software nainstalován, v souladu se Zásadami ochrany osobních údajů.

Poskytování jakýchkoli aktualizací může podléhat „Zásadám konce životnosti“, které jsou k dispozici na webu https://go.eset.com/eol_home. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

b) **Zasílání infiltrací a informací Poskytovateli.** Software obsahuje funkce, které slouží ke shromažďování vzorků počítačových virů a jiných škodlivých počítačových programů a podezřelých, problematických nebo potenciálně nežádoucích nebo nebezpečných objektů, jako jsou soubory, adresy URL, IP pakety a ethernetové rámce (dále jen "Infiltrace") a jejich následnému odeslání Poskytovateli, mimo jiné včetně informací o procesu instalace, počítači a/nebo platformě, kde je Software nainstalován, a informací o operacích a funkcích Softwaru ("Informace"). Informace a Infiltrace mohou zahrnovat údaje (včetně náhodně nebo nezáměrně získaných osobních údajů) o Koncovém uživateli a/nebo jiných uživatelích počítače, na kterém je Software nainstalován, a soubory postižené Infiltracemi, včetně přidružených metadat.

Informace a Infiltrace mohou být shromažďovány následujícími funkcemi Softwaru:

i. Funkce Reputační systém LiveGrid zahrnuje shromažďování a odesílání jednosměrných hodnot hash, které souvisejí s Infiltracemi, Poskytovateli. Tato funkce je povolena v rámci standardního nastavení Softwaru.

ii. Funkce Systém zpětné vazby LiveGrid zahrnuje shromažďování a odesílání Infiltrací s příslušnými metadaty a Informacemi Poskytovateli. Tuto funkci aktivuje Koncový uživatel během procesu instalace Softwaru.

Poskytovatel bude obdržené Informace a Infiltrace používat pouze pro účely analýzy a zkoumání Infiltrací, zlepšování ověřování pravosti Softwaru a Licence a přijme veškerá vhodná opatření, aby zajistil, že obdržené Infiltrace a Informace zůstanou v bezpečí. Po aktivaci této funkce Softwaru mohou být Infiltrace a Informace shromažďovány a zpracovávány Poskytovatelem, jak je uvedeno v Zásadách ochrany osobních údajů a v příslušných právních předpisech. Tyto funkce můžete kdykoliv deaktivovat.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. Výkon práv Koncového uživatele. Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. Omezení práv. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinni dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompileovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelům, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v

rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. Autorská práva. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/nebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/nebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedena na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompileovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčena práva Poskytovatele spojená s porušením této Dohody.

8. Výhrada práv. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělena v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. Víceré jazykové verze, verze pro více operačních systémů, vícené kopie. V případě jestliže Software podporuje vícené platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. Začátek a trvání Dohody. Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechny související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. PROHLÁŠENÍ KONCOVÉHO UŽIVATELE. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. Žádné další závazky. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. OMEZENÍ ODPOVĚDNOSTI. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚŠTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY

VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBU SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBU NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBU JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLE INSTALACÍ, POUŽÍVÁNÍM ANEBU NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBU JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBU POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora.** Technickou podporu poskytuje ESET nebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/nebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/nebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence.** Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zasláného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA.** Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsány v této Dohodě.

19. **Soulad se zákony o kontrole obchodu.**

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží,

softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhá zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. Oznámení. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. Rozhodující právo. Tato Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. Všeobecná ustanovení. V případě, že jakýkoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků,

Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

DODATEK K DOHODĚ

Posouzení zabezpečení zařízení připojených k síti. Na posouzení zabezpečení zařízení připojených k síti se vztahují následující dodatečná ustanovení:

Software je vybaven funkcí určenou pro ověření zabezpečení lokální sítě Koncového uživatele a zařízení v lokální síti, k čemuž potřebuje získat název sítě a informace o zařízeních připojených do lokální sítě jako je jejich přítomnost, typ, název, IP adresa a MAC adresa zařízení v lokální síti společně s informací o licenci. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Tato funkce může dále nabízet informace týkající se dostupnosti bezpečnostního software určeného pro zabezpečení zařízení v lokální síti.

Ochrana proti zneužití dat Na ochranu proti zneužití dat se vztahují následující dodatečná ustanovení:

Software obsahuje funkci, která zabráňuje ztrátě nebo zneužití důležitých dat v přímé souvislosti s odcizením počítače. Tato funkce je ve výchozím nastavení Softwaru vypnutá. Aby bylo možné tuto funkci aktivovat, je nutné si vytvořit účet ESET HOME, přes který funkce aktivuje sběr dat v případě odcizení počítače. Pokud tuto funkci Softwaru aktivujete, budou data o odcizeném počítači shromažďována a odesílány Poskytovateli (může se jednat o údaje o umístění počítače v síti, údaje o obsahu zobrazovaném na obrazovce počítače, údaje o konfiguraci počítače nebo o data zaznamenaná kamerou připojenou k počítači (dále jen "Data"). Koncový uživatel je oprávněn používat Data získaná touto funkcí a poskytnutá prostřednictvím účtu ESET HOME výhradně k nápravě nepříznivé situace způsobené odcizením počítače. Výhradně pro účely této funkce Poskytovatel zpracuje Data v souladu se Zásadami ochrany osobních údajů a příslušnými právními předpisy. Poskytovatel umožní Koncovému uživateli přístup k Datům po dobu nezbytně nutnou k dosažení účelu, pro který byla data získána. Tato doba nesmí překročit dobu uchovávání stanovenou v Zásadách ochrany osobních údajů. Ochrana proti zneužití dat se bude používat výlučně u počítačů a účtů, ke kterým má Koncový uživatel oprávněný přístup. Jakékoli nezákonné používání bude oznámeno příslušným orgánům. Poskytovatel bude v případě zneužití postupovat v souladu s příslušnými zákony a pomáhat orgánům činným v trestním řízení. Souhlasíte a potvrzujete, že je Vaší zodpovědností zabezpečit heslo pro přístup k účtu ESET HOME, a souhlasíte s tím, že nesmíte předat své heslo žádné třetí straně. Koncový uživatel je odpovědný za jakoukoli aktivitu, při které se používá funkce ochrany proti zneužití dat a účet ESET HOME, bez ohledu na to, zda k provádění takovýchto aktivit měl nebo neměl povolení. Pokud zjistíte, že je zabezpečení účtu ESET HOME ohroženo, neprodleně tuto skutečnost Poskytovateli oznamte. Dodatečná ustanovení na ochranu proti zneužití dat se vztahují výhradně na koncové uživatele produktů ESET Internet Security a ESET Smart Security Premium.

ESET Secure Data. Na produkt ESET Secure Data se vztahují následující dodatečná ustanovení:

1. Definice. V těchto dodatečných ustanoveních k produktu ESET Secure Data mají následující slova odpovídající významy:

a) "Informace", jakékoli informace nebo data šifrovaná nebo dešifrovaná pomocí softwaru.

b) „Produkty“, software ESET Secure Data a související dokumentace;

c) "ESET Secure Data" Software používaný k šifrování a dešifrování elektronických dat;

Všechny odkazy na množné číslo zahrnují i jednotné číslo a všechny odkazy na mužský rod zahrnují ženský a střední rod a naopak. Slova bez konkrétní definice se používají v souladu s definicemi stanovenými v této Smlouvě.

2. Další deklarace pro Koncové uživatele. Berete na vědomí a souhlasíte s tím, že:

a) Je vaší zodpovědností chránit, udržovat a zálohovat Informace.

b) Před instalací softwaru ESET Secure Data byste měli na počítači provést úplnou zálohu všech Informací a dat (mimo jiné včetně důležitých informací a dat).

c) Je nutné udržovat v bezpečí záznamy o všech heslech nebo jiných informacích používaných pro nastavení a používání softwaru ESET Secure Data a musíte si také vytvořit záložní kopie všech šifrovacích klíčů, licenčních kódů, souborů s klíči a dalších generovaných dat na samostatná úložná média.

d) Jste zodpovědní za používání Produktů. Poskytovatel nenese odpovědnost za případné ztráty, nároky nebo škody vzniklé v důsledku neoprávněného nebo chybného šifrování nebo dešifrování Informací nebo jiných dat bez ohledu na to, kde a jak jsou tyto Informace nebo jiná data uloženy.

e) Poskytovatel sice přijal veškerá přiměřená opatření k zajištění integrity a zabezpečení softwaru ESET Secure Data, Produkty (nebo kterýkoli z nich) však nesmí být použity v žádné oblasti, která je závislá na zajištění bezpečnosti při poruše nebo je potenciálně nebezpečná, mimo jiné včetně jaderných zařízení, letecké navigace, řídicích nebo komunikačních systémů, zbraňových a obranných systémů, podpůrných zařízení a systémů monitorování životních funkcí.

f) Je povinností Koncového uživatele zajistit, aby úroveň zabezpečení a šifrování zajišťovaná produkty byla adekvátní vašim požadavkům.

g) Jste zodpovědní za používání Produktů (nebo kteréhokoli z nich), mimo jiné včetně zajištění toho, aby bylo jejich používání v souladu se všemi platnými zákony a předpisy Slovenské republiky nebo jakékoli jiné země, oblasti nebo státu, kde se Produkty používají. Před každým použitím Produktů musíte zajistit, aby nebylo v rozporu s embargem žádné vlády (Slovenské republiky nebo jiné země/oblasti).

h) Software ESET Secure Data může čas od času kontaktovat servery Poskytovatele s cílem zkontrolovat informace o licenci a dostupnost oprav, aktualizací Service Pack a dalších aktualizací, které mohou být určeny k vylepšování, údržbě, pozměnění nebo rozšíření softwaru ESET Secure Data a v souladu se Zásadami ochrany osobních údajů může odesílat obecné informace o systému související s funkcí Softwaru.

i) Poskytovatel nenese odpovědnost za jakékoli ztráty, škody, výdaje nebo nároky vyplývající ze ztráty, odcizení, zneužití, poškození nebo zničení hesel, instalačních informací, šifrovacích klíčů, licenčních aktivačních kódů a dalších dat generovaných nebo uložených během používání softwaru.

Dodatečná ustanovení k produktu ESET Secure Data se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

Software Password Manager. Na software Password Manager se vztahují následující dodatečná ustanovení:

1. Další deklarace pro Koncové uživatele. Berete na vědomí a souhlasíte s tím, že nesmíte:

a) Používat software Password Manager k provozování jakékoli aplikace důležité pro chod firmy, kde by mohlo

dojít k ohrožení lidských životů nebo k újmě na majetku. Berete na vědomí, že software Password Manager není k takovým účelům určen a že jeho selhání v takových případech by mohlo vést ke smrti, újmám na zdraví či vážným škodám na majetku nebo prostředí, za které Poskytovatel neodpovídá.

SOFTWARE PASSWORD MANAGER NENÍ NAVRŽEN, URČEN ANI LICENCOVÁN K POUŽITÍ V RIZIKOVÝCH PROSTŘEDÍCH VYŽADUJÍCÍCH ZAJIŠTĚNÍ BEZPEČNOSTI PŘI PORUŠE, MIMO JINÉ VČETNĚ NÁVRHU, VÝSTAVBY, ÚDRŽBY NEBO PROVOZU JADERNÝCH ZAŘÍZENÍ, LETECKÝCH NAVIGAČNÍCH NEBO KOMUNIKAČNÍCH SYSTÉMŮ, ŘÍZENÍ LETOVÉHO PROVOZU A SYSTÉMŮ PODPORY ŽIVOTNÍCH FUNKCÍ NEBO ZBRAŇOVÝCH SYSTÉMŮ. POSKYTOVATEL VÝSLOVNĚ ODMÍTÁ JAKÉKOLI VÝSLOVNĚ UVEDENÉ ČI PŘEDPOKLÁDANÉ ZÁRUKY VHODNOSTI PRO TYTO ÚČELY.

b) Používat software Password Manager způsobem, který porušuje podmínky této smlouvy či zákony Slovenské republiky nebo vaší jurisdikce. Konkrétně nesmíte software Password Manager používat k provádění nebo propagování jakékoli nezákonné činnosti, včetně nahrávání dat škodlivého obsahu či obsahu, který by se mohl používat pro jakoukoli nezákonnou činnost, který by mohl jakýmkoli způsobem porušovat zákony nebo práva jakékoli třetí strany (včetně jakýchkoli práv duševního vlastnictví), mimo jiné včetně jakýchkoli pokusů o získání přístupu k účtům v Úložišti (pro účely těchto dodatečných podmínek k softwaru Password Manager termín Úložiště označuje prostor pro ukládání dat spravovaných Poskytovatelem nebo třetí stranou, která není Poskytovatelem, a uživatelem pro účely umožnění synchronizace a zálohování uživatelských dat) nebo k jakýmkoli účtům a datům jiných uživatelů softwaru Password Manager nebo uživatelů Úložiště. Pokud porušíte kterékoli z těchto ustanovení, je Poskytovatel oprávněn okamžitě ukončit platnost této smlouvy a požadovat od vás náhradu ve výši nákladů na nezbytnou nápravu, jakož i učinit všechny nezbytné kroky k tomu, aby vám zabránil v dalším používání softwaru Password Manager bez možnosti náhrady.

2. OMEZENÍ ODPOVĚDNOSTI. SOFTWARE PASSWORD MANAGER JE POSKYTOVÁN "TAK JAK JE", BEZ ZÁRUKY JAKÉHOKOLIV DRUHU, AŽ UŽ VÝSLOVNĚ VYJÁDŘENÉ NEBO PŘEDPOKLÁDANÉ. SOFTWARE POUŽÍVÁTE NA VLASTNÍ NEBEZPEČÍ. VÝROBCE NEODPOVÍDÁ ZA ZTRÁTU DAT, ŠKODY, OMEZENÍ DOSTUPNOSTI SLUŽEB, VČETNĚ JAKÝCHKOLI DAT ODESLANÝCH SOFTWAREM PASSWORD MANAGER DO EXTERNÍHO ULOŽIŠTĚ PRO ÚČELY SYNCHRONIZACE A ZÁLOHOVÁNÍ DAT. ŠIFROVÁNÍ DAT POMOCÍ SOFTWAREM PASSWORD MANAGER NEZAKLÁDÁ ŽÁDNOU ODPOVĚDNOST POSKYTOVATELE S OHLEDEM NA ZABEZPEČENÍ TĚCHTO DAT. VÝSLOVNĚ SOUHLASÍTE S TÍM, ŽE DATA ZÍSKANÁ, POUŽÍVANÁ, ŠIFROVANÁ, UKLÁDANÁ, SYNCHRONIZOVANÁ NEBO ODESÍLANÁ POMOCÍ SOFTWAREM PASSWORD MANAGER JE TAKÉ MOŽNÉ UKLÁDAT NA SERVERY TŘETÍCH STRAN (VZTAHUJE SE POUZE NA TAKOVÉ POUŽÍVÁNÍ SOFTWAREM PASSWORD MANAGER, KDE BYLY POVOLENY SLUŽBY SYNCHRONIZACE A ZÁLOHOVÁNÍ). POKUD SE POSKYTOVATEL DLE SVÉHO VLASTNÍHO UVÁŽENÍ ROZHODNE POUŽÍVAT TAKOVÉ ULOŽIŠTĚ, WEB, WEBOVÝ PORTÁL, SERVER NEBO SLUŽBU TŘETÍ STRANY, NENESE POSKYTOVATEL ODPOVĚDNOST ZA KVALITU, BEZPEČNOST ČI DOSTUPNOST TAKOVÉ SLUŽBY TŘETÍ STRANY, PŘIČEMŽ POSKYTOVATEL VŮČI VÁM NEMÁ ŽÁDNOU ODPOVĚDNOST ZA PORUŠENÍ SMLUVNÍCH NEBO ZÁKONNÝCH POVINNOSTÍ TŘETÍ STRANOU ANI ZA ŠKODY, UŠLÝ ZISK, FINANČNÍ NEBO NEFINANČNÍ ŠKODY NEBO JAKÝKOLI JINÝ DRUH ZTRÁTY PŘI POUŽÍVÁNÍ TOHOTO SOFTWAREM. POSKYTOVATEL NENÍ ZODPOVĚDNÝ ZA OBSAH ŽÁDNÝCH DAT ZÍSKANÝCH, POUŽÍVANÝCH, ŠIFROVANÝCH, UKLÁDANÝCH, SYNCHRONIZOVANÝCH NEBO ODESÍLANÝCH POMOCÍ SOFTWAREM PASSWORD MANAGER NEBO V ULOŽIŠTI. BERETE NA VĚDOMÍ, ŽE POSKYTOVATEL NEMÁ PŘÍSTUP K OBSAHU ULOŽENÝCH DAT A NENÍ SCHOPEN MONITOROVAT NEBO ODSTRAŇOVAT PRÁVNĚ ZÁVADNÝ OBSAH.

Poskytovatel vlastní všechna práva na vylepšení, upgrady a opravy související se softwarem Password Manager ("Vylepšení"), a to i v případě, že kterákoli z těchto vylepšení byla vytvořena na základě názorů, nápadů nebo návrhů předložených vámi, a to v jakékoliv formě. Nebudete mít nárok na žádnou náhradu škody, mimo jiné včetně jakýchkoli licenčních poplatků souvisejících s takovými Vylepšeními.

SUBJEKTY POSKYTOVATELE A VLASTNÍCI LICENCÍ NEBUDOU MÍT VŮČI VÁM ŽÁDNOU ZODPOVĚDNOST ZA POHLEDÁVKY A ZÁVAZKY JAKÉHOKOLIV DRUHU VZNIKLE Z NEBO SE JAKÝMKOLI ZPŮSOBEM TÝKAJÍCÍ POUŽÍVÁNÍ SOFTWAREM PASSWORD MANAGER VÁMI NEBO TŘETÍMI STRANAMI, POUŽITÍ NEBO NEPOUŽITÍ JAKÉKOLI ZPROSTŘEDKOVATELSKÉ SPOLEČNOSTI ČI PRODEJCE NEBO PRODEJE ČI NÁKUPU JAKÝCHKOLI CENNÝCH PAPÍRŮ

BEZ OHLEDU NA TO, ZDA TAKOVÉ POHLEDÁVKY A ZÁVAZKY VYCHÁZEJÍ Z NĚJAKÉ ZÁKONNÉ NEBO SPRÁVEDLIVÉ TEORIE.

SUBJEKTY POSKYTOVATELY A VLASTNÍCI LICENCÍ NEBUDOU MÍT VŮČI VÁM ŽÁDNOU ZODPOVĚDNOST ZA ŽÁDNÉ PŘÍMÉ, NAHODILÉ, ZVLÁŠTNÍ, NEPŘÍMÉ NEBO NÁSLEDNÉ ŠKODY VYPLÝVAJÍCÍ Z NEBO VE SPOJENÍ S JAKÝMKOLI SOFTWAREM TŘETÍCH STRAN, JAKÝMKOLI DATY VYUŽÍVANÝMI PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, VAŠE POUŽÍVÁNÍ NEBO NESCHOPNOST POUŽÍVAT SOFTWARE PASSWORD MANAGER (NEBO K NĚMU ZÍSKAT PŘÍSTUP) NEBO JAKÝMKOLI DATY POSKYTOVANÝMI PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, AŽ JIŽ JSOU TAKOVÁ ODŠKODNĚNÍ NÁROKOVÁNA NA ZÁKLADĚ JAKÉKOLI ZÁKONNÉ NEBO SPRÁVEDLIVÉ TEORIE. ŠKODY VYLOUČENÉ TOUTO KLAUZULÍ ZAHRNÚJÍ MIMO JINÉ ŠKODY ZPŮSOBENÉ ZTRÁTOU ZISKU, ÚJMOU NA ZDRAVÍ NEBO NA MAJETKU, PŘERUŠENÍ PODNIKATELSKÉ ČINNOSTI NEBO ZTRÁTOU OBCHODNÍCH ČI OSOBNÍCH ÚDAJŮ. NĚKTERÉ JURISDIKCE NEUMOŽŇUJÍ OMEZENÍ NAHODILÝCH NEBO NÁSLEDNÝCH ŠKOD. V TAKOVÝCH PŘÍPADECH SE NA VÁS TOTO OMEZENÍ NEMUSÍ VZTAHOVAT. V TAKOVÉM PŘÍPADĚ BUDE ZODPOVĚDNOST POSKYTOVATELE V MINIMÁLNÍM ROZSAHU POVOLENÉM PLATNÝMI ZÁKONY.

INFORMACE POSKYTNUTÉ PROSTŘEDNICTVÍM SOFTWARE PASSWORD MANAGER, VČETNĚ CEN AKCIÍ, ANALÝZ, INFORMACÍ O TRHU, ZPRÁV A FINANČNÍCH DAT, MOHOU BÝT ZPOŽDĚNY, NEPŘESNÉ NEBO MOHOU OBSAHOVAT CHYBY NEBO OPOMENUTÍ A SUBJEKTY POSKYTOVATELE A VLASTNÍCI LICENCÍ NENESOU V SOUVISLOSTI S NIMI ŽÁDNOU ODPOVĚDNOST. POSKYTOVATEL MŮŽE ZMĚNIT NEBO PŘESTAT NABÍZET VEŠKERÉ ASPEKTY NEBO FUNKCE SOFTWARE PASSWORD MANAGER NEBO POUŽÍVÁNÍ VŠECH NEBO NĚKTERÝCH FUNKCÍ NEBO TECHNOLOGIÍ V SOFTWARE PASSWORD MANAGER, A TO KDYKOLI BEZ PŘEDCHOZÍHO OZNÁMENÍ.

POKUD JSOU USTANOVENÍ V TOMTO ČLÁNKU Z JAKÉHOKOLIV DŮVODU NEPLATNÁ NEBO POKUD JE POSKYTOVATEL POVAŽOVÁN ZA ODPOVĚDNÉHO ZA ŠKODY ATD. PODLE PLATNÝCH ZÁKONŮ, STRANY SE DOHODLY, ŽE ODPOVĚDNOST POSKYTOVATELE VŮČI VÁM BUDE OMEZENÁ NA CELKOVOU ČÁSTKU LICENČNÍCH POPLATKŮ, KTERÉ JSTE ZAPLATILI.

SOUHLASÍTE S TÍM, ŽE ODŠKODNÍTE A BUDETE CHRÁNIT A BRÁNIT POSKYTOVATELE A JEHO ZAMĚSTNANCE, DCEŘINÉ SPOLEČNOSTI, AFILACE, PARTNERY Z OBLASTI REBRANDINGU A DALŠÍ PARTNERY PŘED JAKÝMKOLI A VŠEMI POHLEDÁVKAMI, ZÁVAZKY, ŠKODAMI, ZTRÁTAMI, NÁKLADY, VÝDAJI A POPLATKY TŘETÍCH STRAN (MIMO JINÉ VČETNĚ VLASTNÍKŮ ZAŘÍZENÍ NEBO STRAN, JEJICHŽ PRÁVA BYLA OVLIVNĚNA DATY POUŽITÝMI V SOFTWARE PASSWORD MANAGER NEBO V ÚLOŽIŠTI).

3. Data v softwaru Password Manager. Pokud výslovně nezvolíte jiné nastavení, budou všechna data zadaná vámi, která budou uložena v databázi softwaru Password Manager, uložena v zašifrované podobě na počítači nebo jiném paměťovém zařízení, které definujete. Berete na vědomí, že v případě odstranění nebo poškození jakýchkoli databázových nebo jiných souborů softwaru Password Manager budou všechna data v nich obsažená nenávratně ztracena, přičemž chápete a akceptujete riziko takové ztráty. Skutečnost, že se vaše osobní data ukládají na počítači v zašifrované podobě, neznamená, že tyto informace nemohou být odcizeny nebo zneužity někým, kdo objeví hlavní heslo nebo získá přístup k aktivačnímu zařízení definovanému zákazníkem pro otevření databáze. Jste zodpovědní za udržování bezpečnosti všech způsobů přístupu.

4. Odesílání osobních údajů Poskytovateli nebo do Úložiště. Pokud se tak rozhodnete (a výhradně za účelem zajištění včasné synchronizace a zálohování dat), bude software Password Manager přenášet nebo odesílat osobní údaje z databáze softwaru Password Manager (konkrétně hesla, přihlašovací údaje, informace o účtech a identitách) přes internet do Úložiště. Data jsou přenášena výhradně v šifrované podobě. Použití softwaru Password Manager pro vyplňování hesel, přihlašovacích údajů či jiných údajů do online formulářů může vyžadovat, aby byly informace odesílány přes internet na weby, které určíte. Tento přenos dat není iniciován softwarem Password Manager, Poskytovatel proto nemůže být zodpovědný za bezpečnost takových interakcí s jakýmkoli weby podporovanými různými poskytovateli. Veškeré transakce probíhající přes internet (bez ohledu na to, zda ve spojení se softwarem Password Manager) jsou na vašem vlastním uvážení a na vaše vlastní riziko a budete mít výhradní odpovědnost za jakékoli poškození vašeho počítačového systému nebo ztrátu dat vyplývající ze stažení a/nebo používání takovýchto materiálů nebo služeb. Aby se minimalizovalo riziko ztráty cenných dat,

doporučuje Poskytovatel, aby Koncoví uživatelé prováděli pravidelné zálohy databáze a dalších citlivých souborů na externí disky. Poskytovatel vám není schopen nijak pomoci s obnovením ztracených nebo poškozených dat. Pokud Poskytovatel poskytuje služby zálohování k uživatelským databázovým souborům pro případ poškození nebo odstranění souborů na počítačích uživatelů, je taková služba zálohování poskytována bez jakékoli záruky a neimplikuje žádnou odpovědnost Poskytovatele vůči vám.

Používáním softwaru Password Manager souhlasíte s tím, že software může čas od času kontaktovat servery Poskytovatele s cílem zkontrolovat informace o licenci a dostupnost oprav, aktualizací Service Pack a dalších aktualizací, které mohou být určené k vylepšování, údržbě, pozměnění nebo rozšíření softwaru Password Manager. Software může odesílat obecné systémové informace týkající se fungování softwaru Password Manager v souladu se Zásadami ochrany osobních údajů.

5. Informace a pokyny k odinstalaci. Veškeré informace z databáze, které byste chtěli zachovat, si musíte před odinstalací softwaru Password Manager vyexportovat.

Dodatečná ustanovení k softwaru Password Manager se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

ESET LiveGuard. Na produkt ESET LiveGuard se vztahují následující dodatečná ustanovení:

Software obsahuje funkci další analýzy souborů odeslaných Koncovým uživatelem. Poskytovatel bude soubory odeslané Koncovým uživatelem a výsledky analýzy používat pouze v souladu se Zásadami ochrany osobních údajů a v souladu s příslušnými právními předpisy.

Dodatečná ustanovení k produktu ESET LiveGuard se vztahují výhradně na koncové uživatele produktu ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Zásady ochrany osobních údajů

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvlášť důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Právní základ pro zpracování osobních údajů

Při zpracování dat používáme v souladu s příslušným legislativním rámcem v souvislosti s ochranou osobních údajů jen několik právních základů. Zpracování osobních údajů ve společnosti ESET je potřebné zejména za účelem plnění dokumentu [Licenční ujednání s koncovým uživatelem](#) („EULA“) odsouhlaseného s koncovým uživatelem (dle článku 6 (1) (b) nařízení GDPR), který je platný pro poskytování produktů nebo služeb společnosti ESET, pokud není výslovně uvedeno jinak, například:

- Oprávněný zájem: Právní základ (dle článku 6 (1) (f) nařízení GDPR), který nám umožňuje zpracovávat údaje o tom, jak naši zákazníci využívají naše služby a jak jsou s nimi spokojeni, abychom jim mohli poskytnout nejlepší možnou ochranu, podporu a služby. Podle platných právních předpisů je za oprávněný zájem považován i marketing, proto se při marketingové komunikaci s našimi zákazníky obvykle spoléháme na tento koncept.
- Souhlas (dle článku 6 (1) (a) nařízení GDPR): Můžeme jej od vás vyžadovat v konkrétních situacích, kdy považujeme tento právní základ za nejvhodnější, nebo pokud to vyžaduje zákon.
- Splnění zákonné povinnosti (dle článku 6 (1) (c) nařízení GDPR): Například specifikace požadavků na elektronickou komunikaci nebo uchovávání dokumentů souvisejících s fakturací.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodeje, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Zabezpečení dat

Společnost ESET implementuje příslušná technická a organizační opatření k zajištění úrovně bezpečnosti, která odpovídá potenciálním rizikům. Děláme vše, co je v našich silách, abychom zajistili nepřetržitou důvěrnost, integritu, dostupnost a odolnost zpracovatelských systémů a služeb. Pokud však dojde k narušení ochrany údajů, které ohrožuje vaše práva a svobody, jsme připraveni informovat příslušné dozorčí orgány i ohrožené koncové uživatele jakožto subjekty údajů.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a –

pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úřad na ochranu osobních údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem produktu jsou poskytovány za podmínek uvedených v dokumentu [Licenční ujednání s koncovým uživatelem](#), ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o sběru dat spojených s poskytováním našich služeb. Poskytujeme různé služby popsané v Licenčním ujednání s koncovým uživatelem („EULA“) a v produktové [dokumentaci](#). Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

Licenční a fakturační údaje. Jméno, e-mailová adresa, licenční klíč a (v některých případech) adresa, sídlo společnosti a platební údaje jsou společností ESET shromažďovány a zpracovávány za účely aktivace licence, doručení licenčního klíče, připomenutí konce platnosti, požadavků na podporu, ověření pravosti licence, poskytování našich služeb a dalších oznámení, včetně marketingových zpráv v souladu s příslušnými zákony nebo vašim souhlasem. Společnost ESET má zákonnou povinnost uchovávat fakturační údaje po dobu 10 let, ovšem informace o licencích jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

Aktualizace a další statistiky. Mezi zpracovávané informace patří informace o procesu instalace a vašem počítači, včetně platformy, na které je náš produkt nainstalován, a údaje o činnostech a funkčnosti našich produktů, jako je operační systém, údaje o hardwaru, ID instalace, ID licencí, IP adresa, adresa MAC a nastavení konfigurace produktu. Tyto informace jsou zpracovávány za účelem poskytování služeb aktualizace a upgradu a za účelem údržby, zabezpečení a vylepšování naší backendové infrastruktury.

Tyto informace jsou uchovávány odděleně od identifikačních údajů potřebných pro účely licencování a fakturace, protože nevyžadují identifikaci koncového uživatele. Doba uchovávání je maximálně 4 roky.

Reputační systém **ESET LiveGrid®**. Jednosměrné hodnoty hash, které souvisejí s infiltracemi, jsou zpracovávány pro účely reputačního systému ESET LiveGrid®, který zlepšuje účinnost našich řešení proti malwaru tím, že porovnává kontrolované soubory s databází povolených a zakázaných položek v cloudu. Koncový uživatel během tohoto procesu není identifikován.

Systém zpětné vazby **ESET LiveGrid®**. Podezřelé vzorky a metadata jako součást systému zpětné vazby ESET LiveGrid®, který umožňuje společnosti ESET okamžitě reagovat na potřeby našich koncových uživatelů a udržet akceschopnost tváří v tvář nejnovějším hrozbám. Jsme závislí na tom, že nám zasíláte:

- Infiltrace, jako jsou potenciální vzorky virů a jiných škodlivých programů, a podezřelé; problematické, potenciálně nežádoucí nebo nebezpečné objekty, jako jsou spustitelné soubory nebo e-mailové zprávy, které jsou nahlášeny koncovým uživatelem jako nevyžádané nebo označené naším produktem; údaje o zařízeních v místní síti, jako je typ, dodavatel, model a/nebo název zařízení;
- Údaje týkající se používání internetu, jako jsou IP adresa a informace o zeměpisné poloze, IP pakety, adresy URL a ethernetové rámce;
- Soubory výpisu chyb a v nich obsažené informace.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. Kontaktní informace a údaje obsažené ve vašich požadavcích na podporu mohou být vyžadovány za účelem poskytování podpory. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory.

Veškeré informace získané a zpracovávané prostřednictvím systému zpětné vazby ESET LiveGrid® jsou určeny k použití bez identifikace koncového uživatele.

Posouzení zabezpečení zařízení připojených k síti. Abychom mohli poskytovat funkci posouzení zabezpečení,

zpracováváme název lokální sítě a informace o zařízeních v lokální síti, jako jsou přítomnost, typ, název, IP adresa a adresa MAC zařízení v lokální síti společně s informacemi o licencích. V případě routeru tyto informace dále zahrnují způsob zabezpečení bezdrátové sítě a typ použitého šifrování bezdrátové sítě. Informace o licencích identifikující koncové uživatele jsou anonymizovány nejpozději 12 měsíců po skončení platnosti licence.

Technická podpora. Za účelem poskytování podpory mohou být vyžadovány kontaktní a licenční informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory. Údaje zpracovávány za účelem poskytování technické podpory jsou ukládány na dobu 4 let.

Ochrana proti zneužití dat Pokud koncový uživatel vytvoří účet ESET HOME na webu <https://home.eset.com> a aktivuje tuto funkci v souvislosti s krádeží počítače, budou shromážděny a zpracovány následující informace: údaje o poloze, snímky obrazovky, data o konfiguraci počítače a data zaznamenaná kamerou počítače. Shromážděné údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb a jsou uchovávány po dobu 3 měsíců.

Password Manager. Pokud se rozhodnete aktivovat funkci Password Manager, budou data související s vašimi přihlašovacími údaji uložena v šifrované podobě pouze na vašem počítači nebo jiném určeném zařízení. Pokud aktivujete synchronizační službu, šifrované údaje jsou uloženy na našich serverech nebo na serverech našich poskytovatelů služeb, abychom tuto službu mohli zajistit. Společnost ESET ani poskytovatelé služeb nemají k šifrovaným datům přístup. Pouze Vy máte klíč potřebný k dešifrování dat. Tato data budou odebrána při deaktivaci této funkce.

ESET LiveGuard. Pokud se rozhodnete aktivovat funkci ESET LiveGuard, bude třeba odesílat vzorky, jako jsou soubory předdefinované a vybrané koncovým uživatelem. Vzorky, které vyberete ke vzdálené analýze, budou odeslány do služby společnosti ESET a výsledky analýzy budou odeslány zpět do vašeho počítače. Veškeré podezřelé vzorky se zpracovávají stejným způsobem jako informace shromážděné systémem zpětné vazby ESET LiveGrid®.

Program zvyšování spokojenosti zákazníků Pokud jste se rozhodli aktivovat [Program zvyšování spokojenosti zákazníků](#), budou na základě Vašeho souhlasu shromažďovány a používány anonymní telemetrické informace týkající se používání našich produktů.

Upozorňujeme, že pokud osoba používající naše produkty a služby není koncový uživatel, který si zakoupil produkt nebo službu a uzavřel s námi smlouvu EULA (například zaměstnanec koncového uživatele, člen rodiny nebo osoba, která od koncového uživatele jiným způsobem dostala oprávnění používat produkt nebo službu v souladu se smlouvou EULA), je zpracování údajů prováděno na základě oprávněného zájmu společnosti ESET, jak je definován v článku 6 (1) f) nařízení GDPR, abychom mohli uživateli autorizovanému koncovým uživatelem umožnit používání námi poskytovaných produktů a služeb v souladu se smlouvou EULA.

Kontaktní informace

Pokud byste chtěli uplatnit svá práva jako subjekt údajů nebo máte nějakou otázku či obavy, pošlete nám zprávu na adresu:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk