ESET LiveGuard Advanced

Uživatelská příručka

Klikněte sem pro zobrazení online verze tohoto dokumentu

Digital Security
Progress. Protected.

Copyright ©2024 ESET, spol. s r.o.

ESET LiveGuard Advanced byl vyvinut společností ESET, spol. s r.o.

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

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

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

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

REV. 2024-01-31

1 Vítejte 1
2 Představení produktu 2
2.1 Jak fungují jednotlivé detekční vrstvy 4
2.2 Požadavky a podporované produkty 9
2.3 Používání ESET LiveGuard Advanced společně s proxy 11
2.3 Apache HTTP Proxy 12
2.3 Konfigurace proxy na Linuxu 13
2.3 Konfigurace proxy na Windows 15
3 Jak si mohu zakoupit tuto službu? 18
4 Aktivace ESET LiveGuard Advanced 18
4.1 Importování licencí do EBA 19
4.2 Synchronizace EBA s ESET PROTECT On-Prem 21
4.3 Přidání licence do ESET MSP Administrator 24
4.4 Synchronizace ESET MSP Administrator s ESET PROTECT On-Prem 29
4.5 Hromadná aktivace počítačů 32
4.6 Aktivace jednotlivých počítačů 37
4.7 Vzdálená instalace a aktivace 39
5 Jak zapnout a konfigurovat ESET LiveGuard Advanced? 42
5.1 Konfigurace bezpečnostního produktu ESET 42
5.2 Správa politik 45
6 Používání ESET LiveGuard Advanced 48
6.1 ESET Mail Security 50
6.2 ESET Endpoint Security a ESET Server Security 54
6.3 ESET Cloud Office Security 58
6.4 Proaktivní ochrana 60
6.5 Seznam odeslaných souborů 63
6.6 Vytvoření přehledu 67
6.7 Výsledek analýzy 71
6.7 Přehled chování souboru 73
6.8 Ruční odeslání souboru k analýze 74
6.8 Odeslání prostřednictvím ESET PROTECT On-Prem 75
6.8 Odeslání prostřednictvím ESET Endpoint Security 76
6.8 Odeslání prostřednictvím ESET Server Security 77
6.8 Odeslání prostřednictvím ESET Mail Security 79
6.9 Vytvoření výjimky 80
6.10 Použití výjimek pro zvýšení výkonu 83
6.10 Analyzování seznamu odeslaných souborů 83
6.10 Vyloučení složek 90
6.10 Vyloučení procesu 94
6.10 Analýza počtu odeslaných souborů 97
6.11 Oznámení při detekci hrozby 101
7 FAQ 103
8 Jak otestovat funkčnost služby ESET LiveGuard Advanced 106
9 Řešení problémů 109
9.1 Diagnostika 116
9.2 Řešení problémů – Apache HTTP Proxy 120
10 Bezpečnostní dokumentace pro ESET LiveGuard Advanced 122
11 Fair Use Policy 126
12 Zásady ochrany osobních údajů 127

13 Podmínky použití 129
13.1 ESET Management Agent EULA 133
13.2 Smlouva o zpracování údajů 139
13.3 Standardní smluvní body 141

Vítejte

Vítejte v uživatelské příručce k ESET LiveGuard Advanced. V tomto dokumentu vás seznámíme se správou a používáním ESET LiveGuard Advanced. Detailně vám rovněž představíme komunikaci mezi ESET LiveGuard Advanced a bezpečnostními produkty ESET.

Stránky nápovědy jsou pro lepší orientaci logicky uspořádány do jednotlivých kapitol a podkapitol. Související informace tak naleznete jednoduchým procházením této struktury stránek. Využít můžete rovněž vyhledávání v horší části stránky.

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

- V Databázi znalostí naleznete odpovědi na nejčastější dotazy stejně jako doporučené řešení mnoha situací. Články pravidelně aktualizujeme a připravujeme návody na řešení aktuálních situací.

- ESET forum představuje jednoduchý způsob, jak ESET uživatelé mohou požádat o radu a pomoci ostatním. Můžete sem umístit váš problém nebo dotaz týkající se produktu ESET.

- K dispozici máte možnost ohodnotit naši příručku a poskytnout nám zpětnou vazbu na konkrétní kapitolu. Zpětná vazbu poskytnete kliknutím na možnost Byla pro vás tato informace užitečná?

Informační boxíky použité v této příručce:

Poznámka poskytuje cenné informace k dané funkci nebo odkaz na související kapitoly.

Tato akce vyžaduje vaši pozornost a neměli byste ji ignorovat. Obvykle obsahuje nekritické, ale však důležité informace.

Kritická informace, které byste měli věnovat pozornost. Upozornění 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.

Praktický příklad použití. Příklady používáme pro vysvětlení složitějších témat.

Používané styly textu

Konvence	Význam
Bold type	Názvy položek uživatelského rozhraní jako dialogová okna a tlačítka.
Code	Příklady kódů nebo příkazů.
Hyperlink	Poskytuje rychlý přístup do odkazovaných kapitol nebo externích zdrojů. Hypertextové odkazy jsou zvýrazněny modře, mohou být podtržené.
%ProgramFiles%	Systémová složka operačního systému Windows, do které se standardně instalují programy a další součásti systému.

Představení produktu

Popis služby

ESET LiveGuard Advanced je placená služba poskytovaná společností ESET. Jedná o další vrstvu ochrany navrženou pro snížení dopadu zcela nových hrozeb.

Přejmenování služby

23. března 2022 se název služby ESET Dynamic Threat Defense změnil na ESET LiveGuard Advanced. V nabídce ESET produktů pro firemní zákazníky jej naleznete jako ESET LiveGuard. Oba názvy se však odkazují na stejnou službu.

Dostupnost služby

Prostřednictvím portálu ESET Status Portal získáte aktuální přehled o dostupnosti služeb ESET. Naleznete zde seznam online služeb ESET společně s přehledem o jejich stavu, včetně historie incidentů. Pokud se jako uživatel ESET potýkáte s jakýmkoli problémem souvisejícím se službou ESET, a na portále ESET Status Portal není uveden, kontaktujte technickou podporu ESET.

Jak funguje?

Do ESET cloudu jsou k analýze zasílány všechny podezřelé soubory, u kterých nebylo potvrzeno, že jsou škodlivé a hrozí, že by mohly být zdrojem malware. Odeslané vzorky jsou spouštěny v sandboxu a vyhodnocovány prostřednictvím našich pokročilých detekčních technik. Škodlivé vzorky a podezřelý spam je zasílám do systému ESET LiveGrid®. Přílohy e-mailů jsou zpracovávány samostatně a zasílají se do ESET LiveGuard Advanced. Administrátor může ovlivnit, jaké typy souborů budou k analýze zasílány, stejně tak dobu, po níž budou uchovávány v ESET cloudu. Standardně se k analýze nezasílají dokumenty a PDF s aktivním obsahem (makry, javascript). Detailní popis naleznete v kapitole Jak fungují jednotlivé detekční vrstvy.

Přehled o chování analyzovaného vzorku má administrátor k dispozici v konzoli pro vzdálenou správu v sekci **Další** > Odeslané soubory. Pokud se ukáže, že je soubor škodlivý, blokován jako podezřelý objekt bude u všech uživatelů, kteří jsou zapojeni do systému ESET LiveGrid®. V případě, že je soubor označen jako podezřelý, na základě nastavení může být zablokován na všech zařízení v rámci dané organizace.

Soubory můžete k analýze odesílat manuálně nebo automaticky na základě konfigurace. Prostřednictvím webové konzole ESET PROTECT mohou uživatelé odeslat .exe soubory reportované z klientských stanic.

Jaký je rozdíl mezi ESET LiveGuard Advanced, ESET LiveGrid® a ESET Threat Intelligence?

Architektura

Bezpečnostní produkty ESET a konzole pro vzdálenou správu

Při každém odeslání souboru k analýze do ESET LiveGuard Advanced se zároveň nahrají metadata o objektu do konzole pro vzdálenou správu (pokud se klient dokáže spojit se serverem). Administrátor tak má k dispozici seznam všech objektů nahraných do cloudového systému ESET.

Bezpečnostní produkty ESET a ESET LiveGuard Advanced

Pokud se aktivovaný a nakonfigurovaný bezpečnostní produkt rozhodne pro odeslání vzorku k analýze, nahraje jej do ESET LiveGuard Advanced. Po analyzování vzorku je výsledek ESET LiveGuard Advanced poskytnut všem stanicím ve vaší společnosti (nebo MSP zákazníka) a všem společnostem, které kdy daný soubor zaslali. Bezpečnostní produkt následně provede definovanou akci, dle nastavení v politice. V produktech z řady ESET Endpoint a určených pro ochranu serverů si od verze 7.2 můžete nastavit akci, která se provede nad soubory stahovanými prostřednictvím internetových prohlížečů nebo poštovní klientů.

Za účelem snížení rizika útoku jsou všechna přenášená data podepsaná společností ESET. Při použití HTTP spojení v interní síti produkt vždy ověřuje, zda byla za proxy komunikace převedena na HTTPS. Pokud není proxy správně nakonfigurována, HTTPS spojení se použije také v interní síti.

ESET konzole pro vzdálenou správu a ESET LiveGuard Advanced

ESET LiveGuard Advanced je dostupný jak v on-premises, tak v cloudových konzolích (ESET PROTECT On-Prem / ESET PROTECT) pro správu. Ve chvíli, kdy ESET LiveGuard Advanced obdrží vzorek od bezpečnostního produktu, informace o stavu analýzy je automaticky zaslána do konzole pro vzdálenou správu. Po dokončení analýzy je výsledek přenesen do konzole pro vzdálenou správu.

Mobilní uživatelé a ESET LiveGuard Advanced

Za mobilní uživatele považujeme jakékoli zařízení s nainstalovaným bezpečnostním produktem ESET, které je mimo firemní síť a nemá přístup k ESET PROTECT On-Prem. Typicky, když má zaměstnanec zařízení doma nebo je na služební cestě a nemá aktivní VPN. Mobilní uživatelé nepřichází o žádné výhody ESET LiveGuard Advanced. Pouze v dané době nejsou informace o odeslaných vzorcích zasílány do ESET PROTECT On-Prem. Po připojení zařízení do firemní sítě a připojení k ESET PROTECT On-Prem se metadata synchronizují a dojde k aktualizaci seznamu odeslaných souborů. Ostatní stanice v síti obdrží informaci o výsledku analýze nově objevené hrozby od mobilních uživatelů i bez toho, že by se data musela nahrát nejprve do ESET PROTECT On-Prem.

ESET Cloud Office Security a ESET LiveGuard Advanced

ESET LiveGuard Advanced analyzuje zaslané soubory jejich spuštěním v izolovaném prostředí za účelem vyhodnocení jejich chování. ESET Cloud Office Security k analýze do ESET LiveGuard Advanced zasílá podezřelé přílohy zprávy a vzorky sdílené prostřednictvím Microsoft SharePoint, Teams. K využití této služby v ESET Cloud Office Security není vyžadována ESET konzole pro vzdálenou správu, ani se do ní nenahrávají žádná související data. Informace související s odeslanými soubory a výsledky jejich analýzy jsou dostupné výhradně v ESET Cloud Office Security.

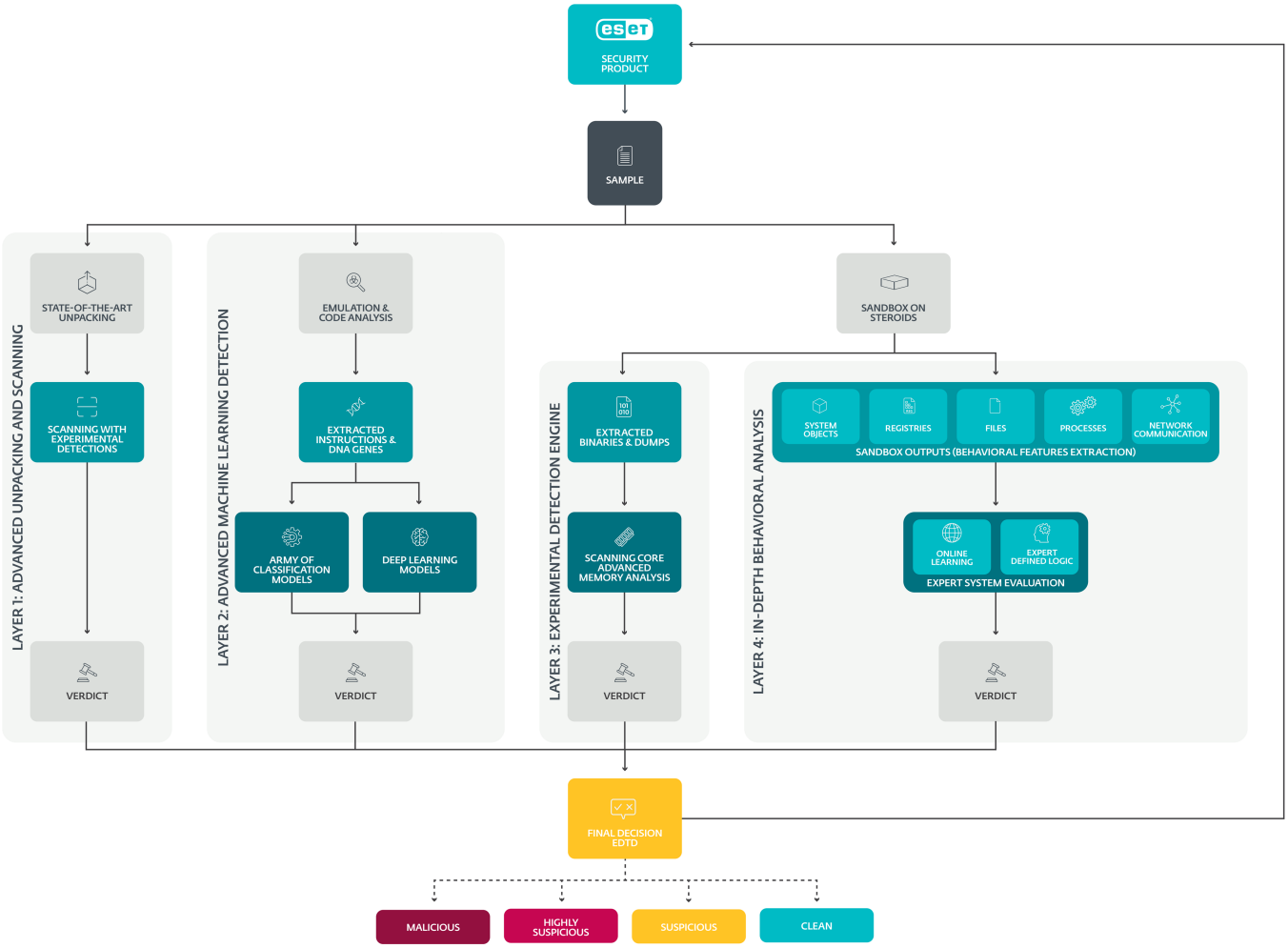
Globální databáze

ESET LiveGuard Advanced ukládá kontrolní součty souborů a výsledky jejich analýzy do dvou datových center (umístěných v Evropě a USA). Využitím datacenter dochází k rychlejšímu doručení výsledku analyzovaných souborů. V centrále společnosti ESET (nacházející se na Slovensku) jsou uloženy všechny odeslané soubory a provádí se zde jejich analýza. Data jednotlivých zákazníků (společností) jsou uchovávána v samostatných databázích. ESET automaticky směruje uživatele k nejbližšímu datacentru.

> V sítích s velkým počtem klientských stanic (stovky a více) doporučujeme využít HTTP Proxy pro cachování odpovědí z ESET serverů. Jejím použitím můžete výrazně snížit množství přenášených dat.
> Pro snížení počtu odesílaných souborů a vylepšení celkového výkonu můžete vyloučit vybrané složky a procesy.

Jak fungují jednotlivé detekční vrstvy

Pro zajištění nejvyšší míry detekce využívá ESET LiveGuard Advanced čtyři odlišné detekční vrstvy. Každá vrstva analyzuje vzorek jiným způsobem a poskytuje samostatný výsledek. Finální rozhodnutí je založeno na základě všech získaných informacích o zaslaném vzorku. Níže uvádíme schéma celého procesu:

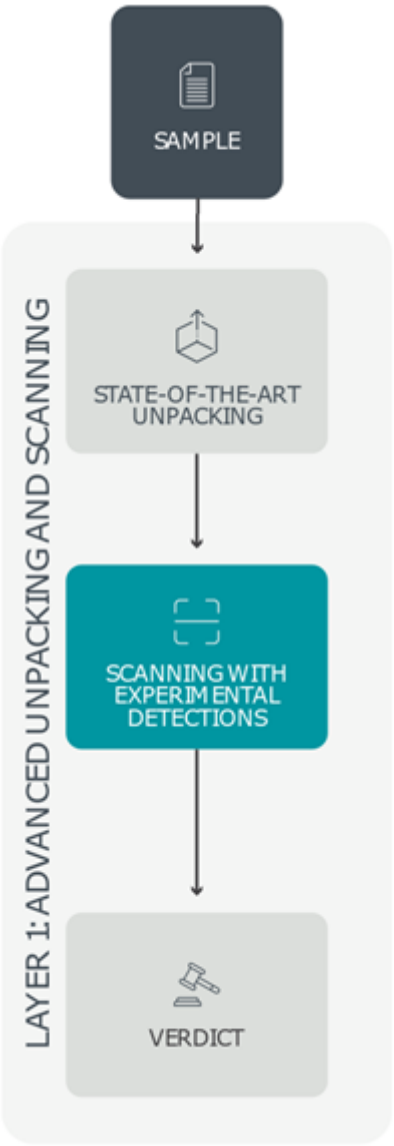


Kliknutím na obrázek si zobrazíte jeho plnou velikost

Vrstva č.1: Pokročilá extrakce a kontrola

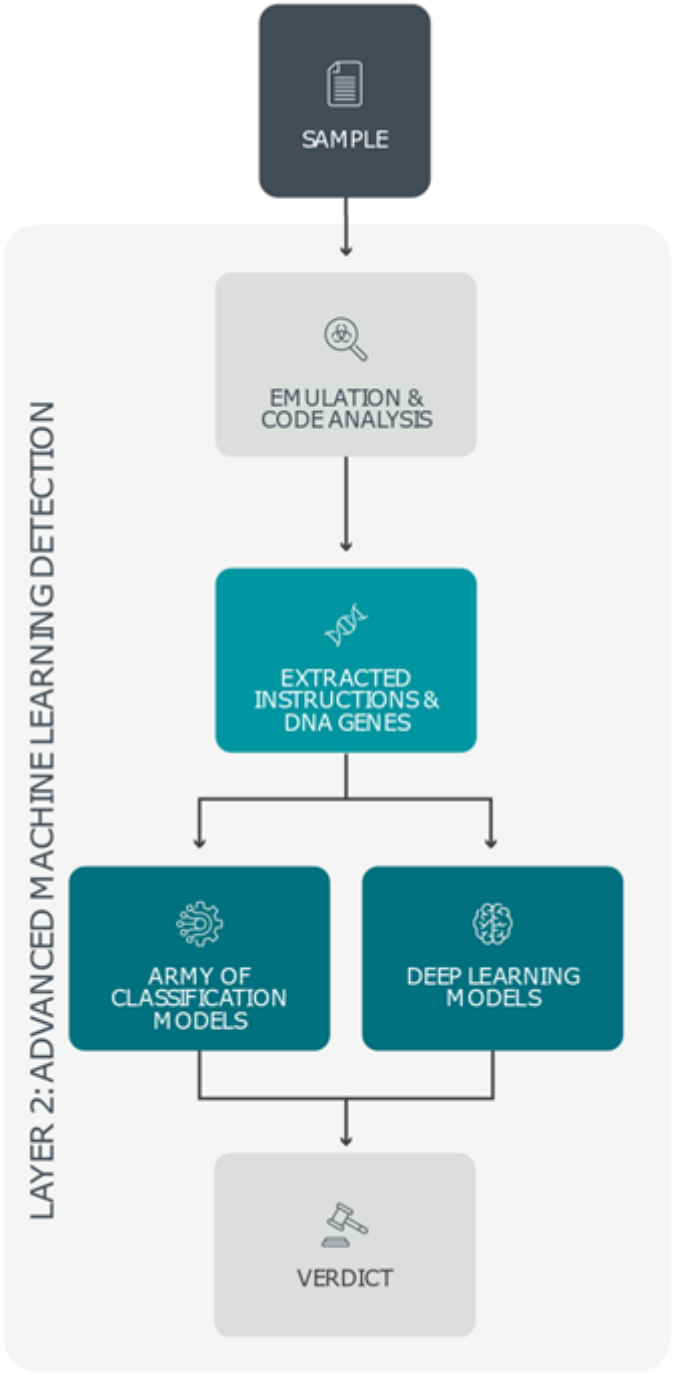
Po vstupu do počáteční vrstvy ESET LiveGuard Advanced – zvané pokročilá extrakce a kontrola – se statické vzorky porovnávají vůči databázi hrozeb společnosti ESET, která je navíc doplněna o experimentální a dosud nezveřejněné detekce. Stejně se vzory porovnávají vůči seznamu čistých, potenciálně nechtěných (PUA) a potenciálně zneužitelných (PUsA) objektů. Malware se často snaží zabránit detekci skrytím svého škodlivého jádra za několik komprimačních vrstev. Pro zajištění správné analýzy je nutné nejprve tento obal odstranit. ESET LiveGuard Advanced k tomu využívá právě vrstvu pokročilé extrakce a kontroly, kdy jsou na vzorky spuštěny velmi specializované nástrojů založené na tzv. packerech, které analytici virových laboratoří ESET objevili ve škodlivém kódu. Tyto specializované nástroje na extrakci odstraní ochranný obal škodlivého kódu, aby ESET LiveGuard

Advanced následně mohl opětovně porovnat vzorek vůči databázi hrozeb doplněné o dosud nezveřejněné detekce. Vrstva pokročilé extrakce a kontroly klasifikuje vzorek jako čistý, malware, PUA nebo PUsA. S ohledem na bezpečnostní rizika a hardwarové požadavky ze strany nástrojů na extrakci a další související procesů, je nezbytným předpokladem k provádění těchto operací velmi výkonné a bezpečné prostředí. Toto jedinečné prostředí zajišťuje robustní a odolná cloudová infrastruktura ESET LiveGuard Advanced.



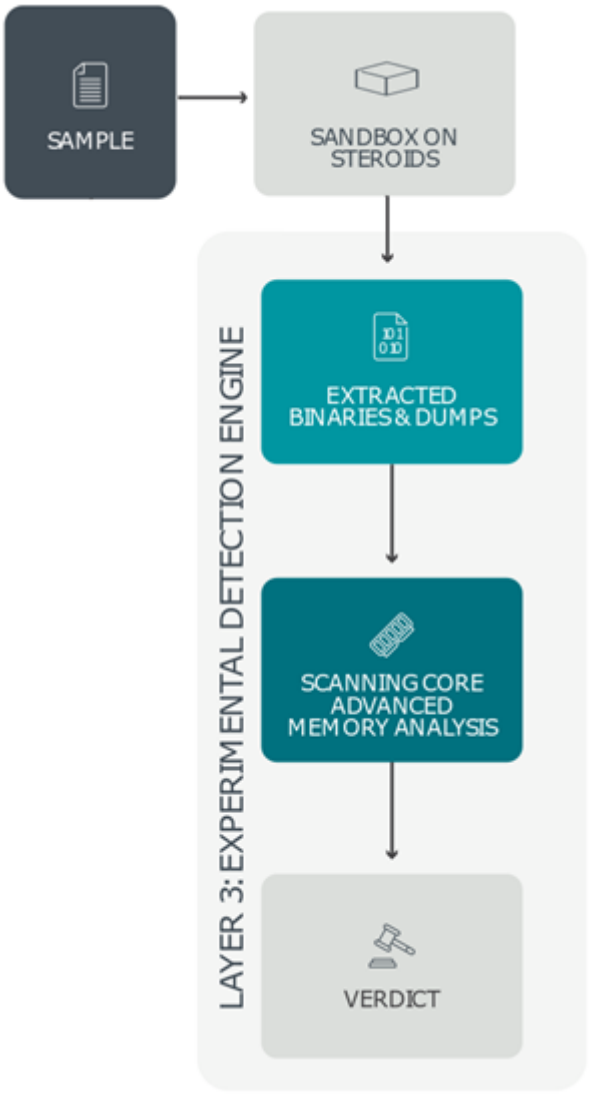
Vrstva č.2: Detekce s využitím pokročilého strojového učení

Každý vzorek odeslaný do ESET LiveGuard Advanced je podroben statické analýze prostřednictvím detekce s využitím pokročilého strojového učení, jejímž výstupem je základní charakteristika vzorku. Pouhá analýza komprimovaného nebo zašifrovaného kódu bez jeho dalšího zpracování by vedla pouze k pokusu o klasifikaci datového šumu bez relevantního výsledku. Proto je objekt zároveň podroben další, dynamické, analýze, která z něj získá jeho instrukce a geny (DNA). Popsáním aktivních vlastností a chování vzorku je možné odhalit charakteristiku komprimovaných nebo obfuskovaných vzorků bez jejich spuštění. Informace získané v předchozích krocích jsou dále zpracovány hrstkou pečlivě vybraných klasifikačních modelů a algoritmů hloubkového učení. Na závěr jsou všechny tyto informace spojeny prostřednictvím neuronové sítě, která klasifikuje vzorek jako čistý, podezřelý, velmi podezřelý nebo škodlivý. V případě že se tato nebo jiná vrstva ESET LiveGuard Advanced nepoužije, zobrazí se informace "analýza není potřebná". Vzhledem na složitost a hardwarové požadavky těchto operací je vyžadovaná výrazně výkonnější infrastruktura, než kterou dokáže nabídnout koncové zařízení uživatele. Na zvládnutí těchto výpočtově náročných úloh vyvinuli inženýři společnosti ESET špičkovou a komplexní sestavu systémů – ESET LiveGuard Advanced.



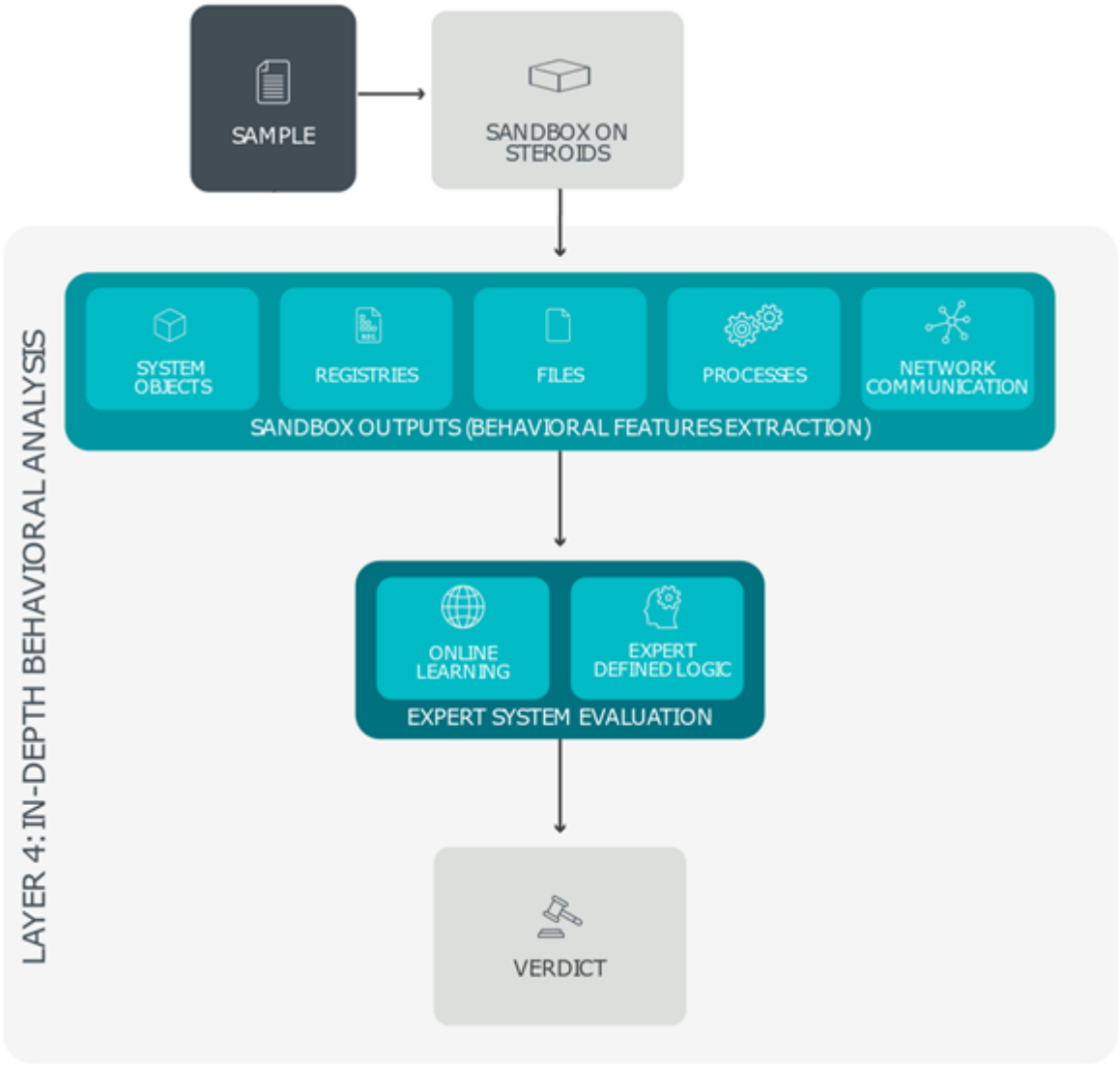
Vrstva č.3: Experimentální detekční jádro

Dále je nezbytné u každého vzorku provést jeho hlubší analýzu chování, která doplní předchozí zjištění. Získání tohoto typu informací o hrozbách zajišťuje v ESET LiveGuard Advanced detekční vrstva zvaná Experimentální detekční jádro. Podezřelé objekty jsou umístěny do sady přesně nakonfigurovaných systémů, které připomínají počítače z reálného života s různými operačními systémy – představit si je můžete jako "sandbox na steroidech". Toto kontrolované prostředí slouží jako monitorovací buňky vybavené řadou detekčních algoritmů ESET, které zaznamenávají každou akci. Za účelem identifikace skrytého škodlivého chování generuje experimentální detekční jádro velké množství výpisů paměti. Ty jsou následně kontrolovány a porovnávány vůči databázi hrozeb společnosti ESET doplněné o experimentální a dosud nezveřejněné detekce, za účelem dosažení velmi přesných výsledků detekce a extrémně nízkého počtu falešných poplachů. Informace získané experimentálním detekčním jádrem jsou zaznamenány do souhrnného seznamu událostí zachycených v sandboxu. Tento seznam je následně využit v poslední detekční vrstvě ESET LiveGuard Advanced.



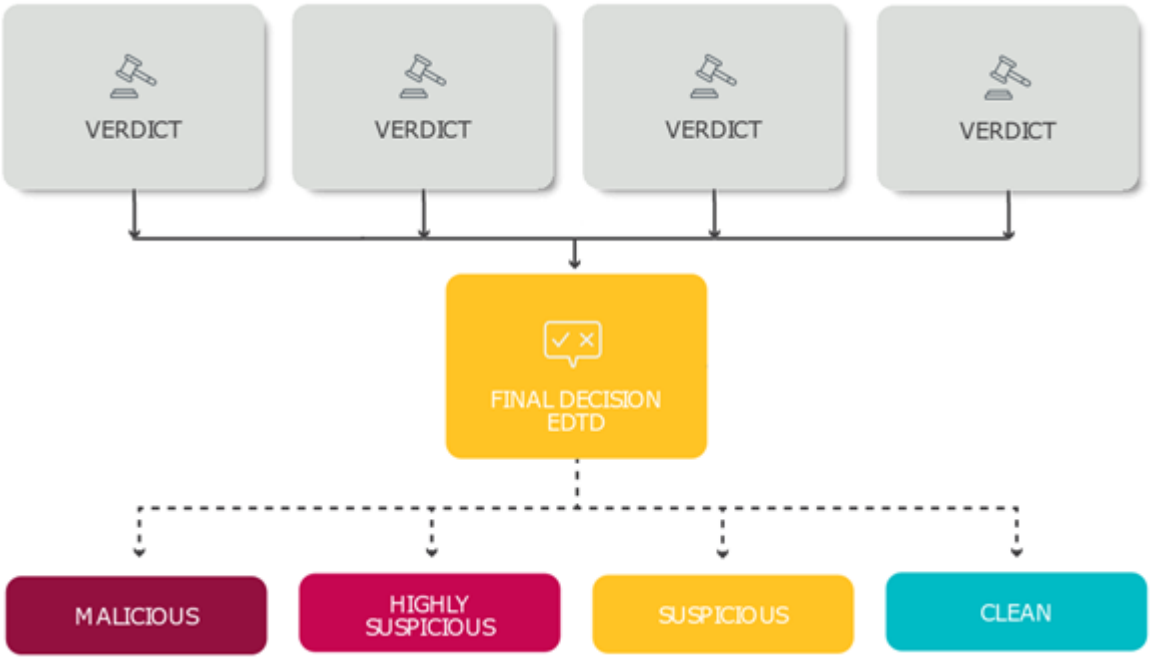
Vrstva č.4: Hloubková analýza chování

Poslední detekční vrstva systému ESET LiveGuard Advanced, známá jako Hloubková analýza chování, podrobně analyzuje aktivitu vzorku – včetně informací o vytvořených nebo smazaných souborech z pevného disku, záznamech v registru Windows, veškerých pokusech o externí komunikaci a spuštěných skriptech. V této fázi se ESET LiveGuard Advanced zaměřuje na škodlivé a podezřelé aktivity jako jsou pokusy o připojení k webovým umístěním se špatnou reputací, použití známých škodlivých objektů a jedinečných řetězců vygenerovaných konkrétními rodinami malware. Za účelem identifikace i nepatrného náznaku škodlivého chování, hloubková analýza chování rozděluje výstupy ze sandboxu do logických bloků, které jsou následně porovnávány vůči rozsáhlé a pravidelně kontrolované databázi dříve analyzovaných vzorců a řetězů aktivit.



Finální výsledek

ESET LiveGuard Advanced použije výsledky z jednotlivých vrstev a na základě nich vyhodnotí stav zaslaného vzorku. Výsledek je doručen bezpečnostnímu produktu ESET, ze kterého byl zaslán, stejně tak všem zařízením v infrastruktuře zákazníka.



Požadavky a podporované produkty

Požadavky pro uživatele on-premise produktů

Pro správnou funkčnost ESET LiveGuard Advanced musí vaše prostředí splňovat následující požadavky:

- Funkční účet na portále ESET Business Account nebo ESET MSP Administrator synchronizovaný s ESET konzolí pro vzdálenou správu
- Podporovaná ESET konzole pro vzdálenou správu
- Nainstalované kompatibilní bezpečnostní produkty ESET ve verzi 7.x nebo novější
- Platná licence pro ESET LiveGuard Advanced
- Aktivovaný bezpečnostní produkt ESET LiveGuard Advanced licencí
- Zapnutý ESET LiveGuard Advanced prostřednictvím politiky v kompatibilním bezpečnostním produktu
- Povoleny porty, stejné jako pro ESET LiveGrid®.
- Pokud používáte Apache HTTP Proxy nebo ESET Bridge, požadavky na porty jsou stejné, jako u ESET LiveGrid®. Jinak bude použit port 443.
  - Přístup k online serverům ESET LiveGuard Advanced.

Požadavky pro uživatele ESET Cloud Office Security

Aby uživatel ESET Cloud Office Security mohl použít ESET LiveGuard Advanced, musí splnit následující požadavky:

- Funkční účet na portále ESET Business Account nebo ESET MSP Administrator připojený k ESET Cloud Office Security

- Platná licence pro ESET LiveGuard Advanced

ESET Cloud Office Security nesdílí žádné informace o odeslaných souborech s ESET konzolí pro vzdálenou správu.

Přístupová oprávnění v konzoli pro vzdálenou správu

Odeslané soubory a výsledky analýzy uvidí ve webové konzoli pouze uživatel s přístupovým oprávněním k zařízení, ze kterého byl vzorek k analýze odeslán. Z webové konzole můžete ručně odeslat k analýze spustitelný soubor reportovaný z ESET Inspect. Takovou akci může provést uživatel v případě, kdy má oprávnění **Použít** nad počítačem, na kterém k detekci došlo, a zároveň má ve své domovské skupině oprávnění **Zápis** pro funkci **Odeslat soubor do ESET LiveGuard**.

Mobilní uživatelé – pokud není ESET PROTECT Server ze zařízení dosažitelný, ale klient má přístup na cloudové servery ESET, soubory odeslané ze zařízení budou dostupné až po připojení zařízení k serveru.

Výkon

Pro cachování výsledků doručených z ESET LiveGuard Advanced můžete použít ESET Bridge. Minimalizuje množství dat stažených z internetu.

V podnikových prostředích (při správě více než 1 000 klientů) doporučujeme pro ESET Bridge použít dedikovaný server. Cachování velkého množství souborů má negativní vliv na výkon serveru. V prostředích, kde vyžadujete vysokou dostupnost, doporučujeme nainstalovat jednotlivé komponenty na samostatné stroje (ESET PROTECT Server, ESET Bridge, databázový server). Zároveň nedoporučujeme provozovat aplikace náročné na prostředky na stejném serveru, kde běží ESET PROTECT On-Prem.

Další možností pro vylepšení celkového výkonu je snížení počtu odesílaných souborů. Toho dosáhnete vyloučením souborů, složek nebo procesů a zároveň zabráníte odeslání osobních souborů k analýze. Další informace naleznete v kapitole Použití výjimek pro zvýšení výkonu.

Podporované licence

ESET LiveGuard Advanced můžete aktivovat prostřednictvím:

- Licencí z EBA s platností jeden, dva nebo tři roky
- MSP licence formou předplatného z ESET MSP Administrator

Podporované produkty

Odeslání souborů k analýze do ESET LiveGuard Advanced je možné pouze z podporovaných produktů. Seznam odeslaných souborů je dostupný pouze v podporované verzi konzole.

Bezpečnostní produkty

Produkt	Verze
ESET Endpoint Antivirus pro Windows* ESET Endpoint Security pro Windows	✓ verze 7 a novější
ESET Mail Security pro Microsoft Exchange	✓ verze 7 a novější
ESET File Security pro Windows Server	✓ verze 7.x

Produkt	Verze
ESET Server Security pro Windows Server (dříve známý jako ESET File Security pro Windows Server)	✔ verze 8 a novější
ESET Endpoint Antivirus pro Linux:	✔ verze 8.1 a novější
ESET Server Security pro Linux:	✔ verze 8.1 a novější
ESET Cloud Office Security	✔ (od prosince 2021)

* Funkčnost ESET LiveGuard Advanced je stejná pro ESET Endpoint Antivirus i ESET Endpoint Security. V příručce však pro zjednodušení vždy odkazujeme do dokumentace k produktu ESET Endpoint Security. Postup pro konfiguraci je v obou produktech (ESET Endpoint Antivirus i ESET Endpoint Security) stejný.

Konzole pro správu

Produkt a verze	Podpora
ESET PROTECT On-Prem 8 a novější	✔
ESET Security Management Center 7.0 a 7.1	⛔ Podpora těchto verzí konzolí byla ukončena.
ESET Security Management Center 7.2	⛔
ESET Remote Administrator 6.x a starší	⛔
ESET PROTECT	✔

Nepodporované operační systémy
ESET LiveGuard Advanced není podporován na klientských stanicích s operačním systémem Windows XP a Windows Server 2003. Tyto systémy nepodporují TLS 1.2, který je nezbytný k zabezpečenému přenosu odesílaných vzorků.

Podporované proxy

ESET Bridge byl vydán s ESET PROTECT On-Prem 10.0 jako náhrada za Apache HTTP Proxy, a je součástí All-in-one instalačního balíčku konzoli pro vzdálenou správu. Ke stažení je rovněž samostatně na webových stránkách společnosti ESET. Apache HTTP Proxy zůstává funkční, doporučujeme však přejít na ESET Bridge.

Používání ESET LiveGuard Advanced společně s proxy

ESET Bridge můžete použít k přesměrování komunikace na ESET servery a cachování přenesených ESET LiveGuard Advanced dat. Cachováním komunikace snížíte množství přenesených dat. Použití proxy je nezbytné pouze v případech, kdy klientská stanice nemá přímý přístup na servery společnosti ESET. Pokud ESET Bridge používáte k přesměrování komunikace mezi ESET Management Agenty a ESET PROTECT Serverem, můžete ji použít rovněž ke cachování výsledků doručených z ESET LiveGuard Advanced. ESET Bridge podporuje též řetězení proxy.

Nastavení proxy na klientských počítačích
V nastavení bezpečnostního produktu je nezbytné v sekci **Nastavení** > **Nástroje** > **Proxy server** definovat proxy server. Provést to můžete vzdáleně prostřednictvím politiky.

Uživatelé ESET PROTECT

Pokud v síti (například v jedné pobočce) máte alespoň 10 počítačů, měli byste pro cachování výsledků používat

ESET Bridge. V případě, že klientské počítače nesdílejí interní síť nebo VPN, proxy nepoužívejte. Více informací o ESET Bridge naleznete v příručce k ESET PROTECT.

> **Uživatelé Apache HTTP Proxy**
> Od ESET PROTECT ve verzi 4.0 a ESET PROTECT On-Prem 10.0 (uvolněnou v listopadu 2022) nahradil ESET Bridge komponentu Apache HTTP Proxy. Od této chvíle je na Apache HTTP Proxy poskytována částečná podpora. Pokud používáte Apache HTTP Proxy, doporučujeme přejít na ESET Bridge.

Uživatelé virtuální appliance ESET PROTECT

ESET Bridge nepodporuje virtuální appliance postavené na operačním systému CentOS 7. Uživatelé virtuální appliance ESET PROTECT si mohou vybrat jednu z následujících možností:

- Nainstalujte ESET Bridge na samostatný server (viz požadavky na ESET Bridge).
- Použijte Apache HTTP Proxy, který je součástí virtuální appliance.

Instalace ESET Bridge

ESET Bridge můžete nainstalovat několika způsoby. Doporučujeme využít nejnovější all-in-one instalační balíček ESET PROTECT.

Ukládání výsledků z ESET LiveGuard Advanced do cache

ESET Bridge má ve výchozím nastavení správnou konfiguraci pro ukládání výsledků do cache. K ukládání výsledků do cache dojde automaticky poté, co provedete konfiguraci ESET Bridge, a budete ji používat jako proxy řešení pro ukládání dat do cache a aktivaci služby ESET LiveGuard Advanced.

Apache HTTP Proxy

Doporučení

Apache HTTP Proxy zůstává funkční, poskytována je na něj však pouze částečná podpora. Místo něj doporučujeme využívat ESET Bridge.

Konfigurační soubor proxy

Na Linuxu a Windows se umístění konfiguračních souborů liší. Nejčastější umístění konfiguračních souborů uvádíme v tabulce níže.

Operační systém	Konfigurační soubory
Windows	*C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
Linux (Debian distribuce)	*/etc/apache2/mods-available/proxy.conf*
Virtuální appliance (Linux)	*/etc/httpd/conf.d/proxy.conf*

Proxy chaining

V případě potřeby můžete komunikaci proxy směrovat na další podporovanou proxy. Do konfigurace vaší proxy přidejte řádek `ProxyRemote * AddressOfNextProxy` Všechny proxy musí mít v tomto případě stejné nastavení.

Příklad, kde 10.1.1.2 je IP adresa nadřazené proxy:

```
ProxyRemote * http://10.1.1.2:3128
```

Pro aplikování nové konfigurace restartujte službu proxy.

Proxy třetích stran (non-Apache)

Proxy řešení třetích stran nejsou podporována. V některých případech komunikace může fungovat, nicméně ESET neposkytuje jejich konfiguraci ani podporu v tomto případě použití.

Řešení problémů

Pro získání detailních protokolů z proxy přidejte/upravte v konfiguračním souboru parametr `LogLevel debug` a restartujte její službu. Následně v protokolech uvidíte bližší informace týkající se řešeného problému, případně diagnostické protokoly předejte specialistům technické podpory.

> Při použití ESET LiveGuard Advanced v enterprise prostředí (stovky a více stanic) doporučujeme nasadit HTTP Proxy na samostatný server. Provozování služby HTTP Proxy na velmi vytíženém serveru (například s ESET PROTECT Server nebo databázovým serverem) může vést k potížím s připojením k ESET LiveGuard Advanced.
> Pro snížení počtu odesílaných souborů a vylepšení celkového výkonu můžete vyloučit vybrané složky a procesy.

Konfigurace proxy na Linuxu

> Tato konfigurace je určený výhradně pro Apache HTTP Proxy. Pokud používáte ESET Bridge, nakonfigurujte jej prostřednictvím webové konzole ESET PROTECT.

V konfigurační souboru proxy ověřte, zda se v něm nacházejí následující řádky. Pokud ne, přidejte je ručně.

1. Pro cachování, komunikaci agenta, HTTPS spojení a protokolování přidejte do konfigurace následující řádky.

```
CacheEnable disk http://

CacheDirLevels 4

CacheDirLength 2

CacheDefaultExpire 3600

CacheMaxFileSize 500000000

CacheMaxExpire 604800
```

```
CacheQuickHandler Off
CacheRoot /var/cache/httpd/proxy

AllowCONNECT 443 2222 53535

ProxyRequests On
ProxyVia On

CacheLock on
CacheLockMaxAge 10
ProxyTimeOut 900
SetEnv proxy-initial-not-pooled 1

ErrorLog "|/usr/sbin/rotatelogs -n 10 /var/log/httpd/error_log 1M"
```

Parametry `CacheRoot` a `ErrorLog` v případě potřeby upravte dle použitého operačního systému.

2. Níže uvedené části kódu přidejte na konec výše uvedených řádků. Pro zapnutí cachování ESET LiveGuard Advanced komunikace na vaší proxy přidejte:

```
<VirtualHost *:3128>
 ProxyRequests On
</VirtualHost>

<VirtualHost *:3128>
        ServerName r.edtd.eset.com

         <If "%{REQUEST_METHOD} == 'CONNECT'">
            Require all denied
        </If>

        ProxyRequests Off
```

```
        CacheEnable disk /

        SSLProxyEngine On


        RequestHeader set Front-End-Https "On"

        ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
0 smax=10

        ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>
```

3. Uložte konfiguraci a restartujte službu proxy.

> **Zapnutí potřebného proxy režimu**
> Při použití vlastní Apache Proxy na Linuxu s ESET LiveGuard Advanced je nezbytné zapnout režimy: `headers ssl alias`.
> Například na distribucích postavených na Debianu použijte níže uvedené příkazy:
> 1.Pro načtení modulů:
> `sudo a2enmod headers ssl alias`
>
> 2.Pro restartování služby:
> `service apache2 restart`

Konfigurace proxy na Windows

> Tato konfigurace je určený výhradně pro Apache HTTP Proxy. Pokud používáte ESET Bridge, nakonfigurujte jej prostřednictvím webové konzole ESET PROTECT.

Při použití vlastní Apache Proxy na Windows je nezbytné pro cachování ESET LiveGuard Advanced komunikace provést úpravy v konfiguračním souboru *httpd.conf*, který obvykle naleznete ve složce *conf* do níž jste Apache nainstalovali.

Části konfigurace přidávejte ve stejném pořadí, jak jsou v této kapitole uvedeny.

4. Pro cachování ESET LiveGuard Advanced komunikace musí být aktivní moduly SSL, headers a alias. Ujistěte se, že jsou moduly načteny, a do konfiguračního souboru proxy serveru přidejte následující řádky pro načtení požadovaných modulů:

```
LoadModule alias_module ..\modules\mod_alias.dll

LoadModule ssl_module ..\modules\mod_ssl.dll

LoadModule headers_module ..\modules\mod_headers.dll
```

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

LoadModule proxy_module ..\modules\mod_proxy.dll
LoadModule proxy_http_module  ..\modules\mod_proxy_http.dll
LoadModule proxy_connect_module ..\modules\mod_proxy_connect.dll
LoadModule cache_module ..\modules\mod_cache.dll
LoadModule cache_disk_module ..\modules\mod_cache_disk.dll
```

5. Pro cachování, komunikaci agenta, HTTPS spojení a protokolování přidejte do konfigurace následující řádky.

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off

AllowCONNECT 443 563 2222 8883

ProxyRequests On
ProxyVia On
SetEnv proxy-initial-not-pooled 1

ErrorLog "logs/error.log"
LogLevel warn
```

Parametry `ErrorLog` a `LogLevel` upravte v případě potřeby dle použitého operačního systému.

6. Níže uvedené části kódu přidejte na konec výše uvedených řádků. Pro zapnutí cachování ESET LiveGuard Advanced komunikace na vaší proxy přidejte:

```
AcceptFilter https none

AcceptFilter http none

EnableSendfile Off

EnableMMAP off


<VirtualHost *:3128>

 ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

        ServerName r.edtd.eset.com


        <If "%{REQUEST_METHOD} == 'CONNECT'">

           Require all denied

        </If>


        ProxyRequests Off

        CacheEnable disk /

        SSLProxyEngine On


        RequestHeader set Front-End-Https "On"

        ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10
0 smax=10

        ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On

</VirtualHost>
```

7. Uložte konfigurační soubor a restartujte službu proxy.

Zakoupení licence

MSP uživatelé

Licenci na ESET LiveGuard Advanced si můžete objednat prostřednictvím ESET MSP programu.

> **ESET MSP Administrator ve verzi 1 není podporován**
> Pokud používáte ESET MSP Administrator, ujistěte se, že využíváte verzi 2 (portál dostupný na adrese msp.eset.com). ESET MSP Administrator ve verzi 1 byl dostupný na adrese ema.eset.com. Tato adresa je nyní přesměrována na ESET MSP Administrator ve verzi 2. EMA ve verzi 1 nepodporuje ESET LiveGuard Advanced.

Uživatelé ESET Business Account

Zakupte si licenci u svého prodejce a přidejte ji do svého účtu na portále ESET Business Account. Synchronizujte importovanou licenci s ESET PROTECT On-Prem a můžete jej začít používat.

Uživatelé ESET Cloud Office Security

Veškeré licenční úrovně ESET Cloud Office Security obsahují funkce ESET LiveGuard Advanced. Licenci poznáte dle toho, že vedle ID licence je uveden štítek ESET LiveGuard. Pokud jste ESET Cloud Office Security licenci zakoupili v minulosti samostatně, její migraci na licenci zahrnující podporu této služby provedla společnost ESET automaticky.

Vyzkoušejte si ESET LiveGuard Advanced bezplatně v rámci ESET PROTECT.

Uživatelé ESET PROTECT si mohou přímo ze své cloudové konzole vyžádat bezplatnou 30denní zkušební licenci na ESET LiveGuard Advanced.

Kontaktujte nás

S dotazy týkající se licencování produktu a jeho nákupu se obraťte na lokální obchodní oddělení společnosti ESET. Podporu ESET můžete kontaktovat e-mailem, prostřednictvím chatu nebo telefonicky. Všechny kontakty naleznete na webových stránkách.

Aktivace ESET LiveGuard Advanced

Uživatelé ESET Cloud Office Security

Funkce ESET LiveGuard Advanced je poskytována v rámci licence ESET Cloud Office Security. Službu ESET LiveGuard Advanced můžete spustit po vytvoření a přiřazení příslušných politik.

Uživatelé ESET PROTECT On-Prem a ESET PROTECT

ESET LiveGuard Advanced můžete ve své síti nasadit mnoha způsoby, závisí na typu a stavu prostředí. Postupujte podle níže uvedených kroků:

I. Získání licence

- Uživatelé ESET Business Account: Zakupte si licenci pro produkt ESET LiveGuard Advanced. Licenční klíč vám následně zašleme elektronicky na zadanou e-mailovou adresu.

- Uživatelé ESET MSP Administrator: Svému zákazníkovi v ESET MSP Administrator přidejte ESET LiveGuard Advanced licenci.

II. Importování licence

- Uživatelé ESET Business Account: Synchronizujte ESET PROTECT On-Prem s EBA účtem.

- Uživatelé ESET MSP Administrator: Synchronizujte ESET PROTECT On-Prem s ESET MSP Administrator účtem (uživatelům ESET PROTECT se cloudové licence synchronizují automaticky).

ESET LiveGuard Advanced je možné aktivovat pouze prostřednictvím licence nahrané v EBA nebo ESET MSP Administrator.

III. Instalace bezpečnostního produktu ESET

Vyberte si scénář, který nejlépe vystihuje vaše prostředí, a postupujte podle pokynů:

^ Mám na spravovaných stanicích nainstalovaný kompatibilní bezpečnostní produkt ESET.

1. Na stanice zašlete klientskou úlohu pro aktivaci, ve které vyberte licenci pro ESET LiveGuard Advanced.
2. Po aktivování produktu vytvořte politiku pro zapnutí ESET LiveGuard Advanced a přiřaďte ji klientským zařízením.

^ Mám na svých zařízeních nasazeného pouze ESET Management Agenta

Postupujte dle kroků uvedených v kapitole Vzdálená instalace a aktivace.

^ Používám ESET PROTECT a nemám na spravovaných zařízeních nainstalovaný bezpečnostní produkt ESET

1.Při instalaci agenta a bezpečnostního produktu na koncová zařízení postupujte podle návodu pro lokální nasazení.
2.Na stanice zašlete klientskou úlohu pro aktivaci, ve které vyberte licenci pro ESET LiveGuard Advanced.
3.Po aktivování produktu vytvořte politiku pro zapnutí ESET LiveGuard Advanced a přiřaďte ji klientským zařízením.

^ Používám ESET PROTECT On-Prem a nemám na spravovaných zařízeních nainstalovaný bezpečnostní produkt ESET

1.Pro nasazení agenta a bezpečnostního produktu postupujte podle návodu pro lokální nasazení.
2.Na stanice zašlete klientskou úlohu pro aktivaci, ve které vyberte licenci pro ESET LiveGuard Advanced.
3.Po aktivování produktu vytvořte politiku pro zapnutí ESET LiveGuard Advanced a přiřaďte ji klientským zařízením.

Importování licencí do EBA

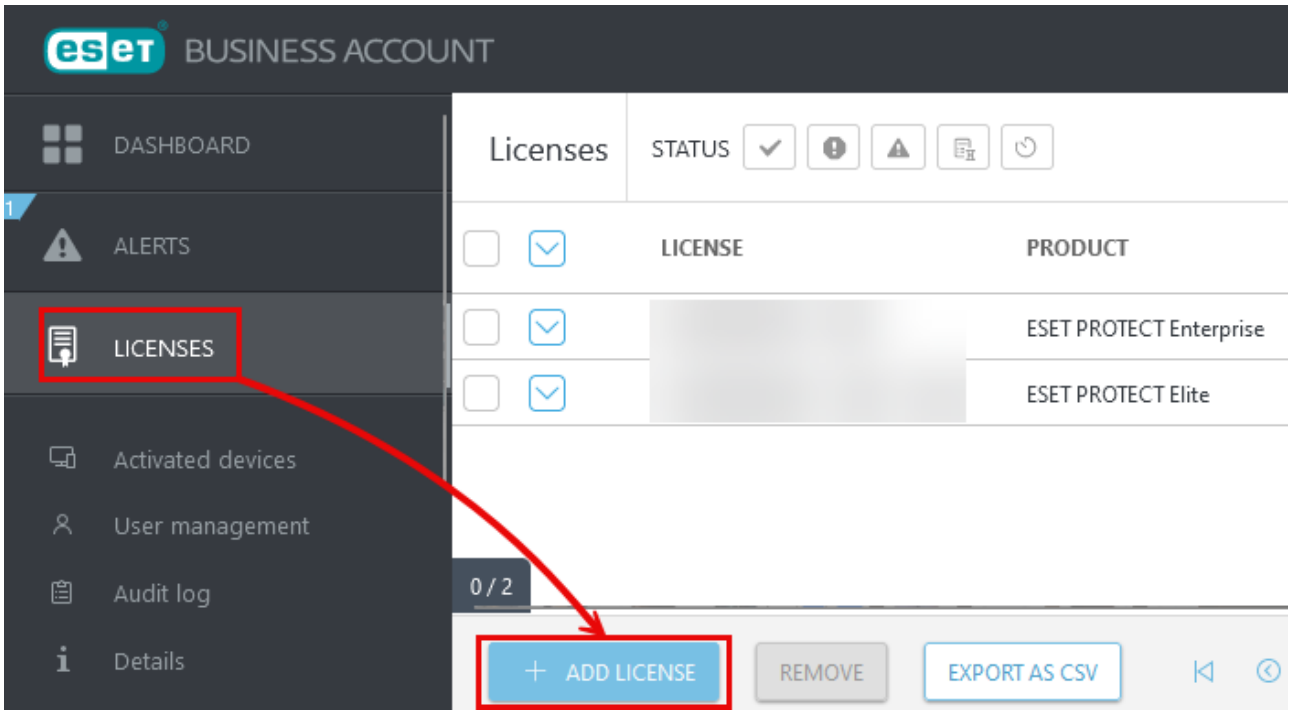
Požadavky

- Uživatelský účet vytvořený účet na portále EBA
- Licenci k ESET LiveGuard Advanced

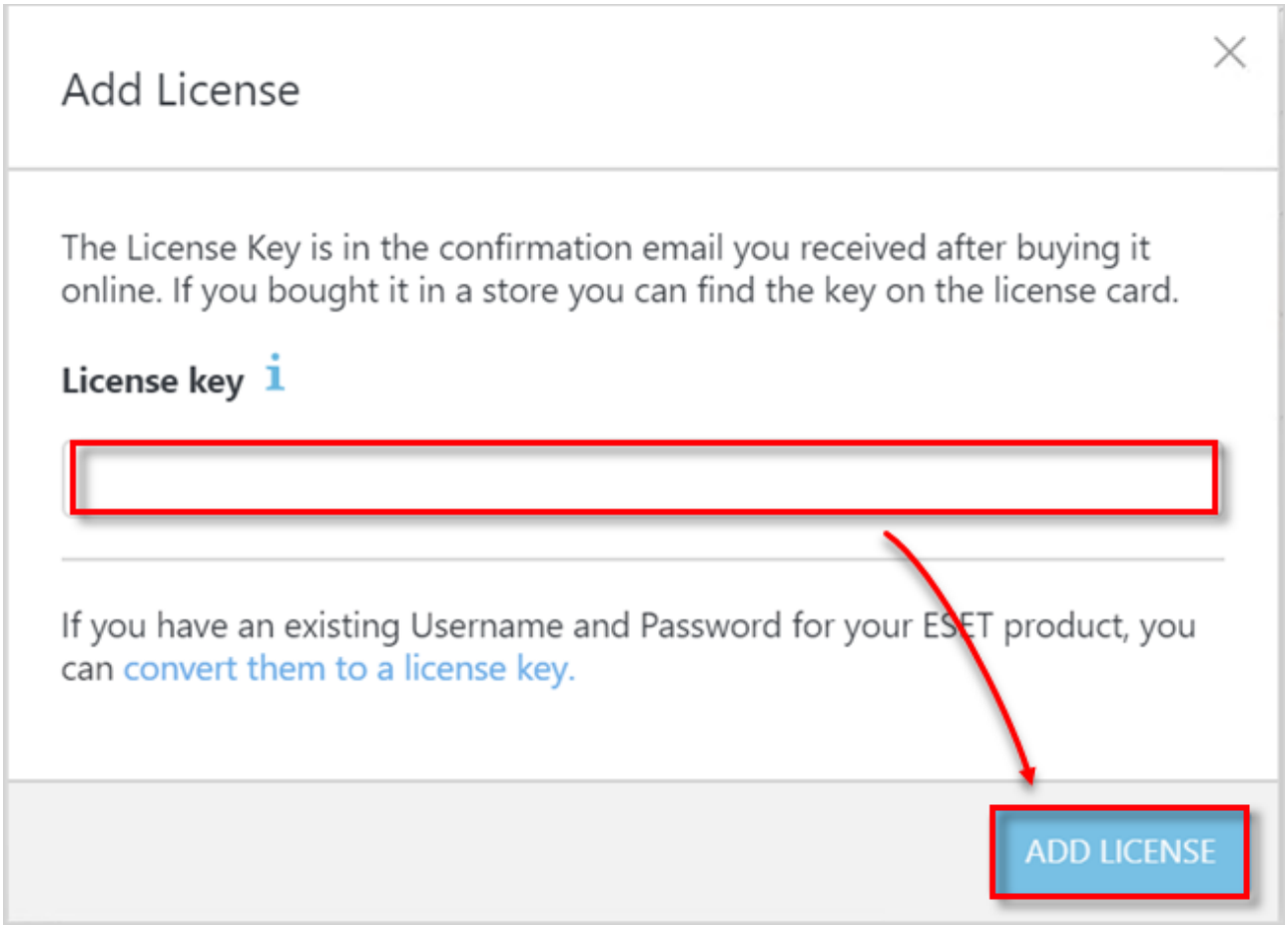
Importovat…

1.Přihlaste se ke svému účtu na portále EBA.

2.V hlavním menu přejděte na záložku **Licence** a klikněte na tlačítko **Přidat licenci** > **Zadejte licenční klíč**.



3.Vložte licenční klíč pro ESET LiveGuard Advanced a dále klikněte na tlačítko **Přidat licenci**.



4.V dalším kroku odsouhlaste licenční ujednání s koncovým uživatelem (EULA). Po úspěšném importování licence se zobrazí v seznamu licencí.

ESET LiveGuard Advanced licence může být dodávána jako bundle, případně samostatně pro jednotlivé produkty:

- ESET LiveGuard Advanced pro ESET Endpoint Security
- ESET LiveGuard Advanced pro ESET Server Security
- ESET LiveGuard Advanced pro ESET Mail Security

Synchronizace EBA s ESET PROTECT On-Prem

Požadavky

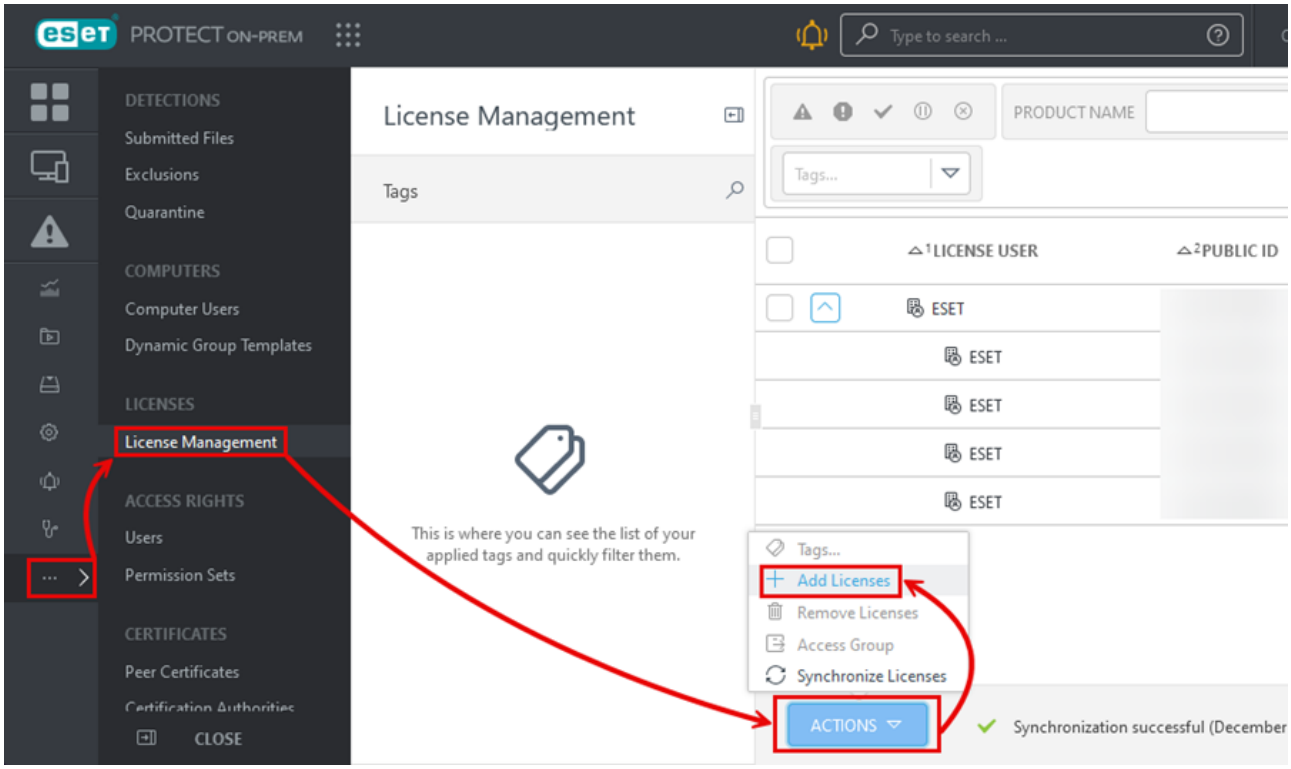
- Přidanou licenci k ESET LiveGuard Advanced v EBA
- Nasazený ESET PROTECT On-Prem
- Funkční spojení mezi ESET PROTECT serverem a portálem EBA

Pokud jste již importovali svůj účet EBA do webové konzole ESET PROTECT, klikněte v sekci **Správa licence** na tlačítko **Synchronizovat**. Tím vynutíte aktualizaci informací o licenci ve webové konzoli. V tomto případě není nutné znovu zadávat přihlašovací údaje do EBA.

Synchronizace

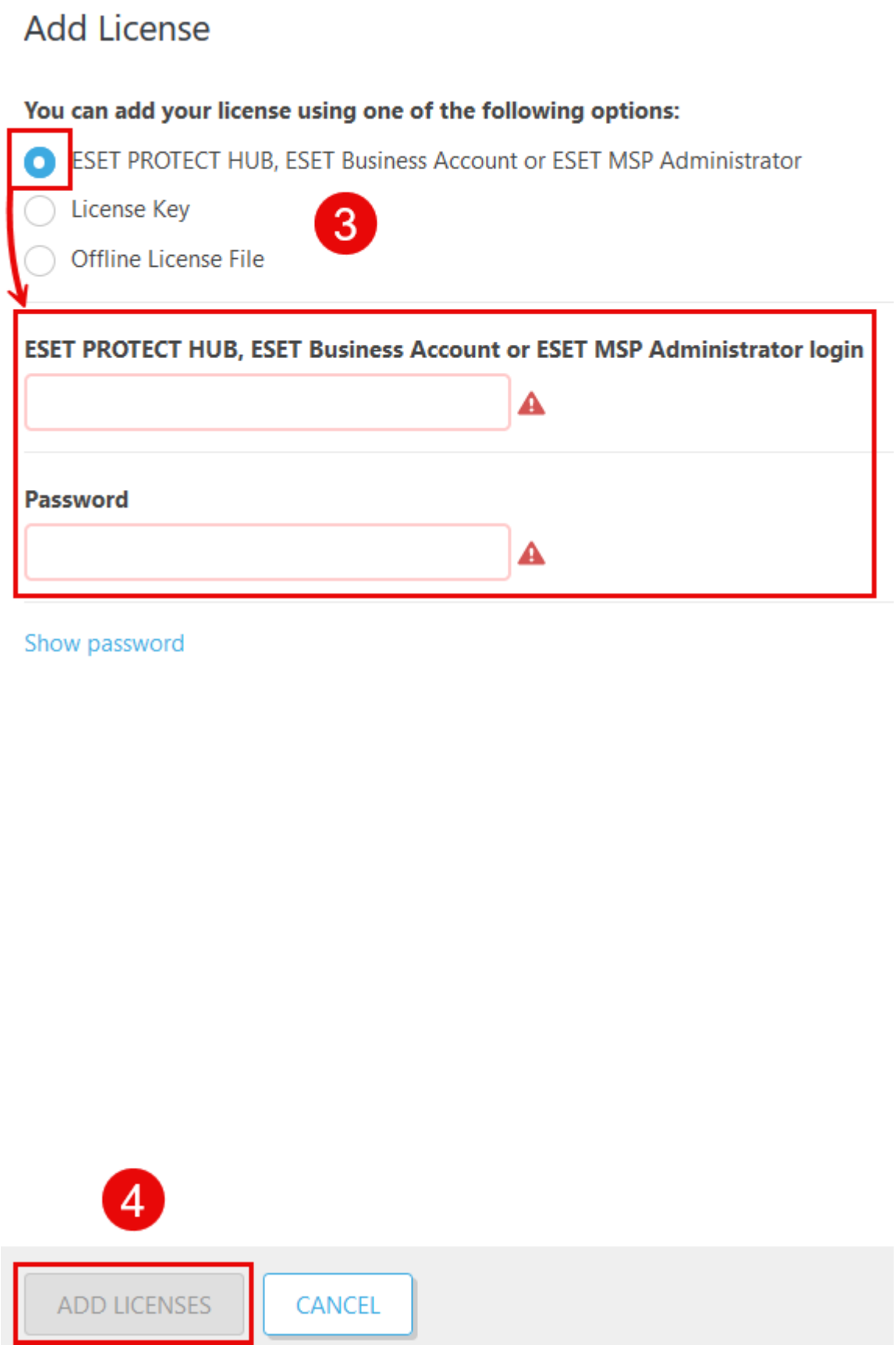
1.Přihlaste se do webové konzole ESET PROTECT jako administrátor nebo jiný uživatel s dostatečným oprávněním.

2.Přejděte do sekce **Další** > **Správa licence**, klikněte na tlačítko **Akce** a vyberte možnost **Přidat licenci**.



3.Vyberte možnost přihlášení pomocí **ESET Business Account nebo ESET MSP Administrator** a zadejte přihlašovací údaje ke svému účtu vytvořeném na portále EBA.

4.Klikněte na tlačítko **Přidat licence**. Následně se do ESET PROTECT On-Prem přidají všechny licence, které máte v účtu nahrány.



Pokud budete přidávat licenční klíč ESET LiveGuard Advanced přímo do webové konzole, může se vám zobrazit chybové hlášení:
"Nepodařilo se přidat licenci prostřednictvím licenčního klíče: Licence je určena pro produkt, který není možné spravovat prostřednictvím ESET PROTECT On-Prem. Prosím, vložte jinou licenci."
ESET LiveGuard Advanced licenci importujte vždy prostřednictvím účtu vytvořeného na portále EBA nebo ESET MSP Administrator.

Přidání licence do ESET MSP Administrator

V ESET MSP Administrator je možné vygenerovat ESET LiveGuard Advanced licence pro níže uvedené typy produktů:

- ESET LiveGuard Advanced pro Endpoint Security a Server Security
- ESET LiveGuard Advanced pro Mail Security

K dispozici jsou rovněž úrovně licencí ESET PROTECT, které obsahují ESET LiveGuard Advanced:

- ESET PROTECT Complete
- ESET PROTECT Mail Plus
- ESET PROTECT Advanced

Ověření dostupnosti ESET LiveGuard Advanced

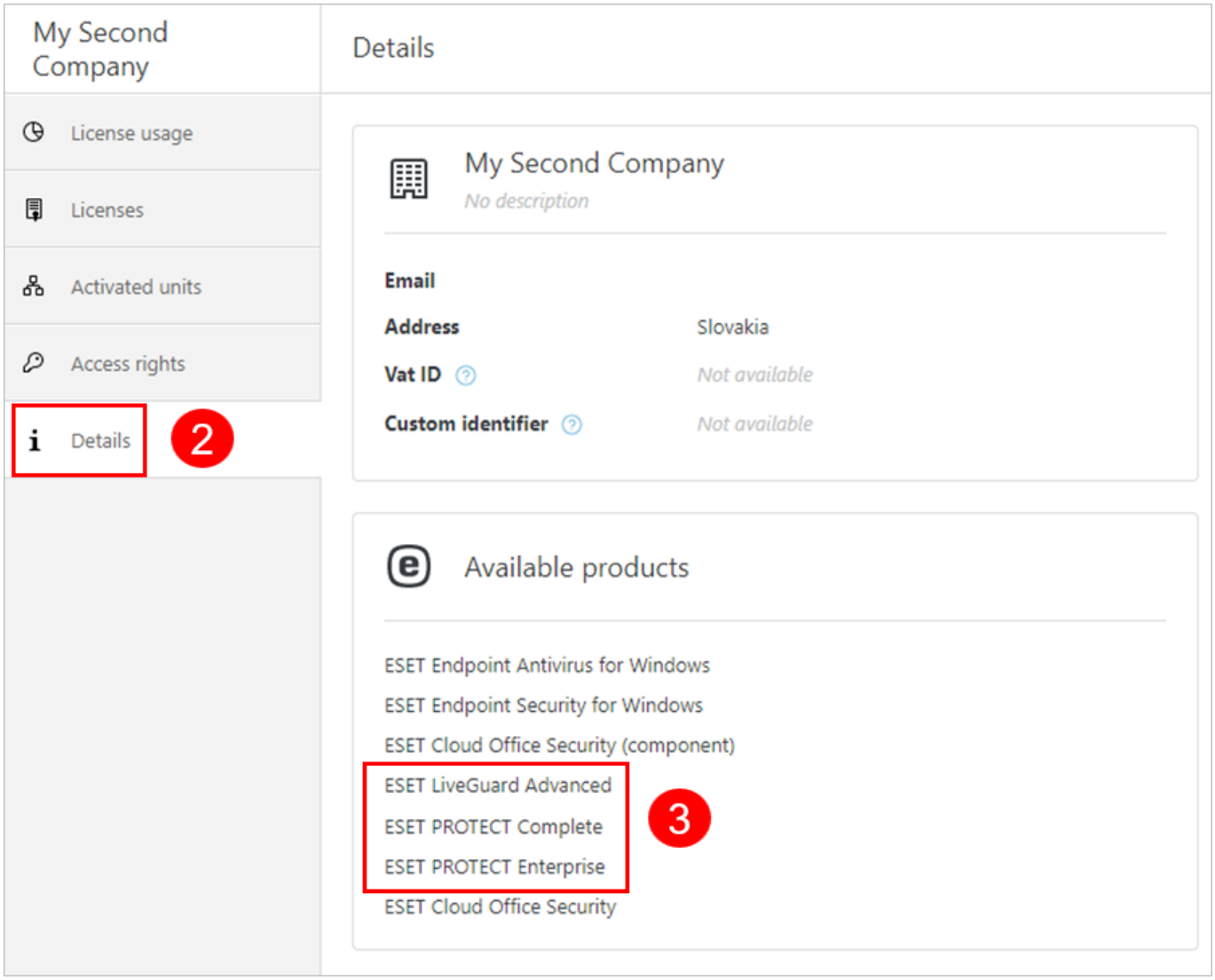
1.Přihlaste se ke svému účtu na portále ESET MSP Administrator.

2.V hlavním menu přejděte do sekce **Společnosti**, vyberte MSP zákazníka a klikněte na **Detaily**.

3.V sekci **Dostupné produkty** najděte **ESET LiveGuard Advanced** nebo úroveň zahrnující ESET LiveGuard Advanced.

Odsouhlaste podmínky použití

Před přidáním licence je nutné na ESET MSP Administrator portále odsouhlasit Podmínky použití (pro službu ESET LiveGuard Advanced). Pokud tuto možnost nemáte dostupnou, Podmínky použití musí odsouhlasit nadřazená společnost, MSP manažer nebo uživatel s přístupovým oprávněním pro **Zápis** ke společnosti.



Pokud váš zákazník nemá k dispozici vhodnou úroveň ze seznamu **Dostupných produktů**, přidejte jej do svého účtu prostřednictvím účtu Distributora (nebo MSP Manažera).

Přidání ESET LiveGuard Advanced licence

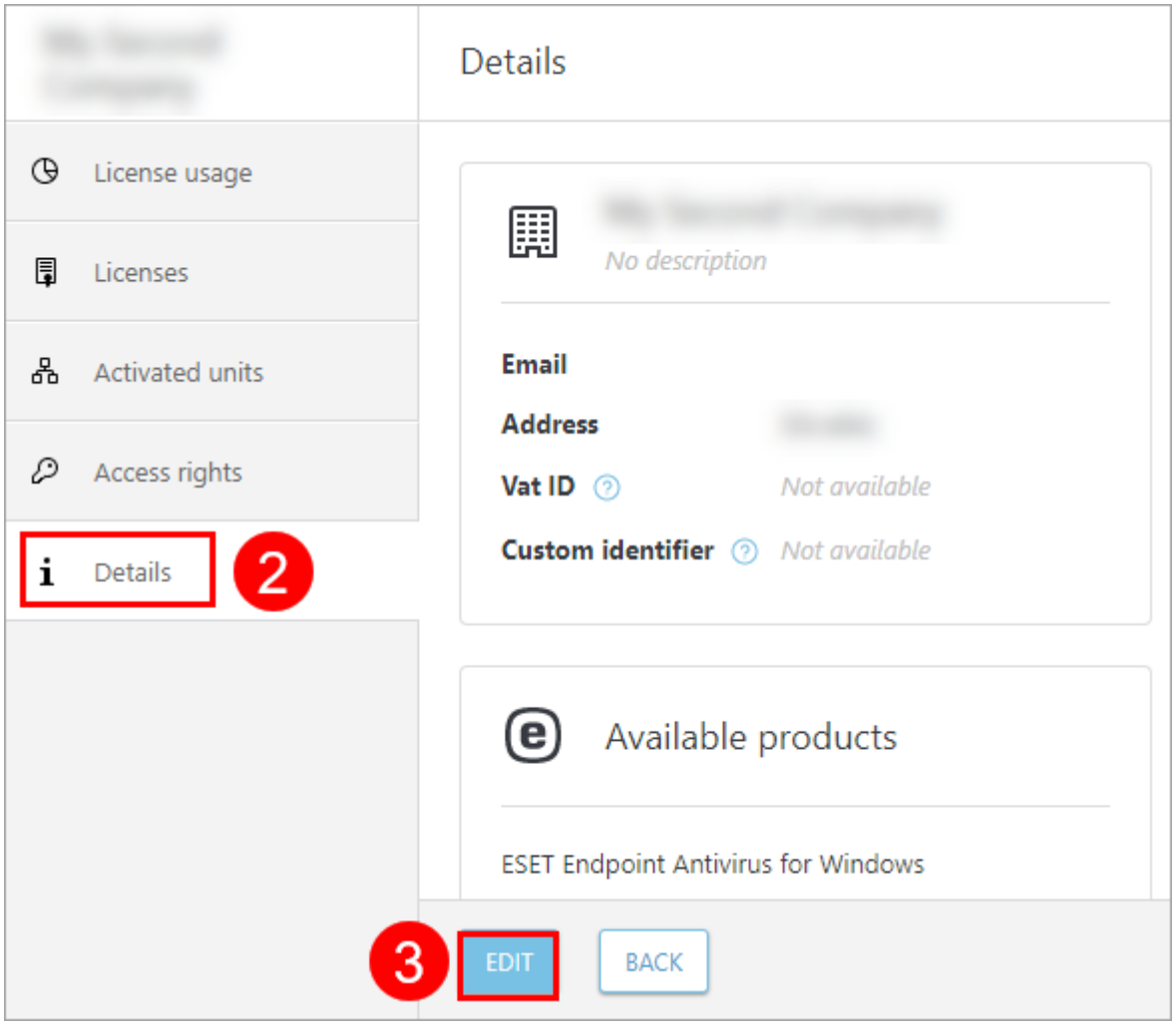
Pokud nemáte v **Detailech** zákazníka k dispozici produkt ESET LiveGuard Advanced, požádejte svého Distributora nebo MSP Manažera o přidání produktu do vašeho ESET MSP Administrator účtu.

Pomocí níže uvedených kroků přidáte prostřednictvím účtu Distributora produkt do seznamu **Dostupných produktů**:

1. Přihlaste se ke svému účtu na portále ESET MSP Administrator.

2. V hlavním menu přejděte do sekce **Společnosti**, vyberte MSP zákazníka a klikněte na **Detaily**.

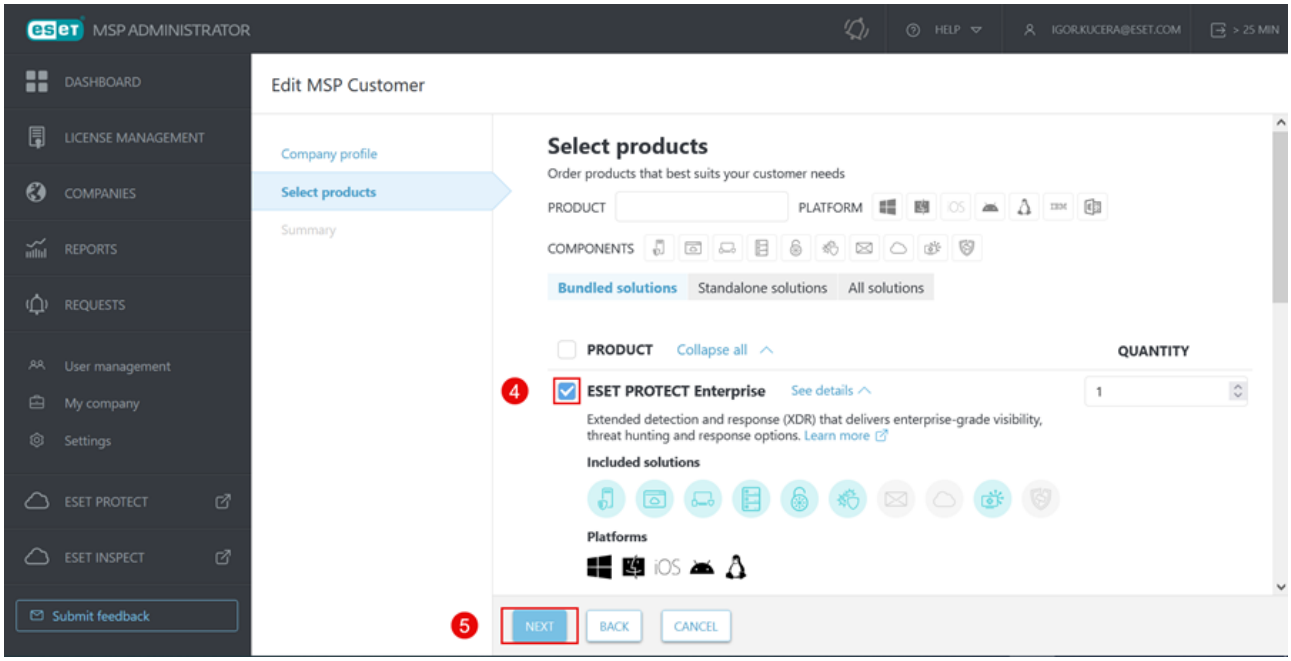
3. Klikněte na tlačítko **Změnit**.



4.Klikněte na tlačítko **Další** a na obrazovce Vybrat produkty vyberte možnost ESET LiveGuard Advanced nebo jinou vhodnou licenci.

5.Klikněte na tlačítko **Další**.

6.Zkontrolujte, zda změny odpovídají vašim představám a klikněte na tlačítko **Dokončit**.



Přidání ESET LiveGuard Advanced licence vašemu MSP zákazníkovi

Pokud má zákazník dostupnou ESET LiveGuard Advanced licenci, můžete mu ji přiřadit.

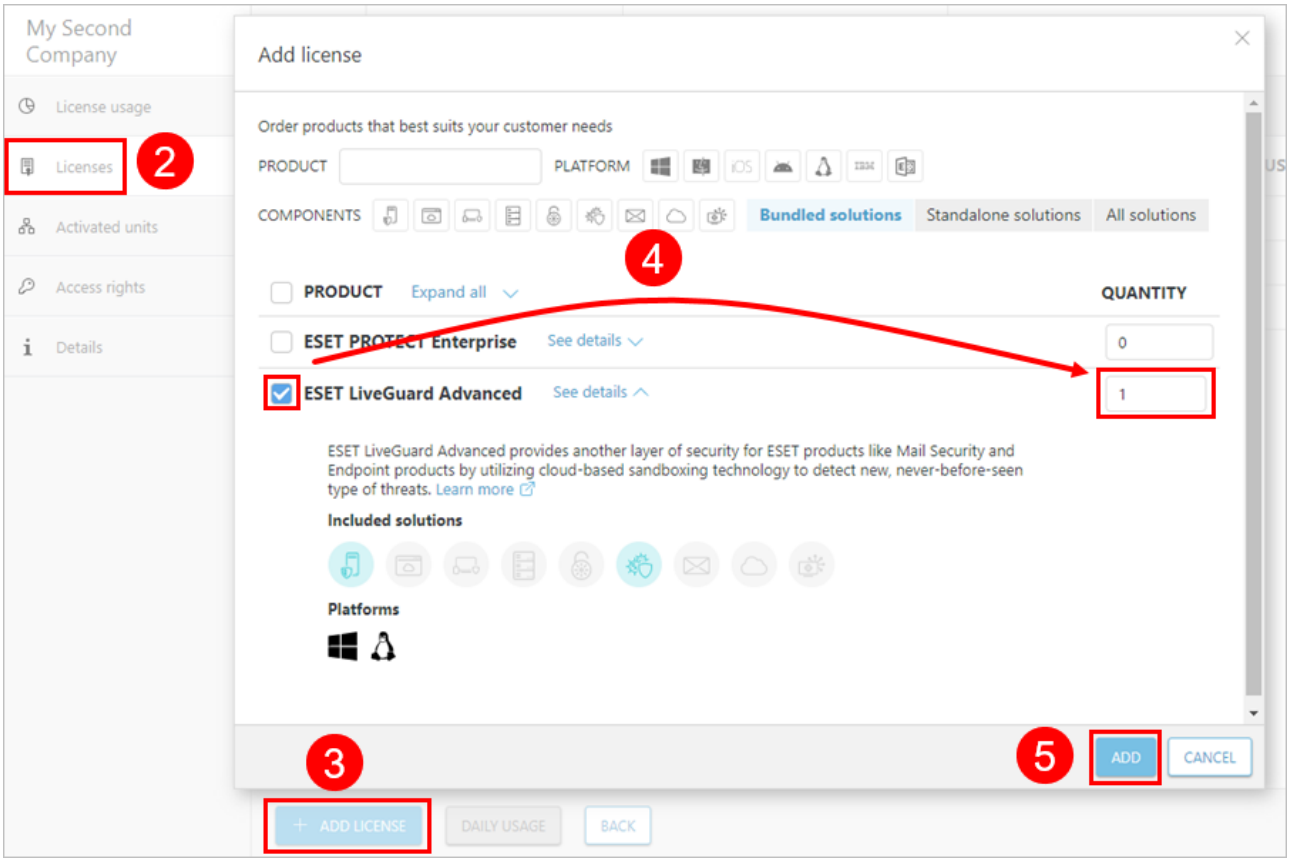
1.Přihlaste se ke svému účtu na portále ESET MSP Administrator.

2.V hlavním menu přejděte do sekce **Společnosti**, vyberte MSP zákazníka a klikněte na **Detaily**.

3.Klikněte na tlačítko **Přidat licence** (případně **Vyžádat licenci**).

4.Pomocí zaškrtávacího pole vyberte **ESET LiveGuard Advanced** a zadejte **počet klientů**.

5.Přidání výjimky potvrďte kliknutím na tlačítko **Přidat**.



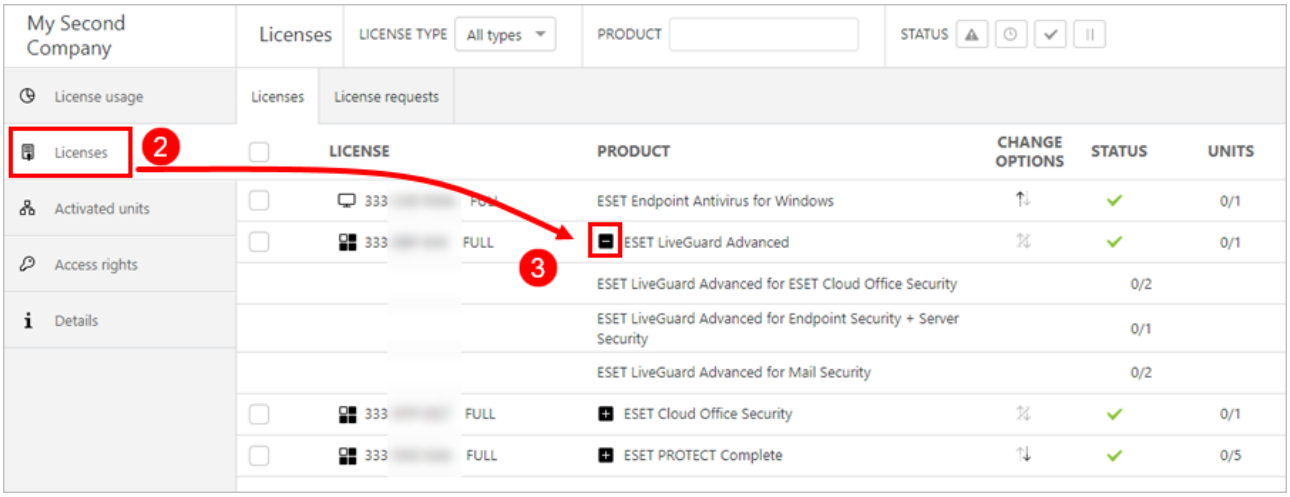
Zobrazení informací o ESET LiveGuard Advanced licence

Jedná se o samotnou licenci k úrovni ESET LiveGuard Advanced. Detaily si můžete kdykoli zobrazit ve svém účtu na portále ESET MSP Administrator.

1.Přihlaste se ke svému účtu na portále ESET MSP Administrator.

2.V hlavním menu přejděte do sekce **Společnosti**, vyberte MSP zákazníka a klikněte na **Detaily**.

3.Pro rozbalení licence klikněte na řádku s ESET LiveGuard Advanced licencí na ikonu ⊞.



Po přidání licence ESET LiveGuard Advanced ji synchronizujte v ESET PROTECT On-Prem.

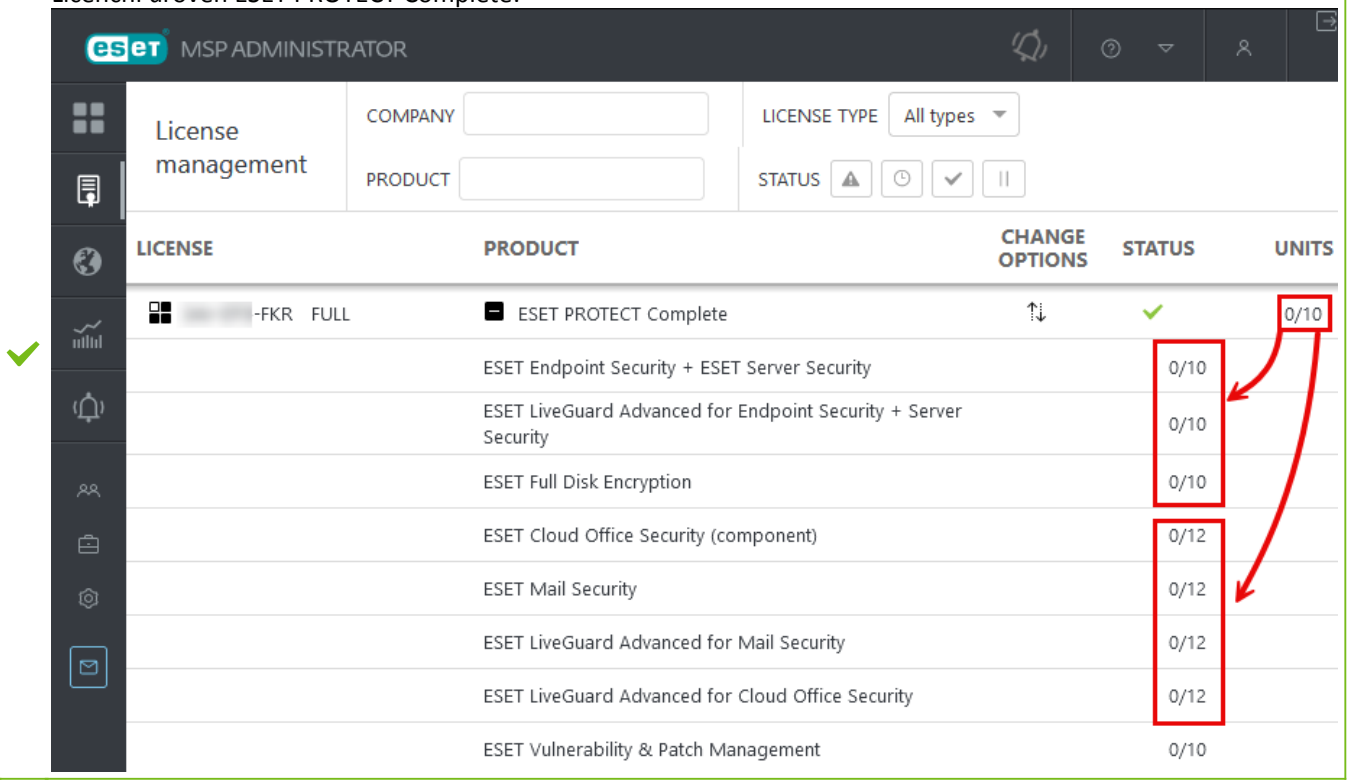
Počet klientů a rozsah

Počet jednotek je počet objednaných uhrazených jednotek licence (úrovně). Každá úroveň licence může mít pro každý zahrnutý produkt jiný poměr jednotek vůči podjednotkám.

LICENSE	PRODUCT	CHANGE OPTIONS	STATUS	UNITS
[redacted] FULL	ESET Endpoint Antivirus for Windows		✓	0/1
[redacted] FULL	ESET LiveGuard Advanced **Tier unit**		✓	0/1
	ESET LiveGuard Advanced for ESET Cloud Office Security **Subunit**			0/2
	ESET LiveGuard Advanced for Endpoint Security + Server Security **Subunit**			0/1
	ESET LiveGuard Advanced for Mail Security **Subunit**			0/2

Příklad rozdělení rozsahu jednotek

Licenční úroveň ESET PROTECT Complete:



Synchronizace ESET MSP Administrator s ESET PROTECT On-Prem

Požadavky

- Licenční klíč pro ESET LiveGuard Advanced importovaný ve vašem účtu na portále ESET MSP Administrator
- Nasazený ESET PROTECT On-Prem

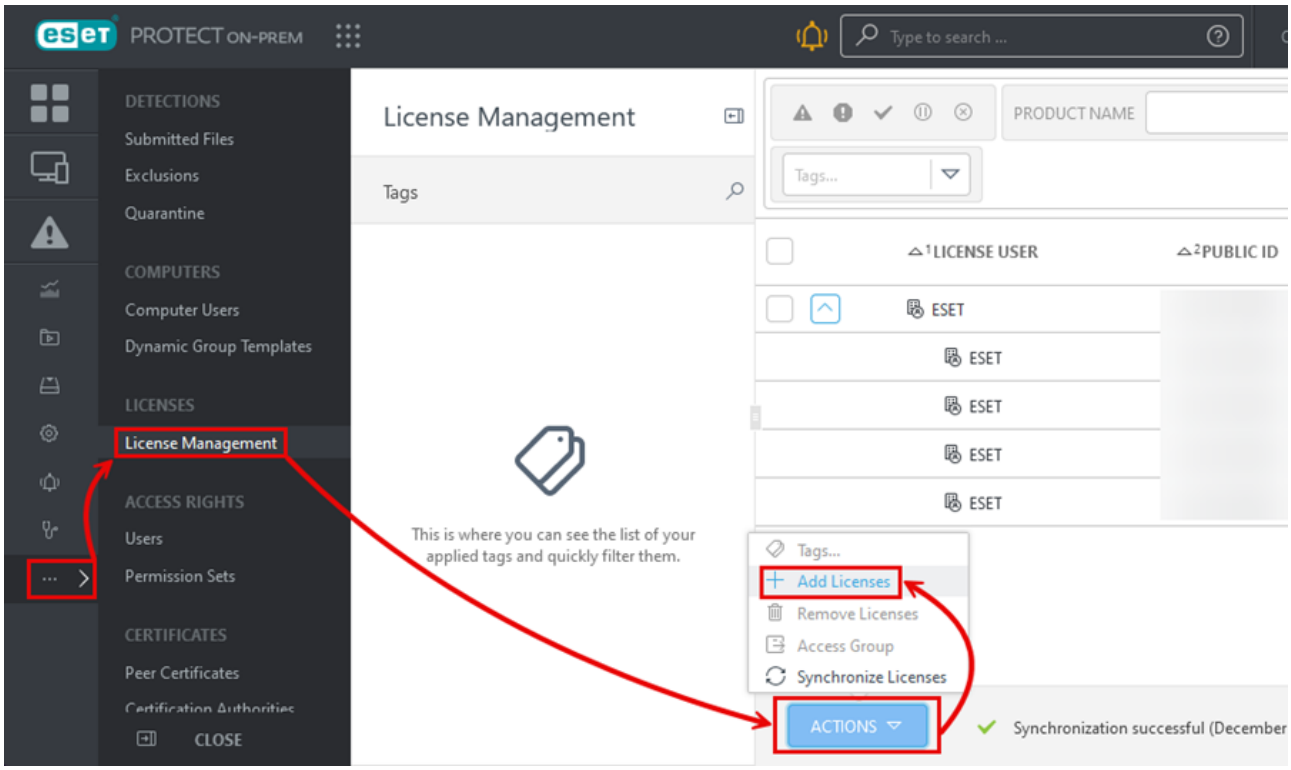
- Musí fungovat spojení mezi ESET PROTECT serverem a portálem ESET MSP Administrator

> Pokud jste již importovali svůj účet EBA do webové konzole ESET PROTECT, klikněte v sekci **Správa licence** na tlačítko **Synchronizovat**. Tím vynutíte aktualizaci informací o licenci ve webové konzoli. V tomto případě není nutné znovu zadávat přihlašovací údaje do ESET MSP Administrator.

Synchronizace

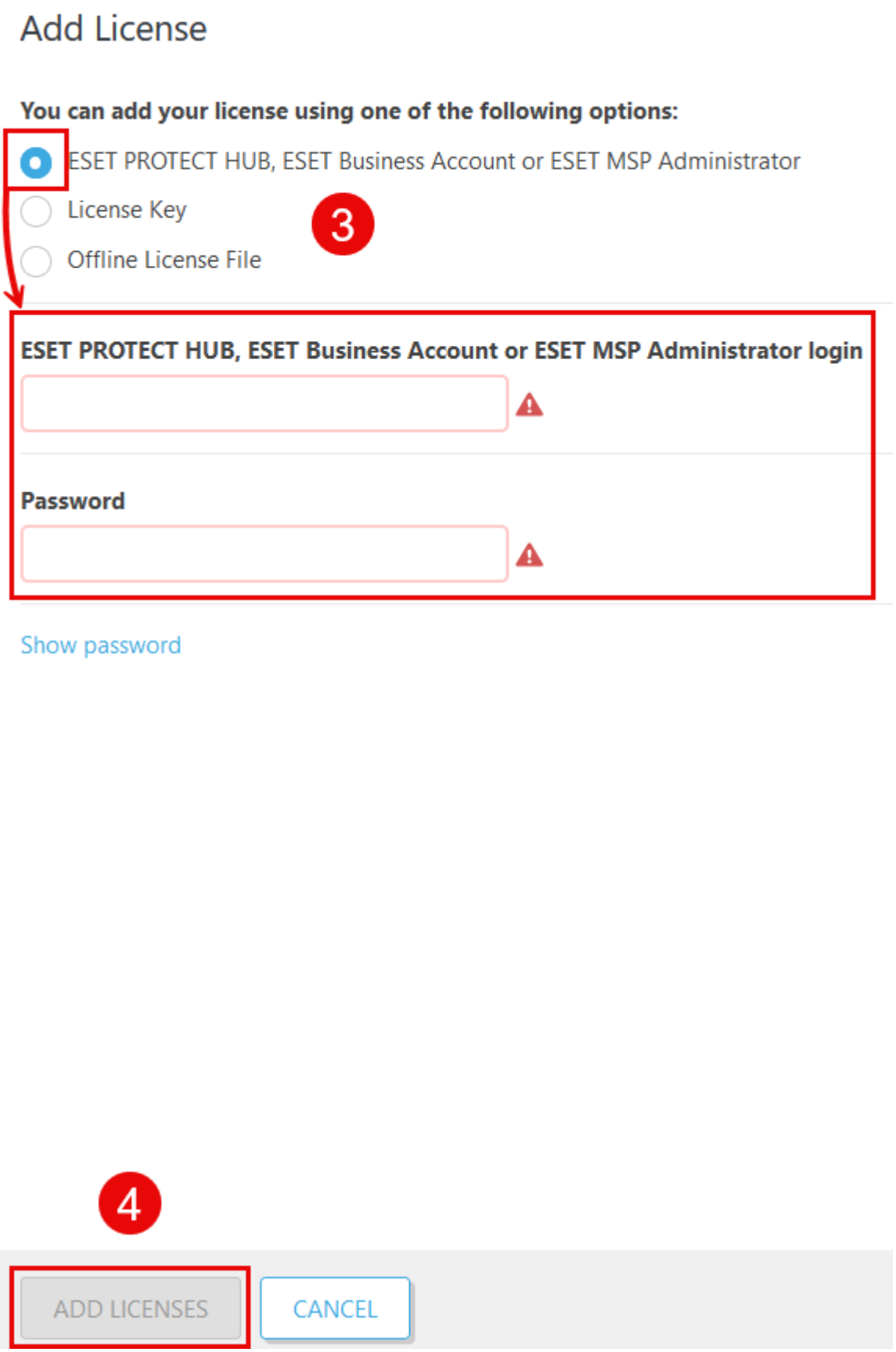
1.Přihlaste se do webové konzole ESET PROTECT jako administrátor nebo jiný uživatel s dostatečným oprávněním.

2.Přejděte do sekce **Další** > **Správa licence**, klikněte na tlačítko **Akce** a vyberte možnost **Přidat licenci**.



3.Vyberte možnost přihlášení pomocí **ESET Business Account nebo ESET MSP Administrator** a zadejte přihlašovací údaje ke svému účtu vytvořeném na portále ESET MSP Administrator.

4.Klikněte na tlačítko **Přidat licence**. Následně se do ESET PROTECT On-Prem přidají všechny licence, které máte v účtu nahrány.



Pokud budete přidávat licenční klíč ESET LiveGuard Advanced přímo do webové konzole, může se vám zobrazit chybové hlášení:
"Nepodařilo se přidat licenci prostřednictvím licenčního klíče: Licence je určena pro produkt, který není možné spravovat prostřednictvím ESET PROTECT On-Prem. Prosím, vložte jinou licenci."
ESET LiveGuard Advanced licenci importujte vždy prostřednictvím účtu vytvořeného na portále EBA nebo ESET MSP Administrator.

Hromadná aktivace počítačů

Pokud potřebujete službu aktivovat pouze na vybraných počítačích, využijte k tomu v ESET PROTECT On-Prem nebo ESET PROTECT zjednodušeného průvodce.

Požadavky pro uživatele ESET PROTECT On-Prem

- Licence pro ESET LiveGuard Advanced přidaná v ESET PROTECT On-Prem
- Klientské stanice s verzí ESET Management Agenta, která není starší než verze serverové komponenty
- Aktivovaný bezpečnostní produkt ESET, který podporuje ESET LiveGuard Advanced

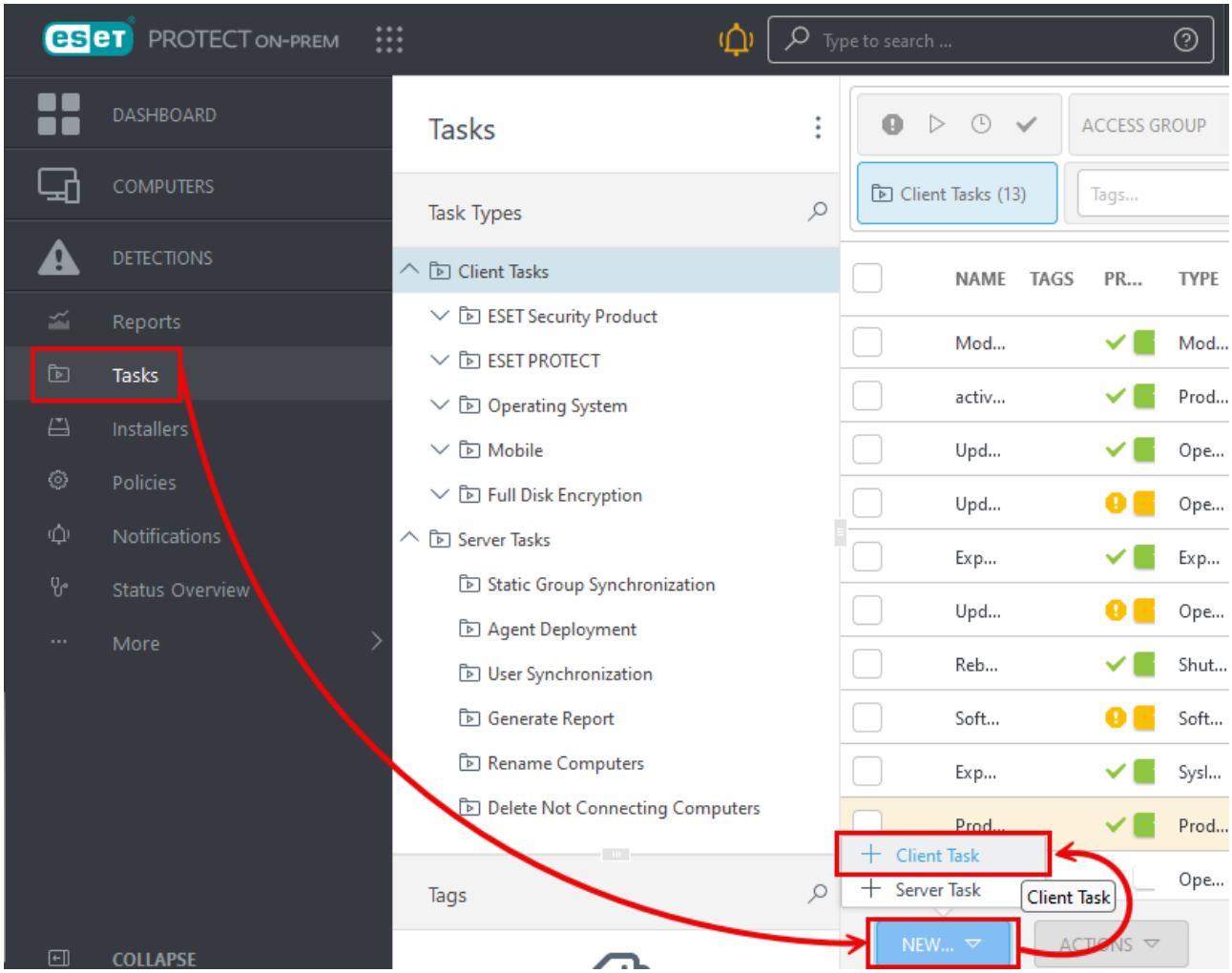
Požadavky pro uživatele ESET PROTECT

- Licence k ESET LiveGuard Advanced přidaná v EBA.
- Na všech klientských stanicích je nainstalovaný ESET Management Agent v nejnovější verzi.
- Na klientské stanici musí být nainstalovaný a aktivovaný bezpečnostní produkt ESET, který podporuje ESET LiveGuard Advanced).

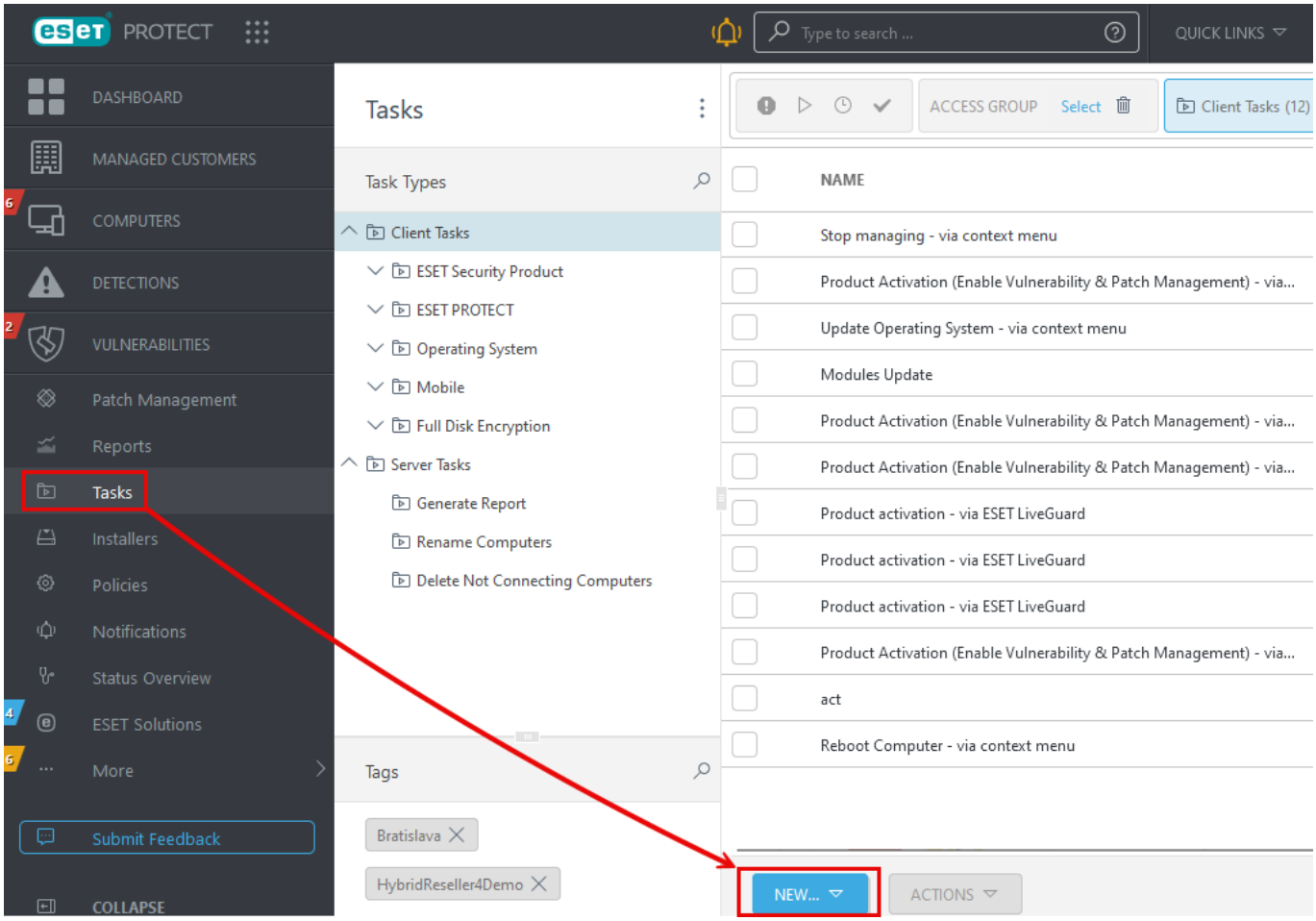
Úloha pro aktivaci

1. Přihlaste se do webové konzole.

2. V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová** a vyberte možnost **Klientská úloha**.

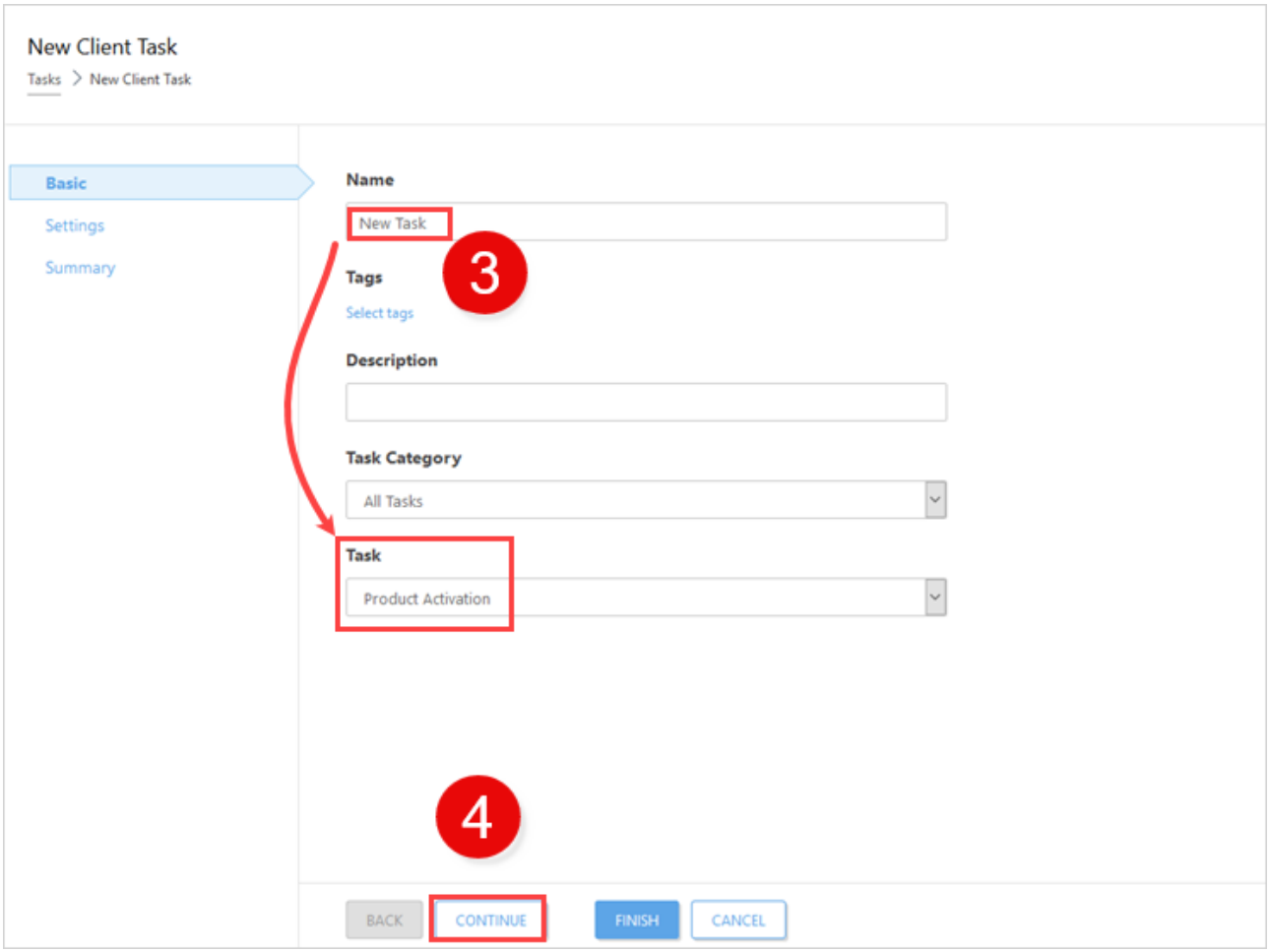


[Používám ESET PROTECT]



3.Zadejte název nově vytvářené úlohy a jako **typ úlohy** vyberte **Aktivace produktu**.

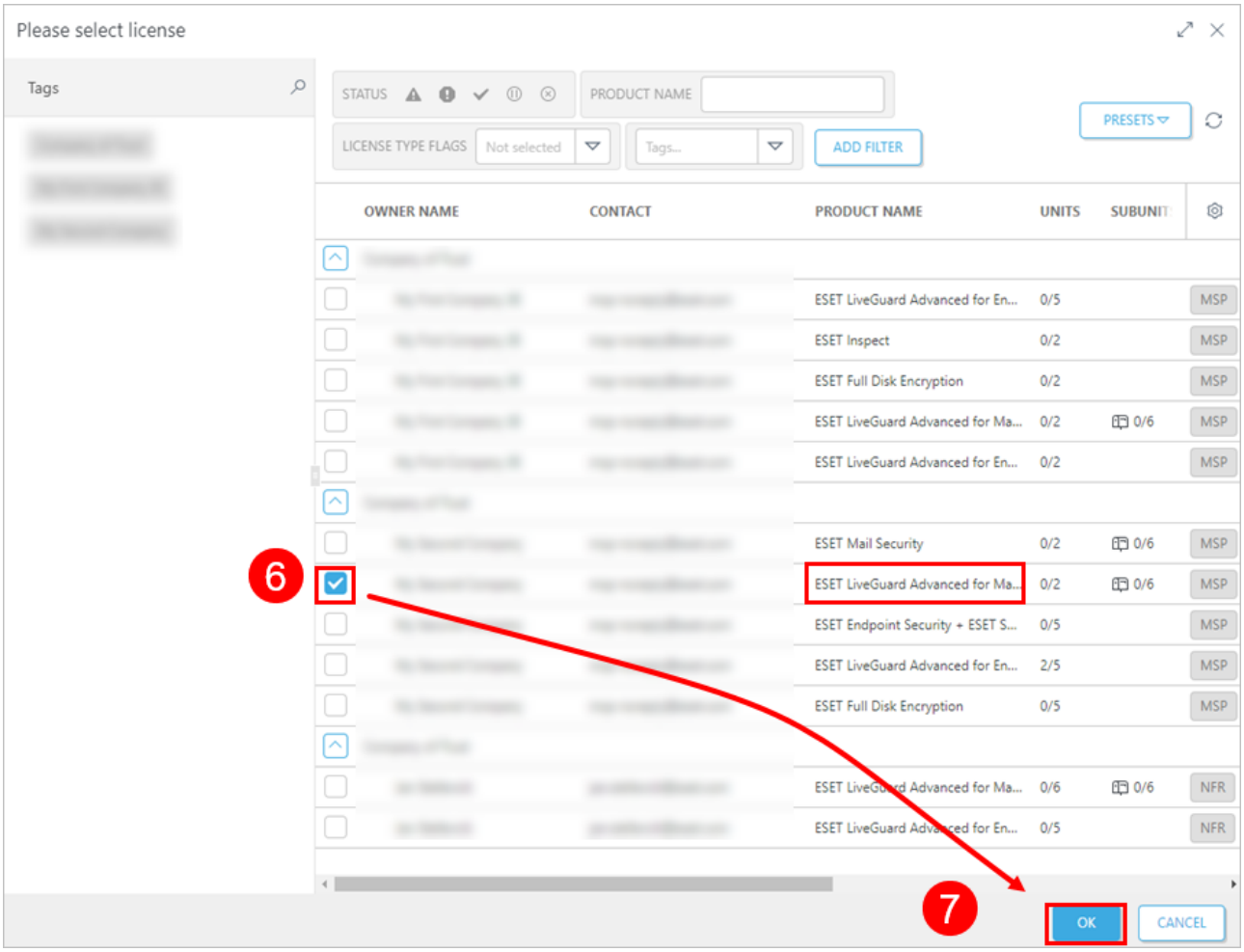
4.Klikněte na tlačítko **Pokračovat**.



5.V zobrazeném dialogovém okně najděte licenci pro ESET LiveGuard Advanced.

6.Licence pro ESET LiveGuard Advanced je součástí úrovně. Rozbalte úroveň a vyberte odpovídající produkt.

7.Dále klikněte na tlačítko **OK**.



8.V sekci **Přehled** si zkontrolujte parametry úlohy.

9.Pokud je vše v pořádku, úlohu vytvořte kliknutím na tlačítko **Dokončit**.

10. Po vytvoření úlohy je potřeba naplánovat její spuštění. Klikněte na tlačítko **Vytvořit podmínku spuštění**.

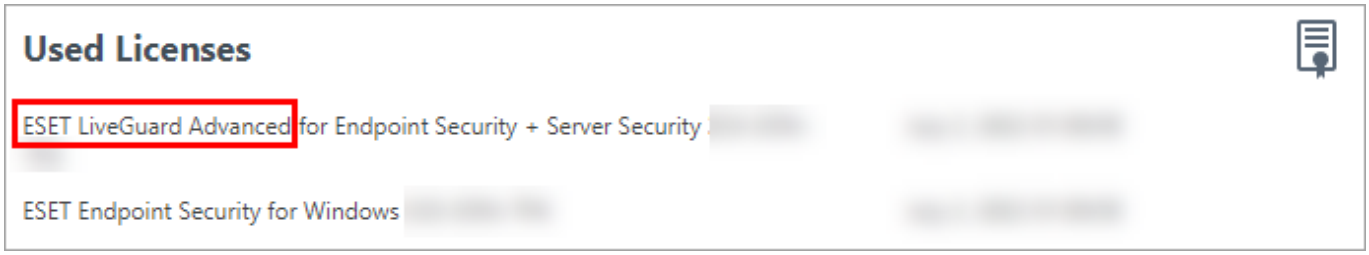
11. Zadejte **popis podmínky spuštění** a klikněte na tlačítko **Pokračovat**.

12. Klikněte na tlačítko **Přidat počítače** nebo **Přidat skupiny** a vyberte zařízení, na kterých chcete úlohu spustit. Ujistěte se, že jste vybrali produkty kompatibilní s danou licencí definovanou v kroku 6. Dále klikněte na tlačítko **OK** a **Pokračovat**.

13. V dalším kroku vyberte **typ podmínky spuštění**. Doporučujeme ponechat výchozí možnost: **Jakmile je to možné**, která zajistí okamžité spuštění úlohy (po připojení agenta k serveru). Při vybrání ostatních možností získáte přístup do sekce **Rozšířená nastavení**.

14. Naplánování spuštění úlohy provedete kliknutím na tlačítko **Dokončit**.

Úspěšnou aktivaci můžete ověřit v detailech zařízení. Ve webové konzoli klikněte na **Počítače**, vyberte zařízení a klikněte na **Zobrazit detaily > Detaily > Produkty a licence**.



Aktivace jednotlivých počítačů

Požadavky pro uživatele ESET PROTECT On-Prem a ESET PROTECT

- V ESET PROTECT On-Prem je přidána licence pro ESET LiveGuard Advanced nebo úroveň ochrany zahrnující tuto službu
- Klientské stanice s verzí ESET Management Agenta kompatibilní s verzí serverové komponenty
- Aktivovaný bezpečnostní produkt ESET, který podporuje ESET LiveGuard Advanced

Požadavky pro uživatele ESET PROTECT

- V EBA je přidána licence pro ESET LiveGuard Advanced nebo úroveň ochrany zahrnující tuto službu.
- Na všech klientských stanicích je nainstalovaný ESET Management Agent v nejnovější verzi.
- Na klientských stanicích je nainstalovaný a aktivovaný bezpečnostní produkt ESET, který podporuje ESET LiveGuard Advanced).

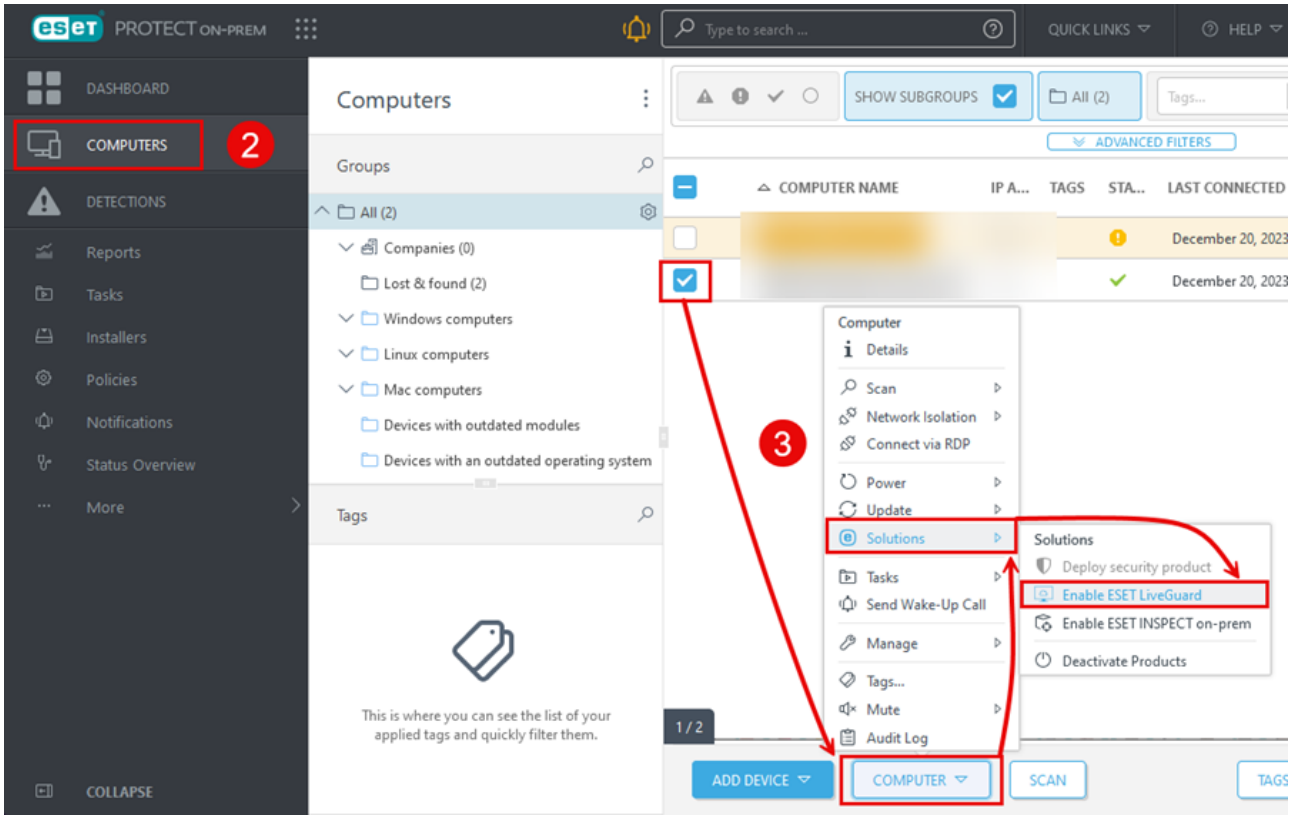
- Nikdy neimportujte licenci pro ESET LiveGuard Advanced do konzole pro vzdálenou správu prostřednictvím licenčního klíče. Pokud jste tak učinili, licenci odeberte a znovu ji přidejte prostřednictvím účtu vytvořeného na portále EBA nebo ESET MSP Administrator.
- Vždy se před použitím licence k ESET LiveGuard Advanced ujistěte, že má cílová stanice podporované bezpečnostní řešení.

Aktivace a spuštění ESET LiveGuard Advanced prostřednictvím ESET PROTECT On-Prem nebo ESET PROTECT

ESET PROTECT On-Prem a ESET PROTECT nabízí průvodce aktivací této služby.

1. Přihlaste se do webové konzole.
2. V hlavním menu webové konzole přejděte na záložku **Počítače**.

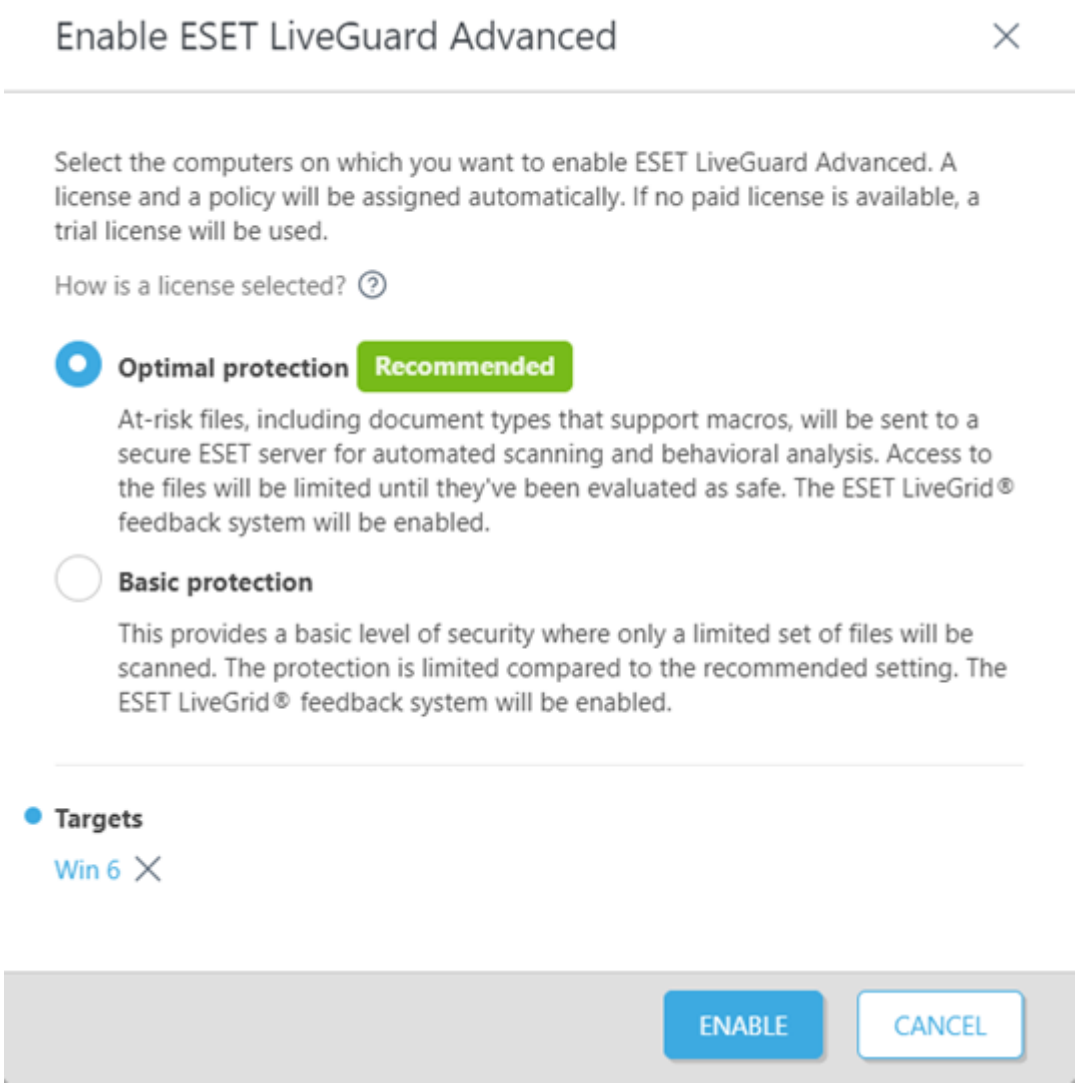
3.V seznamu počítačů vyberte ty, na kterých chcete tuto službu spustit, klikněte na Akce > Zapnout ESET LiveGuard.



4.Vyberte si mezi **Optimální ochranou** a **Základní ochranou**.

5.Ověřte si, že se zařízení, na kterém budete aktivovat ESET LiveGuard Advanced nachází v Cílových stanicích.

6.Kliknutím na tlačítko **Zapnout** naplánujete spuštění úlohy.



Konzole pro správu následně na vybraný počítač zašle klientskou úlohu pro aktivaci produktu a politiku. ESET LiveGuard Advanced se zapne na klientovi v dalším intervalu replikace ESET Management Agenta, obvykle do několika minut.

Vzdálená instalace a aktivace

Při instalaci bezpečnostního produktu prostřednictvím ESET PROTECT On-Prem nebo ESET PROTECT můžete v rámci klientské úlohy zajistit, že dojde zároveň k aktivaci a zapnutí ESET LiveGuard Advanced.

1.Přihlaste se do webová konzole ESET PROTECT.

2.V hlavním menu přejděte na záložku **Úlohy**, klikněte na tlačítko **Nová a vyberte možnost Klientská úloha**.

3.Zadejte název úlohy, volitelně popis, a z rozbalovacího menu **Úloha** vyberte možnost **Instalace aplikace**.

4.Klikněte na tlačítko **Pokračovat**.

5.Klikněte na možnost <Vyberte balíček> a vyberte si požadovaný bezpečnostní produkt ESET.

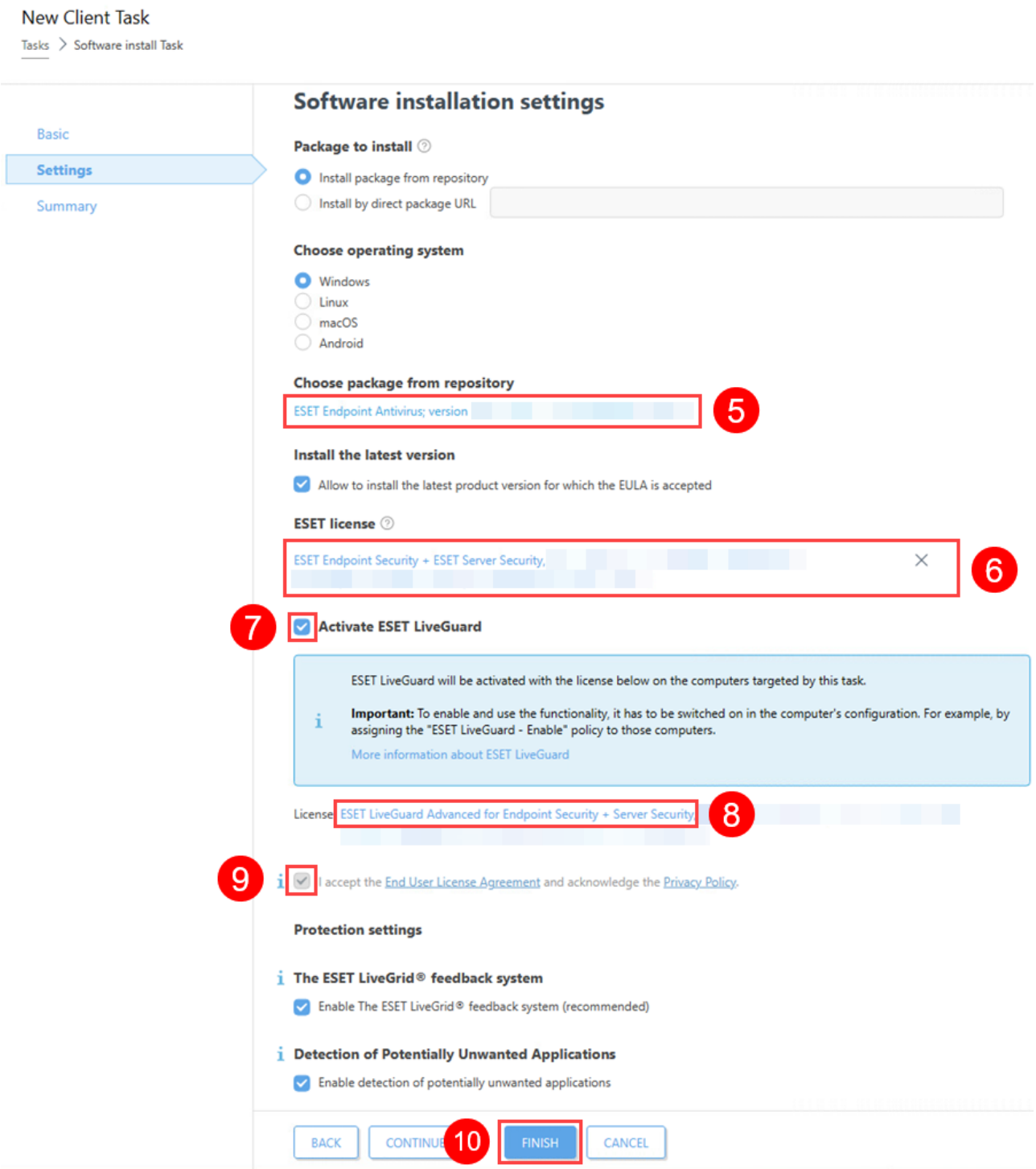
6.Dále vyberte licenci, kterou chcete použít pro aktivaci produktu.

7.Zaškrtněte možnost **Aktivovat ESET LiveGuard**.

8.Vyberte vhodnou ESET LiveGuard Advanced licenci.

9.Zaškrtněte možnost **Přijímám** , pokud souhlasíte s Licenční ujednání s koncovým uživatelem a Zásadami ochrany osobních údajů týkajících se daného bezpečnostního produktu.

10. Klikněte na tlačítko **Dokončit**.



11. Klikněte na tlačítko **Vytvořit podmínku spuštění**.

12. Zadejte název podmínky spuštění a klikněte na tlačítko **Pokračovat**.

13. Klikněte na tlačítko **Přidat cíle** a vyberte požadované počítače nebo skupiny. Dále klikněte na tlačítko **OK**.

14. Pro naplánování spuštění úlohy klikněte na tlačítko **Dokončit**.

Jak zapnout a konfigurovat ESET LiveGuard Advanced?

Požadavky pro aktivaci

- ESET Business Account nebo ESET MSP Administrator účet přidaný do podporované konzole pro vzdálenou správu.
- Nainstalovaná nebo nasazená podporovaná konzole pro vzdálenou správu.
- Nainstalovaný kompatibilní bezpečnostní produkt ESET.
- Platná licence pro ESET LiveGuard Advanced.
- Aktivovaný bezpečnostní produkt ESET LiveGuard Advanced licencí
- ESET LiveGuard Advanced zapnutý prostřednictvím politiky v kompatibilním bezpečnostním produktu.

Jak zapnout ESET LiveGuard Advanced v bezpečnostním produktu

- ESET Endpoint Security
- Jak fungují politiky a jak vytvořím novou?

Jak zapnout ESET LiveGuard Advanced v ESET Cloud Office Security

Více informací naleznete v online příručce k ESET Cloud Office Security, případně si otevřete návod ESET Databázi znalostí.

Konfigurace bezpečnostního produktu ESET

Uživatelé ESET Cloud Office Security

Pro zapnutí služby ESET LiveGuard Advanced v ESET Cloud Office Security vytvořte novou, nebo upravte stávající, politiku. Dodatečnou ochranu získají všichni uživatelé/skupiny, na které politiku aplikujete. Více informací naleznete v online příručce v kapitole nastavení ochrany pro ESET LiveGuard Advanced.

Nastavení ESET Cloud Office Security politiky

1.Přihlaste se do ESET Cloud Office Security.

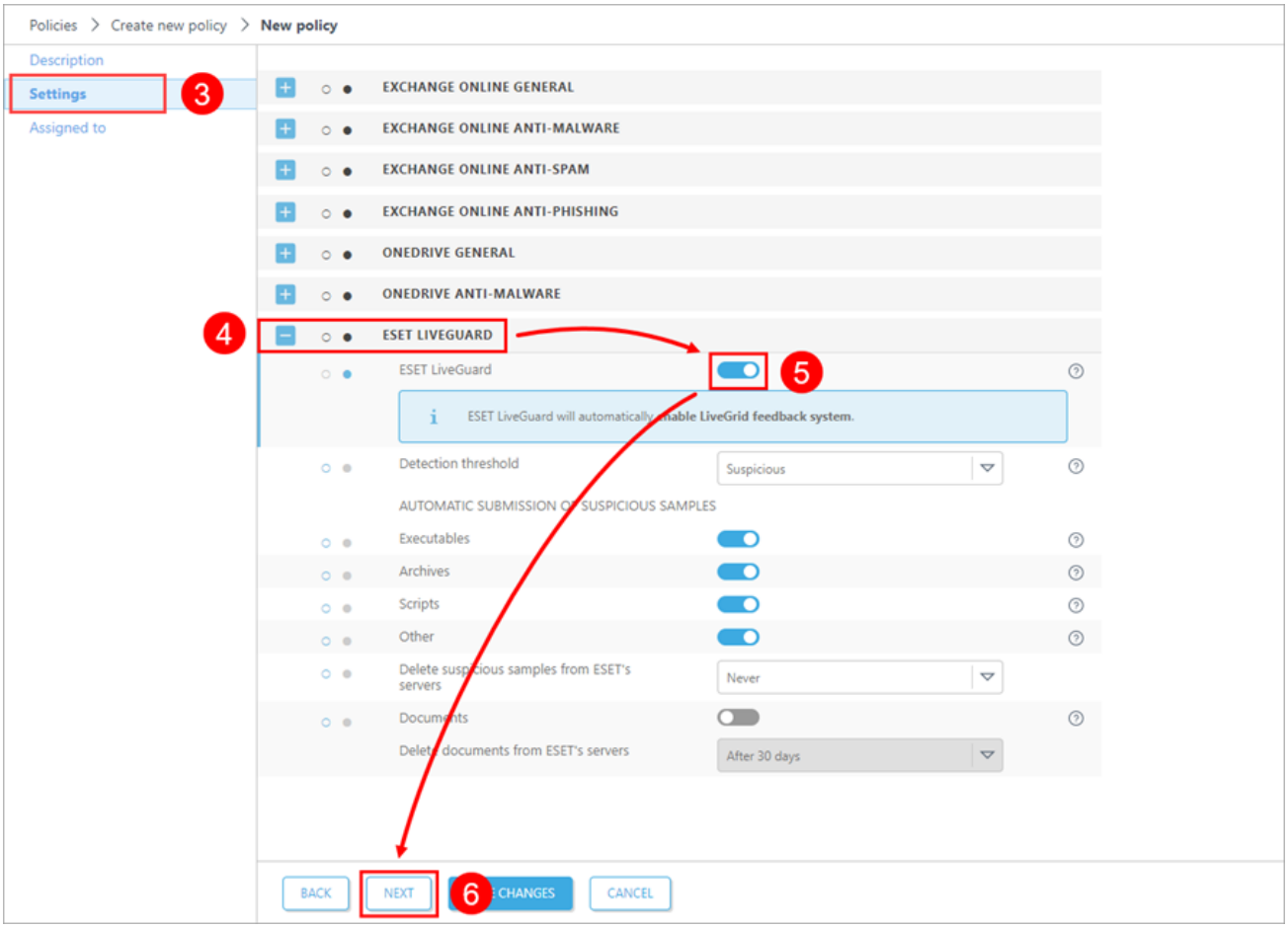
2.V hlavním menu přejděte do sekce **Politiky**, klikněte na existující politiku a vyberte možnost **Změnit**.

3.Klikněte na **Nastavení**.

4.Rozbalte část **ESET LiveGuard**.

5.Klikněte na přepínač **ESET LiveGuard**.

6.Klikněte na tlačítko **Další**.



Uživatelé ESET konzole pro vzdálenou správu

Pro zapnutí ESET LiveGuard Advanced na klientské stanici je nutné splnit všechny předpoklady a následně vytvořit politiku, ve které tuto službu nastavíte.

Ve webové konzoli ESET PROTECT vytvořte novou politiku nebo upravte stávající a přiřaďte ji zařízením, na kterých chcete používat ESET LiveGuard Advanced.

Pokud ESET LiveGuard Advanced zapnete na zařízeních, které nejsou aktivovány odpovídající licencí, dané nastavení se nepropíše. Ostatní nastavení v politice se korektně aplikují. Ostatní nastavení v politice se korektně aplikují.

Nastavení ESET LiveGuard Advanced

1.Přihlaste se do webové konzole a vytvořte novou, nebo upravte stávající, politiku.

2.V sekci **Nastavení** vyberte produkt a přejděte na:

Politiky	Nastavení
ESET Endpoint pro Windows	Detekční jádro > Cloudová ochrana
ESET Mail Security for Microsoft Exchange (V6+)	Počítač > Cloudová ochrana
ESET Server Security for Microsoft Server (V6+)	Detekční jádro > Cloudová ochrana
ESET Endpoint for Linux (V7+)	Detekční jádro > Cloudová ochrana
ESET Server/File Security for Linux (V7+)	Detekční jádro > Cloudová ochrana

3.Pro zapnutí ESET LiveGuard Advanced je nutné aktivovat všechny tři možnosti v sekci **Cloudová ochrana**.



Od ESET Endpoint pro Windows ve verzi 10.1 a novější je odesílání souborů zapnuto ve výchozím nastavení.

Sekce: Cloudová ochrana	Popis
Zapnout reputační systém ESET LiveGrid® (doporučeno)	Aktivováním budou využívána data ze systému ESET LiveGrid®.
Zapnout systém zpětné vazby ESET LiveGrid®	Aktivováním povolíte zasílání souborů do cloudového systému ESET.
Zapnout ESET LiveGuard Advanced	Aktivováním povolíte zasílání souborů k analýze do ESET LiveGuard Advanced.

4.Dále se můžete rozhodnout, které typy souborů budou při detekci nebo podezření, že jsou škodlivé, odesílány do cloudového systému ESET.

Sekce: Odesílat vzorky	Popis a doporučení
Ruční odesílání vzorků	Pomocí této možnosti umožníte ruční odesílání vzorků k analýze do společnosti ESET (platí pouze pro produkty na platformě Windows)
Automatické odesílání detekovaných vzorků	Rozhodněte se, jaké typy vzorků chcete automaticky zasílat do společnosti ESET k analýze, když dojde k jejich detekci detekčním jádrem.
Spustitelné soubory, archivy, skripty a ostatní	Vyberte typy souborů, které chcete automaticky odesílat k analýze do ESET cloudu pokud je lokální detekční jádro nedetekovalo. Doporučujeme aktivovat zasílání všech typů souborů.
Pravděpodobný spam	Odesílání pravděpodobných spamových e-mailů (pouze pro ESET Endpoint for Windows)
Odstranit ze serverů společnosti ESET spustitelné soubory, archivy, skripty, další vzorky a zprávy označené jako pravděpodobný spam	Akce provedená po dokončení analýzy.
Dokumenty	Odesílání dokumentů Tato možnost je standardně zapnutá.
Odstranit dokumenty ze serverů společnosti ESET	Akce provedená po dokončení analýzy.

Sekce: Odesílat vzorky	Popis a doporučení
Výjimky	Seznam vyloučených přípon souborů, které nebudou odesílány. Přípony můžete přidávat ve formátu: `*.ext?`, kde: `*` představuje název souboru `ext` představuje příponu `?` představuje volitelný znak (tato možnost je volitelná).
Maximální velikost vzorku (MB)	Maximum velikost souboru, který je možné odeslat.

5.Ovlivnit můžete mezní hodnotu a akci při pozitivní detekci.

Sekce ESET LiveGuard Advanced:	Popis a doporučení
Mezní hodnota detekčního skóre	Stav výsledku analýzy důležitý pro **akci při detekci**.
Akce při detekci	Akce, kterou bezpečnostní produkt ESET provede, pokud je výsledek analýzy vyšší nebo roven **mezní hodnotě detekčního skóre**.
Maximální čas na analýzu (v min.)	Maximální doba čekání na výsledek analýzy před doručením e-mailu nebo stažením souboru.
Proaktivní ochrana	Nastavení proaktivní ochrany. Můžete povolit spuštění souborů, jejichž analýza ještě nebyla dokončena.

6.Po dokončení konfigurace politiky vyberte počítače nebo skupiny, kterým chcete politiku přiřadit. Nové nastavení se aplikuje při další replikaci mezi serverem a agentem (běžně v řádku několika minut).

Správa politik

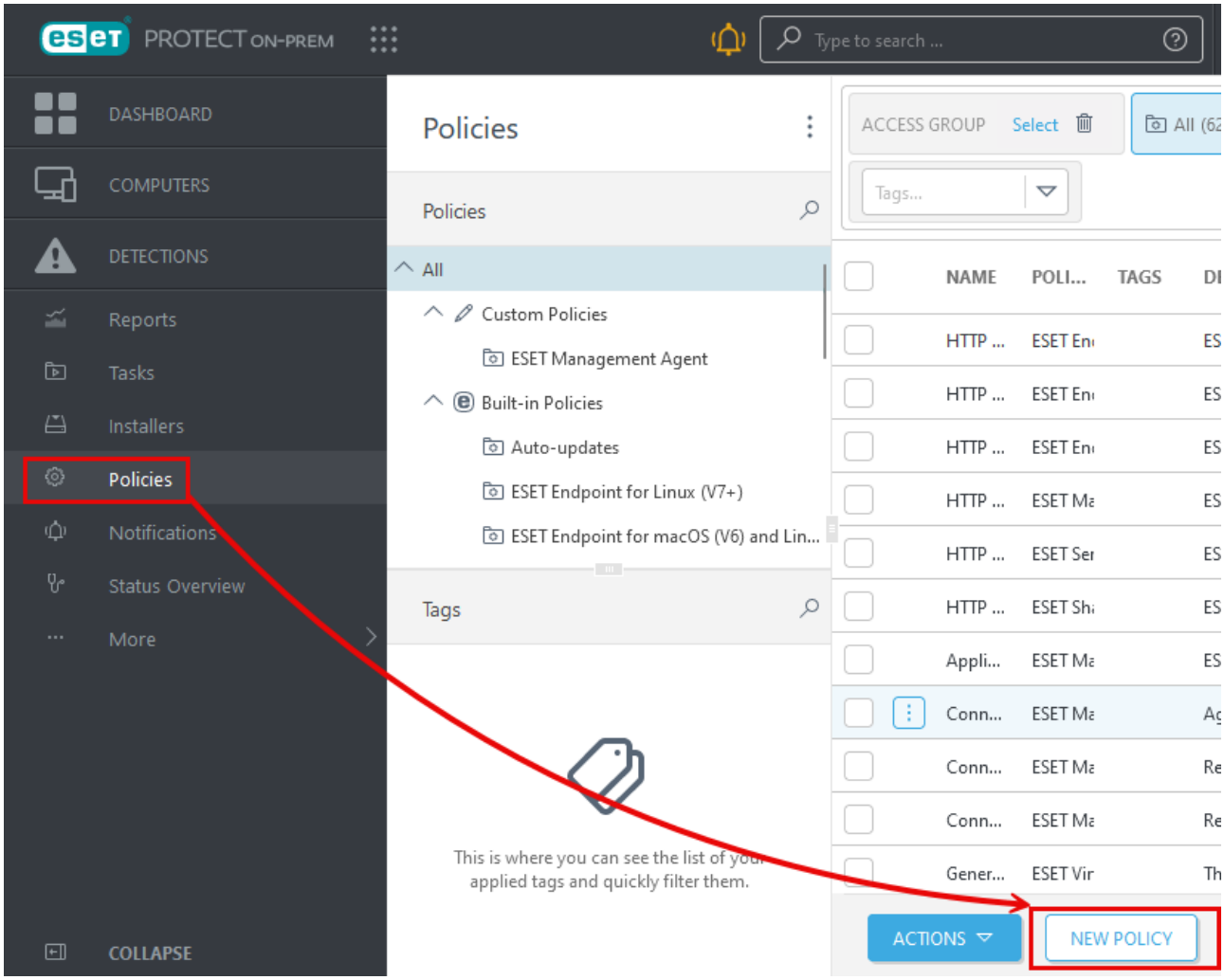
Prostřednictvím politik v konzole pro vzdálenou správu můžete ovlivnit nastavení bezpečnostních produktů ESET nainstalovaných na klientských stanicích. Politiky jsou specifické u každého produktu ESET pro firmy. Přiřadit je můžete skupinám nebo jen konkrétním klientům. V případě, že je na stanici aplikováno více politik, politiky se sečtou a následně se aplikuje výsledné nastavení.

Pro konfiguraci produktu prostřednictvím politik z konzole pro vzdálenou správu musí být na stanici nainstalován ESET Management Agent.

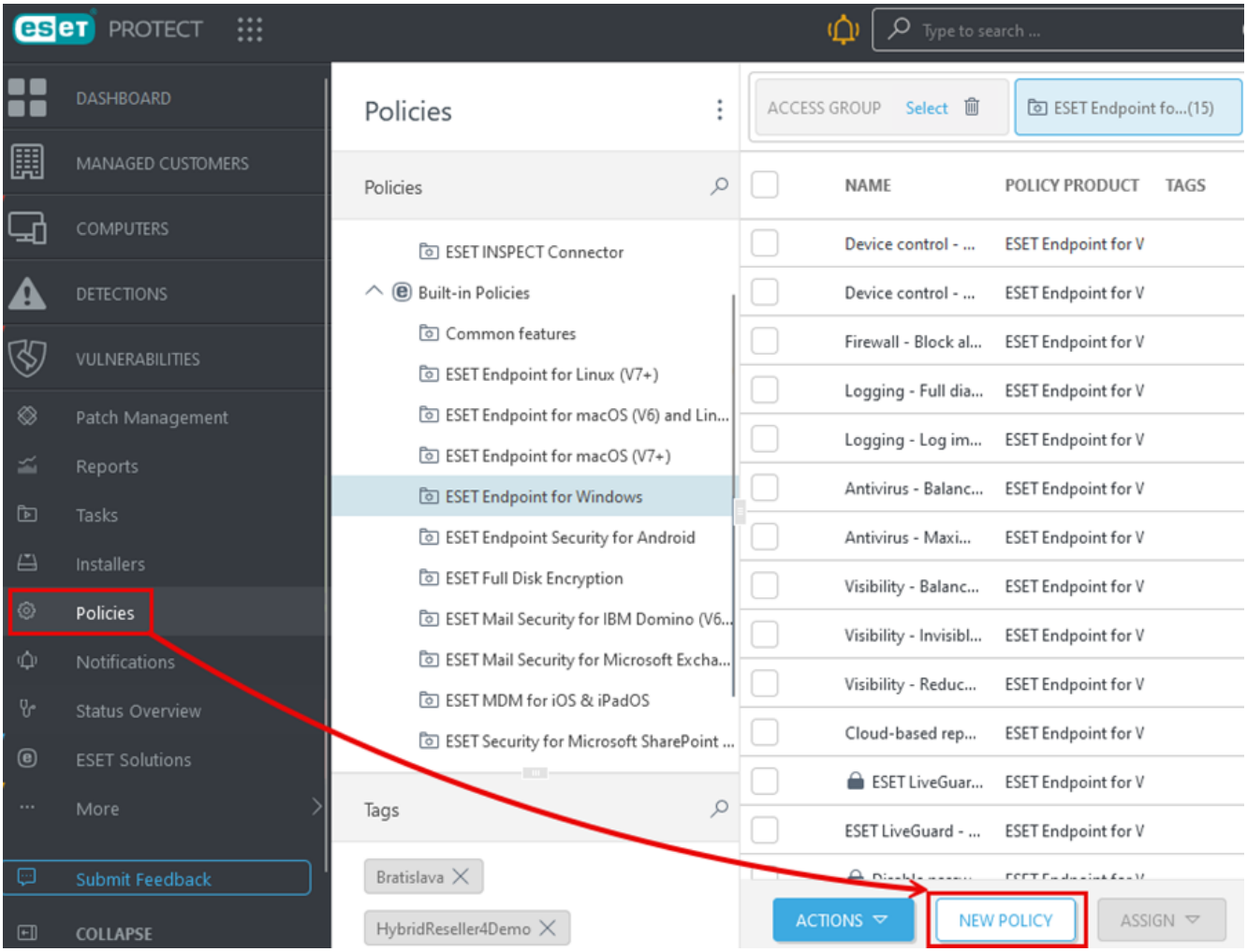
Vytvoření nové politiky

1.Přihlaste se do webové konzole.

2.Klikněte na **Politiky** > **Nová politika**.



Používám ESET PROTECT



3.Nejprve zadejte název a popis nové politiky a klikněte na **Pokračovat**.

4.Dále z rozbalovacího menu Produkt vyberte ESET produkt, pro který chcete vytvořit politiku. Proveďte požadované nastavení a klikněte na tlačítko **Pokračovat**.

5.Vyberte počítače nebo skupiny, kterým chcete politiku aplikovat, a klikněte na tlačítko **Pokračovat**.

6.Na závěr si v sekci **Přehled** zkontrolujte, zda nastavení odpovídá vašim představám. Politiku uložte kliknutím na tlačítko **Dokončit**.

Jak aktivovat ESET LiveGuard Advanced pomocí politiky?

Jak fungují politiky?

V konfigurační šabloně se po výběru produktu zobrazí možnosti, které můžete v daném produktu vzdáleně konfigurovat.

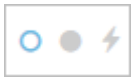
Na řádku v konfigurační šabloně jsou uvedeny následující položky:

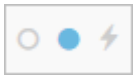
- Stav
- Název položky

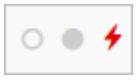
- Štítek definující podporovanou verzi (volitelně)
- Hodnota
- Bublinová nápověda (není uvedena u všech položek)



Příznak stav nastavení reprezentuje, zda, a jak se hodnota v politice na klienta propíše. Níže uvádíme rozdíly mezi jednotlivými možnosti:

 – nastavení není aktivní (politikou se nepropíše)

 – nastavení se aplikuje, ale může jej přepsat další politika

 – nastavení se aplikuje a nebude přepsáno jinou politikou

Při aplikování více politik na zařízení se výsledné nastavení odvíjí od pořadí politik. Více informací o politikách naleznete v Online nápovědě ESET PROTECT On-Prem.

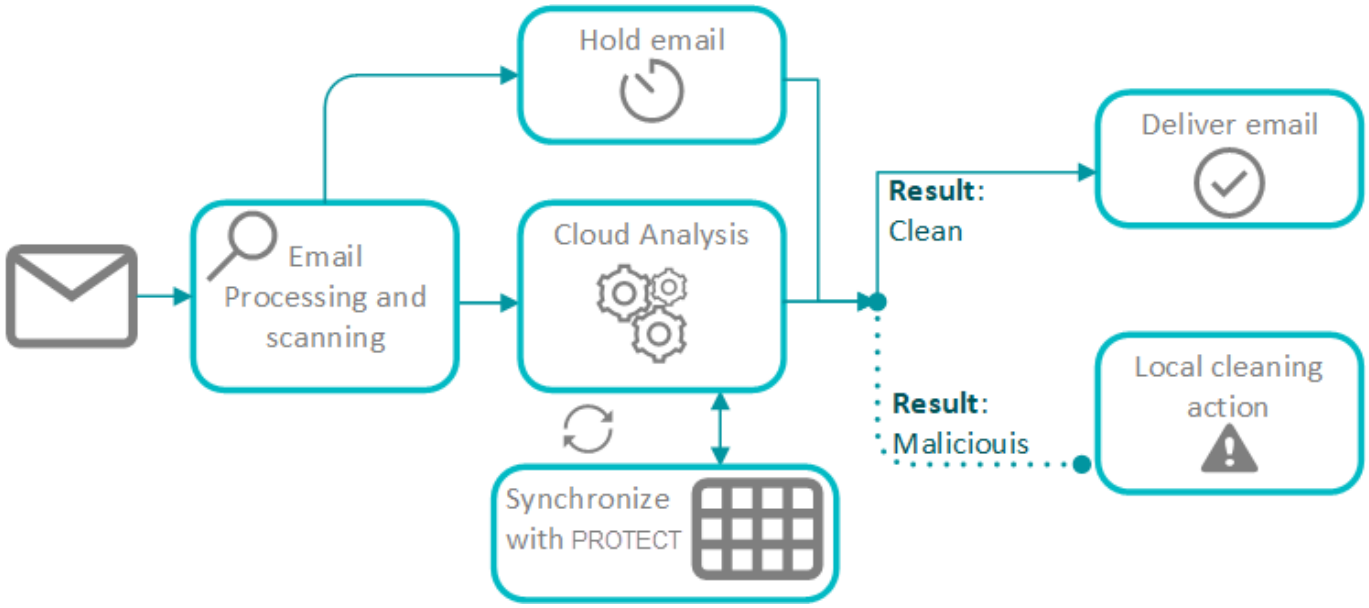
Používání ESET LiveGuard Advanced

Workflow ESET LiveGuard Advanced v ESET Mail Security

Každý e-mail, který zpracuje ESET Mail Security je zkontrolován a doručen. V případě, že je vyhodnocen jako podezřelý, jeho doručení je na definovanou dobou podrženo, a dojde k jeho zaslání na analýzu, při které se použije několik detekčních vrstev.

ESET LiveGuard Advanced zašle výsledek analýzy zpět bezpečnostnímu produktu ESET. Produkt při lokálním léčení objektu vychází z výsledků analýzy a provede akci definovanou v nastavení produktu.

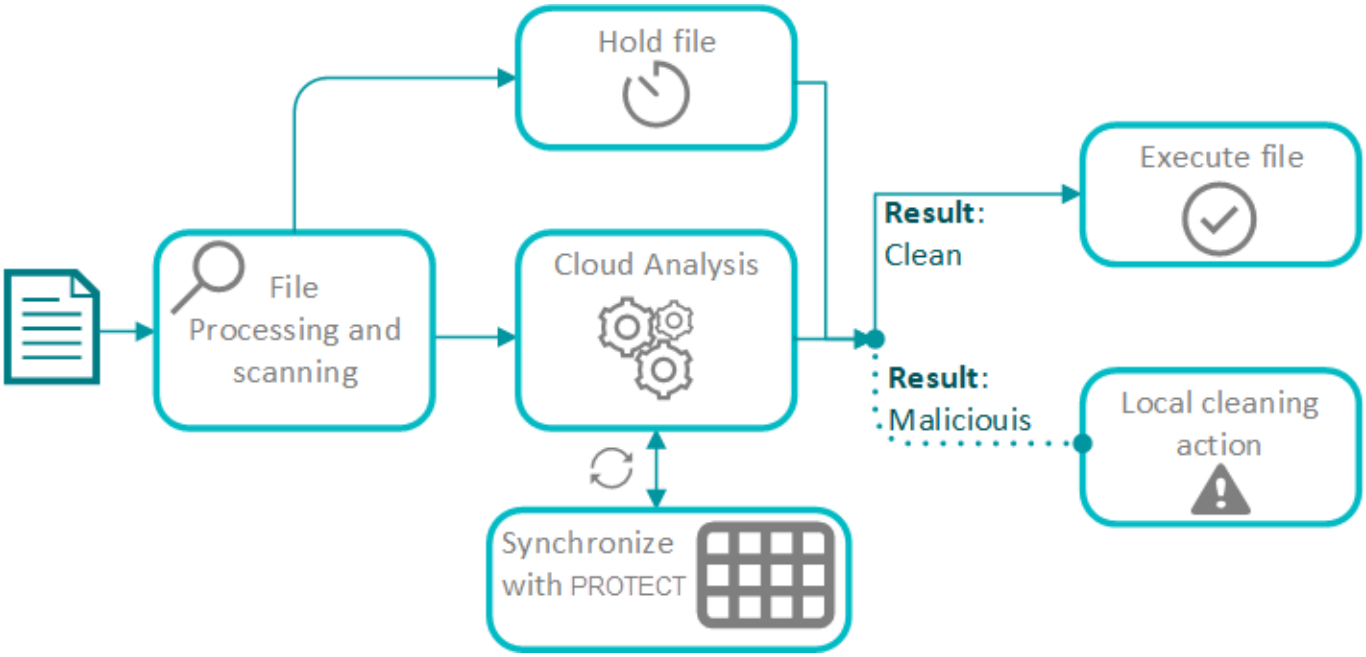
Níže naleznete schéma popisující zpracování objektu produktem ESET Mail Security.



Workflow ESET LiveGuard Advanced v ESET Endpoint Security / ESET Server Security

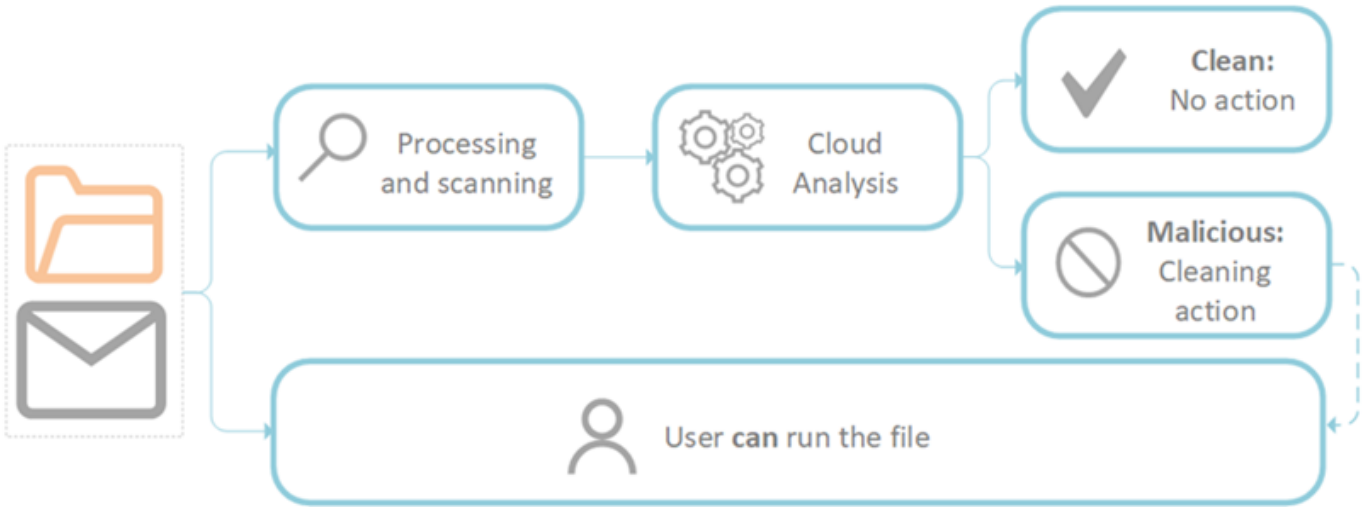
Každý nově vytvořený nebo příchozí soubor definovaného formátu detekovaný produktem ESET Endpoint Security / ESET Server Security je zkontrolován a spuštěn. V případě, že je vyhodnocen jako podezřelý, je zaslán k analýze. Jedná se o součást proaktivní ochrany. Můžete si nastavit dobu, po kterou bude spuštění souboru zablokováno, a uživatel bude nucen vyčkat na výsledek analýzy. V něm je výsledek analýzy uložen v cloudové databázi. Bezpečnostní produkt při lokálním léčení objektu vychází z výsledků analýzy a provede akci definovanou v nastavení produktu (proces je ihned ukončen nebo bude zablokováno jeho další spuštění).

Níže naleznete schéma popisující zpracování objektu produktem ESET Endpoint Security / ESET Server Security.



Workflow ESET LiveGuard Advanced v ESET Cloud Office Security

Kontrolován a spuštěn je každý soubor detekovaný produktem ESET Cloud Office Security. V případě, že skener vyhodnotí soubor jako podezřelý, zašle jej k analýze. V cloudovém systému ESET je ukládán výsledek analýzy v cloudové databázi. Na základě výsledku analýzy provede ESET Cloud Office Security s objektem akci definovanou v nastavení pomocí politiky. Další informace o politikách ESET Cloud Office Security naleznete v kapitole Nastavení ochrany zajišťované prostřednictvím ESET LiveGuard Advanced.

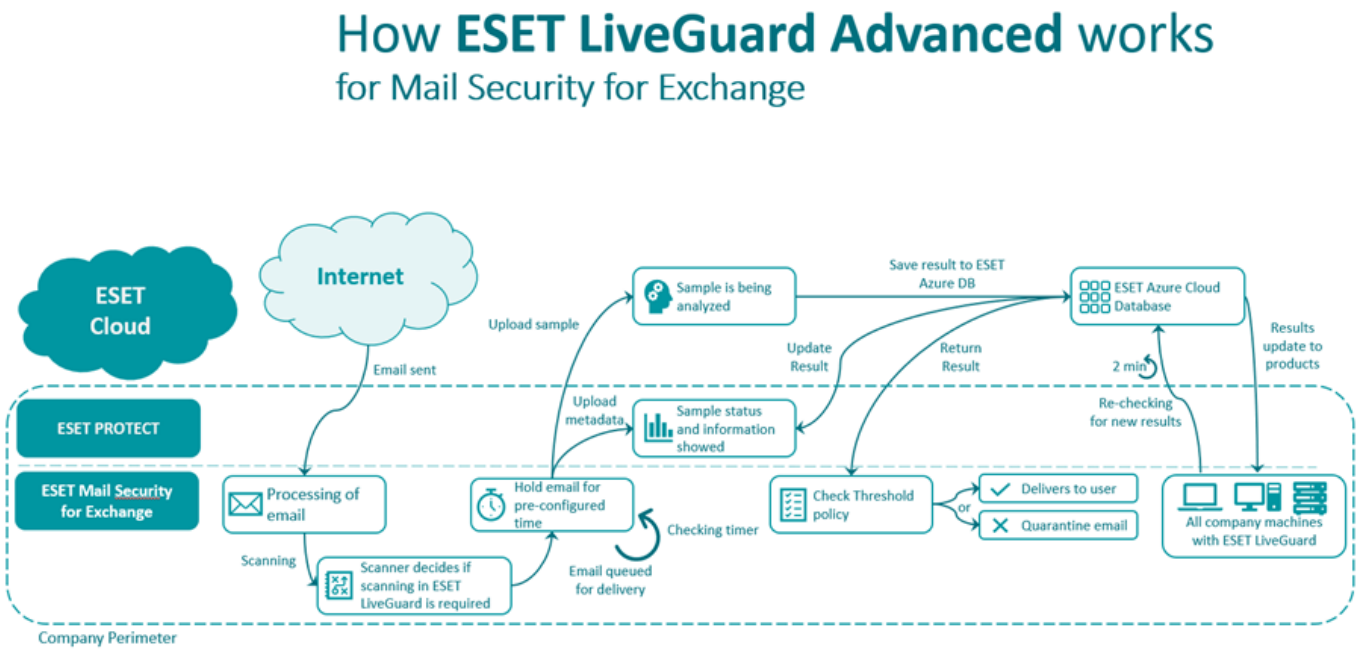


ESET Mail Security

V této kapitole popisujeme posloupnost akcí, které provede ESET Mail Security s aktivní funkcí ESET LiveGuard Advanced při zpracování zprávy. V nastavení produktu můžete definovat:

- pozdržení doručení zprávy (platné pouze pro ochranu poštovních schránek),
- úroveň zabezpečení,
- akci při detekci škodlivého objektu (platné pouze pro ochranu hosta).

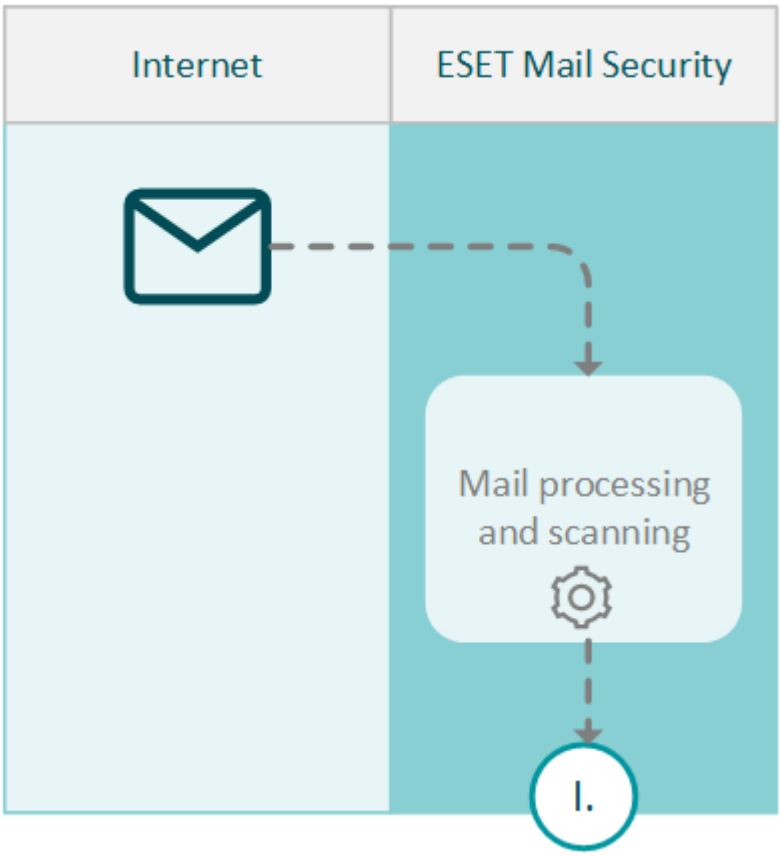
ESET Mail Security chrání hostitelský server včetně poštovních schránek
ESET Mail Security s aktivní funkcí ESET LiveGuard Advanced chrání podle níže uvedeného principu poštovní schránky. Zároveň chrání hosta stejným způsobem jako ESET Server Security.



Analýza zprávy se skládá z následujících čtyř kroků:

1. Kontrola zprávy

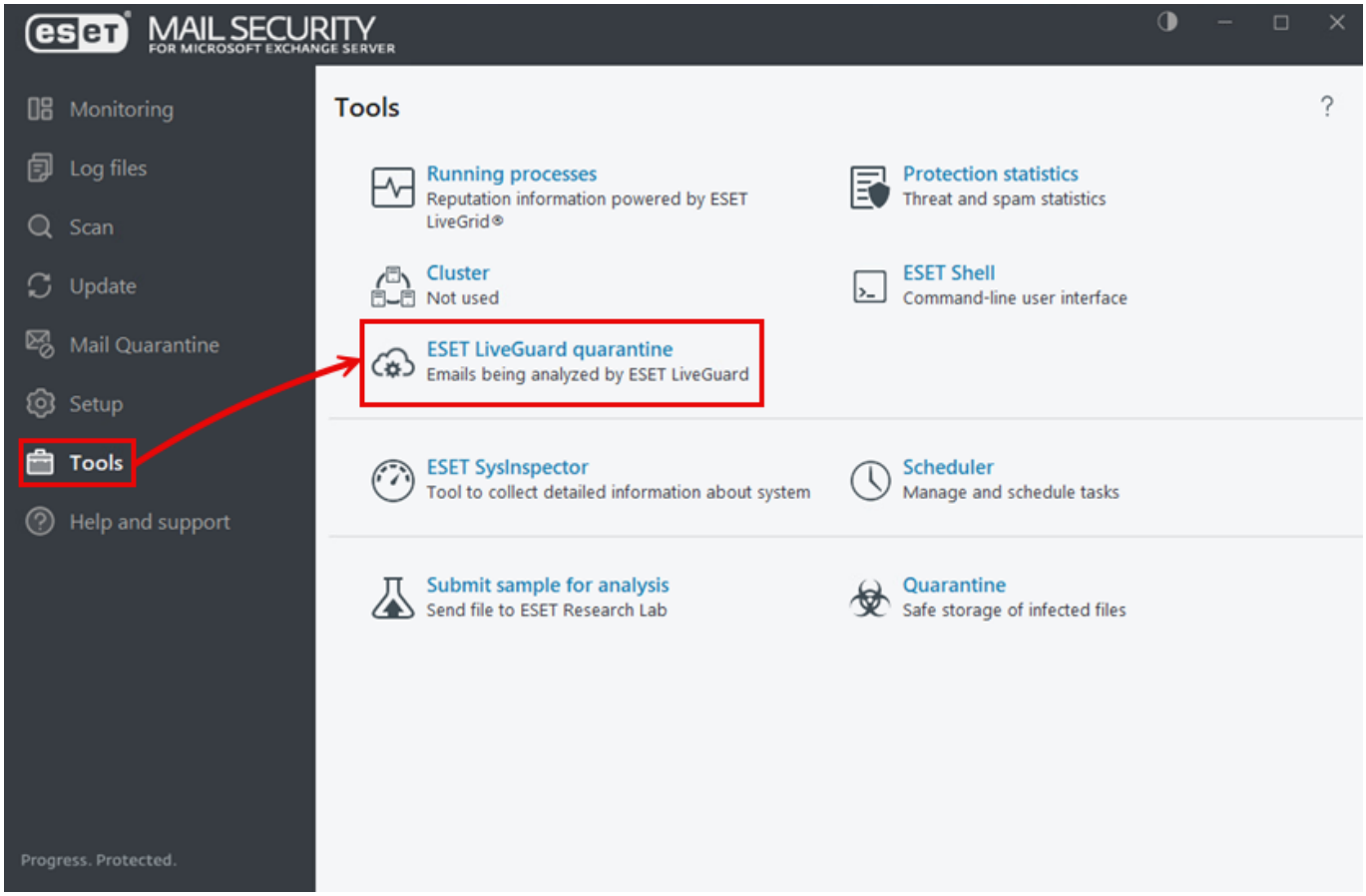
Při stažení zprávy z internetu nebo jiného nedůvěryhodného zdroje bezpečnostní produkt ESET zpracuje a zkontroluje zprávu.

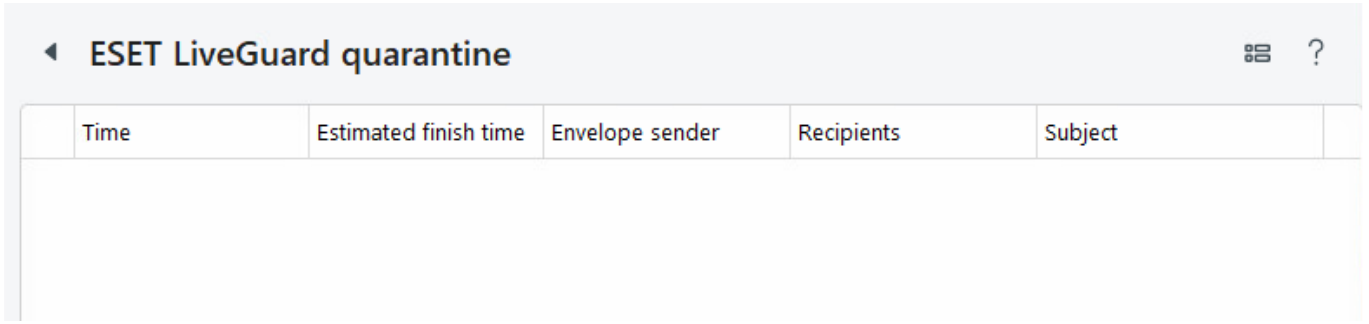


2. Analýza a doručení zprávy

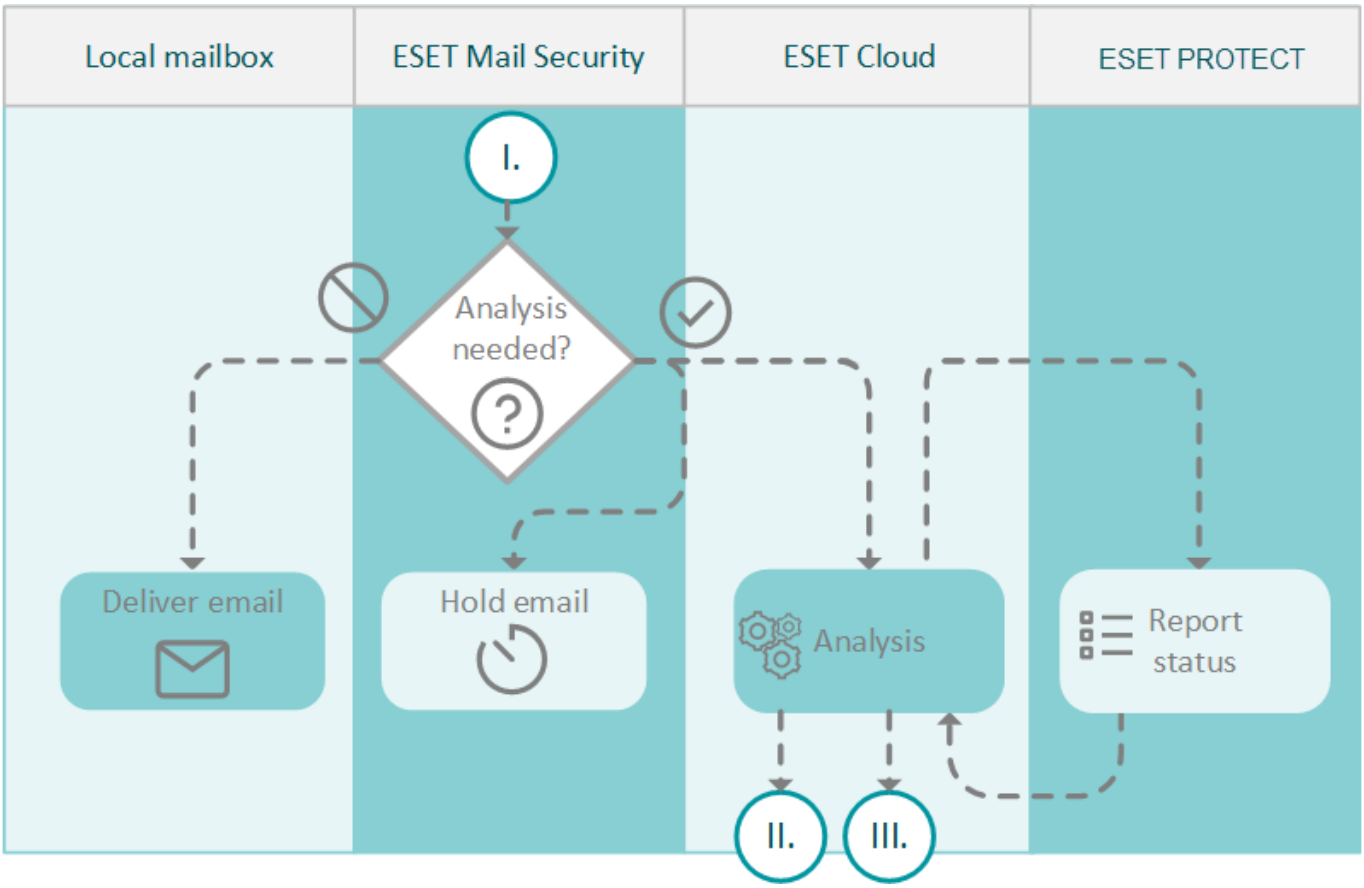
V případě, že bezpečnostní produkt vyhodnotí, že je potřeba analýza, doručení zprávy je na definovanou dobu pozdrženo. Během této doby ESET LiveGuard Advanced analyzuje přílohu zprávy. Pokud je výsledek analýzy jako v pořádku, e-mail je okamžitě doručen. Pokud je škodlivý, dojde ke standardnímu odstranění hrozby. Pokud není výsledek analýzy včas doručen, bezpečnostní produkt zašle příjemcům zprávu. Obdrží-li následně produkt pozitivní výsledek analýzy, k zablokování škodlivého objektu, na všech počítačích v sítích, dojde do dvou minut.

- Seznam pozdržených zpráv naleznete v produktu ESET Mail Security. V hlavním menu programu ESET Mail Security přejděte na záložku **Nástroje** > **ESET LiveGuard Advanced**.



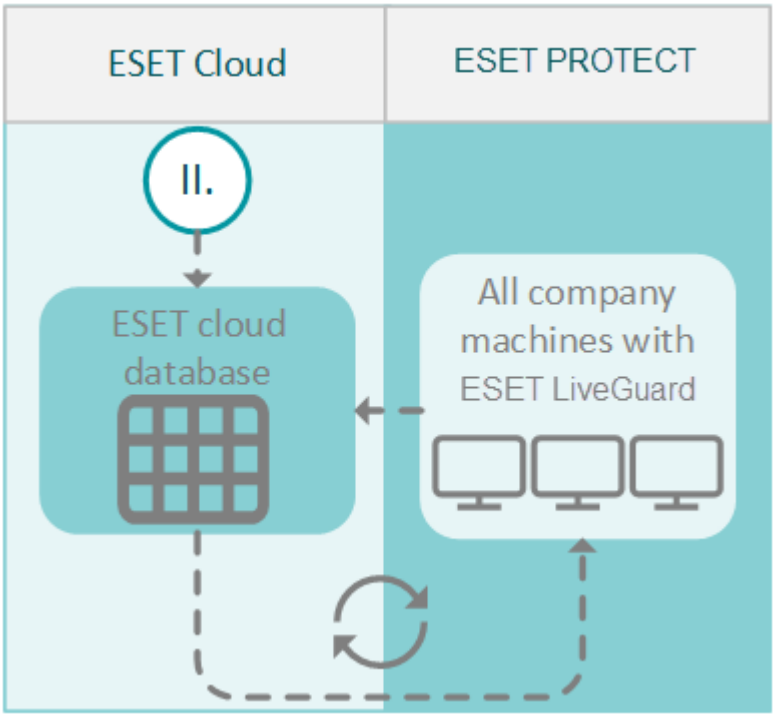


- Maximální dobu čekání na výsledek analýzy nastavíte v politice ESET Mail Security v sekci Počítač > Cloudová ochrana > ESET LiveGuard > Maximální čas na analýzu.



3. Sdílení výsledku analýzy

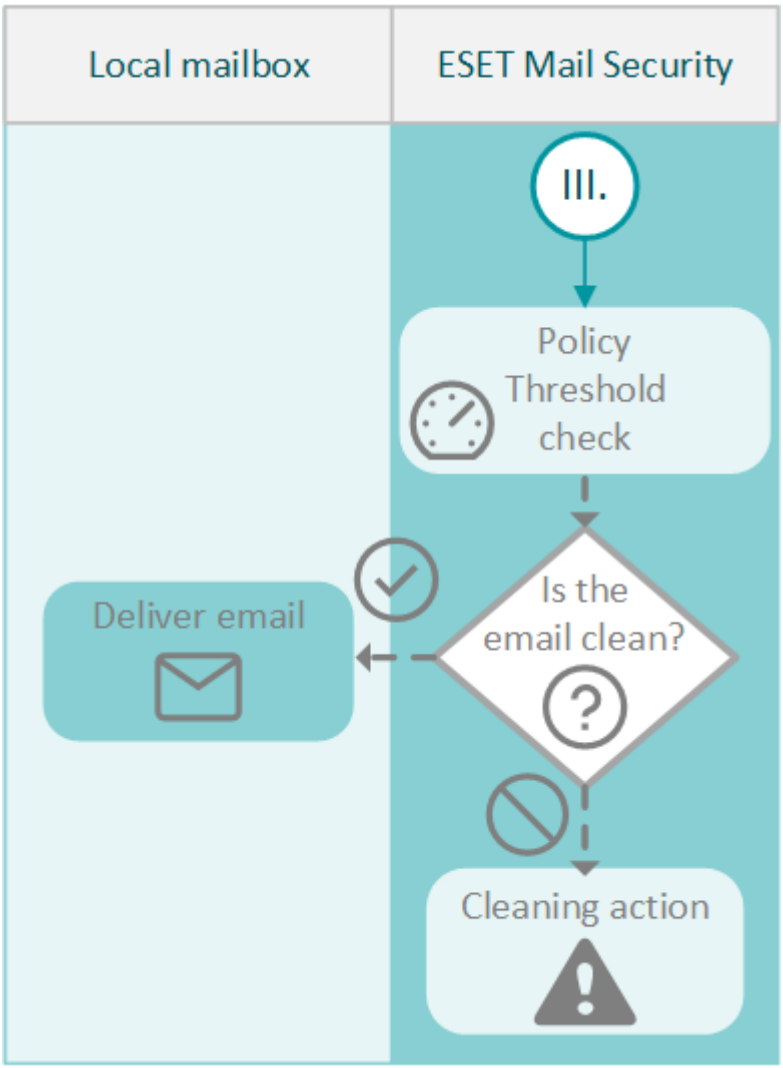
ESET LiveGuard Advanced využívá k analýze čtyři samostatné detekční vrstvy. Výsledek analýzy je následně uložen do databáze v cloudovém systému ESET. Obsah této databáze se s ESET PROTECT On-Prem synchronizuje každou minutu. Zařízení, na kterých je aktivní funkce ESET LiveGuard Advanced, se s cloudovou databází synchronizují každé 2 minuty.



4. Vyhodnocení a léčení

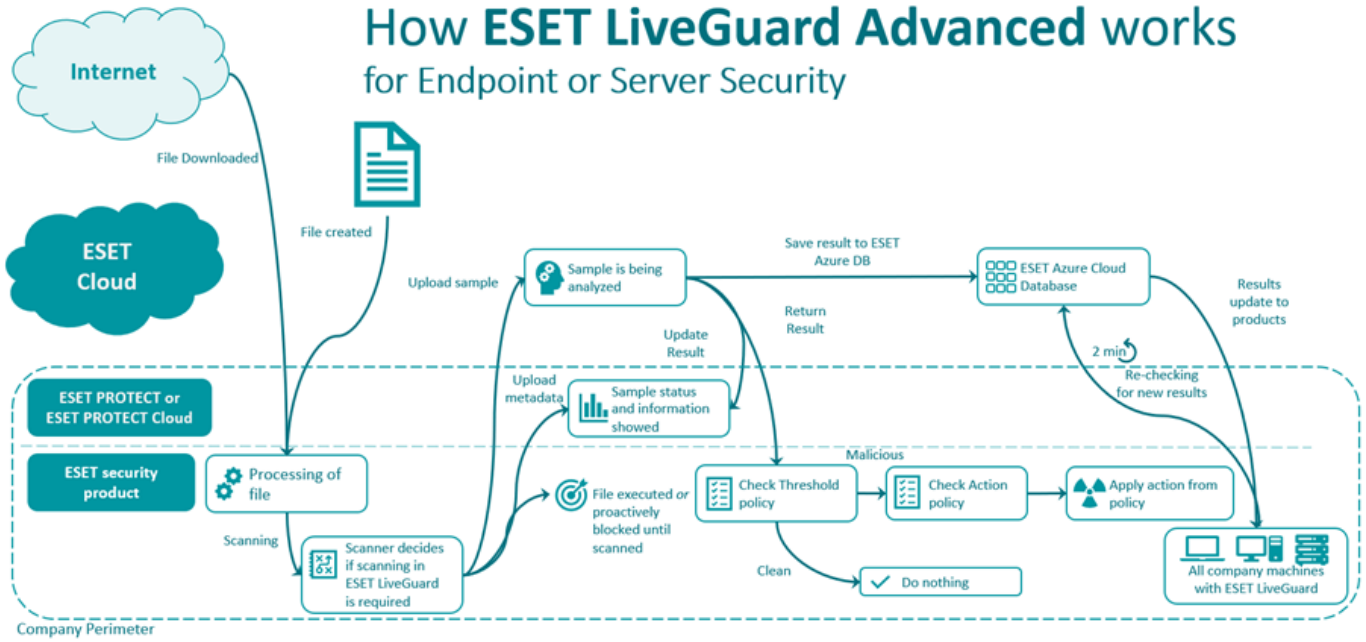
Výsledek analýzy je rovněž zaslán zpět bezpečnostního produktu, který opětovně zkontroluje danou zprávu. Pokud je e-mail čistý, je doručen (pokud zatím neuplynula maximální přípustná doba pro podržení zprávy).

V případě, že je objekt detekován jako škodlivý, ESET Mail Security provede akci definovanou v nastavení (v sekci **Server**).



ESET Endpoint Security a ESET Server Security

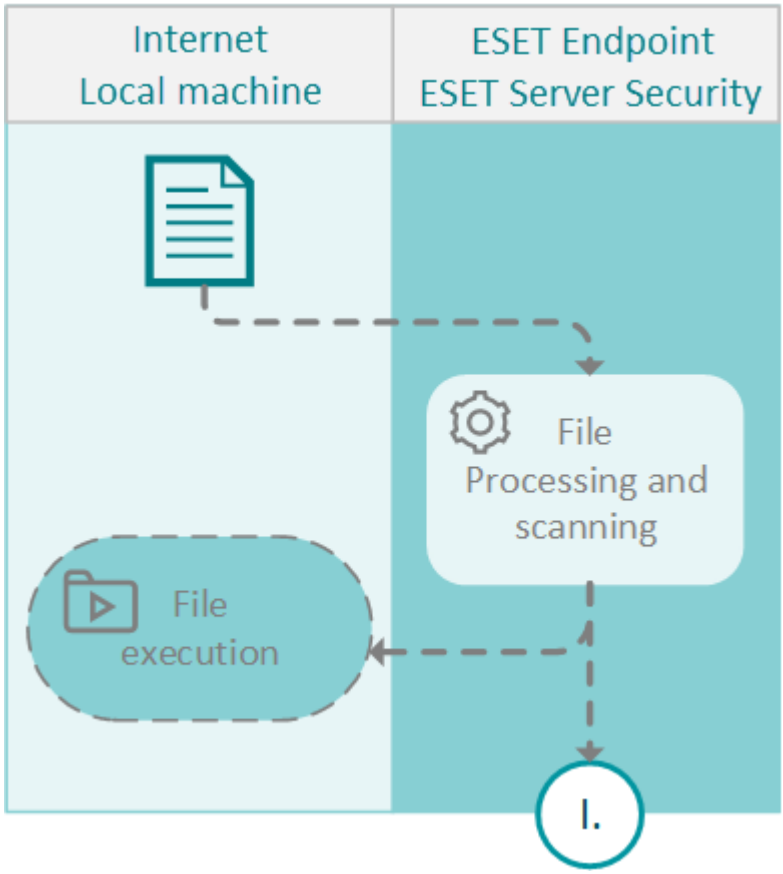
V této kapitole popisujeme posloupnost akcí, které provede ESET Endpoint Security nebo ESET Server Security s aktivní funkcí ESET LiveGuard Advanced při zpracování objektu. Provedenou akci a úroveň léčení můžete ovlivnit prostřednictvím politiky.



Analýza souboru se skládá z následujících čtyř kroků.

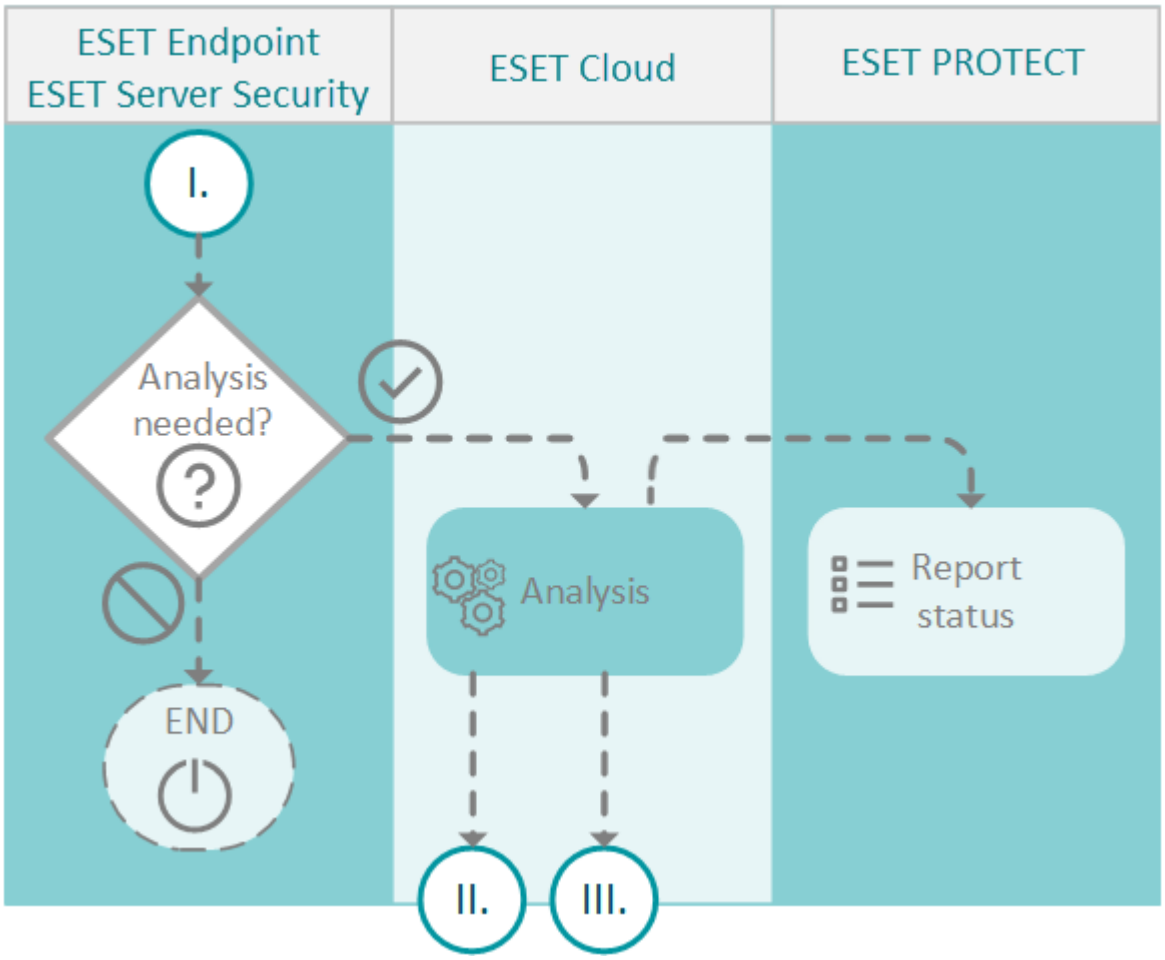
1. Kontrola souboru

Při stažení souboru z internetu, zkopírování z jiného zařízení nebo vytvoření nového, bezpečnostní produkt ESET soubor zpracuje a zkontroluje.



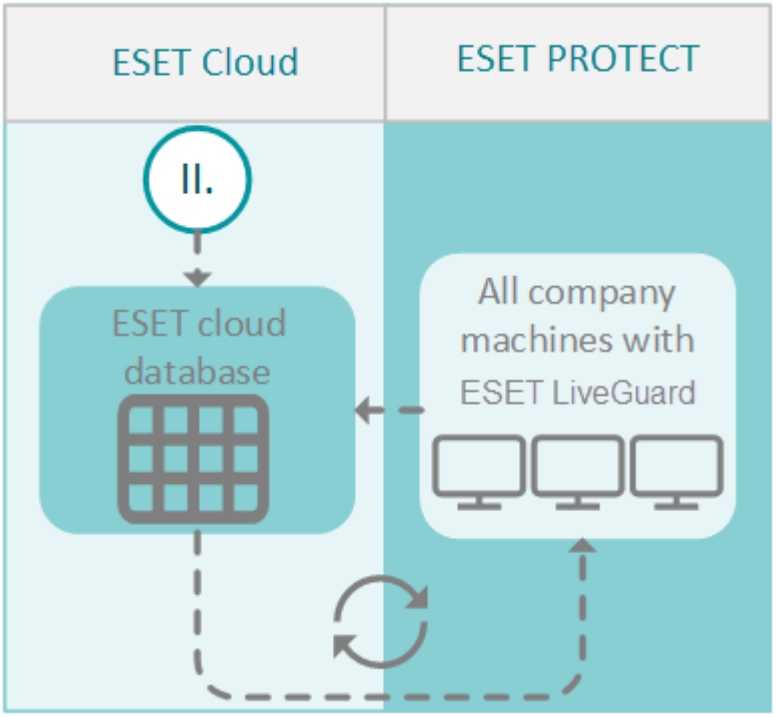
2. Analýza souboru

V případě, že bezpečnostní produkt ESET rozhodne o analýze souboru, zašle jej k analýze. Soubor zpracovávají a na výsledku analýzy se podílí čtyři samostatné detekční vrstvy. Výsledek analýzy je následně zaslán do ESET PROTECT On-Prem. Pokud není analýza vyžadována, proces tímto končí.



3. Sdílení výsledku analýzy

Výsledek analýzy je uložen do databáze v cloudovém systému ESET. Obsah této databáze se s ESET PROTECT On-Prem synchronizuje každé dvě minuty. Všechna zařízení s aktivní funkcí ESET LiveGuard Advanced mají přístup k aktuálním informacím přímo z ESET cloudu.

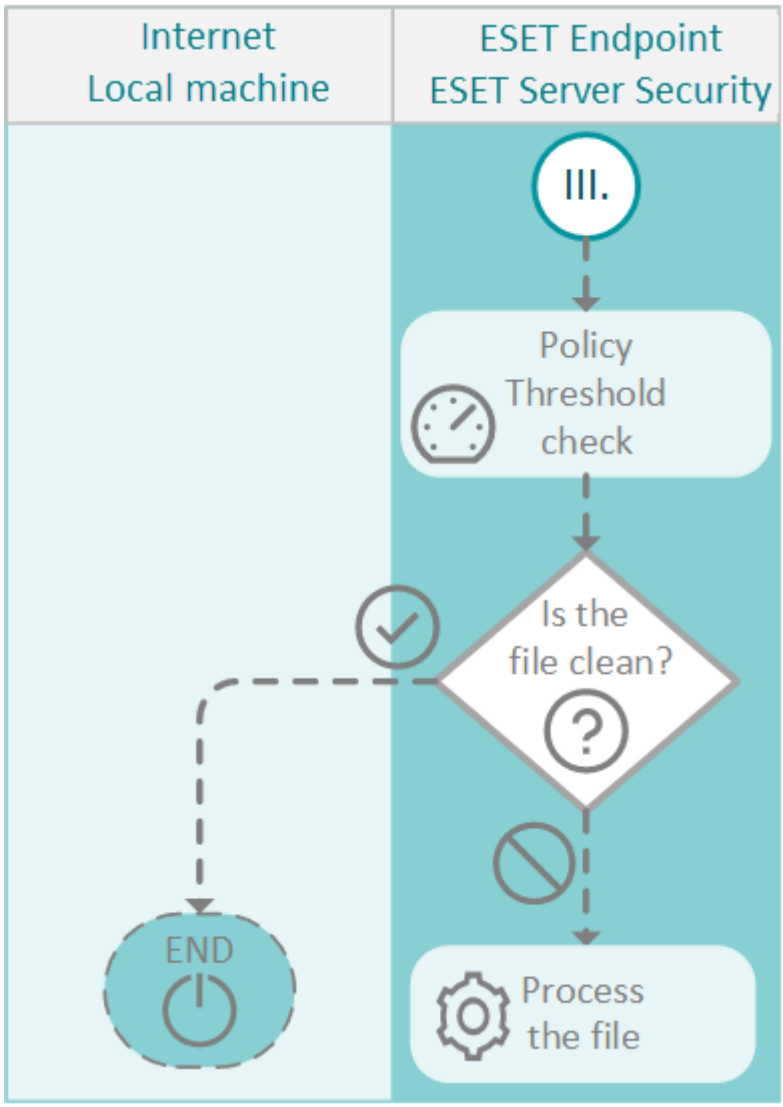


4. Vyhodnocení lokální politiky

Výsledek analýzy je rovněž zaslán zpět bezpečnostního produktu. Bezpečnostní produkt následně provede akci definovanou v nastavení pomocí politiky (léčit, odstranit, žádná akce).

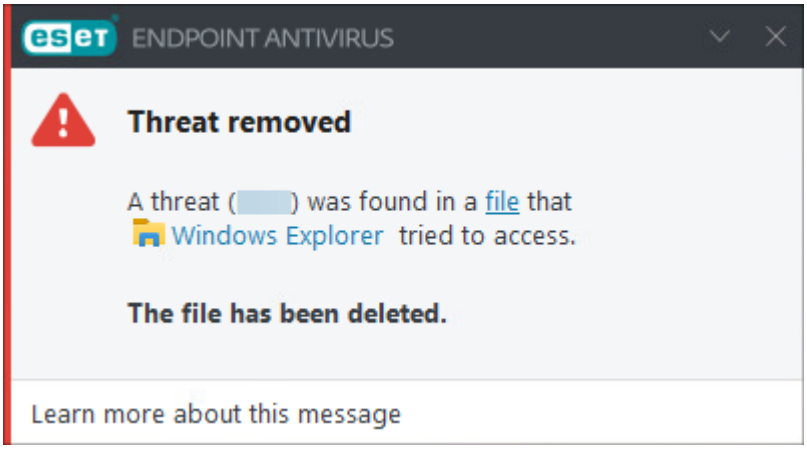
- Mezní hodnotu detekčního skóre nastavíte v politice pro ESET Endpoint Security / ESET Server Security v sekci **Detekční jádro** > **Cloudová ochrana** > **ESET LiveGuard Advanced** > **Mezní hodnota detekčního skóre**

- Akci, která se má provést se škodlivým objektem nastavíte v politice pro ESET Endpoint Security / ESET Server Security v sekci **Detekční jádro** > **Cloudová ochrana** > **ESET LiveGuard Advanced** > **Akce při detekci**.



Příklad oznámení

Pokud ESET LiveGuard Advanced vyhodnotí soubor jako škodlivý, program ESET Endpoint Security provede definovanou akci pro vyléčení hrozby. Po odstranění souboru se uživateli zobrazí níže uvedené systémové oznámení.

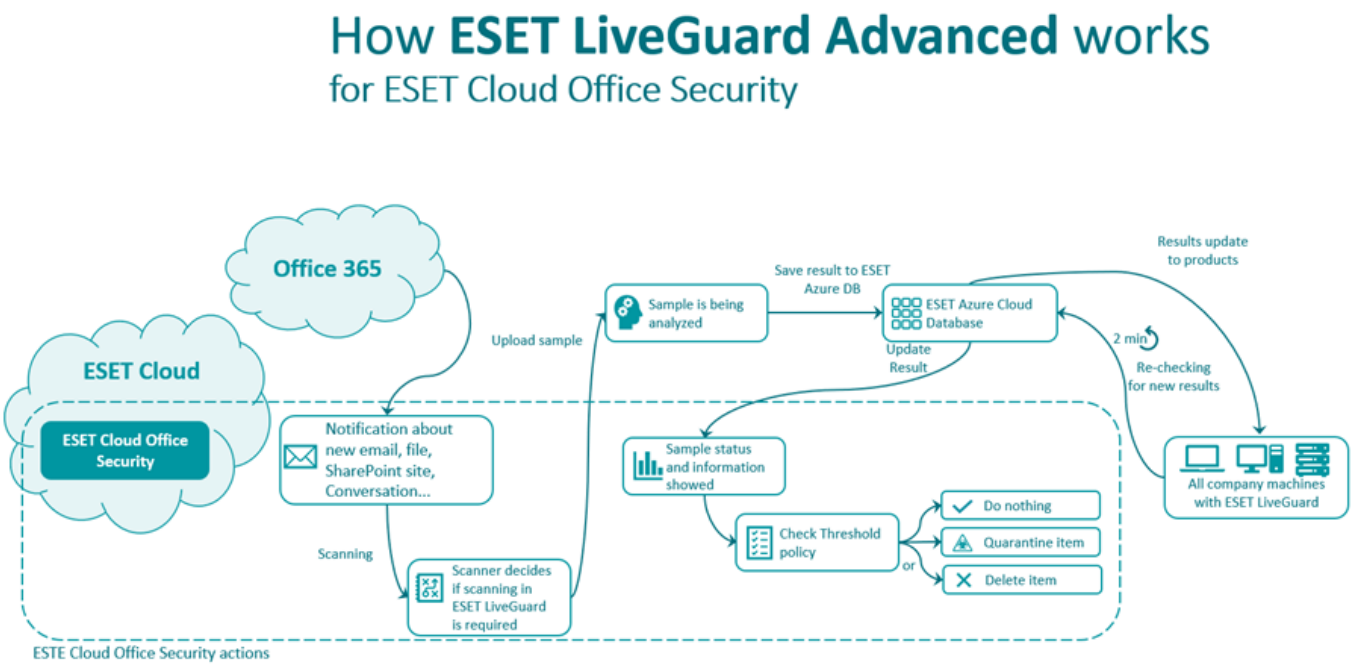


ESET Cloud Office Security

ESET Cloud Office Security vyžívá službu ESET LiveGuard Advanced k analyzování zcela nových hrozeb. K jejímu vyžití není vyžadována ESET konzole pro vzdálenou správu (ESET PROTECT On-Prem / ESET PROTECT). Informace

související s odeslanými soubory a výsledky jejich analýzy jsou dostupné výhradně v ESET Cloud Office Security.

- ESET Cloud Office Security neodesílá žádné informace o ESET konzole pro vzdálenou správu; ani v případě, kdy využívají stejný EBA/EMA účet.
- ESET Cloud Office Security sdílí informace o detekcích s koncovými stanicemi aktivovanými licencí přidanou ve stejném EBA/EMA účtu
- ESET Cloud Office Security může k analýze odeslat podezřelou přílohu zprávy a vzorky sdílené prostřednictvím Microsoft SharePoint, Teams, a dalších částí Office 365.



Analýza souboru odeslaného z ESET Cloud Office Security se skládá z následujících čtyř kroků.

1. Kontrola souboru

Při výskytu nového souboru v cloudovém úložišti skenovací jádro ESET soubor zpracuje a zkontroluje.

2. Analýza souboru

V případě, že skenovací jádro rozhodne o analýze souboru, zašle jej k analýze. Soubor zpracovávají a na výsledku analýzy se podílí čtyři samostatné detekční vrstvy. Pokud není analýza vyžadována, proces tímto končí.

3. Sdílení výsledku analýzy

Výsledek analýzy je uložen do databáze v cloudovém systému ESET. Zároveň je sdílen se všemi zařízeními aktivovanými licencí přidanou ve stejném účtu jako ESET LiveGuard Advanced.

4. Rozhodnutí ESET Cloud Office Security o provedení akce

Výsledek analýzy je rovněž zaslán zpět do ESET Cloud Office Security. Na základě nastavení v politiky se provede definovaná akce (léčit, odstranit, žádná akce). Více informací naleznete v online příručce v kapitole nastavení ochrany pro ESET LiveGuard Advanced.

Proaktivní ochrana

Proaktivní ochrana detekuje soubory v následujících případech:

- Při stahování prostřednictvím podporovaného prohlížeče
- Při stahování z poštovního klienta
- Při vybalování z nešifrovaných i šifrovaných archivů prostřednictvím podporovaných nástrojů na práci s archivy
- Při spouštění a otevírání souborů z výměnných zařízení

Pokud je soubor označen jako podezřelý, Proaktivní ochrana zablokuje jeho spuštění do doby, než detekční vrstvy dokončí jeho analýzu.

Podporované aplikace a zařízení

Tato funkce je dostupná v produktech běžících na zařízení s:

- Windows – všechny podporované produkty z řady ESET Endpoint, ESET Server Security 7.2 a novější, ESET Mail Security 7.2 a novější.
- Linux – všechny podporované produkty.

Podporované aplikace a zařízení na Windows

Webové prohlížeče	Poštovní klienti	Nástroje pro práci s archivy	Výměnná zařízení
Internet Explorer	Microsoft Outlook	WinRAR	USB flash disk
Microsoft Edge	Mozilla Thunderbird	WinZIP	USB pevný disk
Chrome	Microsoft Mail	Vestavěný archivátor v Průzkumníkovi Windows	CD/DVD
Firefox		7zip	Disketová jednotka
Opera			Vestavěná čtečka paměťových karet
Prohlížeč Brave			

Soubory zkopírované prostřednictvím Microsoft Explorer z umístění přidaného na seznamu výjimek do chráněného umístění jsou blokovány proaktivní ochranou produktu ESET LiveGuard Advanced z důvodu, že `explorer.exe` je rozpoznán jako podporovaný nástroj pro práci s archivy.

Podporované aplikace a zařízení na Linuxu

Webové prohlížeče	Poštovní klienti	Nástroje pro práci s archivy	Výměnná zařízení
Chrome	Mozilla Thunderbird	Nepodporováno na Linuxu	USB flash disk
Firefox	Evolution		USB pevný disk
Opera	Mailspring		CD/DVD
Brave Browser	KMail		Disketová jednotka

Webové prohlížeče	Poštovní klienti	Nástroje pro práci s archivy	Výměnná zařízení
Vivaldi	Geary		Vestavěná čtečka paměťových karet
	Mutt		
	claws mail		
	Alpine		

Uživatelé ESET Cloud Office Security

V ESET Cloud Office Security není dostupná proaktivní ochrana.

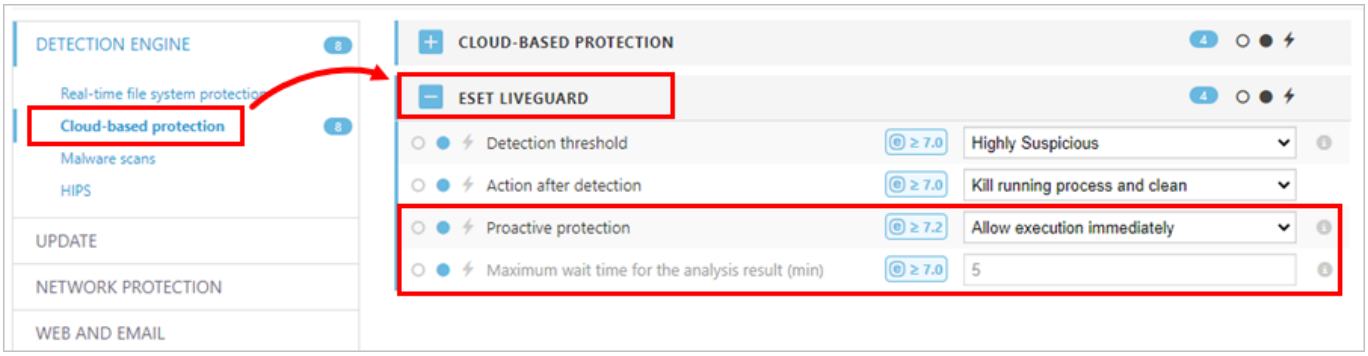
Konfigurace ESET Endpoint Antivirus

Konfiguraci proaktivní ochrany provedete prostřednictvím politiky.

V hlavním menu webové konzole přejděte do sekce Politiky, upravte stávající nebo vytvořte novou politiku. V konfigurační šabloně kompatibilního produktu ESET přejděte do sekce **Detekční jádro** > **Cloudová ochrana** > **ESET LiveGuard Advanced** > **Proaktivní ochrana**.

- **Povolit okamžité spuštění** – při vybrání této možnosti bude schopen uživatel soubor spustit ve chvíli, kdy je stále analyzován. Produkt provede definovanou akci po obdržení výsledku analýzy.

- **Blokovat spuštění do obdržení výsledku analýzy** – při vybrání této možnost bude uživatel nucen vyčkat na výsledek analýzy. Až následně bude umožněno úplné spuštění souboru.

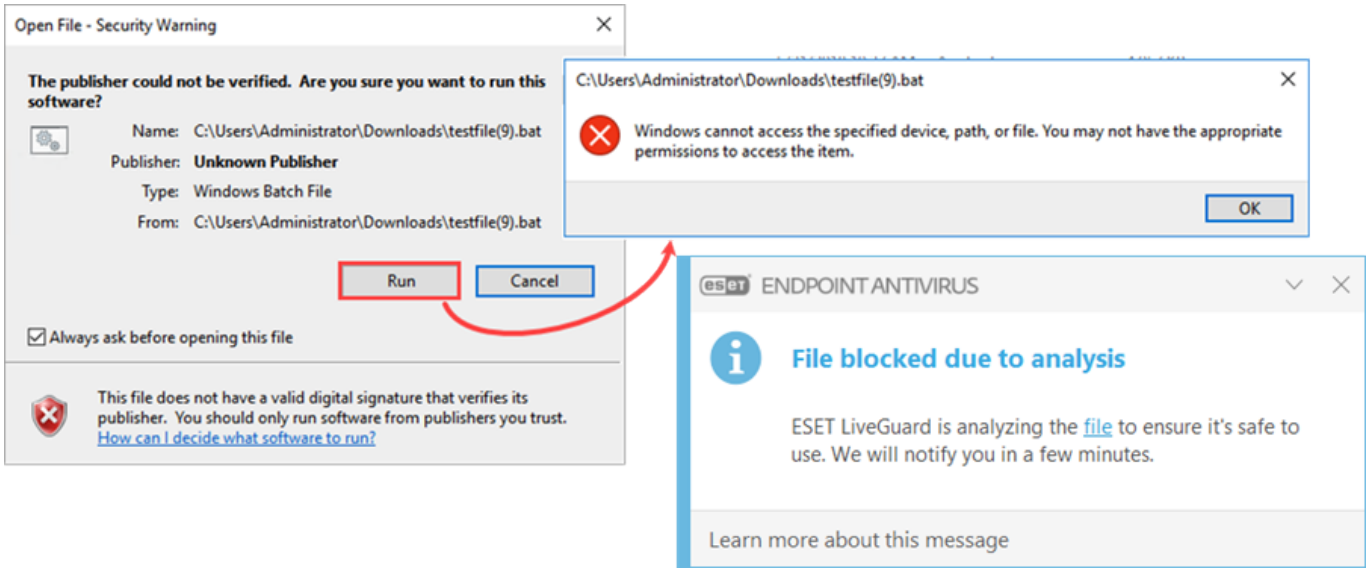


Použití proaktivní ochrany

Při prvním spuštění podezřelého souboru může operační systém Windows zobrazit chybové hlášení. Zároveň v takovém případě produkt ESET zobrazí oznámení, že se zahájilo analyzování souboru. Pokud je však analýza dokončena před prvním spuštěním souboru, uvedené hlášení se **nezobrazí**.

Windows uživatelé

V závislosti na konfiguraci může v průběhu analýzy operační systém Windows povolit nebo zablokovat spuštění souboru.

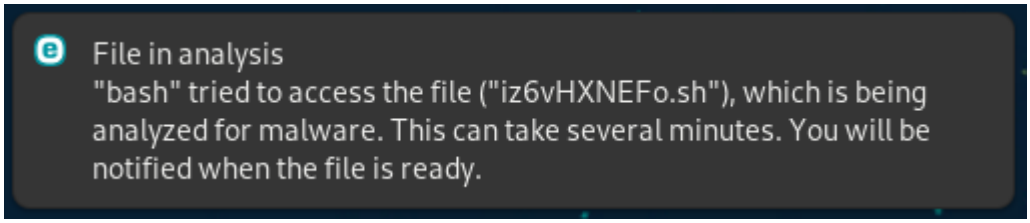


Linux uživatelé

ESET Server Security pro Linux nezobrazí žádné oznámení týkající se probíhající analýzy. Pokud se pokusíte spustit soubor, který blokuje proaktivní ochrana:

- Operační systém vrátí informaci o odepření přístupu.
- V terminálu se zobrazí hláška `Operation not permitted`.

ESET Endpoint Security v případě systému s grafickým rozhraním zobrazí níže uvedené hlášení:

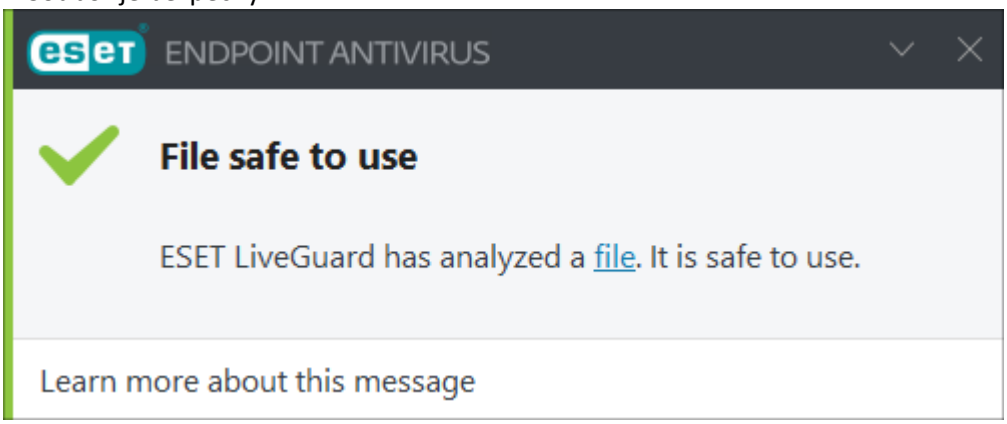


Výsledek analýzy

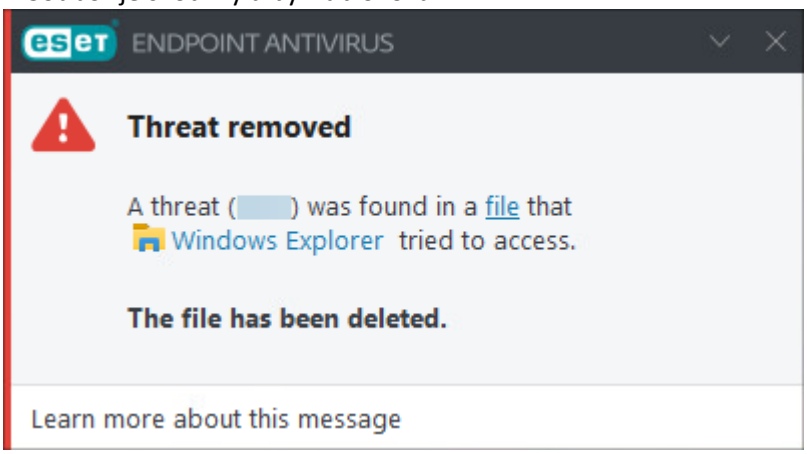
Doručení výsledku v definovaném čase

V konfiguraci produktu můžete definovat maximální čas, po který bude produkt čekat na doručení výsledku analýzy. V případě, že je výsledek doručen včas, může se zobrazit jedno z níže uvedených hlášení:

- Soubor je bezpečný:

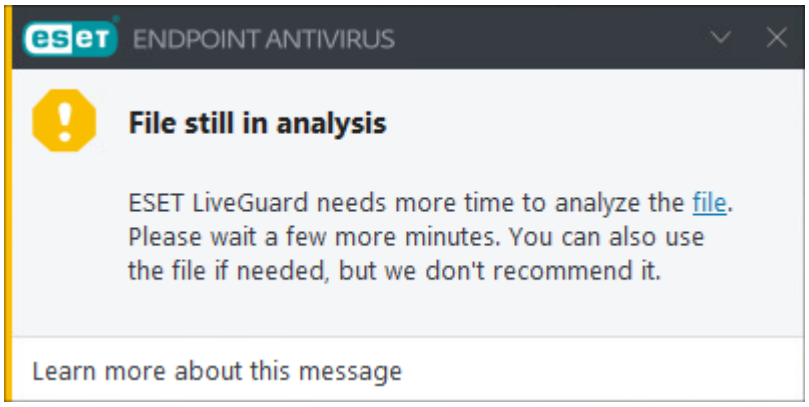


- Soubor je škodlivý a byl zablokován:



Výsledek nebyl doručen v definovaném čase

Pokud analýzy trvá příliš dlouho a dojde k překročení definovaného času, uživateli je umožněno spuštění souboru a zároveň se zobrazí informace o stále probíhající analýze.



V případě, že soubor bude škodlivý, produkt zobrazí upozornění a provede odpovídající akci.

Jak zobrazit seznam odeslaných souborů

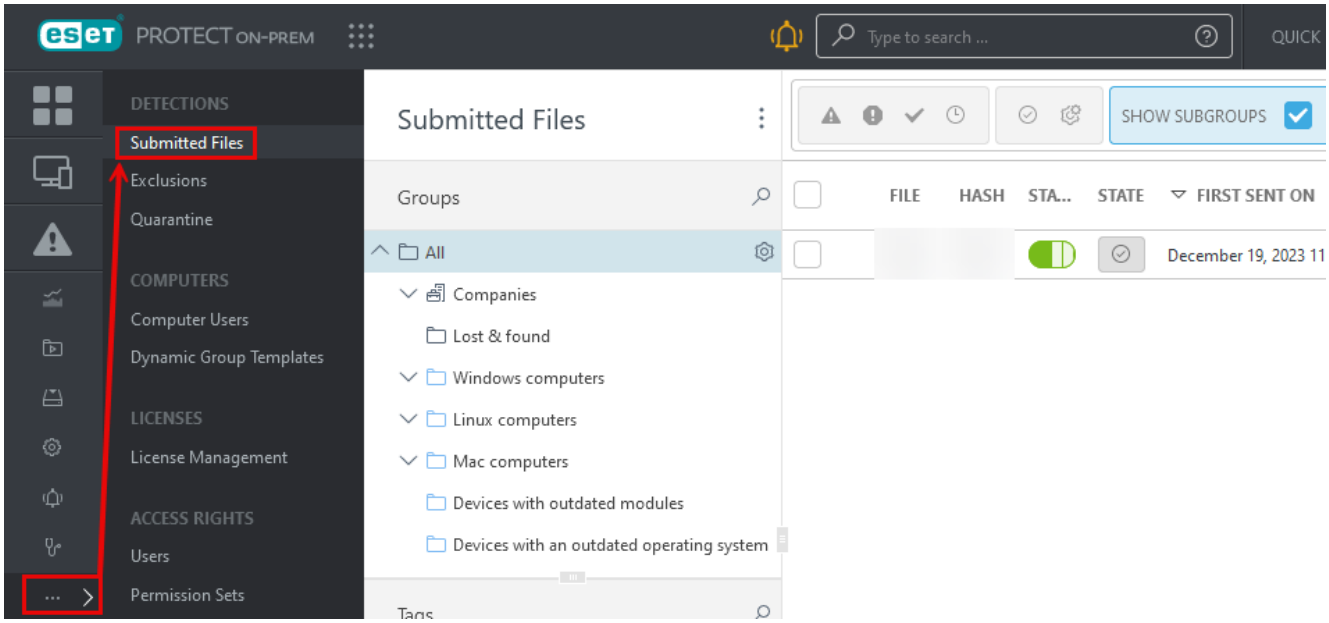
Seznam odeslaných souborů k analýze do společnosti ESET prostřednictvím ESET LiveGuard Advanced nebo ESET LiveGrid® nebo při kontrole e-mailů naleznete v konzoli pro vzdálenou správu v sekci **Další** > **Odeslané soubory**. Jako administrátor webové konzole máte přístup ke všem odeslaným souborům. Pokud nemáte ESET LiveGuard Advanced aktivován, uvidíte pouze soubory zaslané do systému ESET LiveGrid®.

Aby měl uživatel Web Console přístup do sekce **Odeslané soubory**, musí mít přiděleno alespoň oprávnění pro **čtení** (nad počítači).

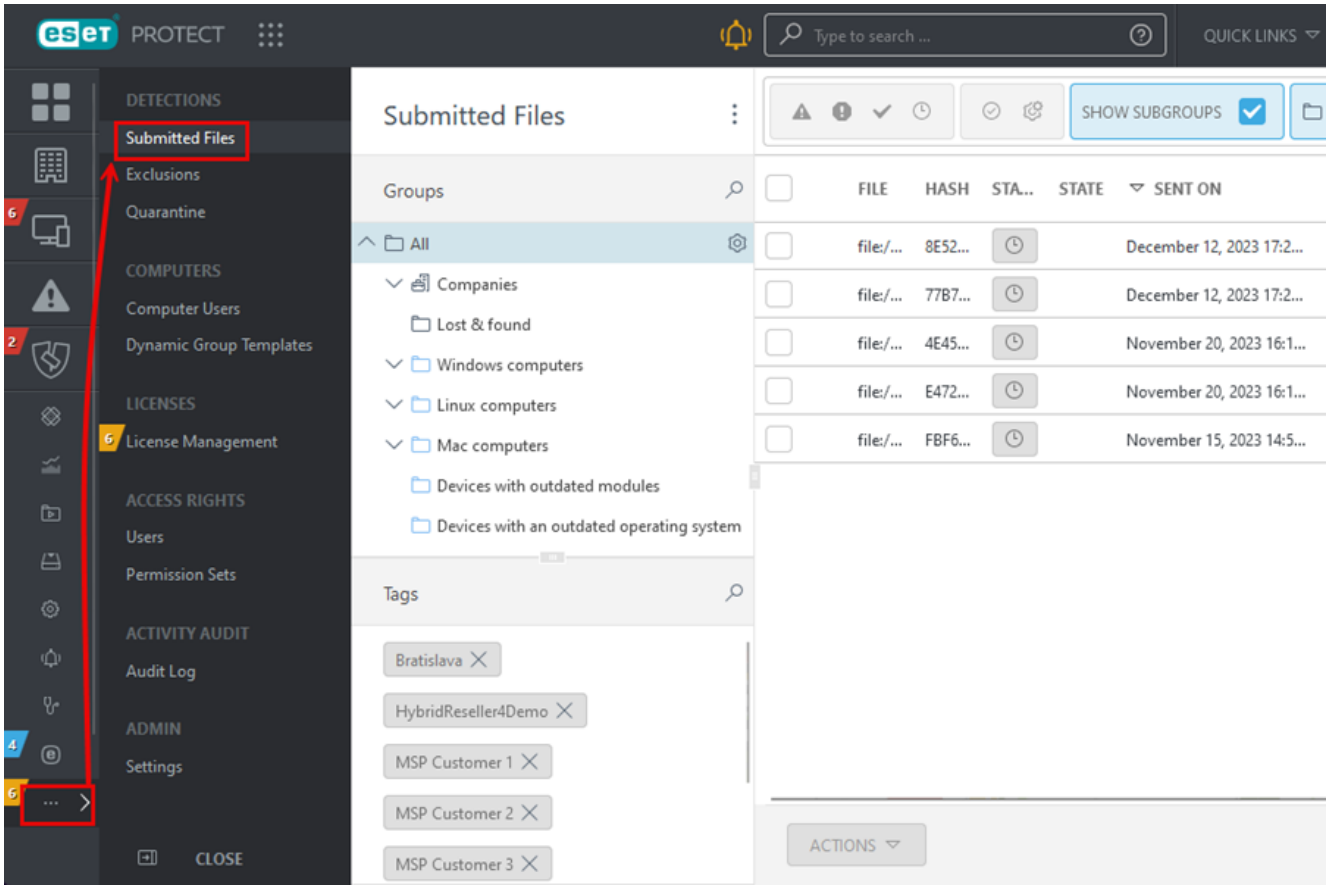
- **První odeslání** – čas, kdy byl soubor poprvé odeslán.

- **Naposledy zpracováno** – jeden soubor může být odeslán k analýze vícekrát a z více počítačů. Jedná se o čas posledního zpracování souboru odeslaného z vaší společnosti.

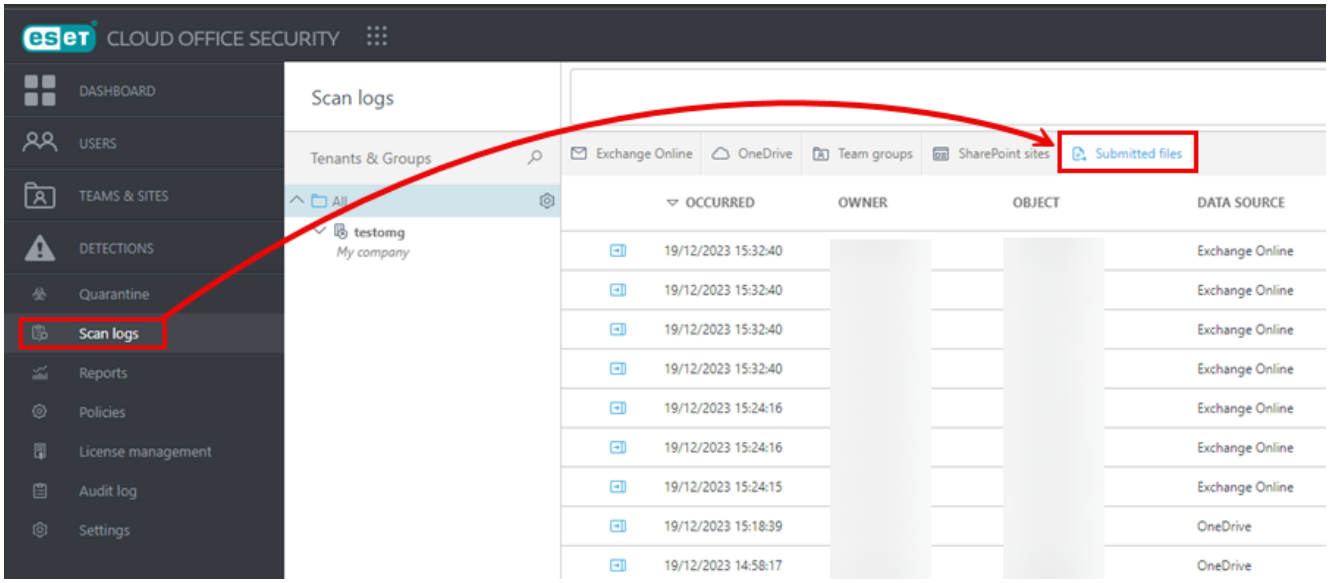
Používám ESET PROTECT On-Prem



Používám ESET PROTECT



Používám ESET Cloud Office Security

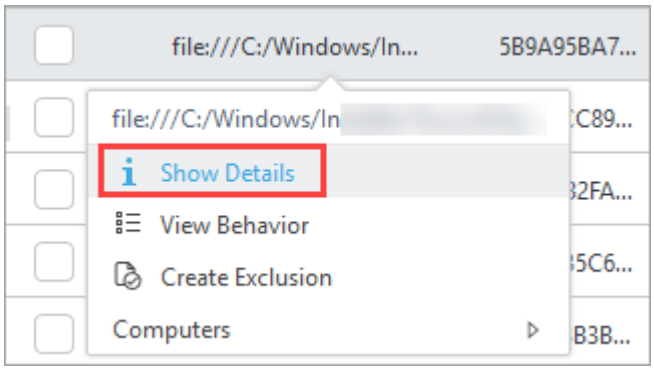


Detaily analyzovaného souboru

Detailní informace o analyzovaném souboru si zobrazíte ve webové konzoli v sekci **Odeslané soubory**.

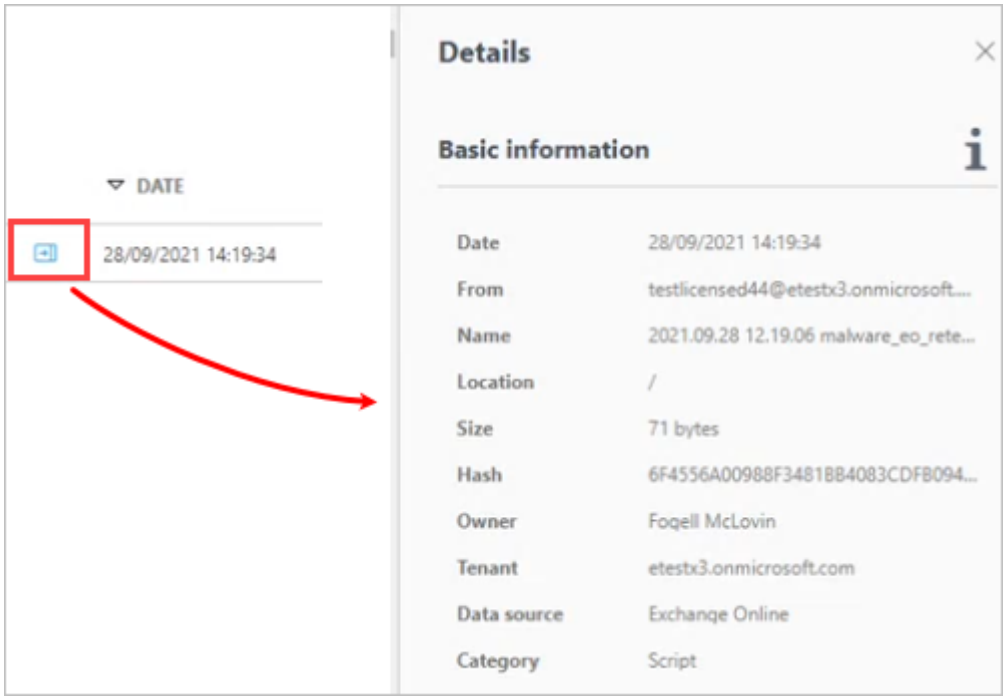
Uživatelé konzole pro správu (ESET PROTECT On-Prem)

Klikněte na konkrétní soubory a vyberte možnost **Zobrazit detaily**.



Uživatelé ESET Cloud Office Security

V sekci Odeslané soubory klikněte na modrou ikonu pro zobrazení postranního panelu s informacemi o souboru.



Linux uživatelé

ESET Server Security pro Linux:

Privilegovaní uživatelé si mohou seznam odeslaných souborů zobrazit v terminálu pomocí příkazu:

```
/opt/eset/efs/bin/lslog -n
```

nebo

```
/opt/eset/efs/bin/lslog --sent-files
```

Více informací naleznete v uživatelské příručce k ESET Server Security.

Pokud používáte webové rozhraní:

1. Přihlaste se do webového rozhraní.

2. V hlavním menu přejděte do sekce **Sent Files**.

ESET Endpoint Antivirus pro Linux:

Privilegovaní uživatelé si mohou seznam odeslaných souborů zobrazit v terminálu pomocí příkazu:

```
/opt/eset/eea/sbin/lslog -n
```

nebo

```
/opt/eset/eea/sbin/lslog --sent-files
```

Vytvoření přehledu

Přehled s daty týkajícími se ESET LiveGuard Advanced si můžete vygenerovat v konzoli pro vzdálenou správu. Využít můžete předdefinované, případně si vytvořit přehledy vlastní.

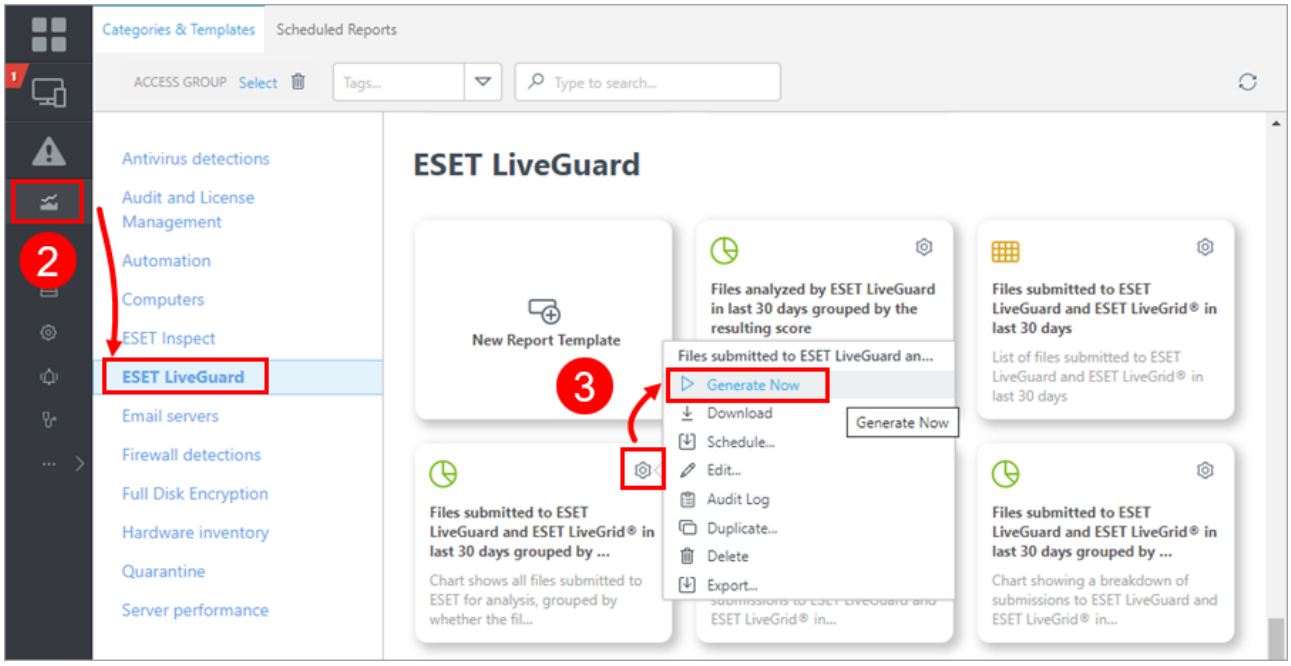
Níže uvedené kroky jsou platné pro ESET PROTECT On-Prem i ESET PROTECT.

Předdefinované přehledy

1.Přihlaste se do webové konzole.

2.V hlavním menu klikněte na záložku **Přehledy** a přejděte do kategorie **ESET LiveGuard**.

3.Vyberte si požadovaný přehled, klikněte na ikonu ozubeného kolečka a v kontextovém menu vyberte možnost **Vygenerovat**.

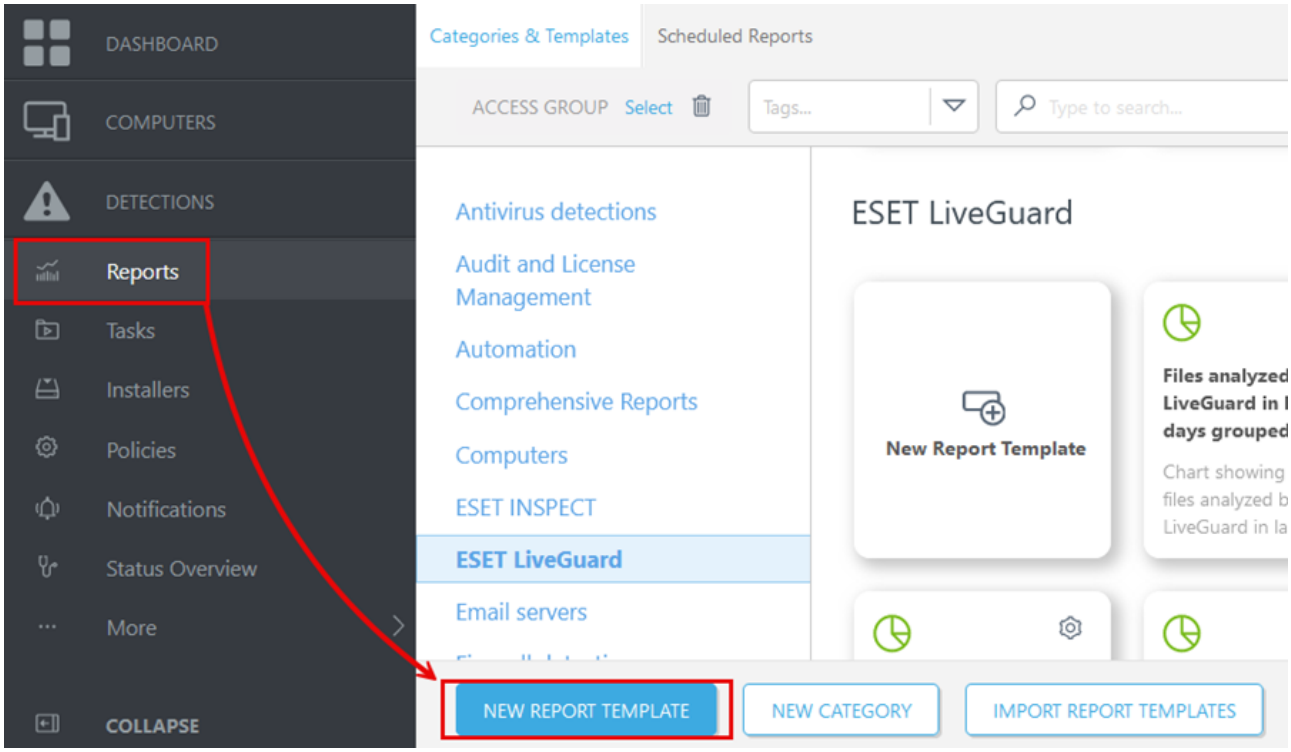


Vytvoření vlastního přehledu

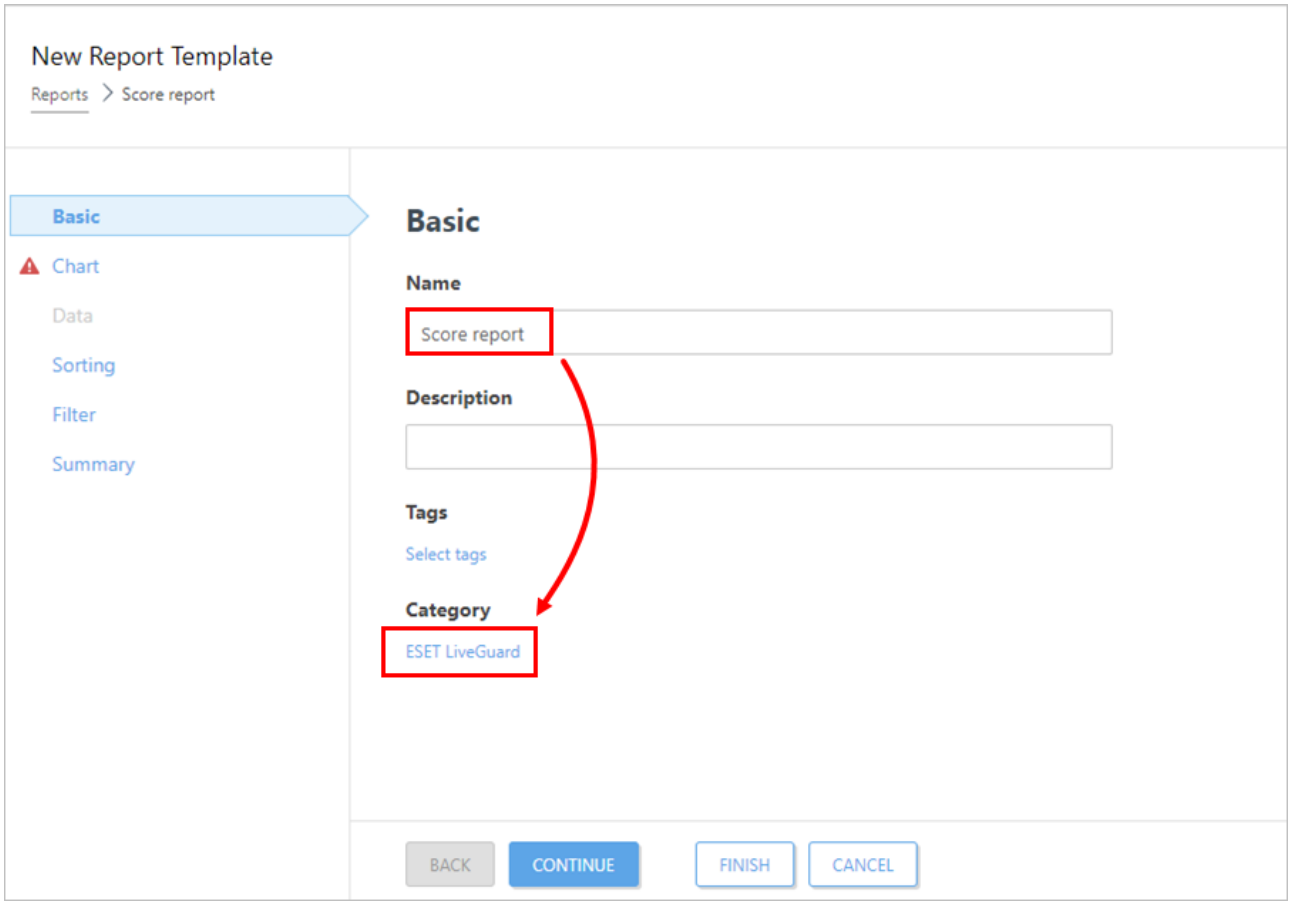
Abyste mohli vytvořit vlastní přehled, který bude obsahovat skóre, cíl a typ odesílaných souborů:

1.Přihlaste se do webové konzole.

2.V hlavním menu přejděte na záložku **Přehledy** a klikněte na tlačítko **Nová šablona přehledu**.

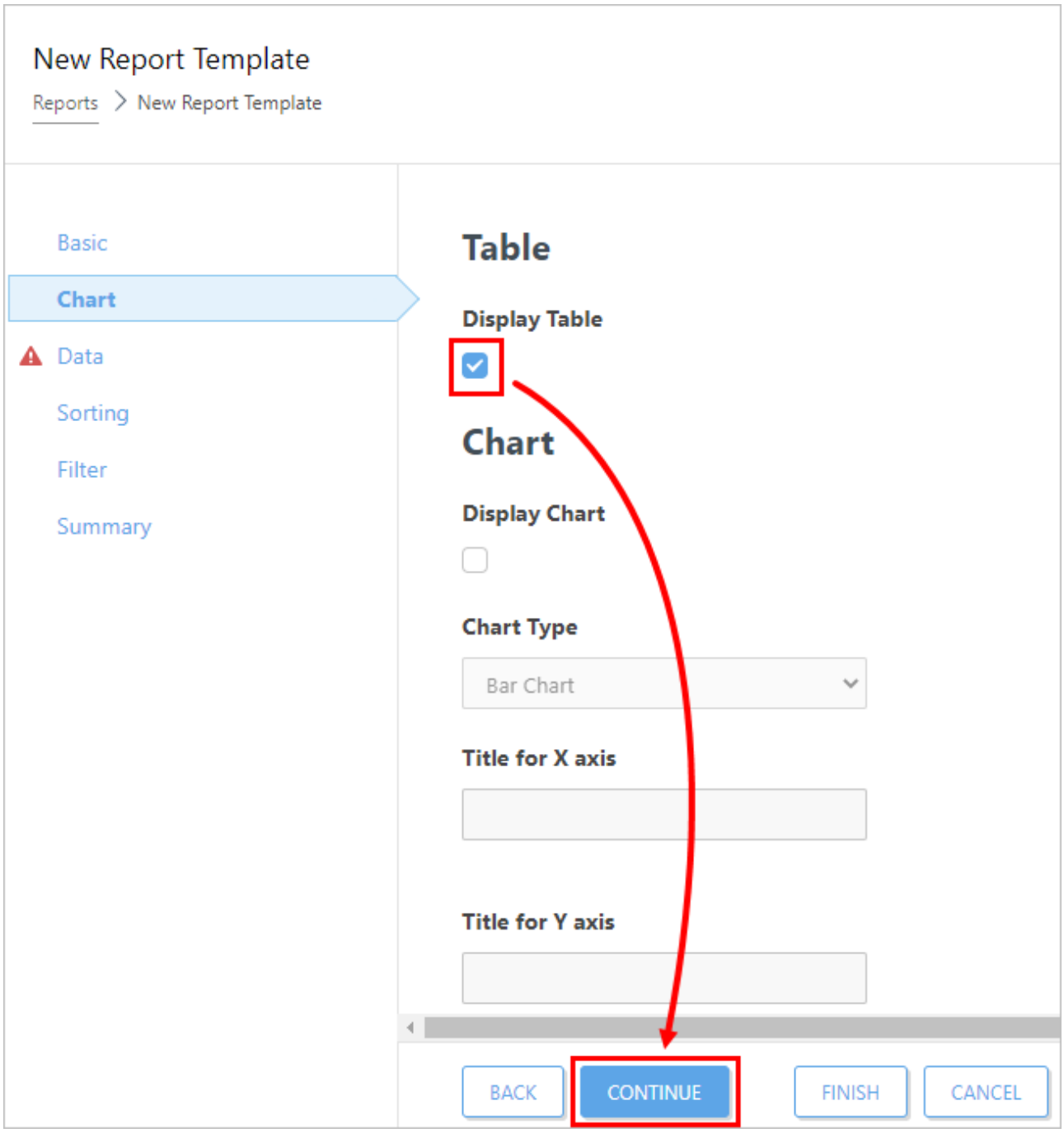


3.Zadejte **název** nové šablony a jako **kategorii** vyberte **ESET LiveGuard**.

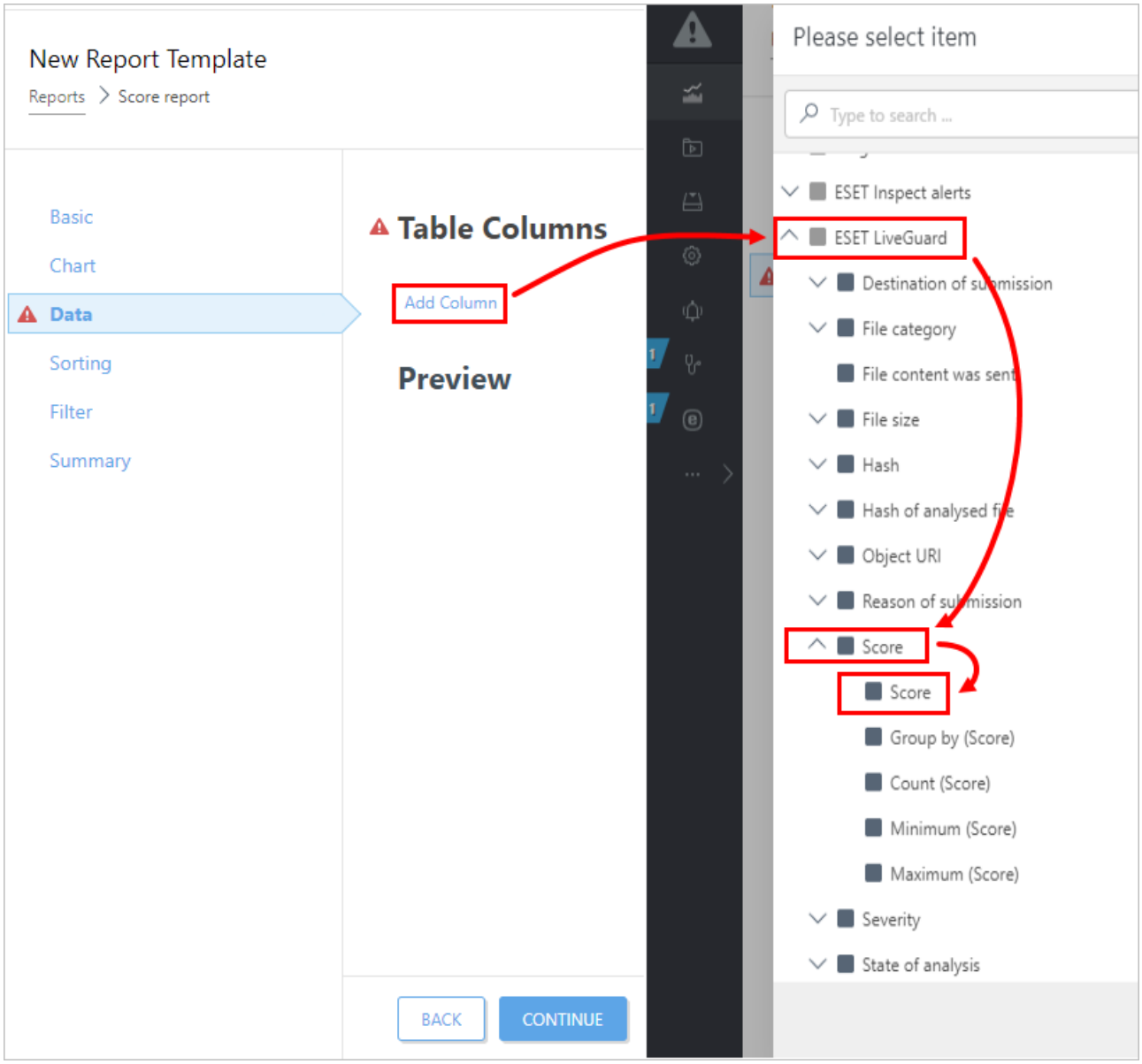


4.Klikněte na tlačítko **Pokračovat**.

5.V sekci graf zaškrtněte možnost **Zobrazit tabulku** a klikněte na **Pokračovat**.



6.Klikněte na možnost **Přidat sloupec** a zobrazeném dialogovém okně vyberte **ESET LiveGuard** > **Skóre** > **Skóre**. Pro potvrzení klikněte na tlačítko **OK**.

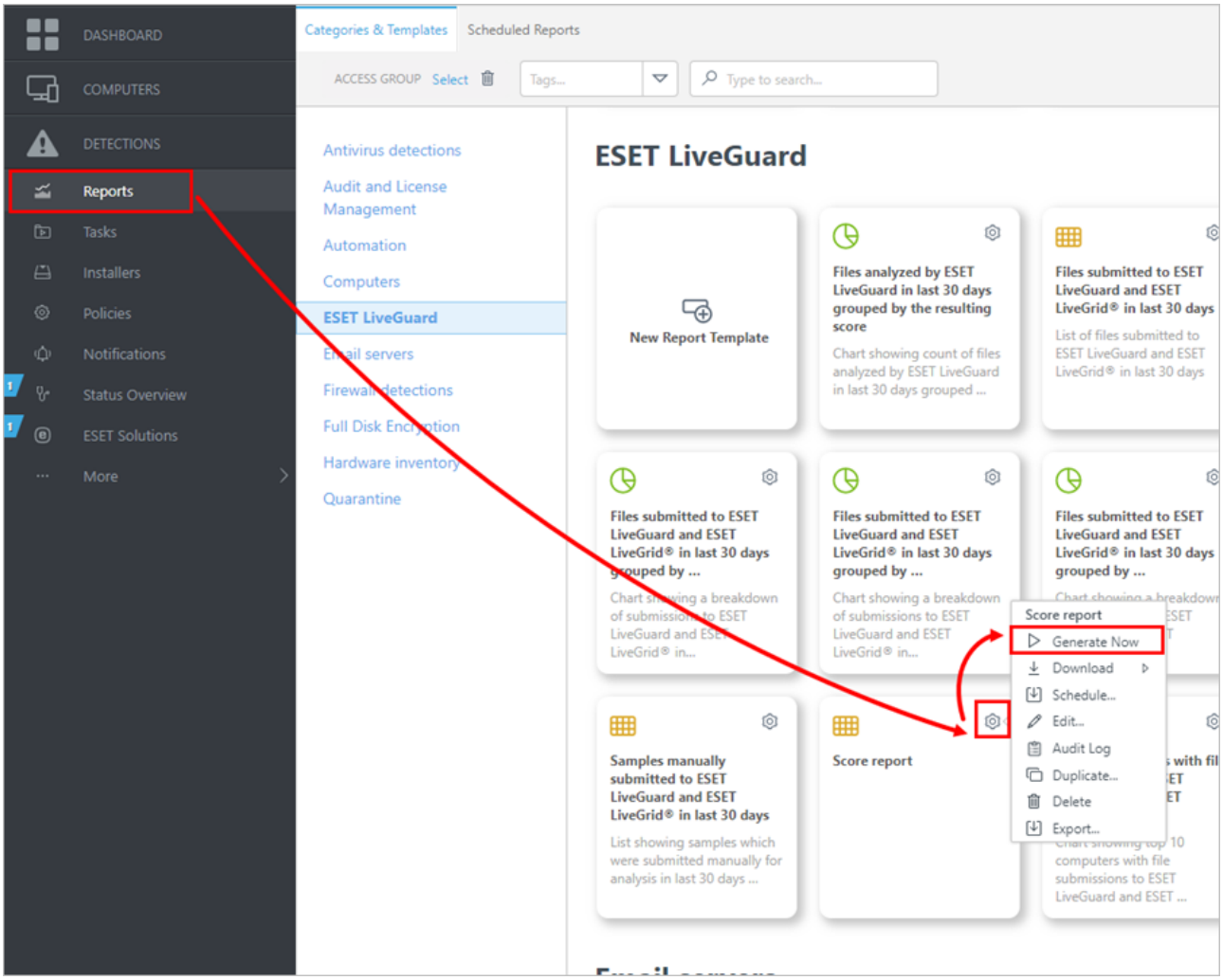


7.Klikněte na možnost **Přidat sloupec** a zobrazeném dialogovém okně vyberte **ESET LiveGuard** > **Kategorie souboru**. Pro potvrzení klikněte na tlačítko **OK**.

8.Klikněte na možnost **Přidat sloupec** a zobrazeném dialogovém okně vyberte **ESET LiveGuard** > **Cíl odeslání**. Pro potvrzení klikněte na tlačítko **OK**.

9.Pro uložení šablony klikněte na tlačítko **Dokončit**.

10. Pro vygenerování vytvořeného **přehledu** klikněte na ikonu ozubeného kolečka a v kontextovém menu vyberte možnost **Vygenerovat**.



Výsledek analýzy

Po analyzování souboru zašle cloudový systém ESET do vaší konzole pro vzdálenou správu (nebo ESET Cloud Office Security) informace o výsledku a stav souboru se změní (z **Neznámý**) na jeden z níže uvedených. Informace o souboru s krátkým popisem analýzy naleznete v **Detailech souboru**.

V ESET Cloud Office Security naleznete seznam odeslaných souborů společně s informací o výsledku v sekci Protokoly.



Parametry souboru	Popis
Počítač	Název počítače, ze kterého byl soubor odeslán.

Parametry souboru	Popis
Uživatel	Uživatel, u zdrojového počítače, který soubor odeslal. V některých případech to může být systémový uživatel.
Důvod	Důvod odeslání (Automaticky, Ručně).
Odesláno do	Informace, do jaké části cloudového systému ESET byl soubor zaslán.
Kontrolní součet	SHA-1 a SHA-256 hashe odesílaných souborů.
Název souboru	Název souboru společně s úplnou cestou k němu v daném počítači.
Velikost	Velikost souboru.
Kategorie	Kategorie (typ) souboru. Kategorie zasílaných souborů můžete ovlivnit v konfiguraci.

Každý vzorek má dva klíčové parametry: **Stav** a **Průběh**

Průběh reprezentuje aktuální stav analýzy souboru.

Průběh	Popis
Odesláno do LiveGrid(R)	Soubor byl odeslán do cloudového systému ESET, ale výsledek nebude k dispozici.
Odesláno do ESET LiveGuard	Soubor byl odeslán do cloudového systému ESET k analýze prostřednictvím ESET LiveGuard Advanced.
Analyzování	Analýza probíhá.
Dokončeno	Soubor byl úspěšně analyzován.
Opětovné analyzování	K dispozici je předchozí výsledek, probíhá opětovná analýza.

Stav reprezentuje výsledek analýzy chování vzorku.

Ikona	Stav	Skóre	Popis
	Neznámý		Soubor nebyl zatím analyzován.
	Čistý	1 - 74	Detekční jádro označilo vzorek jako čistý.
	Podezřelý	75 - 89	Detekční jádro vyhodnotilo soubor jako podezřelý, ale nelze zcela rozhodnout, zda je skutečně škodlivý.
	Velmi podezřelý	90 - 99	
	Škodlivý	100	Chování souboru je považováno za škodlivé.

Doporučení pro uživatele, kteří mají podezřelý vzorek

Pokud byl soubor vyhodnocen jako škodlivý nebo velmi škodlivý, zvažte následující akce:

- pokud máte v rámci licence přístup k přehledu o chování souboru, analyzujte jeho detaily,
- prověřte původ souboru (odkud se k vám dostal) a položte si otázku, zda je pro vás důvěryhodný,
- zkontrolujte soubor prostřednictvím externího nástroje na testování souborů na přítomnost virů, například VirusTotal,
- pokud usoudíte, že je vysoká šance útoku na vaši organizaci, nastavte Mezní hodnotu detekčního skóre na úroveň **Podezřelý**.

Přehled chování souboru

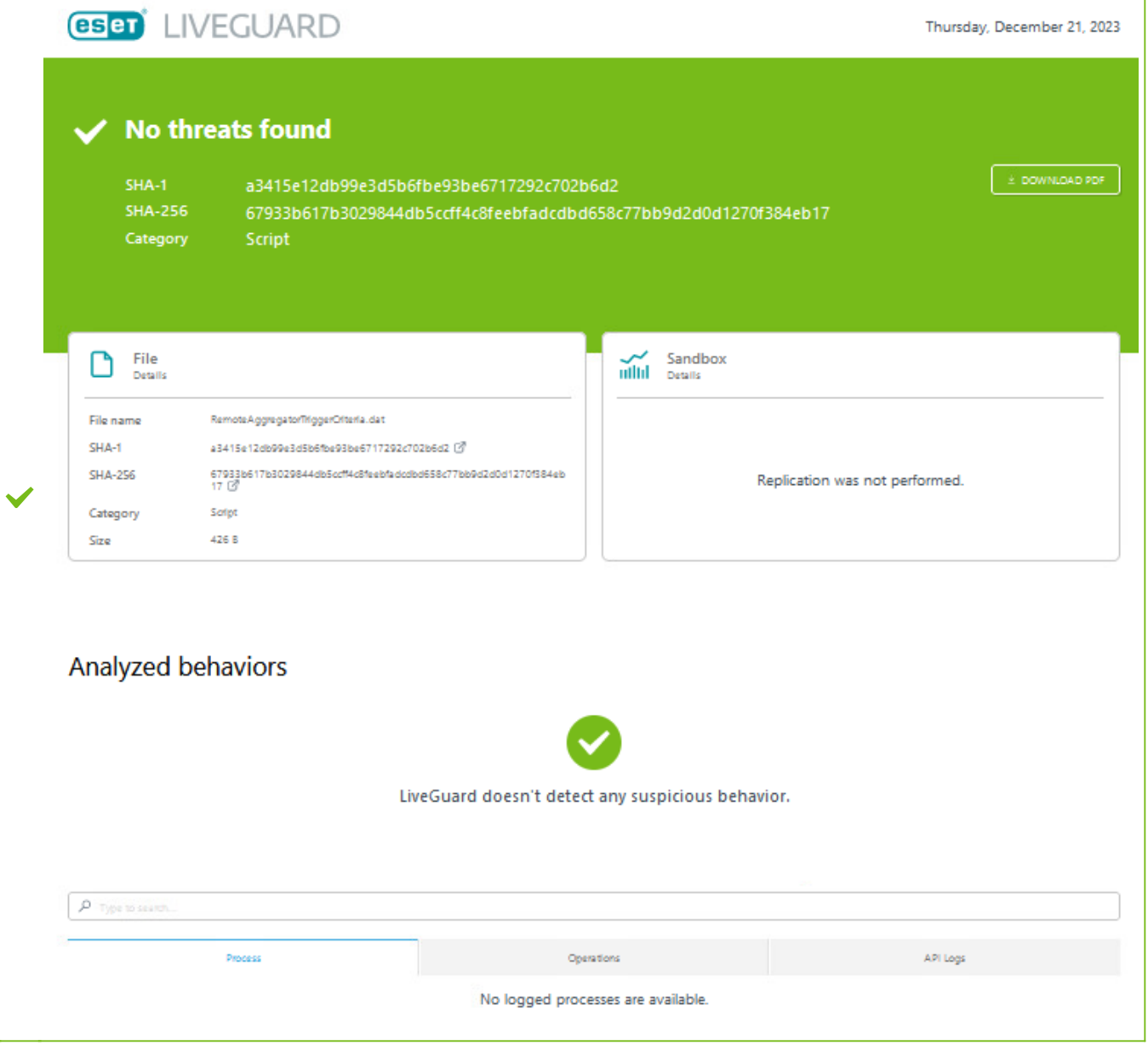
Ve webové konzoli přejděte na položku **Odeslané soubory**. Ze seznamu vyberte **soubor** a v kontextovém menu klikněte na **Zobrazit detaily** > **Zobrazit chování**. Následně se otevře přehled, který obsahuje informace o zkoumaném souboru a jeho chování zjištěné v průběhu analýzy v sandboxu. Analyzovaný vzorek může provádět více akcí.

> Kliknutím na tlačítko **Stáhnout PDF** si stáhnete Přehled chování souboru.

Přehled obsahuje následující informace:

1. **Výsledek** – finální rozhodnutí
2. **SHA-1 hash**, který obsahuje odkaz do VirusTotal
3. **SHA-256 hash**
4. **Detaily souboru** – výsledky z kontrolní vrstvy
5. **Detaily sandboxu** – výsledky z behaviorální vrstvy
6. **Zjištěné chování** – seznam detekovaných aktivit vzorku společně s jejich výsledkem Po analýze si můžete projít detaily pomocí vyhledávací lišty.

Příklad přehledu o chování souboru



Ruční odeslání souboru k analýze

Podezřelé soubory jsou do cloudového systému ESET zasílány automaticky na základě konfigurace bezpečnostního produktu. Uživatel však může prostřednictvím produktu s aktivní funkcí ESET LiveGuard Advanced kdykoli k analýze zaslat libovolný soubor. Pro zobrazení detailního popisu využijte, v závislosti na použitém produktu, jeden z níže uvedených odkazů.

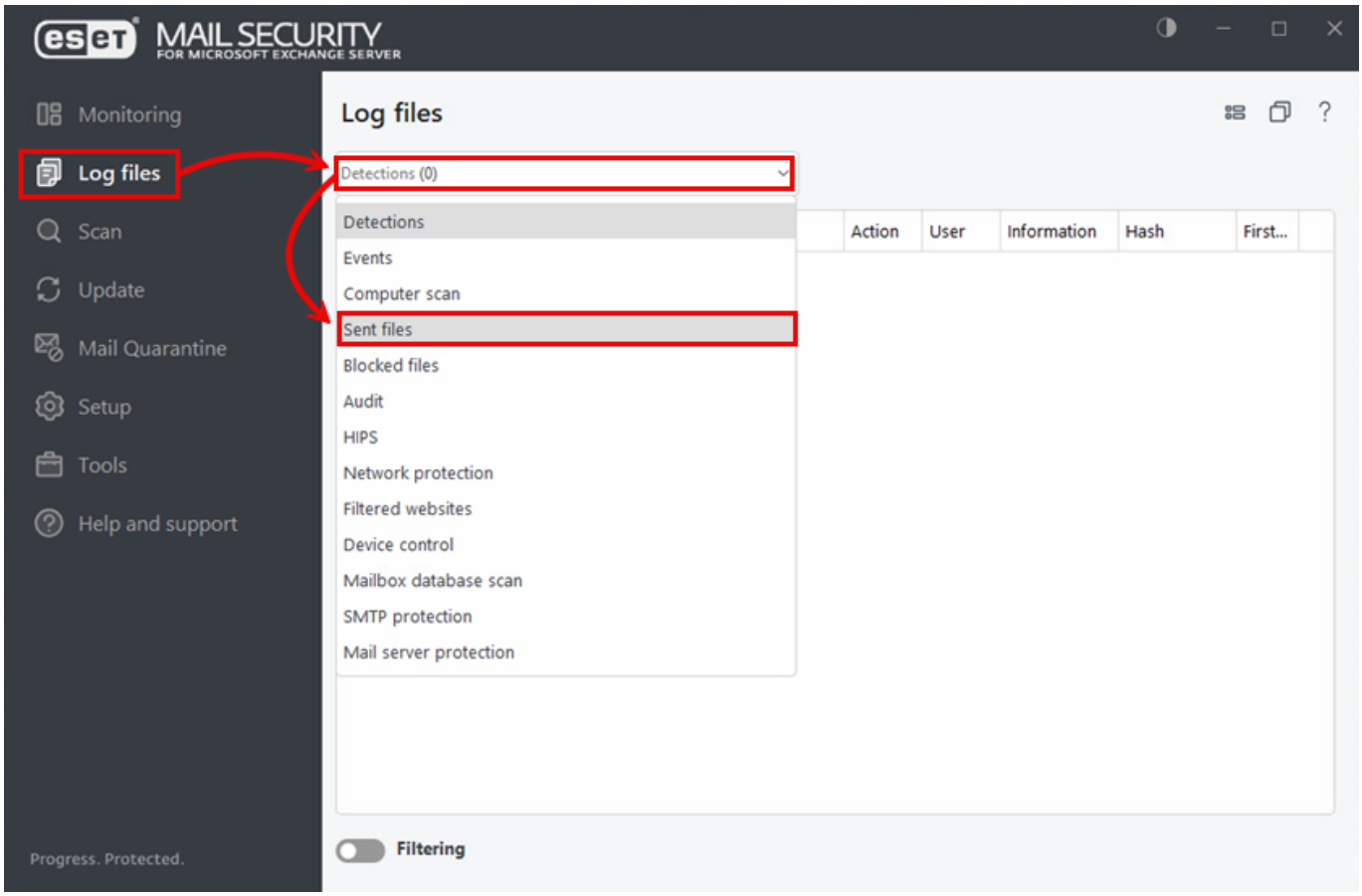
- Odeslání prostřednictvím ESET PROTECT On-Prem
- Odeslání prostřednictvím ESET Endpoint Security
- Odeslání prostřednictvím ESET Server Security
- Odeslání prostřednictvím ESET Mail Security

Lokální seznam odeslaných souborů

V nainstalovaném bezpečnostním produktu ESET podporujícím ESET LiveGuard Advanced si můžete zobrazit seznam souborů zaslaných z daného počítače k analýze do cloudového systému.

Pro zobrazení seznamu souborů v produktu **ESET Server Security**, resp. **ESET Mail Security** přejděte v hlavním okně na záložku **Protokoly** a z rozbalovacího menu vyberte možnost **Odeslané soubory**.

Pro zobrazení seznamu v produktu **ESET Endpoint Security** přejděte v hlavním okně na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu vyberte možnost **Odeslané soubory**.



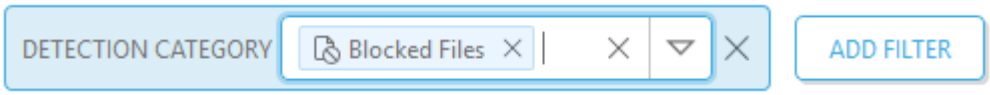
Odeslání prostřednictvím ESET PROTECT On-Prem

V ESET PROTECT On-Prem můžete k analýze odeslat **Blokované soubory** reportované ESET Inspect On-Prem. Pomocí níže uvedených kroků odešlete soubor k analýze:

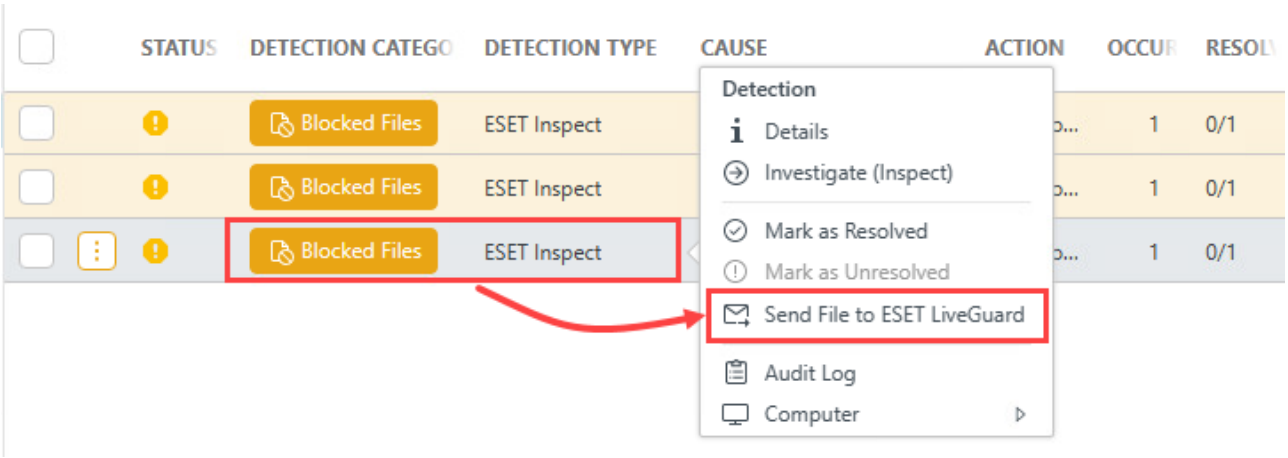
1.Přihlaste se do webové konzole.

Každý uživatel si může zobrazit, a případně k analýze odeslat, detekce ze zařízení, k nimž má na základě oprávnění přístup.

2.V hlavním menu přejděte na záložku **Detekce** a vyberte detekci, kterou chcete odeslat. Mějte na paměti, že odeslat k analýze je možné pouze soubory z **Kategorie detekce**: **Blokované soubory**.



3.V dolní části stránky klikněte na tlačítko **Odeslat do ESET LiveGuard**. Tím vytvoříte úlohu, který zajistí zaslání souboru z klientské stanice k analýze do cloudového systému ESET.



- Vzorek k analýze můžete zaslat také z klientských stanic, na kterých není ESET LiveGuard Advanced aktivován.
- Výsledek však nebude doručen uživateli a bude distribuován prostřednictvím systému ESET LiveGrid®.
- Možnost pro ruční zaslání vzorku je dostupná pouze v případě, kdy je zapnutý reputační systém ESET LiveGrid®.

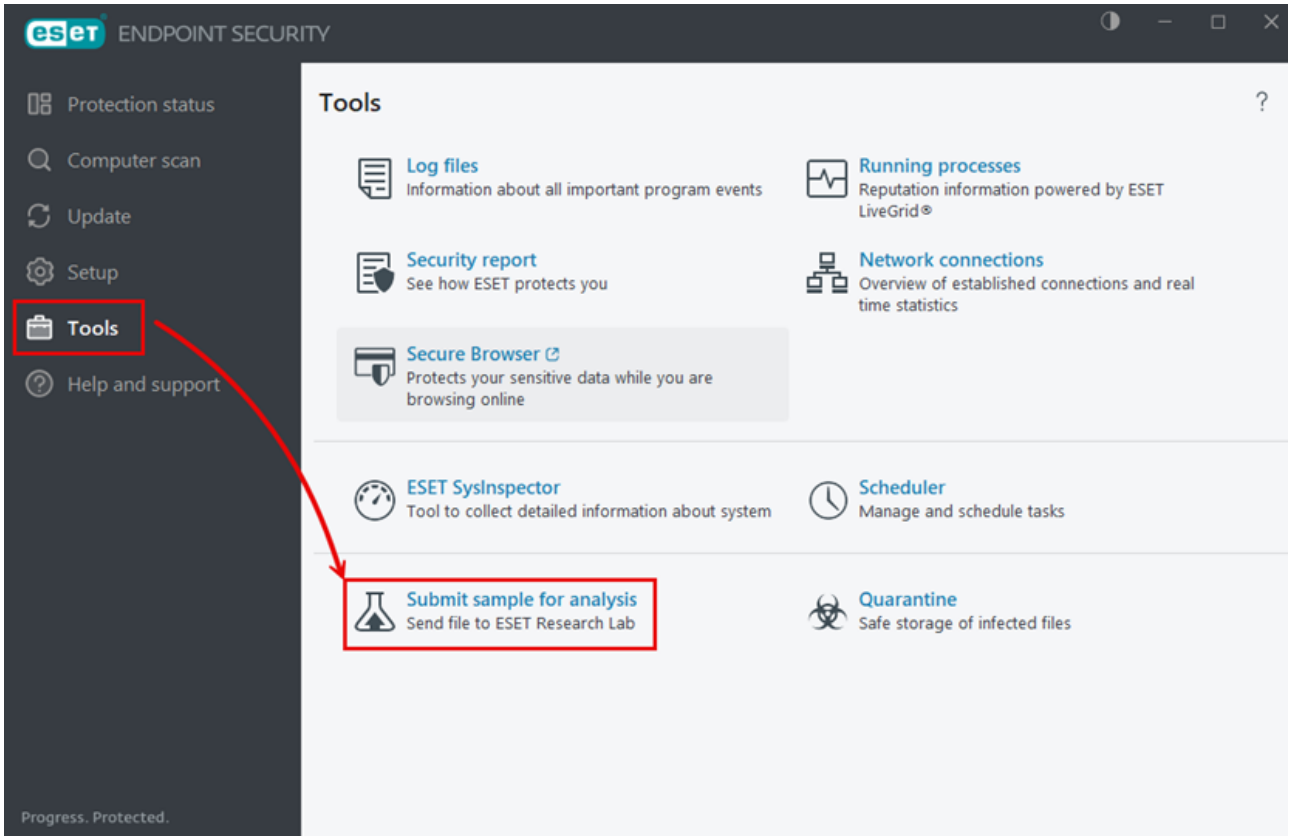
Odeslání prostřednictvím ESET Endpoint Security

Pomocí níže uvedených kroků odešlete soubor k analýze z ESET Endpoint Security:

Windows uživatelé

1.Otevřete si hlavní okno programu ESET Endpoint Security.

2.V hlavním menu přejděte na do sekce **Nástroje** a klikněte na **Odeslat vzorek k analýze**.



3.V dialogovém okně **Vyberte soubor k analýze** vyplňte povinná pole a pokračujte kliknutím na tlačítko **Další**.

4.Volitelně můžete přidat další informace o zasílaném souboru a akci dokončete kliknutím na tlačítko **Odeslat**.

Linux uživatelé

Podezřelé soubory se k analýze odesílají automaticky. Uživatelé nemají v produktu ESET Endpoint Security možnost pro ruční odeslání souboru.

- Vzorek k analýze můžete zaslat také z klientských stanic, na kterých není ESET LiveGuard Advanced aktivován.
- Výsledek však nebude doručen uživateli a bude distribuován prostřednictvím systému ESET LiveGrid®.
- Možnost pro ruční zaslání vzorku je dostupná pouze v případě, kdy je zapnutý reputační systém ESET LiveGrid®.

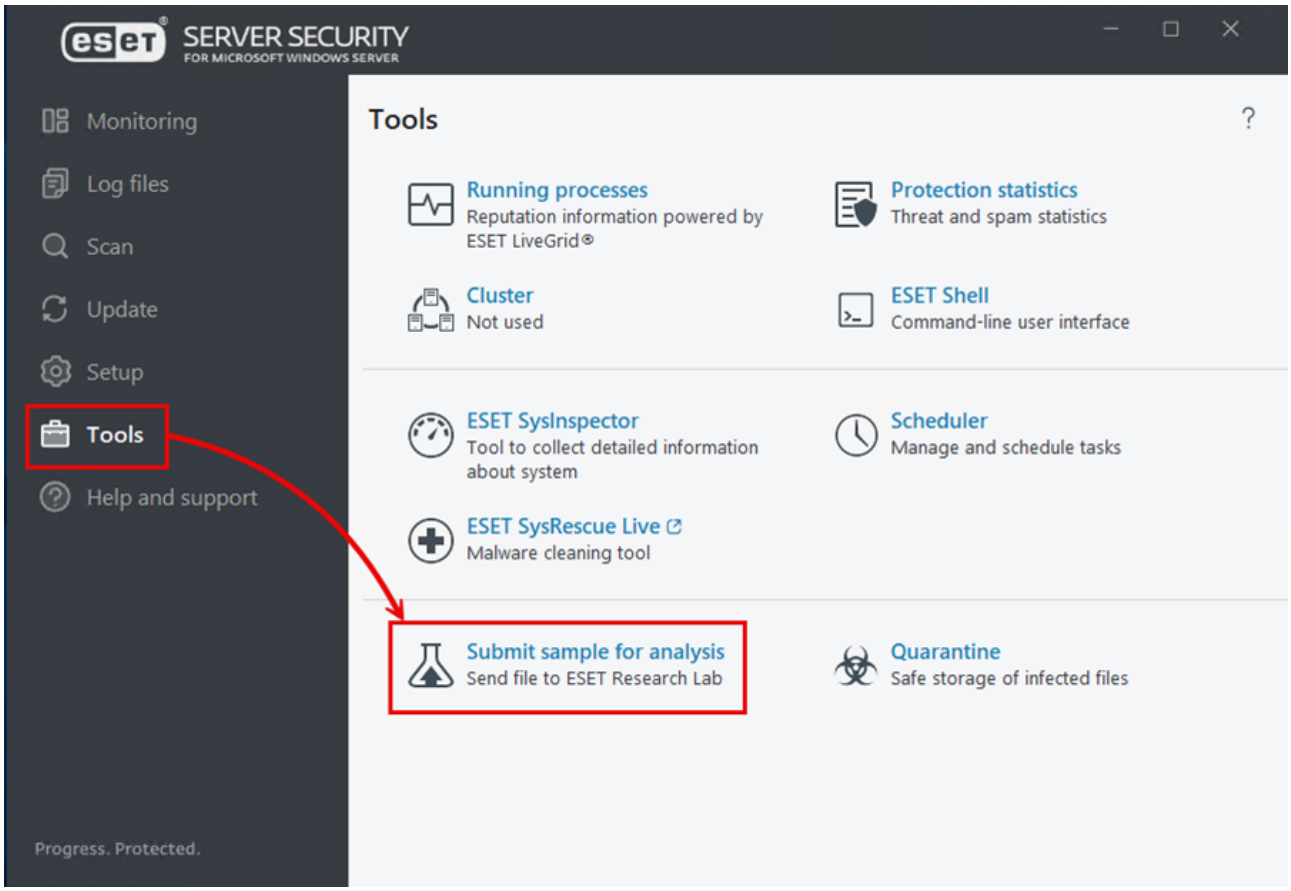
Odeslání prostřednictvím ESET Server Security

Pomocí níže uvedených kroků odešlete soubor z ESET Server Security k analýze do ESET LiveGuard Advanced.

Windows uživatelé

1.Otevřete si hlavní okno programu ESET Server Security.

2.V hlavním menu přejděte na do sekce **Nástroje** a klikněte na **Odeslat vzorek k analýze**.



3.V dialogovém okně **Vyberte soubor k analýze** vyplňte povinná pole a pokračujte kliknutím na tlačítko **Další**.

4.Volitelně můžete přidat další informace o zasílaném souboru a akci dokončete kliknutím na tlačítko **Odeslat**.

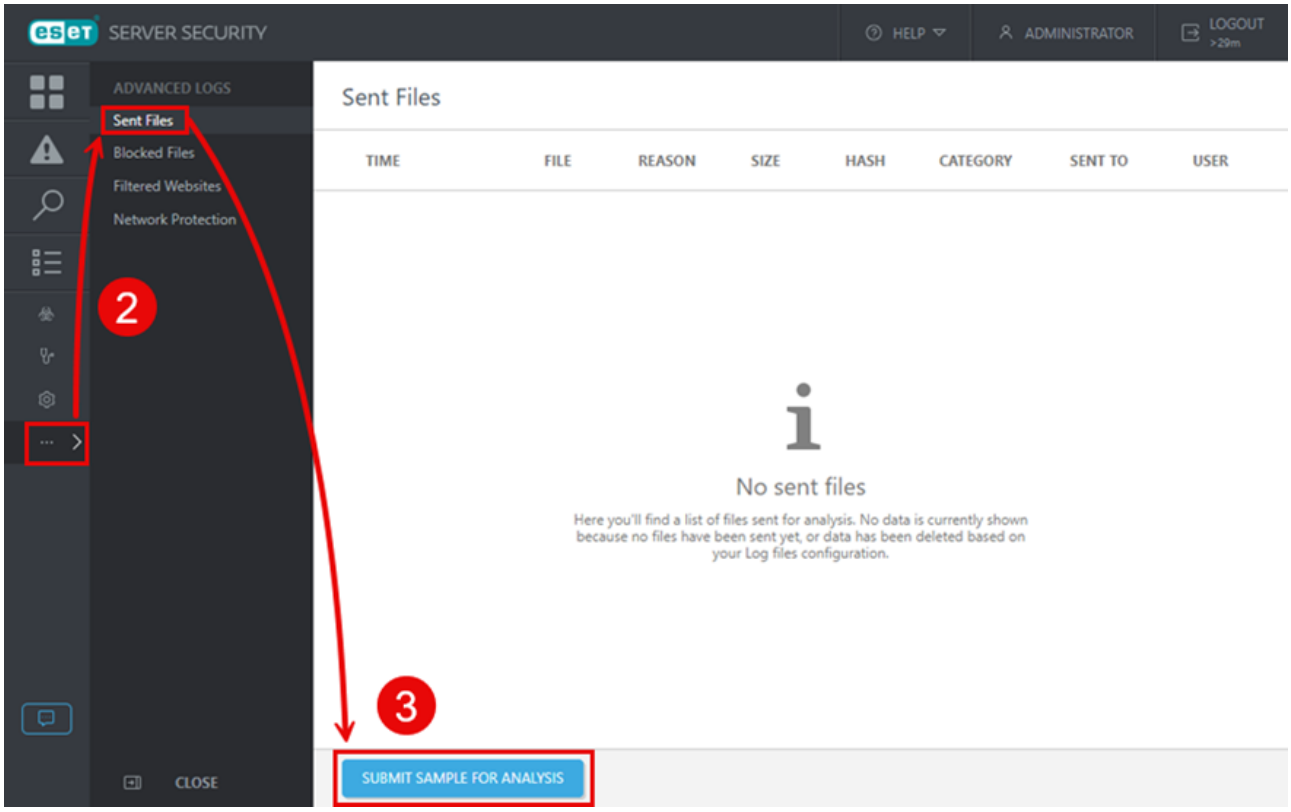
Linux uživatelé

Pro odeslání vzorku k analýze pomocí webového rozhraní:

1.Přihlaste se do webového rozhraní.

2.V hlavním menu přejděte do sekce **Sent Files**.

3.Klikněte na možnost **Submit sample for analysis**.



4.Vyberte **důvod odesílání souboru**.

5.Zadejte URL nebo cestu k souboru.

6.Zadejte svůj e-mail nebo vyberte možnost **Submit anonymously**.

7.Klikněte na tlačítko **Další**.

8.Zadejte doplňující informace.

9.Klikněte na tlačítko **Send**.

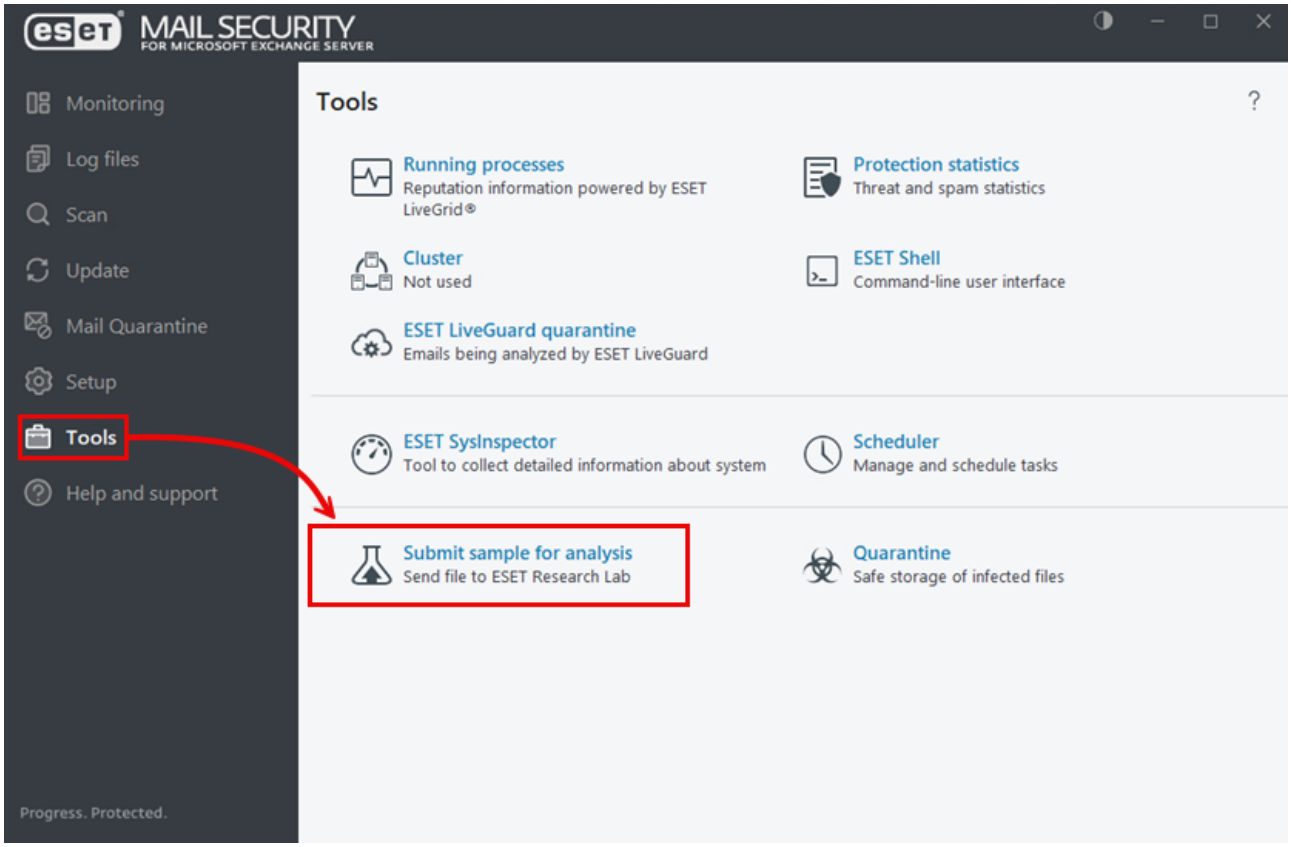
- Vzorek k analýze můžete zaslat také z klientských stanic, na kterých není ESET LiveGuard Advanced aktivován.
- Výsledek však nebude doručen uživateli a bude distribuován prostřednictvím systému ESET LiveGrid®.
- Možnost pro ruční zaslání vzorku je dostupná pouze v případě, kdy je zapnutý reputační systém ESET LiveGrid®.

Odeslání prostřednictvím ESET Mail Security

Pomocí níže uvedených kroků odešlete soubor z ESET Mail Security k analýze do ESET LiveGuard Advanced:

1.Otevřete si hlavní okno programu ESET Mail Security.

2.V hlavním menu přejděte na do sekce **Nástroje** > **Odeslat vzorek k analýze**.



3.V dialogovém okně **Vyberte soubor k analýze** vyplňte povinná pole a pokračujte kliknutím na tlačítko **Další**.

4.Volitelně můžete přidat další informace o zasílaném souboru a akci dokončete kliknutím na tlačítko **Odeslat**.

- Vzorek k analýze můžete zaslat také z klientských stanic, na kterých není ESET LiveGuard Advanced aktivován.
- Výsledek však nebude doručen uživateli a bude distribuován prostřednictvím systému ESET LiveGrid®.
- Možnost pro ruční zaslání vzorku je dostupná pouze v případě, kdy je zapnutý reputační systém ESET LiveGrid®.

Vytvoření výjimky

Standardně, pokud není analyzovaný soubor vyhodnocen jako čistý, bezpečnostní produkt automaticky provede akci definovanou v politice. Pokud je na stanici aktivní karanténa, soubor přesune do karantény (naleznete ji v hlavním menu produktu v sekci **Nástroje** > **Karanténa**). V případě potřeby však můžete pro konkrétní soubor vytvořit výjimku, pokud víte, že je skutečně bezpečný nebo jej nechcete z nějakého důvodu léčit. Výjimky vytvořené na mobilních klientech se ve webové konzoli nezobrazí dříve, než se uživatel se zařízením připojí k serveru pro vzdálenou správu.

> **Vytvoření výjimky může představovat bezpečnostní riziko**
> Po vytvoření výjimky nebude bezpečnostní produkt ESET daný soubor kontrolovat. Při vytváření výjimky byste měli být opatrní.

Požadavky pro vytvoření výjimky:

- Soubor byl zaslán k analýze do ESET LiveGuard Advanced.
- Informace o výsledku analýzy byla synchronizována se serverem pro vzdálenou správu.

Vytvoření výjimky z kontroly se skládá z následujících kroků:

1.Administrátor konzole pro vzdálenou správu přidá kontrolní součet souboru jako výjimku prostřednictvím politiky.

2.Politiku aplikuje na počítače, na kterých nemá být soubor detekován.

Pro každou výjimku můžete mít samostatnou politiku. Před přidáním výjimky již musí politika existovat.

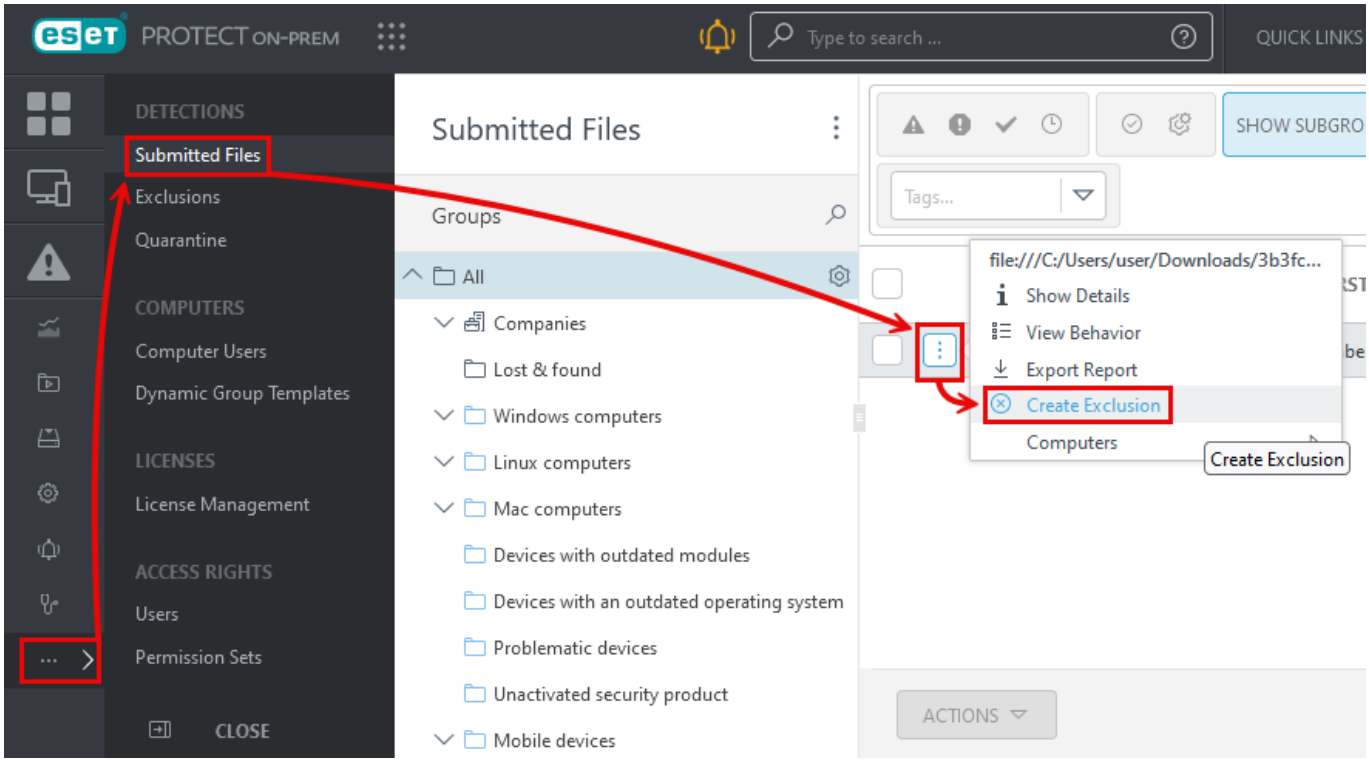
Vytvoření politiky

Vytvoření výjimky

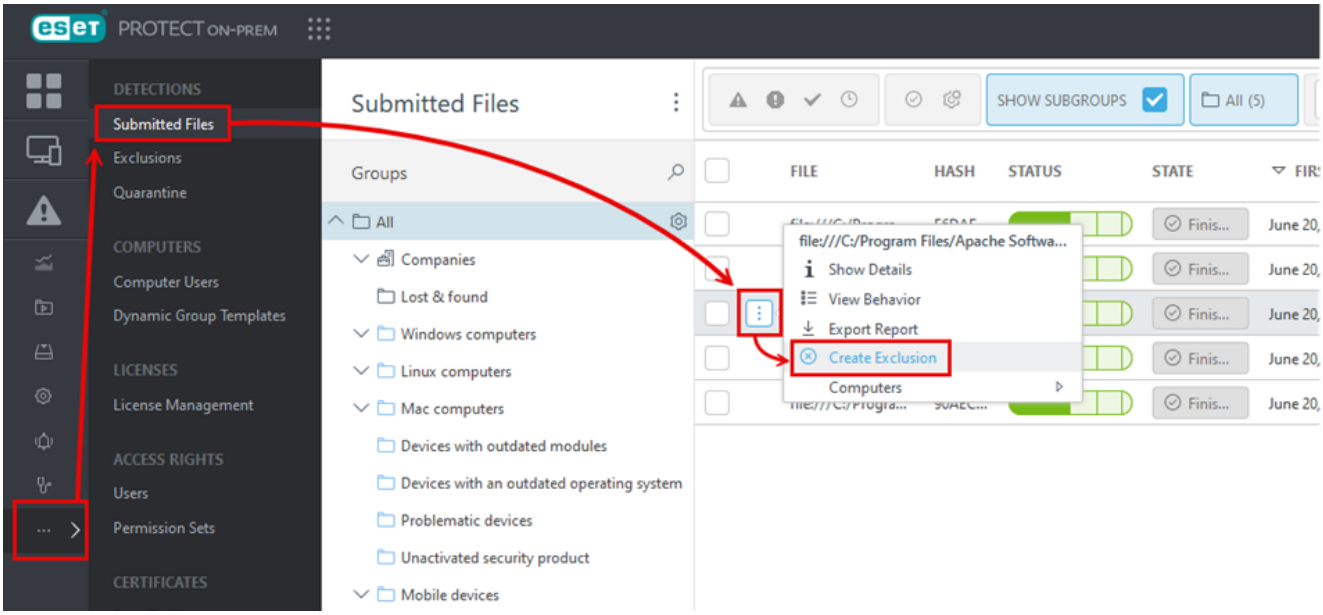
Vytvoření výjimky pro detekovaný soubor, který je ve webové konzoli uveden v sekci **Odeslané soubory**:

1.Přihlaste se do webové konzole jako administrátor nebo uživatel s oprávněním pro přístup k cílovému zařízení.

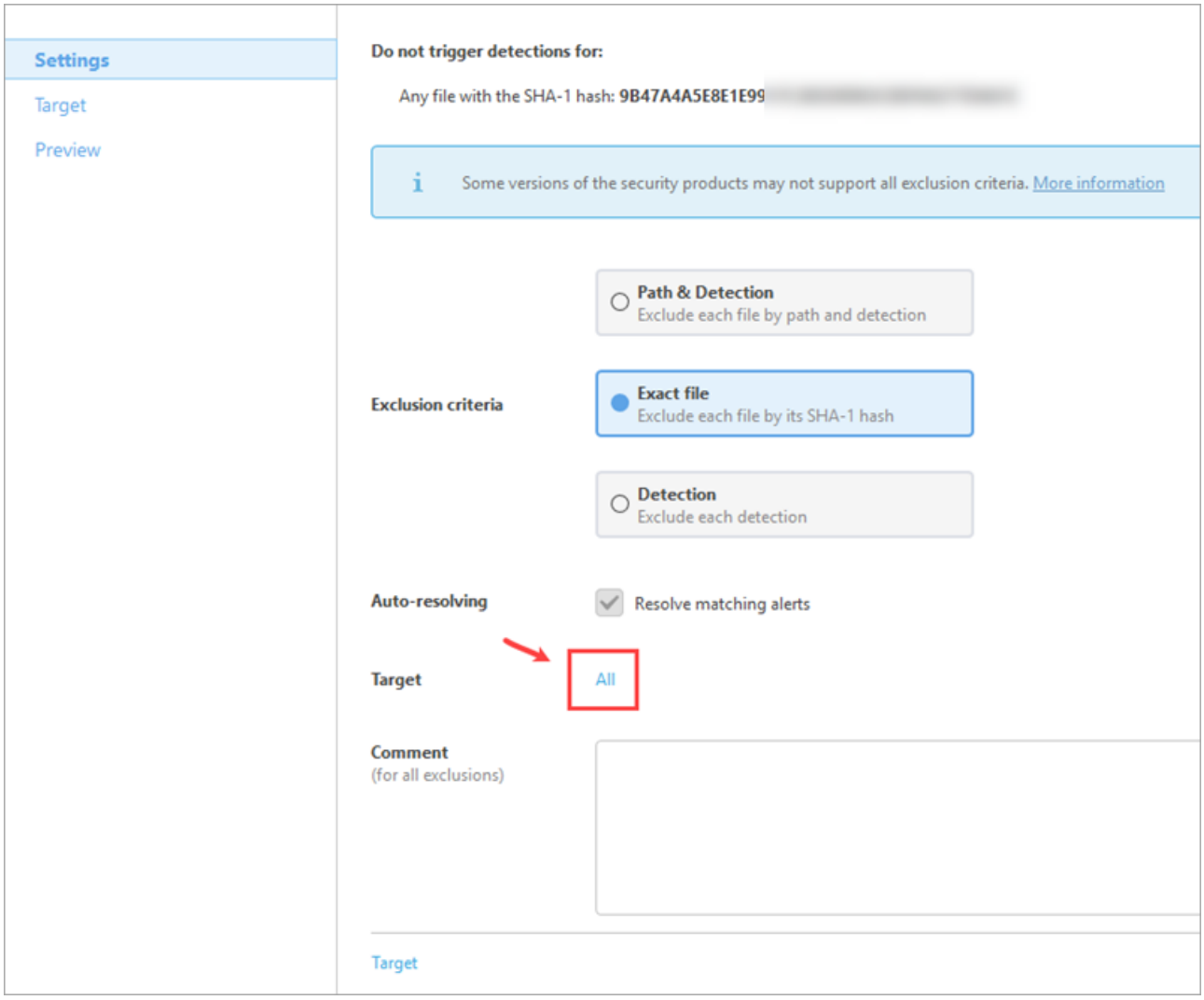
2.Přejděte do sekce **Odeslané soubory**. V zobrazeném seznamu vyberte objekt, který chcete vyloučit z detekce, a v kontextovém menu klikněte na možnost **Vytvořit výjimku**.



Používám ESET PROTECT



3.Jako **Cíl** vyberte počítač nebo skupinu, na kterou chcete výjimku aplikovat. Jako výchozí cíl je vybraná nejnadřazenější statická skupina **Všechna zařízení**. Výjimka se na cílové stanici aplikuje na všechny podporované produkty ESET.



4.Pro uložení a aplikování výjimky klikněte na tlačítko **Dokončit**. Na koncové stanice se propíše nejpozději

do dvou intervalů replikace (připojení agenta k serveru). Seznam vytvořených výjimek naleznete v sekci **Výjimky**.

Použití výjimek pro zvýšení výkonu

ESET LiveGuard Advanced je schopen automatické analýzy. Uživatel se může rozhodnout vyloučit soubory a umístění z procesu odesílání, jako jsou citlivá data nebo důvěryhodné soubory nebo umístění. Vyloučením souborů a složek můžete snížit množství zasílaných dat a tím zátěž na komponenty vaší síťové infrastruktury. Velké množství souborů zasílaných k analýze může zpomalit síťové prvky (například proxy) a prodloužit doručení výsledku analýzy. Pro snížení množství odeslaných souborů a vylepšení výkonu svého systému postupujte podle tří níže uvedených kroků.

Při vytváření výjimek z ESET LiveGuard Advanced buďte velmi opatrní. Jejím nastavením můžete vystavit systém bezpečnostnímu riziku. Vždy zvažte možné důsledky a vektory útoku.

I. Analýza odeslaných souborů

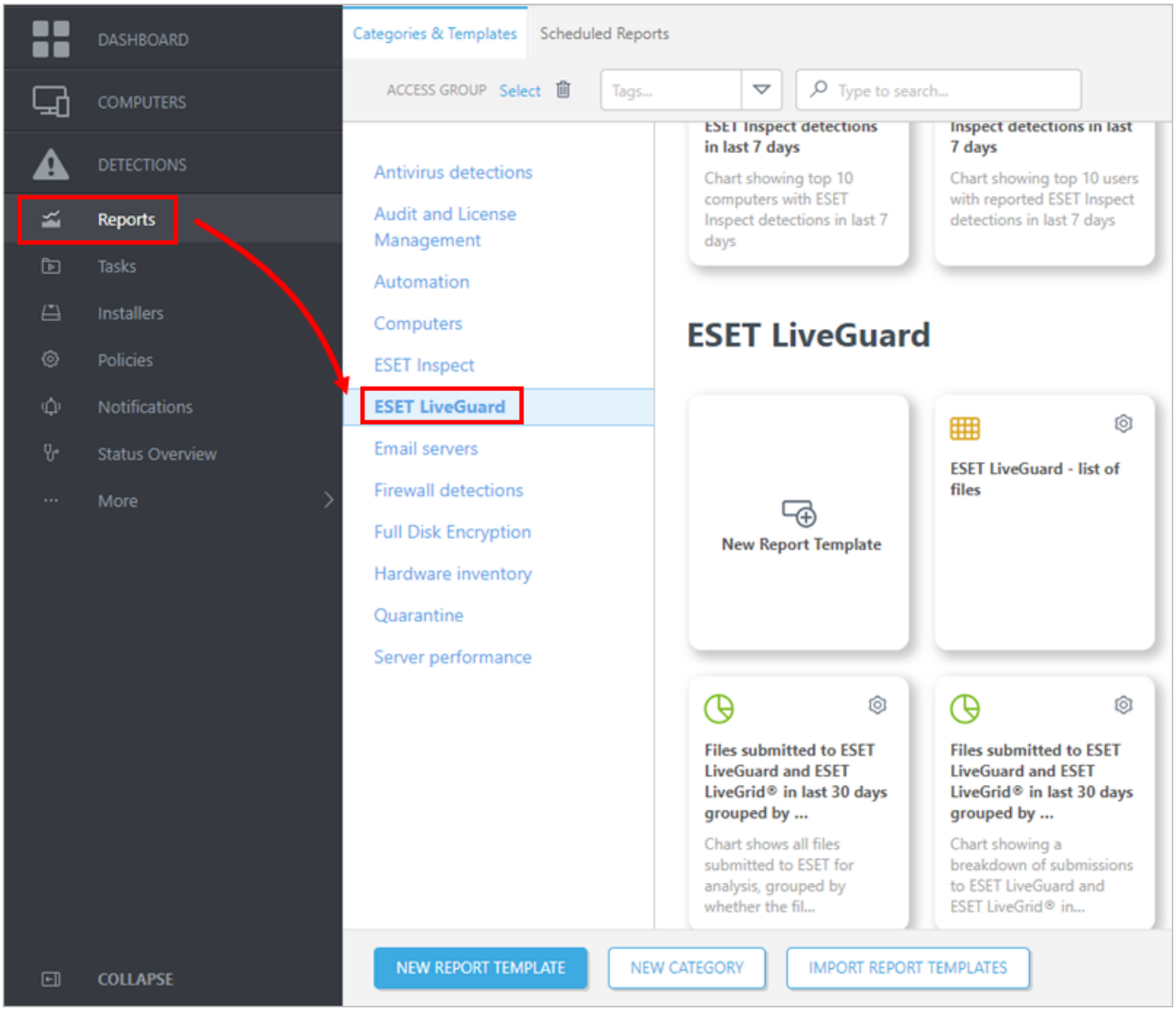
II. Vyloučení složek

III. Vyloučení procesu

Analyzování seznamu odeslaných souborů

Vytvoření seznamu počítačů nejčastěji odesílající soubory

1. V hlavním menu klikněte na záložku **Přehledy** a přejděte do kategorie **ESET LiveGuard**.



2.Najděte šablonu přehledu **Top 10 počítačů s odeslanými soubory do ESET LiveGuard a ESET LiveGrid za posledních 30 dní**.

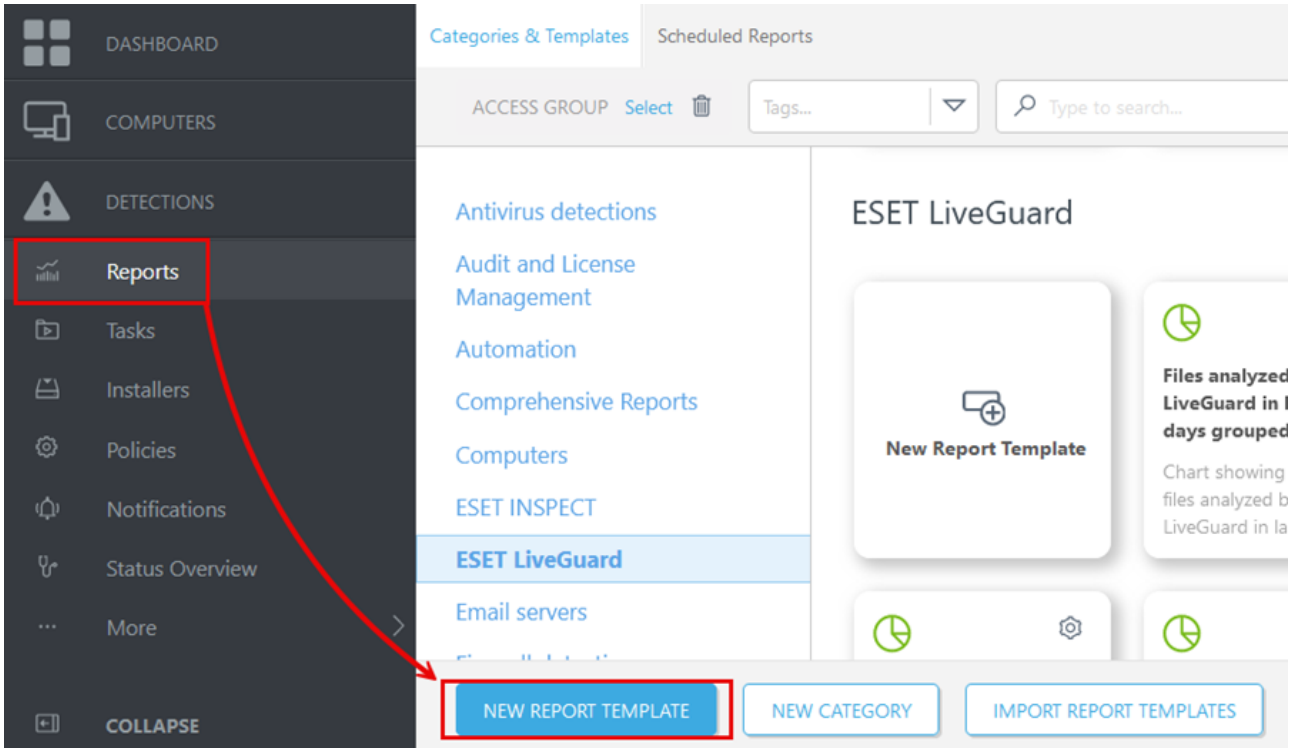
V případě potřeby si šablonu nejprve upravte a změňte počet počítačů (10) nebo časový rozsah (posledních 30 dní). Pokud to situace a vaše síť vyžaduje, upravte si šablonu dle svých potřeb.

3.Klikněte na tlačítko **Vygenerovat** a přehled si uložte (seznam počítačů).

Vytvoření seznamu odeslaných souborů z nejaktivnějších počítačů

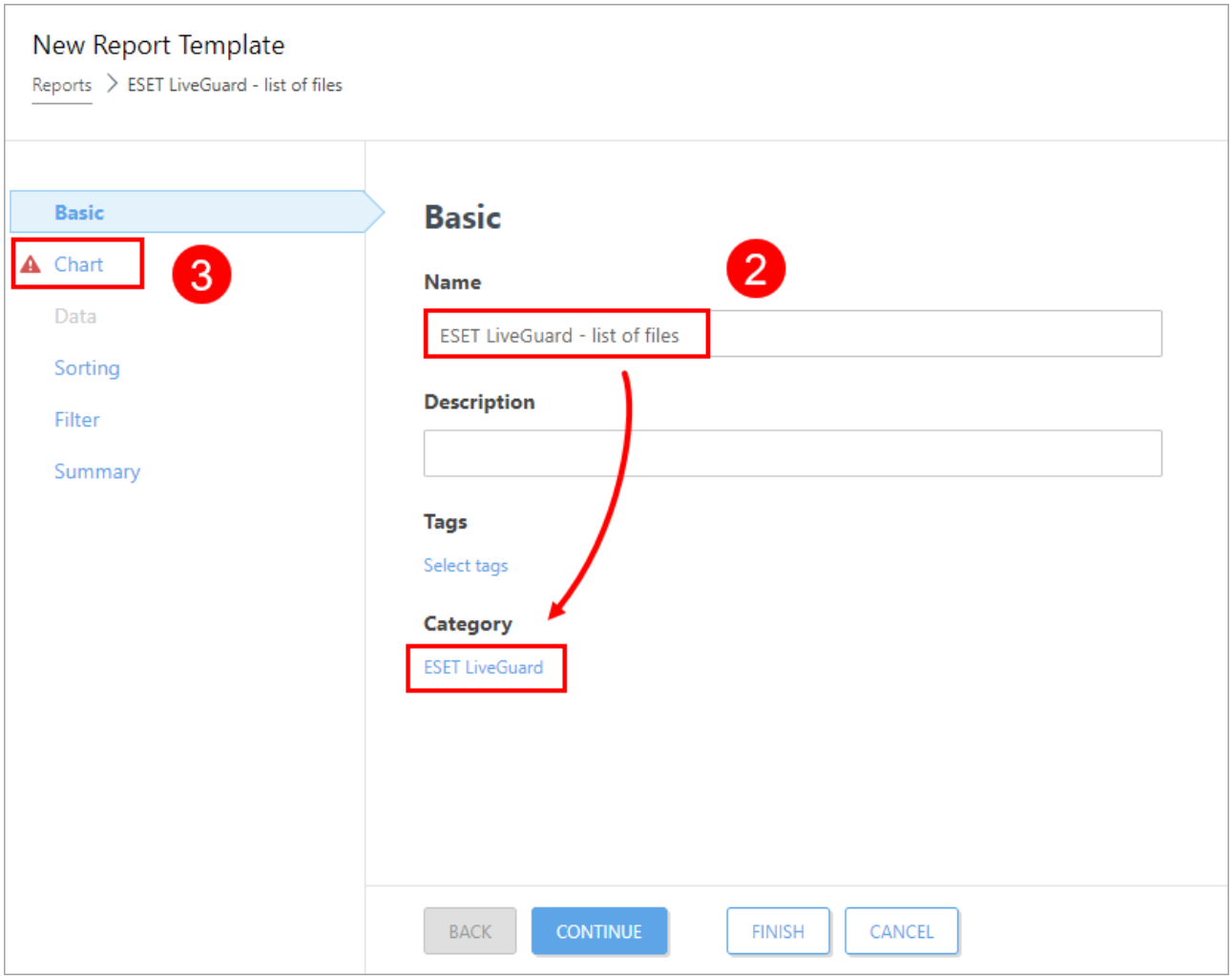
Pro dokončení níže uvedených kroků budete potřebovat výše uvedený seznam počítačů nejčastěji odesílající soubory.

1.Ve webové konzoli klikněte na **Přehledy** > **Nová šablona přehledu**.

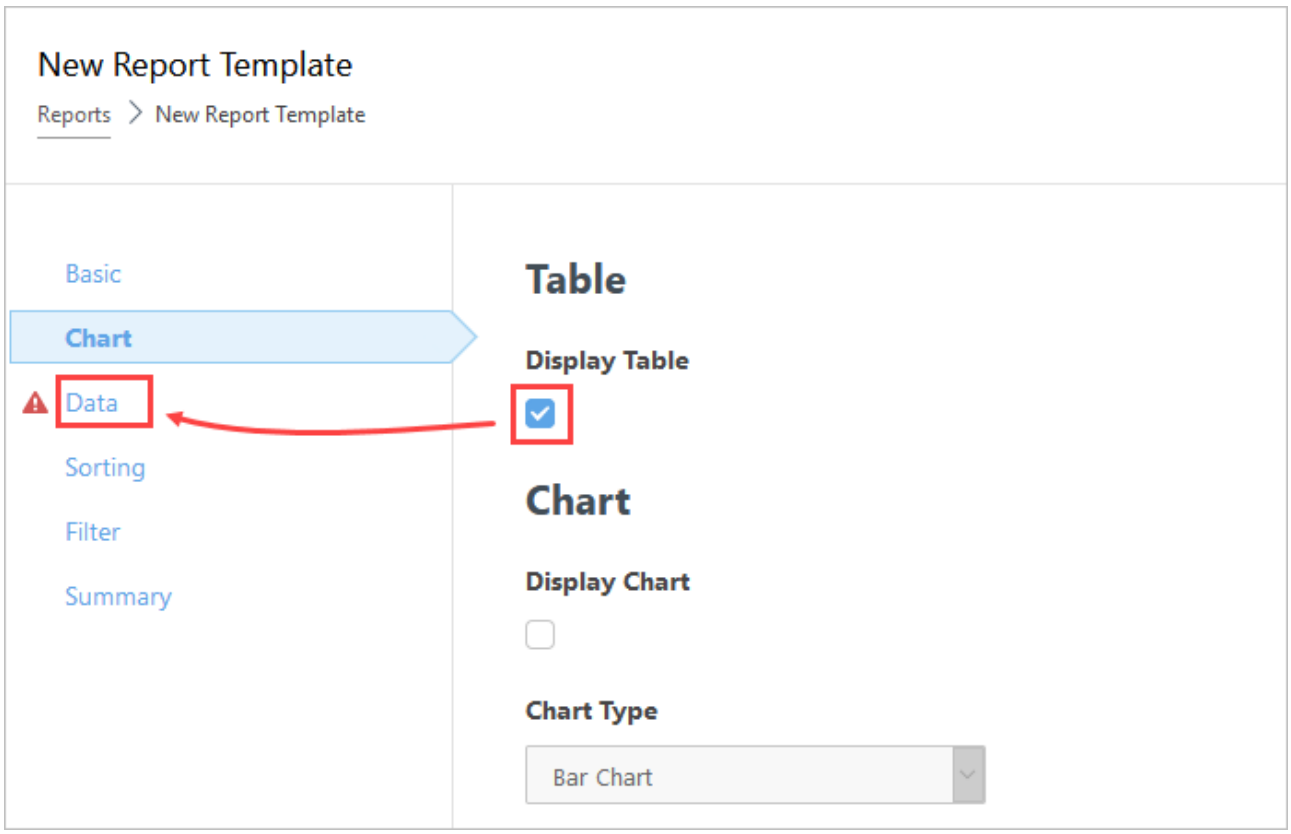


2.Šablonu si vhodně **pojmenujte** a zařaďte do požadované **kategorie**.

3.Pokračujte do sekce **Graf**.

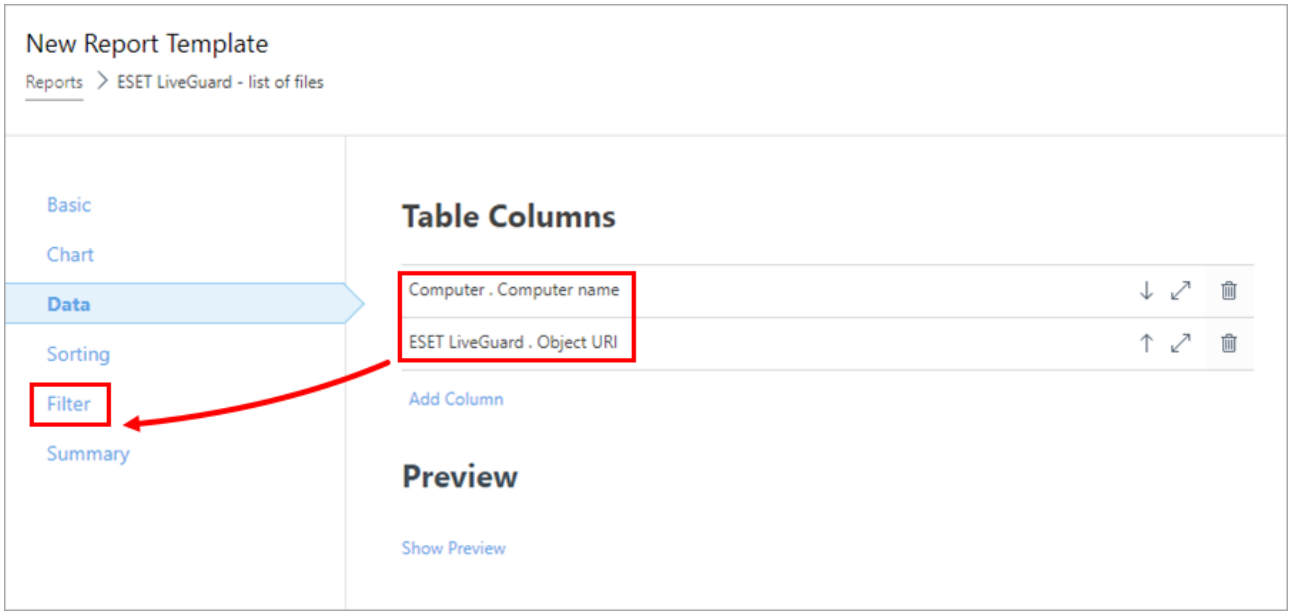


4.V sekci **Graf** vyberte pouze možnost **Zobrazit tabulku** a pokračujte do sekce **Data**.



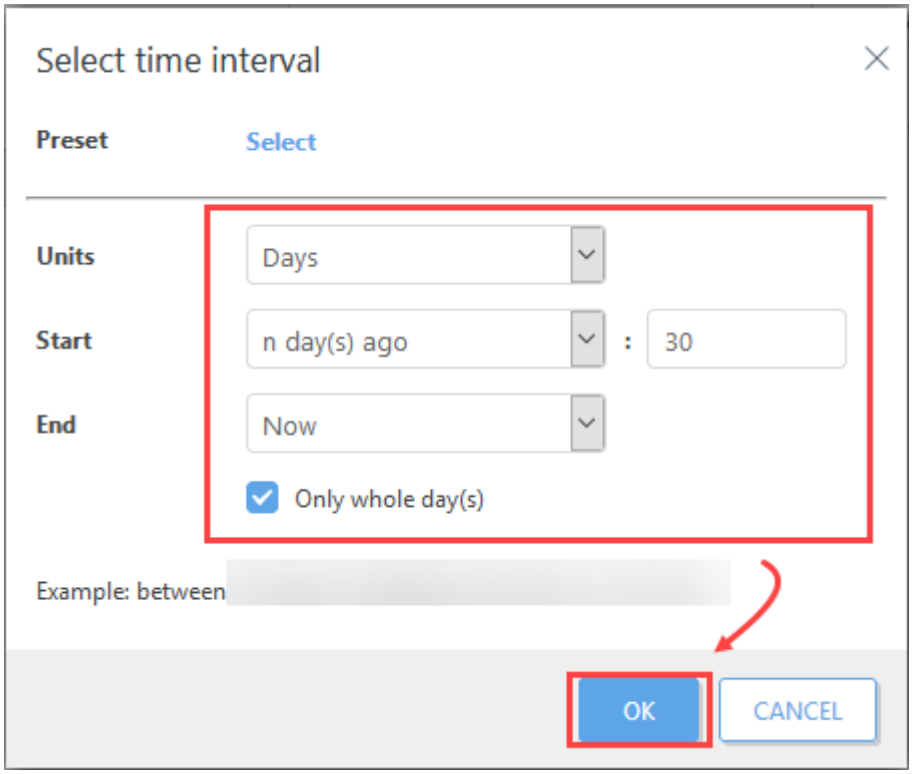
5.V sekci **Data** klikněte na **Přidat sloupec** a přidejte následující položky:
Počítač – Název počítače
ESET LiveGuard – URI objektu

6.Přejděte do sekce **Filtr**.



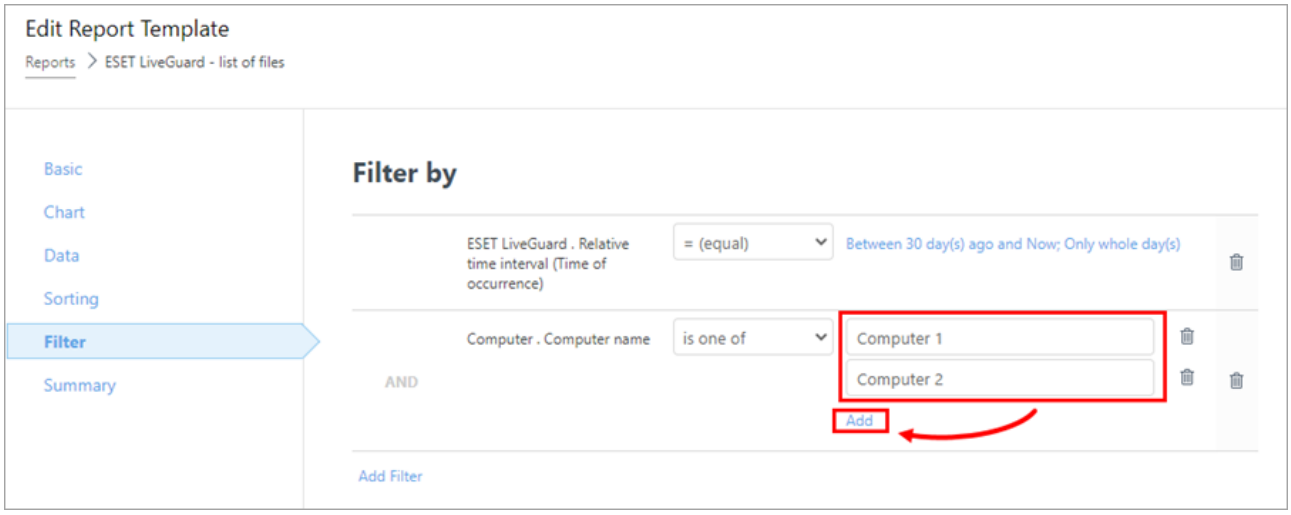
7.Klikněte na možnost **Přidat sloupec** a vyberte položku **ESET LiveGuard . Relativní interval času (čas výskytu)**.

8.Nastavte interval na posledních 30 dní, případně jinou pro vás relevantní hodnotu.



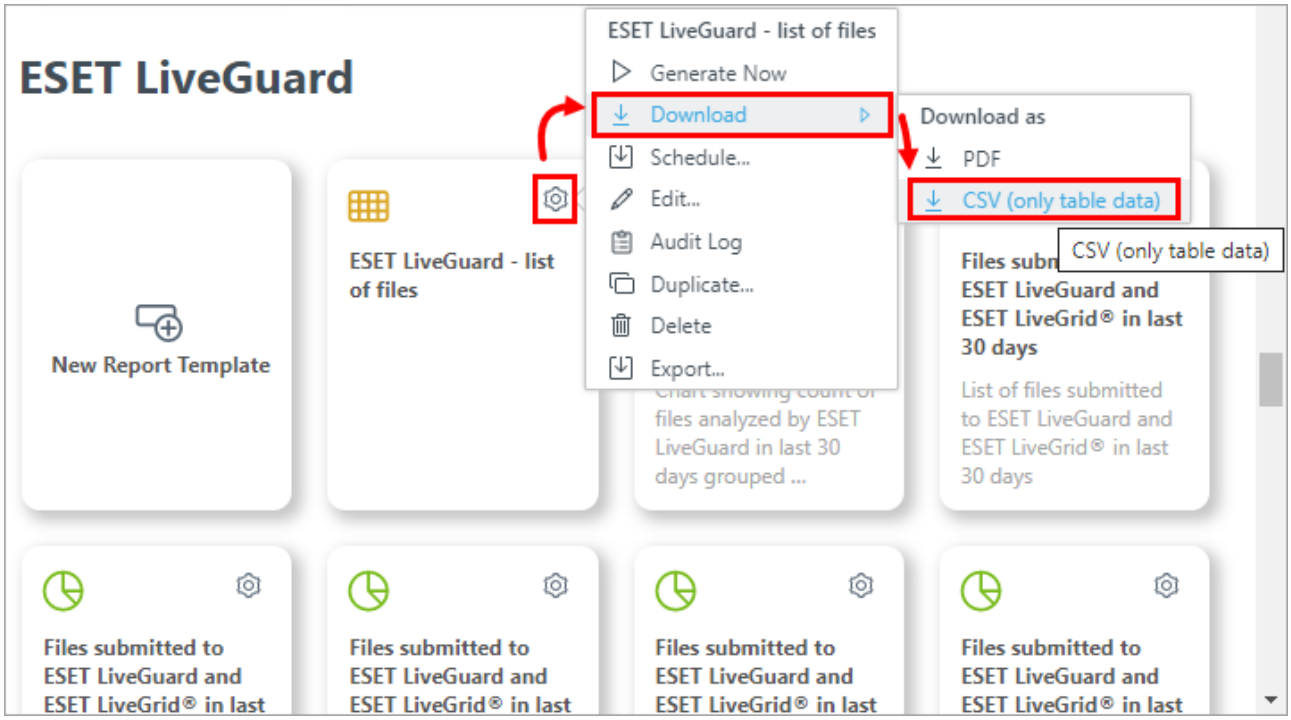
9.Znovu klikněte na možnost **Přidat sloupec** a vyberte položku **Počítač. Název počítače**.

10. Zadejte názvy všech počítačů získaných v předchozím kroku (top 10 počítačů odesílající soubory).



11. Pro uložení šablony přehledu klikněte na tlačítko **Dokončit**.

12. Najděte nově vytvořenou šablonu přehledu a vygenerujte si ji do CSV souboru.

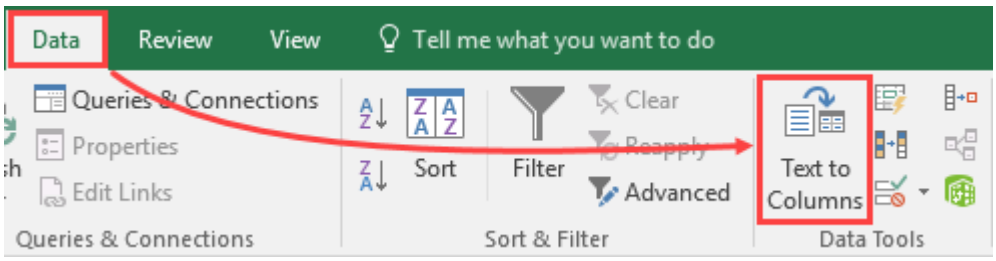


Analýza dat

Níže uvedené kroky vyžadují aplikaci třetí strany (tabulkový procesor) a základní schopnosti pro analyzování dat.

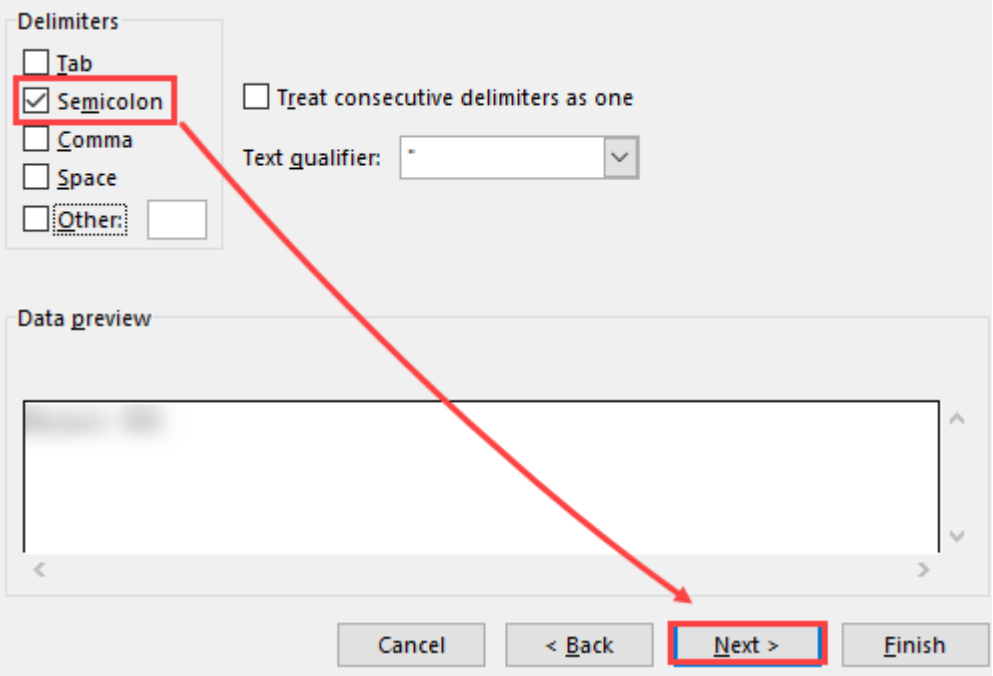
1.V tabulkovém procesoru, například MS Excel, si otevřete exportovaný CSV soubor.

2.Oddělte si data do dvou sloupců. V případě Microsoft Excel vyberte první sloupec a v hlavním menu klikněte na **Data** > **Text do sloupců**.



3.V zobrazeném dialogovém okně vyberte možnost **Oddělovač** a klikněte na tlačítko **Další**.

4.Jako oddělovač vyberte pouze **Středník** a klikněte na tlačítko **Další** > **Dokončit**.



Analyzujte data.

Hledejte vzor v odeslaných souborech a jejich umístění. Zaměřte se nejběžněji na složku, z níž je odesílána drtivá většina souborů. Jakmile vzor, podezřelý počítač nebo aplikaci, naleznete, analyzujte jej.
Odpovězte si na následující otázky:

- Jaká aplikace používá tuto složku?
- K čemu je počítač používán, čím se liší od ostatních?
- Jaký je původ těchto souborů?

Cílem je nalézt vzor, pro který by bylo možné použít pro výjimku.

Po nalezení vzoru pokračujte vyloučením složek.

Vyloučení složek

Zamyslete se nad složkami s projekty

Uživatelé používající vývojový software (například Visual Studio) mohou vyloučit složky, ve kterých kompilují své projekty. V průběhu kompilování projektu může docházet k odesílání nových souborů k analýze do ESET LiveGuard Advanced. Jejich vyloučením můžete zabránit odeslání velkého množství souborů do ESET LiveGuard Advanced. Vyloučit můžete například složku s projektem: D:\Projects*

Vytvoření výjimky na složku

Umožňuje vyjmout určité soubory nebo složky z odesílání do ESET LiveGuard Advanced. Vyloučené soubory nebudou nikdy odeslány k analýze do laboratoří společnosti ESET.

Při vytváření výjimky vždy zvažte bezpečnostní riziko. Zjistěte si, jaké aplikace mohou do vyloučeného umístění zapisovat, jak by mohlo dojít k zneužití výjimky na toto umístění.

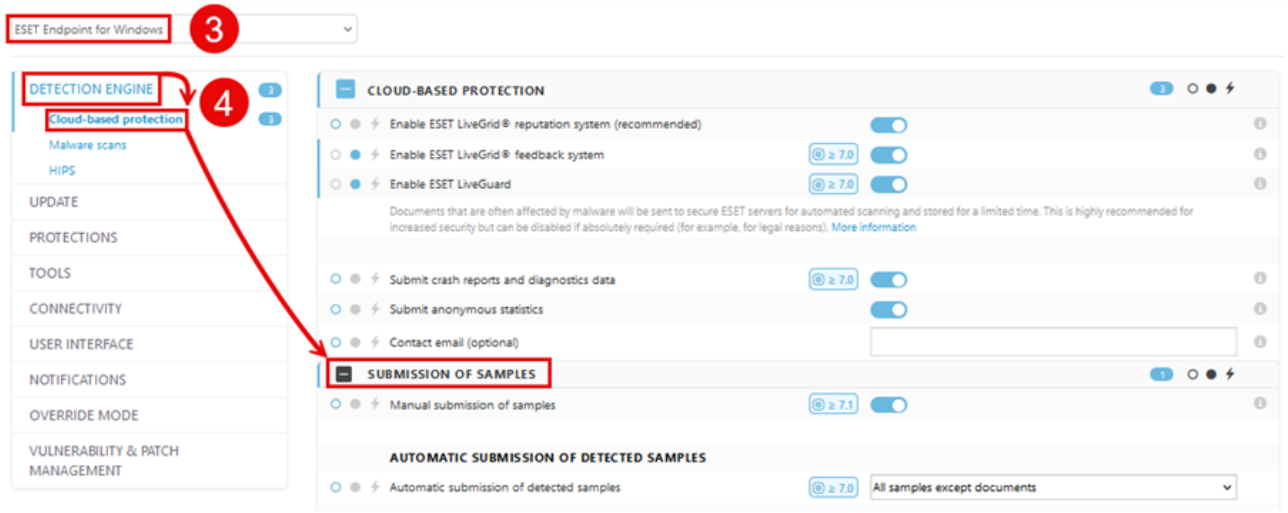
1. Přihlaste se do webové konzole, v hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová**

politika.

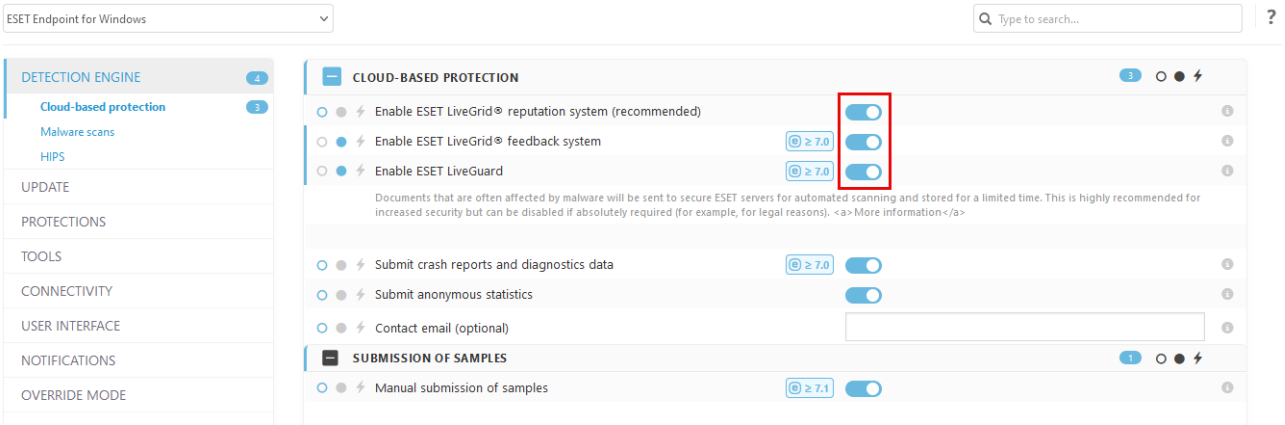
2.V sekci **Obecné** zadejte **název**, volitelně popis.

3.V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows** (nebo jiný kompatibilní produkt).

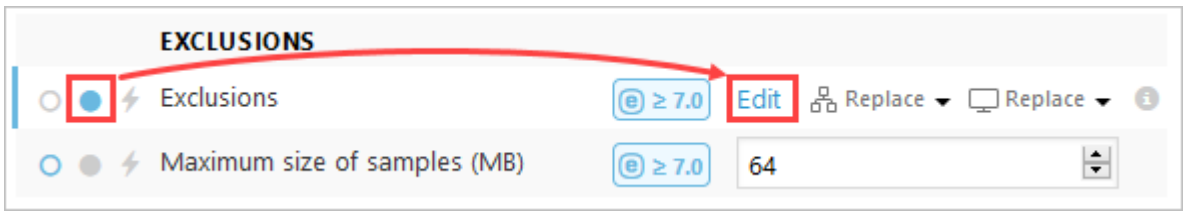
4.Přejděte do sekce **Detekční jádro** > **Cloudová ochrana**.



5.Pomocí přepínačů spusťte **ESET LiveGrid** a **ESET LiveGuard Advanced**



6.V sekci **Výjimky** klikněte na **Změnit** na řádku **Výjimky**.

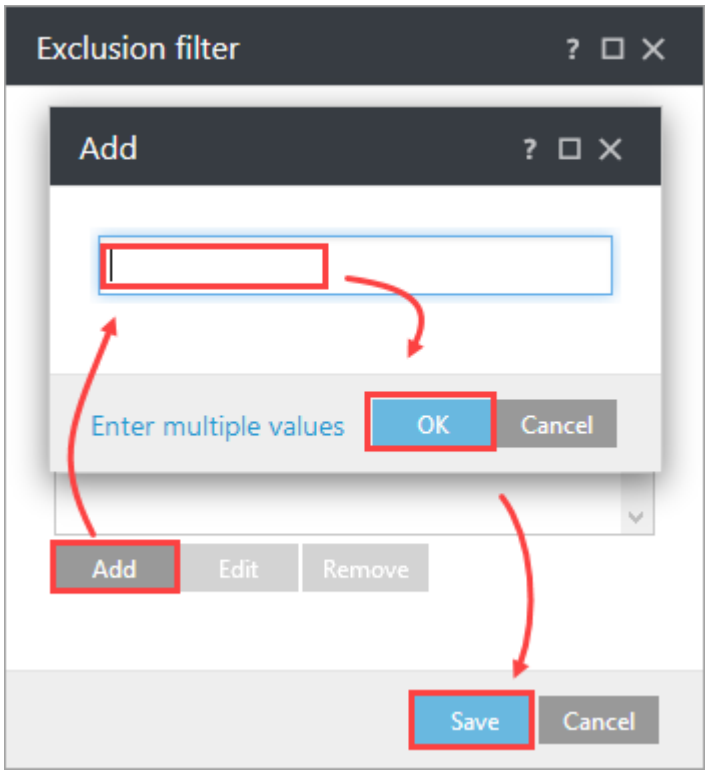


7.Klikněte na tlačítko **Přidat** a definujte výjimku. Pro potvrzení klikněte na tlačítko **OK** > **Uložit**.

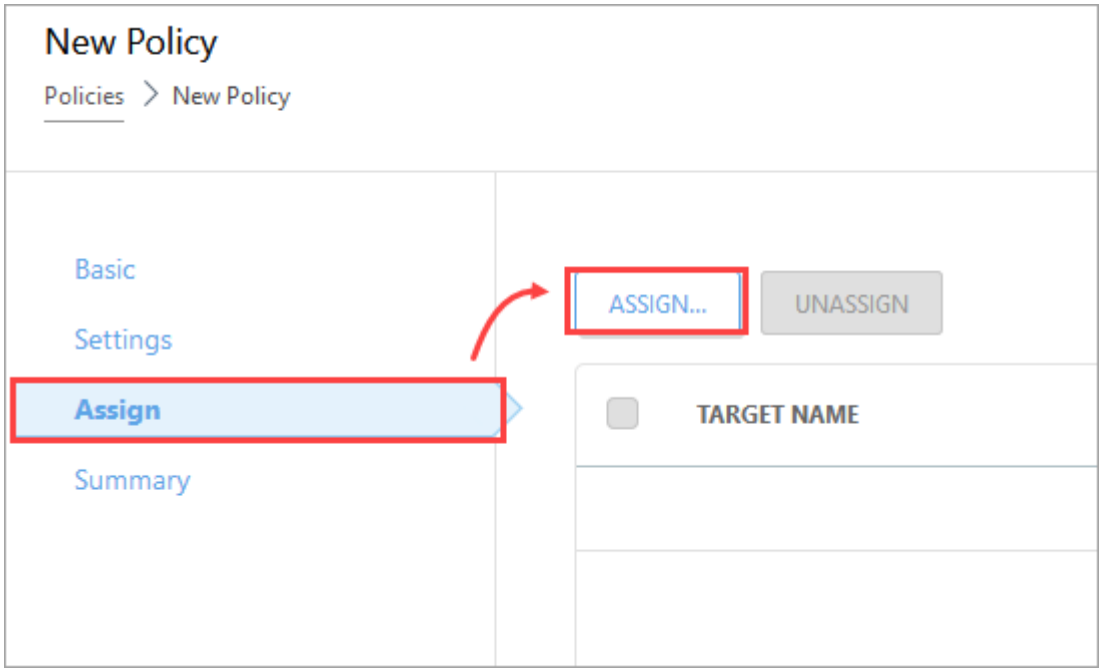
Příklady výjimek:

```
C:\MyProjects\*
*\DEVtool\debug\*
```

- Při definování výjimek můžete použít * a ?. (* – představuje libovolný řetězec, ? – představuje jeden znak).
- U výjimek se nerozlišují velká a malá písmena.
- Systémové proměnné a regulární výrazy nejsou podporovány.



8.V sekci **Přiřadit** vyberte počítače nebo skupiny, na které chcete politiku **aplikovat**.



9.Kliknutím na **OK** a **Dokončit** uložte politiku.

Proces výkonnostní výjimky nad složkou

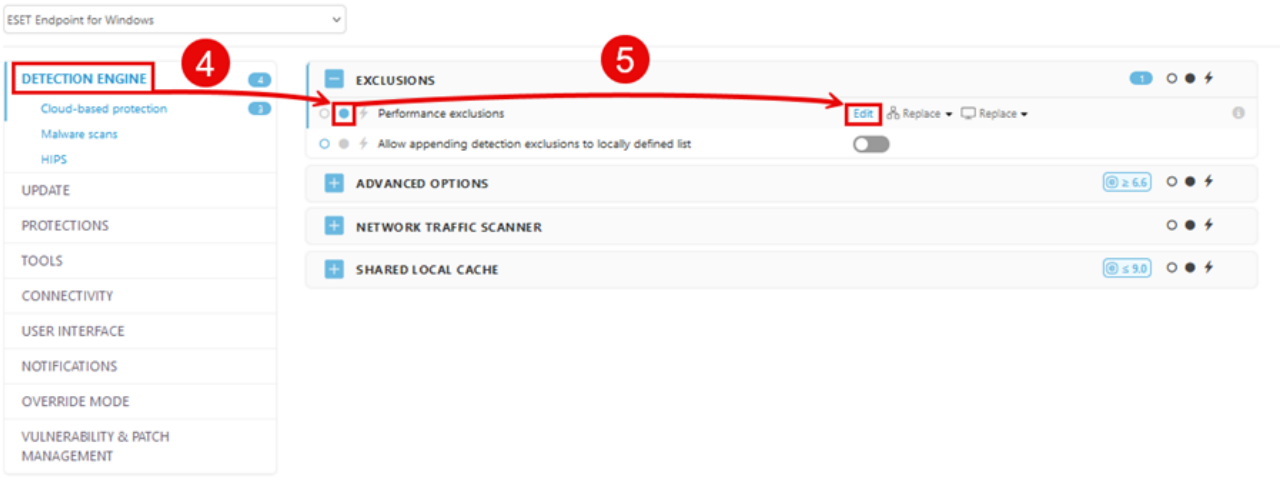
Soubory nebo složky můžete před kontrolou a odesláním do ESET LiveGuard Advanced vyjmout. Pokud ovšem tyto soubory přesunete mimo zadané umístění nebo složku, dojde k jejich odeslání do ESET LiveGuard Advanced.

1.Přihlaste se do webové konzole, v hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.

2.V sekci **Obecné** zadejte **název**, volitelně popis.

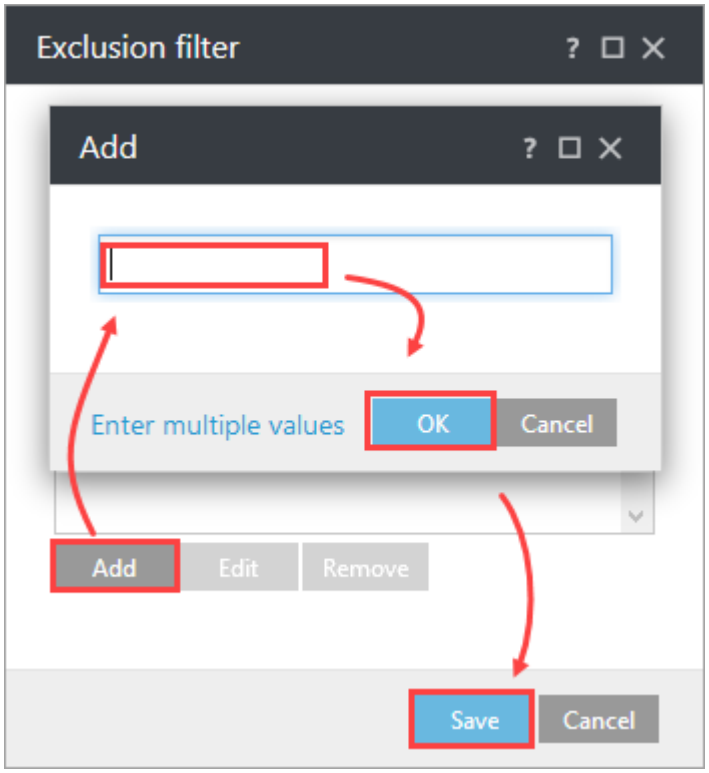
3.V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows** (nebo jiný kompatibilní produkt).

4.Klikněte na **Detekční jádro**.



5.V části **Výjimky** zapněte **Výkonnostní výjimky** a klikněte na **Změnit**.

6.Klikněte na tlačítko **Přidat** a definujte výjimku. Pro potvrzení klikněte na tlačítko **OK** > **Uložit**.



7.V sekci **Přiřadit** vyberte počítače nebo skupiny, na které chcete politiku **aplikovat**.

8.Kliknutím na **OK** a **Dokončit** uložte politiku.

Dále se můžete podívat na vyloučené procesy.

Vyloučení procesu

V některých případech není možné najít vzor pro umístění a názvy souborů, proto je vhodné vytvořit výjimku na konkrétní proces.

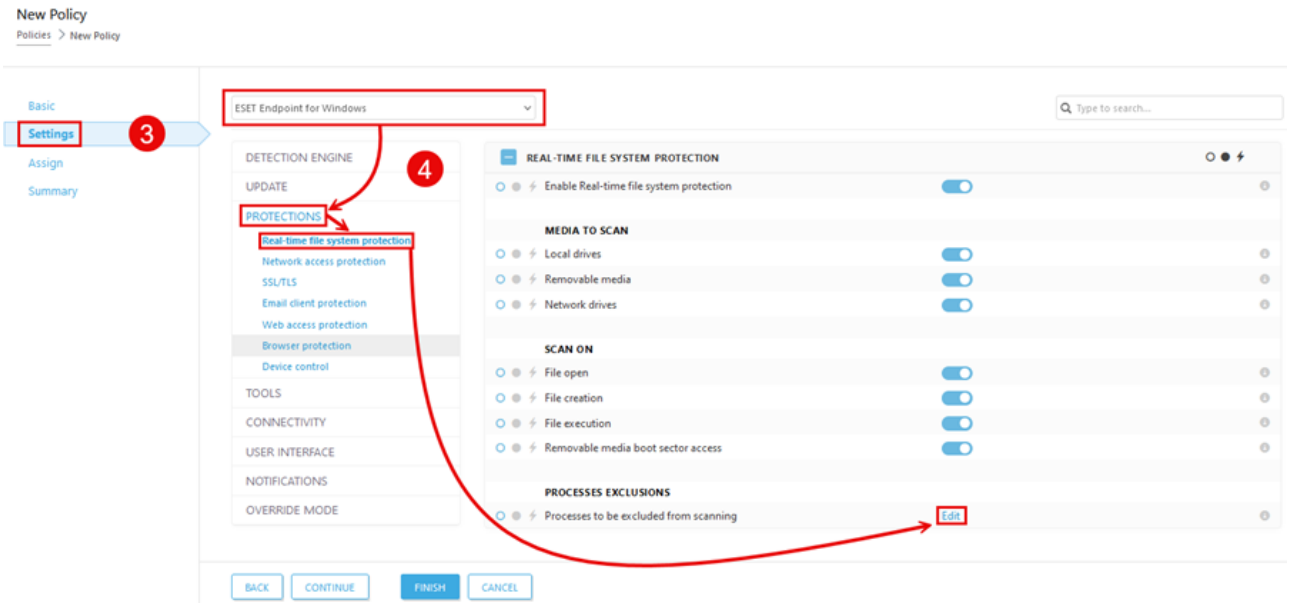
Vytvořením výjimky na procesy nebude docházet ke kontrole a zasílání souborů k analýze, které procesy vytváří nebo s nimi manipulují.

1.Přihlaste se do webové konzole, v hlavním menu přejděte na záložku **Politiky** a klikněte na tlačítko **Nová politika**.

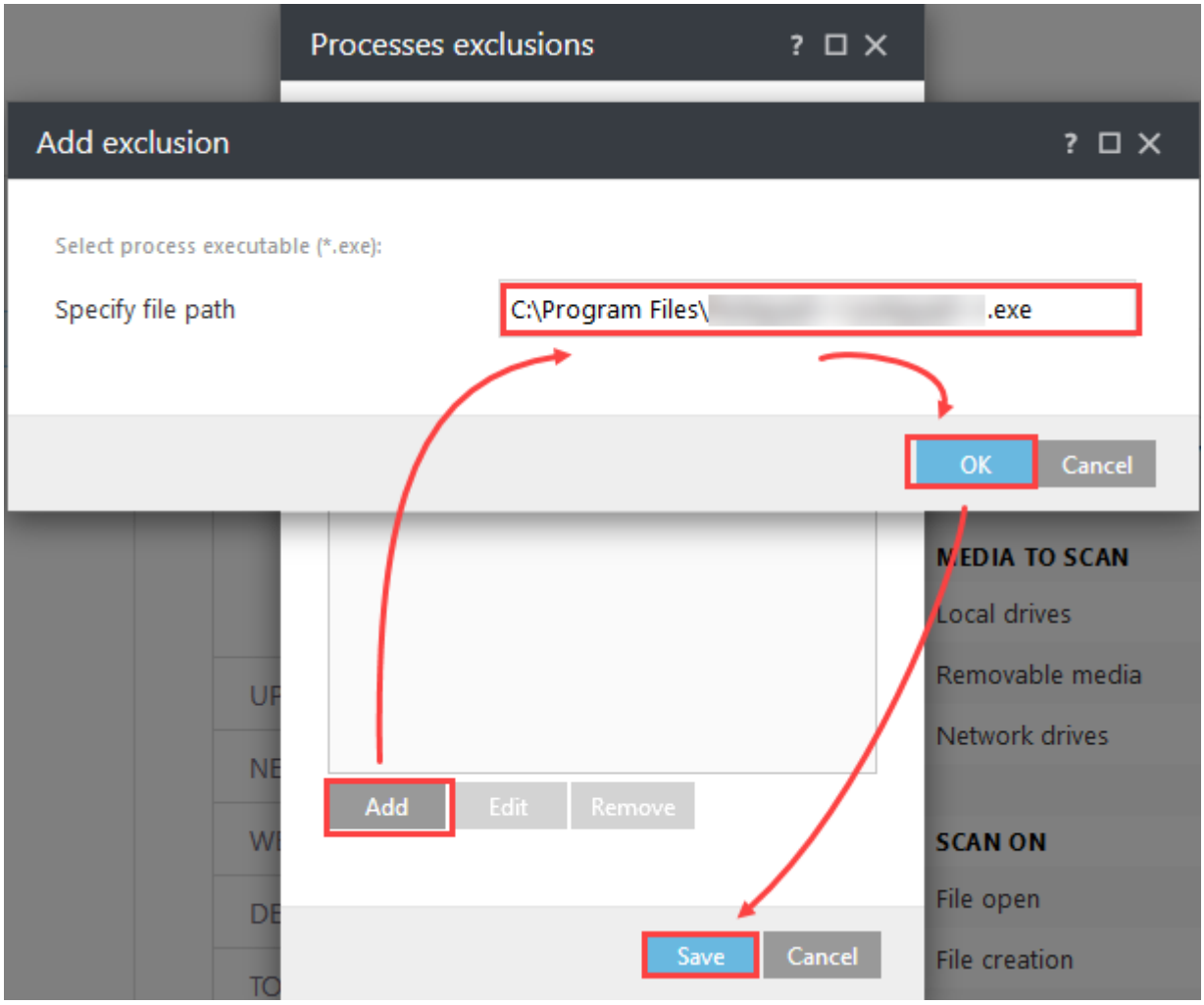
2.V sekci **Obecné** zadejte **název**, volitelně popis.

3.V sekci **Nastavení** vyberte z rozbalovacího menu **ESET Endpoint for Windows** (nebo jiný kompatibilní produkt).

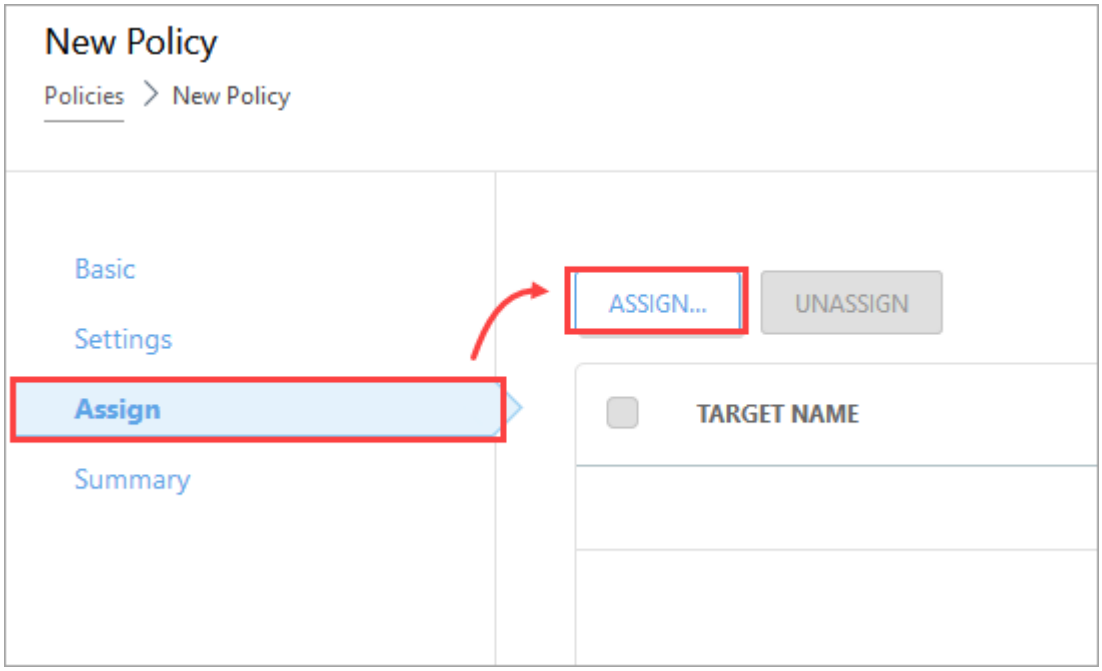
4.Klikněte na **Ochrany** > **Ochrana souborů v reálném čase** > **Ochrana souborů v reálném čase** > **Seznam procesů vyloučených z kontroly** > **Změnit**.



5.Klikněte na tlačítko **Přidat**, zadejte název procesu (úplnou cestu ke spustitelnému souboru), klikněte na **OK** a **Uložit**.



6.V sekci **Přiřadit** vyberte počítače nebo skupiny, na které chcete politiku **aplikovat**.



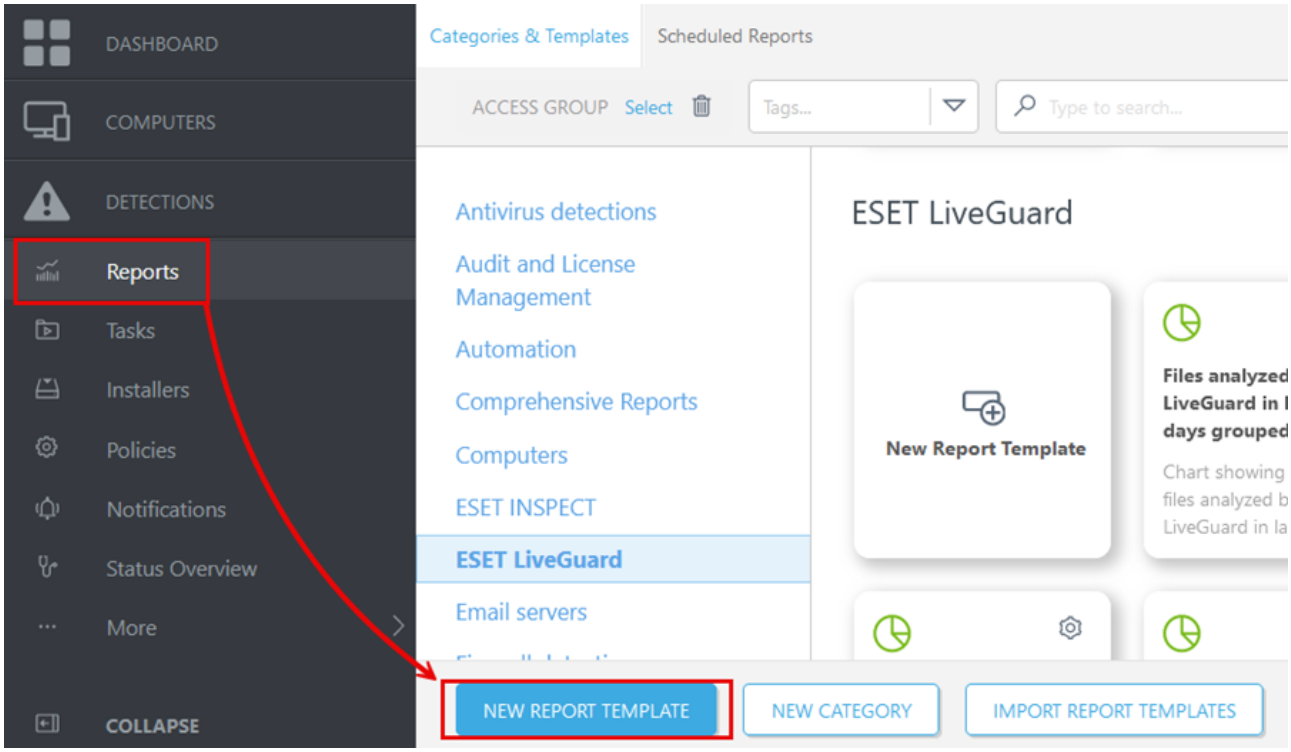
7.Kliknutím na **OK** a **Dokončit** uložte politiku.

Analýza počtu odeslaných souborů

Pro zjištění počtu odeslaných souborů na ESET LiveGuard Advanced servery využijte možnosti reportování v konzoli pro vzdálenou správu.

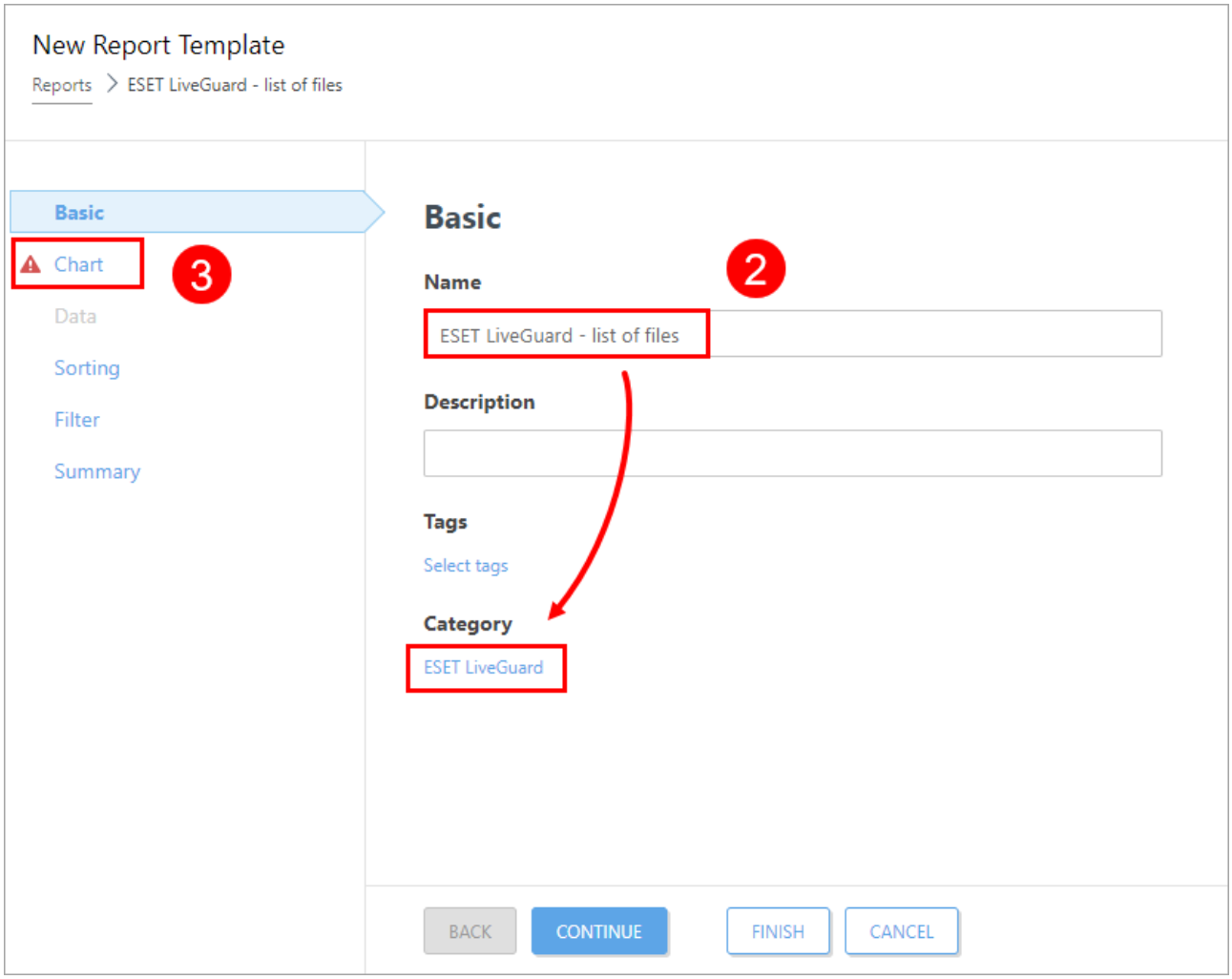
I. Vytvoření seznamu odeslaných souborů

1.Ve webové konzoli přejděte na **Přehledy** > **Nová šablona přehledu**.

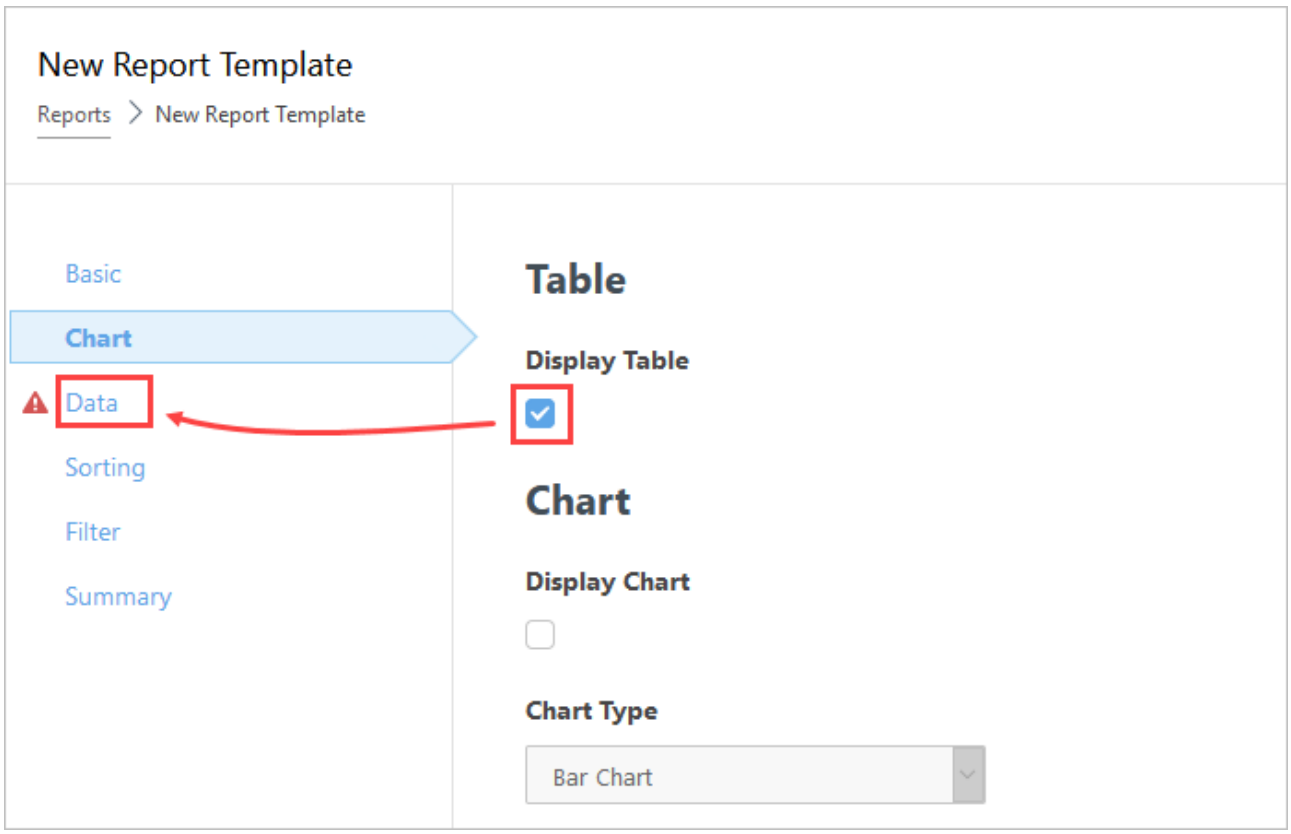


2.Šablonu si vhodně **pojmenujte** a zařaďte do požadované **kategorie**.

3.Pokračujte do sekce **Graf**.



4.V sekci **Graf** vyberte pouze možnost **Zobrazit tabulku** a pokračujte do sekce **Data**.

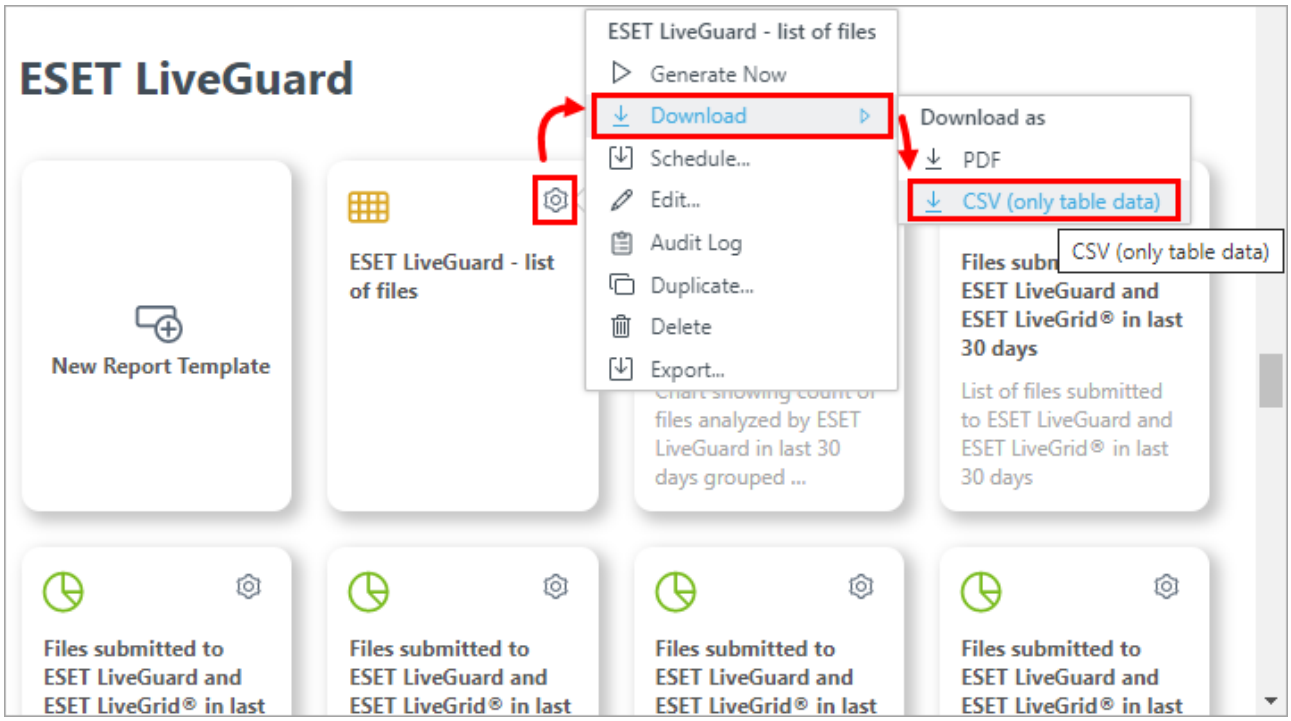


5.V sekci **Data** klikněte na **Přidat sloupec** a přidejte následující položky:
Počítač – Název počítače
ESET LiveGuard – URI objektu
ESET LiveGuard – čas výskytu
ESET LiveGuard – obsah souboru byl odeslán

6.Pro uložení šablony přehledu klikněte na tlačítko **Dokončit**.

7.V sekci **Přehledy** přejděte do kategorie **ESET LiveGuard**.

8.Najděte nově vytvořenou šablonu přehledu a vygenerujte si ji do CSV souboru.

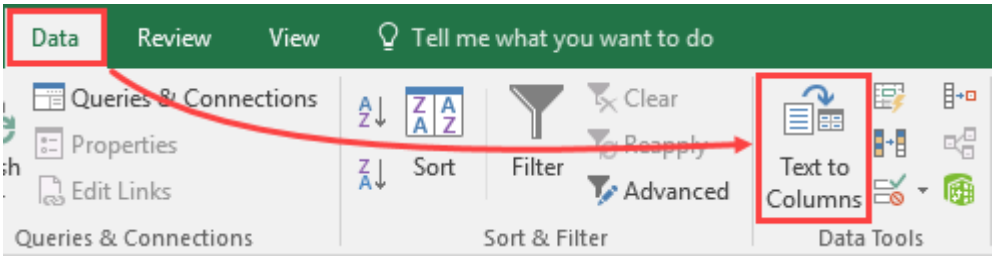


Analýza dat

Níže uvedené kroky vyžadují aplikaci třetí strany (tabulkový procesor) a základní schopnosti pro analyzování dat.

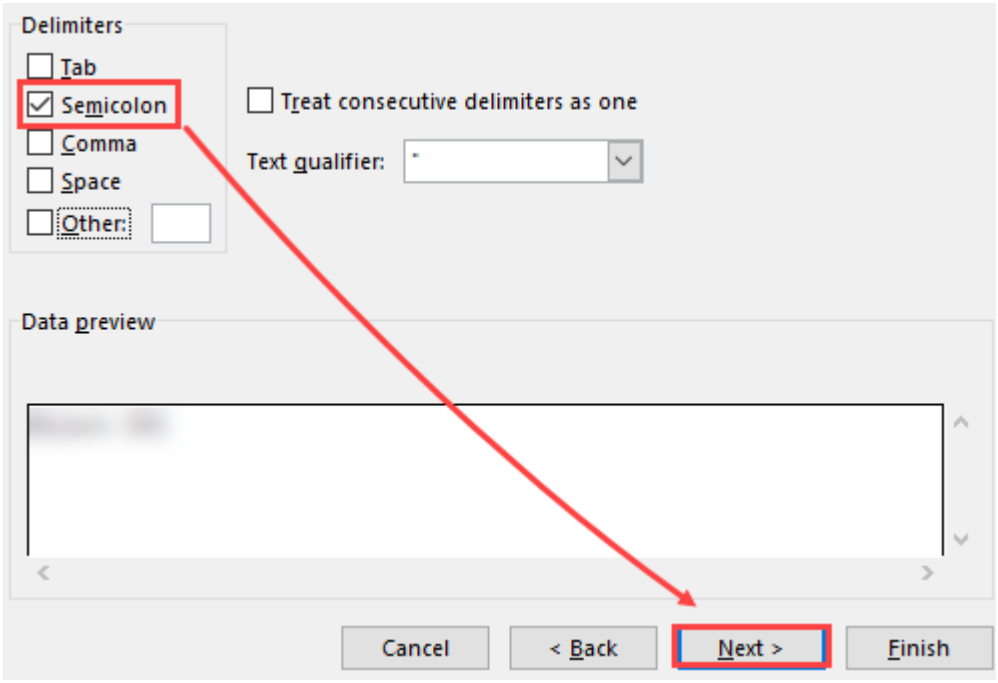
1.V tabulkovém procesoru, například MS Excel, si otevřete exportovaný CSV soubor.

2.Oddělte si data do dvou sloupců. V případě Microsoft Excel vyberte první sloupec a v hlavním menu klikněte na **Data** > **Text do sloupců**.



3.V zobrazeném dialogovém okně vyberte možnost **Oddělovač** a klikněte na tlačítko **Další**.

4.Jako oddělovač vyberte pouze **Středník** a klikněte na tlačítko **Další** > **Dokončit**.



Analyzujte data.

Navržené kroky k analýze

1.Odstraňte řádky, u nichž má atribut **Obsah souboru byl odeslán** hodnotu **Ne**.

2.Seřaďte data sestupně dle sloupce **Čas výskytu**.

3.Vyberte požadované časové okno, například posledních 30 dní, a zkopírujte si data do dalšího listu.

4.Na dalším listu seřaďte data dle sloupce **Název počítače**.

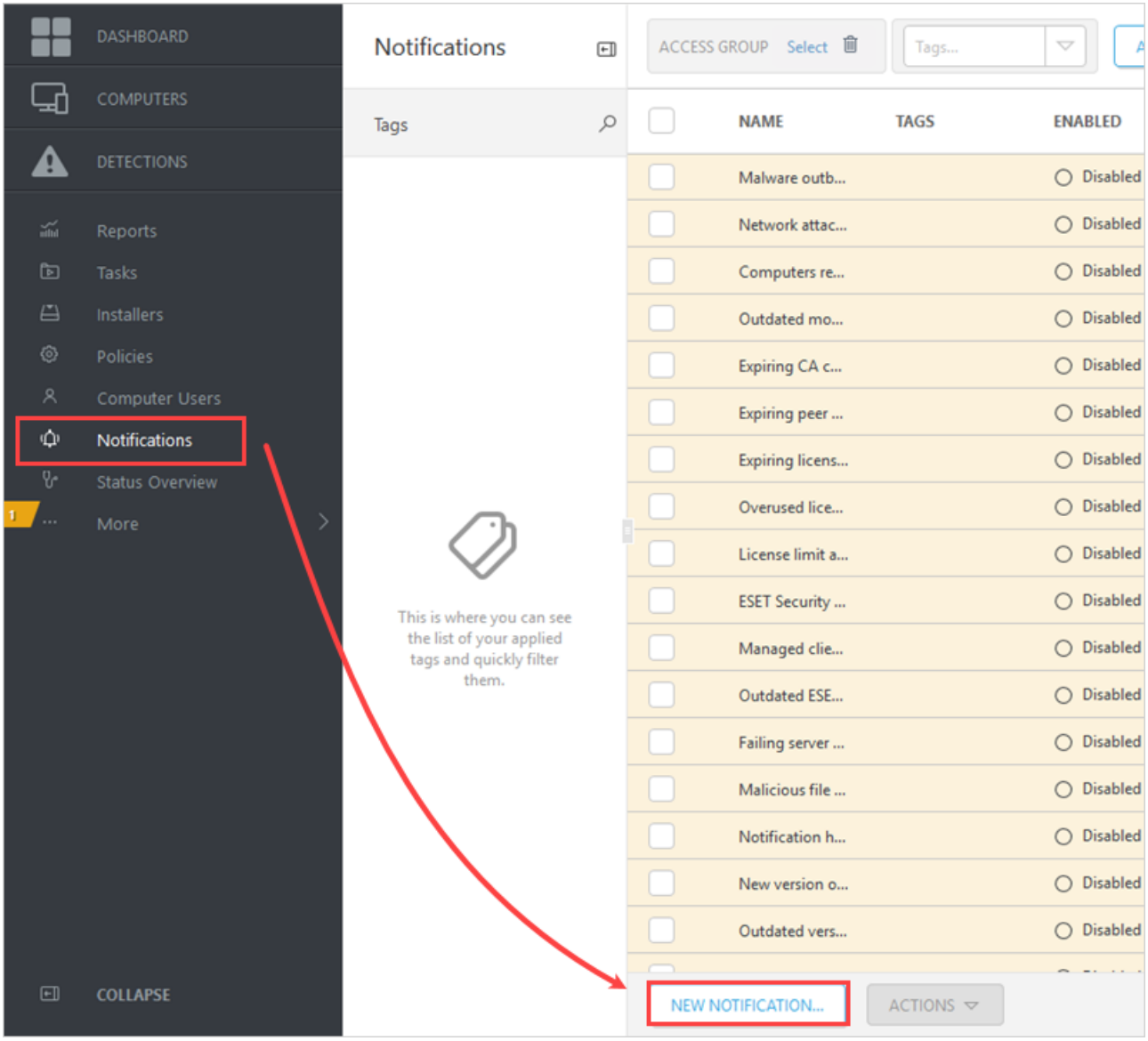
5.Spočítejte řádky (odeslané soubory) pro jednotlivé počítače.

Oznámení při detekci hrozby

V případě potřeby si můžete v konzoli pro vzdálenou správu vytvořit oznámení, a nechat se upozornit na každý objekt, který ESET LiveGuard Advanced označí jako hrozbu.

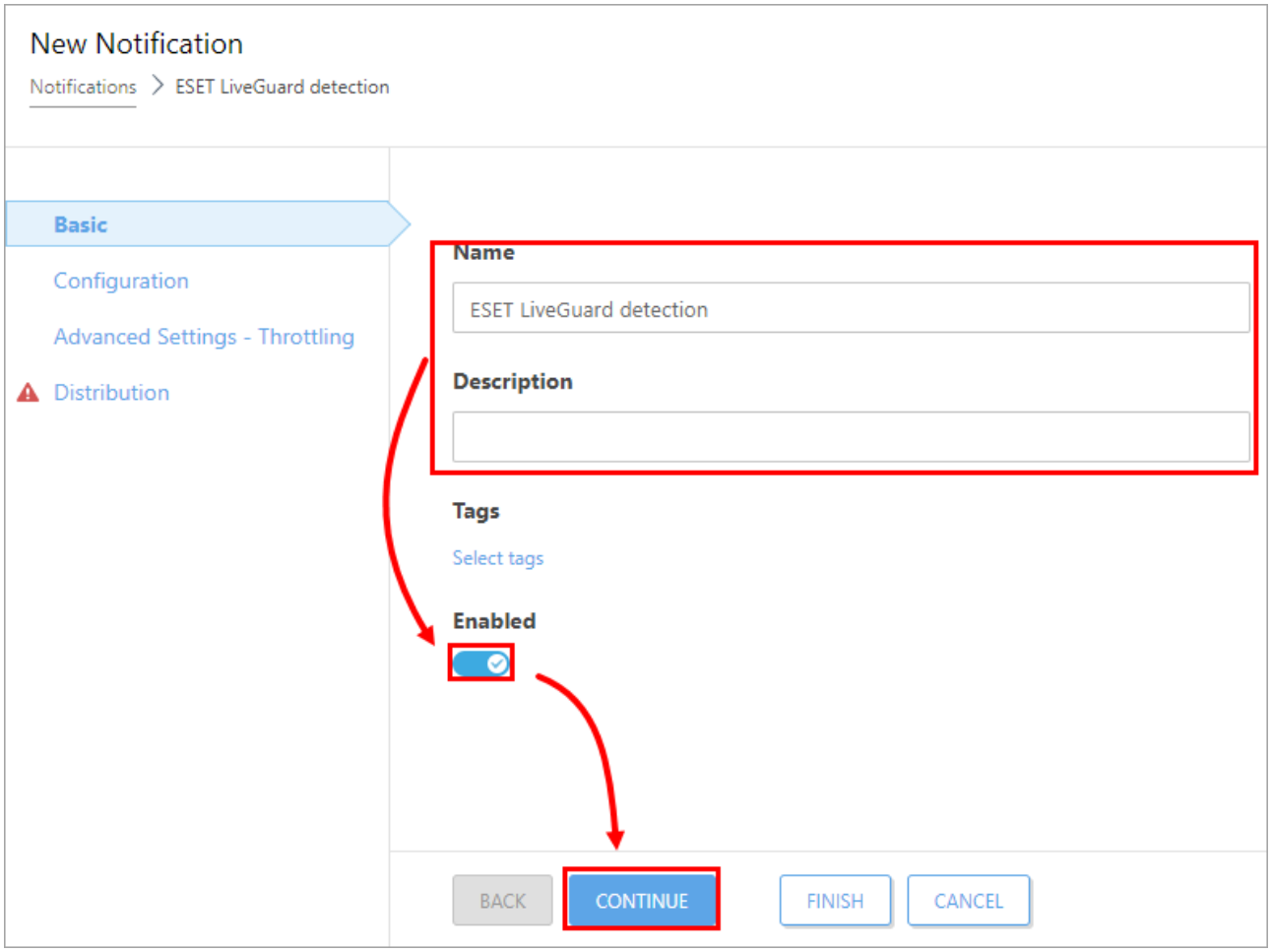
1.Přihlaste se do webové konzole.

2.V hlavním menu přejděte na záložku **Oznámení** a klikněte na tlačítko **Nové oznámení**.



3.Zadejte název a volitelně popis nově vytvářeného oznámení.

4.Přepínač v dolní části přepněte do polohy Zapnuto a klikněte na tlačítko **Pokračovat**.

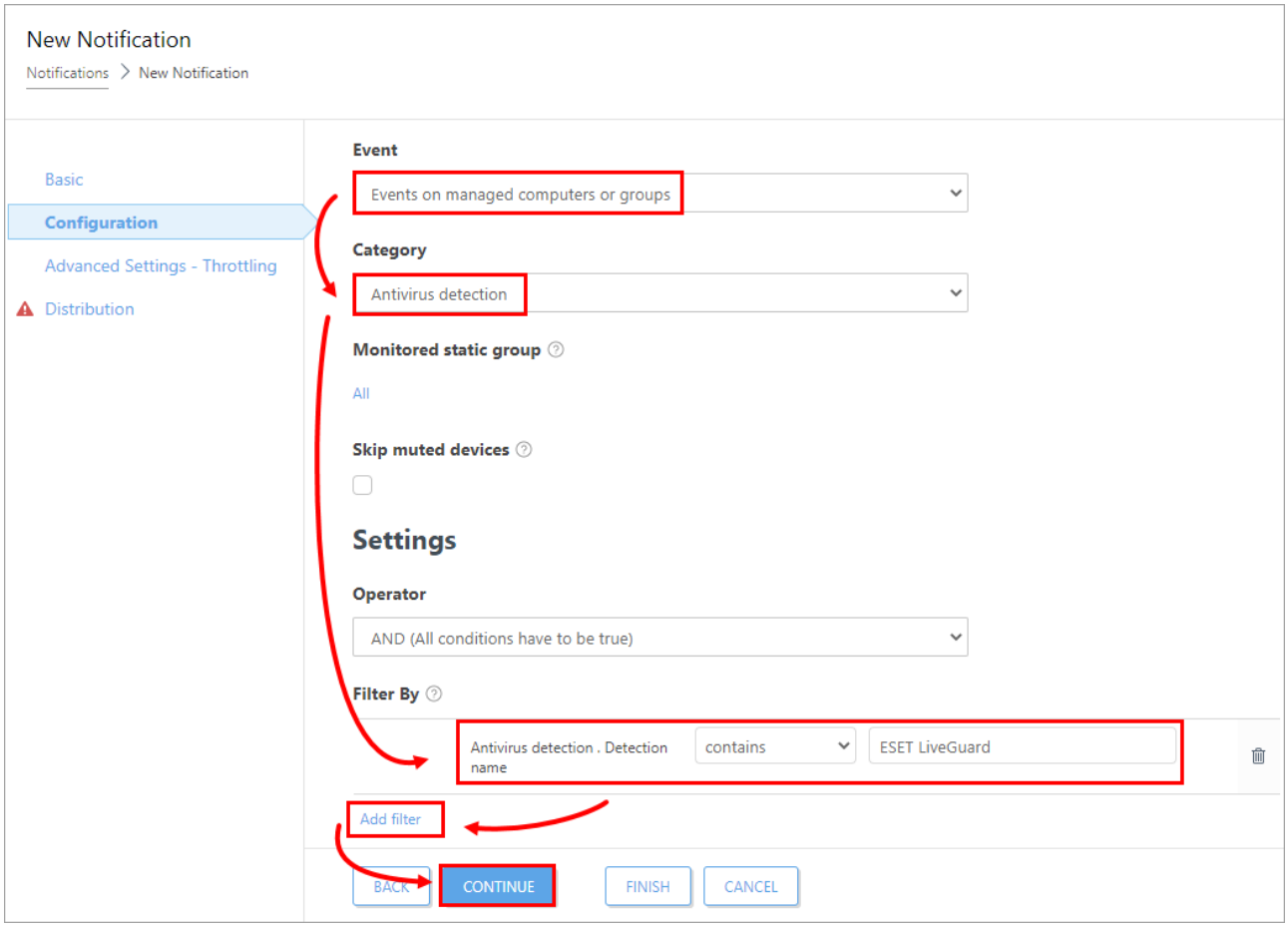


5.V sekci **Konfigurace** vyberte z rozbalovacího menu **Událost** možnost **Události na spravovaných počítačích**. Jako **Kategorii** vyberte pomocí rozbalovacího menu možnost **Detekce antivirem**.

6.Volitelně můžete změnit sledovanou statickou skupinu. Oznámení bude zasláno z počítačů z této skupiny a jejich podskupin, ke kterým má uživatel vytvářející oznámení oprávnění pro přístup.

7.Jako operátor ponechte **AND**, klikněte na **Přidat filtr** a vyberte **Název hrozby**.

8.Filtr použijte **je jeden z** a zadejte řetězec *ESET LiveGuard*. Klikněte na tlačítko **Pokračovat**.



9.V sekci **Rozšířená nastavení** můžete upravit četnost zasílání oznámení.

10. V sekci Distribuce definujte preferovaný způsob zaslání oznámení.

11. Oznámení uložte.

> **ESET File Security pro Windows Server**
> Do června 2021 byly detekce z ESET Server Security reportovány jako: `Zablokoval EDTD` Následně došlo ke sjednocení a jako detekce je uveden `Dynamic Threat Defense`, a po přejmenování `ESET LiveGuard`.

FAQ

Jaké soubory jsou zasílány do sandboxu?

Při manuálním zaslání souboru k analýze do ESET LiveGuard Advanced se nevyhodnocuje typ souboru. Při automatickém odesílání ověří nejprve bezpečnostní produkt, zda již nebyl soubor kontrolován, a zda se jedná o podporovaný typ souboru. Typ souboru je vyhodnocován na základě jeho obsahu, nikoli na jeho příponě – uživatel nebo tvůrce škodlivého kódu ji může snadno změnit.

ESET Mail Security a ESET Endpoint Security pro Windows se k jednotlivým typům souborů chovají odlišně. Jednotlivé typy souborů jsou zpracovávány odlišně.

- ESET Mail Security – zpracování je synchronní, systém čeká na výsledek.
- ESET Endpoint Security a ESET Server Security – zpracování je asynchronní. Systém nečeká na výsledek.

Zda je soubor odeslán nebo ne, závisí na původu souboru (web/mail/https).

Tabulka akcí dle typu souboru

Legenda

– odeslat – neodesílat

Typ souboru	Akce (ESET Mail Security)	Akce (ESET Endpoint Security, ESET Server Security)	Pouze odeslání
Archivy (.zip, .rar, .7z, .bzip2 a další)			• Pokud není archiv šifrován • Pokud je obsah archivu odeslán ke kontrole (v tomto případě je odeslán celý archiv) Pouze ESET Mail Security
Dokumenty (.docm, .xlsm, .pdf a další)			Pokud je aktivní (obsahuje JavaScript nebo jiné aktivní prvky)
Dokumenty ve formátu RTF (.rtf)			
Spustitelné soubory (.exe, .dll, .sys, .elf, .so soubory a další)			• Linuxové produkty zasílají k analýze níže uvedené typy souborů: oSpustitelný soubor na linuxu (.elf) oLinuxové knihovny (.so)
Ostatní (.jar, .lnk, .reg, .msi, .swf a další)			
Skripty (.bat, .cmd, .js, .vbs, .ps, .py, .sh, .pl a další)			• Linuxové produkty zasílají k analýze níže uvedené typy souborů: oPerl skripty (.pl) oPython skripty (.py) oShell skripty (.sh) ovšechny spustitelné textové soubory (označené "x")
Obrázky			
Ole2			Pokud je aktivní (obsahuje JavaScript nebo jiné aktivní prvky) – pouze ESET Mail Security
.hta			

Jaká je maximální velikost souboru, který se může odeslat?

Bezpečnostní produkty ESET mohou k analýze odeslat soubor o maximální velikosti 64 MB. Velikost si můžete upravit prostřednictvím politiky v sekci ESET LiveGuard Advanced.

Co znamenají jednotlivé stavy analýzy a souborů?

Jednotlivé stavy máme popsány v této kapitole.

Jak zabránit smazání konkrétního souboru?

Pro vyloučení konkrétního souboru můžete do výjimek přidat hash souboru. Po vytvoření výjimky dojde k obnovení souboru. Následně již nebude kontrolován.

Jak se ESET LiveGuard Advanced aktualizuje?

ESET LiveGuard Advanced je aktualizován vzdáleně v cloudovém systému ESET. Z vaší strany není vyžadován žádný zásah. Pro získání nových funkcí aktualizujte bezpečnostní produkt na nejnovější verzi.

Co se stane s nastavením produktu, po té, co vyprší platnost ESET LiveGuard Advanced licence?

Nastavení zůstane beze změny a ve webové konzoli se zobrazí varování, že vyprší platnost licence. Pro vypnutí souvisejících nastavení aplikujte na stanice další politiku.

Jak dlouho trvá analýza vzorku?

Analýza vzorků, které dosud nebyly ve službě ESET LiveGuard Advanced analyzovány, trvá obvykle do pět minut. Pokud byl již vzorek analyzován, uživatel obdrží výsledek při další požadavku produktu, tedy do dvou minut.

Mohu využívat výhody ESET LiveGuard Advanced bez odesílání souborů?

Pro počítače s vysokými požadavky na zabezpečení můžete vytvořit můžete samostatnou politiku, ve které zakážete zasílání souborů. Pokud je na stanici ESET LiveGuard Advanced aktivován, bezpečnostní produkt bude využívat výsledky analyzovaných souborů odeslaných jinými zařízeními ve firmě. Soubory vyhodnocené jako škodlivé budou zároveň detekovány prostřednictvím systému ESET LiveGrid®, což přispěje k ochraně všech připojených zařízení.

Další otázky a odpovědi na ně naleznete v samostatném FAQ v naší Databázi znalostí.

Je výsledek analýzy provedený službou ESET LiveGuard Advanced sdílen napříč všemi mými účty nebo zákazníky?

- Výsledek analýzy z ESET LiveGuard Advanced je okamžitě sdílen se všemi zařízeními aktivovanými prostřednictvím konkrétního ESET Business Account účtu – přičemž v daném účtu může být nahráno více licencí.

- Při použití ESET MSP Administrator účtu je výsledek z ESET LiveGuard Advanced okamžitě sdílen výhradně v rámci daného MSP zákazníka. V rámci MSP nejsou výsledky sdíleny mezi jeho zákazníky.

Za jak dlouho jsou výsledky z ESET LiveGuard Advanced dostupné v rámci ESET LiveGrid®?

Nejzávažnější detekce jsou v rámci tohoto systému dostupné do několika hodin od získání výsledku analýzy. Méně závažné detekce později.

Jak otestovat funkčnost služby ESET LiveGuard Advanced

Pro otestování funkčnosti a dostupnosti služby ESET LiveGuard Advanced postupujte podle níže uvedených kroků:

Uživatelé s ESET PROTECT On-Prem

I. Požadavky

Ujistěte se, že máte produkt aktivován ESET LiveGuard Advanced licencí, v nastavení je tato služba zapnutá a produkt je plně funkční.

II. Příprava testovacího souboru

1.Vytvořte si ve svém počítači novou složku.

2.Tuto složku přidejte mezi Výkonnostní výjimky.

3.Do vytvořené složky přidané mezi výjimky si stáhněte testovací soubor:
testovací soubor pro Windows
Testovací soubor pro Linux

4.Archiv v dané složce rozbalte. Archiv je chráněn následujícím heslem: infected

5.Windows uživatelé: Pro vytvoření nového souboru si otevřete příkazový řádek (stiskněte klávesy `Win+R` a zadejte příkaz `powershell`). Přejděte do složky, na níž máte vytvořenou výjimku a nachází se v ní testovací soubor. Pomocí níže uvedeného příkazu přidáte na konec souboru aktuální časové razítko, díky čemuž dojde ke změně kontrolního součtu souboru:

```
Add-Content .\EdtdTestFile.exe $(date)
```

Linux uživatelé: Pro vytvoření nového souboru si otevřete terminál, přejděte do složky, na níž máte vytvořenou výjimku a nachází se v ní testovací soubor. Zadejte příkaz `date >> create_eicar.bin` (volitelně si soubor můžete přejmenovat). Tímto příkazem přidáte na konec souboru aktuální časové razítko, díky čemuž dojde ke změně kontrolního součtu souboru.

III. Test ESET LiveGuard Advanced

1.Zkopírujte soubor vytvořený podle instrukcí v části II. do složky, kterou nemáte na seznamu výjimek. Soubor bude okamžitě odeslán k analýze do ESET LiveGuard Advanced, protože se jedná o nový spustitelný soubor.

2.Přesvědčit se můžete pomocí níže uvedených kroků:
V bezpečnostním produktu ESET: Pro zobrazení seznamu přejděte v hlavním okně na záložku **Nástroje** > **Protokoly** a z rozbalovacího menu vyberte možnost **Odeslané soubory**.
Ve webové konzoli ESET PROTECT: V hlavním menu přejděte do sekce Další **Další** > **Odeslané soubory**.

3.Za několik okamžiků se soubor smaže ze zařízení a zobrazí se oznámení o odstranění škodlivého kódu. Přesvědčit se můžete pomocí níže uvedených kroků:
V bezpečnostním produktu ESET: Pro zobrazení detekce přejděte v hlavním okně na záložku **Nástroje** > Protokoly a z rozbalovacího menu vyberte možnost **Detekce**.
Ve webové konzoli ESET PROTECT: V hlavním menu přejděte do sekce Další **Další** > **Odeslané soubory**.

4.Pokud soubor spustíte před dokončením analýzy, zobrazí se vám informace "ESET LiveGuard Advanced test file has been executed". Testovací soubor spustí Eicar (standardizovaný soubor pro test antimalwarové ochrany), který bude okamžitě smazán. Po dokončení analýzy dojde k vyléčení testovacího souboru.

IV. Testování více souborů

Po detekování souboru dojde k lokálnímu uložení jeho kontrolního součtu. Pokud jej zkusíte zkopírovat ze složky, na níž jste vytvořili výjimku, dojde okamžitě k jeho detekci. Opakováním kroku II. 5. můžete vytvořit nové soubory a dojde k jejich opětovnému zaslání k analýze. Dále postupujte podle kroků ze sekce III.

V. Test proaktivní ochrany

1.Ověřte, zda je zapnutá proaktivní ochrana. V **rozšířeném nastavení** bezpečnostního produktu ESET (dostupném po stisknutí klávesy F5) přejděte do sekce **Detekční jádro** > **Cloudová ochrana** > **ESET LiveGuard Advanced** a v rozbalovacím menu **Proaktivní ochrana** vyberte možnost Blokovat spuštění do obdržení výsledku analýzy.

2.Ujistěte se, že máte povoleno zobrazování souvisejících oznámení. V bezpečnostním produktu ESET stiskněte klávesu F5 nebo klikněte na možnost **Rozšířené předvolby** > **Oznámení** > **Oznámení na pracovní ploše** > **Oznámení na pracovní ploše** > **Upravit** a zapnout:
Soubor byl analyzován
Probíhá analýza souboru
Soubor nebyl analyzován

3.Do složky, kterou nemáte uvedenou na seznamu výjimek, si stáhněte druhý testovací soubor a spusťte.
testovací soubor pro Windows
Testovací soubor pro Linux

4.V tento okamžik se zobrazí oznámení týkající se zamítnuté operace. Soubor není možné v průběhu čekání na výsledek analýzy spustit.

5.Po dokončení analýzy a doručení výsledku, že je soubor čistý, jej bude možné spustit.

Uživatelé ESET Cloud Office Security

I. Požadavky

Ujistěte se, že máte ESET LiveGuard Advanced v ESET Cloud Office Security zapnutý pomocí politiky.

II. Příprava testovacího souboru

1.Do umístění, nebo na stanici, na které není aplikována politika zapínající ESET LiveGuard Advanced, si stáhněte testovací soubor.

2.Rozbalte stažený archiv. Archiv je chráněn heslem. Heslo k archivu: `infected`

3.Pro vytvoření nového souboru si otevřete příkazový řádek (stiskněte klávesy `Win+R` a zadejte příkaz `powershell`).

4.Přejděte do složky s testovacím souborem.

5.Spusťte níže uvedený příkaz: Tímto přidáte na konec souboru aktuální časové razítko, díky čemuž dojde ke změně kontrolního součtu souboru.

```
Add-Content .\EdtdTestFile.exe $(date)
```

III. Test ESET LiveGuard Advanced

1.Soubor z kroku II použijte jedním z následujících způsobů:

Přesuňte soubor na OneDrive.
Vytvořte koncept zprávy (pomocí Microsoft Outlook) s testovacím souborem jako přílohou
Uložte soubor do chráněného umístění na Sharepoint.

2.Soubor se okamžitě odešle k analýze do ESET LiveGuard Advanced.

3.Pro ověření, že došlo k odeslání souboru, přejděte v ESET Cloud Office Security do sekce **Protokoly** > **Odeslané soubory**.

4.Za několik okamžiků dojde k odstranění souboru. Výsledek analýzy najdete v sekci **Odeslané soubory**.

FAQ

Jedná se o skutečný škodlivý kód?

Nikoli, `EdtdTestFile.exe` je pouze tzv. dropper, který spouští Eicar (standardizovaný soubor pro test antimalwarové ochrany). Tato událost je detekována v průběhu analýzy v sandboxu zajišťovaném službou ESET LiveGuard Advanced.

Jak si mohu být jistý?

Níže uvádíme zdrojový kód testovacích souborů:

- Spustitelný soubor Windows

```
#include <fstream>

#include "tchar.h"

#include "windows.h"


int main()
```

```
{

    std::ofstream dropped;

    dropped.open(_T("eicar.com"));

    dropped << "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

    dropped.close();

    ::MessageBox(nullptr, _T("EDTD test file has been executed.\n2020.4.15 10:34"),
_T("EDTD test file"), MB_OK);

    return 0;

}
```

- Linuxová binárka

```
#include <fstream>

#include <iostream>

#include <stdio.h>


int main()

{

   std::ofstream dropped;

   dropped.open("eicar.com");

   dropped << "X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*";

   dropped.close();

   std::cout << "EDTD test file has been executed." << std::endl;

   getchar();

   return 0;

}
```

Řešení problémů

- Služba nefunguje
- ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje

- Jak získám protokoly?
- Ve webové konzoli ESET PROTECT nevidím některé odeslané soubory
- Popis chování vzorku není správný
- Jak mohu vyloučit detekovaný soubor a zabránit jeho přesunutí do karantény?
- Co se stane po vyprší platnosti licenci?
- Co dělat, pokud nevidím žádné odeslané soubory?
- ESET PROTECT On-Prem nestahuje ESET LiveGuard Advanced data
- Ve webové konzoli ESET PROTECT chybí výsledky pro odeslané soubory
- Co mám dělat, pokud u souborů odeslaných do ESET LiveGuard Advanced vidím informaci "Odesláno do LiveGrid"
- Produkt odmítá ESET LiveGuard Advanced licenci
- V sekci Detaily počítače > Upozornění se mi zobrazuje některá z následujících chybových zpráv
- Soubory odeslané do ESET LiveGuard Advanced se nezobrazují ve webové konzoli
- Zobrazila se mi chyba: V rámci své licence nemáte přístup k přehledu o chování souboru.
- Mám podezřelý vzorek, co mám dělat?
- Aktivace ESET LiveGuard Advanced nebyla úspěšná

Služba nefunguje

Ujistěte se, že máte bezpečnostní produkty aktivované ESET LiveGuard Advanced licencí a použití této služby máte povoleno v konfiguraci produktu.

Ověřte také následující:

- Je licencí pro ESET LiveGuard Advanced produkt aktivován?
- Má stanice přiřazenou politiku s nakonfigurovanou službou ESET LiveGuard Advanced?

ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje

Ověřte, zda je funkční síťové spojení mezi ESET Management Agentem a ESET PROTECT serverem.

Případný problém v komunikaci mezi serverem pro vzdálenou správu a ESET LiveGuard Advanced naleznete ve webové konzoli na **Nástěnce**: **ESET PROTECT Server** > **Problémové komponenty ESET PROTECT On-Prem infrastruktury**.

Překontrolujte rovněž nastavení **HTTP Proxy** v nastavení ESET PROTECT.

Sesbírejte protokoly

Více informací o protokolech naleznete v Online nápovědě k ESET PROTECT On-Prem.

Ve webové konzoli nevidím některé odeslané soubory

Toto je typické chování v případě mobilních uživatelů.

Popis chování vzorku není správný

Pokud se štítek reprezentující chování vzorku nezdá být správný:

- Nahlaste tuto situaci na technickou podporu, případně vzorek zašlete na adresu samples@eset.com. Dále si pročtěte informace týkající se zasílání vzorků.
- Navštivte ESET Bezpečnostní fórum a prodiskutujte tuto situaci s ESET komunitou.

Jak mohu vyloučit detekovaný soubor a zabránit jeho přesunutí do karantény?

Pokud se domníváte, že je detekovaný soubor bezpečný, můžete jej vyloučit z kontroly.

Co se stane po vyprší platnosti licenci?

Po vypršení platnosti licenci pro použití ESET LiveGuard Advanced budete nadále schopni zasílat vzorky k analýze. Nicméně již neobdržíte výsledek analýzy ani detailní přehled chování vzorku.

Co dělat, pokud nevidím žádné odeslané soubory?

> **Používáte ESET PROTECT?**
> Tato metoda řešení potíží je určena pro uživatele on-premises konzole pro vzdálenou správu ESET PROTECT On-Prem.

1. Zkontrolujte **nástěnku** ve své konzoli pro vzdálenou správu dle kroků v části: ESET LiveGuard Advanced mám nakonfigurovaný, ale stále nefunguje

2. Klikněte na **Přehledy** > **Audit a správa licencí** > **Audit log** > **Vygenerovat a stáhnout** > **PDF**. Výstup prozkoumejte, případně jej přiložte k žádosti zasílané na technickou podporu ESET.

Pokud v přehledu není uvedena žádná chyba související s ESET LiveGuard Advanced, podle níže uvedených kroků získejte trace protokoly a zašlete je na technickou podporu. Můžete také zkusit na serveru pro vzdálenou správu inicializovat proces opětného získání výsledků.

Jak získat trace protokoly:

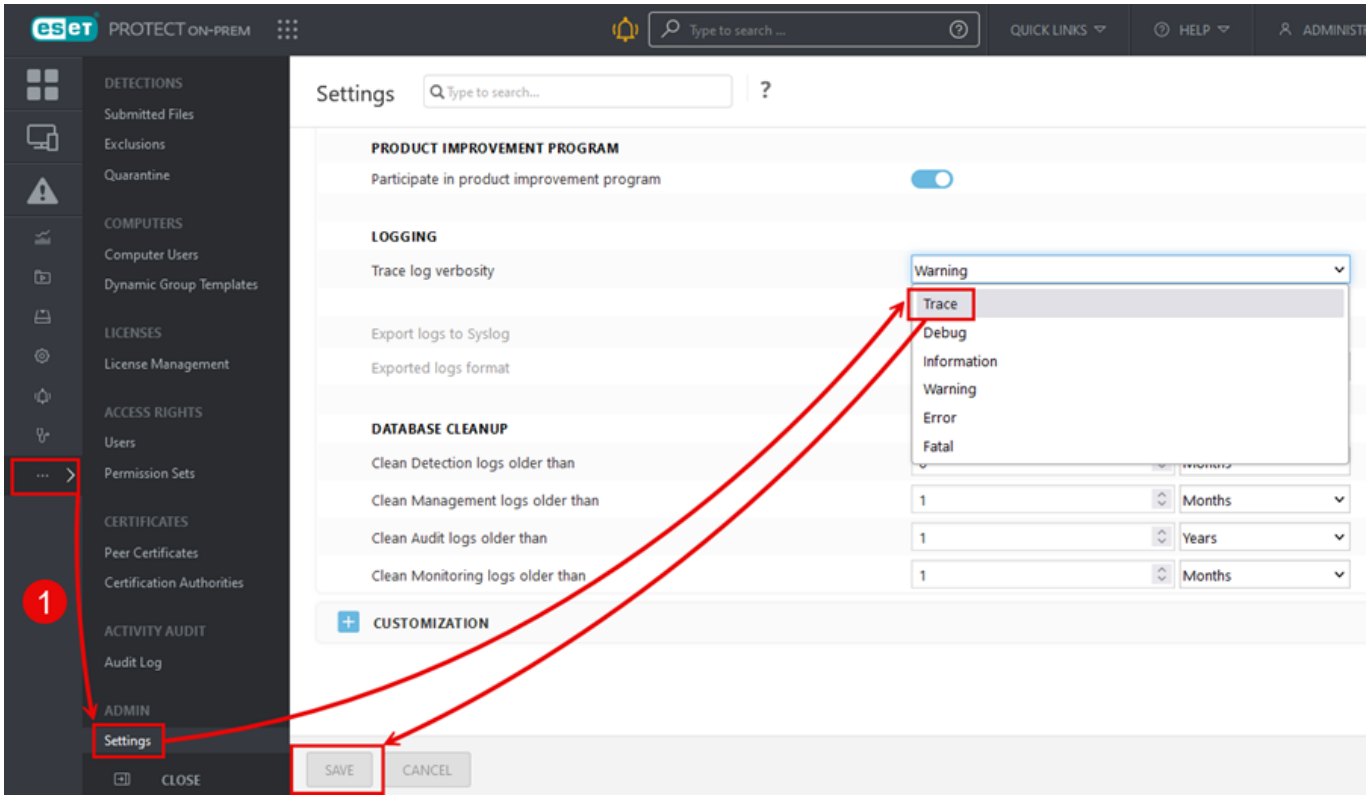
1.Chcete-li ve webové konzoli zapnout trace protokolování, klikněte na **Další…** > **Nastavení** > **Rozšířená nastavení** > **Protokolování** > **Zaznamenávat události od úrovně** > **Trace**.

2.Restartujte službu ESET PROTECT On-Prem nebo celý server a vyčkejte 15 až 20 minut.

3.Protokoly naleznete v na ESET PROTECT serveru:

I.Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*

II.Linux: */var/log/eset/RemoteAdministrator/Server/*



Jak znovu stáhnout výsledky ESET LiveGuard Advanced

Na ESET PROTECT serveru restartujte proces načítání dat. Restartování může pomoci v případě, kdy si server nestahuje z ESET cloudu nová data nebo stažení trvá příliš dlouho.

1.Vypněte službu ESET PROTECT server.

2.Přihlaste se do databáze ESET PROTECT pomocí SQL Server Management Studio nebo klienta MySQL v systémech Linux.

3.V databázi ESET PROTECT upravte tabulku tbl_key_value_pairs:

Při použití SQL Server Management Studio otevřete tabulku a odstraňte řádek obsahující řetězec `eset-dynamic-threat-detection-customers`

Při použití MySQL otevřete databázi a spusťte příkaz `delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';`

Při použití virtuální appliance ESET PROTECT:

a)Připojte se prostřednictvím SSH nebo na appliance přejděte do terminálu.

b)Přihlaste se do databáze: `mysql -u root -p era_db`

c)Zadejte heslo. Obvykle je stejné jako heslo administrátora webové konzole.

d)Spusťte následující příkaz:
delete from tbl_key_value_pairs where pair_key = 'eset-dynamic-threat-detection-customers';

4.Zapněte ESET PROTECT server a vyčkejte 24 hodin. Během této doby nerestartujte ani nevypínejte server.

Ve webové konzoli ESET PROTECT chybí výsledky pro odeslané soubory

Možné důvody:

- ESET LiveGuard Advanced byl aktivován licenčním klíčem, namísto účtem EBA

Řešení:

1.Odeberte stávající licenci z ESET PROTECT On-Prem.

2.Přidejte licenci pro ELGA do účtu ESET Business Account.

3.Pomocí účtu EBA přidejte licenci do ESET PROTECT On-Prem.

4.U klienta znovu aktivujte ESET LiveGuard Advanced.

5.Restartujte službu ESET PROTECT server

Co mám dělat, pokud u souborů odeslaných do ESET LiveGuard Advanced vidím informaci "Odesláno do LiveGrid"

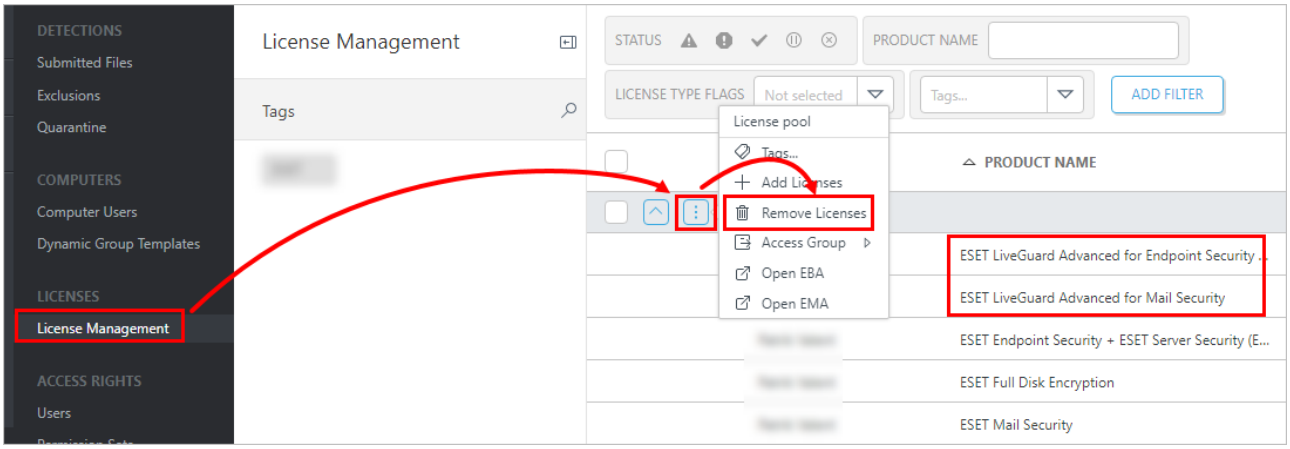
Možné důvody:

- Soubor nebo nevyžádaný e-mail (spam) je již detekován.

- Tato situace může nastat, pokud jste ESET LiveGuard Advanced licenci neimportovali do EBA, ale vložili ji přímo do bezpečnostního produktu nebo konzole pro vzdálenou správu.

Pro zapnutí odesílání souborů do ESET LiveGuard Advanced:

1.Odeberte licenci ze správy licencí.



2.Importujte licenci do svého EBA účtu.

3.Synchronizujte svůj EBA účet se serverem vzdálené správy (ESET PROTECT On-Prem).

4.Na straně klientských stanic (bezpečnostního produktu) je nutné vyčkat na aktualizování vybraných modulů. Dosáhnete toho některým z níže uvedených způsobů:

- Počkejte několik hodin, než se moduly znovu načtou.
- Pro okamžité načtení můžete „restartovat“ ESET LiveGuard Advanced na klientských zařízeních. Pro restartování vytvořte a stanicím přiřaďte politiku pro deaktivování ESET LiveGuard Advanced. Po jejím aplikování na stanice proveďte opětovné zapnutí této služby.

Produkt odmítá ESET LiveGuard Advanced licenci

- Po zadání licenčního klíče k ESET LiveGuard Advanced ve webové konzoli se zobrazí následující chybové hlášení:
  - **Nepodařilo se přidat licenci prostřednictvím licenčního klíče: Licence je určena pro produkt, který není možné spravovat prostřednictvím ESET PROTECT On-Prem. Prosím, vložte jinou licenci**.
- Po zadání licenčního klíče k ESET LiveGuard Advanced přímo do bezpečnostního produktu se může zobrazit následující chybové hlášení:
  - **Aktivace nebyla úspěšná. Licence neodpovídá produktu.**

Licenci je nutné přidat výhradně prostřednictvím účtu vytvořeného na portále EBA. Pro více informací přejděte do kapitoly vložení licence.

V sekci Detaily počítače > Upozornění se mi zobrazuje některá z následujících chybových zpráv

Problém	Detaily problému	Příčina a řešení
ESET LiveGuard Advanced není dosažitelný	ESET LiveGuard Advanced nefunguje. Připojení k autentifikačnímu serveru selhalo.	Licenční servery ESET nejsou dostupné. • Firewall blokuje komunikaci. • Služba je dočasně nedostupná. Zkontrolujte konfiguraci firewallu.

Problém	Detaily problému	Příčina a řešení
ESET LiveGuard Advanced není dosažitelný	Platnost ESET LiveGuard Advanced licence vypršela.	Platnost vaší ESET LiveGuard Advanced licence vypršela a již není funkční Obnovte si licenci nebo vypněte nastavení ESET LiveGuard Advanced prostřednictvím politiky.
ESET LiveGuard Advanced není dosažitelný	ESET LiveGuard Advanced servery nejsou dosažitelné. Může se jednat o chybu v připojení k internetu nebo na serverech probíhá údržba.	Stanice se nedokáže spojit s ESET LiveGuard Advanced servery. Obvykle se jedná o chybu proxy služby. Zkuste restartovat službu proxy. V případě přetrvávajících potíží se může jednat o přetížení proxy. Pro vyřešení můžete: • Rozdělit zátěž agentů na více proxy • Navýšit hardwarové prostředky stroje, na kterém běží proxy • Použít 64bitové sestavení Apache HTTP Proxy (pokud používáte 32bitovou verzi a váš systém má 64bitovou architekturu) • Dočasně přestat používat proxy a ujistit se, zda je proxy příčinou problému • Pokud používáte Apache HTTP Proxy, můžete přejít na ESET Bridge.
Ve webové konzoli se nezobrazují žádné výsledky	Výsledky analýzy nejsou doručeny na ESET PROTECT server.	Může se jednat o přetížení HTTP Proxy. Zkuste přesunout HTTP Proxy na jiný server nebo serveru přidejte více prostředků. Po přesunutí HTTP Proxy nezapomeňte novou adresu aktualizovat v politice určené bezpečnostním produktům.
ESET LiveGuard Advanced není dosažitelný	Chyba offline licenčního souboru na ESET LiveGuard Advanced.	ESET LiveGuard Advanced není možné aktivovat prostřednictvím offline licence. Ověřte stav licence.
ESET LiveGuard Advanced není dosažitelný	ESET LiveGuard Advanced nefunguje. Neznámá chyba při autentifikaci.	Ověřovací servery ESET nejsou z klientské stanice dostupné. Ověřte, zda máte přístup na *edf.eset.com*.

Ve webové konzoli se nezobrazují soubory odeslané do ESET LiveGuard Advanced

• Pokud váš operační systém - obvykle starší verze serveru Windows - nedůvěřuje certifikátu *ts.eset.com* , soubory se neodesílají na servery ESET LiveGuard Advanced. Pro vyřešení si do operačního systému naimportujte kořenové certifikáty DigiCert Global Root G2 a Thawte TLS RSA CA G1.

• Ve webové konzoli se mohou odeslané soubory zobrazit pouze v případě, že se ESET Management Agent připojuje (replikuje data) k ESET PROTECT serveru. Informace o souborech zaslaných z mobilních klientů se zobrazí až po připojení agenta k serveru.

Při použití ESET LiveGuard Advanced v enterprise prostředí (stovky a více stanic) doporučujeme nasadit HTTP Proxy na samostatný server. Provozování služby HTTP Proxy na velmi vytíženém serveru (například s ESET PROTECT Server nebo databázovým serverem) může vést k potížím s připojením k ESET LiveGuard Advanced.
Pro snížení počtu odesílaných souborů a vylepšení celkového výkonu můžete vyloučit vybrané složky a procesy.

Zobrazila se mi chyba: V rámci své licence nemáte přístup k přehledu o chování souboru.

Pokud používáte EBA pro správu licencí a celkový počet klientů v rámci ESET LiveGuard Advanced licence je nižší než 100, nejste oprávněni k zobrazení úplného Přehledu o chování souboru. Některé verze konzolí pro vzdálenou správu nenabízí vůbec přístup k přehledu o chování souboru. Pro získání přehledu navyšte licenci alespoň na 100 klientů.

Mám podezřelý vzorek, co mám dělat?

Podívejte se do kapitoly Doporučení pro uživatele, kteří mají podezřelý vzorek

Aktivace ESET LiveGuard Advanced nebyla úspěšná

Pokud jste přidali licenci prostřednictvím licenčního klíče a poté jste přešli na cloudovou úroveň ochrany, v konzoli se zobrazí licence ESET LiveGuard Advanced, ale aktivace se nezdaří. Je třeba odebrat cloudovou úroveň ochrany ze správy licencí a přidat ji prostřednictvím EBA.

Jak provést diagnostiku

Pokud ESET LiveGuard Advanced nefunguje:

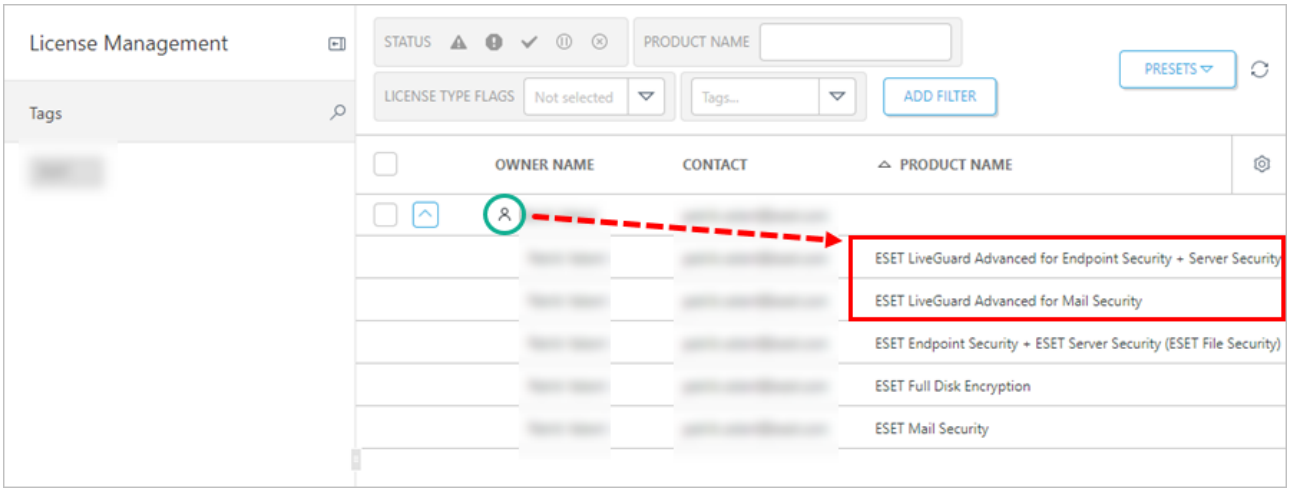
- Ujistěte se, že splňujete všechny požadavky
- Podle níže uvedených postupů můžete ve webové konzoli najít možnou příčinu.

ESET LiveGuard Advanced licence

1. Přihlaste se do webové konzole.

2. Přejděte do sekce **Další** > **Správa licence**.

3. Ověřte, že v seznamu vidíte licenci pro ESET LiveGuard Advanced. Pokud v seznamu licence není, přidejte ji prostřednictvím účtu na portále ESET Business Account nebo ESET MSP Administrator. Pokud jste licenci přidali prostřednictvím ESET Business Account, ujistěte se, že je u licence je uvedena ikona: Ta indikuje, že licence byla importována prostřednictvím EBA účtu.



Uživatelé používající podporované linuxové produkty mohou licenci a seat ID ověřit lokálně prostřednictvím terminálu.

- Ověření licence v ESET Server Security pro Linux.
- Ověření licence v ESET Endpoint Security pro Linux.

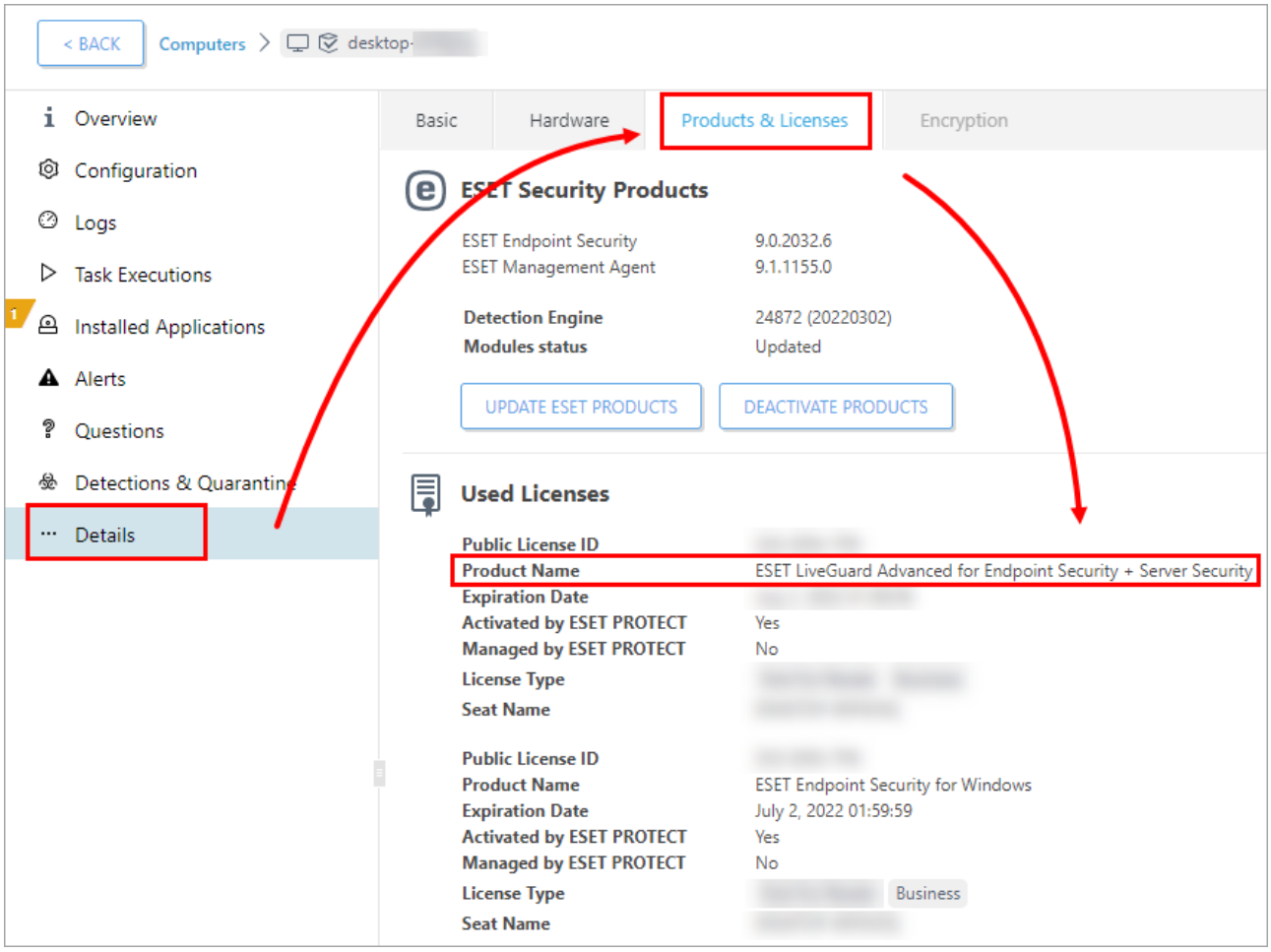
Aktivace produktu

1.V hlavním menu přejděte do sekce **Počítače**.

2.Vyberte zařízení a z kontextového menu možnost **Zobrazit detaily**.

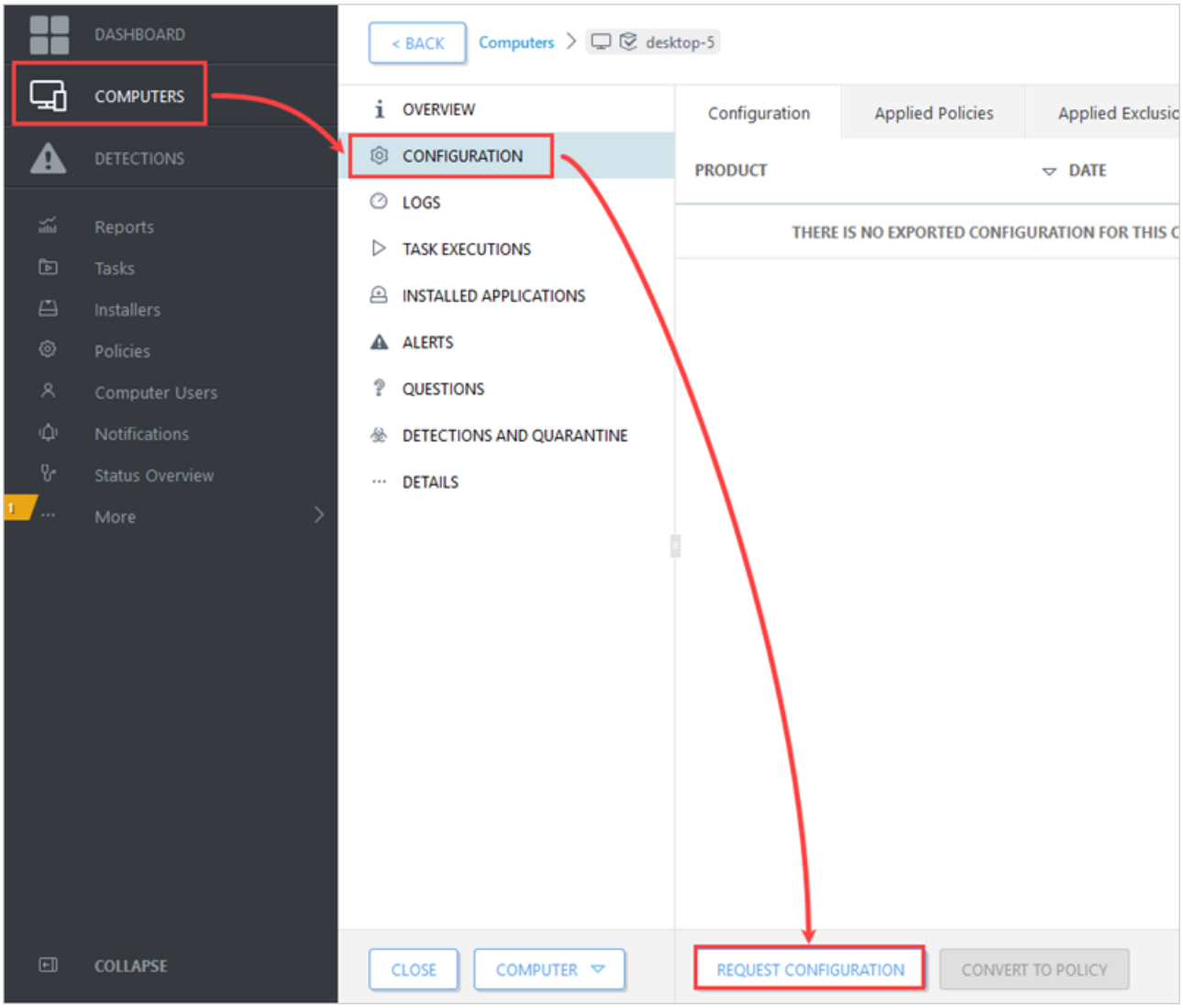
3.Dále přejděte do sekce **Detaily** a na záložku **Produkty a licence**.

4.Ověřte, že je v seznamu uvedena ESET LiveGuard Advanced licence. Pokud v seznamu licenci neuvidíte, aktivujte produkt odpovídající licencí.

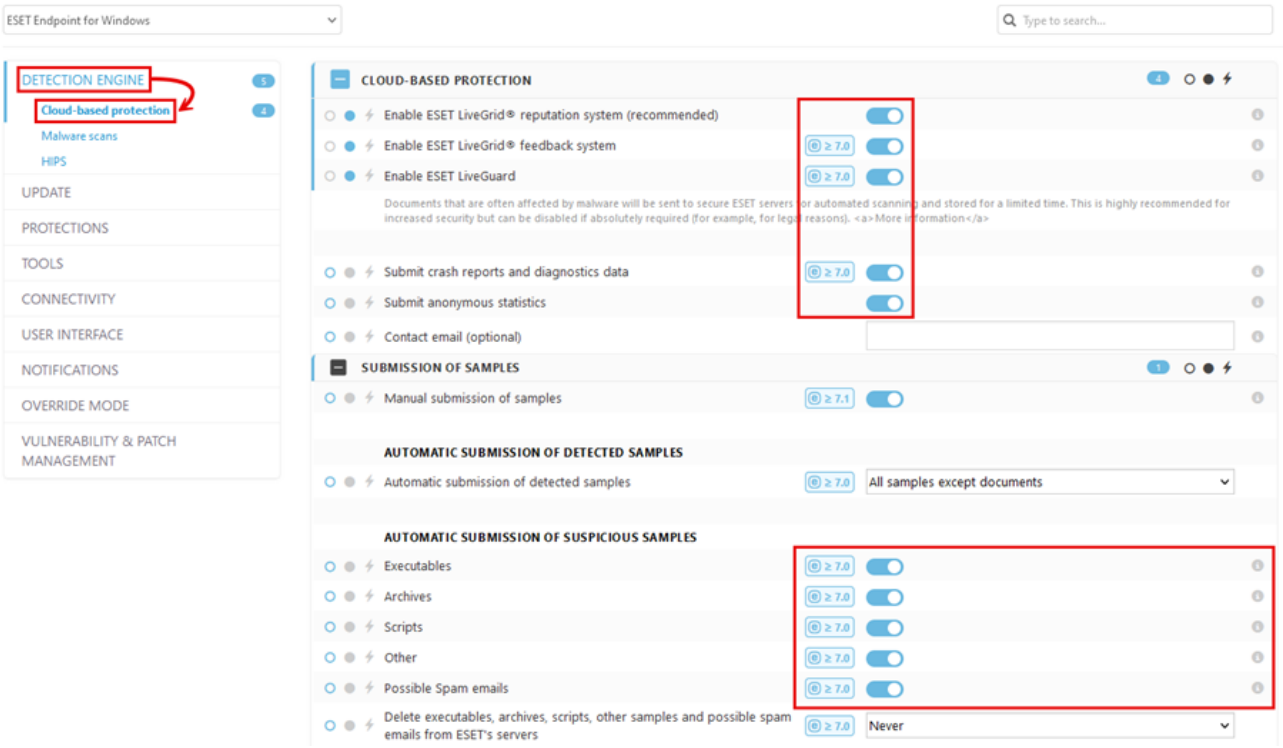


Konfigurace produktu

1.Přejděte do sekce **Počítače**, vyberte zařízení a z kontextového menu možnost **Zobrazit detaily**. Dále přejděte do sekce **Konfigurace** a klikněte na tlačítko **Vyžádat konfiguraci**.



2.Po získání konfigurace (stránku můžete aktualizovat tlačítkem) klikněte na **Bezpečnostní produkt** > **Otevřít konfiguraci**. V konfigurační šabloně přejděte do sekce **Detekční jádro** > **Cloudová ochrana** a ověřte, že je aktivní možnost ESET LiveGrid® a ESET LiveGuard Advanced. V případě serverových produktů odpovídající nastavení naleznete v sekci **Počítač** > **Cloudová ochrana**. Pokud nastavení není aktivní, vytvořte politiku pro zapnutí funkce ESET LiveGuard Advanced na cílovém počítači.



3.V případě, že se nevrátí **žádná konfigurace bezpečnostního produktu**, nainstalujte na cílový počítač podporovaný bezpečnostní produkt.

Řešení problémů – Apache HTTP Proxy

> **ESET Bridge je doporučované proxy řešení pro ESET produkty**
> Společnost ESET distribuuje ESET Bridge společně s ESET PROTECT On-Prem od verze 10.0 a jako Proxy komponenta nahrazuje dříve používaný Apache HTTP Proxy. Další informace naleznete v kapitole Srovnání ESET Bridge a Apache HTTP Proxy.

Pokud pro cachování komunikace používáte Apache HTTP Proxy a ESET LiveGuard Advanced nefunguje, aktivování diagnostického protokolování na Apache HTTP Proxy vám může pomoci při řešení tohoto problému. Protokoly si rovněž mohou vyžádat specialisté technické podpory ESET.

Mějte na paměti, že diagnostické protokolování je proces náročný na výkon. Po jeho aktivování můžete zaznamenat nižší výkon. Proto protokolování aktivujte na nezbytně nutnou dobu.

Aktivace diagnostického protokolování na Apache HTTP Proxy

1.Zastavte službu Apache HTTP Proxy příkazem: sc stop ApacheHttpProxy

2.Zazálohujte si konfigurační soubor httpd.conf. Většinou je umístěn v adresáři C:\Program Files\Apache HTTP Proxy\conf

3.Podle níže uvedených kroků upravte konfigurační soubor:

a)Odkomentujte (smazáním # ze začátku řádku):
`LoadModule log_config_module modules/mod_log_config.dll`

b)Na začátek sekce `<IfModule log_config_module>` přidejte níže uvedený řádek:

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" \"%{cache-
status}e\"" combined-cache
```

c)Zakomentujte řádek (přidáním # na začátek řádku):
`CustomLog "logs/access.log" common`

d)Změňte parametr `CacheLockMaxAge 10` na hodnotu `CacheLockMaxAge 15`.

e)Změňte parametr `ProxyTimeOut 900` na hodnotu `ProxyTimeOut 1200`.

f)V sekci `<VirtualHost *:3128>`, přidejte pod `ServerName r.edtd.eset.com` níže uvedené řádky:

```
<If "%{REQUEST_METHOD} == 'CONNECT'">
Require all denied
</If>
```

g)Změňte řádek:
`ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=10 smax=10`
na:
`ProxyPass / https://r.edtd.eset.com/ timeout=300 enablereuse=On keepalive=On ttl=100 max=100 smax=10`

h)Na konec souboru přidejte níže uvedené řádky:

```
ErrorLog '|"C:/Program Files/Apache HTTP Proxy/bin/rotatelogs.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/error.log" 1M'

CustomLog '|"C:/Program Files/Apache HTTP Proxy/bin/rotatelogs.exe" -
n 10 "C:/Program Files/Apache HTTP Proxy/logs/access.log" 100M' combined-cache
```

4.Uložte si soubor httpd.conf a spusťte službu Apache HTTP Proxy:
sc start ApacheHttpProxy

Další kroky

Protokolování ponechte aktivní po nezbytně nutnou dobu. Po deaktivování si zkopírujte protokoly. Protokoly naleznete v:

`C:/Program Files/Apache HTTP Proxy/logs/error.log`

`C:/Program Files/Apache HTTP Proxy/logs/access.log`

Pro deaktivování diagnostického protokolování:

1.Zastavte službu (Apache HTTP Proxy.

2.Obnovte konfigurační soubor ze zálohy.

3.Spusťte službu Apache HTTP Proxy.

Bezpečnostní dokumentace pro ESET LiveGuard Advanced

Úvod

Účelem tohoto dokumentu je shrnout bezpečnostní zásady a postupy uplatňované v rámci služby ESET LiveGuard Advanced. Bezpečnostní zásady a postupy jsou navrženy tak, aby byla zajištěna důvěrnost, integrita a dostupnost dat zákazníků. Mějte na paměti, že se bezpečnostní zásady a postupy mohou kdykoli změnit.

Rozsah

Účelem tohoto dokumentu je shrnout bezpečnostní postupy a zásady uplatňované v ESET LiveGuard Advanced infrastruktuře, organizaci, personálních a provozních procesech. Mezi bezpečnostní zásady a postupy patří:

1. Politiky informační bezpečnosti
2. Organizace informační bezpečnosti
3. Lidské zdroje a bezpečnost
4. Správa aktiv
5. Kontrola přístupu
6. Kryptografie
7. Environmentální a fyzická bezpečnost
8. Zabezpečení provozu
9. Zabezpečení komunikace
10. Pořízení, vývoj a údržba systému
11. Dodavatelský vztah
12. Správa incidentů v oblasti informační bezpečnosti
13. Aspekty informační bezpečnosti v rámci řízení kontinuity provozu
14. Dodržování požadavků

Bezpečnostní koncept

Společnost ESET, spol. s r.o. je držitelem certifikátu ISO 27001:2013 s integrovaným systémem správy, který pokrývá službu ESET LiveGuard Advanced.

Koncept informační bezpečnosti proto používá standard ISO 27001 k implementaci bezpečnostní strategie vícevrstvé ochrany při aplikování bezpečnostních zásad na vrstvě sítové, operačních systémů, databází, aplikací, zaměstnanců a provozních procesů. Použité bezpečnostní postupy a zásady se mají vzájemně překrývat a doplňovat.

Bezpečnostní zásady a postupy

1. Politiky informační bezpečnosti

Společnost ESET uplatňuje politiky informační bezpečnosti, které pokrývají všechny aspekty standardu ISO 27001, včetně řízení bezpečnosti informací a bezpečnostní zásady a postupy. Politiky jsou každoročně revidovány a po významných změnách aktualizovány, aby byla zajištěna jejich kontinuální vhodnost, přiměřenost a účinnost.

Společnost ESET provádí každoroční revize těchto politik a kontroly interní bezpečnosti za účelem zajištění

souladu s jejich ustanoveními. V případě nedodržování politik informační bezpečnosti jsou zaměstnancům společnosti ESET uložena disciplinární opatření a dodavatelům smluvní sankce, které mohou vést až k ukončení smlouvy.

2. Organizace informační bezpečnosti

Organizace informační bezpečnosti služby ESET LiveGuard Advanced se skládá z více týmů a jednotlivců zapojených do informační bezpečnosti a IT, včetně:

- výkonného managementu společnosti ESET,
- týmů interní bezpečnosti společnosti ESET,
- IT týmů podnikových aplikací,
- dalších podpůrných týmů.

Odpovědnost za informační bezpečnost je přidělována v souladu se zavedenými politikami informační bezpečnosti. Interní procesy jsou identifikovány a posuzovány z hlediska rizik vyplývajících z neoprávněné nebo neúmyslné modifikace nebo zneužití aktiv společnosti ESET. Při rizikových nebo citlivých činnostech souvisejících s interními procesy je za účelem snížení rizika uplatňován princip rozdělení povinností.

Právní tým společnosti ESET je zodpovědný za kontakt s orgány státní správy, včetně slovenských regulačních orgánů v oblasti kybernetické bezpečnosti a ochrany osobních údajů. Tým interní bezpečnosti společnosti ESET je zodpovědný za kontakt se zájmovými skupinami, jako je například ISACA. Výzkumné týmy společnosti ESET jsou zodpovědné za komunikaci s dalšími společnosti zabývajícími se bezpečností a širší komunitou pro kybernetickou bezpečnosti.

Informační bezpečnost je zohledněna v projektovém řízení pomocí aplikovaného rámce řízení projektů od koncepce až po dokončení projektu.

Práci na dálku a práci z domova pokrývají politiky implementované na mobilních zařízeních, které zahrnují použití silné kryptografické ochrany dat na mobilních zařízeních při pohybu mezi nedůvěryhodnými sítěmi. Bezpečnostní kontroly na mobilních zařízeních jsou navrženy tak, aby fungovaly nezávisle na interních sítích a interních systémech společnosti ESET.

3. Lidské zdroje a bezpečnost

Společnost ESET používá standardní postupy v oblasti lidských zdrojů, včetně politik určených k dodržování informační bezpečnosti. Tyto postupy jsou platné po celý životní cyklus zaměstnance a vztahují se na všechny týmy, které mají přístup k prostředí služby ESET LiveGuard Advanced.

4. Správa aktiv

Infrastruktura služby ESET LiveGuard Advanced je součástí inventáře aktiv společnosti ESET s výhradním vlastnictvím a pravidly aplikovanými podle typu a citlivosti aktiv. Společnost ESET má definované interní klasifikační schéma. Veškerá data a konfigurace související se službou ESET LiveGuard Advanced jsou klasifikována jako důvěrná.

5. Kontrola přístupu

Politika řízení přístupu společnosti ESET upravuje každý přístup v rámci služby ESET LiveGuard Advanced. Řízení přístupu se nastavuje na úrovni infrastruktury, síťových služeb, operačního systému, databáze a aplikace. Správa úplného přístupu uživatelů na úrovni aplikace je autonomní.

Přístup k backendu je výhradně omezen na oprávněné osoby a role. Při správě přístupu zaměstnanců společnosti

ESET k infrastruktuře a sítím služby ESET LiveGuard Advanced se využívají standardní procesy společnosti ESET pro (de)registraci uživatelů, (de)provisioning, správu oprávnění a kontrolu přístupových oprávnění uživatelů.

Pro ochranu přístupu ke všem datům souvisejícím se službou ESET LiveGuard Advanced se používá silné ověřování.

6. Kryptografie

Za účelem ochrany dat ESET LiveGuard Advanced jsou při svém přenosu šifrována pomocí silné kryptografie (SSL).

7. Environmentální a fyzická bezpečnost

ESET LiveGuard Advanced je cloudová služba. Společnost ESET využívá privátní cloud a cloudovou platformu Microsoft Azure. Fyzické umístění datového centra privátního cloudu je výhradně v Evropské unii (EU). Cloudová část na platformě Microsoft Azure není omezena na území EU, používá se však pouze k ukládání jednosměrných kontrolní součtů vytvořených z odeslaných souborů bez zahrnutí osobních údajů. Data zákazníků jsou při svém přenosu chráněna silnou kryptografií.

8. Zabezpečení provozu

Služba ESET LiveGuard Advanced je provozována automatizovanými prostředky na základě přísných provozních postupů a konfiguračních šablon. Všechny změny, včetně změn v konfiguraci a nasazení nového balíčku, se nasazením do produkčního prostředí schvalují a testují ve vyhrazeném testovacím prostředí. Vývojová, testovací a produkční prostředí jsou od sebe oddělená. Data služby ESET LiveGuard Advanced se nacházejí výhradně v produkčním prostředí.

Prostředí služby ESET LiveGuard Advanced je sledováno prostřednictvím monitorování provozu za účelem rychlé identifikace problémů a zajištění dostatečné kapacity všem službám na úrovni sítě a hostitele.

Veškerá konfigurační data jsou uložena v našich pravidelně zálohovaných úložištích, aby bylo možné automaticky obnovit konfiguraci prostředí. Zálohovaná data služby ESET LiveGuard Advanced jsou ukládána lokálně i externě.

Zálohy jsou šifrovány a v rámci testování kontinuity podnikání je pravidelně ověřována jejich obnovitelnost.

Audit systémů je prováděn dle interních standardů a směrnic. Protokoly a události z infrastruktury, operačního systému, databáze, aplikačních serverů a prvků zabezpečení se shromažďují nepřetržitě. Protokoly jsou dále zpracovávány týmy IT a interní bezpečnosti za účelem identifikace provozních a bezpečnostních anomálií a incidentů informační bezpečnosti.

Společnost ESET se řídí všeobecným technickým procesem pro správu zranitelností k řízení zranitelností v infrastruktuře ESET, včetně služby ESET LiveGuard Advanced a dalších produktech ESET. Součástí tohoto procesu je proaktivní skenování zranitelností a opakované penetrační testování infrastruktury, produktů a aplikací.

Společnost ESET má zavedené interní směrnice pro bezpečnost interní infrastruktury, sítí, operačních systémů, databází, aplikačních serverů a aplikací. Jejich dodržování je kontrolováno prostřednictvím monitorování technického souladu a našeho programu interního auditu informační bezpečnosti.

9. Zabezpečení komunikace

Prostředí služby ESET LiveGuard Advanced je segmentováno pomocí nativních možností dostupných v cloudu, kdy přístup k síti je omezen pouze na nezbytné služby v rámci síťových segmentů. Dostupnost síťových služeb je dosaženo pomocí nativních možností dostupných v cloudu, jako jsou zóny dostupnosti, vyrovnávání zátěže a redundance. Komponenty vyhrazené pro vyrovnávání zátěže jsou nasazeny za účelem ověřování a směrování

koncových zařízení k instanci služby ESET LiveGuard Advanced. Síťový provoz je nepřetržitě monitorován na výskyt provozních a bezpečnostních anomálií. Potenciální útoky lze vyřešit pomocí nativních možností dostupných v cloudu nebo nasazených bezpečnostních řešení. Veškerá síťová komunikace je šifrována pomocí obecně dostupných technik, včetně protokolů IPsec a TLS.

10. Pořízení, vývoj a údržba systému

Vývoj systémů služby ESET LiveGuard Advanced probíhá v souladu s politikou pro vývoj bezpečného softwaru společnosti ESET. Týmy interní bezpečnosti se na vývoji služby ESET LiveGuard Advanced podílejí již od počáteční fáze a dohlížejí na všechny aspekty vývoje a údržby. Tým interní bezpečnosti definuje a kontroluje plnění bezpečnostních požadavků v různých fázích vývoje softwaru. Bezpečnost všech služeb, včetně nově vyvinutých, je od jejich vydání průběžně testována.

11. Dodavatelský vztah

Relevantní dodavatelský vztah je veden podle platných směrnic společnosti ESET, které upravují řízení vztahů se zákazníky a smluvní požadavky z hlediska informační bezpečnosti a ochrany osobních údajů. Kvalita a bezpečnost služeb poskytovaných poskytovatelem kritických služeb podléhá pravidelnému hodnocení.

Dále společnost ESET u služby ESET LiveGuard Advanced uplatňuje princip přenositelnosti, aby se zabránilo závislosti na konkrétním dodavateli.

12. Správa incidentů v oblasti informační bezpečnosti

Správa incidentů v oblasti informační bezpečnosti souvisejících se službou ESET LiveGuard Advanced je řízena podobně jako u jiných infrastruktur společnosti ESET a opírá se o definované postupy řešení incidentů. Role v rámci reakce na incidenty jsou definovány a rozděleny mezi více týmů, nejen z oblasti IT, bezpečnosti, právní, lidských zdrojů, vztahů s veřejností a výkonného managementu. Incidenty třídí tým interní bezpečnosti, které si následně přebírá sestavený tým zodpovědný za řešení incidentu. Tento tým zajistí další koordinaci ostatních týmů, které se podílejí na řešení incidentu. Tým interní bezpečnost je rovněž zodpovědný za shromažďování důkazů a získaných poznatků. Vznik incidentu a jeho řešení je sděleno dotčeným stranám. Právní tým společnosti ESET je v případě potřeby zodpovědný za informování regulačních orgánů v souladu se všeobecným nařízení o ochraně osobních údajů (GDPR) a aktem EU o kybernetické bezpečnosti EU transponujícím směrnici o bezpečnosti sítí a informačních systémů (NIS).

13. Aspekty informační bezpečnosti v rámci řízení kontinuity provozu

Kontinuita provozu služby ESET LiveGuard Advanced je zakódována v robustní architektuře, která maximalizuje dostupnosti poskytovaných služeb. V případě katastrofického selhání všech redundantních uzlů komponent služby ESET LiveGuard Advanced, nebo služby ESET LiveGuard Advanced samotné, je možné provést kompletní obnovení z externích záloh a konfiguračních dat. Proces obnovy je pravidelně testován.

14. Dodržování požadavků

Dodržování regulačních a smluvních požadavků souvisejících se službou ESET LiveGuard Advanced je pravidelně posuzováno a přezkoumáváno podobně jako jiná infrastruktura a procesy společnosti ESET. Provádějí se nezbytná opatření k zajištění soustavného dodržování požadavků. Společnost ESET je registrována jako poskytovatel digitálních služeb v oblasti cloud computingu, mezi které spadají další služby společnosti ESET včetně ESET LiveGuard Advanced. Mějte na paměti, že aktivity společnost ESET týkající se dodržování předpisů nemusí nemusí nutně znamenat, že jsou splněny celkové požadavky zákazníků na dodržování předpisů.

Fair Use Policy

Popis Fair Use Policy

Fair Use Policy omezuje počet souborů zasílaných zákazníkem k analýze. Limit na počet souborů se odvíjí od úrovně ESET LiveGuard Advanced. Bližší informace naleznete v níže uvedené tabulce.

Limit na počet souborů je následující: **50 souborů / klient / měsíc**. Počet souborů se bere jako celek. To znamená, že jedna stanice můžete k analýze zaslat více vzorků, jiná méně.

Příklad:

- Zákazník s 500 stanicemi může každý měsíc odeslat až 25 000 vzorků.
- Zákazník s 10 000 stanicemi může každý měsíc odeslat až 500 000 vzorků.

Vlastnosti úrovní ESET LiveGuard Advanced

Seznam dostupných úrovní ESET LiveGuard Advanced a jejich vlastnosti naleznete v níže uvedené tabulce.

Název produktové řady	Minimální počet klientů	Dostupné pro ESET PROTECT On-Prem	Dostupné pro ESET PROTECT	Licence umožňuje vytvoření ESET PROTECT instance	Dostupné v ESET MSP Administrator 2	Limit na počet souborů
ESET LiveGuard Advanced	5	✓	✓	⛔	✓	Ne
ESET PROTECT Complete	5	✓	✓	✓	✓	Ano
ESET PROTECT Mail Plus		✓	✓	✓	✓	Ano
ESET PROTECT Advanced	5	✓	✓	✓	✓	Ano
ESET Dynamic Endpoint Protection	5	✓	⛔	⛔	⛔	Ano
ESET Dynamic Endpoint Protection - Antivirus Level	5	✓	⛔	⛔	⛔	Ano
ESET Targeted Attack Protection	250	✓	⛔	⛔	⛔	Ano

Mohu získat licenci bez limitu na počet odeslaných souborů?

Více informací o takové licenci zjistíte u svého lokálního Partnera ESET.

Jak zjistím počet odeslaných souborů?

V konzoli pro vzdálenou správu si vygenerujte přehled týkající se počtu odeslaných souborů.

Jak zabráním v odeslání konkrétních typů souborů?

Pokud překračujete limit na počet odeslaných souborů, analyzujte soubory, které se ze stanic zasílají. Následně zvažte vytvoření výjimek na složky, které jsou pro vás bezpečné. Některé aplikace nebo vývojářské nástroje mohou generovat nadměrné množství souborů, které nepředstavují hrozbu, nebo je není nutné k analýze zasílat. Počet zasílaných souborů k analýze snížíte jejich vyhodnocením a vytvořením odpovídajících výjimek.

Zásady ochrany osobních údajů

Ochrana osobních údajů je pro společnost ESET, spol. s r. o., se sídlem na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, která je zapsaná v Obchodním registru vedeném Okresním soudem Bratislava I, oddíl Sro, vložka číslo 3586/B, IČO: 31333532, jako pro správce údajů („ESET“ nebo „My“) obzvlášť důležitá. Snažíme se dodržovat požadavky na transparentnost, které jsou právně standardizovány v rámci Obecného nařízení EU o ochraně osobních údajů („GDPR“). Abychom dosáhli tohoto cíle, zveřejňujeme tyto Zásady ochrany osobních údajů výhradně za účelem informování našich zákazníků („Koncový uživatel“ nebo „Vy“) jako subjektů údajů o následujících tématech týkajících se ochrany osobních údajů:

- Právní základ pro zpracování osobních údajů
- Sdílení a důvěrnost dat
- Zabezpečení dat
- Vaše práva jako subjektu údajů
- Zpracování vašich osobních údajů
- Kontaktní informace.

Zpracování vašich osobních údajů

Služby poskytované společností ESET implementované v našem webovém produktu jsou poskytovány za podmínek uvedených v Podmínkách použití, ale některé z nich mohou vyžadovat zvláštní pozornost. Rádi bychom vám poskytli další informace o zpracování údajů spojených s poskytováním našich produktů a služeb. Poskytujeme různé služby s přihlédnutím k podmínkám a produktové dokumentaci. Aby všechny tyto služby fungovaly, potřebujeme shromažďovat následující informace:

- Vzorky, jako jsou soubory předdefinované a vybrané Koncovým uživatelem, jsou nahrány do služby ESET za účelem analýzy a výsledek je odeslán zpět uživateli. Meta data jsou shromažďována ve vaší místní konzole pro správu, která musí být uvedena jako podporovaná.

- Informace o licencích, například ID licence, a osobní údaje, jako jsou jméno, příjmení, adresa, e-mailová adresa, jsou vyžadovány pro fakturační účely, ověření pravosti licencí a poskytování našich služeb.
- Za účelem poskytování podpory mohou být vyžadovány kontaktní informace a údaje obsažené ve vašich požadavcích na podporu. V závislosti na kanálu, kterým se nás rozhodnete kontaktovat, můžeme shromáždit vaši e-mailovou adresu, telefonní číslo, informace o licenci, podrobnosti o produktu a popis vašeho případu podpory. Můžete být vyzváni k poskytnutí dalších informací, které usnadní poskytnutí podpory.

Nechceme shromažďovat data mimo uvedený rozsah, někdy je však nemožné tomu zabránit. Náhodně shromážděné údaje mohou být zahrnuty v samotném škodlivém softwaru (kterým byly shromážděny bez vašeho

vědomí nebo souhlasu) nebo mohou být součástí dokumentů. Nemáme v úmyslu, aby byly součástí našich systémů nebo aby byly zpracovány pro účely uvedené v těchto Zásadách ochrany osobních údajů.

Sdílení a důvěrnost dat

Vaše data nesdílíme se třetími stranami. ESET je ale společnost s celosvětovou působností a v rámci naší prodejní, servisní a podpůrné sítě využíváme přidružené firmy a partnery. Informace o licencování, fakturaci a technické podpoře, které společnost ESET zpracovává, mohou být přenášeny k přidruženým firmám nebo partnerům a zpět za účelem plnění smlouvy EULA, jako je poskytování služeb nebo podpora.

Společnost ESET upřednostňuje zpracování svých dat v Evropské unii (EU). V závislosti na vaší poloze (používání našich produktů a/nebo služeb mimo EU) a/nebo službě, kterou jste si zvolili, ovšem může být nutné přenést vaše data do země mimo EU. Služby třetích stran využíváme například ve spojení s cloudovým computingem. V těchto případech si naše poskytovatele služeb pečlivě vybíráme a zajišťujeme příslušnou úroveň ochrany dat prostřednictvím smluvních, ale i technických a organizačních opatření. Je pravidlem, že uzavíráme standardní smluvní klauzule pro EU, ke kterým v případě potřeby přijímáme doplňková smluvní omezení.

U některých zemí mimo EU, jako jsou Spojené království nebo Švýcarsko, již EU uznala srovnatelnou úroveň ochrany dat. Vzhledem ke srovnatelné úrovni ochrany dat nevyžaduje přenos dat do těchto zemí žádnou speciální autorizaci nebo smluvní dohodu.

Spoléháme se na služby třetích stran související s cloud computingem, které poskytuje společnost Microsoft jako poskytovatel cloudových služeb.

Práva subjektu údajů

Práva každého koncového uživatele jsou důležitá a rádi bychom vás informovali, že všichni koncoví uživatelé (z libovolné země v EU nebo mimo ni) mají společností ESET garantována následující práva. Pokud chcete uplatnit svá práva subjektu údajů, můžete nás kontaktovat prostřednictvím formuláře podpory nebo e-mailem na adrese dpo@eset.sk. Za účelem identifikace po vás budeme požadovat následující údaje: Jméno, e-mailová adresa a – pokud jsou k dispozici – licenční klíč nebo číslo zákazníka a afilace společnosti. Neposílejte nám prosím žádné jiné osobní údaje, jako je datum narození. Rádi bychom vás upozornili, že v zájmu zpracování vaší žádosti a za účelem identifikace budeme zpracovávat vaše osobní údaje.

Právo odvolat souhlas. Právo odvolat souhlas lze uplatnit pouze v případě zpracování založeného výhradně na souhlasu. Pokud zpracováváme vaše osobní údaje na základě vašeho souhlasu, máte právo svůj souhlas kdykoli odvolat i bez uvedení důvodu. Vaše odvolání souhlasu bude platné pouze do budoucna a nebude mít vliv na legálnost údajů zpracovaných před odvoláním.

Právo vznést námitku. Právo vznést námitku proti zpracování lze uplatnit v případě zpracování založeného na oprávněném zájmu společnosti ESET nebo třetí strany. Pokud zpracováváme vaše osobní údaje v zájmu ochrany oprávněného zájmu, máte jako subjekt údajů právo kdykoli vznést námitku vůči námi uvedenému oprávněnému zájmu a vůči zpracování vašich osobních údajů. Vaše námitka bude platná pouze do budoucna a nebude mít vliv na zákonnost údajů zpracovaných před vznesením námitky. Pokud vaše osobní údaje zpracováváme pro účely přímého marketingu, není nutné u námitky uvádět důvody. Platí to rovněž pro profilování, pokud je spojeno s přímým marketingem. Ve všech ostatních případech vás žádáme, abyste nás stručně informovali o svých stížnostech vůči oprávněnému zájmu společnosti ESET na zpracování vašich osobních údajů.

Upozorňujeme vás, že v některých případech jsme i přes odvolání vašeho souhlasu oprávněni dále zpracovávat vaše osobní údaje na jiném právním základě, například za účelem plnění smlouvy.

Právo na přístup. Jako subjekt údajů máte právo kdykoli bezplatně získat informace o vašich údajích, které má

společnost ESET uloženy.

Právo na opravu. Pokud si o vás omylem uložíme nesprávné osobní údaje, máte právo na jejich opravu.

Právo na výmaz a právo na omezení zpracování. Jako subjekt údajů máte právo požádat o výmaz nebo o omezení zpracování vašich osobních údajů. Pokud například zpracováváme vaše osobní údaje s vaším souhlasem a vy tento souhlas odvoláte, přičemž neexistuje žádný jiný právní základ (například smlouva), vymažeme vaše osobní údaje okamžitě. Vaše osobní údaje budou rovněž vymazány, jakmile nebudou dále vyžadovány pro uvedené účely na konci období uchovávání.

Pokud vaše údaje využíváme pouze za účelem přímého marketingu a vy odvoláte svůj souhlas nebo vznesete námitku vůči uvedenému oprávněnému zájmu společnosti ESET, omezíme zpracování vašich osobních údajů do té míry, že vaše kontaktní údaje přidáme na naši interní černou listinu, abychom předešli nevyžádanému kontaktování. V ostatních případech budou vaše osobní údaje vymazány.

Upozorňujeme, že může být potřebné, abychom vaše údaje měly uloženy do konce platnosti povinností na uchovávání a období stanovených legislativou nebo dozorčími úřady. Povinnosti na uchovávání a příslušná období mohou také vyplývat ze zákonů Slovenské republiky. Po uplynutí daných lhůt budou příslušné údaje rutinně vymazány.

Právo na přenositelnost dat. Jako subjektu dat vám rádi poskytneme osobní údaje, které o vás společnost ESET zpracovává, ve formátu xls.

Právo podat stížnost. Jako subjekt údajů máte právo kdykoli podat stížnost u dozorčího orgánu. Společnost ESET podléhá regulaci zákonů Slovenské republiky a je vázána právními předpisy o ochraně údajů Evropské unie. Příslušným dozorčím orgánem pro ochranu osobních údajů je Úrad na ochranu osobných údajov Slovenskej republiky, který sídlí na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Věříme, že veškeré informace, které zpracováváme, jsou cenné a nezbytné pro náš legitimní zájem, kterým je poskytování služeb a produktů našim zákazníkům.

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

Podmínky použití

Tyto podmínky použití (dále jako „Podmínky“) představují zvláštní smlouvu mezi společností ESET spol. s r.o., se sídlem Einsteinova 24, 85101 Bratislava, Slovak Republic, zapsanou v Obchodním rejstříku vedeném Okresním soudem Bratislava I v oddílu Sro, vložka 3586/B, s obchodním registračním číslem 31333532 (dále jen „ESET“ nebo „Poskytovatel“) a Vámi, fyzickou anebo právnickou osobou (dále jen „Vy“ nebo „Uživatel“) využívající online služby ESET LiveGuard Advanced, které vlastní a řídí společnost ESET (dále jako „ESET LiveGuard Advanced“). Pokud využíváte ESET LiveGuard Advanced jménem organizace, souhlasíte s těmito Podmínkami jménem dané

organizace a zaručujete se, že máte oprávnění zavázat tuto organizaci těmito Podmínkami. V takovém případě se pojmy „Uživatel“ a „Vy“ budou vztahovat na tuto organizaci. Tyto Podmínky použití si pozorně přečtěte. Vztahují se také na služby poskytované společností ESET prostřednictvím nebo ve vztahu k ESET LiveGuard Advanced. Konkrétní podmínky používání jednotlivých služeb nad rámec těchto Podmínek jsou uváděny u jednotlivých služeb, přičemž jejich přijetí je součástí procesu aktivace služeb.

Zabezpečení a ochrana dat

ESET LiveGuard Advanced zajišťuje přístup ke službám poskytovaným společností ESET. K registraci a používání ESET LiveGuard Advanced a pro účely poskytování a správy služeb ESET LiveGuard Advanced je vyžadováno celé jméno uživatele, název společnosti, stát, platná e-mailová adresa, telefonní číslo, údaje o licenci a statistiky. Souhlasíte s tím, že na servery Poskytovatele anebo jeho obchodních partnerů mohou být shromažďovány a přenášeny údaje, které mají za účel zabezpečit funkčnost a oprávněnost používání Softwaru a ochranu práv Poskytovatele. V souvislosti s uzavřením těchto Podmínek jsou Poskytovatel nebo obchodní partneři oprávněni pro účely poskytování podpory a plnění těchto Podmínek přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu. Jste oprávněni používat službu ESET LiveGuard Advanced výhradně za účelem a způsobem, pro který je určena podle těchto Podmínek, podmínek jednotlivých služeb a dokumentace.

Pro účely poskytování ESET LiveGuard Advanced je vyžadováno odesílání souborů (dále jen „data“). Data poskytujete společnosti ESET výlučně za účelem poskytování služby ESET LiveGuard Advanced. Data jsou zpracovávána a uchovávána v souladu s bezpečnostními politikami a postupy společnosti ESET, stejně tak v souladu se Zásadami ochrany osobních údajů.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů.

Fair Use Policy

Jste povinni dodržovat technická omezení stanovená v dokumentaci. Souhlasíte s tím, že budete Účet 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 Uživatelů, aby mohl služby využívat nejvyšší možný počet Uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Účtu a odstranění dat a informací.

Podrobnosti o férovém používání produktu naleznete v dokumentu Fair Use Policy.

Software

Společnost ESET nebo její příslušní dodavatelé vlastní nebo mohou uplatňovat autorská práva na veškerý software, který je k dispozici stránkách účtu (dále jako „Software“). Software je možné používat jen v souladu s licenční smlouvou s koncovým uživatelem (dále jako „EULA“). Smlouva EULA se poskytuje spolu se Softwarem nebo je jeho součástí. Software dodaný se smlouvou EULA nelze nainstalovat bez souhlasu uživatele se smlouvou EULA. Další informace týkající se licencování, autorských práv, dokumentace a ochranných známek se nacházejí v Právních informacích.

Restrikce

Nesmíte Účet kopírovat, šířit, oddělovat jeho části anebo vytvářet od Účtu odvozená díla. Při používání Účtu jste povinný dodržovat následovné omezení:

(a) Účet nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Účtu anebo kopií Účtu jinak, než je výslovně uvedené v této Dohodě.

(b) Účet nesmíte prodat, sublicencovat, pronajmout anebo pronajmout si, vypůjčit si ho anebo používat na poskytování komerčních služeb.

(c) Účet nesmíte zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusit získat zdrojový kód Účtu s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

(d) Souhlasíte s tím, že budete používat Účet jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Účet používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

Vyloučení odpovědnosti

JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE ÚČET A SLUŽBY JSOU POSKYTOVÁNY „TAK JAK JSOU", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ PLATNÝMI PRÁVNÍMI PŘEDPISY. 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 ÚČET NEBO SLUŽBY NEPORUŠUJÍ ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. POSKYTOVATEL ANI ŽÁDNÁ JINÁ STRANA NEPOSKYTUJE ŽÁDNOU ZÁRUKU, ŽE ÚČET NEBO SLUŽBY BUDOU SPLŇOVAT VAŠE POŽADAVKY ANI ŽE ÚČET NEBO SLUŽBY BUDOU FUNGOVAT NEPŘERUŠENĚ NEBO BEZCHYBNĚ. VEŠKEROU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR A POUŽÍVÁNÍ ÚČTU A SLUŽEB NA DOSAŽENÍ ZAMYŠLENÝCH VÝSLEDKŮ A ZA VÝSLEDKY Z NICH ZÍSKANÉ PŘEBÍRÁTE VY.

Tyto Podmínky nezakládají na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v těchto Podmínkách žádné jiné závazky.

Omezení zodpovědnosti

V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ ZÁKONY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO DODAVATELÉ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ ČINNOSTI, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, POJISTNÉ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, AŤ UŽ NA ZÁKLADĚ SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT ÚČET, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL, JEHO DODAVATELÉ ANEBO PŘIDRUŽENÉ SPOLEČNOSTI BYLI UVĚDOMĚNÍ O MOŽNOSTI VZNIKU TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ, DODAVATEŮ ANEBO PŘIDRUŽENÝCH SPOLEČNOSTÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA DANOU SLUŽBU NEBO ÚČET.

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 těchto Podmínek, 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 těchto Podmínek, 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 oddílu (a) bodu Soulad se zákony o kontrole obchodu těchto Podmínek; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z těchto Podmínek 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 těchto Podmínkách 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.

Rozhodné právo a jazyk

Tyto Podmínky se řídí a musí být vykládány v souladu se zákony Slovenské republiky. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Jste-li spotřebitelem s obvyklým bydlištěm v EU, vztahuje se na vás také další ochrana, kterou vám poskytují závazná ustanovení právních předpisů platných v zemi vašeho bydliště.

Výslovně souhlasíte, že řešením jakýchkoli sporů nebo nároků vůči Poskytovateli nebo sporů a nároků souvisejících s vaším používáním Softwaru, Účtu nebo Služeb nebo sporů vyplývající z těchto Podmínek nebo Zvláštních podmínek (pokud jsou k dispozici) bude pověřen příslušný Obvodní soud v Bratislavě I. (Slovenská republika) a výslovně souhlasíte s výkonem jurisdikce tímto soudem. Jste-li spotřebitelem s obvyklým bydlištěm v EU, můžete také uplatnit nárok na vymáhání svých spotřebitelských práv v místě příslušné jurisdikce nebo v zemi EU, ve které žijete. Kromě toho můžete také použít online platformu pro řešení sporů, kterou naleznete zde: https://ec.europa.eu/consumers/odr/. Před oficiálním uplatněním nároku nás však prosím nejprve kontaktujte.

V případě jakýchkoli rozporů mezi jazykovými verzemi těchto Podmínek bude vždy rozhodující anglická verze, která je dostupná zde.

Všeobecná ustanovení

Společnost ESET si vyhrazuje právo kdykoli upravit tyto Podmínky a dokumentaci nebo jakékoli jejich části, a to aktualizací příslušného dokumentu tak, aby se do něj promítly změny zákonů nebo změny týkající se účtu.
O jakékoli změně Podmínek v rámci účtu budete informováni. Pokud s danými změnami Podmínek nebudete

souhlasit, můžete účet zrušit. Pokud po upozornění na tyto změny svůj účet nezrušíte, jste vázáni případnými dodatky nebo úpravami těchto Podmínek. Doporučujeme vám pravidelně navštěvovat tuto stránku a přečíst si aktuální Podmínky, které se vztahují k používání účtu.

Oznámení

Všechna oznámení je třeba doručit na následující adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Dodatek č.1

ESET Management Agent EULA

Dodatek č.2

Smlouva o zpracování údajů

Dodatek č.3

Standardní smluvní body

ESET Management Agent EULA

Platné od 25. ledna 2024.

DŮLEŽITÉ UPOZORNĚNÍ: Před stáhnutím, instalací, kopírováním anebo použitím si pozorně přečtěte níže uvedené podmínky používání produktu. **INSTALACÍ, STÁHNUTÍM, KOPÍROVÁNÍM ANEBO POUŽITÍM SOFTWARU VYJADŘUJETE SVŮJ SOUHLAS S TĚMITO PODMÍNKAMI A BERETE NA VĚDOMÍ ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ.**

Licenční ujednání s koncovým uživatelem

Tato Licenční smlouva s koncovým uživatelem („Smlouva“) uzavřená mezi společností ESET, spol. s r. o., se sídlem Einsteinova 24, 851 01 Bratislava, Slovenská republika, s obchodním registračním číslem 31333532 ("ESET" nebo "Poskytovatel") a Vámi, fyzickou anebo právnickou osobou ("Vy" anebo "Koncový uživatel") Vás opravňuje k používání Softwaru definovaného v článku 1 této Smlouvy. Software definovaný v článku 1 této Smlouvy může být uložen na fyzickém datovém nosiči, zaslán elektronickou poštou, stažen z internetu, stažen ze serverů Poskytovatele nebo získán z jiných zdrojů za podmínek a ujednání uvedených níže.

TOTO NENÍ KUPNÍ SMLOUVA, ALE DOHODA O PRÁVECH KONCOVÉHO UŽIVATELE. Poskytovatel zůstává vlastníkem kopie Software a případného fyzického média na kterém se Software dodává v obchodním balení jako i všech kopií Software na které má Koncový uživatel právo podle této Dohody.

Kliknutím na tlačítko „Přijímám“ nebo „Přijímám...“ při instalaci, stahování, kopírování nebo používání Softwaru vyjadřujete souhlas s podmínkami této Smlouvy a berete na vědomí Zásady ochrany osobních údajů. V případě, že s některými podmínkami této Smlouvy nebo ustanoveními Zásad ochrany osobních údajů nesouhlasíte, ihned klikněte na možnost pro zrušení, zrušte instalaci nebo stahování nebo zlikvidujte, případně vraťte Software, instalační média, průvodní dokumentaci a doklad o nákupu Poskytovateli nebo pracovníkům prodejny, kde jste Software pořídili.

SOUHLASÍTE S TÍM, ŽE VAŠE POUŽÍVÁNÍ SOFTWARE JE ZNAKEM TOHO, ŽE JSTE SI PŘEČETLI TUTO DOHODU, ROZUMÍTE JÍ, A SOUHLASÍTE S TÍM, ŽE JSTE VÁZANÍ JEJÍMI USTANOVENÍMI.

1. **Software**. Pojem „Software“ v této Smlouvě znamená: (i) počítačový program doprovázený touto Smlouvou včetně všech jeho součástí; (ii) obsah disků, médií CD-ROM, médií DVD, e-mailů a jejich všech případných příloh, anebo jiných médií ke kterým je přiložená tato Smlouva včetně Softwaru dodaného ve formě objektového kódu na hmotném nosiči dat, elektronickou poštou nebo staženého prostřednictvím internetu, (iii) se Softwarem související vysvětlující materiály a jakoukoliv dokumentaci, zejména jakýkoliv popis Software, jeho specifikaci, popis vlastností, popis ovládání, popis operačního prostředí ve kterém se Software používá, návod na použití anebo instalaci Softwaru anebo jakýkoliv popis správného používání Software („Dokumentace“), (iv) kopie Softwaru, opravy případných chyb Softwaru, dodatky k Softwaru, rozšíření Softwaru, modifikované verze Softwaru a aktualizace součástí Softwaru, jak jsou dodané, na které Vám Poskytovatel uděluje Licenci ve smyslu článku 3. této Smlouvy. Software se dodává výlučně ve formě objektového spustitelného kódu.

2. **Instalace, počítač a licenční klíč**. Software dodaný na datovém nosiči, zaslaný elektronickou poštou, stažený z internetu, stažený ze serverů Poskytovatele nebo získaný z jiných zdrojů vyžaduje instalaci. Software musíte nainstalovat na správně nakonfigurovaný počítač splňující minimální požadavky uvedené v Dokumentaci. Způsob instalace je popsaný v Dokumentaci. Na počítači, na který Software instalujete, nesmí být nainstalované žádné počítačové programy anebo technické vybavení, které by mohlo Software nepříznivě ovlivnit. Počítačem se rozumí hardware, mimo jiné včetně osobních počítačů, notebooků, pracovních stanic, palmtopů, smartphonů, ručních elektronických zařízení nebo jiných elektronických zařízení, pro který je Software navržen, na který je nainstalován anebo používán. Licenčním klíčem se rozumí jedinečná sekvence symbolů, písmen, čísel nebo zvláštních znaků poskytnutých Koncovému uživateli, aby bylo možné legálně využívat Software, jeho konkrétní verzi nebo prodloužit dobu trvání Licence v souladu s touto Smlouvou.

3. **Licence**. Za předpokladu, že jste souhlasili s podmínkami této Smlouvy a splníte všechna pravidla a ujednání stanovená v těchto podmínkách, Vám Poskytovatel udělí následující práva („Licence“):

a) **Instalace a používání**. Máte nevýhradní a nepřevoditelné, časově omezené právo instalovat Software na pevný disk počítače anebo na jiné podobné médium sloužící na trvalé ukládání dat, instalaci a na ukládání Software do paměti počítačového systému, na vykonávání, na ukládání a na zobrazování Software.

b) **Stanovení počtu licencí**. Právo na použití Software se váže na počet Koncových uživatelů. Jedním Koncovým uživatelem se přitom rozumí: (i) instalace Software na jednom počítačovém systému, anebo (ii) pokud se rozsah licence váže na počet poštovních schránek, potom se rozumí jedním Koncovým uživatelem uživatel počítače, který si pomocí Mail User Agent („MUA“) přebírá elektronickou poštu. Pokud MUA přebírá elektronickou poštu a následně ji automaticky rozděluje vícerým uživatelům potom se počet Koncových uživatelů stanovuje podle skutečného počtu uživatelů, pro které je elektronická pošta rozdělovaná. V případě, že poštovní server vykonává funkci poštovní brány, je počet Koncových uživatelů shodný s počtem uživatelů poštovních serverů, pro které poskytuje tato brána služby. Pokud je jednomu uživateli směřovaný libovolný počet adres elektronické pošty (například pomocí aliasů) a přebírá si je jeden uživatel, a zprávy nejsou automaticky na straně klienta rozdělované pro více uživatelů je potřebná licence pro jeden počítač. Jednu licenci nesmíte současně používat na vícerých počítačích. Koncový uživatel je oprávněn zadávat Licenční klíč do Softwaru pouze v rozsahu, v němž je oprávněn používat Software v souladu s omezením vyplývajícím z počtu Licencí poskytnutých Poskytovatelem. Licenční klíč je považován za důvěrný. Licenci nesmíte sdílet s třetími stranami nebo povolit třetím stranám používat Licenční klíč, pokud to nepovoluje tato Smlouva nebo Poskytovatel. Pokud je Licenční klíč zneužit, okamžitě informujte Poskytovatele.

c) **Home/Business Edition.** Verzi Home Edition tohoto Softwaru lze používat výlučně v soukromém a/nebo nekomerčním prostředí pouze pro domácí a rodinné použití. Pro použití Softwaru v komerčním prostředí a na mailových serverech, mail relay serverech, mailových branách anebo internetových branách musíte získat Software ve verzi Business Edition.

d) **Trvání Licence**. Vaše právo používat Software je časově omezené.

e) **OEM Software**. Software označovaný jako „OEM“ je vázán na počítač, se kterým jste ho získali. Není ho možné přenést na jiný počítač.

f) **NFR, TRIAL Software.** Software označený jako "Not-for -resale", NFR anebo TRIAL nemůžete převést za protihodnotu anebo používat na jiný účel, jako na předvádění, testování jeho vlastností anebo vyzkoušení.

g) **Zánik licence**. Licence zaniká automaticky uplynutím období na které byla udělená. Pokud nedodržíte kterékoliv ustanovení této Dohody má Poskytovatel právo odstoupit od Dohody bez toho, aby byl dotknutý jakýkoliv nárok anebo prostředek, který má Poskytovatel pro takovýto případ k dispozici. V případě zrušení Licence musíte neprodleně na vlastní náklady Software včetně všech záložních kopií odstranit, zničit nebo vrátit společnosti ESET nebo prodejně či obchodu, od kterých jste Software získali. Po ukončení Licence je Poskytovatel rovněž oprávněn zrušit nárok Koncového uživatele na používání funkcí Softwaru, které vyžadují připojení k serverům Poskytovatele nebo třetích stran.

4. **Funkce sběru dat a požadavky na připojení k internetu.** Software vyžaduje pro správné fungování připojení k internetu a v pravidelných intervalech se připojuje k serverům Poskytovatele anebo serverům třetích stran a provádí související sběr dat v souladu se Zásadami ochrany osobních údajů. Připojení k internetu a související sběr dat jsou potřebné pro fungování Softwaru a pro jeho aktualizaci a upgrade. 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_business. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebudou poskytovány žádné aktualizace.

Pro účely této Smlouvy je nutné shromažďovat, zpracovávat a ukládat data, která Vás umožňují Poskytovateli identifikovat v souladu se Zásadami ochrany osobních údajů. Tímto berete na vědomí, že Poskytovatel smí kontrolovat pomocí vlastních prostředků, zda Software používáte v souladu s ustanoveními této Smlouvy. Tímto berete na vědomí, že pro účely této Smlouvy je nutné, aby byla vaše data přenášena při komunikaci mezi Softwarem a počítačovými systémy Poskytovatele nebo jeho obchodních partnerů za účelem zajištění funkčnosti Softwaru, ověření oprávnění k používání Softwaru a ochrany práv Poskytovatele.

V souvislosti s uzavřením této Smlouvy jsou Poskytovatel nebo obchodní partneři, kteří jsou součástí jeho distribuční a podpůrné sítě, oprávnění pro účely fakturace a plnění této Dohody přenášet, zpracovávat a uchovávat údaje, které Vás umožní identifikovat v nevyhnutelném rozsahu.

Podrobnosti o ochraně soukromí, ochraně osobních údajů a Vašich práv týkajících se údajů naleznete v Zásadách ochrany osobních údajů, které jsou k dispozici na webu Poskytovatele. Můžete si je také zobrazit z nabídky nápovědy v Softwaru.

5. **Výkon práv Koncového uživatele.** Práva Koncového uživatele musíte vykonávat osobně anebo prostřednictvím svých případných zaměstnanců. Software můžete použít výlučně jen na zabezpečení své činnosti a na ochranu výlučně těch počítačových systémů, pro které jste získali Licenci.

6. **Omezení práv**. Nesmíte Software kopírovat, šířit, oddělovat jeho části anebo vytvářet od Software odvozená díla. Při používání Software jste povinný dodržovat následovné omezení:

a) Můžete pro sebe vytvořit jedinou kopii Software na médiu určeném na trvalé ukládání dat jako záložní kopii, za předpokladu, že vaše archivní záložní kopie se nebude instalovat anebo používat na jiném počítači. Vytvoření jakékoliv další kopie Software je porušením této Dohody.

b) Software nesmíte používat, upravovat, překládat, reprodukovat, anebo převádět práva na používání Software anebo kopií Software jinak, než je výslovně uvedené v této Dohodě.

c) Software nesmíte prodat, sublicencovat, pronajmout ani zapůjčit a nesmíte jej ani používat k poskytování komerčních služeb.

d) Nesmíte Software zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokoušet získat zdrojový kód Softwaru s výjimkou rozsahu, ve kterém je takovéto omezení výslovně zakázané zákonem.

e) Souhlasíte s tím, že budete používat Software jen způsobem, který je v souladu se všemi platnými právními předpisy v právním systému, ve kterém Software používáte, zejména v souladu s platnými omezeními vyplývajícími z autorského práva a dalších práv duševního vlastnictví.

f) Souhlasíte s tím, že budete Software a jeho funkce používat pouze způsobem, který neomezuje přístup k těmto službám pro ostatní Koncové uživatele. Poskytovatel si vyhrazuje právo omezit rozsah poskytovaných služeb jednotlivým Koncovým uživatelů, aby mohl služby využívat nejvyšší možný počet Koncových uživatelů. Omezením rozsahu služeb se rozumí též úplné ukončení možnosti využívat některé z funkcí Softwaru a odstranění dat a informací o serverech Poskytovatele nebo třetích stran vztahujících se na konkrétní funkce Softwaru.

g) Souhlasíte s tím, že nebudete provádět žádné činnosti zahrnující používání Licenčního klíče, které jsou v rozporu s podmínkami této Smlouvy nebo by vedly k poskytnutí Licenčního klíče jakékoli osobě, která není oprávněna používat tento Software, jako je například převod použitého nebo nepoužitého Licenčního klíče v jakékoliv formě, stejně jako neoprávněná reprodukce nebo distribuce duplikovaných nebo generovaných Licenčních klíčů nebo používání Softwaru v důsledku použití Licenčního klíče získaného z jiného zdroje než od Poskytovatele.

7. **Autorská práva**. Software a všechna práva, zejména vlastnická práva a práva duševního vlastnictví k němu, jsou vlastnictvím společnosti ESET a/anebo jejích poskytovatelů licencí. Tato jsou chráněná ustanoveními mezinárodních dohod a všemi dalšími aplikovatelnými zákony krajiny, ve které se Software používá. Struktura, organizace a kód Software jsou obchodními tajemstvími a důvěrnými informacemi společnosti ESET a/anebo jejích poskytovatelů licencí. Software nesmíte kopírovat, s výjimkou uvedenou v ustanovení článku 6 písmeno a). Jakékoliv kopie, které smíte vytvořit podle této Dohody, musí obsahovat stejná upozornění na autorská a vlastnická práva, jaká jsou uvedená na Software. V případě, že v rozporu s ustanoveními této Dohody budete zpětně analyzovat, dekompilovat, převádět do zdrojového kódu anebo se jiným způsobem pokusíte získat zdrojový kód, souhlasíte s tím, že takto získané informace se budou automaticky a neodvolatelně považovat za převedené na Poskytovatele a vlastněné v plném rozsahu Poskytovatelem od okamžiku jejich vzniku, tím nejsou dotčená práva Poskytovatele spojená s porušením této Dohody.

8. **Výhrada práv**. Všechna práva k Software, kromě práv které Vám jako Koncovému uživateli Software byly výslovně udělená v této Dohodě, si Poskytovatel vyhrazuje pro sebe.

9. **Víceré jazykové verze, verze pro více operačních systémů, víceré kopie**. V případě jestliže Software podporuje víceré platformy anebo jazyky, anebo jestliže jste získali více kopií Software, můžete Software používat jen na takovém počtu počítačových systémů a v takových verzích, na které jste získali Licenci. Verze anebo kopie Software, které nepoužíváte nesmíte prodat, pronajmout, sublicencovat, zapůjčit anebo převést na jiné osoby.

10. **Začátek a trvání Dohody.** Tato Dohoda je platná a účinná ode dne, kdy jste odsouhlasili tuto Dohodu. Dohodu můžete kdykoliv ukončit tak, že natrvalo odinstalujete zničíte anebo na své vlastní náklady vrátíte Software, všechny případné záložní kopie a všechen související materiál, který jste získali od Poskytovatele anebo jeho obchodních partnerů. Vaše právo používat Software a všechny jeho funkce mohou podléhat Zásadám konce životnosti. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, vaše právo používat Software zanikne. Bez ohledu na způsob zániku této Dohody, ustanovení

jejích článků 7, 8, 11, 13, 19 a 21 zůstávají v platnosti bez časového omezení.

11. **PROHLÁŠENÍ KONCOVÉHO UŽIVATELE**. JAKO KONCOVÝ UŽIVATEL UZNÁVÁTE, ŽE SOFTWARE JE POSKYTOVANÝ "JAK STOJÍ A LEŽÍ", BEZ VÝSLOVNÉ ANEBO IMPLIKOVANÉ ZÁRUKY JAKÉHOKOLIV DRUHU A V MAXIMÁLNÍ MÍŘE DOVOLENÉ APLIKOVATELNÝMI ZÁKONY. ANI POSKYTOVATEL, ANI JEHO POSKYTOVATELÉ LICENCÍ, ANI DRŽITELÉ AUTORSKÝCH PRÁV NEPOSKYTUJÍ JAKÉKOLIV VÝSLOVNÉ ANEBO IMPLIKOVANÉ PROHLÁŠENÍ ANEBO ZÁRUKY, ZEJMÉNA NE ZÁRUKY PRODEJNOSTI ANEBO VHODNOSTI PRO KONKRÉTNÍ ÚČEL ANEBO ZÁRUKY, ŽE SOFTWARE NEPORUŠUJE ŽÁDNÉ PATENTY, AUTORSKÁ PRÁVA, OCHRANNÉ ZNÁMKY ANEBO JINÁ PRÁVA TŘETÍCH STRAN. NEEXISTUJE ŽÁDNÁ ZÁRUKA ZE STRANY POSKYTOVATELE ANI ŽÁDNÉ DALŠÍ STRANY, ŽE FUNKCE, KTERÉ OBSAHUJE SOFTWARE, BUDOU VYHOVOVAT VAŠÍM POŽADAVKŮM, ANEBO ŽE PROVOZ SOFTWARE BUDE NERUŠENÝ A BEZCHYBNÝ. PŘEBÍRÁTE ÚPLNOU ZODPOVĚDNOST A RIZIKO ZA VÝBĚR SOFTWARE PRO DOSÁHNUTÍ VÁMI ZAMÝŠLENÝCH VÝSLEDKŮ A ZA INSTALACI, POUŽÍVÁNÍ A VÝSLEDKY, KTERÉ SE SOFTWARE DOSÁHNETE.

12. **Žádné další závazky**. Tato Dohoda nezakládá na straně Poskytovatele a jeho případných poskytovatelů licencí kromě závazků konkrétně uvedených v této Dohodě žádné jiné závazky.

13. **OMEZENÍ ODPOVĚDNOSTI**. V MAXIMÁLNÍ MÍŘE, JAKOU DOVOLUJÍ PLATNÉ PRÁVNÍ PŘEDPISY, V ŽÁDNÉM PŘÍPADĚ NEBUDE POSKYTOVATEL, JEHO ZAMĚSTNANCI ANEBO JEHO POSKYTOVATELÉ LICENCÍ ZODPOVÍDAT ZA JAKÝKOLIV UŠLÝ ZISK, PŘÍJEM ANEBO PRODEJ, ANEBO ZA JAKOUKOLIV ZTRÁTU DAT, ANEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARÁNÍ NÁHRADNÍHO ZBOŽÍ ANEBO SLUŽEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÍ ÚJMU, ZA PŘERUŠENÍ PODNIKÁNÍ, ZA ZTRÁTU OBCHODNÍCH INFORMACÍ, ANI ZA JAKÉKOLIV SPECIÁLNÍ, PŘÍMÉ, NEPŘÍMÉ, NÁHODNÉ, EKONOMICKÉ, KRYCÍ, TRESTNÉ, SPECIÁLNÍ ANEBO NÁSLEDNÉ ŠKODY, JAKKOLIV ZAPŘÍČINĚNÉ, ČI UŽ VYPLYNULY ZE SMLOUVY, ÚMYSLNÉHO JEDNÁNÍ, NEDBALOSTI ANEBO JINÉ SKUTEČNOSTI, ZAKLÁDAJÍCÍ VZNIK ZODPOVĚDNOSTI, VZNIKLÉ INSTALACÍ, POUŽÍVÁNÍM ANEBO NEMOŽNOSTÍ POUŽÍVAT SOFTWARE, A TO I V PŘÍPADĚ, ŽE POSKYTOVATEL ANEBO JEHO POSKYTOVATELÉ LICENCÍ BYLI UVĚDOMĚNÍ O MOŽNOSTI TAKOVÝCHTO ŠKOD. POKUD NĚKTERÉ STÁTY A NĚKTERÉ PRÁVNÍ SYSTÉMY NEDOVOLUJÍ VYLOUČENÍ ZODPOVĚDNOSTI, ALE MOHOU DOVOLOVAT OMEZENÍ ZODPOVĚDNOSTI, JE ZODPOVĚDNOST POSKYTOVATELE, JEHO ZAMĚSTNANCŮ ANEBO POSKYTOVATELŮ LICENCÍ OMEZENÁ DO VÝŠE CENY, KTEROU JSTE ZAPLATILI ZA LICENCI.

14. Žádné ustanovení této Dohody se nedotýká práv strany, které zákon přiznává práva a postavení spotřebitele, pokud je s nimi v rozporu.

15. **Technická podpora**. Technickou podporu poskytuje ESET anebo ním pověřená třetí strana na základě vlastního uvážení bez jakýchkoliv záruk anebo prohlášení. Poté, co Software nebo některé z jeho funkcí dosáhnou data konce životnosti definovaného v Zásadách konce životnosti, nebude poskytována žádná technická podpora. Koncový uživatel je povinný před poskytnutím technické podpory zálohovat všechny jeho existující data, software a programové vybavení. ESET a/anebo ním pověřená třetí strana nepřebírají zodpovědnost za poškození anebo ztrátu dat, majetku, software anebo hardware anebo ušlý zisk při poskytování technické podpory. ESET a/anebo ním pověřená třetí strana si vyhrazuje právo na rozhodnutí, že řešený problém přesahuje rozsah technické podpory. ESET si vyhrazuje právo odmítnout, pozastavit anebo ukončit poskytování technické podpory na základě vlastního uvážení. Za účelem poskytování technické podpory mohou být vyžadovány informace o licenci, Informace a další údaje v souladu se Zásadami ochrany osobních údajů.

16. **Převod Licence**. Software můžete přenést z jednoho počítačového systému na jiný počítačový systém, pokud to není v rozporu s Dohodou. Pokud to není v rozporu s Dohodou, Koncový uživatel může jednorázově trvale převést Licenci a všechna práva z této Dohody na jiného Koncového uživatele jen se souhlasem Poskytovatele za podmínky, že (i) původní Koncový uživatel si neponechá žádnou kopii Software, (ii) převod práv musí být přímý, tedy z původního Koncového uživatele na nového Koncového uživatele, (iii) nový Koncový uživatel musí přebrat všechna práva a povinnosti, které má podle této Dohody původní Koncový uživatel (iv) původní Koncový uživatel musí odevzdat novému Koncovému uživateli doklady umožňující ověření legality Software jako je uvedené

v článku 17.

17. **Ověření pravosti Softwaru.** Koncový uživatel může prokázat nárok na užívání Softwaru jedním z následujících způsobů: (i) na základě certifikátu licence vydaného Poskytovatelem nebo třetí stranou jmenovanou Poskytovatelem, (ii) prostřednictvím písemné licenční smlouvy, byla-li taková smlouva uzavřena, (iii) předložením e-mailu zaslaného Poskytovatelem obsahujícího licenční údaje (uživatelské jméno a heslo). Za účelem ověření pravosti Softwaru mohou být v souladu se Zásadami ochrany osobních údajů vyžadovány Informace o licenci a identifikační údaje Koncového uživatele.

18. **Licencování pro státní orgány a vládu USA**. Software se poskytuje státním orgánům včetně vlády Spojených států amerických s licenčními právy a omezeními popsanými v této Dohodě.

19. **Soulad se zákony o kontrole obchodu**.

a) Nebudete přímo ani nepřímo exportovat, reexportovat, převádět nebo jinak zpřístupňovat Software žádné osobě, používat jej jakýmkoli způsobem nebo se podílet na jakémkoli jednání, které by mohlo mít za následek, že by společnost ESET nebo její holdingové společnosti, její dceřiné společnosti a dceřiné společnosti kterékoli z jejích holdingových společností, jakož i subjekty ovládané jejími holdingovými společnostmi („přidružené společnosti“), porušily nebo podléhaly negativním důsledkům zákonů o kontrole obchodu, které zahrnují

i. zákony, které kontrolují, omezují nebo ukládají licenční požadavky na export, reexport nebo převod zboží, softwaru, technologie nebo služeb, vydané nebo přijaté jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována a

ii. jakékoli hospodářské, finanční, obchodní nebo jiné sankce, omezení, embargo, zákaz importu nebo exportu, zákaz převodu finančních prostředků nebo aktiv nebo poskytování služeb nebo rovnocenné opatření uložené jakoukoli vládou, státem nebo regulačním orgánem Spojených států amerických, Singapuru, Spojeného království, Evropské unie nebo kteréhokoli z jejích členských států, nebo libovolné země, ve které mají být plněny povinnosti vyplývající z této Dohody, nebo v níž má společnost ESET nebo kterákoli z jejích přidružených společností sídlo nebo je v ní provozována.

(právní akty uvedené v bodech i. a ii. výše společně jako „zákony o kontrole obchodu“).

b) Společnost ESET má právo pozastavit své závazky podle těchto Podmínek nebo je ukončit s okamžitou platností v případě, že:

i. Společnost ESET rozhodne, že podle jejího opodstatněného názoru Uživatel porušil nebo pravděpodobně poruší ustanovení článku 19 a) Dohody; nebo

ii. Koncový uživatel a/nebo Software podléhají zákonům o kontrole obchodu a v důsledku toho společnost ESET stanoví, že podle jejího opodstatněného názoru by pokračující plnění jejích závazků vyplývajících z Dohody mohlo vést k tomu, že by společnost ESET nebo její přidružené společnosti porušily zákony o kontrole obchodu nebo podléhaly jejich negativním důsledkům.

c) Nic v této Dohodě není zamýšleno a nic by nemělo být interpretováno ani vykládáno tak, aby přimělo nebo nutilo některou ze stran jednat nebo zdržet se jednání (nebo souhlasit s jednáním nebo zdržet se jednání) jakýmkoli způsobem, který je v rozporu s platnými zákony o kontrole obchodu nebo je jimi penalizován či zakázán.

20. **Oznámení**. Veškerá oznámení a vrácení Softwaru a Dokumentace je nutné doručit na adresu ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic. Tím není dotčeno právo společnosti ESET sdělovat Vám jakékoli změny této Dohody, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace v souladu s čl. 22 této

Dohody. Společnost ESET Vám může posílat e-maily, oznámení v aplikaci prostřednictvím Softwaru nebo zveřejňovat komunikaci na našich webových stránkách. Souhlasíte s tím, že od společnosti ESET obdržíte právní sdělení v elektronické podobě, včetně jakýchkoli sdělení o změně podmínek, zvláštních podmínek nebo zásad ochrany osobních údajů, jakéhokoli návrhu/přijetí smlouvy nebo pozvánek k jednáním, oznámení nebo jiných právních sdělení. Tato elektronická komunikace se považuje za přijatou písemně, pokud platné právní předpisy výslovně nevyžadují jinou formu komunikace.

21. **Rozhodující právo**. Táto Dohoda se řídí a musí být vykládána v souladu se zákony Slovenské republiky s vyloučením ustanovení o kolizi právních norem. Koncový uživatel a Poskytovatel se dohodli, že kolizní ustanovení rozhodujícího právního řádu a Dohod OSN o smlouvách při mezinárodní koupi zboží se nepoužijí. Výslovně souhlasíte, že řešení jakýchkoliv sporů anebo nároků z této Dohody vůči Poskytovateli anebo spory a nároky související s používáním software je příslušný Okresní soud Bratislava V a výslovně souhlasíte s výkonem jurisdikce tímto soudem.

22. **Všeobecná ustanovení**. V případě, že jakékoliv ustanovení této Dohody je neplatné anebo nevykonatelné, neovlivní to platnost ostatních ustanovení Dohody. Ta zůstanou platná a vykonatelná podle podmínek v ní stanovených. Tato Dohoda byla uzavřena v angličtině. V případě, že je pro pohodlí uživatelů nebo pro jiný účel vyhotoven překlad této Dohody, nebo v případě rozporů mezi jazykovými verzemi této Dohody je rozhodující anglická verze.

Společnost ESET si vyhrazuje právo kdykoli provést změny Softwaru a úpravy této Dohody, jejích příloh, dodatků, Zásad ochrany osobních údajů, Zásad konce životnosti a Dokumentace nebo jakýchkoli jejich částí, a to aktualizací příslušného dokumentu (i) tak, aby se do něj promítly změny týkající se Softwaru nebo změny způsobu podnikání společnosti ESET, (ii) z právních, regulačních nebo bezpečnostních důvodů nebo (iii) s cílem zabránit zneužití nebo poškození. O jakékoli změně Dohody budete informováni e-mailem, oznámením v aplikaci nebo jinými elektronickými prostředky. Pokud nesouhlasíte s navrhovanými změnami Dohody, můžete ji vypovědět v souladu s čl. 10 do 30 dnů od obdržení oznámení o změně. Pokud Dohodu v této lhůtě nevypovíte, budou navrhované změny považovány za přijaté a vstoupí vůči Vám v platnost ode dne, kdy jste obdrželi oznámení o změně.

Tato Dohoda mezi Vámi a Poskytovatelem představuje jedinou a úplnou Dohodu vztahující se na Software, a plně nahrazuje jakékoliv předcházející prohlášení, jednání, závazky, zprávy anebo reklamní informace, týkající se Software.

DODATEK K DOHODĚ

Komunikace a Správa dat. Na komunikaci a správu údajů se vztahují následující dodatečná ustanovení:

Tento Software obsahuje funkci, která umožňuje přenos informací mezi počítačem a softwarem pro vzdálenou správu. Informace, které jsou předmětem přenosu, obsahují data o správě, jako jsou informace o hardwaru a softwaru na spravovaném počítači, a pokyny pro správu ze softwaru pro vzdálenou správu. Další obsah dat přenášených z počítače je určen nastavením softwaru nainstalovaného v počítači. Obsah pokynů ze softwaru pro správu je určen nastavením softwaru pro vzdálenou správu.

EULAID: EULA-PRODUCT-AGENT; 3537.0

Smlouva o zpracování údajů

Podle požadavků Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen GDPR) vstupujete vy (dále jen správce) a poskytovatel (dále jen zpracovatel) do smluvního vztahu zpracování dat, abyste definovali podmínky a ujednání pro zpracování osobních údajů, způsob jejich

ochrany, jakož i vymezení dalších práv a povinností obou stran při zpracovávání osobních údajů subjektů údajů jménem správce v průběhu provádění předmětu těchto podmínek jako hlavní smlouvy.

1. **Zpracování osobních údajů.** Služby poskytované v souladu s těmito podmínkami zahrnují zpracování informací týkajících se identifikované nebo identifikovatelné fyzické osoby uvedené v zásadách ochrany osobních údajů (dále jen osobní údaje).

2. **Oprávnění.** Správce opravňuje zpracovatele zpracovávat osobní údaje, což zahrnuje následující:

(i) Účelem zpracování se rozumí poskytování služeb v souladu s těmito podmínkami. Zpracovatel je oprávněn zpracovávat osobní údaje jménem správce pouze v souvislosti s poskytováním služeb požadovaných správcem. Veškeré informace shromážděné pro další účely jsou zpracovávány mimo smluvní vztah mezi správcem a zpracovatelem.

(ii) Obdobím zpracování se rozumí období od vstupu do spolupráce za těchto podmínek do ukončení služeb.

(iii) Rozsah a kategorie osobních údajů. Služby jsou určeny pouze ke zpracování obecných osobních údajů. Za určení rozsahu osobních údajů však odpovídá výhradně správce.

(iv) Subjektem údajů se rozumí fyzická osoba jako oprávněný uživatel zařízení správce.

(v) Operacemi zpracování se rozumějí všechny operace nezbytné pro zpracování.

(vi) Doloženými pokyny se rozumějí instrukce popsané v těchto podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb. Správce odpovídá za právní přípustnost zpracování osobních údajů zpracovatelem z hlediska příslušných platných ustanovení právních předpisů o ochraně osobních údajů.

3. **Povinnosti zpracovatele**. Zpracovatel je povinen:

(i) zpracovávat osobní údaje pouze na základě doložených pokynů a pro účely definované v podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb,

(ii) poučit osoby oprávněné zpracovávat osobní údaje (dále označované jako „autorizované osoby“) o jejich právech a povinnostech podle nařízení GDPR a o jejich odpovědnosti v případě porušení povinností a zajistit, aby se autorizované osoby zavázaly k zachovávání důvěrnosti a dodržování zdokumentovaných pokynů.

(iii) implementovat a dodržovat opatření popsaná v podmínkách, jejich přílohách, zásadách ochrany osobních údajů a dokumentaci služeb,

(iv) pomáhat správci při vyřizování žádostí subjektů údajů týkající se jejich práv. Zpracovatel nesmí opravit, vymazat nebo omezit zpracování osobních údajů bez pokynu správce. Veškeré žádosti subjektu údajů týkající se osobních údajů zpracovávaných jménem správce budou neprodleně předány správci.

(v) pomáhat správci s oznamováním porušení zabezpečení osobních údajů dozorčímu orgánu a subjektu údajů, Zpracovatel je povinen upozornit správce na jakýkoli problém při zpracování osobních údajů nebo se zabezpečením osobních údajů ihned po jeho zjištění. Zpracovatel bude v přiměřeném rozsahu spolupracovat při vyšetřování a nápravě takového problému a přijme přiměřená opatření k omezení dalších negativních dopadů.

(vi) na základě volby správce vymazat nebo vrátit všechny osobní údaje správci po skončení období zpracování. Správce se zavazuje informovat zpracovatele o svém rozhodnutí do deseti (10) dnů od konce období zpracování. Tímto ustanovením není dotčeno právo zpracovatele uchovávat osobní údaje v nezbytném rozsahu pro účely archivace ve veřejném zájmu, pro účely vědeckého výzkumu, pro statistické účely nebo pro účely stanovení, výkonu nebo obrany právních nároků.

(vii) vést aktuální registr všech kategorií zpracovatelských činností, které zpracovatel provedl jménem správce;

(viii) zpřístupnit správci všechny informace nezbytné k prokázání dodržování těchto podmínek, jejich příloh, zásad ochrany osobních údajů a dokumentace služeb. V případě auditu nebo kontroly zpracování osobních údajů ze strany správce je správce povinen informovat zpracovatele písemně nejméně třicet (30) dnů před plánovaným auditem nebo kontrolou.

4. **Zapojení dalšího zpracovatele.** Zpracovatel je oprávněn zapojit jiného zpracovatele za účelem provádění zvláštních zpracovatelských činností, jako je poskytování cloudového úložiště a infrastruktury pro služby v souladu s těmito podmínkami, jejich přílohami, zásadami ochrany osobních údajů a dokumentací služeb. V současné době společnost Microsoft poskytuje cloudové úložiště a infrastrukturu jako součást cloudové služby Azure. I v tomto případě musí být zpracovatel jediným kontaktním subjektem a stranou, která je odpovědná za dodržování pravidel. Zpracovatel se tímto zavazuje informovat správce o jakémkoli přidání dalšího zpracovatele nebo nahrazení zpracovatele, aby bylo možné vznést proti takové změně námitku.

5. **Území zpracování.** Zpracovatel zajišťuje, že se zpracování uskuteční v Evropském hospodářském prostoru nebo na základě rozhodnutí správce v zemi označené rozhodnutím Evropské komise jako bezpečné. V případě převodů a zpracování umístěných mimo Evropský hospodářský prostor nebo v zemi, která byla rozhodnutím Evropské komise na žádost správce označena jako bezpečná, platí standardní smluvní doložky.

6. **Zabezpečení.** Zpracovatel je certifikován na ISO 27001:2013 a používá soustavu ISO 27001 k implementaci bezpečnostní strategie vrstvené obrany při použití prvků zabezpečení ve vrstvě sítě, operačních systémů, databází, aplikací, zaměstnanců a provozních procesů. Dodržování regulačních a smluvních požadavků je pravidelně posuzováno a přezkoumáváno podobně jako jiná infrastruktura a operace zpracovatele. Provádějí se nezbytná opatření k zajištění soustavného dodržování požadavků. Zpracovatel zajistil zabezpečení údajů pomocí systému řízení bezpečnosti (ISMS) na základě ISO 27001. Bezpečnostní dokumentace zahrnuje především dokumenty zásad pro bezpečnost informací, fyzickou bezpečnost a bezpečnost zařízení, správu incidentů, postupy při úniku dat a bezpečnostních incidentech atd.

7. **Technická a organizační opatření**. Zpracovatel bude chránit osobní údaje před neúmyslným nebo nezákonným poškozením či zničením, neúmyslnou ztrátou, změnou, neoprávněným přístupem a vyzrazením. Za tímto účelem zpracovatel přijme adekvátní technická a organizační opatření odpovídající režimu zpracování a riziku, které zpracování představuje pro práva subjektů údajů, v souladu s požadavky GDPR. Podrobný popis technických a organizačních opatření je uveden v zásadách zabezpečení.

8. **Kontaktní informace zpracovatele.** Všechna oznámení, žádosti, požadavky a jiná sdělení týkající se ochrany osobních údajů je třeba adresovat společnosti ESET, spol. s.r.o.: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standardní smluvní body

ODDÍL I

Doložka 1 Účel a rozsah působnosti

(a) Účelem těchto standardních smluvních doložek je zajistit dodržování požadavků uvedených v nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů) (1), pokud jde o předávání osobních údajů do třetí země.

b) Smluvní strany:

(i) fyzická nebo právnická osoba či osoby, orgán či orgány veřejné moci, agentura či agentury nebo jiný subjekt či jiné subjekty (dále jen "subjekt" či "subjekty") předávající osobní údaje, uvedené v příloze I části A (dále jen "vývozce údajů"), a

(ii) subjekt či subjekty ve třetí zemi, přijímající přímo nebo nepřímo prostřednictvím jiného subjektu, jenž je rovněž stranou těchto doložek, osobní údaje od vývozce údajů, uvedené v příloze I části A (dále jen "dovozce údajů"),

se dohodly na těchto standardních smluvních doložkách (dále jen "Doložky").

(c) Tyto doložky se použijí s ohledem na předávání osobních údajů podle přílohy I části B.

(d) Dodatek k těmto doložkám obsahující přílohy, na něž se v těchto doložkách odkazuje, tvoří nedílnou součást těchto doložek.

Doložka 2 Účinek a neměnnost doložek

Tyto doložky stanoví vhodné záruky, včetně vymahatelných práv subjektu údajů a účinné právní ochrany, podle čl. 46 odst. 1 a čl. 46 odst. 2 písm. c) nařízení (EU) 2016/679 a s ohledem na předávání údajů od správců zpracovatelům a/nebo od zpracovatelů zpracovatelům, standardní smluvní doložky podle čl. 28 odst. 7 nařízení (EU) 2016/679, pokud nebudou změněny, s výjimkou výběru vhodného modulu (vhodných modulů) nebo za účelem přidání nebo aktualizace informací v dodatku. To smluvním stranám nebrání v tom, aby zahrnuly standardní smluvní doložky stanovené v těchto doložkách do širší smlouvy a/nebo přidaly další doložky nebo dodatečné záruky, pokud nebudou přímo nebo nepřímo v rozporu s těmito doložkami nebo nebudou dotčena základní práva nebo svobody subjektů údajů.

(b) Těmito doložkami nejsou dotčeny povinnosti, které se vztahují na vývozce údajů na základě nařízení (EU) 2016/679.

Doložka 3 Oprávněné třetí strany

(a) Subjekty údajů se mohou jako oprávněné třetí strany ve vztahu k vývozci a/nebo dovozci údajů dovolávat těchto doložek a vymáhat je, a to s následujícími výjimkami:

i) Doložka 1, Doložka 2, Doložka 3, Doložka 6, Doložka 7;

ii) Doložka 8 – Modul 1: Doložka 8.5. písm. e) a Doložka 8.9. písm. b); Modul 2: Doložka 8.1. písm. b), Doložka 8.9. písm. a), c), d) a e); Modul 3: Doložka 8.1. písm. a), c) a d) a Doložka 8.9. písm. a), c), d), e), f) a g); Modul 4: Doložka 8.1. písm. b) a Doložka 8.3 písm. b);

(iii) Doložka 9 – Modul dva: Doložka 9 písm. a), c), d) a e); Modul 3: Doložka 9 písm. a), c), d) a e);

(iv) Doložka 12 – Modul 1: Doložka 12 písm. a) a d); Moduly 2 a 3: Doložka 12 písm. a), d) a f);

(v) Doložka 13;

(vi) Doložka 15.1 písm. c), d) a e);

(vii) Doložka 16 písm. e);

(viii) Doložka 18 – Moduly 1, 2 a 3: Doložka 18 písm. a) a b); Modul 4: Doložka 18.

(b) Písmenem a) nejsou dotčena práva subjektů údajů podle nařízení (EU) 2016/679.

Doložka 4 Výklad

(a) Pokud tyto doložky používají pojmy, které jsou vymezeny v nařízení (EU) 2016/679, mají tyto pojmy stejný význam jako v uvedeném nařízení.

(b) Tyto doložky je třeba číst a vykládat s ohledem na ustanovení nařízení (EU) 2016/679.

(c) Tyto doložky nebudou vykládány žádným způsobem, který by byl v rozporu s právy a povinnostmi stanovenými v nařízení (EU) 2016/679.

Doložka 5 Hierarchie

V případě rozporu mezi těmito doložkami a ustanoveními souvisejících dohod mezi stranami, které existovaly v době sjednání těchto doložek, nebo které byly uzavřeny až po jejich sjednání, mají tyto doložky přednost.

Doložka 6 Popis předávání

Podrobnosti týkající se předávání, zejména kategorie osobních údajů, které jsou předávány, a účel nebo účely, pro které jsou předávány, jsou uvedeny v příloze I části B.

Doložka 7 – volitelná Doložka o přistoupení

(a) Subjekt, který není stranou těchto doložek, může se souhlasem stran k těmto doložkám kdykoli přistoupit, buď jako vývozce údajů, nebo jako dovozce údajů, a to vyplněním dodatku a podepsáním přílohy I části A.

(b) Poté, co přistupující subjekt vyplní dodatek a podepíše přílohu I část A, stane se stranou těchto doložek a má práva a povinnosti vývozce údajů nebo dovozce údajů v souladu se svým určením v příloze I části A.

(c) Přistupující subjekt nemá žádná práva ani povinnosti na základě těchto doložek plynoucí z období před tím, než se stal stranou.

ODDÍL II – POVINNOSTI STRAN

Doložka 8 Záruky ochrany údajů

Vývozce údajů zaručuje, že vynaložil přiměřené úsilí, aby mohl stanovit, zda je dovozce údajů schopen – zavedením vhodných technických a organizačních opatření – plnit své povinnosti podle těchto doložek.

MODUL 1: Předání od správce správci

8.1. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání v souladu s přílohou I částí B. Osobní údaje může zpracovávat pro jiný účel pouze tehdy, pokud:

i) získal předchozí souhlas subjektu údajů;

(ii) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iii) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

8.2. Transparentnost

(a) Aby subjekty údajů mohly účinně vykonávat svá práva podle doložky 10, dovozce údajů je informuje přímo nebo prostřednictvím vývozce údajů:

i) o své totožnosti a kontaktních údajích;

(ii) o kategoriích zpracovávaných osobních údajů;

(iii) o právu získat kopii těchto doložek;

(iv) pokud má v úmyslu osobní údaje dále předat jakékoli třetí straně nebo stranám, o příjemci nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), o účelu takového dalšího předávání a o důvodu pro další předávání podle doložky 8.7.

(b) Písmeno a) se nepoužije, pokud subjekt údajů již tyto informace má, a to i v případě, že tyto informace již poskytl vývozce údajů, nebo pokud je poskytnutí těchto informací nemožné nebo by to pro dovozce údajů znamenalo nepřiměřené úsilí. V druhém případě dovozce údajů informace v maximální možné míře zveřejní.

(c) Strany poskytnou subjektu údajů na požádání a bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, mohou strany před sdílením kopie upravit část znění dodatku, ale poskytnou smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny.

(d) Písmeny a) až c) nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.3. Přesnost a minimalizace údajů

(a) Každá strana zajistí, aby osobní údaje byly přesné a v případě potřeby aktualizovány. Dovozce údajů přijme veškerá smysluplná opatření, aby zajistil, že osobní údaje, které jsou nepřesné, budou s ohledem na účel nebo účely zpracování bezodkladně vymazány nebo opraveny.

(b) Pokud se jedna ze stran dozví, že osobní údaje, které předala nebo přijala, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje druhou stranu.

(c) Dovozce údajů zajistí, aby osobní údaje byly přiměřené, relevantní a omezené na to, co je nezbytné z hlediska účelu nebo účelů, pro které jsou zpracovávány.

8.4. Minimalizace uchovávání

Dovozce údajů uchová osobní údaje pouze po dobu nezbytnou pro účel nebo účely, pro který (které) jsou zpracovávány. Přijme vhodná technická nebo organizační opatření k zajištění dodržování této povinnosti, včetně vymazání nebo anonymizace údajů (2) a všech záloh na konci doby uchovávání.

8.5. Bezpečnost zpracování

a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení osobních údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení oni řádně zohlední aktuální stav

techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování.

(b) Strany se dohodly na technických a organizačních opatřeních stanovených v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(c) Dovozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(d) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení osobních údajů, včetně opatření ke zmírnění jeho možných nepříznivých účinků.

(e) V případě porušení zabezpečení osobních údajů, které by mohlo vést k ohrožení práv a svobod fyzických osob, dovozce údajů bez zbytečného odkladu informuje vývozce údajů i příslušný dozorový úřad v souladu s doložkou 13. Toto ohlášení obsahuje i) popis povahy daného případu porušení zabezpečení osobních údajů (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů), ii) jeho pravděpodobných důsledků, iii) popis opatření, která byla přijata nebo byla navržena s cílem vyřešit dané porušení zabezpečení, a iv) údaje kontaktního místa, kde lze získat více informací. Není-li možné, aby dovozce údajů veškeré informace poskytl současně, mohou být poskytnuty postupně bez dalšího zbytečného odkladu.

(f) V případě porušení zabezpečení osobních údajů, které pravděpodobně bude představovat vysoké riziko pro práva a svobody fyzických osob, dovozce údajů rovněž bez zbytečného odkladu podá hlášení dotčeným subjektům údajů o porušení zabezpečení osobních údajů a jeho povaze – v případě potřeby ve spolupráci s vývozcem údajů – a sdělí jim také informace uvedené v písm. e) bodu ii) až iv), pokud dovozce údajů nezavedl opatření za účelem značného snížení rizika pro práva a svobody fyzických osob nebo pokud dané hlášení nevyžaduje nepřiměřené úsilí. V posledně uvedeném případě dovozce údajů místo toho vydá veřejné oznámení nebo zajistí obdobné opatření, kterým veřejnost o porušení zabezpečení osobních údajů informuje.

(g) Dovozce údajů dokumentuje veškeré relevantní skutečnosti týkající se porušení zabezpečení osobních údajů, včetně jeho účinků a přijatých nápravných opatření, a vede si o tom záznamy.

8.6. Citlivé údaje

Jestliže předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech nebo trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky přizpůsobené zvláštní povaze údajů a souvisejícím rizikům. To může zahrnovat omezení personálu, který má povolen přístup k osobním údajům, dodatečná bezpečnostní opatření (jako je pseudonymizace) a/nebo dodatečná omezení s ohledem na další zpřístupnění.

8.7. Další předávání

Dovozce údajů nezpřístupní osobní údaje třetí straně se sídlem mimo Evropskou unii (3) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), ledaže by tato třetí strana byla podle příslušného modulu těmito doložkami vázána nebo by souhlasila s tím, že jimi bude vázána. K dalšímu předání dovozcem údajů jinak může dojít pouze tehdy, pokud:

(i) se provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679,

jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dotčené zpracování;

(iii) třetí strana uzavře s dovozcem údajů závazný instrument zajišťující stejnou úroveň ochrany údajů jako podle těchto doložek a dovozce údajů poskytne kopii těchto záruk vývozci údajů;

(iv) je to nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení;

(v) je to nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby, nebo

(vi) pokud neplatí žádná z dalších podmínek, dovozce údajů získal výslovný souhlas subjektu údajů s dalším předáváním v konkrétní situaci poté, co jej informoval o jeho účelu nebo účelech, totožnosti příjemce a možných rizicích, která pro něj vyplývají z takového předávání vzhledem k nedostatku vhodných záruk ochrany údajů. V takovém případě dovozce údajů informuje vývozce údajů a na žádost vývozce údajů mu předá kopii informací poskytnutých subjektu údajů.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.8. Zpracování z pověření dovozce údajů

Dovozce údajů zajistí, aby jakákoli osoba, která jedná z jeho pověření, včetně zpracovatele, zpracovávala údaje pouze na základě jeho pokynů.

8.9. Dokumentace a plnění povinností

(a) Každá strana musí být schopna prokázat plnění svých povinností podle těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování, za jejichž provádění odpovídá.

(b) Dovozce údajů tuto dokumentaci na požádání zpřístupní příslušnému dozorovému úřadu.

MODUL 2: Předání od správce zpracovateli

8.1. Pokyny

(a) Dovozce údajů zpracovává osobní údaje pouze na základě doložených pokynů od vývozce údajů. Vývozce údajů může takové pokyny vydávat po celou dobu trvání smlouvy.

(b) Dovozce údajů okamžitě informuje vývozce údajů, pokud není schopen tyto pokyny dodržet.

8.2. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání uvedené v příloze I části B, ledaže vývozce údajů vydá další pokyny.

8.3. Transparentnost

Na požádání poskytne vývozce údajů subjektu údajů bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně opatření popsaných v příloze II a osobních údajů, může vývozce údajů před sdílením kopie upravit část znění dodatku k těmto doložkám, ale poskytne smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen

porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny. Touto doložkou nejsou dotčeny povinnosti vývozce údajů podle článků 13 a 14 nařízení (EU) 2016/679.

8.4. Přesnost

Pokud se dovozce údajů dozví, že osobní údaje, které přijal, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje vývozce údajů. V takovém případě dovozce údajů spolupracuje s vývozcem údajů na jejich vymazání nebo opravě.

8.5. Doba zpracování a vymazání nebo vrácení údajů

Dovozce údajů zpracovává údaje pouze po dobu uvedenou v příloze I části B. Po skončení poskytování zpracovatelských služeb dovozce údajů v souladu s volbou vývozce údajů vymaže všechny osobní údaje zpracovávané jménem vývozce údajů a potvrdí vývozci údajů, že tak učinil, nebo vývozci údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže existující kopie. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a že bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to místní právo vyžaduje. Tím není dotčena doložka 14, zejména požadavek, aby dovozce údajů podle doložky 14 písm. e) informoval vývozce údajů po celou dobu trvání smlouvy, pokud má důvod se domnívat, že se na něj vztahují nebo se na něj začaly vztahovat právní předpisy nebo postupy, jež nejsou v souladu s požadavky podle doložky 14 písm. a).

8.6. Bezpečnost zpracování

(a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění uvedených údajů (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení strany řádně zohlední aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování. V případě pseudonymizace zůstanou dodatečné informace pro přiřazení osobních údajů konkrétnímu subjektu údajů, pokud je to možné, pod výlučnou kontrolou vývozce údajů. Za účelem dodržení svých povinností podle tohoto odstavce musí dovozce údajů přinejmenším zavést technická a organizační opatření uvedená v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(b) Dovozce údajů poskytne přístup k osobním údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(c) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení, včetně opatření ke zmírnění jeho nepříznivých dopadů. Dovozce údajů rovněž bez zbytečného odkladu poté, co se o porušení dozvěděl, podá hlášení vývozci údajů. Takové hlášení obsahuje podrobnosti o kontaktním místě, které může poskytnout bližší informace, popis povahy daného případu porušení zabezpečení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a přibližného množství záznamů osobních údajů), jeho pravděpodobných důsledků a opatření přijatých nebo navržených s cílem vyřešit dané porušení zabezpečení, včetně případných opatření ke zmírnění jeho možných nepříznivých dopadů. Není-li možné poskytnout všechny informace současně, původní hlášení obsahuje informace, které byly v danou dobu k dispozici, a další informace, jakmile budou k dispozici, budou následně poskytovány bez zbytečného odkladu.

(d) Dovozce údajů spolupracuje s vývozcem údajů a pomáhá mu tak, aby mu umožnil plnit jeho povinnosti podle nařízení (EU) 2016/679, zejména povinnost podávat hlášení příslušnému dozorovému úřadu a dotčeným subjektům údajů, s přihlédnutím k povaze zpracování a informacím, které jsou dovozci údajů dostupné.

8.7. Citlivé údaje

Pokud předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech a trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky popsané v příloze I části B.

8.8. Další předávání

Dovozce údajů zpřístupní osobní údaje třetí straně pouze na základě doložených pokynů od vývozce údajů. Údaje mohou být navíc zpřístupněny třetí straně se sídlem mimo Evropskou unii (4) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), pokud je tato třetí strana podle příslušného modulu vázána těmito doložkami nebo souhlasí s tím, že jimi bude vázána, nebo pokud:

(i) se další předávání provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679 s ohledem na dotčené zpracování;

(iii) je další předávání nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iv) je další předávání nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.9. Dokumentace a plnění povinností

(a) Dovozce údajů neprodleně a odpovídajícím způsobem vyřídí dotazy vývozce údajů, které se týkají zpracování podle těchto doložek.

b) Strany musí být schopny prokázat dodržování těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování prováděných za vývozce údajů.

(c) Dovozce údajů poskytne vývozci údajů veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v těchto doložkách, a na žádost vývozce údajů umožní audity činností zpracování, na které se tyto doložky vztahují, a bude k nim přispívat, a to v přiměřených intervalech, nebo pokud existují okolnosti nasvědčující tomu, že doložky nejsou dodržovány. Při rozhodování o přezkumu nebo auditu může vývozce údajů vzít v úvahu příslušná osvědčení, kterými disponuje dovozce údajů.

(d) Vývozce údajů se může rozhodnout provést audit sám nebo pověřit nezávislého auditora. Audity mohou zahrnovat inspekce v prostorách nebo ve fyzických zařízeních dovozce údajů a v příslušných případech se provádějí na základě přiměřeně včasného oznámení.

(e) Strany na požádání příslušnému dozorovému úřadu poskytnou informace uvedené v písmenech b) a c), včetně výsledků jakýchkoli auditů.

MODUL 3: Předání od zpracovatele zpracovateli

8.1. Pokyny

(a) Vývozce údajů informoval dovozce údajů, že jedná jako zpracovatel na základě pokynů svého správce nebo správců, a tyto pokyny vývozce údajů před zpracováním zpřístupní dovozci údajů.

(b) Dovozce údajů zpracovává osobní údaje pouze na základě dokumentovaných pokynů správce, které byly vývozcem údajů sděleny dovozci údajů, a na základě jakýchkoli dodatečných dokumentovaných pokynů od vývozce údajů. Tyto dodatečné pokyny nesmí být v rozporu s pokyny správce. Správce nebo vývozce údajů může po dobu trvání smlouvy vydat další dokumentované pokyny týkající se zpracování údajů.

(c) Dovozce údajů okamžitě informuje vývozce údajů, pokud není schopen tyto pokyny dodržet. Jestliže dovozce údajů není schopen postupovat podle pokynů správce, vývozce údajů o tom správce neprodleně uvědomí.

(d) Vývozce údajů zaručuje, že uložil dovozci údajů stejné povinnosti v oblasti ochrany údajů, jaké stanoví smlouva nebo jiný právní akt podle práva Unie nebo členského státu mezi správcem a vývozcem údajů (5).

8.2. Omezení účelu

Dovozce údajů zpracovává osobní údaje pouze pro konkrétní účel nebo účely předání v souladu s přílohou I částí B, pokud neexistují další pokyny ze strany správce, které dovozci údajů sdělil vývozce údajů, ani další pokyny ze strany vývozce údajů.

8.3. Transparentnost

Na požádání poskytne vývozce údajů subjektu údajů bezplatně kopii těchto doložek, včetně dodatku, který tyto strany vyplnily. V rozsahu nezbytném k ochraně obchodního tajemství nebo jiných důvěrných informací, včetně osobních údajů, může vývozce údajů před sdílením kopie upravit část znění dodatku, ale poskytne smysluplné shrnutí, pokud by jinak subjekt údajů nebyl schopen porozumět jeho obsahu nebo uplatnit svá práva. Strany poskytnou subjektu údajů na požádání důvody uvedených úprav, a to v co největší možné míře, aniž by byly upravené informace odhaleny.

8.4. Přesnost

Pokud se dovozce údajů dozví, že osobní údaje, které přijal, jsou nepřesné nebo zastaralé, bez zbytečného odkladu o tom informuje vývozce údajů. V takovém případě dovozce údajů spolupracuje s vývozcem údajů na jejich opravě nebo vymazání.

8.5. Doba zpracování a vymazání nebo vrácení údajů

Dovozce údajů zpracovává údaje pouze po dobu uvedenou v příloze I části B. Po skončení poskytování zpracovatelských služeb dovozce údajů v souladu s volbou vývozce údajů vymaže všechny osobní údaje zpracovávané jménem správce a potvrdí vývozci údajů, že tak učinil, nebo vývozci údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže všechny existující kopie. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a že bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to místní právo vyžaduje. Tím není dotčena doložka 14, zejména požadavek, aby dovozce údajů podle doložky 14 písm. e) informoval vývozce údajů po celou dobu trvání smlouvy, pokud má důvod se domnívat, že se na něj vztahují nebo se na něj začaly vztahovat právní předpisy nebo postupy, jež nejsou v souladu s požadavky podle doložky 14 písm. a).

8.6. Bezpečnost zpracování

(a) Dovozce údajů a během předávání také vývozce údajů přijmou vhodná technická a organizační opatření k zajištění zabezpečení údajů, včetně ochrany před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění uvedených údajů (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení oni řádně zohlední aktuální stav techniky, náklady na provedení, povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním. Strany zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování. V případě pseudonymizace zůstanou dodatečné informace pro přiřazení osobních údajů konkrétnímu subjektu údajů, pokud je to možné, pod výlučnou kontrolou vývozce údajů nebo správce. Za účelem dodržení svých povinností podle tohoto odstavce musí dovozce údajů přinejmenším zavést technická a organizační opatření uvedená v příloze II. Dovozce údajů provádí pravidelné kontroly, aby zajistil, že tato opatření stále poskytují odpovídající úroveň zabezpečení.

(b) Dovozce údajů poskytne přístup k údajům svým zaměstnancům pouze v rozsahu nezbytně nutném pro provádění, správu a monitorování smlouvy. Zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

(c) V případě porušení zabezpečení osobních údajů týkajících se osobních údajů zpracovávaných dovozcem údajů podle těchto doložek přijme dovozce údajů vhodná opatření k řešení porušení zabezpečení, včetně opatření ke zmírnění jeho nepříznivých dopadů. Dovozce údajů rovněž bez zbytečného odkladu poté, co se o porušení zabezpečení dozvěděl, podá hlášení vývozci údajů, a je-li to vhodné a proveditelné, také správci. Takové hlášení obsahuje podrobnosti o kontaktním místě, které může poskytnout bližší informace, popis povahy daného případu porušení zabezpečení (včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a přibližného množství záznamů osobních údajů), jeho pravděpodobných důsledků a opatření přijatých nebo navržených s cílem vyřešit dané porušení zabezpečení údajů, včetně opatření ke zmírnění jeho možných nepříznivých dopadů. Není-li možné poskytnout všechny informace současně, původní hlášení obsahuje informace, které byly v danou dobu k dispozici, a další informace, jakmile budou k dispozici, budou následně poskytovány bez zbytečného odkladu.

(d) Dovozce údajů spolupracuje s vývozcem údajů a pomáhá mu tak, aby mu umožnil plnit jeho povinnosti podle nařízení (EU) 2016/679, zejména povinnost podávat hlášení svému správci, aby tento správce mohl informovat příslušný dozorový úřad a dotčené subjekty údajů, s přihlédnutím k povaze zpracování a informacím, které jsou dovozci údajů dostupné.

8.7. Citlivé údaje

Pokud předávání zahrnuje osobní údaje vypovídající o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetické údaje nebo biometrické údaje za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údaje týkající se rozsudků v trestních věcech a trestných činů (dále jen "citlivé údaje"), dovozce údajů uplatní zvláštní omezení a/nebo dodatečné záruky stanovené v příloze I části B.

8.8. Další předávání

Dovozce údajů zpřístupní osobní údaje třetí straně pouze na základě doložených pokynů od správce, které dovozci údajů sdělil vývozce údajů. Údaje mohou být navíc zpřístupněny třetí straně se sídlem mimo Evropskou unii (6) (ve stejné zemi jako dovozce údajů nebo v jiné třetí zemi, dále jen "další předávání"), pokud je tato třetí strana podle příslušného modulu vázána těmito doložkami nebo souhlasí s tím, že jimi bude vázána, nebo pokud:

(i) se další předávání provádí do země, která využívá rozhodnutí o odpovídající ochraně podle článku 45 nařízení (EU) 2016/679, jenž upravuje další předávání;

(ii) třetí strana jinak zajišťuje vhodné záruky podle článků 46 nebo 47 nařízení (EU) 2016/679;

(iii) je další předávání nezbytné pro určení, výkon nebo obhajobu právních nároků v rámci zvláštních správních, regulačních nebo soudních řízení, nebo

(iv) je další předávání nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby.

Na jakékoli další předávání se vztahuje podmínka, že dovozce údajů dodrží všechny ostatní záruky podle těchto doložek, zejména účelové omezení.

8.9. Dokumentace a plnění povinností

(a) Dovozce údajů neprodleně a odpovídajícím způsobem vyřídí dotazy vývozce údajů nebo správce, které se týkají zpracování podle těchto doložek.

b) Strany musí být schopny prokázat dodržování těchto doložek. Dovozce údajů zejména vede příslušnou dokumentaci o činnostech zpracování prováděných za správce.

(c) Dovozce údajů poskytne vývozci údajů veškeré informace nezbytné k prokázání dodržování povinností stanovených v těchto doložkách, přičemž vývozce údajů je pak poskytne správci.

(d) Dovozce údajů umožní audity ze strany vývozce údajů, které se týkají činností zpracování, na něž se tyto doložky vztahují, a k těmto auditům přispívá, a to v přiměřených intervalech, nebo pokud existují okolnosti nasvědčující tomu, že doložky nejsou dodržovány. Totéž platí, pokud vývozce údajů požaduje audit na základě pokynů správce. Při rozhodování o auditu může vývozce údajů zohlednit příslušná osvědčení, kterými disponuje dovozce údajů.

(e) Pokud je audit prováděn na základě pokynů od správce, bude správce o jeho výsledcích informován vývozcem údajů.

(f) Vývozce údajů se může rozhodnout provést audit sám nebo pověřit nezávislého auditora. Audity mohou zahrnovat inspekce v prostorách nebo ve fyzických zařízeních dovozce údajů a v příslušných případech se provádějí na základě přiměřeně včasného oznámení.

(g) Strany na požádání příslušnému dozorovému úřadu poskytnou informace uvedené v písmenech b) a c), včetně výsledků jakýchkoli auditů.

MODUL 4: Předání od zpracovatele správci

8.1. Pokyny

(a) Vývozce údajů zpracovává osobní údaje pouze na základě doložených pokynů od dovozce údajů, který jedná jako jeho správce.

(b) Vývozce údajů neprodleně informuje dovozce údajů, pokud není schopen tyto pokyny dodržovat, včetně případů, kdy tyto pokyny porušují nařízení (EU) 2016/679 nebo jiné právní předpisy Unie nebo členského státu v oblasti ochrany údajů.

(c) Dovozce údajů se zdrží přijímání jakýchkoli opatření, která by vývozci údajů bránila v plnění jeho povinností podle nařízení (EU) 2016/679, mimo jiné v kontextu dílčího zpracování, nebo pokud se jedná o spolupráci s příslušnými dozorovými úřady.

(d) Po skončení poskytování zpracovatelských služeb vývozce údajů v souladu s volbou dovozce údajů vymaže všechny osobní údaje zpracovávané jménem dovozce údajů a potvrdí dovozci údajů, že tak učinil, nebo dovozci

údajů vrátí všechny osobní údaje zpracovávané jeho jménem a vymaže všechny existující kopie.

8.2. Bezpečnost zpracování

a) Strany zavedou vhodná technická a organizační opatření k zajištění zabezpečení údajů, a to i během předávání, a zajistí ochranu před porušením zabezpečení vedoucím k náhodnému nebo protiprávnímu zničení, ztrátě, změně, neoprávněnému poskytnutí nebo zpřístupnění (dále jen "porušení zabezpečení osobních údajů"). Při posuzování vhodné úrovně zabezpečení strany náležitě zohlední aktuální stav techniky, náklady na provedení, povahu osobních údajů (7), povahu, rozsah, kontext a účel nebo účely zpracování a rizika pro subjekty údajů spojená se zpracováním, a zejména zváží použití šifrování nebo pseudonymizace, a to i během předávání, pokud lze tímto způsobem splnit účel zpracování.

(b) Vývozce údajů pomáhá dovozci údajů při zajišťování odpovídajícího zabezpečení údajů v souladu s písmenem a). V případě porušení zabezpečení osobních údajů týkajícího se osobních údajů zpracovávaných vývozcem údajů podle těchto doložek vývozce údajů podá hlášení dovozci údajů bez zbytečného odkladu poté, co se o něm dozvěděl, a dovozci údajů bude při řešení uvedeného porušení nápomocen.

(c) Vývozce údajů zajistí, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.

8.3. Dokumentace a plnění povinností

(a) Strany musí být schopny prokázat dodržování těchto doložek.

(b) Vývozce údajů poskytne dovozci údajů veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v těchto doložkách, umožní provedení auditů a bude k nim přispívat.

Doložka 9 Využití dílčích zpracovatelů

MODUL 2: Předání od správce zpracovateli

(a) Dovozce údajů má obecné povolení vývozce údajů pro zapojení dílčího zpracovatele nebo dílčích zpracovatelů ze schváleného seznamu. Dovozce údajů výslovně písemně informuje vývozce údajů o veškerých zamýšlených změnách uvedeného seznamu, které spočívají v přidání nebo nahrazení dílčích zpracovatelů nejméně [uveďte časové období] předem, čímž poskytne vývozci údajů dostatek času, aby mohl proti takovým změnám vznést námitky před zapojením dílčího zpracovatele nebo zpracovatelů. Dovozce údajů poskytne vývozci údajů informace nezbytné k tomu, aby vývozce údajů mohl uplatnit své právo vznést námitku.

Pokud dovozce údajů pro výkon konkrétních činností zpracování zapojí dílčího zpracovatele (jménem vývozce údajů), učiní tak prostřednictvím písemné smlouvy, která v zásadě stanoví stejné povinnosti v oblasti ochrany údajů jako ty, které jsou závazné pro dovozce údajů na základě těchto doložek, a to i pokud jde o práva náležející oprávněné třetí straně v případě subjektů údajů. (8) Strany se dohodly, že dodržováním této doložky dovozce údajů plní své povinnosti podle doložky 8.8. Dovozce údajů zajistí, aby dílčí zpracovatel dodržoval povinnosti, které se v souladu s těmito doložkami vztahují na dovozce údajů.

(c) Dovozce údajů poskytne vývozci údajů na jeho žádost kopii takové dohody s dílčím zpracovatelem a veškeré její následné změny. V rozsahu nezbytném k ochraně obchodních tajemství nebo jiných důvěrných informací, včetně osobních údajů, může dovozce údajů před sdílením kopie znění této dohody upravit.

(d) Dovozce údajů je i nadále vývozci údajů plně odpovědný za plnění povinností dílčího zpracovatele na základě smlouvy, kterou s dovozcem údajů uzavřel. Dovozce údajů informuje vývozce údajů o každém případu, kdy dílčí zpracovatel nesplnil svou povinnost, jež z uvedené smlouvy vyplývá.

(e) Dovozce údajů sjedná s dílčím zpracovatelem doložku ve prospěch oprávněné třetí strany, přičemž – v případě, že dovozce údajů fakticky zmizel, z právního hlediska zanikl nebo se dostal do platební neschopnosti – má vývozce údajů právo smlouvu s dílčím zpracovatelem vypovědět a dát dílčímu zpracovateli pokyn, aby osobní údaje vymazal nebo vrátil.

MODUL 3: Předání od zpracovatele zpracovateli

(a) Dovozce údajů má obecné povolení správce pro zapojení dílčího zpracovatele nebo dílčích zpracovatelů ze schváleného seznamu. Dovozce údajů výslovně písemně informuje správce o veškerých zamýšlených změnách uvedeného seznamu, které spočívají v přidání nebo nahrazení dílčích zpracovatelů nejméně [uveďte časové období] předem, čímž poskytne správci dostatek času, aby mohl proti takovým změnám vznést námitky před zapojením dílčího zpracovatele nebo zpracovatelů. Dovozce údajů poskytne správci informace nezbytné k tomu, aby správce mohl uplatnit své právo vznést námitku. Dovozce údajů o zapojení dílčího zpracovatele nebo dílčích zpracovatelů informuje vývozce údajů.

(b) Pokud dovozce údajů pro výkon konkrétních činností zpracování zapojí dílčího zpracovatele (jménem správce), učiní tak prostřednictvím písemné smlouvy, která v zásadě stanoví stejné povinnosti v oblasti ochrany údajů jako ty, které jsou závazné pro dovozce údajů na základě těchto doložek, a to i pokud jde o práva náležející oprávněné třetí straně v případě subjektů údajů. (9) Strany se dohodly, že dodržováním této doložky dovozce údajů plní své povinnosti podle doložky 8.8. Dovozce údajů zajistí, aby dílčí zpracovatel dodržoval povinnosti, které se v souladu s těmito doložkami vztahují na dovozce údajů.

(c) Dovozce údajů poskytne na žádost vývozce údajů nebo správce kopii takové dohody s dílčím zpracovatelem a veškeré její následné změny. V rozsahu nezbytném k ochraně obchodních tajemství nebo jiných důvěrných informací, včetně osobních údajů, může dovozce údajů před sdílením kopie znění této dohody upravit.

(d) Dovozce údajů je i nadále vývozci údajů plně odpovědný za plnění povinností dílčího zpracovatele na základě smlouvy, kterou s dovozcem údajů uzavřel. Dovozce údajů informuje vývozce údajů o každém případu, kdy dílčí zpracovatel nesplnil svou povinnost, jež z uvedené smlouvy vyplývá.

(e) Dovozce údajů sjedná s dílčím zpracovatelem doložku ve prospěch oprávněné třetí strany, přičemž – v případě, že dovozce údajů fakticky zmizel, z právního hlediska zanikl nebo se dostal do platební neschopnosti – má vývozce údajů právo smlouvu s dílčím zpracovatelem vypovědět a dát dílčímu zpracovateli pokyn, aby osobní údaje vymazal nebo vrátil.

Doložka 10 Práva subjektu údajů

MODUL 1: Předání od správce správci

(a) Dovozce údajů, případně za pomoci vývozce údajů, vyřizuje veškeré dotazy a žádosti, které obdrží od subjektu údajů, týkající se zpracování jeho osobních údajů a výkonu jeho práv podle těchto doložek, a to bez zbytečného odkladu a nejpozději do jednoho měsíce od obdržení dotazu nebo žádosti. (10) Dovozce údajů přijme vhodná opatření k usnadnění vyřizování těchto dotazů, žádostí a výkonu práv subjektu údajů. Veškeré informace poskytované subjektu údajů musí být ve srozumitelném a snadno přístupném znění za použití jasných a jednoduchých jazykových prostředků.

(b) Na žádost subjektu údajů dovozce údajů zejména bezplatně:

(i) poskytne subjektu údajů potvrzení o tom, zda se zpracovávají osobní údaje, které se ho týkají, a v takovém případě mu poskytne kopii údajů, které se ho týkají, a informace uvedené v příloze I; pokud osobní údaje byly nebo budou dále předávány, poskytne informace o příjemcích nebo kategoriích příjemců (podle potřeby za účelem poskytnutí smysluplných informací), kterým osobní údaje byly nebo budou dále předávány, účel těchto dalších předání a jejich důvod v souladu s doložkou 8.7.; a poskytne informace o právu podat stížnost u

dozorového úřadu v souladu s doložkou 12 písm. c) bodem i);

ii) opraví nepřesné nebo neúplné údaje týkající se subjektu údajů;

(ii) vymaže osobní údaje týkající se subjektu údajů, pokud tyto údaje jsou nebo byly zpracovávány v rozporu s kteroukoli z těchto doložek, která zajišťuje práva náležející oprávněné třetí straně, nebo pokud subjekt údajů odvolá souhlas, na kterém je zpracování založeno.

(c) Pokud dovozce údajů zpracovává osobní údaje pro účely přímého marketingu, přestane je pro tyto účely zpracovávat, vznese-li proti tomu subjekt údajů námitky.

(d) Dovozce údajů nepřijme rozhodnutí založené výhradně na automatizovaném zpracování předávaných osobních údajů (dále jen "automatizované rozhodnutí"), které by mělo právní účinky týkající se subjektu údajů nebo by ho obdobně významně ovlivnilo, ledaže by k tomu subjekt údajů dal výslovný souhlas, nebo pokud by mu to bylo na základě právních předpisů země určení povoleno, za předpokladu, že takové právní předpisy stanoví vhodná opatření na ochranu práv a oprávněných zájmů subjektu údajů. V tomto případě dovozce údajů, v případě potřeby ve spolupráci s vývozcem údajů:

(i) informuje subjekt údajů o předpokládaném automatizovaném rozhodnutí, předpokládaných důsledcích a použitém postupu a

(ii) zavede vhodná ochranná opatření, přinejmenším tím, že umožní subjektu údajů napadnout rozhodnutí, vyjádřit svůj názor a dosáhnout přezkumu prováděného člověkem.

(e) Jestliže jsou žádosti subjektu údajů nepřiměřené, zejména proto, že se opakují, může dovozce údajů buď uložit přiměřený poplatek, v němž budou zohledněny administrativní náklady související s vyhověním dané žádosti, nebo může odmítnout žádosti vyhovět.

(f) Dovozce údajů může žádost subjektu údajů odmítnout, pokud je takové odmítnutí umožněno podle práva země určení a je v demokratické společnosti nezbytné a přiměřené za účelem ochrany jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679.

(g) Pokud má dovozce údajů v úmyslu žádost subjektu údajů odmítnout, informuje subjekt údajů o důvodech odmítnutí a možnosti podat stížnost u příslušného dozorového úřadu a/nebo požádat o soudní ochranu.

MODUL 2: Předání od správce zpracovateli

(a) Dovozce údajů neprodleně informuje vývozce údajů o každé žádosti, kterou od subjektu údajů přijal. Na tuto žádost sám neodpoví, pokud k tomu nedostal povolení od vývozce údajů.

(b) Dovozce údajů vývozci údajů pomáhá při plnění jeho povinností reagovat na žádosti subjektů údajů týkající se výkonu jejich práv podle nařízení (EU) 2016/679. V tomto ohledu stanoví strany v příloze II příslušná technická a organizační opatření s přihlédnutím k povaze zpracování, prostřednictvím něhož bude pomoc poskytována, a stanoví i rozsah a dosah požadované pomoci.

(c) Při plnění svých povinností podle písmen a) a b) musí dovozce údajů dodržovat pokyny vývozce údajů.

MODUL 3: Předání od zpracovatele zpracovateli

(a) Dovozce údajů neprodleně informuje vývozce údajů a v příslušném případě i správce o každé žádosti, kterou od subjektu údajů přijal, aniž by na tuto žádost reagoval, ledaže by k tomu dostal od správce povolení.

(b) Dovozce údajů, případně ve spolupráci s vývozcem údajů, pomáhá správci při plnění jeho povinností reagovat na žádosti subjektů údajů týkající se výkonu jejich práv podle nařízení (EU) 2016/679 nebo v příslušném případě

nařízení (EU) 2018/1725. V tomto ohledu stanoví strany v příloze II příslušná technická a organizační opatření s přihlédnutím k povaze zpracování, prostřednictvím něhož bude pomoc poskytována, a stanoví i rozsah a dosah požadované pomoci.

(c) Při plnění svých povinností podle písmen a) a b) musí dovozce údajů dodržovat pokyny správce, které mu jsou sděleny vývozcem údajů.

MODUL 4: Předání od zpracovatele správci

Strany si vzájemně pomáhají při odpovídání na dotazy a žádosti subjektů údajů podle místního práva použitelného na dovozce údajů nebo v případě zpracování údajů dovozcem údajů v EU podle nařízení (EU) 2016/679.

Doložka 11 Náprava

(a) Dovozce údajů transparentně a ve snadno přístupném formátu informuje subjekty údajů prostřednictvím individuálního oznámení nebo na svých internetových stránkách o kontaktním místě oprávněném vyřizovat stížnosti. Takové místo neprodleně vyřídí jakékoli stížnosti, které od subjektu údajů přijme.

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(b) V případě sporu mezi subjektem údajů a jednou ze smluvních stran týkajícího se dodržování těchto doložek vyvine tato strana veškeré úsilí k tomu, aby takovou záležitost vyřešila smírně a včas. Strany se o těchto sporech navzájem informují a v příslušných případech při jejich řešení spolupracují.

(c) Pokud se subjekt údajů dovolává práva ve prospěch oprávněné třetí strany podle doložky 3, dovozce údajů akceptuje rozhodnutí subjektu údajů:

(i) podat stížnost u dozorového úřadu v členském státě svého obvyklého bydliště nebo místa výkonu práce nebo u příslušného dozorového úřadu podle doložky 13;

(ii) postoupit spor příslušným soudům ve smyslu doložky 18.

(d) Strany jsou srozuměny, že subjekt údajů může být zastoupen neziskovým subjektem, organizací nebo sdružením za podmínek stanovených v čl. 80 odst. 1 nařízení (EU) 2016/679.

(e) Dovozce údajů dodržuje rozhodnutí závazné podle platného práva EU nebo členského státu.

(f) Dovozce údajů souhlasí s tím, že výběr provedený subjektem údajů nebude mít vliv na jeho hmotná a procesní práva požadovat nápravu v souladu s platnými právními předpisy.

Doložka 12 Odpovědnost

MODUL 1: Předání od správce správci

MODUL 4: Předání od zpracovatele správci

(a) Každá strana je vůči druhé straně/ostatním stranám odpovědná za jakoukoli újmu, kterou druhé straně/ostatním stranám při porušení těchto doložek způsobí.

(b) Každá strana je odpovědná vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou strana způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek. Tím není dotčena odpovědnost vývozce údajů podle nařízení (EU) 2016/679.

(c) Pokud je za újmu způsobenou subjektu údajů v důsledku porušení těchto doložek odpovědná více než jedna strana, nesou společnou a nerozdílnou odpovědnost všechny odpovědné strany a subjekt údajů je oprávněn proti kterékoli z těchto stran podat žalobu u soudu.

(d) Smluvní strany se dohodly, že pokud je jedna ze smluvních stran odpovědná podle písmene c), je oprávněna požadovat od druhé smluvní strany/ostatních smluvních stran zpět část náhrady újmy odpovídající její odpovědnosti za újmu.

(e) Dovozce údajů se nemůže dovolávat jednání zpracovatele nebo dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) Každá strana je vůči druhé straně/ostatním stranám odpovědná za jakoukoli újmu, kterou druhé straně/ostatním stranám při porušení těchto doložek způsobí.

(b) Dovozce údajů je odpovědný vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou dovozce údajů nebo jeho dílčí zpracovatel způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek.

(c) Aniž by bylo dotčeno písmeno b), vývozce údajů je odpovědný vůči subjektu údajů a subjekt údajů má nárok na náhradu jakékoli hmotné nebo nehmotné újmy, kterou vývozce údajů nebo dovozce údajů (nebo jeho dílčí zpracovatel) způsobí subjektu údajů porušením práv náležejících oprávněné třetí straně na základě těchto doložek. Tím není dotčena odpovědnost vývozce údajů, a pokud je vývozcem údajů zpracovatel jednající jménem správce, odpovědnost správce podle nařízení (EU) 2016/679 nebo nařízení (EU) 2018/1725.

(d) Strany se dohodly, že pokud je vývozce údajů odpovědný podle písmene c) za újmu způsobenou dovozcem údajů (nebo jeho dílčím zpracovatelem), je oprávněn požadovat od dovozce údajů část náhrady újmy odpovídající odpovědnosti dovozce údajů za újmu.

(e) Pokud je za újmu způsobenou subjektu údajů v důsledku porušení těchto doložek odpovědná více než jedna strana, nesou společnou a nerozdílnou odpovědnost všechny odpovědné strany a subjekt údajů je oprávněn proti kterékoli z těchto stran podat žalobu u soudu.

(f) Smluvní strany se dohodly, že pokud je jedna ze smluvních stran odpovědná podle písmene e), je oprávněna požadovat od druhé smluvní strany/ostatních smluvních stran zpět část náhrady újmy odpovídající její odpovědnosti za újmu.

(g) Dovozce údajů se nemůže dovolávat jednání dílčího zpracovatele, aby se vyhnul své vlastní odpovědnosti.

Doložka 13 Dohled

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) [Pokud je vývozce údajů usazen v členském státě EU:] Dozorový úřad uvedený v příloze I části C, který je odpovědný za zajištění, že vývozce údajů dodržuje nařízení (EU) 2016/679, pokud jde o předávání údajů, jedná jako příslušný dozorový úřad.

[Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2 a jmenoval zástupce podle čl. 27 odst. 1 nařízení (EU) 2016/679:] Dozorový úřad členského státu – uvedený v příloze I části C–, v němž je usazen zástupce ve smyslu čl. 27 odst. 1 nařízení (EU) 2016/679, jedná jako příslušný dozorový úřad.

[Pokud vývozce údajů není usazen v členském státě EU, ale spadá do územní působnosti nařízení (EU) 2016/679 v souladu s jeho čl. 3 odst. 2, aniž by však musel jmenovat zástupce podle čl. 27 odst. 2 nařízení (EU) 2016/679:] Dozorový úřad jednoho z členských států, v nichž se nacházejí subjekty údajů, jejichž osobní údaje jsou předávány podle těchto doložek v souvislosti se zbožím nebo službami jim nabízenými, nebo jejichž chování je monitorováno, uvedený v příloze I části C, jedná jako příslušný dozorový úřad.

(b) Dovozce údajů souhlasí, že se podřídí pravomoci příslušného dozorového úřadu a bude s ním spolupracovat v rámci všech postupů zaměřených na zajištění dodržování těchto doložek. Dovozce údajů zejména souhlasí, že bude reagovat na dotazy, podrobovat se auditům a dodržovat opatření přijatá dozorovým úřadem, včetně nápravných a kompenzačních opatření. Dozorovému úřadu poskytne písemné potvrzení, že byla přijata nezbytná opatření.

ODDÍL III – MÍSTNÍ PRÁVNÍ PŘEDPISY A POVINNOSTI V PŘÍPADĚ PŘÍSTUPU ORGÁNŮ VEŘEJNÉ MOCI

Doložka 14 Místní právní předpisy a postupy mající dopad na dodržování doložek

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci (pokud zpracovatel z EU kombinuje osobní údaje přijaté od správce ve třetí zemi s osobními údaji shromážděnými zpracovatelem v EU)

(a) Strany zaručují, že nemají důvod se domnívat, že právní předpisy a postupy ve třetí zemi určení, které se vztahují na zpracování osobních údajů dovozcem údajů, včetně jakýchkoli požadavků na zpřístupnění osobních údajů nebo opatření, kterými se povoluje přístup orgánům veřejné moci, brání dovozci údajů při plnění svých povinností podle těchto doložek. To je založeno na předpokladu, že právní předpisy a postupy, které respektují podstatu základních práv a svobod a nepřekračují to, co je v demokratické společnosti nezbytné a přiměřené k zajištění jednoho z cílů uvedených v čl. 23 odst. 1 nařízení (EU) 2016/679, nejsou v rozporu s těmito doložkami.

(b) Smluvní strany prohlašují, že při poskytování záruky uvedené v písmenu a) náležitě zohlednily zejména následující prvky:

(i) konkrétní okolnosti předání, včetně délky zpracovatelského řetězce, počtu zapojených subjektů a použitých kanálů pro přenos údajů, zamýšlené další předání, druh příjemce, účely zpracování, kategorie a formát předávaných osobních údajů, hospodářské odvětví, v němž se předávání uskutečňuje, místo, kde se předané údaje uchovávají;

(ii) právní předpisy a postupy třetí země určení – včetně těch, které vyžadují zpřístupnění údajů orgánům veřejné moci nebo povolují přístup těchto orgánů – relevantní s ohledem na konkrétní okolnosti předání, jakož i použitelná omezení a záruky (12);

(iii) veškeré příslušné smluvní, technické nebo organizační záruky zavedené za účelem doplnění záruk podle těchto doložek, včetně opatření uplatňovaných během předání a zpracování osobních údajů v zemi určení.

(c) Dovozce údajů zaručuje, že při provádění posouzení podle písmene b) vynaložil maximální úsilí, aby poskytl vývozci údajů relevantní informace, a souhlasí s tím, že bude při zajišťování dodržování těchto doložek s vývozcem údajů i nadále spolupracovat.

(d) Strany souhlasí, že posouzení podle písmene b) zdokumentují a na požádání zpřístupní příslušnému dozorovému úřadu.

(e) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, pokud má po vyjádření souhlasu s těmito ustanoveními a po dobu trvání smlouvy důvod se domnívat, že se na něj vztahují, nebo se začaly vztahovat právní předpisy nebo postupy, které nejsou v souladu s požadavky podle písmene a), a to i po změně v právních předpisech třetí země nebo opatření (jako je například žádost o poskytnutí údajů), jež svědčí o tom, že uplatňování těchto právních předpisů v praxi není v souladu s požadavky uvedenými v písmeni a). [Pokud jde o modul 3: Vývozce údajů předá oznámení správci.]

(f) Po oznámení podle písmene e), nebo pokud má vývozce údajů jinak důvod se domnívat, že dovozce údajů již nemůže plnit své povinnosti na základě těchto doložek, vývozce údajů neprodleně určí vhodná opatření (např. technická nebo organizační opatření k zajištění bezpečnosti a důvěrnosti), která má přijmout vývozce údajů a/nebo dovozce údajů k řešení situace [pokud jde o modul 3: případně po konzultaci se správcem]. Vývozce údajů pozastaví předávání údajů, pokud se domnívá, že pro toto předávání nemohou být zajištěny žádné vhodné záruky, nebo pokud mu dá pokyn [pokud jde o modul 3: správce nebo] příslušný dozorový úřad. V tomto případě je vývozce údajů oprávněn vypovědět smlouvu, pokud jde o zpracování osobních údajů podle těchto doložek. Pokud smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak. Jestliže je smlouva vypovězena podle této doložky, použije se doložka 16 písm. d) a e).

Doložka 15 Povinnost dovozce údajů v případě přístupu orgánů veřejné moci

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci (pokud zpracovatel z EU kombinuje osobní údaje přijaté od správce ve třetí zemi s osobními údaji shromážděnými zpracovatelem v EU)

15.1. Oznámení

(a) Dovozce údajů souhlasí s tím, že neprodleně uvědomí vývozce údajů, a je-li to možné, subjekt údajů (v případě potřeby s pomocí vývozce údajů), pokud:

/i) na základě právních předpisů země určení obdrží právně závaznou žádost od orgánu veřejné moci, včetně soudních orgánů, o zpřístupnění osobních údajů předaných podle těchto doložek; takové oznámení obsahuje informace o požadovaných osobních údajích, dožadujícím orgánu, právním základu žádosti a poskytnuté

odpovědi, nebo

(ii) se dozví o jakémkoli přímém přístupu orgánů veřejné moci k osobním údajům předávaným podle těchto doložek v souladu s právními předpisy země určení; takové oznámení obsahuje všechny informace dostupné dovozci.

[Pokud jde o modul 3: Vývozce údajů předá oznámení správci.]

(b) Pokud je podle právních předpisů země určení dovozci údajů zakázáno informovat vývozce údajů a/nebo subjekt údajů, souhlasí dovozce údajů s tím, že za účelem co nejrychlejšího sdělení co největšího množství informací vynaloží maximální úsilí, aby od tohoto zákazu bylo upuštěno. Dovozce údajů souhlasí, že zdokumentuje své maximální úsilí, aby je mohl na žádost vývozce údajů prokázat.

(c) Je-li to povoleno právními předpisy země určení, dovozce údajů souhlasí, že bude poskytovat vývozci údajů v pravidelných intervalech po dobu trvání smlouvy co nejrelevantnější informace o přijatých žádostech (zejména informace o počtu žádostí, druhu požadovaných údajů, dožadujícím orgánu nebo orgánech, zda byly tyto žádosti napadeny a výsledek takového napadení atd.). [Pokud jde o modul 3: Vývozce údajů předá informace správci.]

(d) Dovozce údajů souhlasí s tím, že po dobu trvání smlouvy bude informace podle písmene a) až c) uchovávat a na vyžádání je poskytne příslušnému dozorovému úřadu.

(e) Písmeny a) až c) není dotčena povinnost dovozce údajů podle doložky 14 písm. e) a doložky 16 neprodleně informovat vývozce údajů, pokud není schopen tyto doložky dodržovat.

15.2. Přezkum zákonnosti a minimalizace údajů

(a) Dovozce údajů souhlasí s tím, že přezkoumá zákonnost žádosti o poskytnutí údajů, zejména zda nepřekročila meze pravomocí udělených dožadujícímu orgánu veřejné moci, a že žádost napadne, pokud po pečlivém posouzení dojde k závěru, že existují opodstatněné důvody se domnívat, že žádost je podle právních předpisů země určení, platných závazků podle mezinárodního práva a zásad mezinárodní zdvořilosti protiprávní. Dovozce údajů za stejných podmínek využívá možností odvolání. Při napadení žádosti dovozce údajů přijme předběžná opatření s cílem pozastavit účinky žádosti, dokud příslušný soudní orgán nerozhodne o její opodstatněnosti. Nezpřístupní požadované osobní údaje, dokud mu taková povinnost nebude stanovena na základě platných procesních pravidel. Těmito požadavky nejsou dotčeny povinnosti dovozce údajů podle doložky 14 písm. e).

(b) Dovozce údajů souhlasí, že zdokumentuje své právní posouzení i jakékoli napadení žádosti o poskytnutí údajů a v rozsahu povoleném právními předpisy země určení zpřístupní dokumentaci vývozci údajů. Na požádání ji rovněž zpřístupní příslušnému dozorovému úřadu. [Pokud jde o modul 3: Vývozce údajů posouzení zpřístupní správci.]

(c) Dovozce údajů souhlasí s poskytnutím minimálního přípustného množství informací při odpovědi na žádost o zpřístupnění, a to na základě přiměřeného výkladu žádosti.

ODDÍL IV – ZÁVĚREČNÁ USTANOVENÍ

Doložka 16 Nedodržení doložek a vypovězení

(a) Dovozce údajů neprodleně informuje vývozce údajů, pokud není z jakéhokoli důvodu schopen tyto doložky dodržet.

(b) Pokud dovozce údajů poruší tyto doložky nebo není schopen tyto doložky dodržet, vývozce údajů pozastaví předávání osobních údajů dovozci údajů, dokud není dodržování opět zajištěno nebo smlouva vypovězena. Tímto

není dotčena doložka 14 písm. f).

(c) Vývozce údajů je oprávněn vypovědět smlouvu v rozsahu, v němž se jedná o zpracování osobních údajů podle těchto doložek, pokud:

(i) vývozce údajů pozastavil předávání osobních údajů dovozci údajů podle písm. b) a dodržování těchto doložek není v přiměřené lhůtě a v každém případě do jednoho měsíce od pozastavení obnoveno;

(ii) dovozce údajů tyto doložky podstatně nebo trvale porušuje nebo

(iii) dovozce údajů nedodrží závazné rozhodnutí příslušného soudu nebo dozorového úřadu týkajícího se jeho povinností podle těchto doložek.

V takových případech o nedodržení informuje příslušný dozorový úřad [pokud jde o modul 3: a správce]. Jestliže smlouva zahrnuje více než dvě smluvní strany, může vývozce údajů toto právo na vypovězení uplatnit pouze ve vztahu k příslušné straně, pokud se strany nedohodly jinak.

d) [Pokud jde o modul 1, 2 a 3: Osobní údaje, které byly předány před vypovězením smlouvy podle písmene c), musí být podle volby vývozce údajů neprodleně vráceny vývozci údajů nebo vymazány v celém rozsahu. To samé se uplatní ve vztahu k veškerým kopiím údajů.] [Pokud jde o modul 4: Osobní údaje shromážděné vývozcem údajů v EU, které byly předány před vypovězením smlouvy podle písmene c), musí být neprodleně vymazány v celém rozsahu, včetně veškerých jejich kopií.] Dovozce údajů potvrdí vývozci údajů, že byly údaje vymazány. Dokud nejsou údaje vymazány nebo vráceny, dovozce údajů nadále zajišťuje soulad s těmito doložkami. V případě, že se na dovozce údajů vztahují místní právní předpisy, které mu zakazují předané osobní údaje vrátit nebo vymazat, dovozce údajů zaručuje, že bude i nadále zajišťovat dodržování těchto doložek a bude údaje zpracovávat pouze v takovém rozsahu a tak dlouho, jak to uvedené místní právo vyžaduje.

(e) Kterákoli ze stran může odvolat svůj souhlas s tím, že bude vázána těmito doložkami, pokud i) Evropská komise přijme rozhodnutí podle čl. 45 odst. 3 nařízení (EU) 2016/679 týkající se předávání osobních údajů, na které se tyto doložky vztahují, nebo ii) se nařízení (EU) 2016/679 stane součástí právního rámce země, do které jsou osobní údaje předávány. Tím nejsou dotčeny další povinnosti vztahující se na dotčené zpracování podle nařízení (EU) 2016/679.

Doložka 17 Rozhodné právo

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

Tyto doložky se řídí právem jednoho z členských států EU, pokud takové právo umožňuje uplatňovat práva náležející oprávněné třetí straně. Strany se dohodly, že se budou řídit právem definovaným v Podmínkách.

MODUL 4: Předání od zpracovatele správci

Tyto doložky se řídí právem země, jež umožňuje uplatňovat práva náležející oprávněné třetí straně. Strany se dohodly, že se budou řídit právem definovaným v Podmínkách.

Doložka 18 Volba soudu a příslušnost

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

(a) Veškeré spory vyplývající z těchto doložek budou řešeny soudy členského státu EU.

(b) Strany se dohodly, že se budou řídit soudy definovanými v Podmínkách.

(c) Subjekt údajů může rovněž zahájit soudní řízení proti vývozci údajů a/nebo dovozci údajů před soudy členského státu, v němž má subjekt údajů své obvyklé bydliště.

(d) Smluvní strany se dohodly, že se příslušnosti těchto soudů podřídí.

MODUL 4: Předání od zpracovatele správci

Veškeré spory vyplývající z těchto doložek budou řešeny soudy jak je definováno v Podmínkách.

DODATEK

VYSVĚTLIVKY: Musí být možné jasně rozlišit informace, které se vztahují na každé předání nebo každou kategorii předání, a v tomto ohledu určit příslušnou úlohu/příslušné úlohy stran v postavení vývozce/vývozců údajů a/nebo dovozce/dovozců údajů. To nemusí nutně vyžadovat vyplnění a podepsání samostatných dodatků pro každé předání/kategorii předání a/nebo smluvní vztah, pokud lze této transparentnosti dosáhnout prostřednictvím jednoho dodatku. Pokud je to však nutné k zajištění dostatečné srozumitelnosti, měly by se použít samostatné dodatky.

PŘÍLOHA I

A. SEZNAM SMLUVNÍCH STRAN

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci

Vývozce (vývozci) údajů: [Totožnost a kontaktní údaje vývozce/vývozců údajů a v příslušném případě jeho/jejich pověřence pro ochranu osobních údajů a/nebo zástupce v Evropské unii]

1. Správce, jak je definován ve Smlouvě o zpracování údajů

2. Zpracovatel, jak je definován ve Smlouvě o zpracování údajů

(na základě toku dat)

Dovozce nebo dovozci údajů: [Totožnost a kontaktní údaje dovozce/dovozců údajů, včetně jakékoli kontaktní osoby, která je odpovědná za ochranu údajů]

1. Správce, jak je definován ve Smlouvě o zpracování údajů

2. Zpracovatel, jak je definován ve Smlouvě o zpracování údajů

(na základě toku dat)

B. POPIS PŘEDÁNÍ

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

MODUL 4: Předání od zpracovatele správci

Kategorie subjektů údajů, jejichž osobní údaje se předávají: Jak je definováno ve Smlouvě o zpracování údajů.

Kategorie předávaných osobních údajů: Jak je definováno ve Smlouvě o zpracování údajů a Zásadách ochrany osobních údajů.

Citlivé údaje, které se předávají (v příslušných případech), a uplatněná omezení nebo záruky, jež plně zohledňují povahu údajů a související rizika, například přísné účelové omezení, omezení přístupu (včetně přístupu pouze pro zaměstnance, kteří absolvovali specializované školení), vedení záznamu o přístupu k údajům, omezení pro další předávání nebo dodatečná bezpečnostní opatření: Jak je definováno ve Smlouvě o zpracování údajů a Zásadách ochrany osobních údajů.

Četnost předávání (např. zda jsou údaje předávány jednorázově nebo průběžně): Průběžně.

Povaha zpracování: Automatizovaně.

Účel nebo účely předání údajů a další zpracování: Poskytování služeb, jak je definováno v Podmínkách, jejich Přílohách, Zásadách ochrany osobních údajů a servisní dokumentaci.

Doba, po kterou budou osobní údaje uchovávány, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby: Jak je definováno ve Smlouvě o zpracování údajů.

Pokud jde o předávání (dílčím) zpracovatelům, rovněž uveďte předmět, povahu a trvání zpracování: Jak je definováno ve Smlouvě o zpracování údajů.

C. PŘÍSLUŠNÝ DOZOROVÝ ÚŘAD

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

V souladu s doložkou 13 určete příslušný dozorový úřad nebo příslušné dozorové úřady: Jak je definováno v Zásadách ochrany osobních údajů

PŘÍLOHA II TECHNICKÁ A ORGANIZAČNÍ OPATŘENÍ VČETNĚ TECHNICKÝCH A ORGANIZAČNÍCH OPATŘENÍ K ZAJIŠTĚNÍ ZABEZPEČENÍ ÚDAJŮ

MODUL 1: Předání od správce správci

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

VYSVĚTLIVKY: Technická a organizační opatření musí být popsána konkrétně (nikoli obecně). Viz také obecnou poznámku na první stránce dodatku, týkající se zejména potřeby jasně uvést, která opatření se vztahují na každé jednorázové nebo souborné předání.

Popis technických a organizačních opatření zavedených dovozcem nebo dovozci údajů (včetně veškerých příslušných certifikací) za účelem zajištění vhodné úrovně zabezpečení s přihlédnutím k povaze, rozsahu, kontextu a účelu zpracování a rizikům pro práva a svobody fyzických osob: Jak je definováno v Bezpečnostní dokumentaci

Pokud jde o předávání údajů (dílčím) zpracovatelům, popište také konkrétní technická a organizační opatření, která má (dílčí) zpracovatel přijmout, aby mohl poskytnout pomoc správci; a – v případě předávání od zpracovatele dílčímu zpracovateli – vývozci údajů.

PŘÍLOHA III SEZNAM DÍLČÍCH ZPRACOVATELŮ

MODUL 2: Předání od správce zpracovateli

MODUL 3: Předání od zpracovatele zpracovateli

VYSVĚTLIVKY: Tuto přílohu je třeba vyplnit pro moduly 2 a 3 pro případ zvláštního povolení dílčích zpracovatelů (doložka 9 písm. a), varianta 1).

Správce udělil povolení pro zapojení následujících dílčích zpracovatelů: Jak je definováno ve Smlouvě o zpracování údajů

Odkazy:

(1) Pokud je vývozcem údajů zpracovatel, na nějž se vztahuje nařízení (EU) 2016/679 a který jedná jménem orgánu nebo subjektu Unie jako správce, spoléhání se na tyto doložky při zapojení jiného zpracovatele (dílčí zpracování), na kterého se nařízení (EU) 2016/679 nevztahuje, rovněž zajišťuje soulad s čl. 29 odst. 4 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie, a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí 1247/2002/ES (Úř. věst. L 295 ze dne 21.11.2018, s. 39), v rozsahu, v němž jsou tyto doložky a povinnosti týkající se ochrany údajů stanovené ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle čl. 29 odst. 3 nařízení (EU) 2018/1725 sladěny. To bude zejména případ, kdy se správce a zpracovatel spoléhají na standardní smluvní doložky obsažené v rozhodnutí 2021/915.

(2) To vyžaduje anonymizaci údajů takovým způsobem, aby již nikdo nemohl být nikým identifikovatelný, v souladu s 26. bodem odůvodnění nařízení (EU) 2016/679, a aby byl tento proces nevratný.

(3) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(4) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(5) 28 odst. 4 nařízení (EU) 2016/679, a pokud je správcem orgán nebo jiný subjekt EU, čl. 29 odst. 4 nařízení (EU) 2018/1725.

(6) Dohoda o Evropském hospodářském prostoru (Dohoda o EHP) stanoví rozšíření vnitřního trhu Evropské unie o tři státy EHP, a to Island, Lichtenštejnsko a Norsko. Dohoda o EHP zahrnuje právní předpisy Unie o ochraně údajů, včetně nařízení (EU) 2016/679, které jsou začleněny do přílohy XI uvedené dohody. Jakékoli zpřístupnění dovozcem údajů třetí straně se sídlem v EHP se proto pro účely těchto doložek nepovažuje za další předávání.

(7) Mimo jiné se jedná o to, zda se předávání a další zpracování týká i osobních údajů vypovídajících o rasovém nebo etnickém původu, politických názorech, náboženském vyznání nebo filozofickém přesvědčení nebo členství v odborech, genetických údajů nebo biometrických údajů za účelem jedinečné identifikace fyzické osoby, údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby nebo údajů týkajících se rozsudků v trestních věcech nebo trestných činů.

(8) Tento požadavek může být splněn dílčím zpracovatelem přistupujícím k těmto doložkám v rámci příslušného modulu v souladu s doložkou 7.

(9) Tento požadavek může být splněn dílčím zpracovatelem přistupujícím k těmto doložkám v rámci příslušného modulu v souladu s doložkou 7.

(10) Tuto lhůtu lze v nezbytném rozsahu s přihlédnutím ke složitosti a počtu žádostí prodloužit nejvýše o další dva měsíce. Dovozce údajů o takovém prodloužení řádně a neprodleně informuje subjekt údajů.

(11) Dovozce údajů může nabídnout nezávislé řešení sporů prostřednictvím rozhodčího orgánu pouze v případě, že je usazen v zemi, která ratifikovala Newyorskou úmluvu o výkonu rozhodčích nálezů.

(12) Pokud jde o dopad takových právních předpisů a postupů na dodržování těchto doložek, za součást celkového posouzení lze považovat různé prvky. Mezi tyto prvky mohou patřit relevantní a zdokumentované praktické zkušenosti s předchozími případy žádostí o zpřístupnění od orgánů veřejné moci nebo neexistence takových žádostí, které pokrývají dostatečně reprezentativní časový rámec. Týká se to zejména interních záznamů nebo jiné dokumentace, vypracovávané průběžně v souladu s náležitou péčí a certifikované na úrovni vrcholového vedení, za předpokladu, že tyto informace lze v souladu s právními předpisy sdílet se třetími stranami. Pokud se na základě této praktické zkušenosti dospěje k závěru, že dovozci údajů nebude bráněno v dodržování těchto doložek, je třeba to podpořit dalšími relevantními, objektivními prvky a je na smluvních stranách, aby pečlivě zvážily, zda tyto prvky mají společně dostatečnou váhu na podporu tohoto závěru, pokud jde o jejich spolehlivost a reprezentativnost. Smluvní strany musí zejména zohlednit, zda jsou jejich praktické zkušenosti potvrzeny veřejně dostupnými nebo jinak přístupnými spolehlivými informacemi o existenci či neexistenci žádostí ve stejném odvětví a/nebo o uplatňování práva v praxi, jako je například judikatura a zprávy nezávislých orgánů dohledu, a nejsou s nimi v rozporu.