ESET Mail Security

Používateľská príručka

Pre zobrazenie tohto dokumentu v online verzii kliknite sem

Digital Security
Progress. Protected.

ESET Mail Security bol vyvinutý spoločnosťou ESET, spol. s r. o.

Viac informácií nájdete na webovej stránke www.eset.sk.

Kontaktný formulár: https://www.eset.com/sk/podpora/kontakt/

REV. 17.1.2024

Prehľad

ESET Mail Security for Microsoft Exchange Server je integrované bezpečnostné riešenie, ktoré chráni e□mailové servery a e□mailové schránky používateľov pred rôznymi typmi škodlivého obsahu vrátane e□mailových príloh infikovaných červami alebo trójskymi koňmi, dokumentov obsahujúcich nebezpečné skripty, phishingových schém, spamu, podvodných e□mailov a správ so sfalšovaným odosielateľom.

ESET Mail Security poskytuje štyri typy ochrany: antivírusovú, antispamovú, antiphishingovú a ochranu na základe pravidiel. ESET Mail Security filtruje škodlivý obsah v databázach e□mailových schránok a na vrstve prenosu e□mailov predtým, ako sa dostane do e□mailovej schránky príjemcu.

ESET Mail Security podporuje Microsoft Exchange Server 2007 a novšie verzie, ako aj Microsoft Exchange Server v klastrovom prostredí. Podporované sú aj špecifické roly Exchange servera (mailbox, hub, edge).

Popri poskytovaní ochrany pre Microsoft Exchange Server ESET Mail Security tiež obsahuje funkcie na zabezpečenie samotného servera (rezidentná ochrana, ochrana prístupu na web a ochrana e-mailových klientov).

Vzdialenú správu produktu ESET Mail Security vo väčších sieťach umožňuje nástroj ESET PROTECT. ESET Mail Security môžete navyše používať spolu s nástrojmi tretích strán, ktoré sú určené na vzdialený monitoring a správu (RMM).

Hlavné funkcie

V nasledujúcej tabuľke nájdete zoznam funkcií, ktoré sú dostupné v ESET Mail Security.

64-bitové jadro	Prispieva k vyššej výkonnosti a stabilite súčastí tvoriacich jadro produktu.
Antimalvér	Oceňovaná a inovatívna ochrana pred malvérom. Ide o najmodernejšiu technológiu, ktorá zabraňuje útokom a eliminuje všetky druhy hrozieb vrátane vírusov, ransomvéru, rootkitov, červov a spyvéru pomocou kontroly s podporou cloudu, vďaka ktorej je detekcia ešte účinnejšia. Navyše nezaťažuje systém, šetrí systémové prostriedky a nemá negatívny vplyv na výkon. Táto technológia pracuje na viacerých vrstvách. Každá vrstva (fáza) pozostáva z niekoľkých technológií. Pre-execution phase has technologies such as UEFI Scanner, Network Attack Protection, Reputation & Cache, In-product Sandbox, DNA Detections. Medzi technológie, ktoré sa využívajú vo fáze execution, patrí Exploit Blocker, Ransomware Shield, Pokročilá kontrola pamäte a Kontrola skriptov (AMSI), pričom vo fáze post-execution nachádza uplatnenie Ochrana pred botnetmi, Cloudový systém ochrany pred malvérom a Sandboxing. Kombinácia týchto kľúčových technológií vám poskytuje bezkonkurenčnú úroveň ochrany.
Antispam	Antispam je kľúčovým komponentom akéhokoľvek e-mailového servera. ESET Mail Security využíva špičkové antispamové jadro, ktoré filtruje spam a phishing s vysokou mierou detekcie. ESET Mail Security je niekoľkonásobným víťazom testu filtrovania a zachytávania spamu realizovaného poprednou testovacou organizáciou Virus Bulletin a niekoľkoročným držiteľom certifikácie VBSpam+. Naše antispamové jadro dosiahlo mieru detekcie spamu 99,99 % s nulovým výskytom falošne pozitívnych nálezov (false positive), vďaka čomu môžeme hovoriť o poprednej technológii v oblasti ochrany proti spamu. Antispam programu ESET Mail Security zahŕňa pre zaručenie maximálnej detekcie rôzne technológie (RBL a DNSBL, Fingerprinting, Kontrola reputácie, Analýza obsahu, Pravidlá, Whitelisting/blacklisting, Ochrana proti spätnému rozptylu a overovanie správ pomocou SPF a DKIM). Antispam v produkte ESET Mail Security je založený na dátach z cloudu, pričom väčšina využívaných cloudových databáz je umiestnených v datacentrách spoločnosti ESET. Antispamové cloudové služby umožňujú v prípade objavenia nového spamu pohotovo aktualizovať dáta v databázach a zabezpečiť tak rýchlejší reakčný čas.

Antiphishingová ochrana	Funkcia, ktorá zabraňuje používateľom v prístupe na phishingové webové stránky. E-mailové správy môžu obsahovať odkazy, ktoré smerujú na phishingové webové stránky. ESET Mail Security používa pokročilú a sofistikovanú metódu analýzy, pomocou ktorej sú telo a predmet prichádzajúcej správy prehľadávané s cieľom identifikácie takýchto odkazov (URL). Odkazy sú porovnávané voči databáze s phishingovým obsahom.
Pravidlá	Pravidlá umožňujú správcom filtrovať neželané e-mailové správy a prílohy v súlade s firemnou politikou. Môže ísť o prílohy, ako akými sú napríklad spustiteľné súbory, multimediálne súbory, archívy chránené heslom atď. Pre filtrované e-mailové správy a ich prílohy je možné vykonávať rôzne akcie, ako napríklad presunutie do karantény, vymazanie, odoslanie oznámenia, prípadne zapisovanie do protokolu udalostí.
Exportovať na syslog server (Arcsight)	Obsah protokolu ochrany e-mailových serverov je možné duplikovať na syslog server vo formáte Common Event Format (CEF) na použitie s riešeniami na správu protokolov, ako je napríklad Micro Focus ArcSight. Udalosti je možné odosielať cez SmartConnector do ArcSight, prípadne ich exportovať v podobe súborov. Poskytuje to pohodlný spôsob centralizovaného monitorovania a správy bezpečnostných udalostí. Túto funkciu môžete využiť najmä v prípade, že máte komplexnú infraštruktúru s veľkým počtom Microsoft Exchange Serverov, na ktorých používate riešenie ESET Mail Security.
Kontrola e-mailových schránok Office 365	Táto funkcia je určená pre firmy, ktoré používajú hybridné prostredie Exchange a zároveň pridáva možnosť kontrolovať e-mailové schránky v cloude.
ESET LiveGuard Advanced	Cloudová služba od spoločnosti ESET. Ak ESET Mail Security vyhodnotí e-mailovú správu ako podozrivú, správa je dočasne presunutá do ESET LiveGuard Advanced karantény. Podozrivá e-mailová správa je automaticky odoslaná na ESET LiveGuard Advanced server, kde dôjde k jej analýze pomocou pokročilých techník detekcie. ESET Mail Security následne dostane výsledky analýzy, podľa ktorých bude podozrivá správa spracovaná.
Správca e-mailovej karantény s webovým rozhraním	Správca môže prezerať súbory v karanténe a rozhodovať sa, či ich odstráni alebo uvoľní. Táto funkcia poskytuje ľahko použiteľný nástroj určený na správu. Webové rozhranie karantény umožňuje vzdialenú správu obsahu. Je možné určiť správcov karantény, prípadne delegovať prístup. Používatelia si po prihlásení do webového rozhrania e-mailovej karantény môžu prezerať a spravovať svoju spamovú poštu, pričom prístup majú len k svojim správam.
Reporty o e-mailovej karanténe	Reporty o karanténe sú e-maily odosielané vybraným používateľom alebo správcom, ktoré im poskytujú informácie o všetkých e-mailových správach presunutých do karantény. Táto funkcia im taktiež umožňuje vzdialene spravovať obsah umiestnený v karanténe.
Manuálna kontrola databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok umožňuje správcom manuálne kontrolovať e-mailové schránky, prípadne naplánovať kontrolu mimo pracovnej doby. Kontrola databáz e-mailových schránok využíva EWS (Exchange Web Services) API na pripojenie na Microsoft Exchange Server pomocou HTTP/HTTPS. Okrem toho sa pre zlepšenie výkonnosti využíva paralelná kontrola.
Klaster ESET	Klaster ESET umožňuje správu viacerých serverov z jedného miesta. Podobne ako v produkte ESET File Security pre Microsoft Windows Server, spájanie serverových uzlov do klastra robí spravovanie jednoduchším vďaka schopnosti distribuovať jednu konfiguráciu naprieč všetkými členmi klastra. Klaster ESET môže byť tiež použitý na synchronizáciu greylistingových databáz a obsahu lokálnej e-mailovej karantény.
Vylúčenia procesov	Táto funkcia slúži na vylúčenie konkrétnych procesov z antimalvérovej kontroly. Antimalvérová kontrola môže spôsobovať v určitých situáciách konflikty, napríklad počas zálohovania alebo živej migrácie virtuálnych počítačov. Vylúčenie procesov znižuje riziko konfliktov a zvyšuje celkový výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu celého systému. Vylúčenie procesu/aplikácie je vylúčenie samotného spustiteľného súboru (.exe).
eShell (ESET Shell)	eShell 2.0 je teraz dostupný pre ESET Mail Security. eShell je nástroj s príkazovým riadkom pre pokročilých používateľov, ktorým ponúka komplexnú správu produktov ESET určených pre server.

ESET PROTECT	Lepšia integrácia s nástrojom ESET PROTECT vrátane možnosti naplánovať rôzne úlohy. Viac informácií sa nachádza v Online pomocníkovi pre ESET PROTECT.
Inštalácia súčastí	Inštaláciu je možné prispôsobiť tak, aby obsahovala iba vybrané časti produktu.
Ochrana pred sfalšovaním identity odosielateľa	Nová funkcia, ktorá chráni pred rozšírenou technikou (v angličtine nazývanou spoofing), pri ktorej útočník sfalšuje informácie o odosielateľovi s cieľom oklamať príjemcu e□mailu. E□mailová správa sa javí byť odoslaná z legitímneho zdroja a pre príjemcu je tak veľmi ťažké rozlíšiť, či ide o pravého alebo falošného odosielateľa. Ochranu pred sfalšovaním identity odosielateľa môžete zapnúť a nakonfigurovať v Rozšírených nastaveniach alebo si vytvoriť vlastné pravidlá.
Podpisovanie DKIM	ESET Mail Security poskytuje funkciu podpisovania DKIM s cieľom posilniť zabezpečenie pre odchádzajúce e-mailové správy. Vyberte certifikát klienta a určite, ktoré e□mailové hlavičky sú podpísané podpisom DKIM. Podpisovanie DKIM môžete pri viacerých doménach nastaviť pre každú doménu zvlášť.

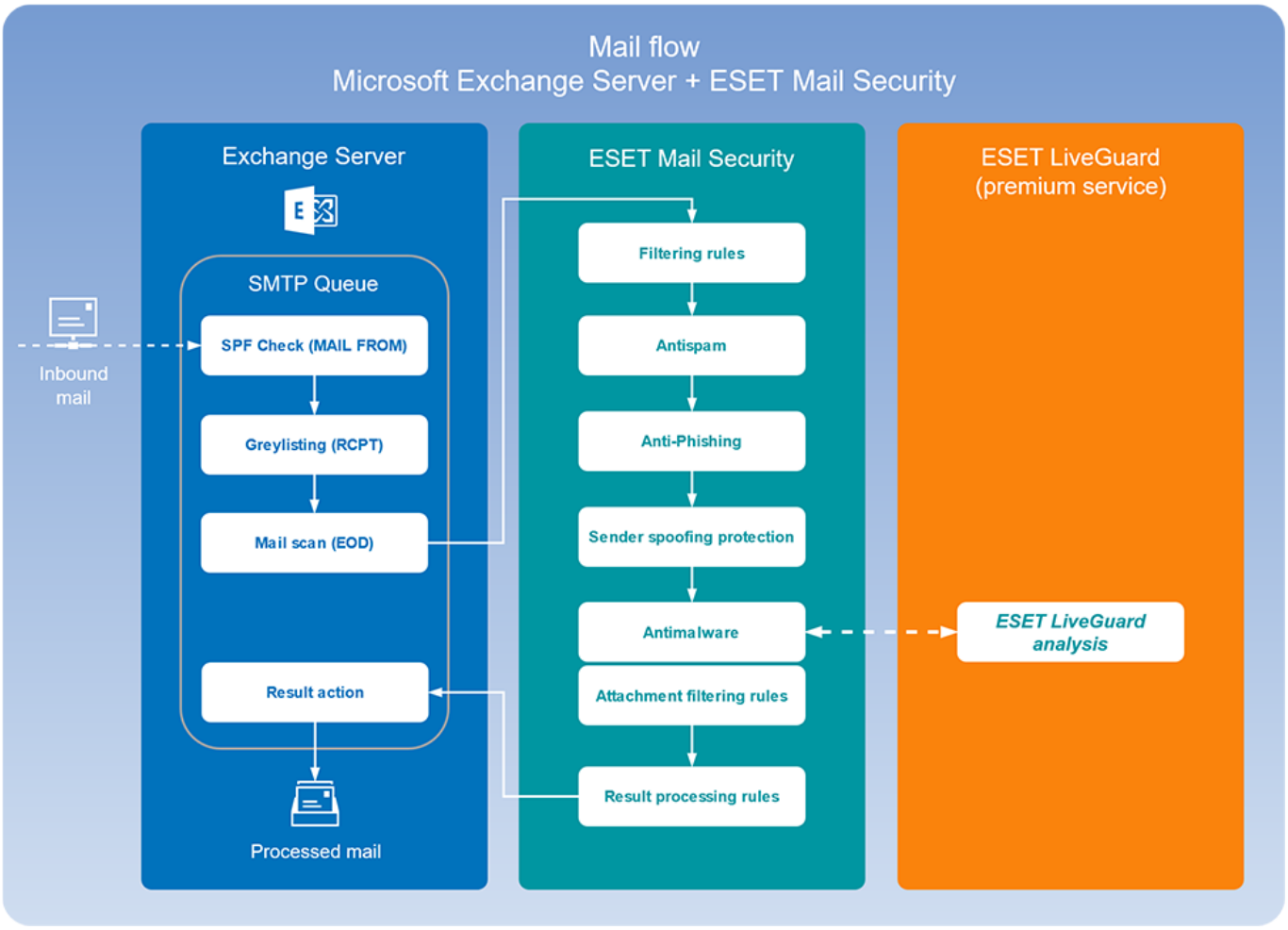
Čo je nové

Nové funkcie a vylepšenia v ESET Mail Security:

- 64-bitové jadro
- Kontrola e-mailových schránok Office 365
- Antiphishingová ochrana
- Ochrana proti spätnému rozptylu
- Správcovské reporty o e-mailovej karanténe
- Synchronizácia lokálnej e-mailovej karantény naprieč klastrom ESET
- Protokol SMTP ochrany
- ESET LiveGuard Advanced
- Podpora ESET Inspect
- ESET RMM
- Exportovať na syslog server (Arcsight)
- Izolácia od siete
- Ochrana využívajúca strojové učenie
- Protokoly auditu
- Mikroaktualizácie programových súčastí (µPCU)
- Ochrana pred sfalšovaním identity odosielateľa
- Podpisovanie DKIM

Tok pošty

Nasledujúci diagram zobrazuje tok pošty v rámci Microsoft Exchange Servera a ESET Mail Security. Podrobné informácie o používaní ESET LiveGuard Advanced spolu s ESET Mail Security nájdete v Online pomocníkovi k ESET LiveGuard Advanced.



ESET Mail Security – funkcie produktu a roly Exchange servera

Pomocou nasledujúcej tabuľky môžete zistiť, ktoré funkcie sú dostupné pre každú podporovanú verziu Microsoft Exchange Servera a jeho roly. Sprievodca inštaláciou ESET Mail Security kontroluje počas inštalácie vaše prostredie a po dokončení inštalácie produktu ESET Mail Security budete mať k dispozícii len tie funkcie, ktoré sú v danom prostredí podporované.

Verzia Exchange servera a rola servera	Antispamová ochrana	Antiphishingová ochrana	Pravidlá	Ochrana prenosu e-mailov	Manuálna kontrola databáz e-mailových schránok	Ochrana databáz e-mailových schránok
Microsoft Exchange Server 2007 (viaceré roly)	✓	✓	✓	✓	✓	✓

Verzia Exchange servera a rola servera	Antispamová ochrana	Antiphishingová ochrana	Pravidlá	Ochrana prenosu e-mailov	Manuálna kontrola databáz e-mailových schránok	Ochrana databáz e-mailových schránok
Microsoft Exchange Server 2007 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2007 (Hub)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2007 (Mailbox)	?	✓	✓	?	✓	✓
Microsoft Exchange Server 2010 (viaceré roly)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2010 (Mailbox)	?	✓	✓	?	✓	✓
Microsoft Exchange Server 2013 (viaceré roly)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2013 (Mailbox)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2016 (Mailbox)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	?	?
Microsoft Exchange Server 2019 (Mailbox)	✓	✓	✓	✓	✓	?
Windows Small Business Server 2011 SP1	✓	✓	✓	✓	✓	✓

Roly Exchange servera

Rola Edge a rola Hub

Obe roly, Edge Transport a Hub Transport, majú štandardne vypnutý antispam. Ide o požadované nastavenie v Exchange konfigurácii s Edge Transport serverom. Odporúčame mať na Edge Transport serveri ESET Mail Security antispam nastavený tak, aby filtroval správy pred tým, ako sú presmerované do Exchange.

Rola Edge je preferovaná pre antispamovú kontrolu, pretože umožňuje ESET Mail Security odmietnuť spam skoro a bez toho, aby zaťažoval sieťové vrstvy. Pri použití tejto konfigurácie sú prichádzajúce správy filtrované prostredníctvom ESET Mail Security na Edge Transport serveri, tak aby mohli byť bezpečne presunuté na Hub Transport server bez potreby ďalšieho filtrovania.

Ak vaša organizácia nepoužíva Edge Transport server a má iba Hub Transport server, odporúčame zapnúť funkciu

Antispam na Hub Transport serveri, ktorý prijíma prichádzajúce správy z internetu prostredníctvom SMTP.

Z dôvodu technických obmedzení systému Microsoft Exchange Server 2007 a novších systémov program ESET Mail Security nepodporuje nasadenie Microsoft Exchange Servera iba s rolou CAS (samostatný Client Access Server).

POP3 Connector a antispam

Operačné systémy typu Microsoft Windows Small Business Server (SBS) obsahujú zabudovaný nástroj POP3 Connector, ktorý umožňuje serveru sťahovať e-mailové správy z externých POP3 serverov. Implementácie nástroja Microsoft SBS POP3 Connector sa odlišujú pre rôzne verzie SBS systémov.

ESET Mail Security podporuje nástroj Microsoft SBS POP3 Connector, pokiaľ je správne nastavený. E-mailové správy stiahnuté pomocou nástroja Microsoft SBS POP3 Connector sú kontrolované na spam. Antispamová ochrana je funkčná vďaka tomu, že POP3 Connector odosiela e-mailové správy z POP3 účtu na Microsoft Exchange Server cez SMTP.

ESET Mail Security bol testovaný s najrozšírenejšími e□mailovými službami, akými sú Gmail.com, Outlook.com, Yahoo.com, Yandex.com a gmx.de, na nasledujúcom SBS systéme:

Microsoft Windows Small Business Server 2011 SP1

Ak používate zabudovaný nástroj Microsoft SBS POP3 Connector a chcete, aby boli všetky správy kontrolované na prítomnosť spamu, stlačením **F5** zobrazte okno **Rozšírené nastavenia**, prejdite do sekcie **Server** > **Ochrana prenosu e□mailov** > Pokročilé nastavenia a z roletového menu **Skontrolovať aj správy prijaté z overených alebo interných pripojení** vyberte možnosť **Antivírusová, antiphishingová a antispamová ochrana**. Toto nastavenie zaručuje antispamovú ochranu pre sťahované e-mailové správy z POP3 účtov.

Môžete tiež použiť nástroj tretích strán, ako napríklad P3SS konektor (namiesto zabudovaného nástroja Microsoft SBS POP3 Connector).

Moduly ochrany

Medzi kľúčové funkcie ESET Mail Security patria nasledujúce moduly ochrany:

Antivírus

Antivírusová ochrana je jednou zo základných funkcií produktu ESET Mail Security. Zabezpečuje komplexnú ochranu pred nebezpečnými programami a útokmi ohrozujúcimi systém. Zahŕňa kontrolu súborov, e□mailovej a internetovej komunikácie. V prípade zistenia škodlivého kódu dokáže antivírusový modul tento kód eliminovať jeho zablokovaním, následným vyliečením, zmazaním alebo presunutím do Karantény.

Antispam

Antispamová ochrana zahŕňa rôzne technológie pre maximalizáciu detekcie e-mailových hrozieb (RBL, DNSBL, Fingerprinting, kontrola reputácie, analýza obsahu, pravidlá, používateľské whitelisty/blacklisty atď.).
Antispam v produkte ESET Mail Security je založený na dátach z cloudu, pričom väčšina využívaných cloudových databáz je umiestnených v datacentrách spoločnosti ESET. Antispamové cloudové služby umožňujú v prípade objavenia nového spamu pohotovo aktualizovať dáta v databázach a zabezpečiť tak rýchlejší reakčný čas. Aktualizované sú taktiež aj cloudové blacklisty, z ktorých sú odstraňované nesprávne údaje. Komunikácia produktu s antispamovými cloudovými službami je zabezpečovaná prostredníctvom proprietárneho protokolu na porte 53535. V prípade, že nie je možné komunikovať cez ESET protokol, použijú sa DNS služby (port 53). DNS však nie je také efektívne, keďže počas spamovej klasifikácie jednej e-mailovej správy sa vyžaduje zaslanie viacerých požiadaviek.

> Odporúčame povoliť TCP a UDP komunikáciu na porte 53535 pre IP adresy uvedené v tomto článku Databázy znalostí spoločnosti ESET. Tento port používa ESET Mail Security na odosielanie požiadaviek.

Počas spamovej klasifikácie sa štandardne neodosielajú e-mailové správy ani žiadne ich súčasti. Avšak ak máte v produkte aktivovanú technológiu ESET LiveGrid® a povolili ste možnosť odosielania vzoriek na analýzu, e-mailové správy označené ako spam (alebo pravdepodobný spam) môžu byť odosielané do laboratórií spoločnosti ESET na podrobnú analýzu s cieľom vylepšovať cloudové databázy pre modul Antispam.
Ak došlo k nesprávnemu zaradeniu e-mailovej správy medzi spam alebo naopak nevyžiadaná správa ako spam označená nebola, môžete nám takúto skutočnosť nahlásiť. Viac informácií nájdete v tomto článku Databázy znalostí spoločnosti ESET.
Súčasťou antispamovej ochrany v ESET Mail Security je aj technika Greylisting (predvolene vypnutá).

Anti-Phishing

ESET Mail Security obsahuje Antiphishingovú ochranu, ktorá zabraňuje používateľom v prístupe na phishingové webové stránky. V prípade e-mailových správ, ktoré môžu obsahovať odkazy smerujúce na phishingové webové stránky, používa ESET Mail Security pokročilú a sofistikovanú metódu analýzy, pomocou ktorej sú telo a predmet prichádzajúcej správy prehľadávané s cieľom identifikácie takýchto odkazov (URL). Odkazy sú porovnávané voči databáze s phishingovým obsahom a vyhodnocované sú pravidlá s podmienkou typu Telo správy.

Pravidlá

Dostupnosť pravidiel pre Ochranu databáz e-mailových schránok, Manuálnu kontrolu databáz e-mailových schránok a Ochranu prenosu e-mailov závisí od toho, aká verzia Microsoft Exchange Servera je nainštalovaná na serveri, kde sa nachádza ESET Mail Security.
Pravidlá vám umožňujú manuálne definovať podmienky filtrovania e-mailových správ, ako aj akcie, ktoré budú vykonané s filtrovanými správami. K dispozícii máte rozličné podmienky a akcie. Môžete vytvárať individuálne pravidlá, ktoré môžu byť aj kombinované. Ak jedno pravidlo používa viac podmienok, podmienky budú prepojené pomocou logického operátora AND. Takéto pravidlo sa teda spustí len v prípade, že budú splnené všetky jeho podmienky. Pri viacerých pravidlách sa používa operátor OR, pričom program spustí prvé pravidlo, ktorého podmienky budú splnené.
Pri kontrole je na prvom mieste sekvencie použitá technika nazvaná greylisting (ak je povolená). Nasledujúce procedúry spúšťajú v rámci postupnosti kontroly tieto techniky: ochrana založená na pravidlách definovaných používateľom, antivírusová kontrola a nakoniec antispamová kontrola.

Viacvrstvové zabezpečenie

ESET Mail Security poskytuje komplexnú ochranu na rôznych úrovniach:

- Ochrana databáz e-mailových schránok
- Ochrana prenosu e-mailov
- Manuálna kontrola databáz e-mailových schránok
- Kontrola e-mailových schránok Office 365

Pre komplexnejší prehľad si pozrite maticu funkcií produktu ESET Mail Security a verzií a rol Microsoft Exchange Servera.

Ochrana databáz e-mailových schránok

Kontrola e-mailových databáz je spúšťaná a kontrolovaná pomocou Microsoft Exchange Servera. Správy v databáze MS Exchange Servera sú neustále kontrolované. Kontrola sa spúšťa v nasledujúcich situáciách, v závislosti od verzie MS Exchange Servera, verzie rozhrania VSAPI a používateľských nastavení:

- Ak používateľ pristupuje k správam, napríklad cez e-mailového klienta (správy sú vždy kontrolované s najnovšou verziou detekčného jadra).
- Na pozadí, ak je nízke zaťaženie MS Exchange Servera.
- Proaktívne (na základe vnútorného algoritmu MS Exchange Servera).

Ochrana databáz e-mailových schránok nie je dostupná pre Microsoft Exchange Server 2013, 2016 a 2019.

Ochrana databáz e-mailových schránok je dostupná pre nasledujúce typy systémov:

Verzia Exchange servera a rola servera	Antispamová ochrana	Antiphishingová ochrana	Pravidlá	Ochrana prenosu e-mailov	Manuálna kontrola databáz e-mailových schránok	Ochrana databáz e-mailových schránok
Microsoft Exchange Server 2007 (Mailbox)		✓	✓		✓	✓
Microsoft Exchange Server 2007 (viaceré roly)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Mailbox)		✓	✓		✓	✓
Microsoft Exchange Server 2010 (viaceré roly)	✓	✓	✓	✓	✓	✓
Windows Small Business Server 2011 SP1	✓	✓	✓	✓	✓	✓

Tento typ kontroly môže byť použitý aj pre konfiguráciu, pri ktorej je použitý len jediný server s viacerými rolami Exchange servera (len ak má server rolu Mailbox alebo Back-End).

Ochrana prenosu e-mailov

Filtrovanie na úrovni SMTP servera je zabezpečené špeciálnym doplnkom. Na systémoch Microsoft Exchange Server 2007 a 2010 je tento doplnok registrovaný ako agent prenosu rol Edge a Hub Microsoft Exchange Servera.

Filtrovanie na úrovni SMTP servera pomocou agenta prenosu poskytuje ochranu vo forme antivírusu, antispamu a používateľských pravidiel. Na rozdiel od filtrovania VSAPI, filtrovanie na úrovni SMTP servera prebieha pred tým,

ako je skontrolovaný e-mail doručený do e-mailovej schránky Microsoft Exchange Servera.

Predtým tiež známa ako Filtrovanie správ na úrovni SMTP servera, Táto ochrana je poskytovaná pomocou agenta prenosu a je dostupná len pre Microsoft Exchange Server 2007 (alebo novšie verzie). Váš Exchange Server však musí mať rolu Edge Transport Server alebo Hub Transport Server. Tento typ kontroly môže byť použitý aj pre konfiguráciu, pri ktorej je použitý len jediný server s viacerými rolami Exchange servera (len ak má server jednu zo spomenutých rolí).

Ochrana prenosu e-mailov je dostupná pre nasledujúce typy systémov:

Verzia Exchange servera a rola servera	Antispamová ochrana	Antiphishingová ochrana	Pravidlá	Ochrana prenosu e-mailov	Manuálna kontrola databáz e-mailových schránok	Ochrana databáz e-mailových schránok
Microsoft Exchange Server 2007 (Hub)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2007 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2010 (viaceré roly)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2013 (viaceré roly)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2013 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2013 (Mailbox)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2016 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2016 (Mailbox)	✓	✓	✓	✓	✓	☐
Microsoft Exchange Server 2019 (Edge)	✓	✓	✓	✓	☐	☐
Microsoft Exchange Server 2019 (Mailbox)	✓	✓	✓	✓	✓	☐
Windows Small Business Server 2011	✓	✓	✓	✓	✓	✓

Manuálna kontrola databáz e-mailových schránok

Manuálna kontrola databáz e☐mailových schránok vám umožňuje spustiť alebo naplánovať kontrolu databáz e☐mailových schránok Microsoft Exchange. Táto funkcia je dostupná len pre Microsoft Exchange Server 2007 (alebo novšie verzie) s rolami Mailbox server alebo Hub Transport. Týka sa to aj konfigurácie, pri ktorej je použitý len jediný server s viacerými rolami Exchange servera (len ak má server jednu zo spomenutých rolí).

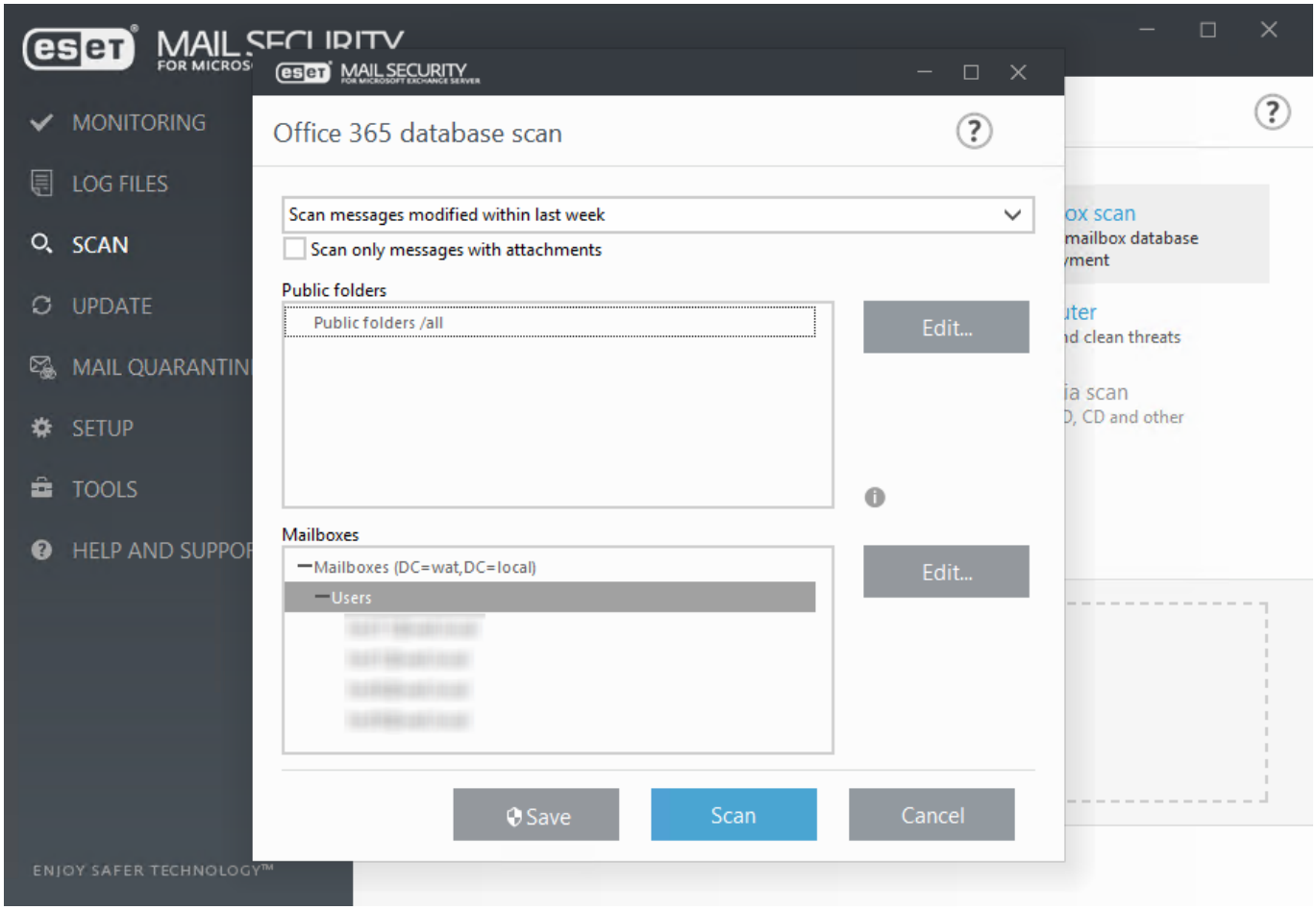
Manuálna kontrola databáz e-mailových schránok je dostupná pre nasledujúce systémy:

Verzia Exchange servera a rola servera	Antispamová ochrana	Antiphishingová ochrana	Pravidlá	Ochrana prenosu e-mailov	Manuálna kontrola databáz e-mailových schránok	Ochrana databáz e-mailových schránok
Microsoft Exchange Server 2007 (viaceré roly)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2007 (Hub)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2007 (Mailbox)	?	✓	✓	?	✓	✓
Microsoft Exchange Server 2010 (viaceré roly)	✓	✓	✓	✓	✓	✓
Microsoft Exchange Server 2010 (Hub)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2010 (Mailbox)	?	✓	✓	?	✓	✓
Microsoft Exchange Server 2013 (viaceré roly)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2013 (Mailbox)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2016 (Mailbox)	✓	✓	✓	✓	✓	?
Microsoft Exchange Server 2019 (Mailbox)	✓	✓	✓	✓	✓	?
Windows Small Business Server 2011 SP1	✓	✓	✓	✓	✓	✓

Kontrola e-mailových schránok Office 365

ESET Mail Security umožňuje vykonávať kontrolu v hybridných prostrediach Office 365. Táto funkcia je dostupná v ESET Mail Security len v prípade, že používate hybridné prostredie Exchange (lokálne alebo v cloude). Podporované sú obidva scenáre smerovania správ – buď prostredníctvom **Exchange Online**, alebo **lokálne** vo vašej organizácii. Podrobnejšie informácie nájdete v tomto článku spoločnosti Microsoft.

Môžete kontrolovať vzdialené e-mailové schránky Office 365 a verejné priečinky rovnako ako pomocou Manuálnej kontroly databáz e-mailových schránok.



Spustenie úplnej kontroly databáz vo veľkých prostrediach môže spôsobiť nežiaduce zaťaženie systému. Ak sa chcete tomuto problému vyhnúť, kontrolu spustite len na vybraných databázach alebo e-mailových schránkach. Na zníženie systémovej záťaže použite časový filter umiestnený v hornej časti okna. Z roletového menu tak môžete namiesto **Kontrolovať všetky správy** zvoliť napríklad možnosť **Kontrolovať správy zmenené za posledný týždeň**.

Odporúčame, aby ste si nastavili účet Office 365. Stlačte kláves **F5** a prejdite do sekcie **Server** > **Manuálna kontrola databáz e-mailových schránok**. Ďalšie informácie nájdete takisto v kapitole Podrobnosti účtu kontroly databáz.

Ak si chcete pozrieť aktivitu Kontroly e-mailových schránok Office 365, prejdite do časti **Protokoly** > **Kontrola databáz e-mailových schránok**.

Systémové požiadavky

Podporované operačné systémy:

- Microsoft Windows Server 2022 (Server Core a Desktop Experience)
- Microsoft Windows Server 2019 (Server Core a Desktop Experience)
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2

- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1 s nainštalovanými aktualizáciami KB4474419 a KB4490628 (prečítajte si informácie týkajúce sa vyžadovanej podpory SHA-2)
- Microsoft Windows Small Business Server 2011 SP1 (x64) s nainštalovanými aktualizáciami KB4474419 a KB4490628

Na operačnom systéme Windows Server 2008 R2 SP1 sa pri **Typickej** inštalácii predvolene neinštaluje komponent **Ochrana siete**. Ak chcete mať tento komponent nainštalovaný, zvoľte **Vlastnú** inštaláciu.

Inštalácia či aktualizácia produktov ESET vydaných po konci júla 2023 vyžaduje na všetkých operačných systémoch Windows podporu služby Azure Code Signing. Pre viac informácií kliknite sem.
Ak používate Windows Server 2008 R2 SP1, uistite sa, že máte nainštalovanú aktualizáciu KB5006728, ktorá podporuje Azure Code Signing. Na inštaláciu aktualizácie KB5006728 je potrebný program ESU (Extended Security Updates).

Podporované verzie Exchange serverov:

- Microsoft Exchange Server 2019 až do CU13
- Microsoft Exchange Server 2016 až do CU23
- Microsoft Exchange Server 2013 až do CU23 (CU1 a CU4 nie sú podporované)
- Microsoft Exchange Server 2010 SP1, SP2, SP3 až do RU32
- Microsoft Exchange Server 2007 SP1, SP2, SP3

Server iba s rolou CAS (samostatný Client Access Server) nie je podporovaný. Viac informácií nájdete v kapitole Roly Exchange servera.
Odporúčame prečítať si aj kapitolu o funkciách produktu ESET Mail Security a rolách Exchange servera, kde zistíte, ktoré funkcie sú dostupné pre každú podporovanú verziu Microsoft Exchange servera a jeho roly.

Minimálne hardvérové požiadavky:

Komponent	Požiadavky
Procesor	Jednojadrový x64 AMD alebo Intel
Pamäť	256 MB voľnej pamäte
Pevný disk	700 MB voľného miesta na disku
Rozlíšenie obrazovky	800 x 600 pixelov alebo vyššie

Pre ESET Mail Security platia rovnaké odporúčané hardvérové požiadavky ako pre Microsoft Exchange Server. Viac informácií nájdete v nasledujúcich technických článkoch spoločnosti Microsoft:

Microsoft Exchange Server 2007

Microsoft Exchange Server 2010

Microsoft Exchange Server 2013

Microsoft Exchange Server 2016

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

Potrebná kompatibilita s SHA-2

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

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

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

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

Microsoft Windows Server 2008 R2 SP1 – nainštalujte aktualizáciu KB4474419 a KB4490628 (môže byť potrebný reštart systému).

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

Po nainštalovaní aktualizácií a reštartovaní systému otvorte hlavné okno programu ESET Mail Security a skontrolujte jeho stav. V prípade, že stav je oranžový, vykonajte ďalší reštart systému. Stav by potom mal byť zelený, čo predstavuje maximálne zabezpečenie.

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

Príprava na inštaláciu

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

- Po zakúpení produktu ESET Mail Security si stiahnite inštalačný balík .msi z webovej stránky ESET.
- Uistite sa, že server, na ktorý plánujete nainštalovať ESET Mail Security, spĺňa systémové požiadavky.
- Prihláste sa na server pomocou účtu správcu.

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

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

- V prípade potreby zo svojho systému odinštalujte akýkoľvek antivírusový softvér tretích strán. Odporúčame použiť nástroj ESET AV Remover. Zoznam antivírusových programov tretích strán, ktoré možno odstrániť pomocou nástroja ESET AV Remover, nájdete v našom článku Databázy znalostí.

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

- Pri inštalácii ESET Mail Security na Windows Server 2019 spoločnosť Microsoft odporúča prepnúť Windows Defender do pasívneho režimu, aby ste predišli problémom zapríčineným súčasným používaním viacerých antivírusových riešení.

Ak je počas inštalácie produktu ESET Mail Security na vašom systéme **Windows Server 2016** alebo **2019** aktívny **Windows Defender**, ESET Mail Security vypne funkcie programu Windows Defender, aby sa predišlo konfliktom, ku ktorým dochádza pri súbežnom používaní viacerých antivírusových riešení. Funkcie nástroja Windows Defender sú vypnuté produktom ESET Mail Security taktiež pri každom spustení počítača alebo po reštarte.
Existuje však výnimka – ak inštalujete komponenty osobitne bez **rezidentnej ochrany súborového systému** , funkcie nástroja Windows Defender na operačnom systéme Windows Server 2016 nebudú vypnuté.

- Pre komplexnejší prehľad si pozrite maticu funkcií produktu ESET Mail Security a verzií a rol Microsoft Exchange Servera.

- Počet e□mailových schránok môžete zistiť spustením nástroja Mailbox Count. Bližšie informácie nájdete v nasledujúcom článku Databázy znalostí. Po nainštalovaní ESET Mail Security bude aktuálny počet e□mailových schránok zobrazený v dolnej časti okna Monitorovanie.

Inštalátor programu ESET Mail Security môžete spustiť v dvoch režimoch:

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

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

Odporúčame inštalovať ESET Mail Security na čistú inštaláciu nakonfigurovaného operačného systému. Ak však potrebujete nainštalovať ESET Mail Security na zabehnutý systém, najprv odinštalujte staršie verzie programu, reštartujte server a až potom nainštalujte novú verziu ESET Mail Security.

Aktualizácia na novú verziu
Ak používate staršiu verziu ESET Mail Security, môžete si vybrať vhodnú metódu aktualizácie.

Po úspešnej inštalácii alebo aktualizácii svojho produktu ESET Mail Security ešte môžete vykonať nasledovné:

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

Úlohy po inštalácii
Pozrite si zoznam úloh, ktoré odporúčame vykonať po úspešnej inštalácii ESET Mail Security.

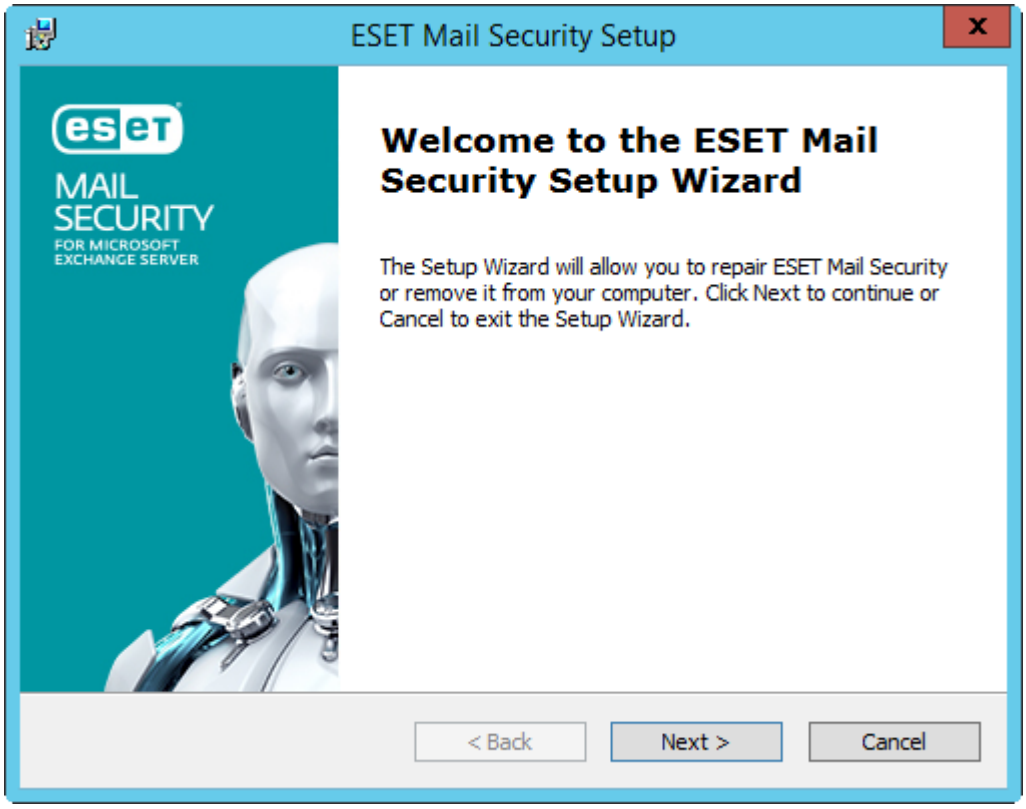
Konfigurácia ochrany servera
Svoj produkt ESET Mail Security si môžete prispôsobiť podľa potreby úpravou pokročilých nastavení každej funkcie.

Inštalácia ESET Mail Security

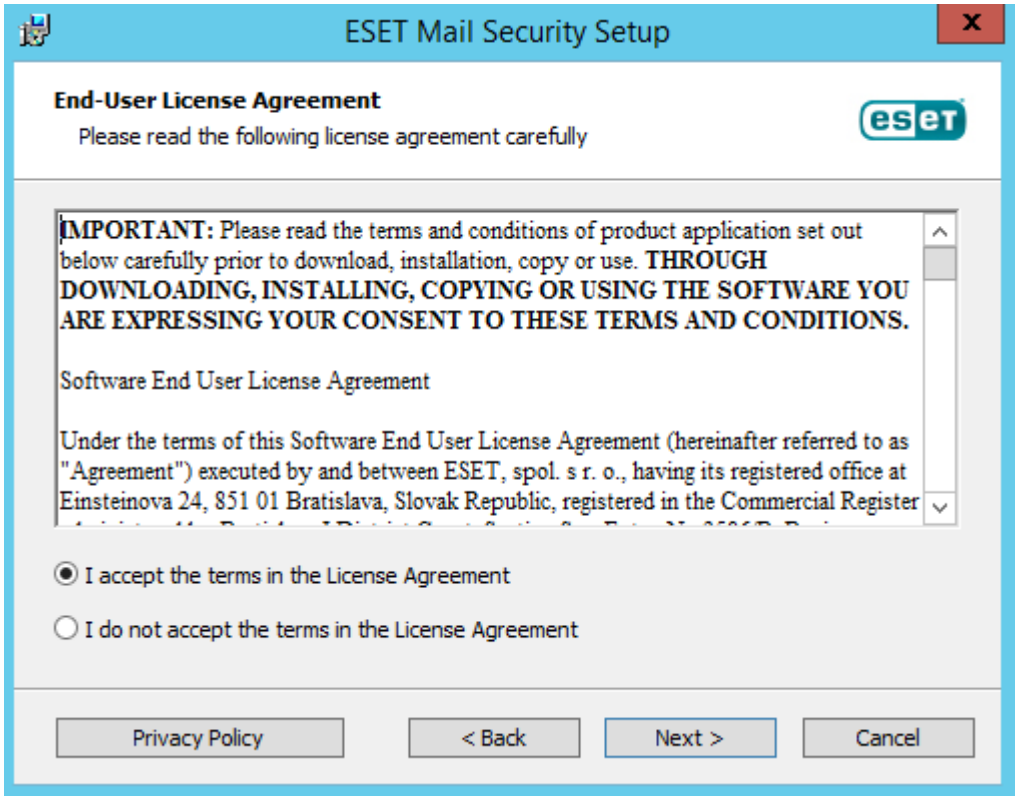
Ide o typického sprievodcu inštaláciou prostredníctvom grafického požívateľského rozhrania. Dvakrát kliknite na inštalačný balík .msi a postupujte podľa nasledujúcich krokov pre inštaláciu ESET Mail Security:

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

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



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

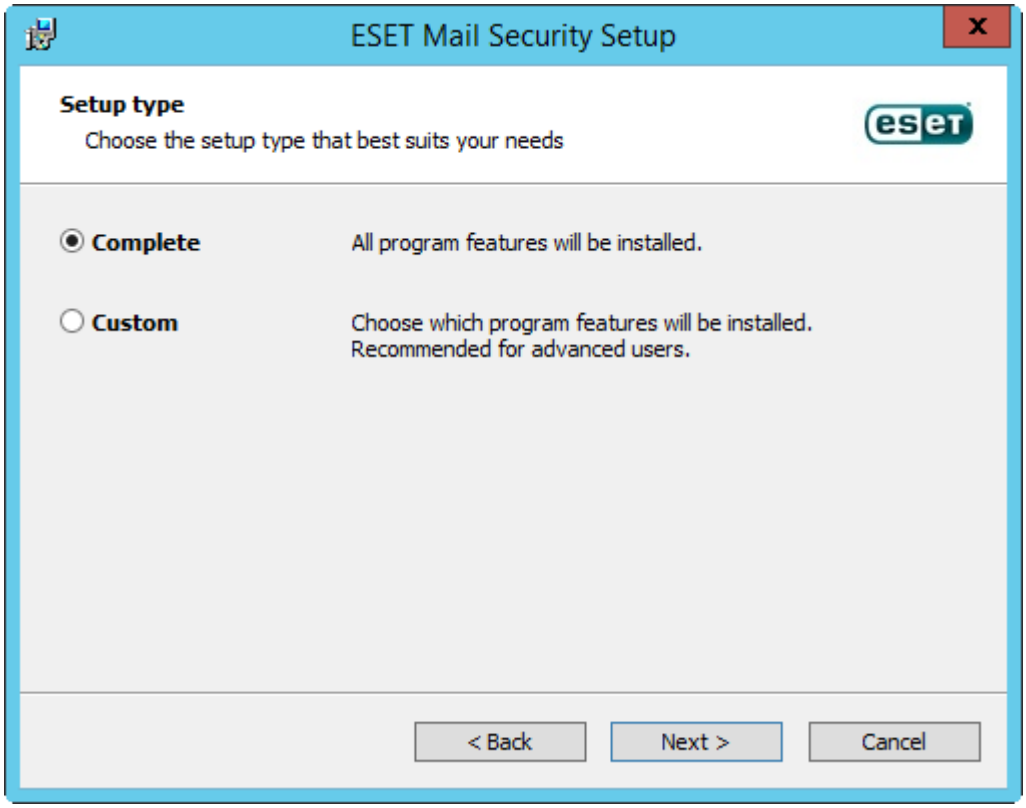


4. Vyberte si jeden z dostupných typov inštalácie (dostupnosť závisí od vášho operačného systému).

Úplná

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

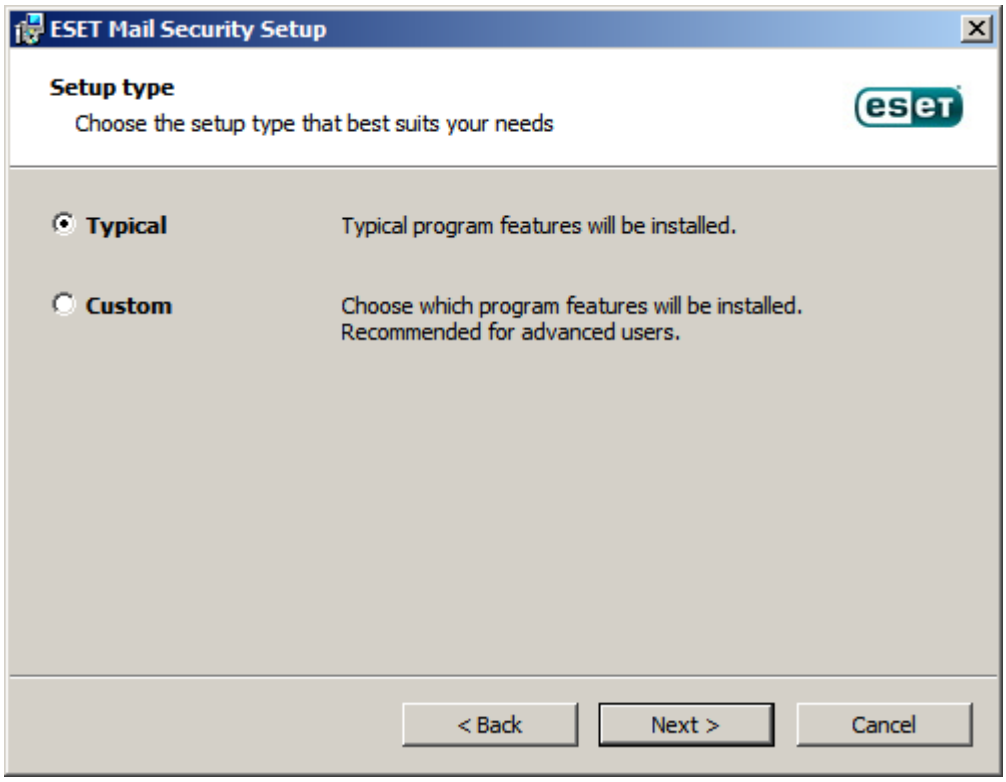
V prípade, že plánujete použiť Lokálnu karanténu pre e□mailové správy a nechcete mať súbory správ umiestnených v karanténe uložené na vašom disku C:, zmeňte cestu **Priečinka s dátami** na váš preferovaný disk a umiestnenie. Avšak, majte na pamäti, že všetky dátové súbory ESET Mail Security budú uložené v tomto umiestnení.



Typická

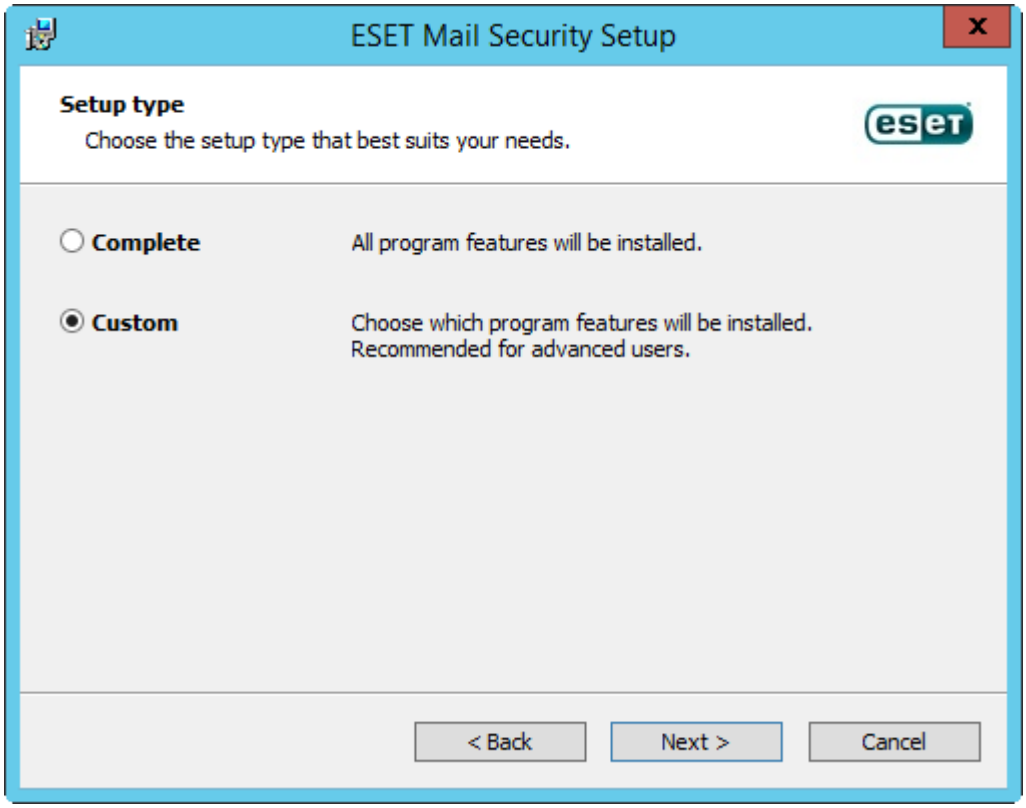
Nainštaluje odporúčané funkcie produktu ESET Mail Security. Táto inštalácia je dostupná pre Windows Server 2008 R2 SP1 a Windows Small Business Server 2011 SP1.

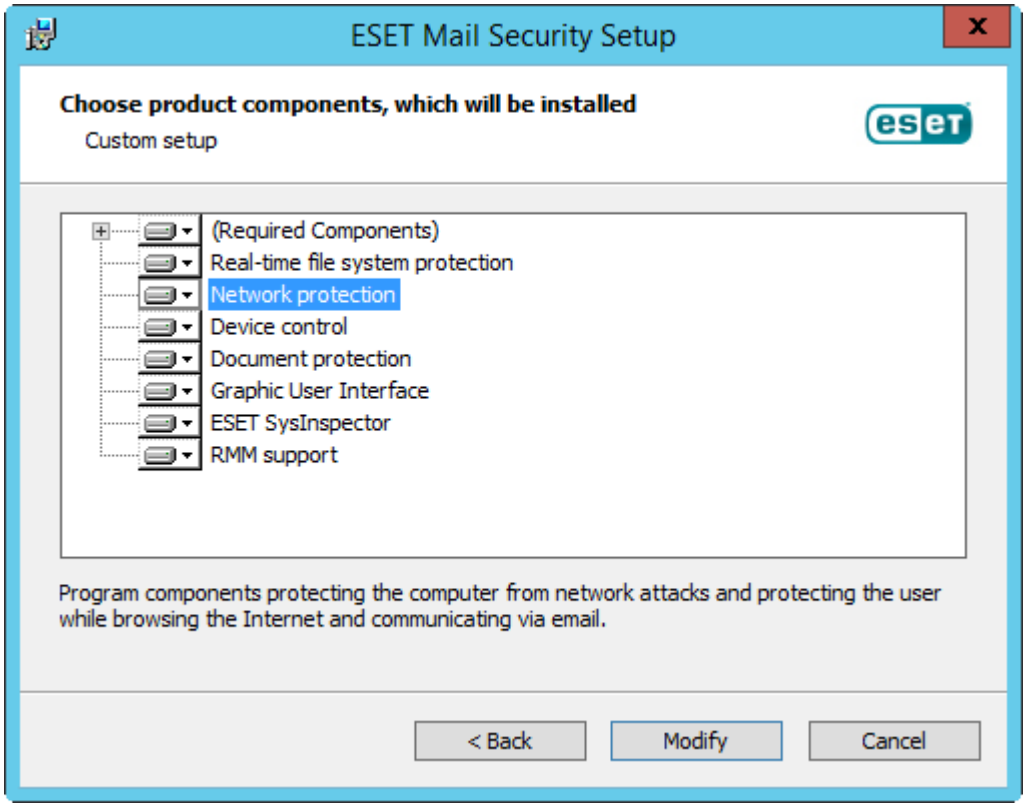
Na operačnom systéme Windows Server 2008 R2 SP1 je inštalácia komponentu **Ochrana siete** štandardne zakázaná (**Typická** inštalácia). Ak chcete mať tento komponent nainštalovaný, zvoľte **Vlastný** typ inštalácie.



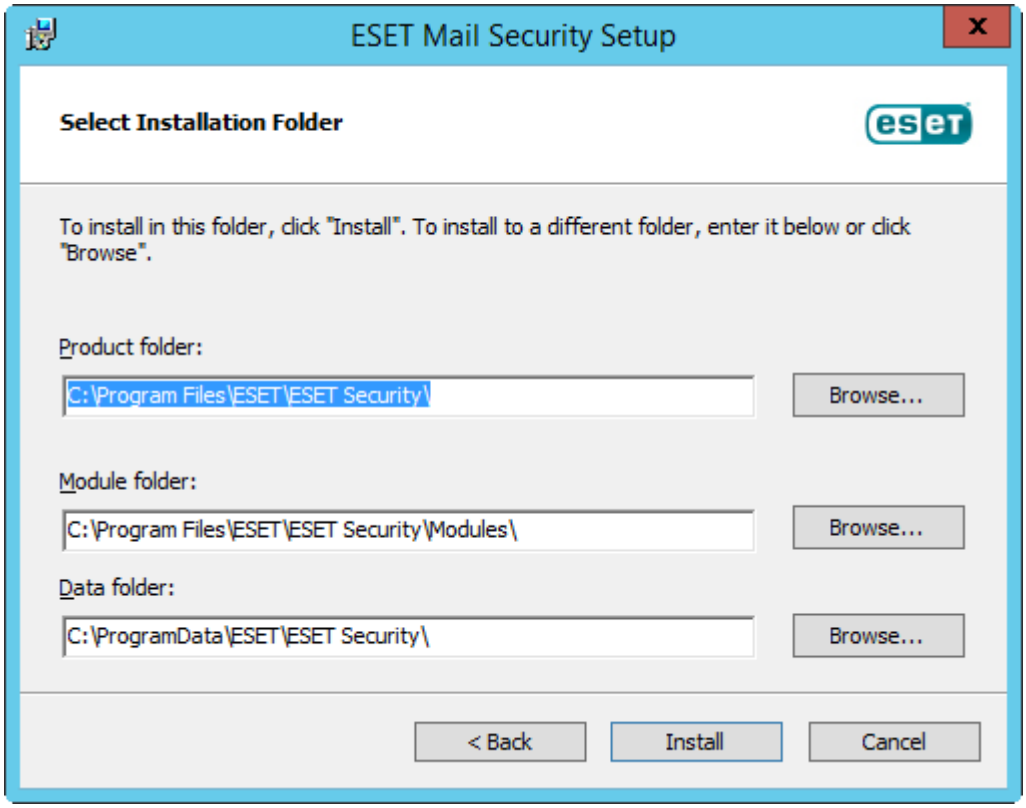
Vlastná

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





5. Zobrazí sa vám výzva na nastavenie cesty k adresáru, kam bude ESET Mail Security nainštalovaný. Štandardne sa program inštaluje do adresára *C:\Program Files\ESET\ESET Mail Security*. Ak chcete umiestnenie zmeniť (neodporúča sa), kliknite na možnosť **Prehľadávať**.

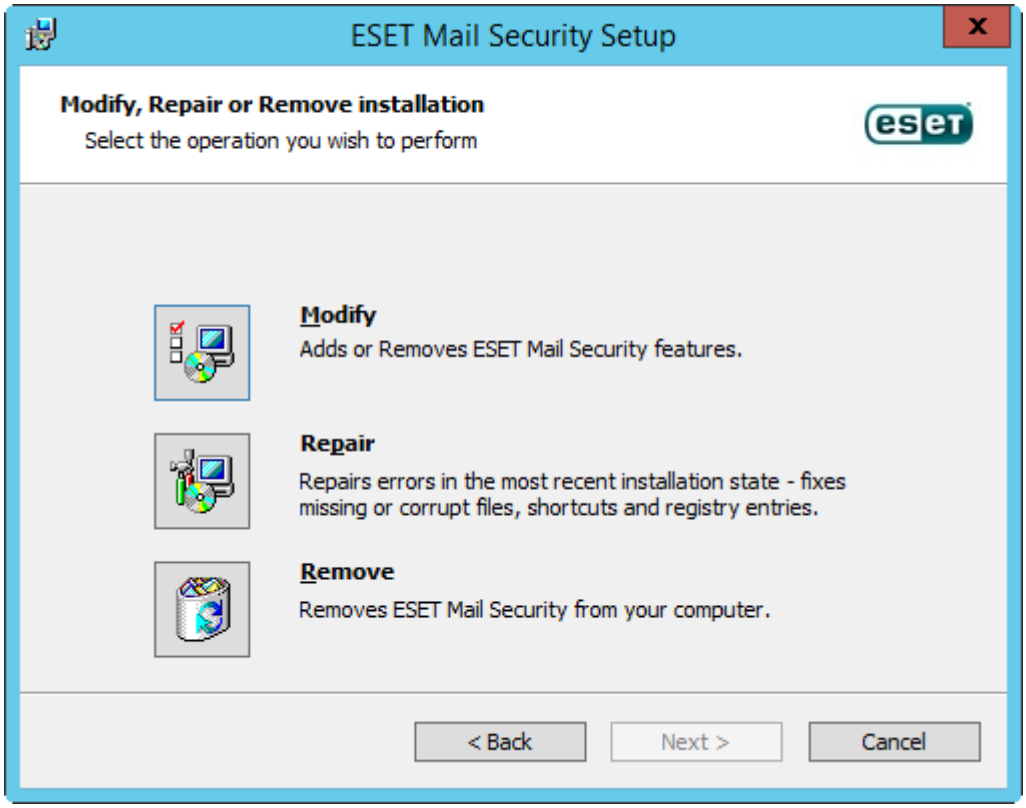


6. Kliknite na tlačidlo **Inštalovať** pre spustenie inštalačného procesu. Po dokončení inštalácie sa zobrazí hlavné okno programu ESET a v oblasti oznámení systému Windows sa zobrazí ikona.

Export nastavení alebo odstránenie inštalácie

Nastavenia môžete exportovať a uložiť alebo môžete inštaláciu úplne odstrániť. Stačí znova spustiť inštalačný balík s koncovkou `.msi`, pomocou ktorého ste program nainštalovali, alebo cez Ovládací panel v systéme Windows otvorte **Programy a súčasti**, v tomto okne kliknite pravým tlačidlom na ESET Mail Security a vyberte možnosť **Zmeniť**.

Môžete **exportovať** nastavenia programu ESET Mail Security alebo ESET Mail Security úplne **odstrániť** (odinštalovať).



Tichá inštalácia/inštalácia bez obsluhy

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

Na operačnom systéme Windows Server 2008 R2 SP1 nebude nainštalovaná funkcia **Ochrana siete**.

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

Úplná inštalácia na 64-bitovom systéme:
```
msiexec /i emsx_nt64.msi /qn /l*xv msi.log ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,SysInspector,SysRescue,Rmm,eula
```

Po dokončení inštalácie sa spustí grafické používateľské rozhranie ESET a v oblasti oznámení systému Windows sa zobrazí ikona.

Inštalácia produktu v konkrétnom jazyku (nemčina):
```
msiexec /i emsx_nt64.msi /qn ADDLOCAL=NetworkProtection,RealtimeProtection,^
DeviceControl,DocumentProtection,Cluster,GraphicUserInterface,^
SysInspector,SysRescue,Rmm,eula PRODUCT_LANG=1031 PRODUCT_LANG_CODE=de-de
```
Podrobnejšie informácie a zoznam jazykových kódov nájdete v sekcii Jazykové parametre v kapitole Inštalácia cez príkazový riadok.

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

Kompletné odstránenie (odinštalovanie) z 64-bitového systému:
`msiexec /x emsx_nt64.msi /qn /l*xv msi.log`

Po úspešnom odinštalovaní sa server automaticky reštartuje.

Inštalácia cez príkazový riadok

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

Podporované parametre:

APPDIR=<path>

- path – platná cesta k adresáru
- Adresár, do ktorého bude aplikácia nainštalovaná.
- Napríklad: `emsx_nt64.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>

- path – platná cesta k adresáru
- Adresár, do ktorého budú nainštalované dátové súbory aplikácie.

MODULEDIR=<path>

- path – platná cesta k adresáru
- Adresár, do ktorého budú nainštalované moduly aplikácie.

ADDLOCAL=<list>

- Inštalácia súčastí – zoznam voliteľných funkcií, ktoré budú nainštalované lokálne.
- Použitie s inštalačnými balíkmi ESET vo formáte .msi: `emsx_nt64.msi /qn ADDLOCAL=<list>`
- Viac informácií o parametri `ADDLOCAL` nájdete na webovej stránke https://docs.microsoft.com/en-gb/windows/desktop/Msi/addlocal.
- Zoznam `ADDLOCAL` je zoznam čiarkou oddelených funkcií, ktoré budú nainštalované.
- Pri výbere funkcie na inštaláciu musí byť v zozname uvedená úplná cesta (vrátane všetkých nadradených funkcií).

REMOVE=<list>

- Inštalácia súčastí – nadradená funkcia, ktorú nechcete mať nainštalovanú lokálne.
- Použitie s ESET inštalačnými balíkmi .msi: `emsx_nt64.msi /qn REMOVE=<list>`

- Viac informácií o parametri REMOVE nájdete na webovej stránke https://docs.microsoft.com/en-gb/windows/desktop/Msi/remove.

- Zoznam REMOVE je zoznam čiarkou oddelených nadradených funkcií, ktoré nebudú nainštalované (alebo budú odstránené v prípade existujúcej inštalácie).

- Stačí, ak uvediete iba nadradenú funkciu. Nie je potrebné zadávať do zoznamu každú podradenú funkciu.

ADDEXCLUDE=<list>

- Zoznam ADDEXCLUDE je zoznam čiarkou oddelených funkcií, ktoré nebudú nainštalované.

- Pri výbere funkcie, ktorá nemá byť nainštalovaná, musí byť v zozname zadaná jej úplná cesta (t. j. vrátane všetkých podfunkcií) a všetky súvisiace neviditeľné funkcie.

- Napríklad: emsx_nt64.msi /qn ADDEXCLUDE=<list>

ADDEXCLUDE nemôže byť používaný spolu s parametrom ADDLOCAL.

Prítomnosť funkcie:

- **Povinné** – táto funkcia bude nainštalovaná vždy.

- **Voliteľné** – výber tejto funkcie môžete zrušiť.

- **Neviditeľné** – funkcia je potrebná pre správne fungovanie inej funkcie.

Zoznam funkcií programu ESET Mail Security:

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

Názov funkcie	Prítomnosť funkcie
SERVER	Povinné
RealtimeProtection	Povinné
MAILSERVER	Povinné
WMIProvider	Povinné
HIPS	Povinné
Updater	Povinné
eShell	Povinné
UpdateMirror	Povinné
DeviceControl	Voliteľné
DocumentProtection	Voliteľné
WebAndEmail	Voliteľné
ProtocolFiltering	Neviditeľné
NetworkProtection	Voliteľné
IdsAndBotnetProtection	Voliteľné
Rmm	Voliteľné

Názov funkcie	Prítomnosť funkcie
WebAccessProtection	Voliteľné
EmailClientProtection	Voliteľné
MailPlugins	Neviditeľné
Cluster	Voliteľné
_Base	
eula	
ShellExt	Voliteľné
_FeaturesCore	
GraphicUserInterface	Voliteľné
SysInspector	Voliteľné
SysRescue	Voliteľné
EnterpriseInspector	Voliteľné

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

```
GraphicUserInterface,ShellExt
```

```
NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,ProtocolFiltering,MailPlugins,EmailClientProtection
```

Vylúčenie sekcie **NetworkProtection** vrátane podradených funkcií z inštalácie zadaním len nadradenej funkcie a použitím parametra `REMOVE`:
`msiexec /i emsx_nt64.msi /qn ADDLOCAL=ALL REMOVE=NetworkProtection`
Môžete prípadne použiť parameter `ADDEXCLUDE`, musíte však zadať aj všetky podradené funkcie:
`msiexec /i emsx_nt64.msi /qn ADDEXCLUDE=NetworkProtection,WebAccessProtection,IdsAndBotnetProtection,^ ProtocolFiltering,MailPlugins,EmailClientProtection`

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

Inštalácia ESET Mail Security s vypnutou technológiou ESET LiveGrid®:
`msiexec /i emsx_nt64.msi /qn /l*xv msi.log CFG_LIVEGRID_ENABLED=0`

Zoznam konfiguračných parametrov:

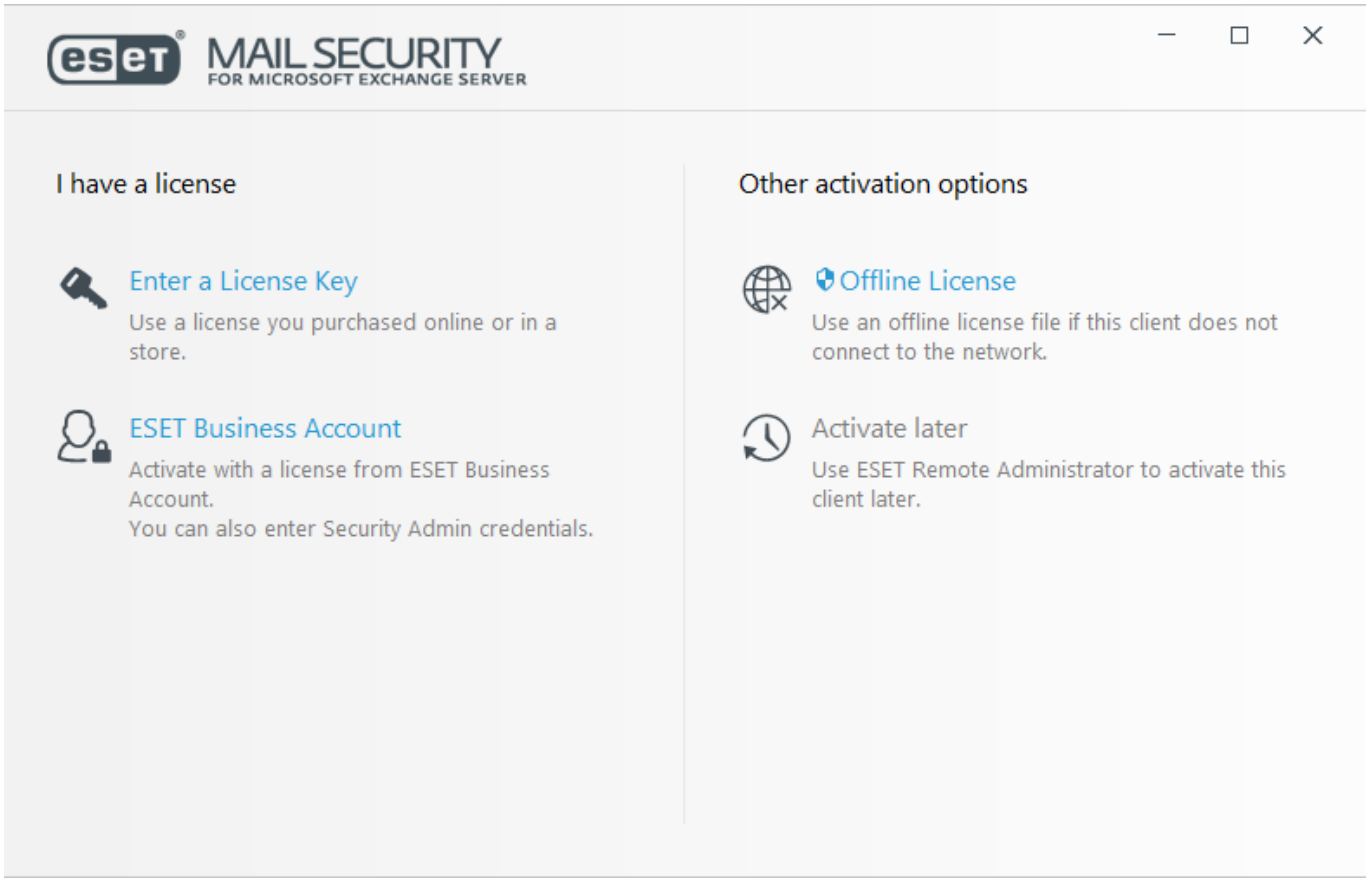
Prepínač	Hodnota
CFG_POTENTIALLYUNWANTED_ENABLED=1/0	0 – vypnuté, 1 – zapnuté
CFG_LIVEGRID_ENABLED=1/0	0 – vypnuté, 1 – zapnuté
FIRSTSCAN_ENABLE=1/0	0 – vypnuté, 1 – zapnuté
CFG_PROXY_ENABLED=0/1	0 – vypnuté, 1 – zapnuté
CFG_PROXY_ADDRESS=<ip>	IP adresa proxy.
CFG_PROXY_PORT=<port>	Číslo portu proxy.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

Jazykové parametre: Jazyk produktu (musíte zadať oba parametre)

Prepínač	Hodnota
PRODUCT_LANG=	Identifikátor LCID uvedený v desiatkovej sústave (identifikátor miestnych nastavení – Locale ID), napríklad 1033 pre English - United States. Pozrite si zoznam jazykových kódov.
PRODUCT_LANG_CODE=	Reťazec LCID (Language Culture Name) uvedený malými písmenami, napríklad en-us pre English - United States. Pozrite si zoznam jazykových kódov.

Aktivácia produktu

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



ESET Mail Security môžete aktivovať nasledujúcimi spôsobmi:

Použiť zakúpený licenčný kľúč

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

ESET Business Account

Túto možnosť použite v prípade, že ste sa zaregistrovali a máte účet ESET Business Account, do ktorého bola importovaná vaša licencia ESET Mail Security. Zadať môžete aj prihlasovacie údaje bezpečnostného správcu, ktoré používate v rámci portálu ESET License Administrator.

Offline licenčný súbor

Automaticky vygenerovaný offline licenčný súbor s informáciami o vašej licencii. Offline licenčný súbor je

generovaný pomocou licenčného portálu spoločnosti ESET a používa sa v sieťach, odkiaľ sa aplikácia nemôže pripojiť na licenčné servery.

Kliknite na možnosť **Aktivovať neskôr** pomocou nástroja ESET PROTECT, ak sa váš počítač nachádza v spravovanej sieti a váš správca vykoná vzdialenú aktiváciu prostredníctvom nástroja ESET PROTECT. Túto možnosť môžete tiež použiť v prípade, že daného klienta chcete aktivovať neskôr.

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

Po úspešnej aktivácii ESET Mail Security sa otvorí hlavné okno programu s aktuálnym stavom ochrany zobrazeným v okne Monitorovanie. Je možné, že bude potrebné nakonfigurovať počiatočné nastavenia, napríklad pre ESET LiveGrid®.

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

Pre aktiváciu produktu ESET Mail Security priamo z programu kliknite na ikonu v oblasti oznámení systému Windows a vyberte možnosť **Produkt nie je aktivovaný**. Prípadne v hlavnom okne programu kliknite na **Pomocník a podpora** > **Aktivovať produkt** alebo **Monitorovanie** > **Produkt nie je aktivovaný**.

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

ESET Business Account

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

Viac informácií nájdete v Online pomocníkovi pre ESET Business Account (EBA).

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

Úspešná aktivácia

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

Chyba aktivácie

Aktivácia ESET Mail Security nebola úspešná. Uistite sa, že ste zadali správny **Licenčný kľúč** alebo vložili správnu **Offline licenciu**. Ak máte rozdielnu **Offline licenciu**, skúste ju zadať znova. Pre skontrolovanie zadaného

licenčného kľúča kliknite na **Skontrolovať licenčný kľúč**, prípadne **zadajte inú licenciu**.

Ak sa vám produkt nedarí aktivovať, využite sprievodcu riešením problémov pri aktivácii.

Licencia

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

Aktualizácia na novú verziu

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

Metódy aktualizácie:

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

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

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

Počas aktualizácie ESET Mail Security bude vyžadovaný reštart servera.

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

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

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

Nasledujúce nastavenia sú zachované z predošlých verzií produktu ESET Mail Security:

- Všeobecné nastavenia ESET Mail Security.

Nastavenia Antispamovej ochrany:

- Všetky nastavenia, ktoré sú identické s predchádzajúcimi verziami. Pre všetky nové nastavenia budú použité štandardné hodnoty.

- Položky whitelistov a blacklistov.

Po aktualizácii produktu ESET Mail Security odporúčame prejsť si všetky nastavenia a uistiť sa, že program je nakonfigurovaný správne a podľa vašich požiadaviek.

Aktualizácia pomocou nástroja ESET PROTECT

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

Samotná procedúra pozostáva z nasledujúcich fáz:

- Najprv manuálne aktualizujte prvý server nainštalovaním najnovšej verzie produktu ESET Mail Security cez existujúcu inštaláciu, aby bola zachovaná celková konfigurácia vrátane pravidiel, whitelistov, blacklistov atď. Táto fáza sa vykonáva lokálne na serveri, na ktorom je spustený produkt ESET Mail Security.

- V nástroji ESET Mail Security požiadajte o konfiguráciu novej verzie ESET PROTECT a konvertujte ju na politiku. Politika bude neskôr aplikovaná na všetky aktualizované servery. Táto fáza, ako aj ďalšie fázy, sa vykonávajú vzdialene prostredníctvom nástroja ESET PROTECT.

- Spustite úlohu Odinštalovanie softvéru na všetkých serveroch so staršou verziou ESET Mail Security.

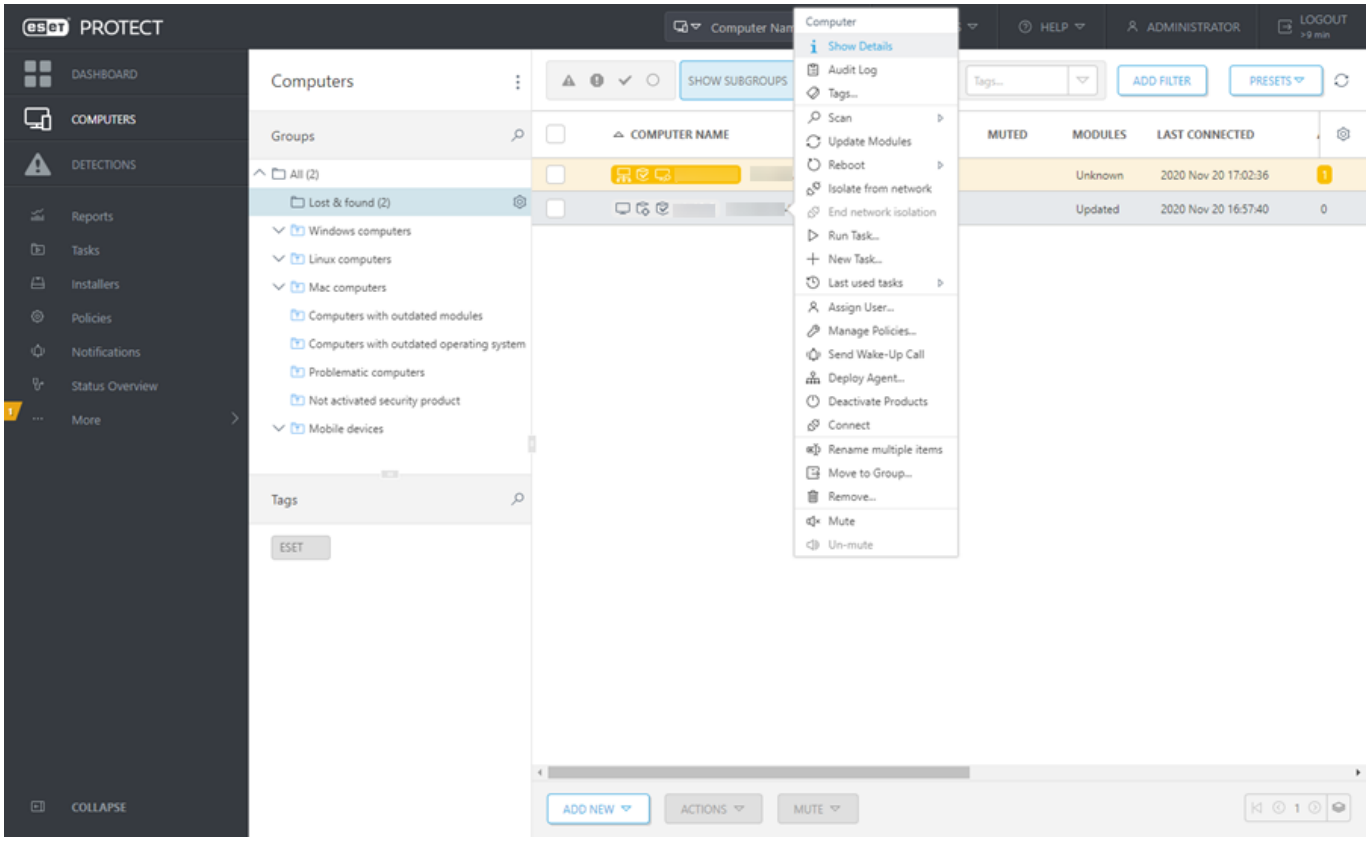
- Spustite úlohu Inštalácia softvéru na všetkých serveroch, na ktorých chcete pracovať s najnovšou verziou produktu ESET Mail Security.

- Priraďte konfiguračnú politiku k všetkých serverom s najnovšou verziou produktu ESET Mail Security.

Postup krok za krokom:

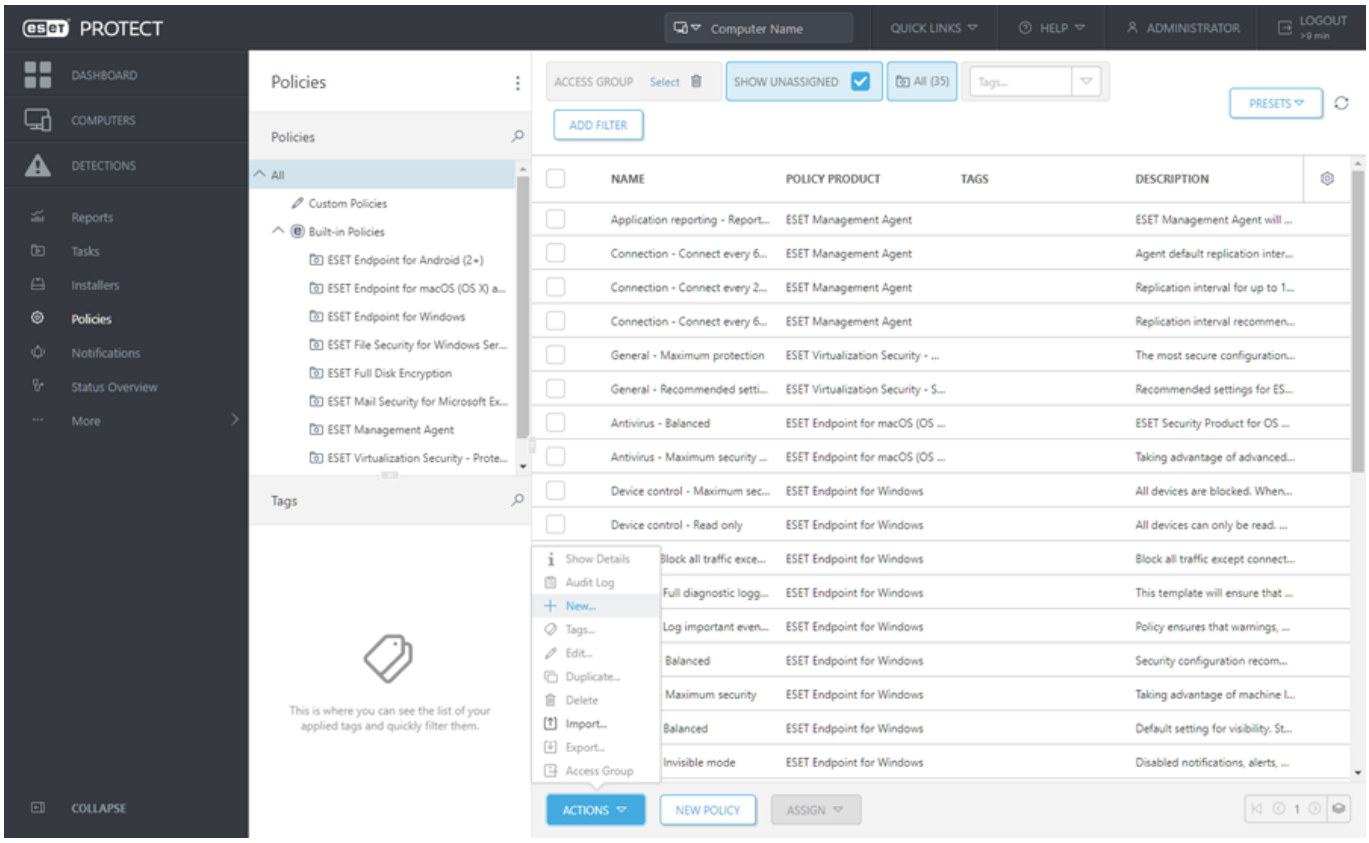
1. Prihláste sa na jeden zo serverov, na ktorých sa nachádza ESET Mail Security, a aktualizujte ho stiahnutím a inštaláciou najnovšej verzie na vašu existujúcu verziu. Postupujte podľa krokov pre štandardnú inštaláciu. Počas inštalácie bude zachovaná celá pôvodná konfigurácia vašej staršej verzie produktu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

2. Otvorte ESET PROTECT Web Console, vyberte klientsky počítač zo statickej alebo dynamickej skupiny a kliknite na možnosť **Zobraziť podrobnosti**.



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

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



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

6. Uistite sa, že produkt ESET Mail Security bol odinštalovaný zo všetkých cieľových počítačov.

7. Vytvorte úlohu Inštalácia softvéru na inštaláciu najnovšej verzie ESET Mail Security na všetky požadované ciele.

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

Aktualizácia prostredníctvom klastra ESET

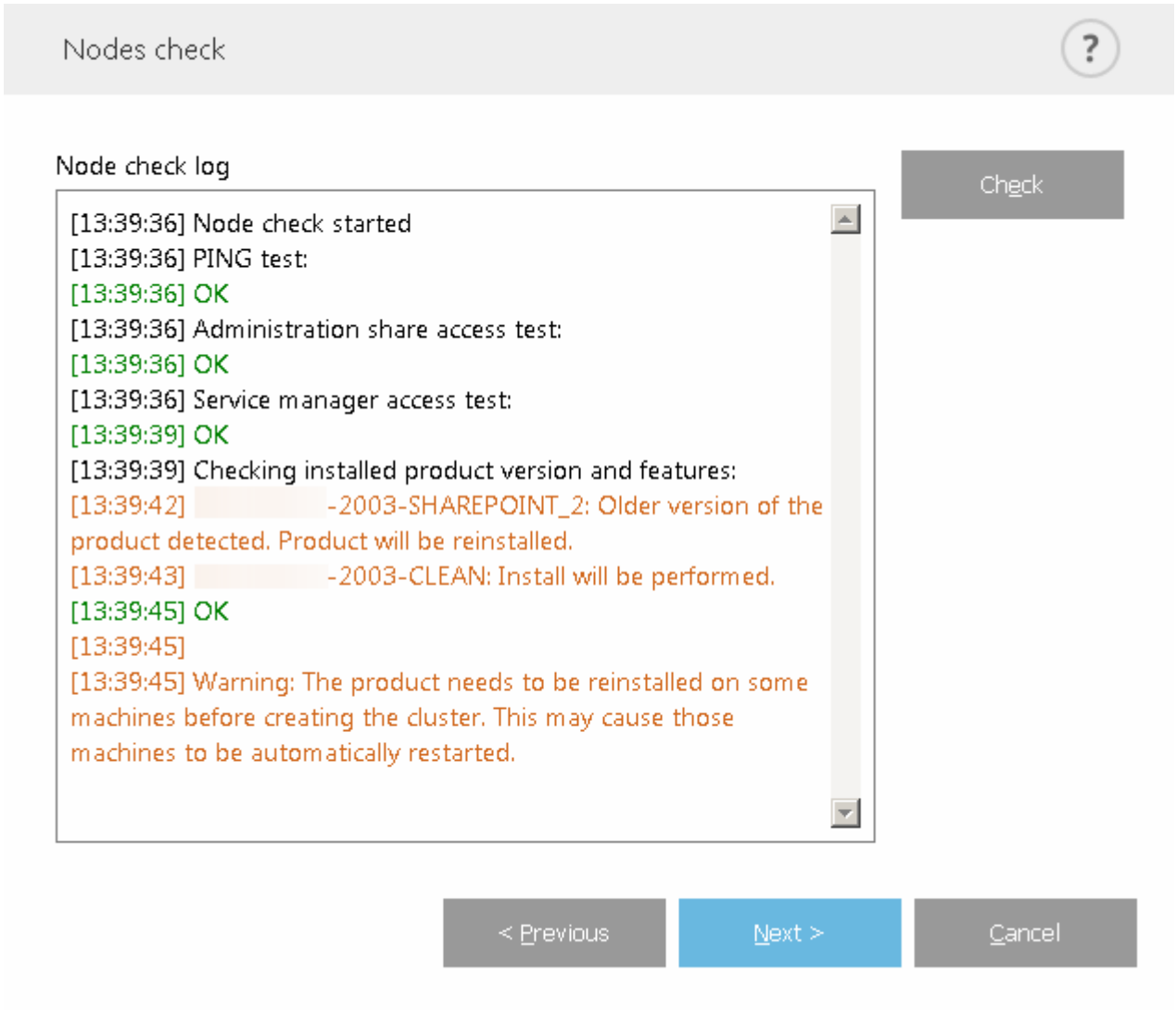
Vytvorenie klastra ESET vám umožňuje aktualizovať viacero serverov, ktoré používajú staršie verzie produktu ESET Mail Security. Metódu aktualizácie pomocou klastra ESET odporúčame použiť v prípade, ak máte vo vašom prostredí 2 alebo viac serverov s nainštalovaným produktom ESET Mail Security. Ďalšou z výhod tejto metódy aktualizácie je, že môžete pokračovať v používaní klastra ESET, aby mal produkt ESET Mail Security synchronizovanú konfiguráciu na všetkých uzloch.

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

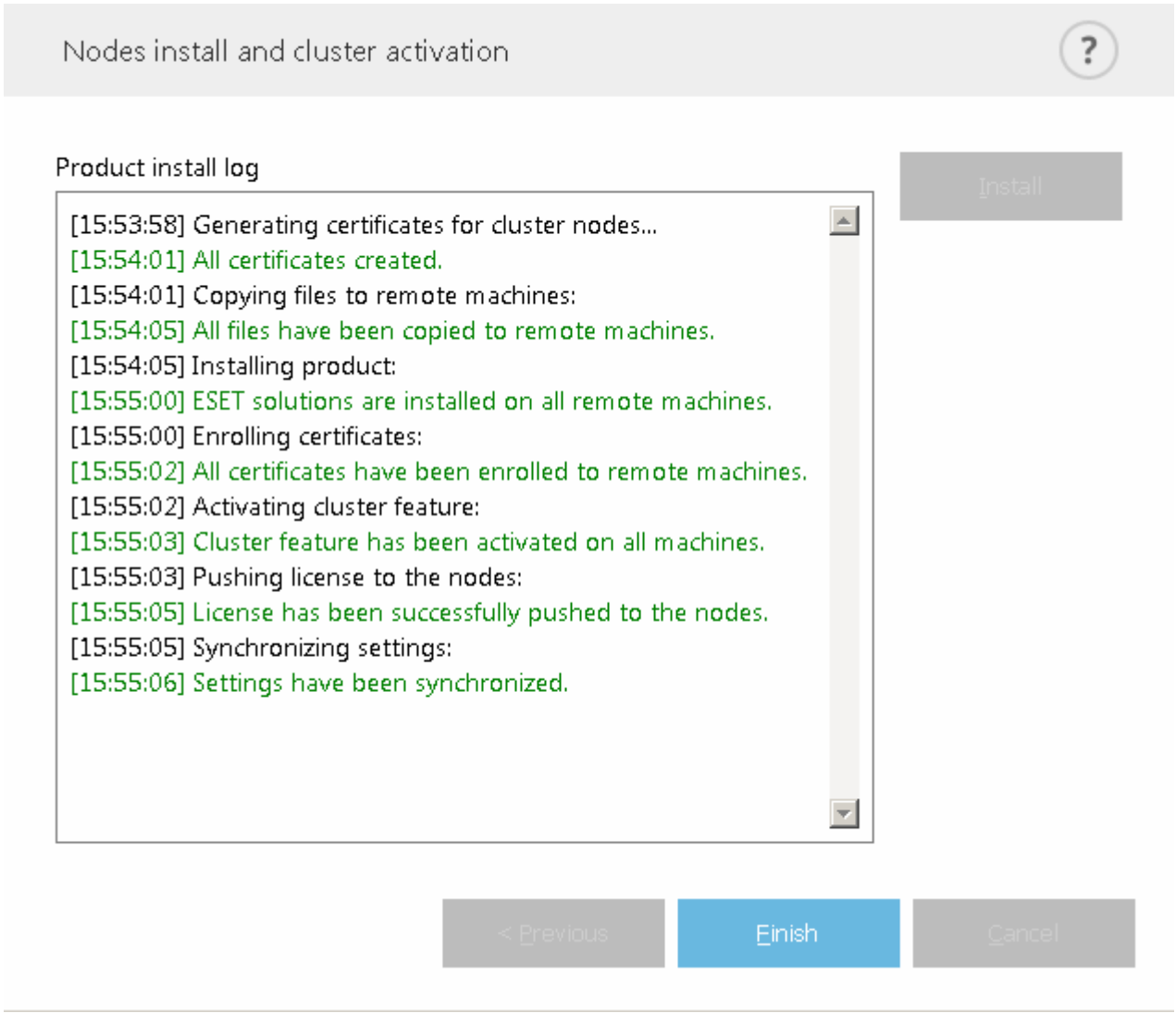
1. Prihláste sa na jeden zo serverov, na ktorých sa nachádza ESET Mail Security, a aktualizujte ho stiahnutím a inštaláciou najnovšej verzie na vašu existujúcu verziu. Postupujte podľa krokov pre štandardnú inštaláciu. Počas inštalácie bude zachovaná celá pôvodná konfigurácia vašej staršej verzie produktu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

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

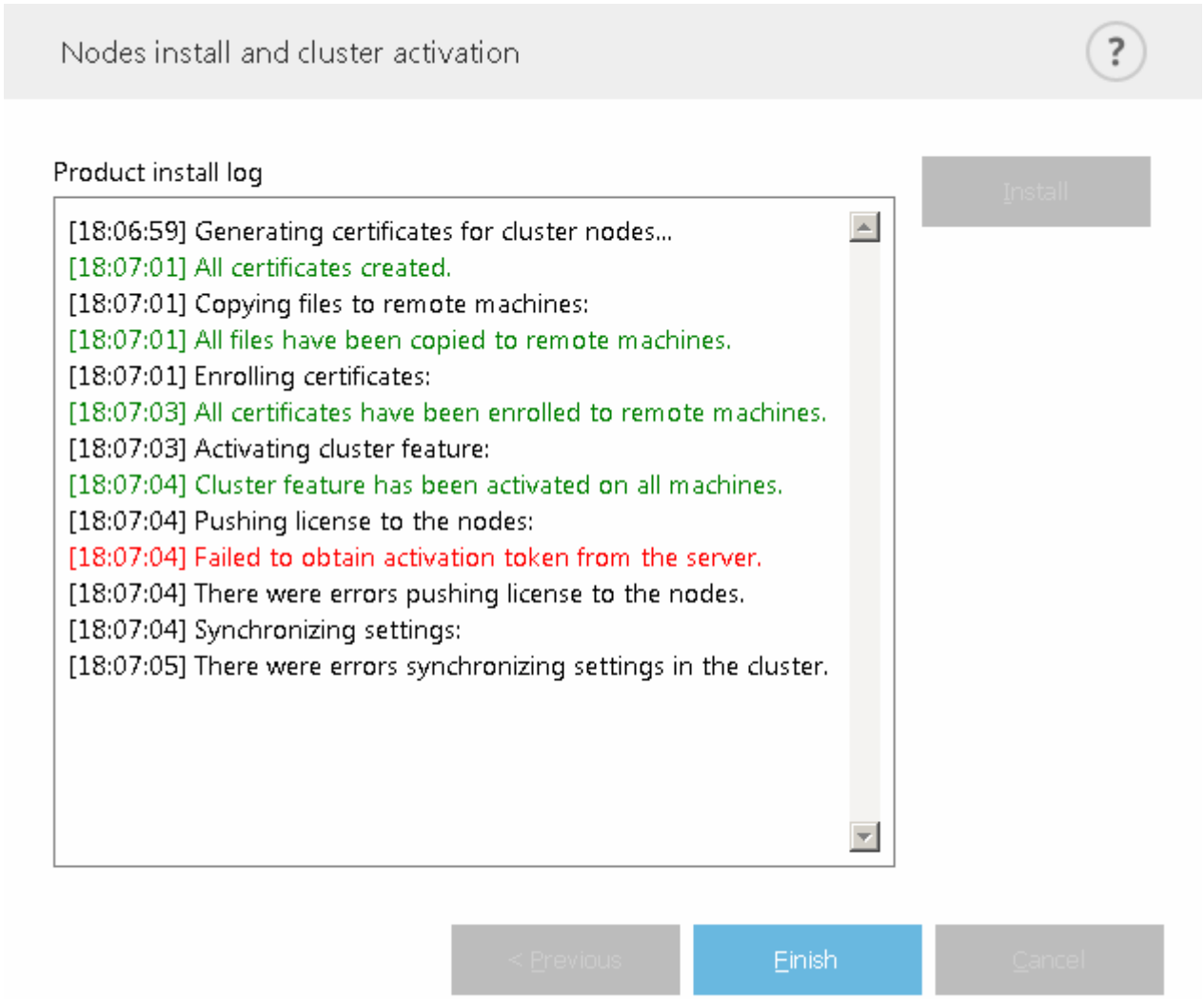
3. Skontrolujte Protokol kontroly uzlov. V danom protokole budú zobrazené severy so staršími verziami produktu a na ktorých bude produkt preinštalovaný. ESET Mail Security bude taktiež nainštalovaný na všetky pridané servery, kde nainštalovaný nie je.



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



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



Inštalácia v klastrovom prostredí

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

Terminálový server

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

Multiserverové/DAG prostredie

ESET Mail Security podporuje multiserverové prostredia. Ak vašu infraštruktúru tvorí viacero serverov, napr. Database availablity group (DAG), ESET Mail Security môžete nainštalovať na každý Exchange Server v role Mailbox.

Najjednoduchším spôsobom inštalácie ESET Mail Security na servery je použitie klastra ESET. Takisto vám odporúčame zapnúť možnosť Použiť klaster ESET pre uloženie všetkých správ v karanténe na jednom uzle v nastaveniach E-mailovej karantény. Ak plánujete používať greylisting, povoľte možnosť Synchronizovať databázy greylistingu naprieč klastrom ESET.

Ako začať

Nasledujúca časť by vám mala pomôcť začať s používaním programu ESET Mail Security.

Úlohy po inštalácii

V tejto kapitole nájdete zoznam úloh vykonávaných po inštalácií programu, ktoré vám môžu pomôcť s jeho počiatočnou konfiguráciou.

Monitorovanie

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

Spravovanie pomocou nástroja ESET PROTECT

Na vzdialenú správu programu ESET PROTECT môžete použiť nástroj ESET Mail Security.

Úlohy po inštalácii

V tabuľke nižšie nájdete zoznam odporúčaných úloh, ktoré pokrývajú počiatočnú konfiguráciu vášho programu ESET Mail Security.

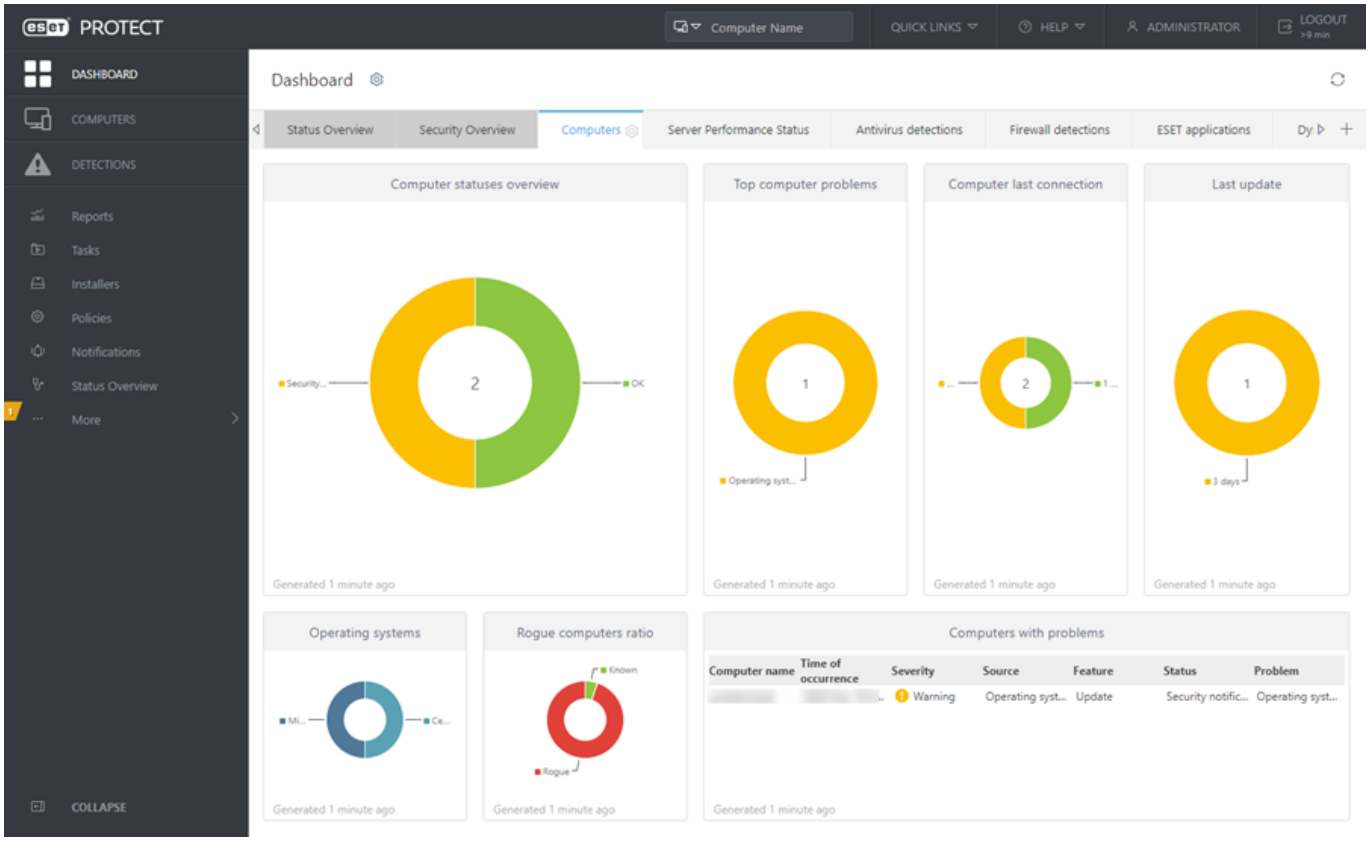
Téma	Popis
Aktivácia produktu	Uistite sa, že váš produkt ESET Mail Security je aktivovaný. Aktiváciu je možné vykonať viacerými spôsobmi.
Aktualizácia	Po aktivácii produktu je aktualizácia modulov spúšťaná automaticky. Ak si chcete overiť, či aktualizácia prebehla úspešne, pozrite si stav aktualizácie.
Správca e-mailovej karantény	Oboznámte sa so Správcom e-mailovej karantény, ktorý je dostupný z používateľského rozhrania programu. Táto funkcia vám umožňuje spravovať správy, ktoré boli presunuté do karantény, ako napr. spam, infikované prílohy obsahujúce malvér, phishingové správy a správy odfiltrované pomocou pravidiel. Môžete zobraziť podrobnosti o každej správe a vykonať pre danú správu príslušnú akciu (uvoľniť alebo vymazať).
Webové rozhranie e-mailovej karantény	Webové rozhranie e-mailovej karantény je používateľské rozhranie, ktoré je alternatívou k Správcovi e-mailovej karantény, umožňujúce vzdialené spravovanie položiek umiestnených v karanténe. Webové rozhranie e-mailovej karantény navyše umožňuje používateľom (príjemcom e-mailových správ) spravovať svoje vlastné správy, ktoré boli presunuté do karantény. Používatelia môžu byť informovaní o novom obsahu v karanténe pomocou reportov o e-mailovej karanténe odosielaných prostredníctvom e-mailu. Odporúčame, aby ste nastavili reporty.

Téma	Popis
Reporty o e-mailovej karanténe	Môžete vytvoriť naplánovanú úlohu, pomocou ktorej budú odosielané reporty o e-mailovej karanténe vám a vybraným používateľom, vďaka čomu budú môcť uvoľňovať (doručovať) určité typy nesprávne detegovaných správ a tiež spravovať svoj obsah umiestnený v karanténe prostredníctvom webového rozhrania e-mailovej karantény (online zobrazovač). Používatelia budú môcť vstupovať do webového rozhrania kliknutím na odkaz, ktorý sa nachádza v reportoch o e-mailovej karanténe, a následne sa doň prihlasovať pomocou svojich doménových prihlasovacích údajov.
Antispam – Filtrovanie a overenie	Antispam je sofistikovaná funkcia založená na cloude, ktorá zabraňuje doručovaniu spamu vašim používateľom (príjemcom e-mailových správ). Odporúčame používať filtrovanie a overovanie a pridať svoju lokálnu IP adresu do zoznamu ignorovaných IP adries. Tým pádom budú IP adresy vo vašej sieti počas klasifikácie ignorované. Nastavením a spravovaním ostatných zoznamov povolených, blokovaných a ignorovaných IP adries si môžete prispôsobiť filtrovanie a overovanie. Môžete tiež zapnúť Greylisting, ak sa rozhodnete používať túto funkciu.
Pravidlá	Ide o efektívnu funkciu, ktorá umožňuje filtrovať e-mailové správy podľa definovaných podmienok a akcií. Môžete použiť buď preddefinované pravidlá (ktoré môžete v prípade potreby dodatočne upraviť), alebo vytvoriť nové, vlastné pravidlá, ktoré budú vyhovovať vašim požiadavkám. Pravidlá môžu byť nastavené pre ktorúkoľvek vrstvu ochrany (Ochrana prenosu e-mailov, Ochrana databáz e-mailových schránok alebo Manuálna kontrola databáz e-mailových schránok).
Test antivírusu	Overte, či antivírusová ochrana funguje správne.
Test antispamu	Overte, či antispamová ochrana funguje správne.
Antiphishingový test	Overte, či Antiphishingová ochrana funguje správne.

Spravovanie pomocou nástroja ESET PROTECT

ESET PROTECT je nástroj, ktorý vám umožňuje spravovať produkty spoločnosti ESET v sieťovom prostredí z jednej centrálnej lokality. Systém správy úloh v nástroji ESET PROTECT umožňuje inštalovať bezpečnostné riešenia ESET na vzdialené počítače v sieti a okamžite reagovať na vzniknuté problémy a hrozby.

ESET PROTECT neposkytuje ochranu pred škodlivým kódom, keďže tú zaisťujú bezpečnostné riešenia ESET nainštalované na pripojených klientskych počítačoch. Bezpečnostné riešenia spoločnosti ESET podporujú siete, ktoré zahŕňajú rôzne typy platforiem. Vaša sieť môže obsahovať kombináciu aktuálnych operačných systémov Microsoft, Linux a Mac OS.



Viac informácií o nástroji ESET PROTECT nájdete v Online pomocníkovi pre ESET PROTECT.

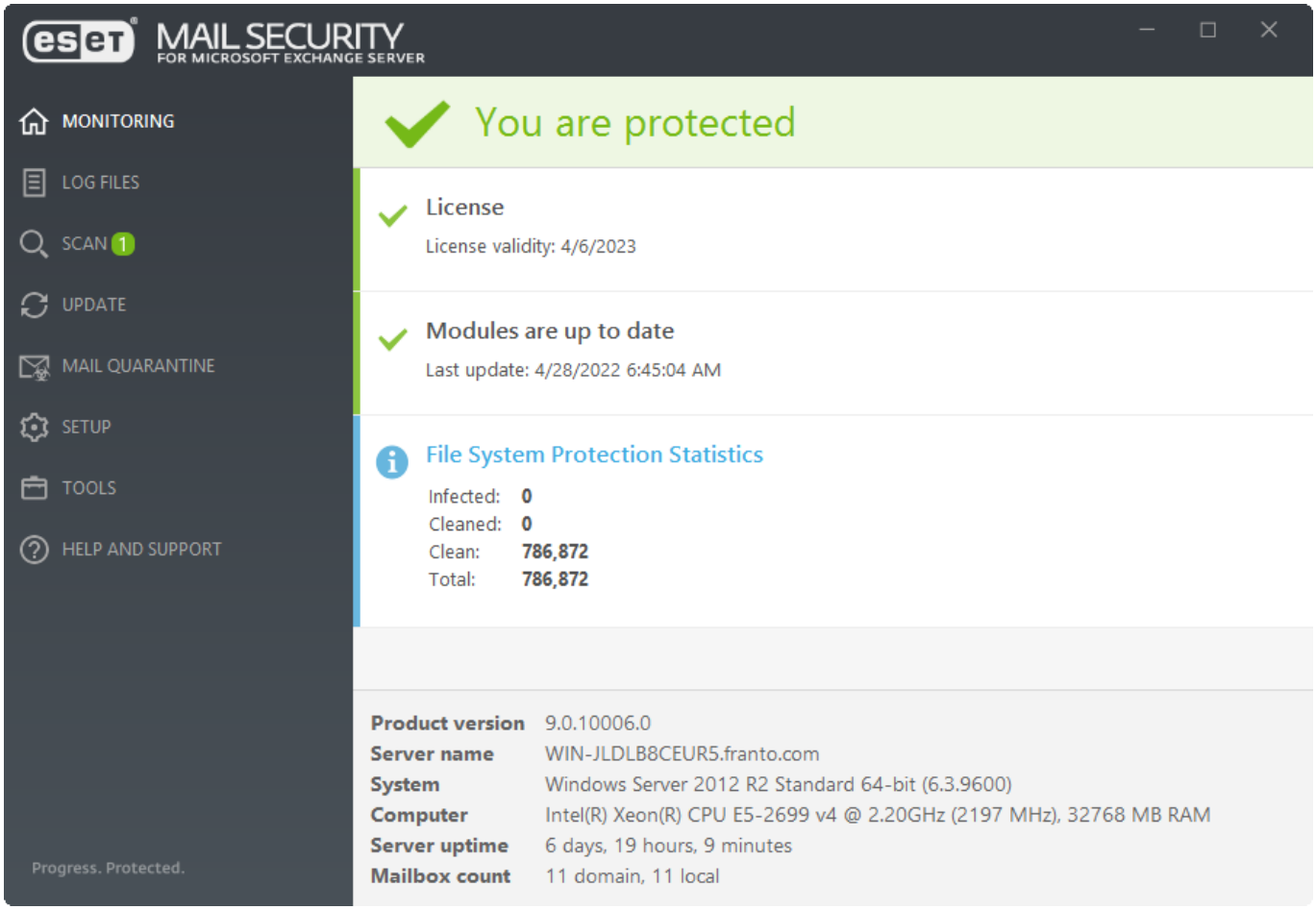
Monitorovanie

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

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

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

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



Moduly, ktoré pracujú správne, majú pridelené zelené symboly. Moduly, ktoré nie sú plne funkčné sa zobrazujú buď s červeným výkričníkom, alebo s oranžovou notifikáciou. Dodatočné informácie o module sú zobrazené vo vrchnej časti okna. Taktiež je zobrazené navrhované riešenie v prípade problému s modulom.

Stav jednotlivých modulov je možné zmeniť kliknutím na Nastavenia v hlavnom okne a označením požadovaného modulu.

Sekcia Monitorovanie tiež obsahuje informácie o vašom systéme:

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

Počet e-mailových schránok

ESET Mail Security deteguje počet e-mailových schránok a zobrazuje ho na základe detekcie:

- **Doména** – počet všetkých e-mailových schránok v konkrétnej doméne, do ktorej patrí Exchange Server.
- **Lokálna strana** – týka sa počtu e-mailových schránok Exchange Servera (ak nejaké existujú), kde je nainštalovaný produkt ESET Mail Security.

V prípade, že problém nie je možné vyriešiť pomocou navrhnutých riešení, prejdite do sekcie **Pomocník a podpora** alebo vyhľadajte informácie o danom probléme v Databáze znalostí spoločnosti ESET. Ak aj napriek tomu potrebujete pomoc, môžete kontaktovať technickú podporu spoločnosti ESET. Špecialisti technickej podpory spoločnosti ESET reagujú na otázky rýchlo a efektívne vám pomôžu s vyriešením vášho problému.

Stav ochrany

Súhrnné informácie o stave programu ESET Mail Security budú zobrazené v hlavnom okne spolu s podrobnými informáciami o vašom systéme.

Za normálnych okolností, keď všetko funguje správne, má stav ochrany zelenú farbu. Stav ochrany sa však za určitých podmienok môže zmeniť.

Ak dôjde k niektorej z udalostí spomenutých v tabuľke nižšie, stav ochrany zmení farbu na oranžovú alebo červenú a zobrazí sa príslušné upozornenie.

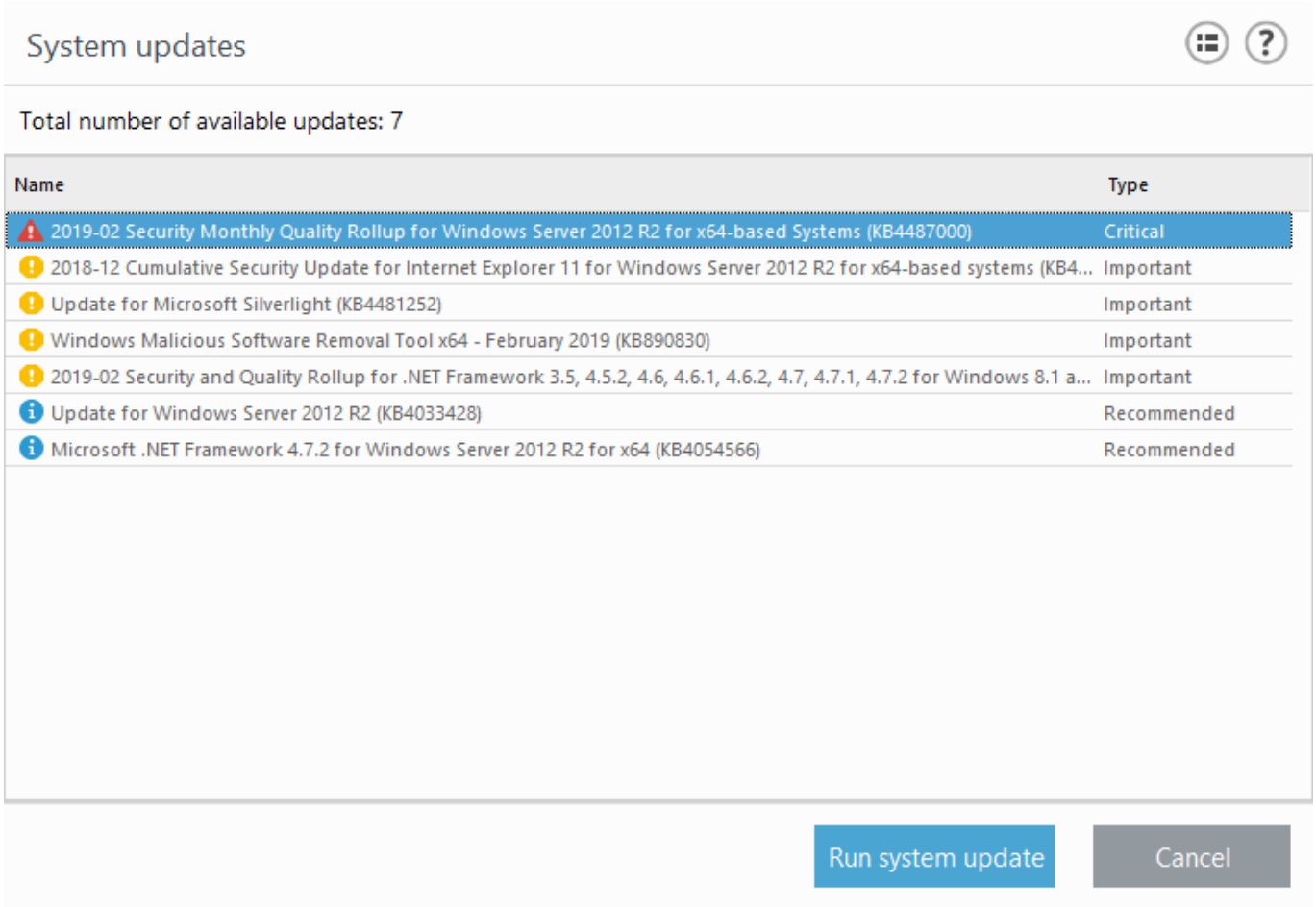
Upozornenie	Popis
Antivírusová ochrana e-mailových serverov je vypnutá	Kliknite na možnosť Zapnúť antivírusovú ochranu v sekcii Monitorovanie alebo opätovne povoľte Antivírusovú a antispyvérovú ochranu na karte Nastavenia v hlavnom okne programu.
Integrácia s e-mailovým serverom je vypnutá	Integrácia s e-mailovým serverom bola vypnutá používateľom. Ak chcete zapnúť Ochranu prenosu e-mailov, kliknite na Upraviť nastavenia integrácie.
Antispamové jadro má obmedzené pripojenie na cloud	Pravdepodobne ide o problémy s pripojením. Uistite sa, že sú povolené potrebné porty.
Detekcia potenciálne nechcených aplikácií nie je nakonfigurovaná	Potenciálne nechcená aplikácia (PUA) je program, ktorý obsahuje advér, inštaluje panely s nástrojmi alebo má iné nejasné úmysly. Vyskytujú sa situácie, keď sa používateľ rozhodne, že výhody, ktoré mu potenciálne nechcená aplikácia poskytuje, prevyšujú riziko spojené s jej používaním.
Produkt nie je aktivovaný alebo Platnosť licencie uplynula	V takomto prípade ikona stavu ochrany zmení farbu na červenú. Po uplynutí platnosti licencie nebude možné program aktualizovať. Pre obnovenie licencie postupujte podľa inštrukcií uvedených vo výstražnom okne.
ESET LiveGrid® je vypnutý	Toto upozornenie sa zobrazuje v prípade, ak je ESET LiveGrid® vypnutý v Rozšírených nastaveniach.
Rezidentná ochrana súborového systému je pozastavená	Kliknite na možnosť Zapnúť rezidentnú ochranu v sekcii Monitorovanie alebo opätovne povoľte Rezidentnú ochranu súborového systému na karte Nastavenia v hlavnom okne programu.
Operačný systém nie je aktualizovaný	Okno aktualizácií operačného systému zobrazuje zoznam dostupných aktualizácií pripravených na inštaláciu.
Vaše zariadenie čoskoro stratí ochranu	Kliknutím na Zobraziť možnosti riešenia zobrazíte podrobné informácie o tom, ako aktualizovať váš systém Microsoft Windows. Ak používate Microsoft Windows Server 2008 R2 SP1, uistite sa, že váš systém je kompatibilný s SHA-2. Nainštalujte potrebné aktualizácie podľa verzie svojho operačného systému.
Vyžaduje sa reštart zariadenia	Kliknite na Reštartovať zariadenie na okamžitý reštart, prípadne kliknite na Zatvoriť, ak chcete reštartovať počítač neskôr. Táto správa sa môže zobraziť po nainštalovaní aktualizácie programových súčastí (PCU), prípadne mikroaktualizácie programových súčastí (µPCU). Viac informácií o PCU a µPCU nájdete v kapitole Nastavenia aktualizácie.
Ochrana pred sieťovými útokmi (IDS) je pozastavená	Kliknite na Zapnúť ochranu pred sieťovými útokmi (IDS) pre opätovné zapnutie tejto funkcie.

Upozornenie	Popis
Ochrana pred botnetmi je pozastavená	Kliknite na Zapnúť ochranu pred botnetmi pre opätovné zapnutie tejto funkcie.
Ochrana prístupu na web je pozastavená	Kliknite na možnosť Zapnúť ochranu prístupu na web v sekcii Monitorovanie alebo opätovne povoľte Ochranu prístupu na web na karte Nastavenia v hlavnom okne programu.
Antiphishingová ochrana je nefunkčná	Táto funkcia nefunguje, pretože požadované programové moduly nie sú aktívne.
Prepísanie politiky je aktívne	Konfigurácia stanovená politikou je dočasne prepísaná, pravdepodobne dovtedy, kým nebudú vyriešené prípadné problémy. Ak spravujete ESET Mail Security pomocou nástroja ESET PROTECT a máte k nemu priradenú politiku, odkaz na stav bude uzamknutý (sivý) v závislosti od toho, ktoré funkcie patria danej politike.

V prípade, že sa vám problém nedarí vyriešiť, vyhľadajte príslušné informácie v Databáze znalostí spoločnosti ESET. Ak aj napriek tomu potrebujete pomoc, môžete kontaktovať technickú podporu spoločnosti ESET. Špecialisti technickej podpory spoločnosti ESET reagujú na otázky rýchlo a efektívne vám pomôžu s vyriešením vášho problému.

K dispozícii sú aktualizácie Windows

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



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

Izolácia od siete

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

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

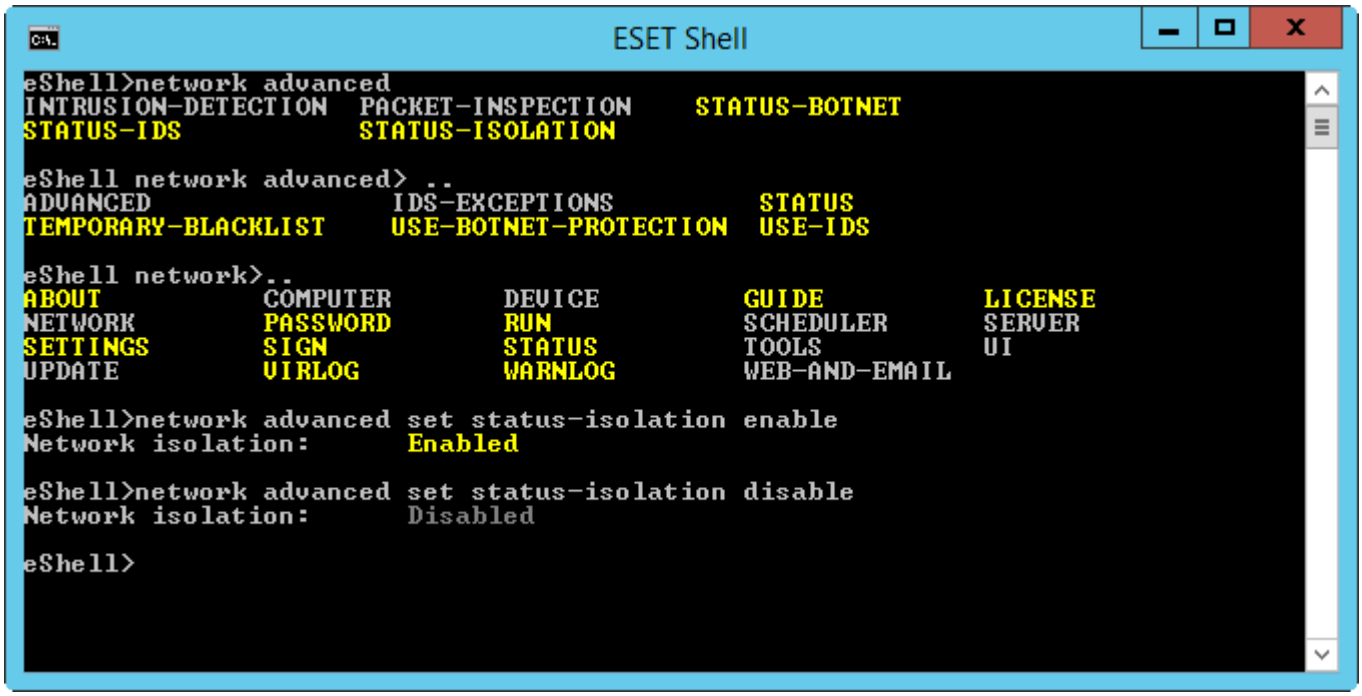
- Pripojenie k doménovému radiču.
- ESET Mail Security stále dokáže komunikovať.
- ESET Management Agent a ESET Inspect Connector môžu aj naďalej komunikovať cez sieť.

Aktivovať a deaktivovať izoláciu od siete môžete pomocou príkazu eShell alebo prostredníctvom klientskej úlohy v konzole ESET PROTECT.

eShell

V interaktívnom režime:

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



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

ESET PROTECT

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

Ak je aktivovaná izolácia od siete, stav programu ESET Mail Security sa zmení na červenú farbu a zobrazí sa oznámenie **Prístup na sieť bol zablokovaný**.

Používanie programu ESET Mail Security

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

Používateľské rozhranie umožňuje rýchly prístup k najčastejšie používaným funkciám produktu:

- Monitorovanie
- Protokoly
- Kontrola
- Aktualizácia
- E-mailová karanténa
- Nastavenia
- Nástroje

Kontrola

Manuálna kontrola je dôležitou súčasťou ESET Mail Security. Umožňuje kontrolu diskov, jednotlivých priečinkov a súborov na počítači. Na zaistenie zabezpečenia vašej siete je kľúčové, aby kontrola počítača bola spúšťaná nielen v prípade podozrenia výskytu infekcie, ale aj priebežne v rámci celkovej prevencie.

Hĺbkovú kontrolu odporúčame vykonávať v pravidelných časových intervaloch (napr. raz mesačne), aby sa detegovali prípadné vírusy, ktoré v čase zápisu na disk neboli zachytené pomocou Rezidentnej ochrany. Toto sa môže stať v prípade výskytu hrozby v čase, keď je rezidentná ochrana deaktivovaná, detekčné jadro nie je aktualizované alebo súbor nebol detegovaný, keď bol prvýkrát uložený na disk.

Vyberte si v rámci ESET Mail Security niektorú z dostupných manuálnych kontrol:

Kontrola databáz e-mailových schránok

Umožňuje spustiť manuálnu kontrolu databáz. Môžete zvoliť ciele kontroly – Verejné priečinky, E-mailové servery a E-mailové schránky. Na spustenie kontroly databáz v konkrétnom čase alebo pri špecifickej udalosti môžete použiť aj Plánovač.

> Ak používate Microsoft Exchange Server 2007, 2010, 2013 alebo 2016, môžete si vybrať medzi Ochranou databáz e-mailových schránok a Manuálnou kontrolou databáz, nie je však možné mať aktivované oba tieto typy ochrany súčasne. Ak sa rozhodnete pre manuálnu kontrolu databáz, integrácia ochrany databáz e-mailových musí byť vypnutá v Rozšírených nastaveniach v časti Server. V opačnom prípade nebude manuálna kontrola databáz dostupná.

Kontrola e-mailových schránok Office 365

Tento typ kontroly umožňuje kontrolovať vzdialené e-mailové schránky v hybridných prostrediach Office 365. Kontrola e-mailových schránok Office 365 funguje rovnako ako Manuálna kontrola databáz e-mailových schránok.

Kontrola úložiska

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

Skontrolovať váš počítač

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

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

Vlastná kontrola

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

Kontrola vymeniteľných médií

Funguje podobne ako Kontrola lokálnych diskov – spustí rýchlu kontrolu vymeniteľných médií pripojených do počítača (napr. CD, DVD a USB). Toto môže byť užitočné v prípade, ak pripojíte USB kľúč do počítača a želáte si skontrolovať jeho obsah na prítomnosť vírusov alebo iných potenciálnych hrozieb. Tento typ kontroly počítača je možné spustiť aj kliknutím na možnosť Vlastná kontrola > Ciele kontroly a následným kliknutím na Vymeniteľné médiá > Kontrolovať.

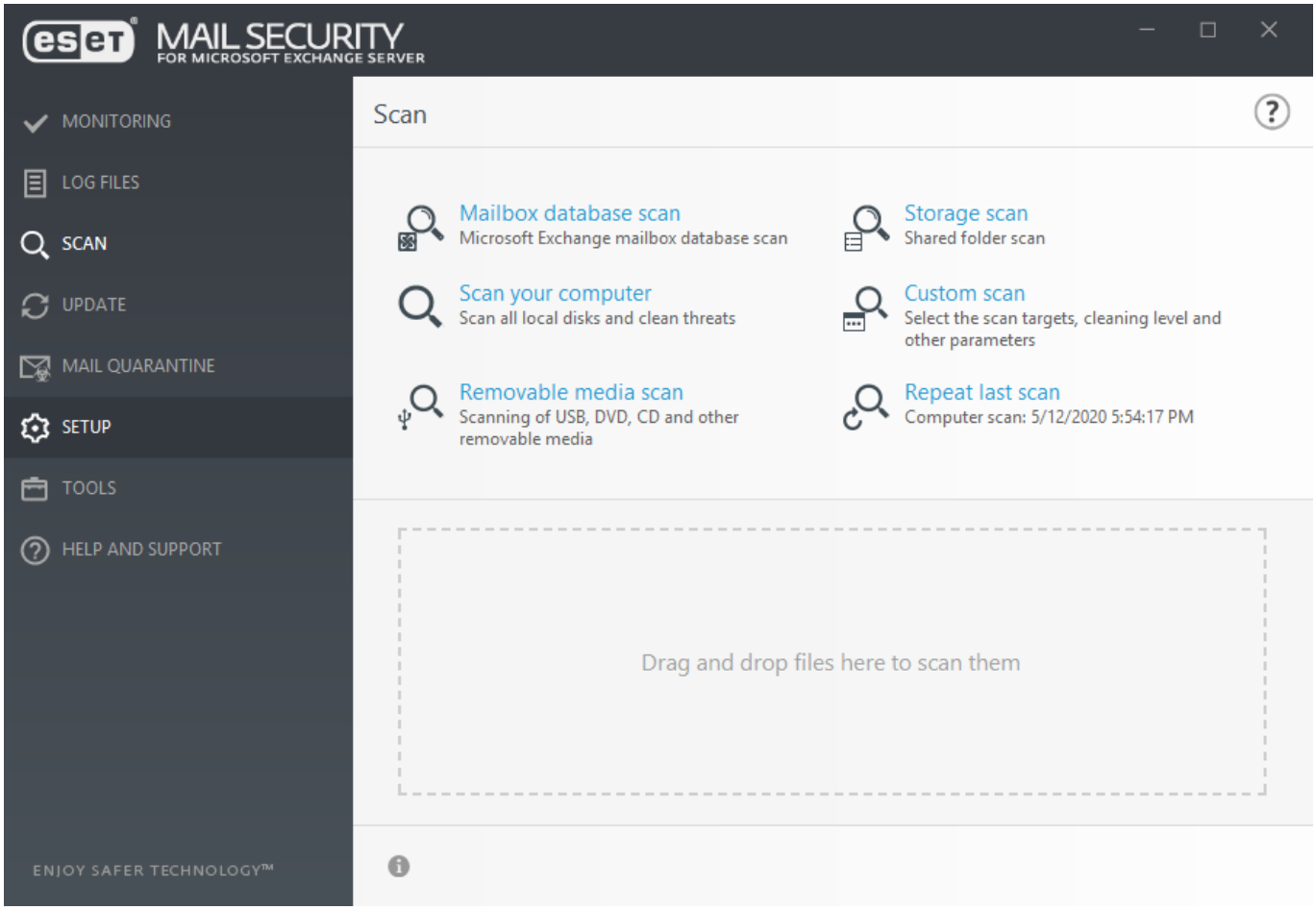
Kontrola Hyper-V

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

Opakovať poslednú kontrolu

Zopakuje poslednú kontrolu s rovnakými nastaveniami.

Zopakovanie poslednej kontroly nie je dostupné pri manuálnej kontrole databáz.



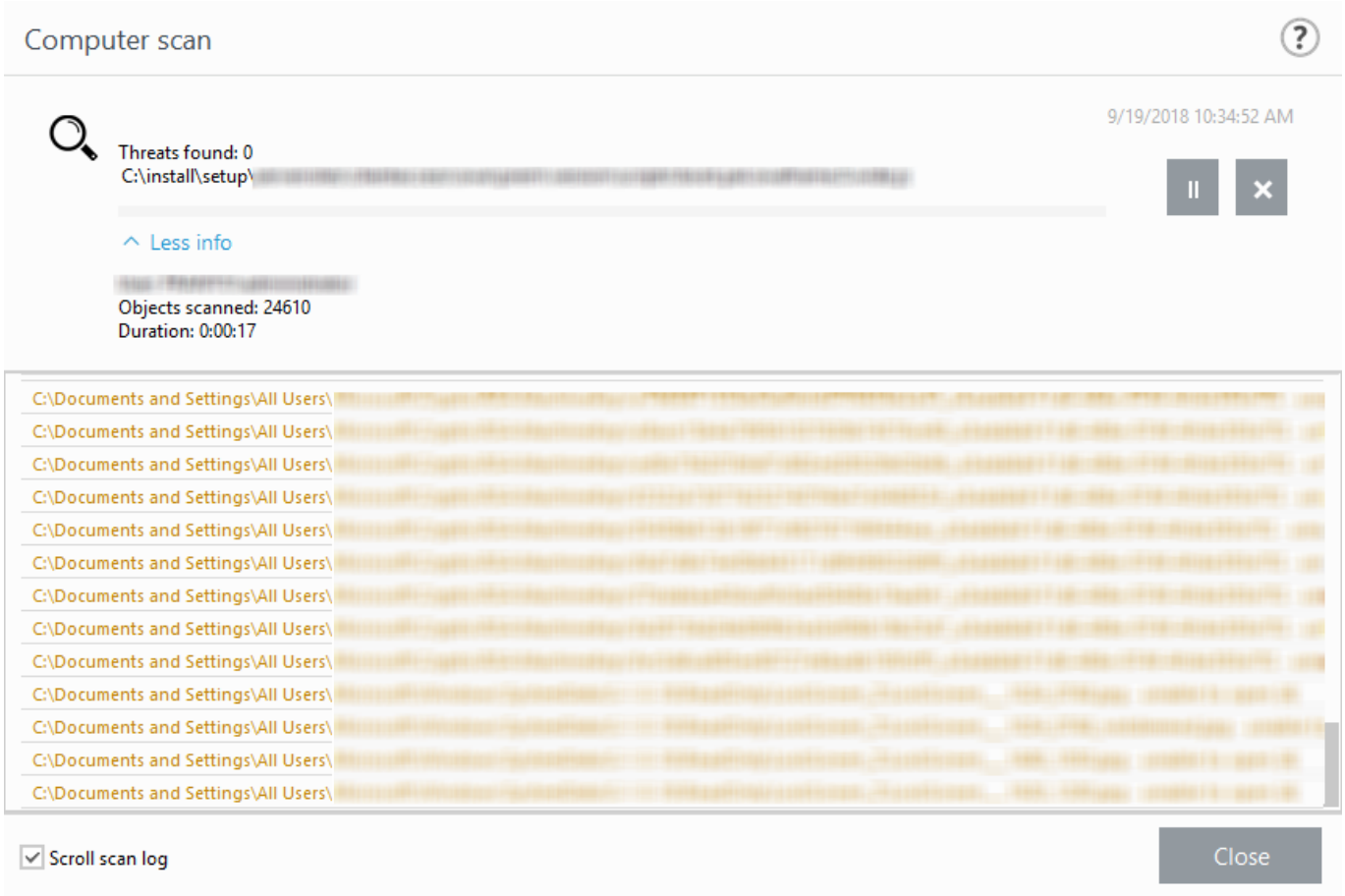
Pomocou nižšie spomenutých možností môžete získať podrobnejšie informácie o prebiehajúcich kontrolách:

Drag and drop	**Súbory môžete skontrolovať aj tak, že ich presuniete myšou do okna kontroly v ESET Mail Security. Tieto súbory budú následne okamžite skontrolované.**
Zatvoriť/Zatvoriť všetko	Kliknutím na tieto možnosti zatvoríte konkrétne správy.
Stav kontroly	Zobrazí stav počiatočnej kontroly, konkrétne, či bola kontrola dokončená, alebo bola prerušená používateľom.
Zobraziť protokol	Kliknutím zobrazíte podrobnejšie informácie.
Viac informácií	Počas kontroly môžete kliknúť na túto možnosť pre zobrazenie podrobností, ako napr. Používateľ, ktorý spustil kontrolu z grafického používateľského rozhrania, počet Skontrolovaných objektov a **Trvanie** kontroly. Ak je spustená manuálna Kontrola databáz, zobrazí sa používateľ, ktorý spustil kontrolu, nie Účet kontroly databázy, ktorý sa používa na pripojenie do EWS (Exchange Web Services) počas priebehu kontroly.
Otvoriť okno kontroly	Okno priebehu kontroly ukazuje aktuálny stav kontroly a počet nájdených súborov, ktoré obsahujú škodlivý kód.

Okno kontroly a protokol o kontrole

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

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

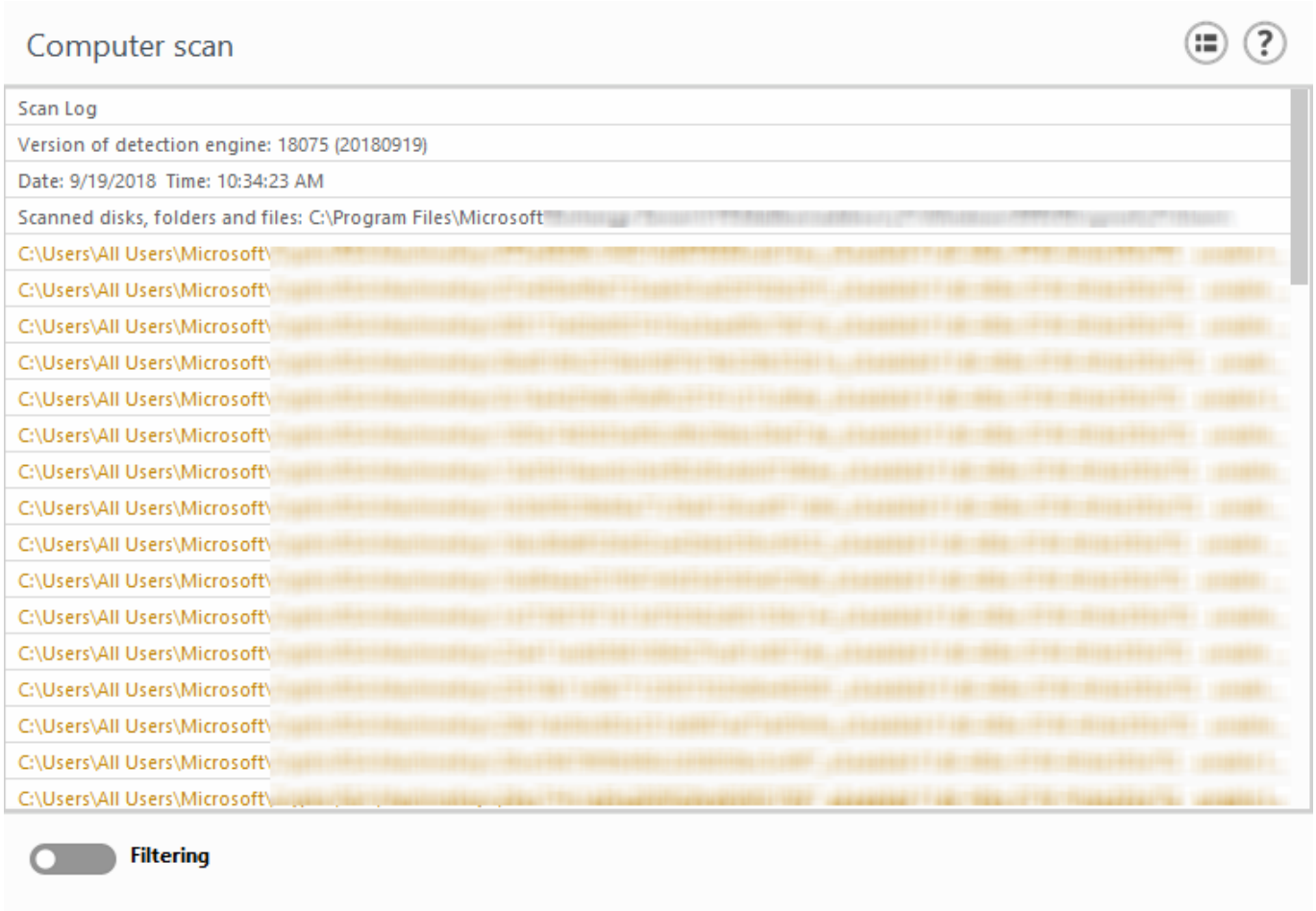


Rolovanie výpisu protokolu kontroly

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

> Je v poriadku, ak určité typy súborov, ako napríklad súbory chránené heslom alebo využívané výhradne systémom (napr. *pagefile.sys* a niektoré protokoly), nie je možné skontrolovať.

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



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

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

Protokoly

Protokoly obsahujú informácie o dôležitých systémových udalostiach a poskytujú prehľad o výsledkoch kontroly, odhalených hrozbách atď. Predstavujú silný nástroj systémovej analýzy, odhaľovania problémov a rizík a v

neposlednom rade hľadania riešení. Vytváranie protokolov prebieha aktívne na pozadí bez akejkoľvek interakcie zo strany používateľa. Zaznamenávajú sa informácie podľa aktuálnych nastavení detailnosti protokolov. Prezeranie alebo exportovanie protokolov je možné priamo z prostredia ESET Mail Security.

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

Detekcie

Protokol Detekcie ponúka podrobné informácie o infiltráciách zachytených modulmi ESET Mail Security. Informácie zahŕňajú čas detekcie, názov infiltrácie, umiestnenie, vykonanú akciu a používateľa prihláseného v čase detekcie.

Dvojitým kliknutím na akúkoľvek položku protokolu zobrazíte jej podrobnosti v novom okne. V prípade potreby môžete vytvoriť vylúčenie detekcie – pravým tlačidlom myši kliknite na záznam protokolu (detekciu) a potom na **Vytvoriť vylúčenie**. Otvorí sa sprievodca vylúčeniami s preddefinovanými kritériami. Ak je pri vylúčenom súbore uvedený aj názov detekcie, znamená to, že v rámci súboru je vylúčená iba daná detekcia, nie je vylúčený súbor ako celok. Ak by teda došlo k infikovaniu tohto súboru iným typom malvéru, takáto hrozba bude detegovaná.

Udalosti

V tomto protokole sú zaznamenané všetky dôležité operácie vykonané produktom ESET Mail Security. Protokol udalostí obsahuje informácie o udalostiach v programe a chybách, ktoré sa vyskytli. Je navrhnutý tak, aby pomáhal správcom systémov a používateľom pri riešení problémov. Informácie získané z tohto protokolu vám často pomôžu nájsť príčiny problémov, prípadne ich riešenie.

Kontrola počítača

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

Blokované súbory

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

Odoslané súbory

Protokol obsahuje prehľad súborov zachytených cloudovou ochranou (ESET LiveGuard Advanced a ESET LiveGrid®).

Protokoly auditu

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

HIPS

Obsahuje záznamy konkrétnych pravidiel systému HIPS označených na zaznamenávanie. V protokole je zobrazená

aplikácia, ktorá danú operáciu vyvolala, výsledok (tzn. či bolo pravidlo povolené alebo zakázané), prípadne aj názov vytvoreného pravidla.

Ochrana siete

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

Filtrované webové stránky

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

Správa zariadení

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

Ochrana e-mailových serverov

Všetky správy detegované programom ESET Mail Security ako infiltrácia alebo spam sa nachádzajú tu. Tieto protokoly sa vzťahujú na nasledujúce typy ochrany: Antispam, Anti-Phishing, Ochrana pred sfalšovaním identity odosielateľa, Pravidlá a Antimalvér.

Ak dvakrát kliknete na konkrétnu položku, zobrazí sa okno s dodatočnými informáciami o detegovanej e-mailovej správe, ako napr. IP adresa, reťazec HELO, ID správy a Typ kontroly, pričom uvidíte, na ktorej vrstve ochrany došlo k detekcii. Taktiež si môžete pozrieť výsledok antivírusovej, antiphishingovej a antispamovej kontroly, ako aj dôvod, prečo došlo k detekcii, prípadne či bolo aktivované pravidlo.

> Do tohto protokolu sa nezapisujú všetky správy spracované ochranou e-mailových serverov. Zapisujú sa len správy, v ktorých došlo k nejakej zmene (napr. odstránenie prílohy, pridanie vlastného reťazca do hlavičky správy a pod.).

Kontrola databáz e-mailových schránok

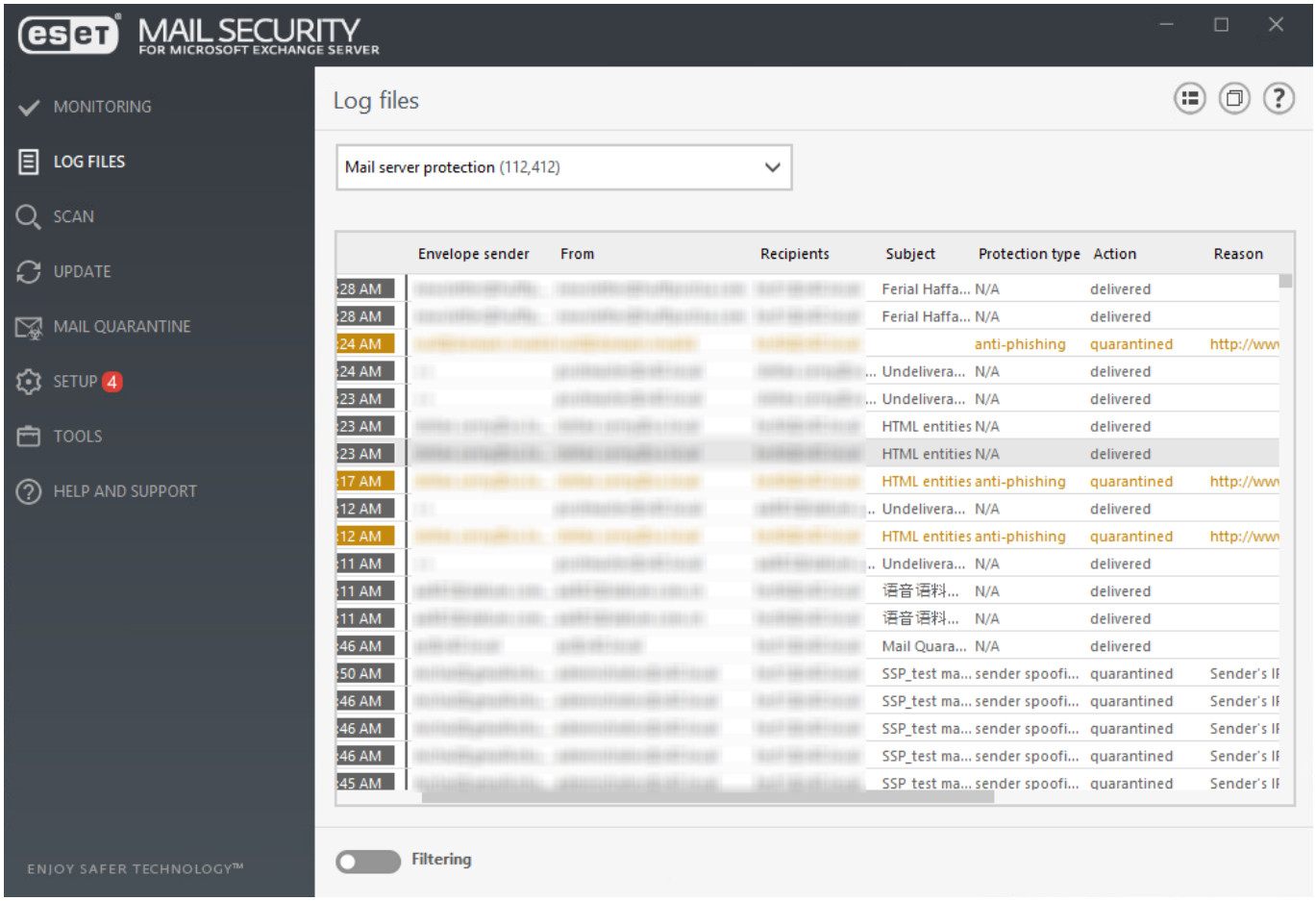
Tento protokol obsahuje verziu detekčného jadra, dátum, lokalitu kontroly, počet kontrolovaných objektov, počet zistených hrozieb, počet uplatnených pravidiel a čas ukončenia kontroly.

SMTP ochrana

Tu sa nachádzajú všetky správy vyhodnocované pomocou metódy greylisting. Nachádzajú sa tu aj SPF záznamy a Backscatter. Každý záznam obsahuje reťazec HELO, IP adresu odosielateľa a príjemcu, stavy akcií (odmietnuté, odmietnuté (neoverené) a overené prichádzajúce správy). Bola pridaná nová akcia na pridanie subdomény do greylistingového whitelistu – pozrite si tabuľku nižšie.

Kontrola Hyper-V

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



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

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

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

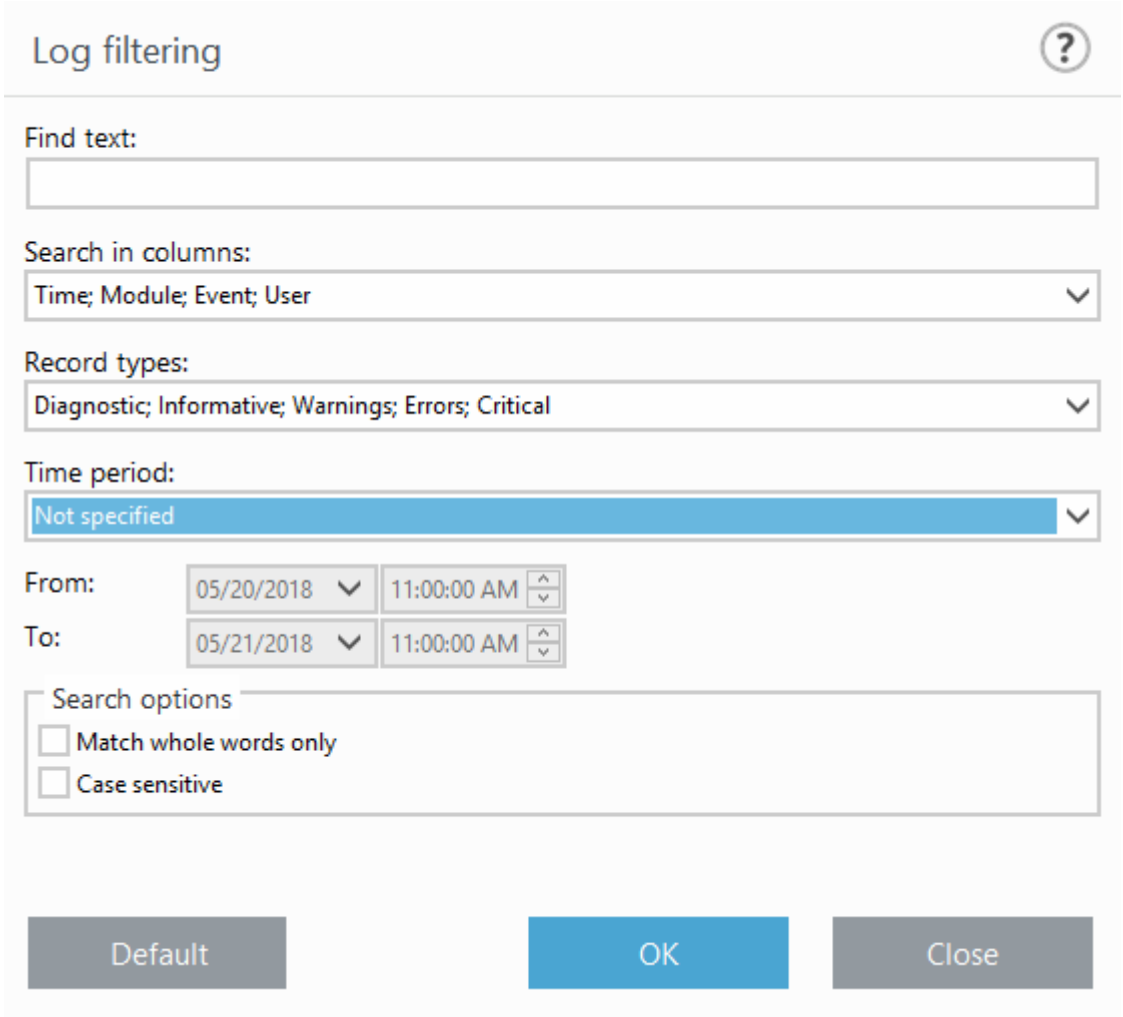
Pridať IP adresu do greylistingového whitelistu	Pridá IP adresu odosielateľa do whitelistu IP adries. Whitelist IP adries nájdete v sekcii Greylisting a SPF v časti Filtrovanie a overovanie. Toto sa vzťahuje na položky zapisované greylistingom alebo SPF.
Pridať doménu na whitelist pre greylisting a SPF kontrolu	Pridá doménu odosielateľa do whitelistu domén preložených na IP adresy. Pridaná bude len doména, subdoména bude ignorovaná. Napríklad, ak je adresa odosielateľa sub.domain.com, do whitelistu bude pridaná len časť domain.com. Whitelist domén preložených na IP adresy nájdete v sekcii Greylisting a SPF v časti Filtrovanie a overovanie. Toto sa vzťahuje na položky zapisované greylistingom.
Pridať subdoménu na whitelist pre greylisting a SPF kontrolu	Pridá subdoménu odosielateľa do whitelistu domén preložených na IP adresy. Bude pridaná celá doména vrátane jej subdomény (napr. sub.domain.com). Vďaka tomu budete mať v prípade potreby k dispozícii vyššiu mieru flexibility filtrovania. Whitelist domén preložených na IP adresy nájdete v sekcii Greylisting a SPF v časti Filtrovanie a overovanie. Toto sa vzťahuje na položky zapisované greylistingom.

Filtrovanie protokolov

Filtrovanie protokolov vám umožňuje nájsť konkrétnu informáciu v protokoloch. Vďaka tejto funkcii môžete zobraziť záznamy protokolu, ktoré spĺňajú určité kritériá; napr. môžete filtrovať konkrétny typ udalosti, stav alebo časové obdobie.

Vyberte Typy záznamov a nastavte Časové obdobie pre vyhľadávanie v určitom časovom období. Upresnením nastavení vyhľadávania docielite zobrazenie len tých výsledkov, ktoré sú pre vás dôležité.

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



Hľadať text

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

Hľadať v stĺpcoch

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

Typy záznamov

Z roletového menu vyberte jeden alebo viacero typov záznamov:

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

Časové obdobie

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

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

Hľadať iba celé slová

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

Rozlišovať veľké a malé písmená

Túto možnosť použite v prípade, ak je dôležité pri filtrovaní rozlišovať malé a veľké písmená. Pri konfigurácii možností filtrovania/vyhľadávania kliknite na **OK**, ak chcete zobraziť filtrované záznamy protokolov, alebo na **Hľadať**, ak chcete spustiť vyhľadávanie.

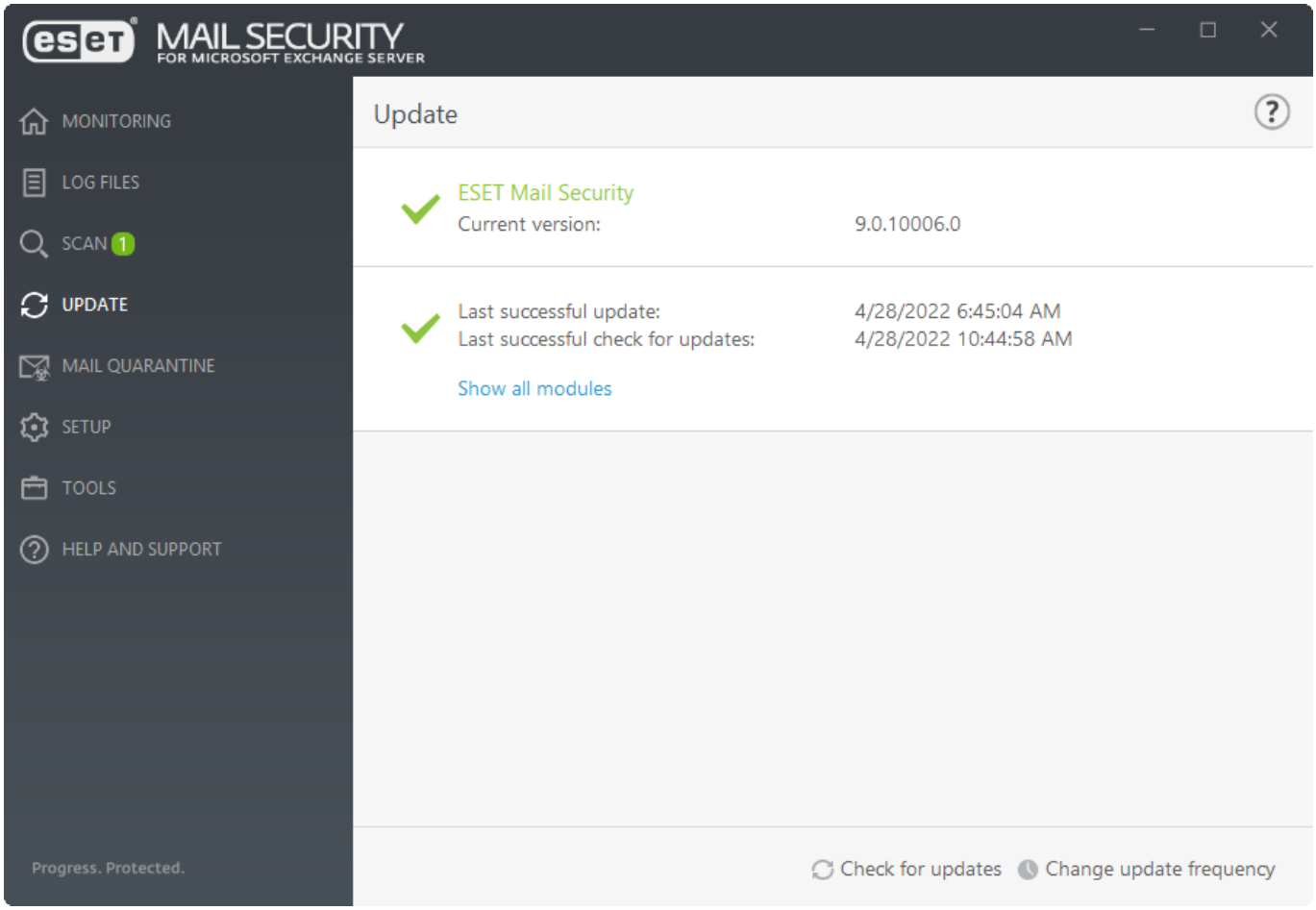
Protokoly sú prehľadávané smerom zhora nadol, začínajúc z aktuálnej pozície (záznam, ktorý je momentálne označený). Vyhľadávanie sa zastaví pri prvom nájdenom zázname. Stlačením klávesu **F3** budete pokračovať vo vyhľadávaní ďalšieho záznamu, prípadne môžete kliknúť pravým tlačidlom myši, vybrať možnosť **Hľadať** a upresniť možnosti vyhľadávania.

Aktualizácia

V sekcii Aktualizácia je zobrazený stav aktualizácie vášho produktu ESET Mail Security vrátane dátumu a času poslednej úspešnej aktualizácie. Pravidelná aktualizácia produktu ESET Mail Security a programových modulov je tou najlepšou metódou, ako zabezpečiť maximálnu úroveň ochrany vášho servera.

Modul Aktualizácia zabezpečuje, aby bol program stále aktuálny, čo zahŕňa aktualizáciu detekčného jadra, ako aj aktualizáciu všetkých komponentov systému. Aktualizácia detekčného jadra a programových súčastí je dôležitá na zabezpečenie komplexnej ochrany pred škodlivým kódom.

> Ak ste ešte nezadali licenčný kľúč, aktualizáciu nebude možné vykonať a zobrazí sa vám výzva, aby ste aktivovali svoj produkt. Pre aktiváciu produktu prejdite do sekcie **Pomocník a podpora** > **Aktivovať produkt**.



Aktuálna verzia

Aktuálna verzia produktu ESET Mail Security.

Posledná úspešná aktualizácia

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

Posledné úspešné overenie dostupnosti aktualizácií

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

Zobraziť všetky moduly

Otvorí sa zoznam nainštalovaných modulov.

Overiť dostupnosť aktualizácií

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

Zmeniť frekvenciu aktualizácií

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

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

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

Nastavenia proxy servera sa v prípade rôznych aktualizačných profilov môžu líšiť. Ak ide o takýto prípad, nakonfigurujte jednotlivé aktualizačné profily v okne **Rozšírené nastavenia** (**F5**) kliknutím na sekciu **Aktualizácia** > Profily.

E-mailová karanténa

E-mailové správy a ich súčasti, ako napr. prílohy, sú namiesto štandardnej súborovej karantény umiestňované do e-mailovej karantény. E-mailová karanténa poskytuje pohodlnejší spôsob spravovania spamových správ, infikovaných príloh obsahujúcich malvér alebo phishingových stránok. Do karantény môžu byť e-mailové správy presunuté z rôznych dôvodov. Závisí to od toho, ktorý modul ochrany programu ESET Mail Security vyhodnocuje konkrétnu správu (antimalvérová, antispamová alebo antiphishingová ochrana, ochrana pred sfalšovaním identity odosielateľa alebo pravidlá).

Filtrovanie podľa ikon

Na filtrovanie správ môžete použiť ikony – môžete zobraziť prílohy, správy alebo správy s prílohami.

Časový rozsah

Vyberte časový rozsah, pre ktorý chcete zobraziť e-maily umiestnené v karanténe. Ak použijete možnosť **Vlastný**, môžete určiť vlastný rozsah (Dátum od a Dátum do).

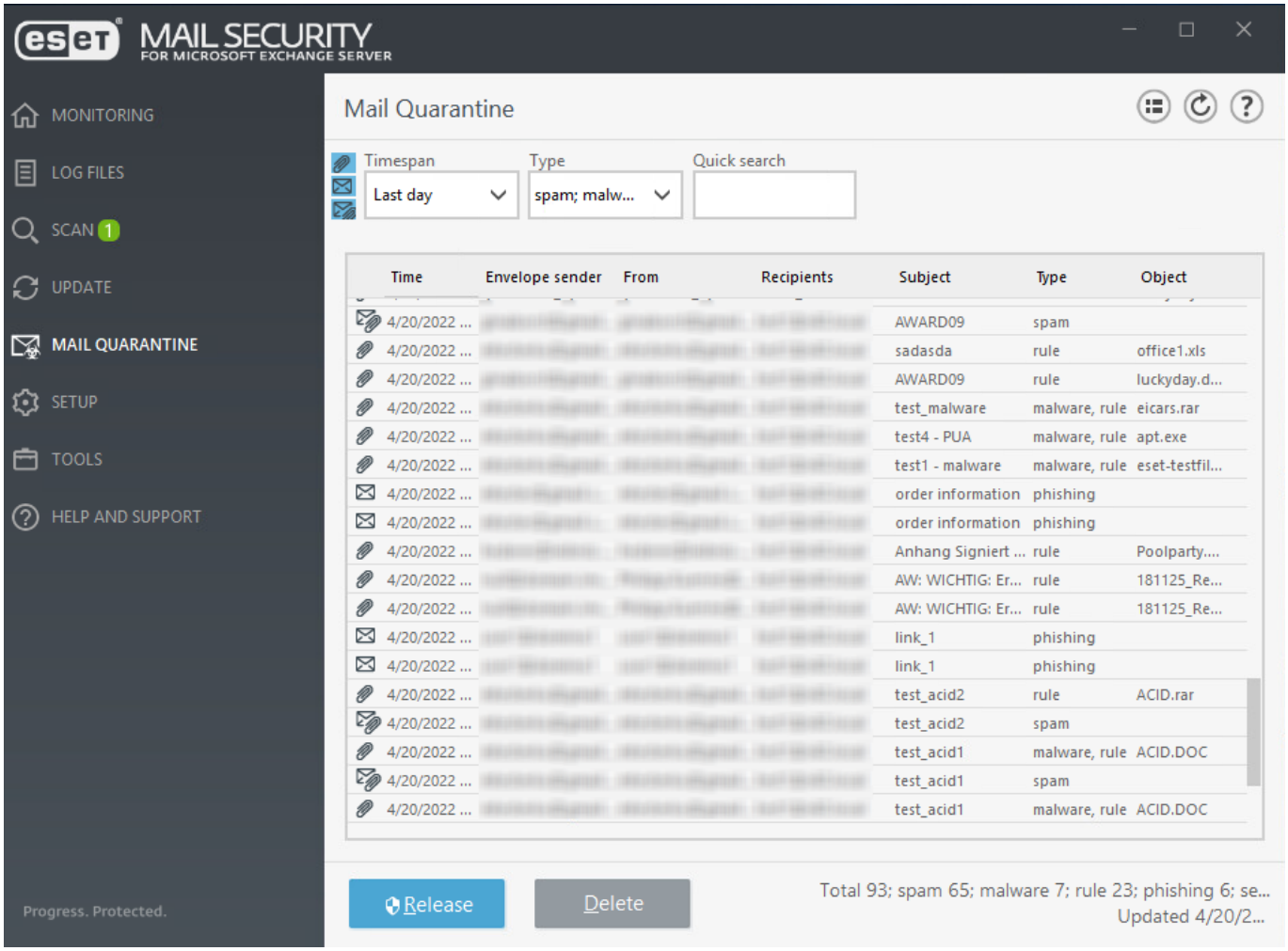
Rýchle vyhľadávanie

Pomocou tohto textového poľa môžete filtrovať zobrazované správy (vyhľadávanie prebieha vo všetkých stĺpcoch).

Dôvod

Použitím príslušných začiarkavacích políčok môžete ďalej filtrovať podľa typu (spam, malvér, pravidlo, phishing alebo sfalšovaný odosielateľ).

Dáta Správcu e-mailovej karantény sa neaktualizujú automaticky, na zobrazenie aktuálnych objektov v okne E-mailová karanténa odporúčame kliknúť na tlačidlo **Obnoviť** .



Uvoľniť

Uvoľníte e-mail jeho pôvodnému príjemcovi prostredníctvom Replay directory a odstránite ho z karantény. Kliknutím na Áno potvrdíte vykonanie akcie. Ak je položka v karanténe prílohou z verejného priečinka, ktorý nepodporuje poštu, tlačidlo Uvoľniť nebude dostupné.

Pri uvoľňovaní e-mailu z karantény ESET Mail Security ignoruje MIME hlavičku `To:` z dôvodu, že môže byť ľahko sfalšovaná. Namiesto toho sú použité informácie o pôvodnom príjemcovi z príkazu `RCPT TO:`, získané počas SMTP spojenia. Vďaka tomu sa zabezpečí, že e-mail, ktorý je uvoľnený z karantény, bude doručený správnemu príjemcovi.

Ak používate klastrové prostredie a uvoľníte konkrétnu správu z karantény, na ďalších uzloch ESET Mail Security sa už rovnaká správa opätovne nedostane do karantény. Zabezpečuje to synchronizácia pravidiel medzi uzlami klastra.

Odstrániť

Odstránite položku z karantény. Kliknutím na **Áno** potvrdíte vykonanie akcie. Položky odstránené pomocou hlavného okna programu budú odstránené z okna karantény, avšak naďalej zostanú v úložisku. K ich automatickému odstráneniu dôjde neskôr (predvolene po troch dňoch).

Obnoviť do

Umožňuje obnoviť prílohy do konkrétneho umiestnenia. Táto možnosť je dostupná len pre prílohy (pre správy bude uzamknutá). Ak potrebujete spracovať celú správu, použite na tento účel funkciu Uvoľniť.

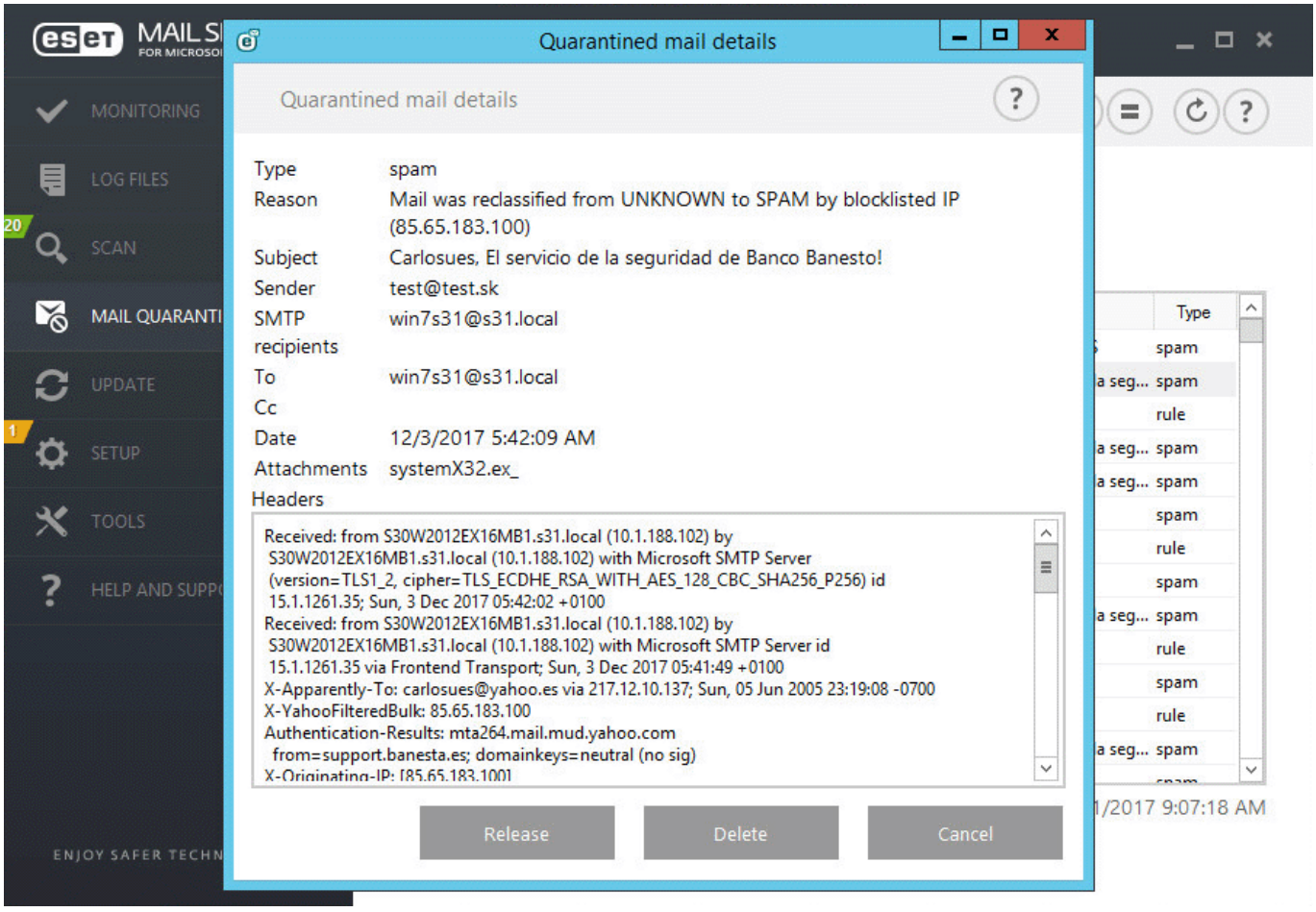
Podrobnosti e-mailu v karanténe

Dvojitým kliknutím na správu v karanténe alebo kliknutím pravým tlačidlom myši a zvolením možnosti **Podrobnosti** zobrazíte okno s podrobnosťami o e‑mailovej správe umiestnenej v karanténe. Ďalšie informácie o e‑maile je možné nájsť v RFC hlavičke e‑mailu.

Podrobnosti prílohy v karanténe

Okno s podrobnosťami, ktoré sa zobrazí po dvojitom kliknutí na prílohu, je odlišné od okna s podrobnosťami pre e-mailové správy. RFC hlavičky správ nie sú k dispozícii, namiesto toho sa zobrazuje plocha s textom obálky prílohy. Môžete zadať vlastný text, ktorý sa zobrazí adresátovi pri doručení objektu uvoľneného z karantény.

Akcie sú dostupné aj prostredníctvom kontextového menu. V prípade potreby kliknite na **Uvoľniť**, **Odstrániť** alebo **Natrvalo odstrániť**. Kliknutím na **Áno** potvrdíte vykonanie akcie. Ak vyberiete možnosť **Natrvalo odstrániť**, správa bude odstránená aj zo súborového systému, na rozdiel od akcie **Odstrániť**, pri ktorej sa správa odstráni len z okna Správca e‑mailovej karantény.

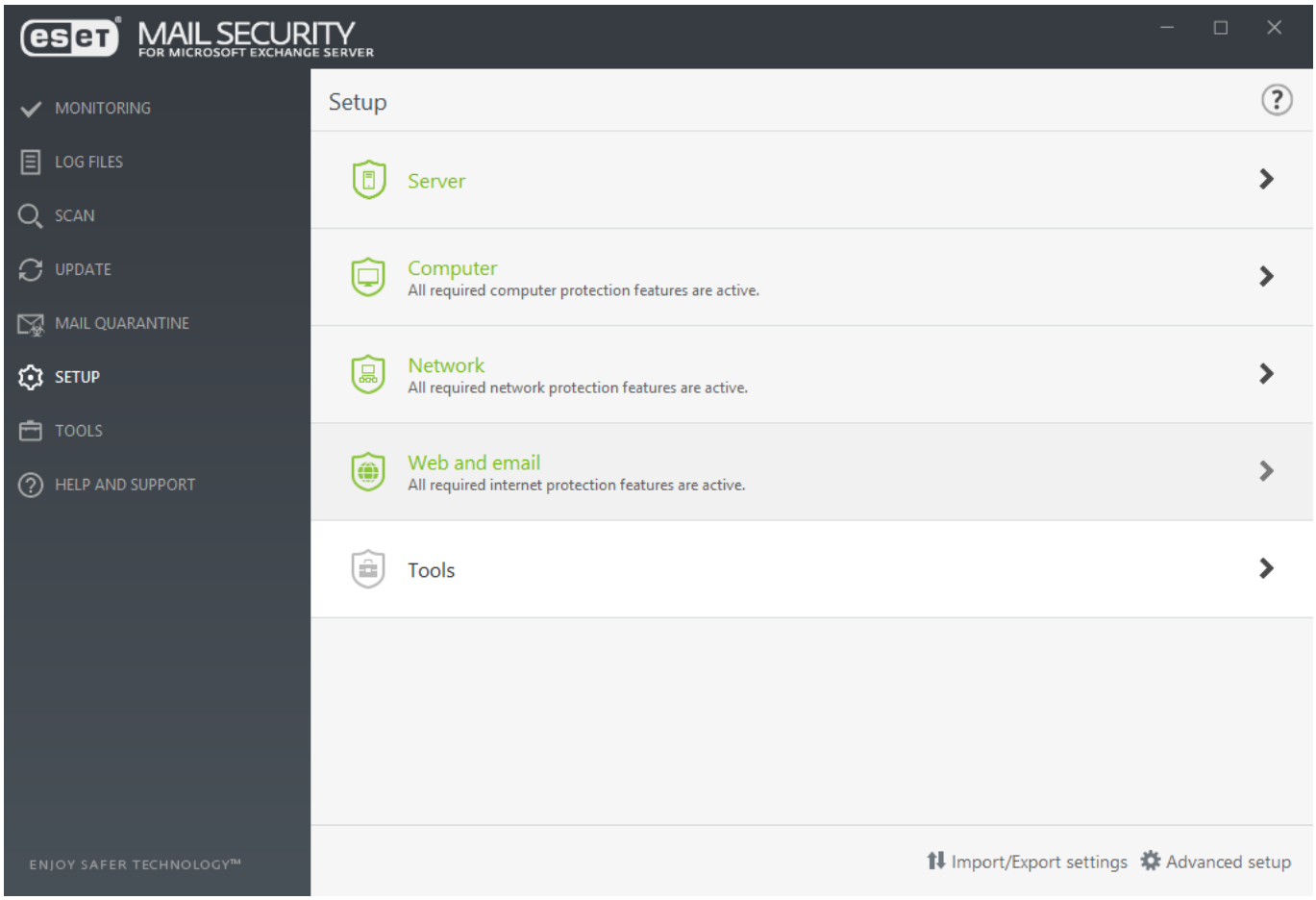


Nastavenia

Sekcia Nastavenia obsahuje nasledujúce časti:

- Server
- Počítač
- Sieť

- Web a e-mail
- Nástroje – Diagnostické zapisovanie do protokolu



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

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

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

Import/export nastavení

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

Rozšírené nastavenia

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

Server

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

Antivírusová ochrana

Zabezpečuje komplexnú ochranu pred nebezpečnými programami a útokmi ohrozujúcimi systém. Zahŕňa kontrolu súborov, e-mailovej a internetovej komunikácie.

Antispamová ochrana

Zahŕňa rôzne technológie pre maximalizáciu detekcie e-mailových hrozieb (RBL, DNSBL, Fingerprinting, kontrola reputácie, analýza obsahu, pravidlá, whitelisting/blacklisting atď.).

Antiphishingová ochrana

Analyzuje telá e-mailových správ a hľadá v nich phishingové odkazy (URL).

Automatické vylúčenia

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

Klaster

V tejto sekcii môžete nakonfigurovať a aktivovať klaster ESET.

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

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

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

Import/export nastavení

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

Rozšírené nastavenia

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

Počítač

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

Rezidentná ochrana súborového systému

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

Správa zariadení

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

Host Intrusion Prevention System (HIPS)

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

- Advanced memory scanner
- Exploit Blocker
- Ransomware Shield

Prezentačný režim

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

Pozastaviť antivírusovú a antispyvérovú ochranu

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

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

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

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

Import/export nastavení

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

Rozšírené nastavenia

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

Sieť

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

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

Ochrana pred sieťovými útokmi (IDS)

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

Ochrana pred botnetmi

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

Dočasný blacklist IP adries (blokované adresy)

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

Sprievodca riešením problémov (nedávno blokované aplikácie alebo zariadenia)

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

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

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

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

Import/export nastavení

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

Rozšírené nastavenia

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

Sprievodca riešením problémov so sieťou

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

Web a e-mail

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

Ochrana prístupu na web

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

Ochrana e-mailových klientov

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

Antiphishingová ochrana

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

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

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

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

Import/export nastavení

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

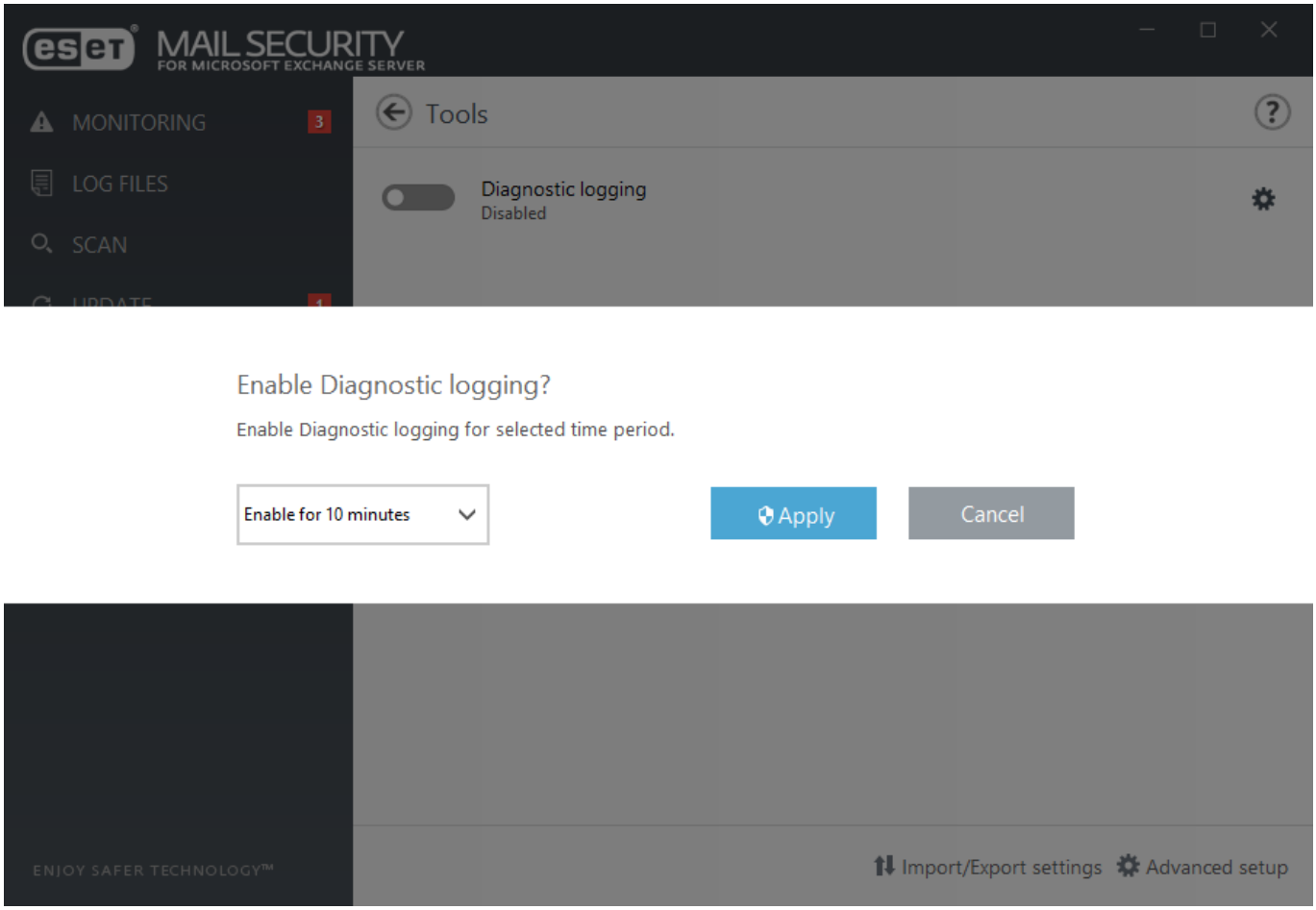
Rozšírené nastavenia

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

Nástroje – Diagnostické zapisovanie do protokolu

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

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



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

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

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

Import/export nastavení

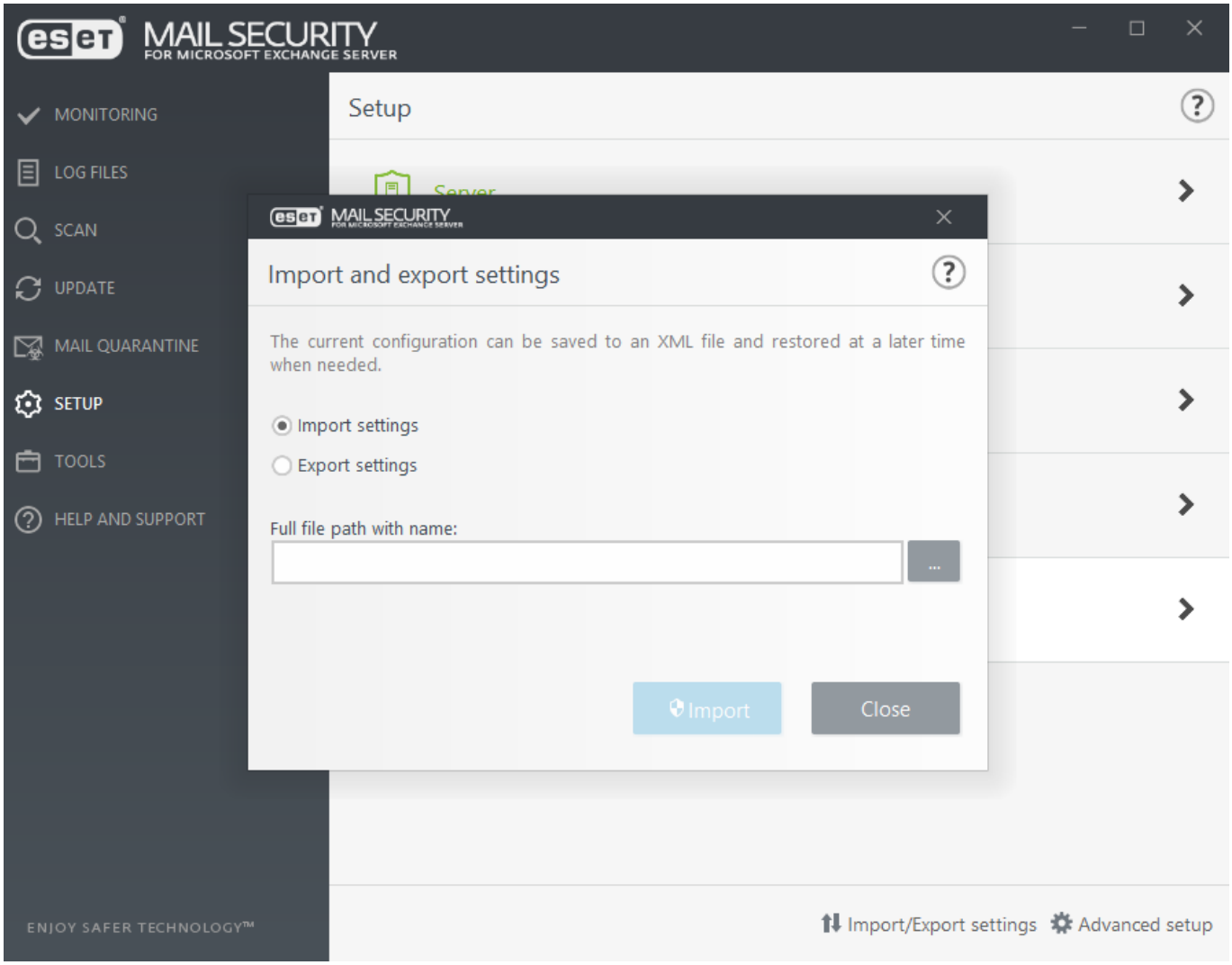
Pomocou tejto funkcie môžete načítať nastavenia zo súboru *.xml* alebo si nastavenia môžete v podobe súboru uložiť.

Rozšírené nastavenia

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

Import a export nastavení

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



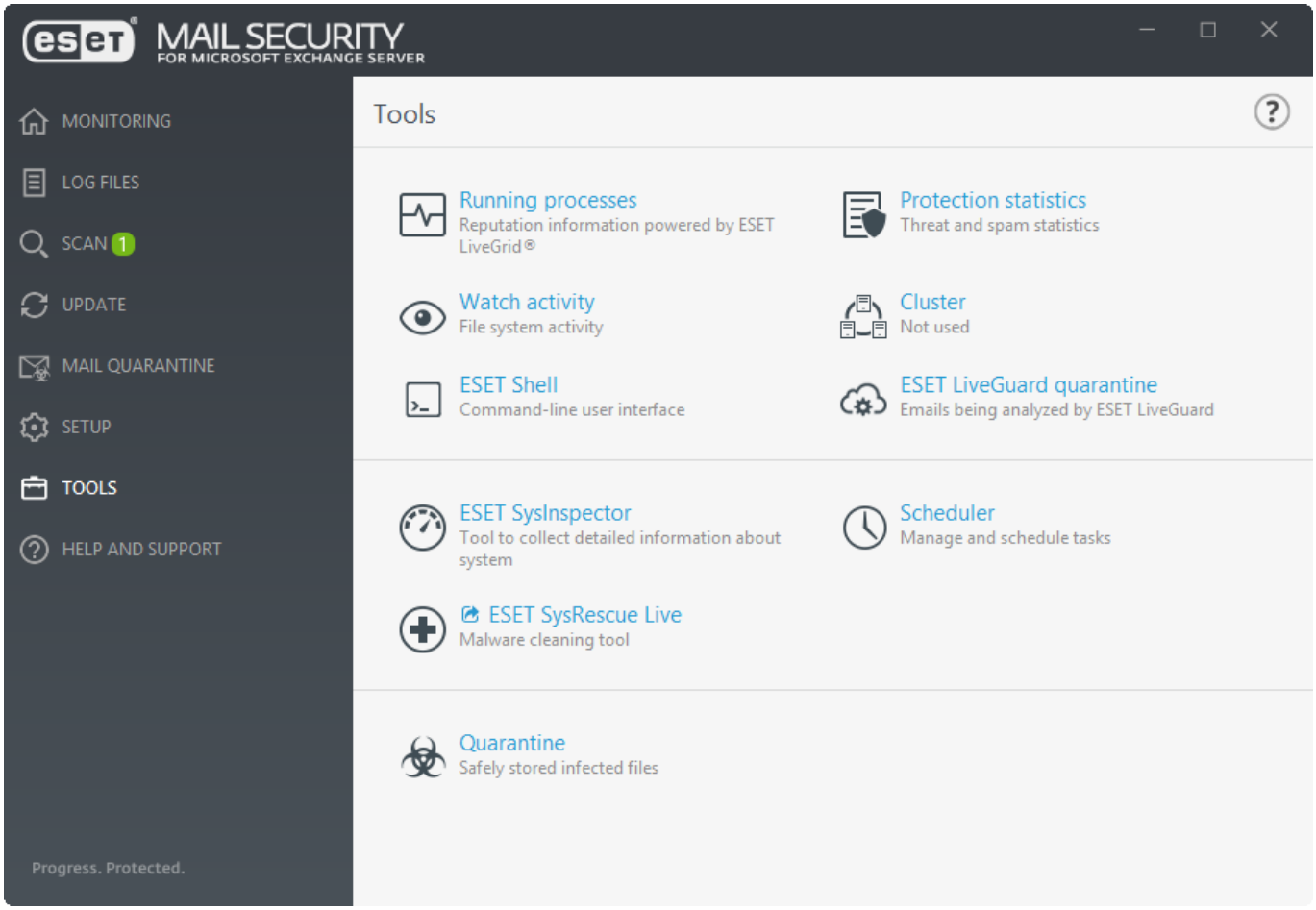
Ak nemáte dostatočné oprávnenia na zapisovanie exportovaného súboru do určeného adresára, môže sa pri exportovaní zobraziť chybové hlásenie.

Nástroje

Na správu programu ESET Mail Security sú dostupné nasledujúce funkcie:

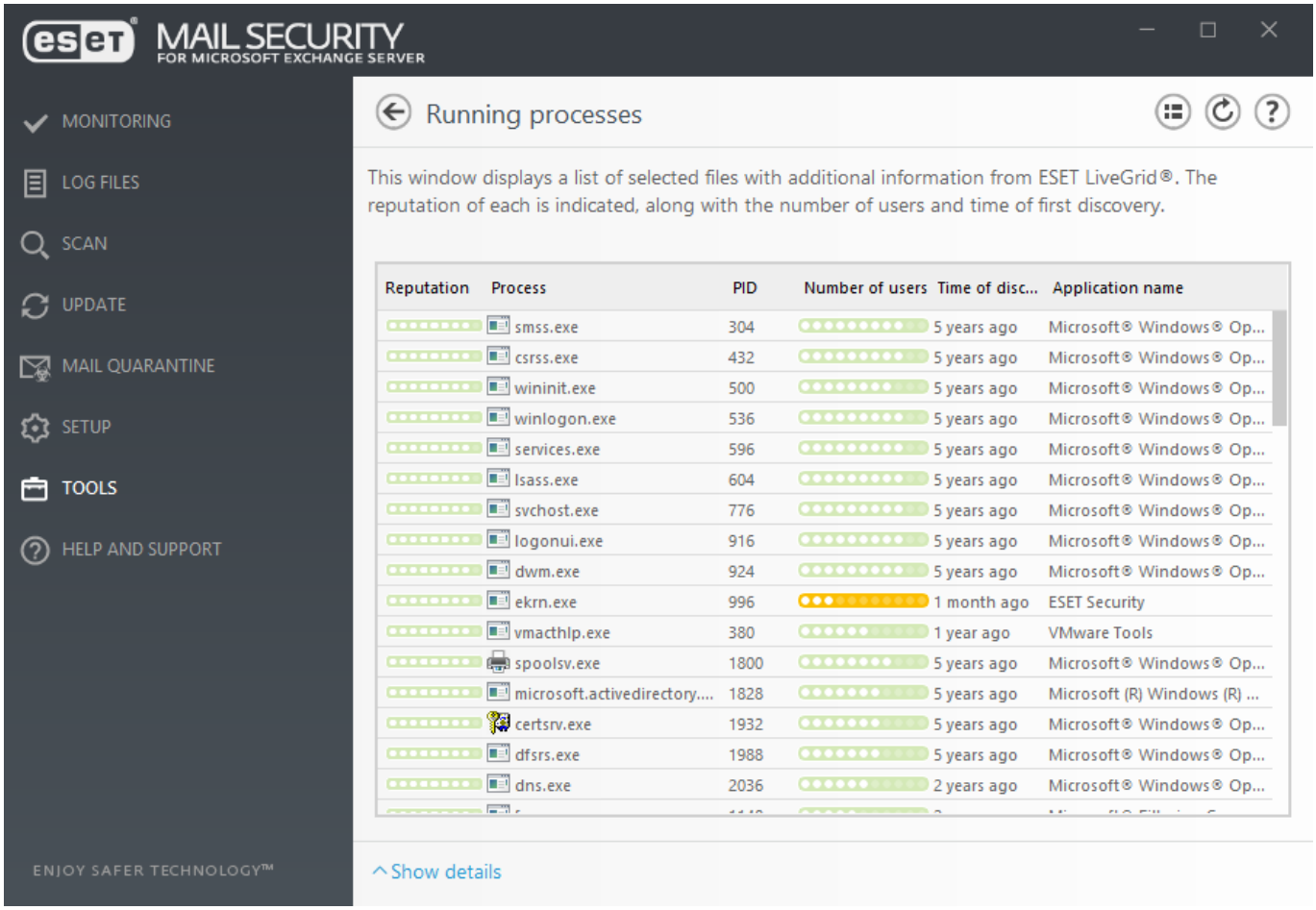
- Spustené procesy
- Sledovanie aktivity
- Štatistiky ochrany
- Klaster
- ESET Shell
- ESET LiveGuard Advanced
- ESET SysInspector
- ESET SysRescue Live

- Plánovač
- Odoslanie vzorky na analýzu
- Karanténa



Spustené procesy

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



Známe aplikácie označené zelenou farbou nepredstavujú riziko a sú bezpečné. Budú preto vyňaté z kontroly, čím sa zvyšuje rýchlosť kontroly počítača a rezidentnej ochrany súborového systému na vašom počítači.

Úroveň rizika	**Vo väčšine prípadov ESET Mail Security pomocou technológie ESET LiveGrid® priradí objektom (súborom, procesom, kľúčom databázy Registry atď.) určitý stupeň rizika na základe heuristických pravidiel, ktoré preskúmajú každý objekt a vyhodnotia pravdepodobnosť nebezpečnej aktivity. Podľa výsledkov heuristiky sa objektom pridelí úroveň rizika od 9 – najlepšia reputácia (zelenou farbou) až po 0 – najhoršia reputácia (červenou farbou).**
Proces	Názov aplikácie alebo procesu, ktorý je momentálne spustený na počítači. Pre lepší prehľad o všetkých procesoch použite Správcu úloh (MS Windows). Správcu úloh môžete otvoriť kliknutím pravým tlačidlom myši kdekoľvek na panel úloh a zvolením možnosti Správca úloh, prípadne použite klávesovú skratku CTRL + SHIFT + ESC.
PID	Identifikačné číslo procesu spusteného na operačnom systéme Windows.
Počet používateľov	Počet používateľov, ktorí používajú danú aplikáciu. Tieto informácie sú zhromažďované pomocou technológie ESET LiveGrid®.
Čas objavenia	Doba, odkedy bol proces objavený technológiou ESET LiveGrid®.
Názov aplikácie	Názov vydavateľa aplikácie alebo procesu.

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

Zobraziť podrobnosti

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

- Cesta – umiestnenie aplikácie vo vašom počítači.
- Veľkosť – veľkosť súboru v kB (kilobajtoch) alebo MB (megabajtoch).
- Popis – charakteristika súboru vychádzajúca z popisu daného súboru operačným systémom.
- Spoločnosť – názov vydavateľa aplikácie alebo procesu.
- Verzia – táto informácia pochádza od vydavateľa aplikácie alebo procesu.
- Produkt – názov aplikácie, zvyčajne obchodné meno.
- Vytvorené – dátum a čas, kedy bola aplikácia vytvorená.
- Upravené – dátum a čas, kedy bola aplikácia naposledy upravená.

Pridať vylúčenia procesov

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

Sledovanie aktivity

V okne Sledovanie aktivity môžete prostredníctvom grafov sledovať aktivitu:

Aktivita súborového systému

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

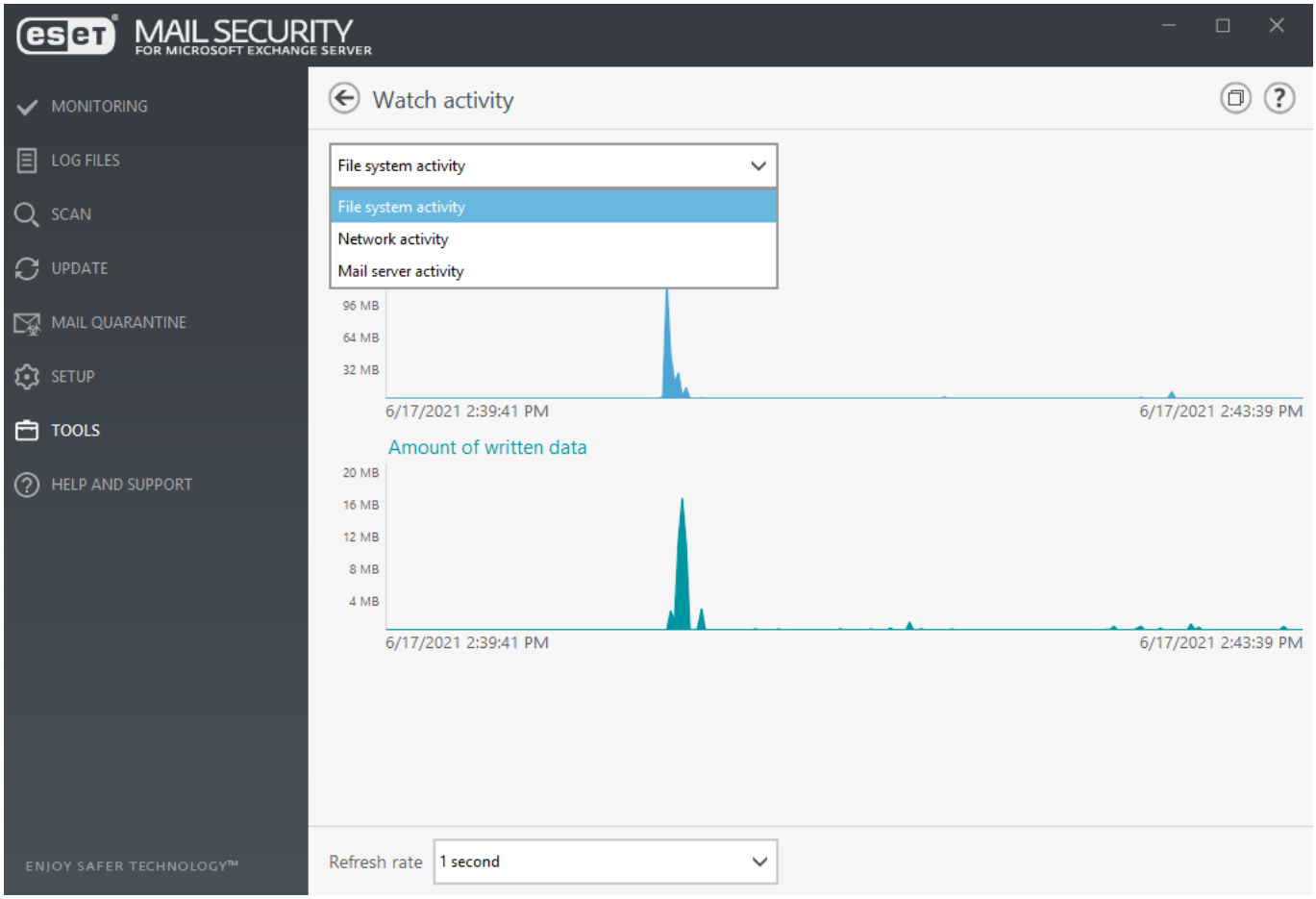
Sieťová aktivita

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

Aktivita e-mailového servera

Zobrazuje množstvo dát spracovaných ochranou prenosu e-mailov (modrou farbou) a množstvo dát spracovaných ochranou databáz (zelenou farbou).

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



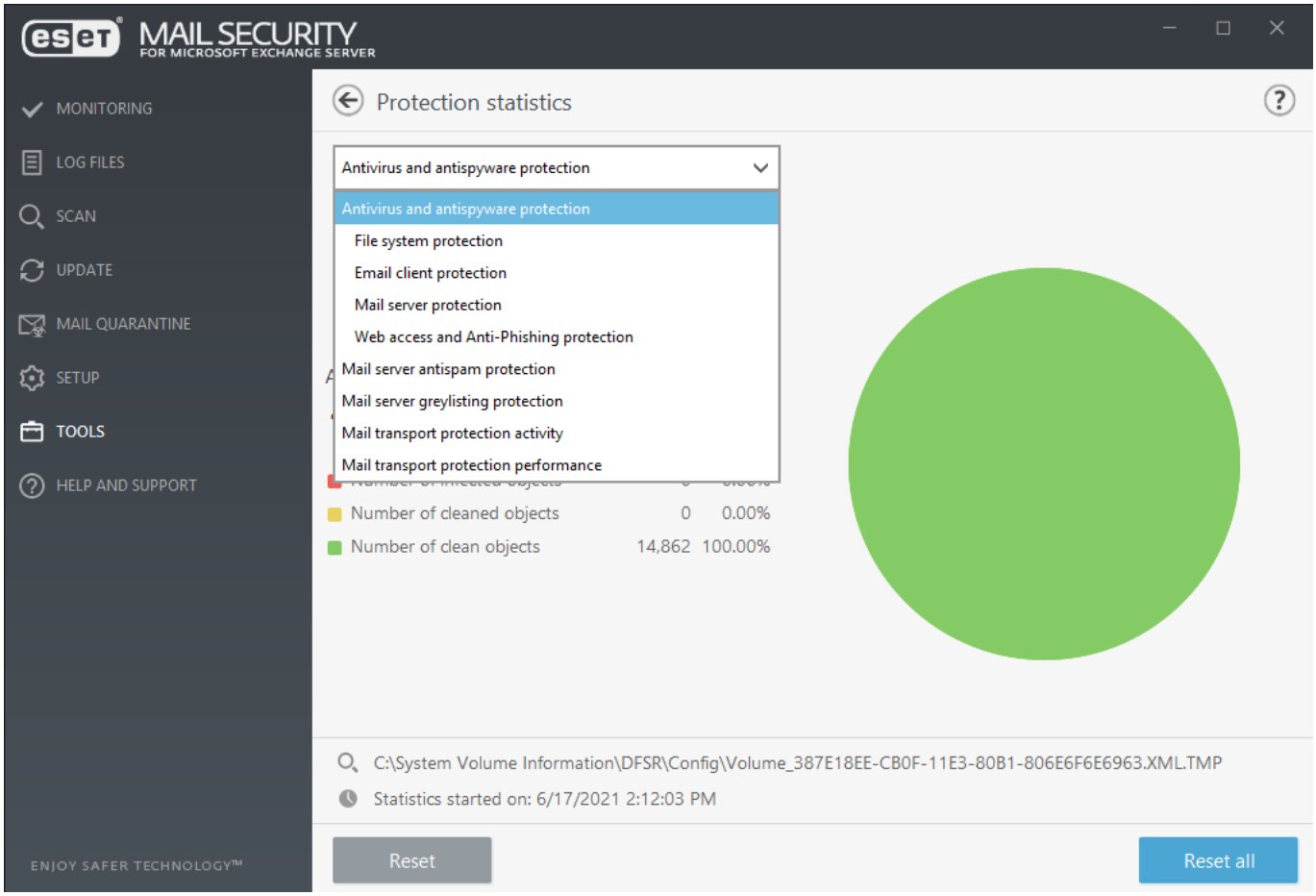
Na výber sú tieto možnosti:

1 sekunda	**Graf sa obnovuje každú sekundu, časová os zobrazuje posledných 10 minút.**
1 minúta (posledných 24 hodín)	Graf sa obnovuje každú minútu, časová os zobrazuje posledných 24 hodín.
1 hodina (posledný mesiac)	Graf sa obnovuje každú hodinu, časová os zobrazuje posledný mesiac.

Štatistiky ochrany

Ak chcete zobraziť štatistické údaje týkajúce sa modulov ochrany produktu ESET Mail Security, vyberte príslušný modul z roletového menu. Štatistiky obsahujú informácie, ako napr. počet všetkých skontrolovaných objektov, počet infikovaných objektov, počet vyliečených objektov a počet neinfikovaných objektov.

Po ponechaní kurzora na zvolenej položke umiestnenej vedľa grafu sa v danom grafe zobrazia len údaje pre konkrétnu položku. Ak chcete vynulovať štatistické údaje pre príslušný modul ochrany, kliknite na **Vynulovať**. Ak chcete vynulovať údaje pre všetky moduly, kliknite na **Vynulovať všetko**.



V ESET Mail Security sú dostupné tieto grafy:

Antivírusová a antispyvérová ochrana

Zobrazuje celkový počet infikovaných a vyliečených objektov.

Ochrana súborového systému

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

Ochrana Hyper-V

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

Ochrana e-mailových klientov

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

Ochrana prístupu na web a antiphishingová ochrana

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

Ochrana e-mailových serverov

Zobrazuje štatistiky antimalvérovej ochrany na e-mailovom serveri.

Antispamová ochrana e-mailových serverov

Zobrazuje históriu antispamových štatistík. Počet položiek označených ako Neskontrolované sa týka objektov vylúčených z kontroly (na základe pravidiel, interných správ, overených spojení atď.).

Greylistingová ochrana e-mailových serverov

Zobrazuje antispamové štatistiky vygenerované za pomoci metódy greylisting.

Aktivita ochrany prenosu e-mailov

Zobrazuje len tie objekty, ktoré boli overené/blokované/odstránené pomocou e-mailového servera.

Výkon ochrany prenosu e-mailov

Zobrazuje údaje spracované pomocou VSAPI/agenta prenosu v B/s.

Aktivita ochrany databáz e-mailových schránok

Zobrazuje objekty spracované pomocou VSAPI (počet overených objektov, objektov v karanténe a odstránených objektov).

Výkon ochrany databáz e-mailových schránok

Zobrazuje údaje spracované pomocou VSAPI (priemerné hodnoty pre aktuálny deň, za posledných 7 dní a od posledného vynulovania).

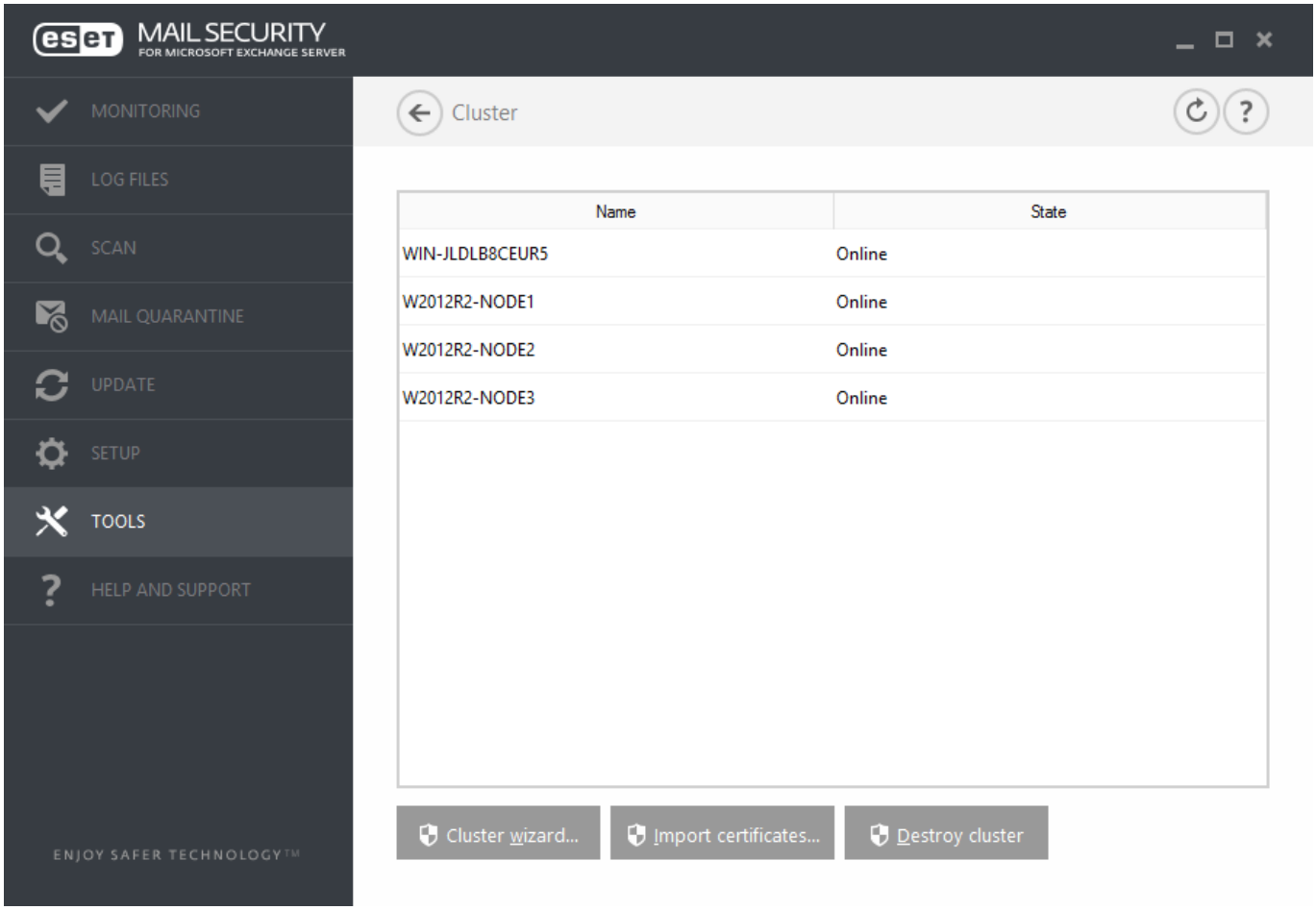
Klaster

Klaster ESET je komunikačná infraštruktúra založená na technológii Peer-to-Peer, určená pre produkty spoločnosti ESET pre servery typu Microsoft Windows Server. Klaster ESET je ideálne využiť v prípade, že máte vo svojej infraštruktúre Exchange viacero serverov, napr. v skupine DAG.

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

> Nastavenia používateľského rozhrania a naplánovaných úloh sa medzi uzlami klastra ESET nesynchronizujú. Toto správanie je zámerné. Predíde sa tak napríklad spusteniu plánovanej kontroly databáz na všetkých uzloch klastra v rovnakom čase, čo by spôsobilo nežiaduce problémy s výkonom.
> Protokoly ochrany e-mailových serverov sa pre každý uzol klastra uchovávajú zvlášť, a preto sa nesynchronizujú. Na každom uzle môžete použiť funkciu Exportovať na syslog server, aby sa protokoly duplikovali na Syslog server vo formáte CEF alebo ich bolo možné použiť s nástrojom SIEM. Prípadne môžete použiť funkciu Exportovať do protokolov aplikácií a služieb systému Windows, ak dávate prednosť zbieraniu protokolov odtiaľ.

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



Vytváranie klastra ESET medzi produktmi ESET Mail Security a ESET File Security for Linux nie je podporované.

Pri nastavovaní klastra sú dostupné dva spôsoby pridania uzlov:

- **Autodetekcia** – ak už máte klaster Windows Failover/NLB, autodetekcia automaticky pridá jeho uzly do klastra ESET.
- **Vybrať** – manuálne pridanie uzlov zadaním názvov serverov (z rovnakej pracovnej skupiny alebo domény)

Pri uvoľňovaní e-mailu z karantény ESET Mail Security ignoruje MIME hlavičku `To:` z dôvodu, že môže byť ľahko sfalšovaná. Namiesto toho sú použité informácie o pôvodnom príjemcovi z príkazu `RCPT TO:`, získané počas SMTP spojenia. Vďaka tomu sa zabezpečí, že e-mail, ktorý je uvoľnený z karantény, bude doručený správnemu príjemcovi.

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

- **Doména** – zadajte prihlasovacie údaje správcu domény.
- **Pracovná skupina** – zadajte prihlasovacie údaje lokálneho správcu a uistite sa, že daný účet existuje na všetkých uzloch.

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

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

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

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

Import certifikátov

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

Zrušenie klastra

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

Sprievodca konfiguráciou klastra – výber uzlov

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

Autodetekcia

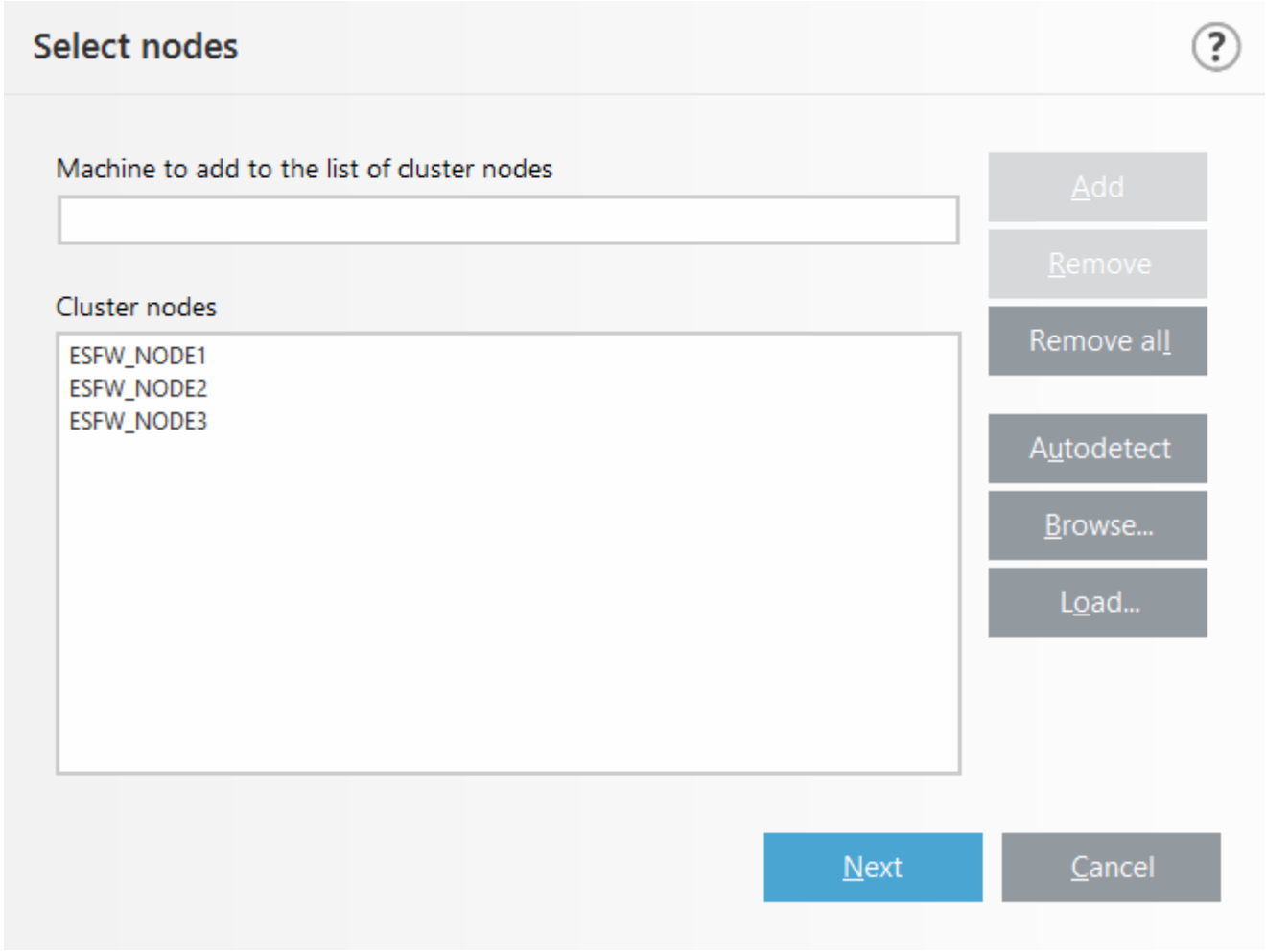
Autodetekcia automatický pridá uzly z existujúceho klastra Windows Failover Cluster/Network Load Balancing (NLB) Cluster. Server, ktorý používate na vytvorenie klastra ESET, musí byť členom daného klastra Windows Failover Cluster/NLB Cluster, aby bolo možné automatické pridanie uzlov. Klaster NLB musí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

Vybrať

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

Načítať

Táto možnosť slúži na import zoznamu uzlov zo súboru.



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

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

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

Sprievodca konfiguráciou klastra – nastavenie klastra

Zadajte názov klastra a v prípade potreby podrobnosti o sieti.

Názov klastra

Zadajte názov klastra a kliknite na Ďalej.

Načúvací port (predvolene 9777)

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

Otvoriť port vo firewalle systému Windows

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

Sprievodca konfiguráciou klastra – nastavenia inštalácie klastra

Definujte distribúciu certifikátov a inštaláciu produktov na uzly.

Distribúcia certifikátov

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

Inštalácia produktu na ostatné uzly

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

Doručiť licenciu k uzlom bez aktivovaného produktu

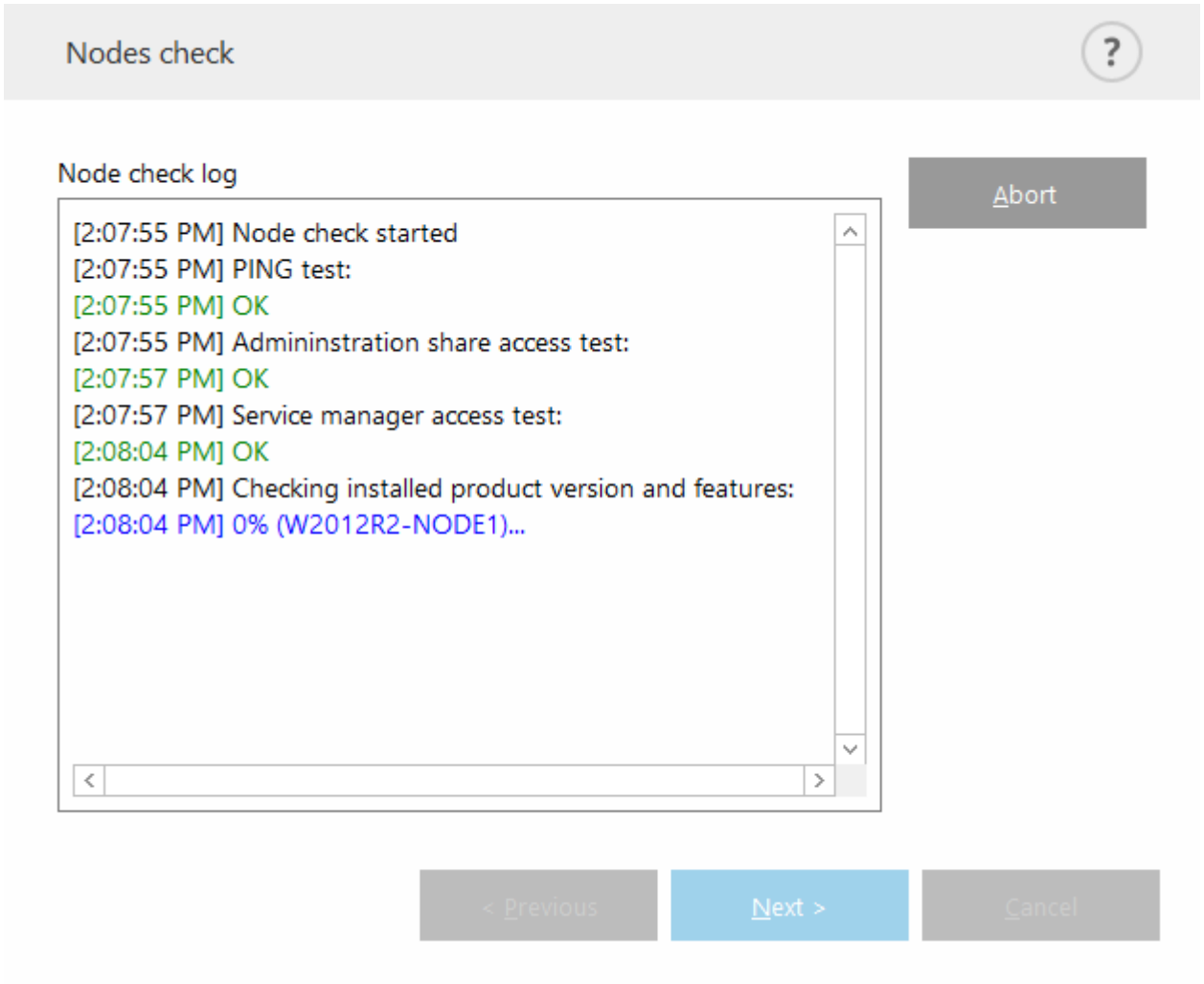
Túto možnosť je vhodné použiť v prípade, ak chcete, aby bol bezpečnostný produkt spoločnosti ESET inštalovaný na uzly klastra automaticky aktualizovaný.

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

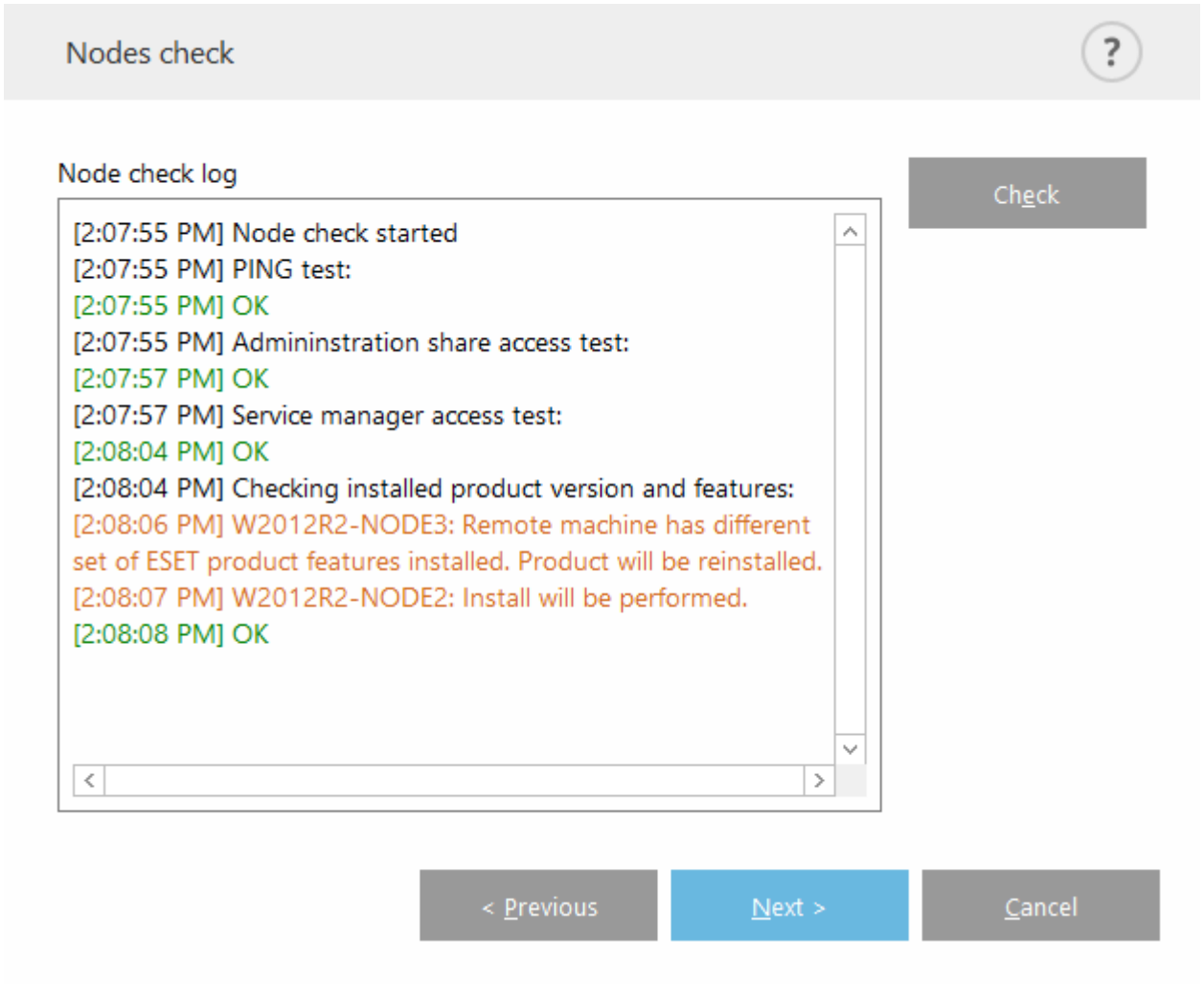
Sprievodca konfiguráciou klastra – kontrola uzlov

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

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

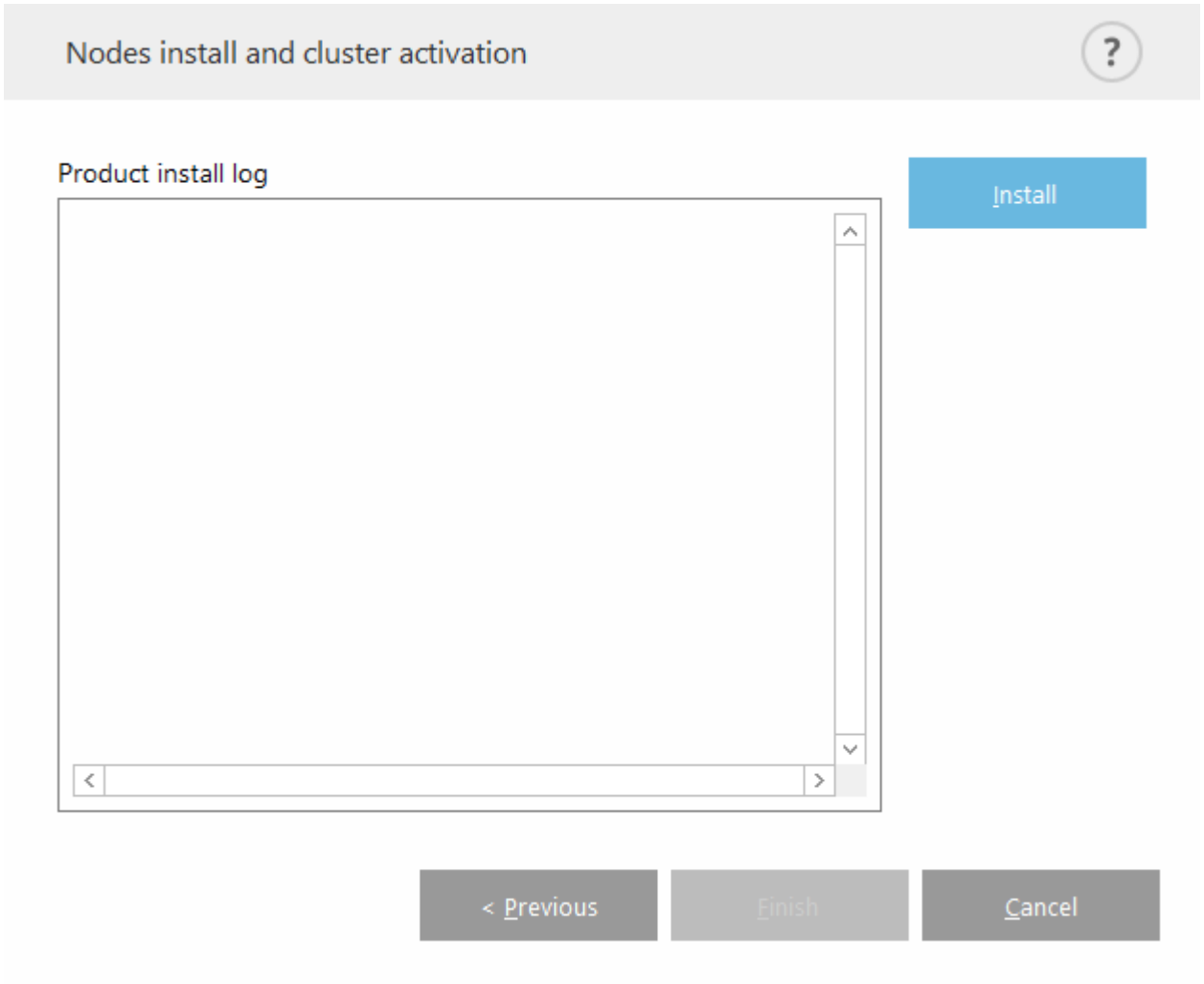


Po ukončení kontroly bude zobrazené hlásenie:

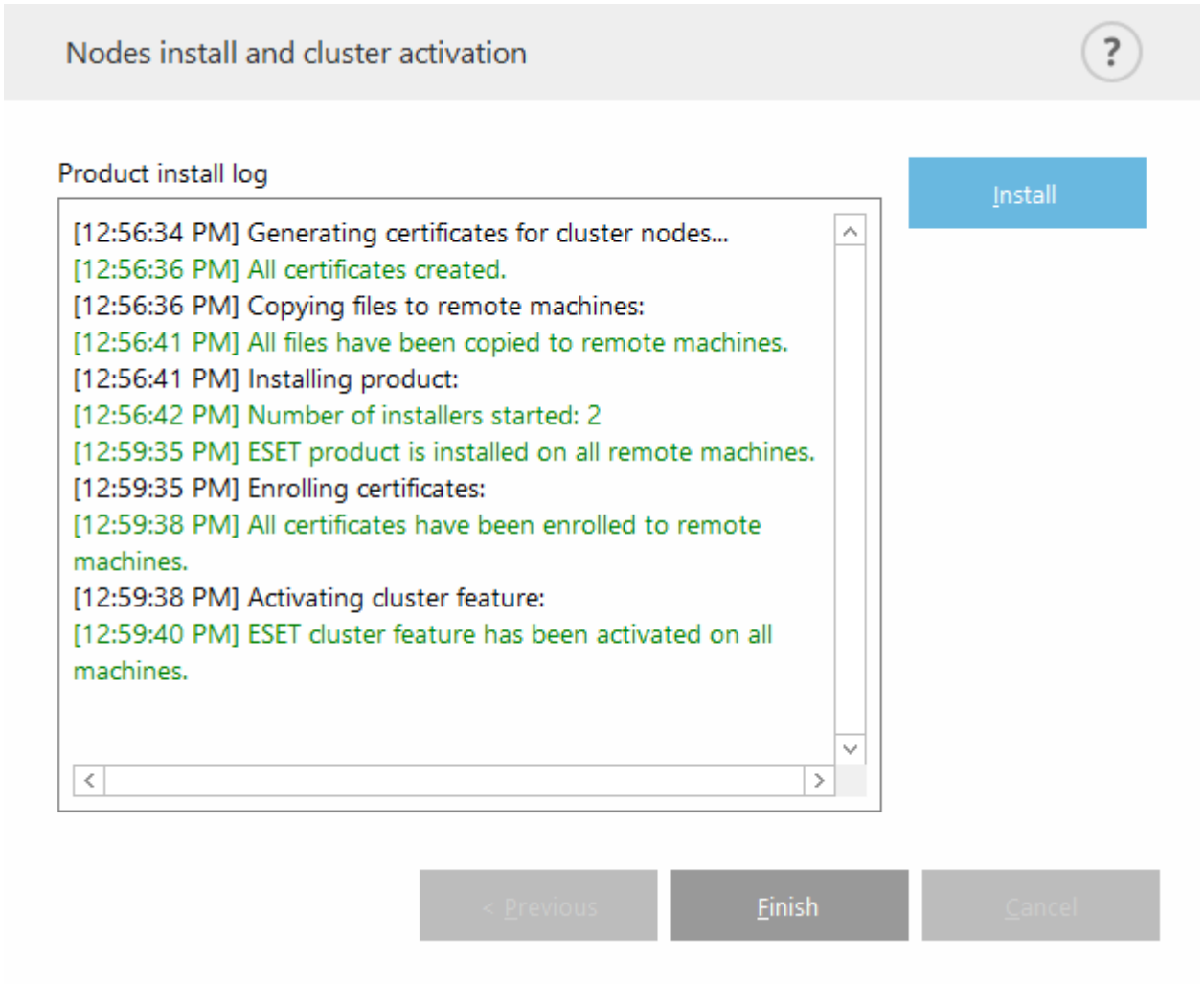


Sprievodca konfiguráciou klastra – inštalácia uzlov

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

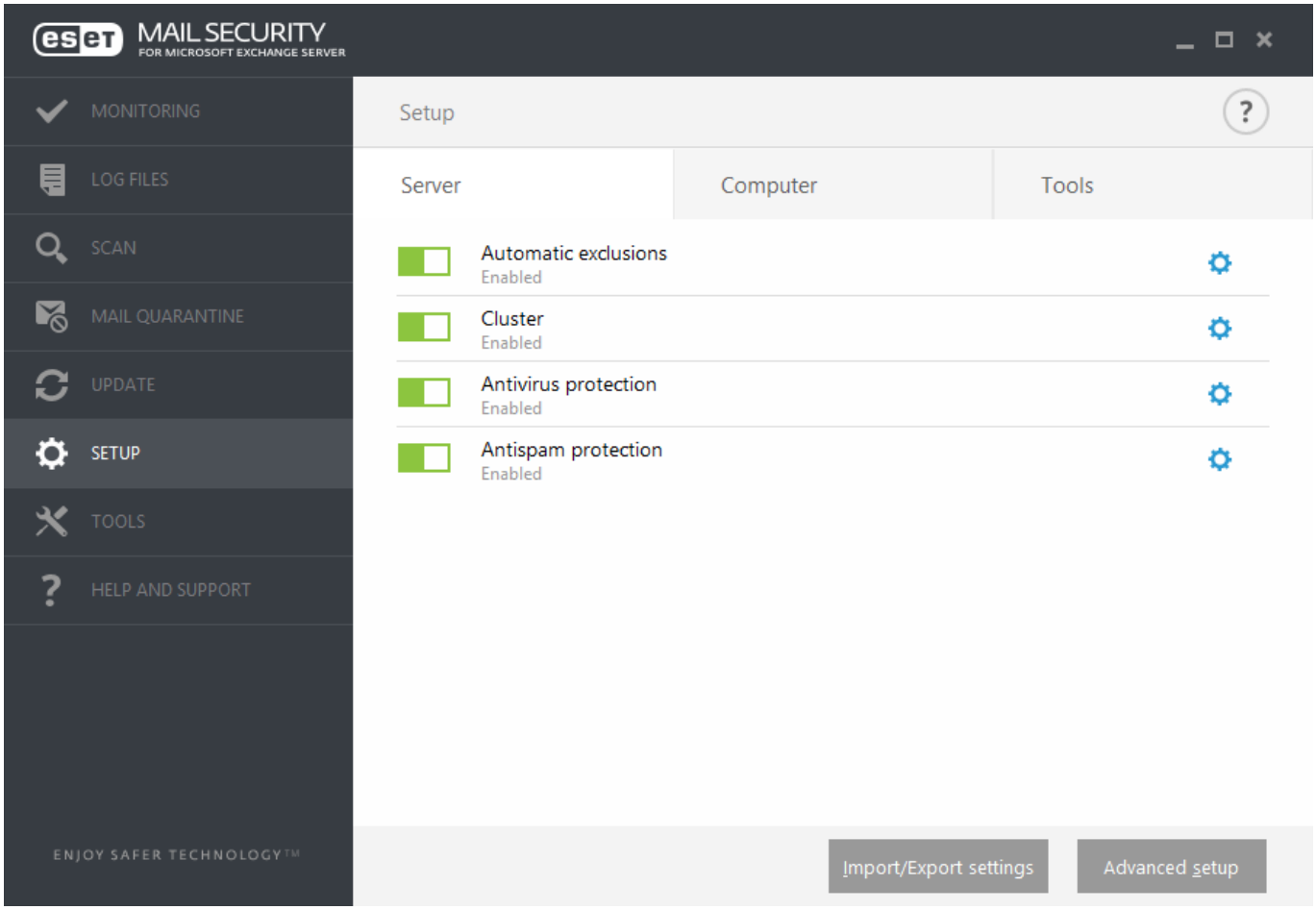


Pri vzdialenej automatickej inštalácii na uzol s rozdielnou architektúrou (32‑bitovým alebo 64‑bitovým operačným systémom) sa zobrazí výzva na vykonanie manuálnej inštalácie.



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

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



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

ESET Shell

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

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

Na zaistenie úplnej funkčnosti odporúčame otvoriť eShell cez možnosť Spustiť ako správca. To isté platí pre spúšťanie jednotlivých príkazov v príkazovom riadku Windows (cmd). Spustite príkazový riadok použitím možnosti Spustiť ako správca. Ak nespustíte príkazový riadok ako správca, nebudete môcť spúšťať príkazy z dôvodu nedostatočných oprávnení.

Existujú dva režimy, v ktorých je možné eShell spustiť:

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

2. **Spustenie jednotlivého príkazu/režim batch** – môžete ho použiť, ak potrebujete len spustiť príkaz bez vstupovania do interaktívneho režimu nástroja eShell. Stačí v príkazovom riadku Windows napísať `eshell` s

potrebnými parametrami.

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

Na spustenie niektorých príkazov (napr. druhý príklad uvedený vyššie) v režime batch/skript je potrebné najprv nakonfigurovať niekoľko nastavení. V opačnom prípade sa zobrazí hlásenie **Prístup odmietnutý**. Toto hlásenie sa zobrazí z bezpečnostných dôvodov.

ℹ Na povolenie príkazov eShell v príkazovom riadku systému Windows je potrebné vykonať zmeny v nastaveniach. Prečítajte si viac o spúšťaní dávkových súborov.

Existujú dva spôsoby vstúpenia do interaktívneho režimu v nástroji eShell:

1. Windows **Štart menu**: Štart > Všetky programy > ESET > ESET MAIL SECURITY > ESET Shell

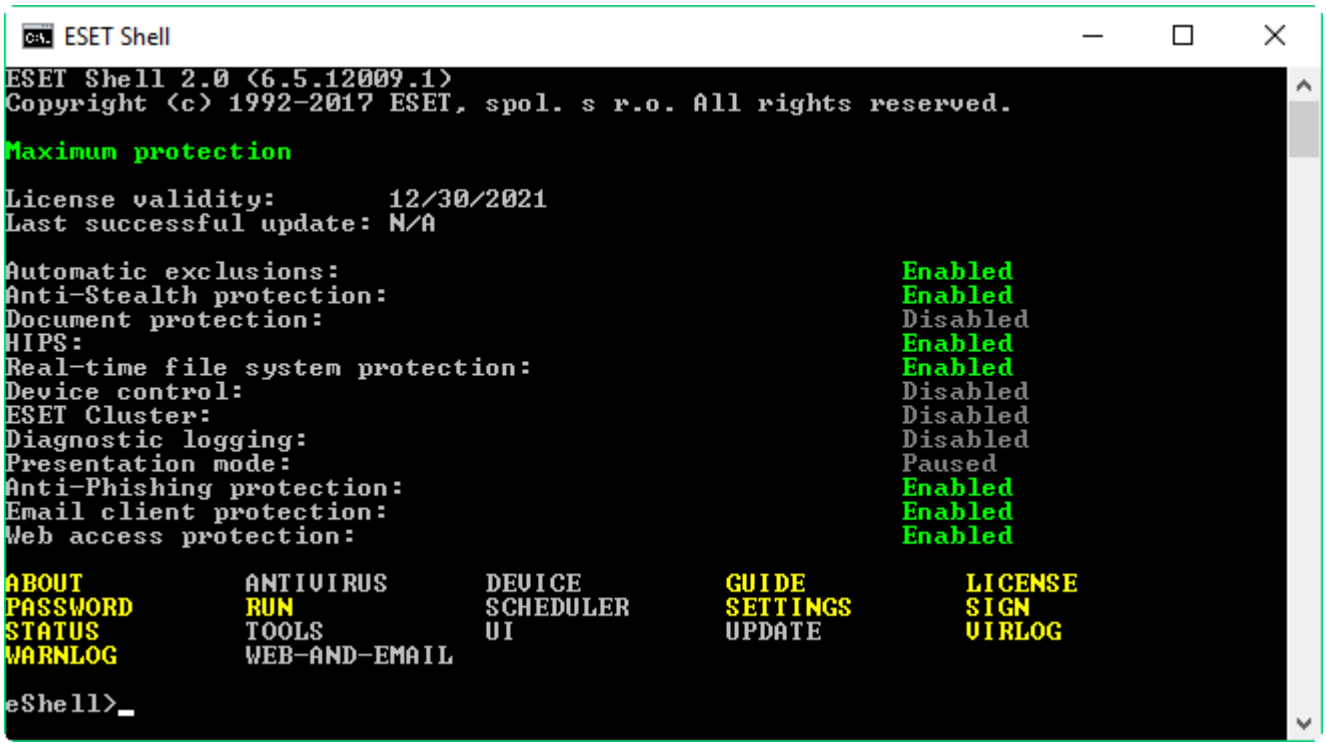
2. Pomocou **príkazového riadka Windows** napísaním `eshell` a stlačením klávesu Enter.

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

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

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

Po začatí novej relácie eShell sa zobrazí nasledujúca obrazovka:



> V príkazoch sa nerozlišujú veľké a malé písmená. Môžete používať veľké alebo malé písmená, nemá to vplyv na spustenie príkazu.

Prispôsobenie eShell

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

Použitie

Syntax

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

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

Príklad (tento príkaz aktivuje ochranu dokumentov):

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

`SET` – operácia (prefix)

`COMPUTER SCANS DOCUMENT` – cesta k danému príkazu, kontext príkazu

`REGISTER` – samotný príkaz

`ENABLED` – argument pre daný príkaz

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

SYNTAX:

```
[get] status
```

OPERÁCIE:

`get` – zobraziť stav všetkých modulov ochrany

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

> V príkazoch sa nerozlišujú veľké a malé písmená. Môžete používať veľké alebo malé písmená, nemá to vplyv na spustenie príkazu.

Operácia/prefix

Operácia alebo tzv. predpona (prefix) určuje, akú operáciu ma príkaz vykonať. Operácia `GET` vám poskytne informácie o tom, ako je určitá funkcia programu ESET Mail Security nakonfigurovaná, prípadne ukáže stav (napr. `GET COMPUTER REAL-TIME STATUS` vám ukáže momentálny stav Rezidentnej ochrany). Operácia `SET`

nakonfiguruje funkciu alebo zmení jej stav (`SET COMPUTER REAL-TIME STATUS ENABLED` aktivuje Rezidentnú ochranu).

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

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

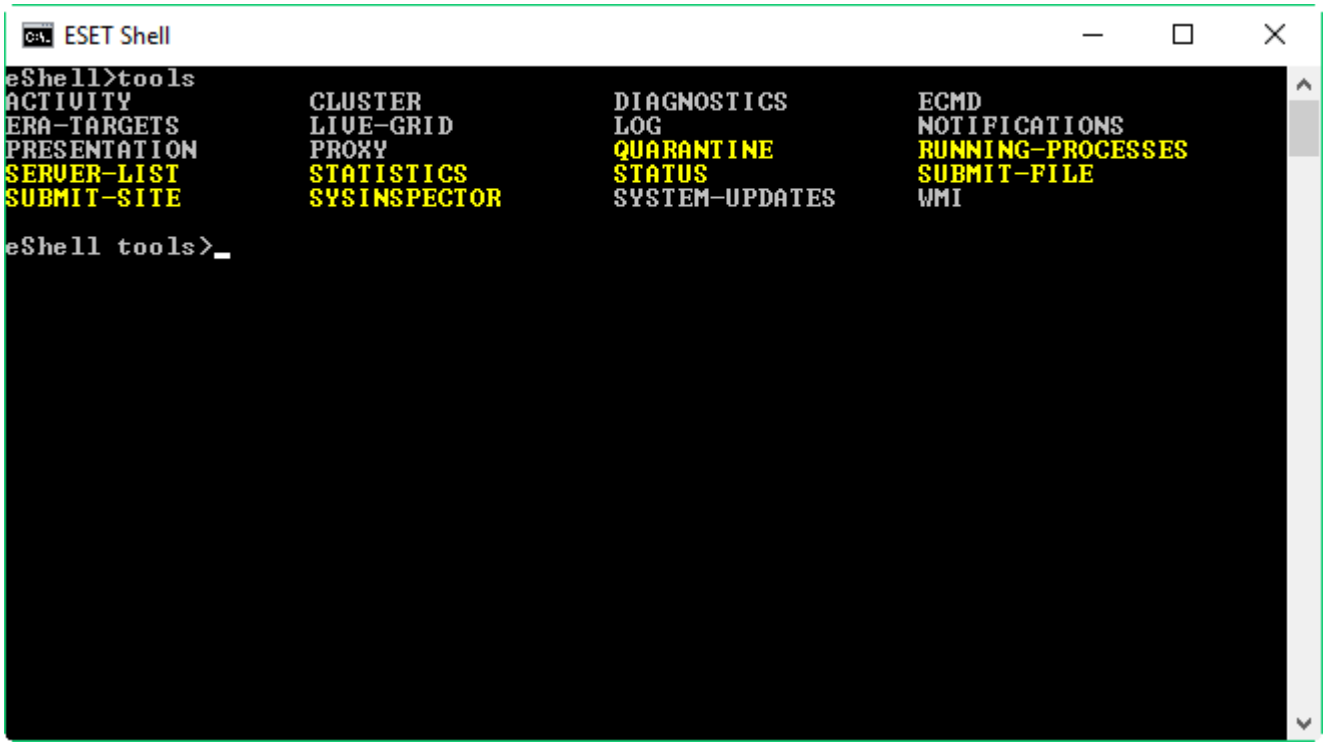
> Operácie ako `GET` a `SET` sa používajú s veľkým množstvom príkazov, avšak niektoré príkazy (napr. `EXIT`) nepoužívajú operáciu.

Cesta príkazu/kontext

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

```
eShell>
```

Príkaz môžete vykonať priamo odtiaľto alebo môžete zadať názov kontextu. Týmto spôsobom sa pohybujete v rámci stromovej štruktúry. Napríklad pri použití kontextu `TOOLS` sa zobrazia všetky príkazy a podkontexty, ktoré sú k dispozícii.



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

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

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

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

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

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

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

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

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

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

Argument

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

`rigorous` – vždy vyriešiť detekciu

`safe` – vyriešiť detekciu, a ak to nie je možné, ponechať ju

`normal` – vyriešiť detekciu, a ak to nie je možné, spýtať sa

`none` – vždy sa spýtať koncového používateľa

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

Skrátená forma príkazov

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

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

Príklady skrátenej formy:

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

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

```
eShell>a

The following command is not unique: a
```

V kontexte `COMPUTER` sú dostupné nasledujúce podkontexty:

`ADVANCED`

`AUTO-EXCLUSIONS`

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

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

Automatické dopĺňanie

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

Aliasy

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

`(global) close` – koniec

`(global) quit` – koniec

`(global) bye` – koniec

`warnlog` – protokol udalostí

`virlog` – protokol detekcií

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

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

Ochrana nastavení heslom

ESET Mail Security nastavenia môžu byť ochránené heslom. Heslo môžete nastaviť pomocou grafického rozhrania (GUI) alebo použitím nástroja eShell pomocou príkazu `set ui access lock-password`.

Toto heslo budete musieť zadať pre niektoré príkazy (napríklad pri zmene nastavení alebo zmene údajov). Ak plánujete pracovať s nástrojom eShell dlhší čas a nechcete opakovane zadávať heslo, môžete eShell nastaviť tak, aby si heslo zapamätal. Využite na to príkaz `set password` (spustením cez `root`). Heslo bude potom automaticky vyplnené pre všetky ďalšie príkazy, ktoré vyžadujú heslo. eShell si heslo zapamätá, až kým reláciu neukončíte. To znamená, že pri začatí novej relácie eShell bude nutné znova použiť príkaz `set password` na zapamätanie hesla.

Sprievodca/pomocník

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

História príkazov

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

CLS/vymazať obrazovku

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

EXIT/CLOSE/QUIT/BYE

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

Príkazy

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

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

Príklady príkazov (nachádzajú sa v koreňovom kontexte ROOT):

ABOUT

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

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

KONTEXT:

`root`

PASSWORD

Na spustenie príkazov chránených heslom musíte z bezpečnostných dôvodov zadať heslo. Týka sa to napríklad príkazov na vypnutie ochrany a príkazov, ktoré môžu ovplyvniť konfiguráciu produktu ESET Mail Security. Pri každom spustení takéhoto príkazu budete vyzvaný na zadanie hesla. Toto heslo môžete definovať, aby ste ho nemuseli vždy zadávať. eShell si heslo zapamätá a pri spustení príkazu chráneného heslom ho automaticky vloží na príslušné miesto.

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

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

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

Takýto zreťazený príkaz definuje heslo a vypína ochranu.

Odporúčame, aby ste používali podpísané dávkové súbory vždy, keď je to možné. Vyhnete sa tak tomu, že budete mať v dávkovom súbore heslá v podobe obyčajného textu (pri použití metódy popísanej vyššie). Viac informácií nájdete v kapitole Dávkové súbory/skriptovanie (sekcia Podpísané dávkové súbory).

KONTEXT:

`root`

SYNTAX:

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

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

OPERÁCIE:

`get` – zobrazí heslo

`set` – nastaví alebo zmaže heslo

`restore` – zruší heslo

ARGUMENTY:

`plain` – zadanie hesla ako parametra

`password` – heslo

PRÍKLADY:

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

`restore password` – zruší heslo

PRÍKLADY:

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

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

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

STATUS

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

KONTEXT:

```
computer real-time
```

SYNTAX:

```
[get] status
```

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

```
restore status
```

OPERÁCIE:

`get` – vráti aktuálne nastavenie/stav

`set` – nastaví hodnotu/stav

`restore` – obnoví pôvodné nastavenia/objekt/súbor

ARGUMENTY:

`enabled` – zapne ochranu/funkciu

`disabled` – vypne ochranu/funkciu

`10m` – vypne na 10 minút

`30m` – vypne na 30 minút

`1h` – vypne na 1 hodinu

`4h` – vypne na 4 hodiny

`temporary` – vypne do reštartu

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

Zoznam funkcií s príkazom `status`:

Funkcia	Kontext a príkaz
Automatické vylúčenia	`COMPUTER AUTO-EXCLUSIONS STATUS`
Host Intrusion Prevention System (HIPS)	`COMPUTER HIPS STATUS`
Rezidentná ochrana súborového systému	`COMPUTER REAL-TIME STATUS`
Správa zariadení	`DEVICE STATUS`
Ochrana pred botnetmi	`NETWORK ADVANCED STATUS-BOTNET`

Funkcia	Kontext a príkaz
Ochrana pred sieťovými útokmi (IDS)	`NETWORK ADVANCED STATUS-IDS`
Izolácia od siete	`NETWORK ADVANCED STATUS-ISOLATION`
Klaster ESET	`TOOLS CLUSTER STATUS`
Diagnostické zapisovanie do protokolu	`TOOLS DIAGNOSTICS STATUS`
Prezentačný režim	`TOOLS PRESENTATION STATUS`
Antiphishingová ochrana	`WEB-AND-EMAIL ANTIPHISHING STATUS`
Ochrana e-mailových klientov	`WEB-AND-EMAIL MAIL-CLIENT STATUS`
Ochrana prístupu na web	`WEB-AND-EMAIL WEB-ACCESS STATUS`

VIRLOG

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

WARNLOG

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

Dávkové súbory/skriptovanie

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

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

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

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

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

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

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

Podpísané dávkové súbory

eShell umožňuje zabezpečiť bežné dávkové súbory (**.bat*) podpisom. Skripty sú podpísané rovnakým heslom, aké je použité na ochranu nastavení. Aby bolo možné skript podpísať, je potrebné najprv povoliť ochranu nastavení heslom. Môžete tak urobiť v hlavnom okne programu alebo v rámci nástroja eShell pomocou príkazu `set ui`

`access lock-password`. Po nastavení hesla môžete začať podpisovať dávkové súbory.

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

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

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

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

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

Script.bat je cesta k batch súboru.

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

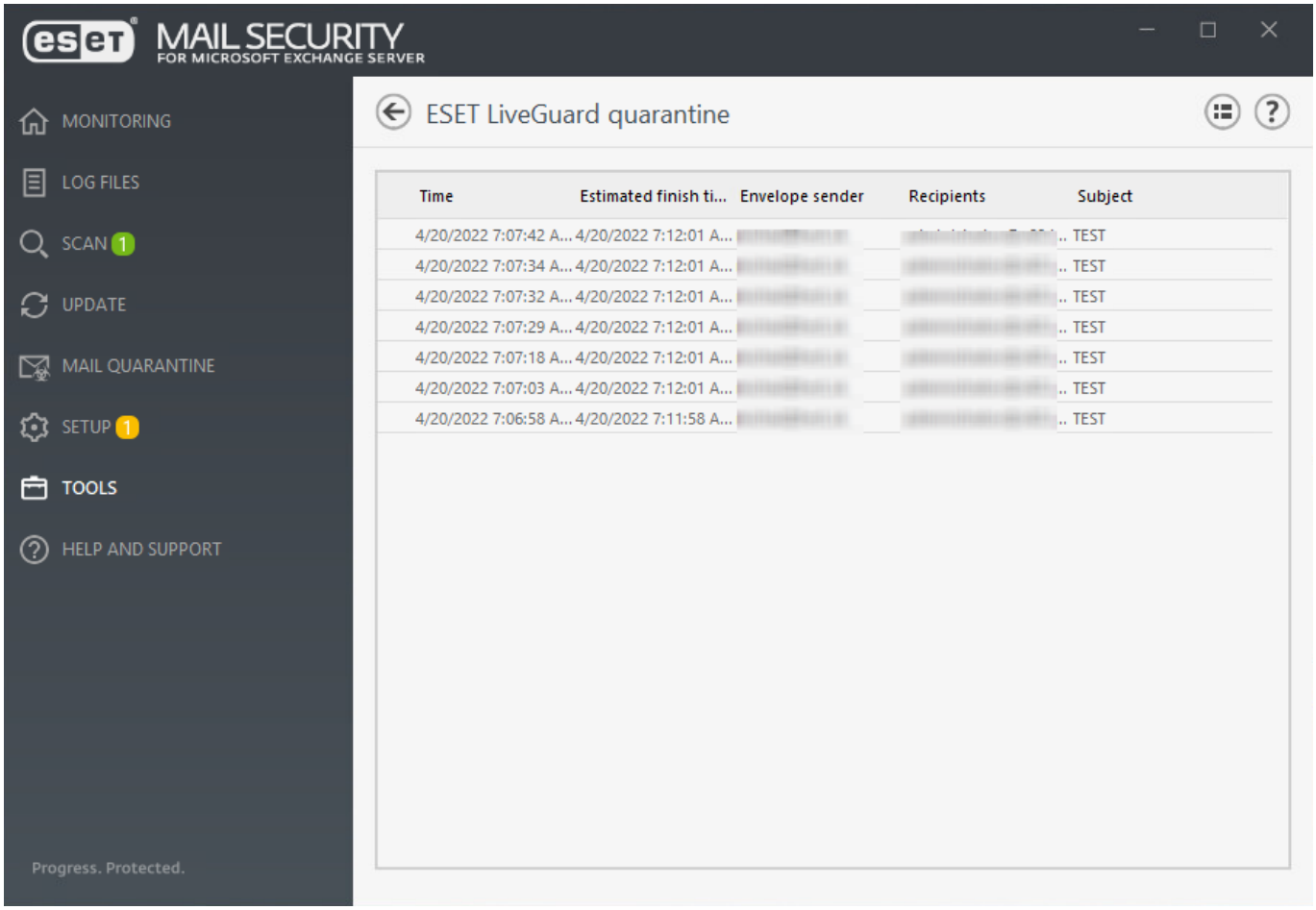
ESET LiveGuard Advanced

ESET LiveGuard Advanced poskytuje ďalšiu vrstvu ochrany prostredníctvom pokročilej cloudovej technológie ESET umožňujúcej detekciu novoobjavených druhov hrozieb. Ide o platenú službu, ktorá je svojou funkčnosťou podobná službe ESET LiveGrid®. Vďaka technológii ESET LiveGuard Advanced získate ochranu pred možnými následkami spôsobenými novými druhmi hrozieb. V prípade, že ESET LiveGuard Advanced identifikuje podozrivý kód alebo správanie konkrétneho objektu, zabráni ďalšej nebezpečnej aktivite tým, že daný objekt dočasne presunie do ESET LiveGuard Advanced karantény.

Podozrivá vzorka (napr. súbor alebo e-mailová správa) je zároveň automaticky odoslaná do ESET cloudu, kde ESET LiveGuard Advanced server vykoná jej analýzu pomocou pokročilých techník detekcie. Kým sú podozrivé súbory umiestnené v ESET LiveGuard Advanced karanténe, ESET Mail Security čaká na výsledky analýzy z ESET LiveGuard Advanced servera.

Po vykonaní analýzy váš produkt ESET Mail Security dostane správu obsahujúcu súhrn zistení o aktivite danej vzorky. Ak sa ukáže, že vzorka nie je nijakým spôsobom škodlivá, dôjde k jej uvoľneniu z ESET LiveGuard Advanced karantény. V opačnom prípade bude v karanténe ponechaná. Ak ide o nesprávne detegovaný objekt a ste si istý, že súbor alebo e-mailová správa nepredstavuje žiadnu hrozbu, môžete daný objekt manuálne uvoľniť z ESET LiveGuard Advanced karantény predtým, ako ESET Mail Security dostane výsledky analýzy z ESET LiveGuard Advanced servera.

Čo sa týka e-mailových správ, ESET LiveGuard Advanced server zvyčajne odošle výsledky analýzy vzoriek po niekoľkých minútach. Predvolená doba čakania je však nastavená na 5 minút. V ojedinelých prípadoch sa môže stať, že výsledky z ESET LiveGuard Advanced nie sú doručené v rámci stanoveného intervalu. V takomto prípade je správa uvoľnená z karantény. Predvolený interval je možné zmeniť podľa potreby v rozmedzí od 5 do 60 minút, pričom minimálna hodnota, s ktorou je možné pracovať, je 1 minúta.



Funkcia ESET LiveGuard Advanced sa zobrazuje v ESET Mail Security bez ohľadu na to, či je aktivovaná. Ak nemáte potrebnú licenciu, ESET LiveGuard Advanced nebude fungovať. Licencia pre ESET LiveGuard Advanced je spravovaná prostredníctvom nástroja ESET PROTECT a samotná aktivácia musí byť vykonaná z nástroja ESET PROTECT pomocou politiky.

Po úspešnej aktivácii ESET LiveGuard Advanced vám bude na ESET LiveGuard Advanced serveri vytvorený váš vlastný ESET LiveGuard Advanced profil. V tomto profile budú uložené všetky výsledky analýz vzoriek z ESET LiveGuard Advanced, ktoré boli odoslané prostredníctvom ESET Mail Security.

Pre fungovanie ESET LiveGuard Advanced je potrebné splniť nasledujúce podmienky:

Produkt ESET Mail Security musí byť spravovaný pomocou nástroja ESET PROTECT.

Produkt ESET Mail Security musí byť aktivovaný pomocou licencie ESET LiveGuard Advanced.

Je potrebné povoliť ESET LiveGuard Advanced v produkte ESET Mail Security pomocou politiky ESET PROTECT.

Po splnení týchto požiadaviek budete mať prístup k všetkým výhodám technológie ESET LiveGuard Advanced vrátane možnosti manuálneho odosielania vzoriek do ESET LiveGuard Advanced na účely analýzy.

ESET SysInspector

ESET SysInspector je aplikácia slúžiaca na dôkladné preskúmanie stavu vášho počítača, ktorá je schopná zhromažďovať údaje o nainštalovaných ovládačoch a programoch, sieťových pripojeniach či údaje z databázy registrov systému a zobraziť ich v jednoduchej čitateľnej forme.

Tieto informácie vám môžu pomôcť zistiť príčiny podozrivého správania systému, či už vplyvom nekompatibility, alebo infekcie škodlivého kódu.

Kliknite na **Vytvoriť** a napíšte stručný **Komentár** popisujúci vytváraný protokol. Počkajte, kým ESET SysInspector vytvorí protokol (kým jeho stav nebude zobrazený ako „Vytvorený“). Vytváranie protokolu môže určitý čas trvať v závislosti od konfigurácie hardvéru a systémových údajov.

V okne ESET SysInspector sa nachádzajú informácie o vytvorených protokoloch:

- **Čas** – čas vytvorenia.
- **Komentár** – stručný komentár.
- **Používateľ** – meno používateľa, ktorý vytvoril protokol.
- **Stav** – stav vytvorenia protokolu.

Sú dostupné tieto akcie:

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

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

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

ESET SysRescue Live

ESET SysRescue Live je bezplatný nástroj, ktorý umožňuje vytvoriť spúšťací disk CD/DVD alebo USB. Spustenie infikovaného počítača z takto vytvoreného záchranného média vám poskytuje možnosť skontrolovať počítač

na prítomnosť malvéru a liečiť infikované súbory.

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

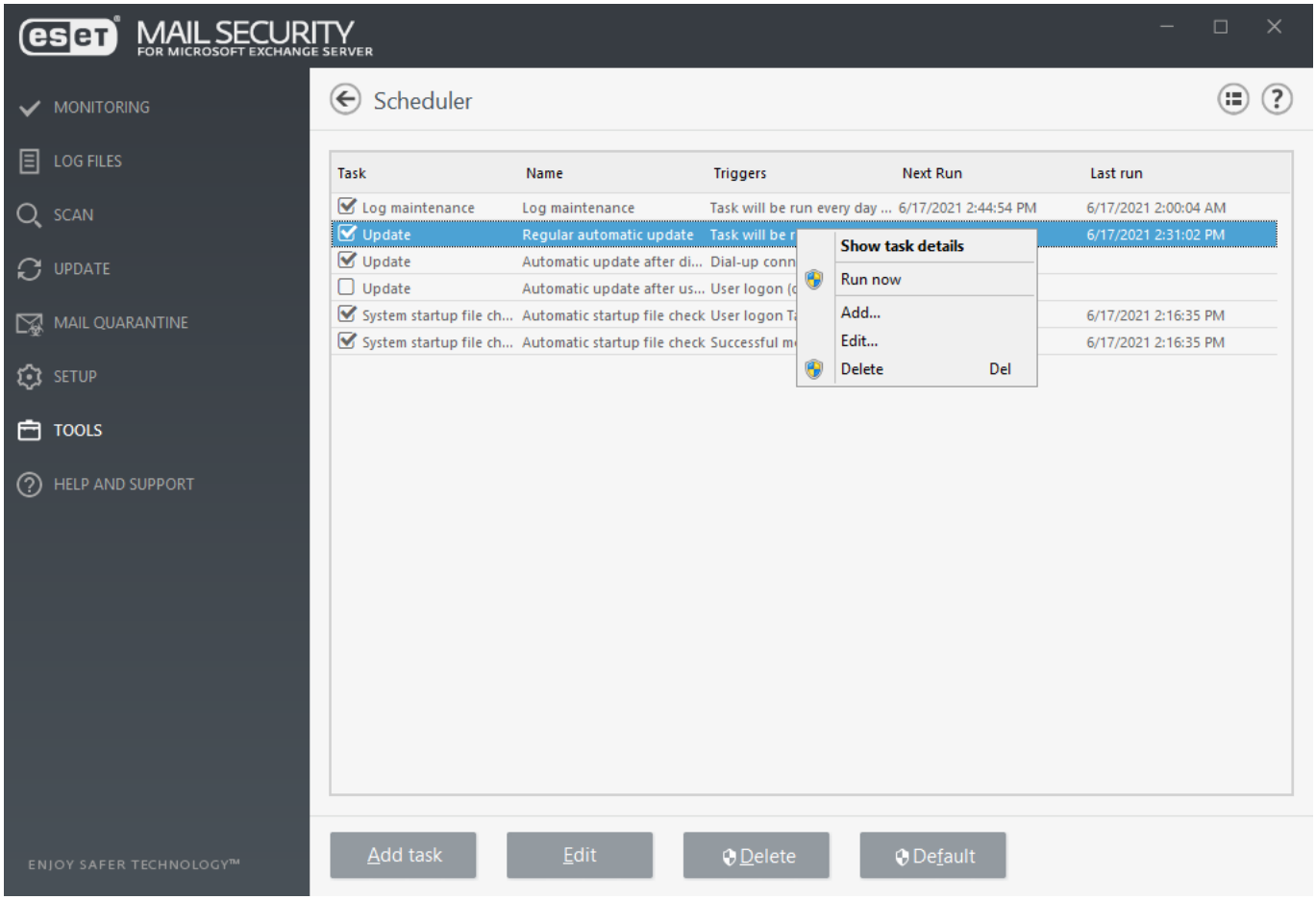
Plánovač

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

K dispozícii je tento súbor preddefinovaných úloh:

- Údržba protokolov
- Pravidelná automatická aktualizácia (túto úlohu môžete použiť na zmenu intervalu aktualizácie)
- Automatická aktualizácia po modemovom pripojení
- Automatická aktualizácia po prihlásení používateľa
- Kontrola súborov spúšťaných pri štarte počítača (po prihlásení používateľa)
- Kontrola súborov spúšťaných pri štarte počítača (po úspešnej aktualizácii modulov)

Aktivovať alebo deaktivovať úlohy môžete pomocou začiarkavacích políčok.



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

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

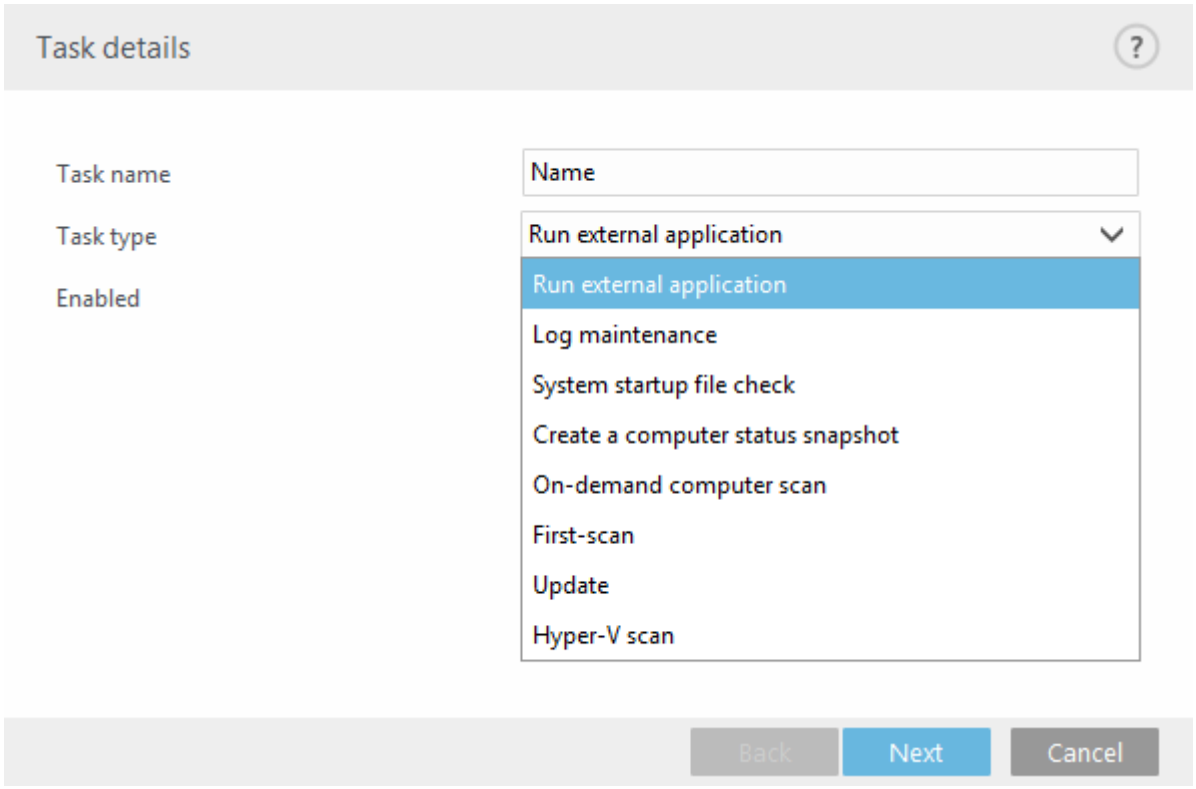
Plánovač – pridanie úlohy

Konfigurácia novej úlohy:

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

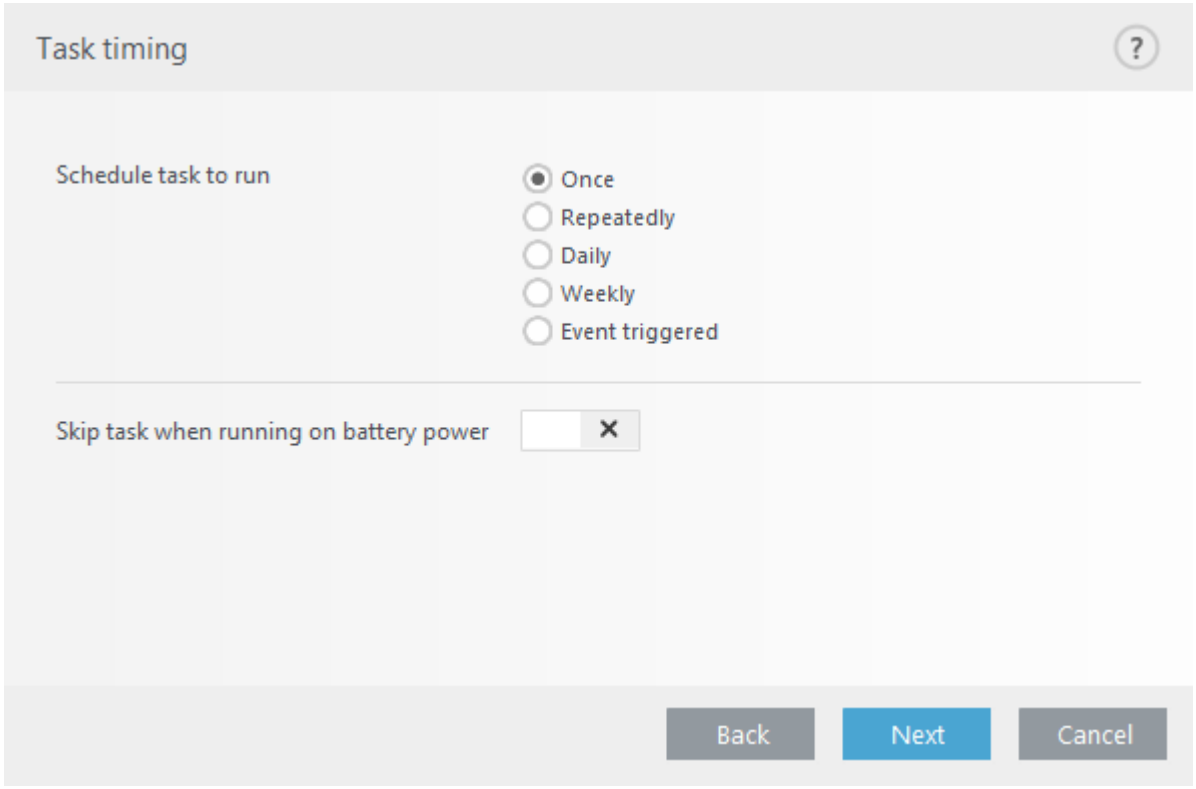
2. Zadajte **Názov úlohy** a nakonfigurujte si svoju vlastnú plánovanú úlohu.

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

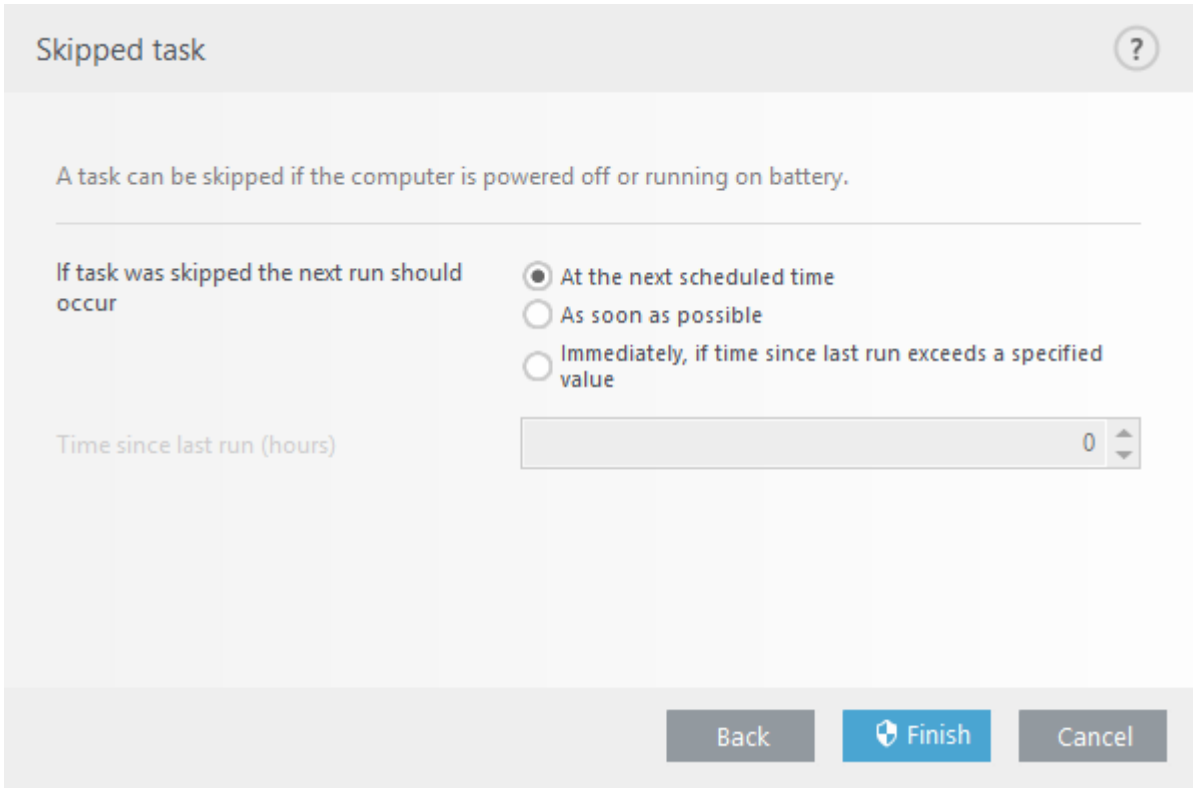


Ak chcete úlohu deaktivovať, kliknite na tlačidlo vedľa možnosti **Zapnuté**. Úlohu môžete aktivovať neskôr pomocou začiarkavacieho políčka v okne Plánovača.

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



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



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

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

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

Nová naplánovaná úloha sa zobrazí v okne Plánovača.

Typ úlohy

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

- **Spustenie externej aplikácie** – umožňuje naplánovať spustenie externej aplikácie.
- **Údržba protokolov** – protokoly obsahujú aj zvyšky odstránených záznamov. Táto úloha pravidelne optimalizuje záznamy v protokoloch, aby sa zefektívnila práca s nimi.
- **Kontrola súborov spúšťaných po štarte** – kontroluje súbory, ktoré sa spúšťajú pri štarte alebo prihlásení do systému.
- **Vytvorenie záznamu o stave počítača** – ide o snímku stavu počítača vytvorenú nástrojom ESET SysInspector, ktorá slúži na zhromažďovanie podrobných informácií o systémových súčastiach (napr. ovládače, aplikácie) a posudzuje úroveň rizika každej súčasti.
- **Manuálna kontrola počítača** – vykoná manuálnu kontrolu diskov, jednotlivých priečinkov a súborov v počítači.

• **Aktualizácia** – zabezpečuje aktualizáciu detekčného jadra, ako aj aktualizáciu všetkých programových modulov.

• **Kontrola databáz e□mailových schránok** – umožňuje vám nastaviť kontrolu databáz a vybrať položky, ktoré budú kontrolované. Ide v podstate o Manuálnu kontrolu databáz.

> Ak máte povolenú Ochranu databáz e□mailových schránok, môžete stále naplánovať túto úlohu, avšak v hlavnom okne programu v sekcii Kontrola sa zobrazí chybové hlásenie „Kontrola databáz e□mailových schránok – Vyskytla sa chyba a kontrola bola prerušená“. Aby ste tomuto predišli, je potrebné sa ubezpečiť, že Ochrana databáz e-mailových je vypnutá v čase, na kedy je naplánovaná Kontrola databáz e-mailových schránok.

• **Odosielať reporty o e□mailovej karanténe** – naplánuje odoslanie reportu o e□mailovej karanténe prostredníctvom e□mailu.

• **Odosielať správcovské reporty o e□mailovej karanténe** – naplánuje odoslanie reportu o e□mailovej karanténe prostredníctvom e□mailu.

• **Kontrola na pozadí** – v prípade potreby umožní Exchange serveru vykonať kontrolu databáz na pozadí.

• **Kontrola Hyper□V** – umožňuje vám nastaviť kontrolu virtuálnych diskov v rámci Hyper□V.

• **Kontrola databáz Office 365** – umožňuje vám nastaviť kontrolu v rámci hybridných prostredí Office 365.

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

Načasovanie úlohy

Vyberte si jednu z nasledujúcich možností načasovania úlohy:

• **Raz** – úloha sa vykoná iba raz v presne určený dátum a čas. Umožní vykonať úlohu iba raz v stanovenom čase. V okne **Vykonanie úlohy** zadajte dátum a čas vykonania úlohy.

• **Opakovane** – úloha sa bude vykonávať opakovane v určenom časovom intervale (v minútach). V okne **Vykonanie úlohy** zadajte čas, kedy bude úloha vykonaná každý deň.

• **Denne** – úloha sa bude vykonávať opakovane každý deň v určenom čase.

• **Týždenne** – Úloha sa bude vykonávať týždenne v určité dni a v určený čas. Umožní vykonávať úlohu opakovane v konkrétnych dňoch týždňa počnúc stanoveným dňom a časom. Do poľa Čas vykonania úlohy zadajte čas spustenia. Zvoľte deň alebo dni v týždni, kedy má byť úloha spustená.

• Pri udalosti – Úloha sa bude vykonávať po určenej udalosti.

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

Pri udalosti

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

Úlohu môžu spustiť tieto udalosti:

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

Spustenie aplikácie

Táto úloha naplánuje spustenie externej aplikácie.

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

Vynechaná úloha

V prípade, že sa naplánovanú úlohu nepodarí spustiť v určenom čase, môžete nastaviť, kedy má nastať ďalšie spustenie úlohy:

- **V najbližšom naplánovanom čase** – úloha sa vykoná v konkrétny čas po uplynutí určitej doby (napr. 24 hodín).
- **Hneď ako to bude možné** – úloha sa vykoná okamžite alebo hneď po odstránení problémov, ktoré bránili spusteniu danej úlohy.
- **Okamžite, ak od posledného spustenia uplynul stanovený časový interval** – nastavte Čas od posledného spustenia (v hodinách). Po zvolení tejto možnosti sa bude daná úloha vždy opakovať po uplynutí určitej doby (v hodinách).

Informácie o naplánovanej úlohe

Toto dialógové okno obsahuje podrobné informácie o naplánovanej úlohe. Zobrazuje sa po dvojitom kliknutí na úlohu v okne **Plánovač** alebo po kliknutí pravým tlačidlom myši a vybratí možnosti **Zobraziť podrobnosti**.

Odoslanie vzorky na analýzu

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

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

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

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

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

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

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

Súbor/Stránka

Cesta k súboru alebo webovej stránke, ktorú chcete odoslať.

Kontaktný e-mail

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

Odoslať anonymne

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

Podozrivý súbor

Spozorované príznaky a správanie malvéru

Opíšte správanie podozrivého súboru v počítači.

Pôvod súboru (URL adresa alebo výrobca aplikácie)

Uveďte pôvod súboru (zdroj) a ako ste sa k danému súboru dostali.

Poznámky a dodatočné informácie

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

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

Podozrivá stránka

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

Infikovaná stránka

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

Phishing

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

Podvodná stránka

Podvodná, zavádzajúca webová stránka.

Iné

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

Poznámky a dodatočné informácie

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

Nesprávne detegovaný súbor

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

konkrétneho súboru zhoduje so vzorom obsiahnutým v detekčnom jadre.

> Prvé tri parametre sú povinné z dôvodu lepšej identifikácie legitímnej aplikácie a jej odlíšenia od škodlivého kódu. Poskytnutím doplňujúcich informácií pomôžete významnou mierou našim laboratóriám pri identifikácii a spracovaní vzoriek.

Názov a verzia aplikácie

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

Pôvod súboru (URL adresa alebo výrobca aplikácie)

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

Účel aplikácie

Uveďte účel a typ aplikácie (napr. prehliadač, prehrávač médií atď.) pre rýchlejšie zaradenie a identifikáciu.

Poznámky a dodatočné informácie

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

Nesprávne detegovaná stránka

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

Poznámky a dodatočné informácie

Môžete uviesť ďalšie informácie, ktoré by mohli pomôcť pri spracovaní podozrivého súboru.

Iné

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

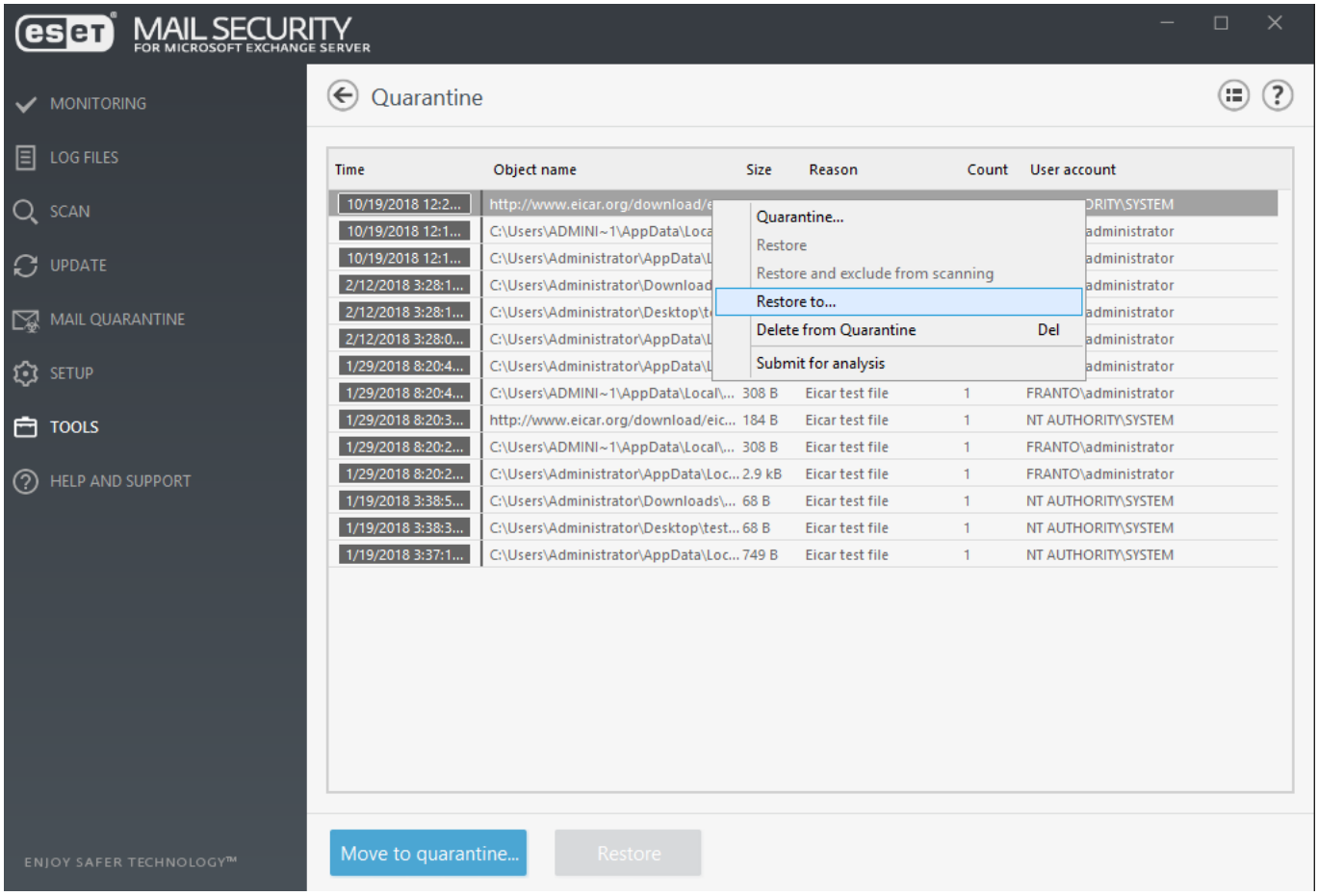
Dôvod odoslania súboru

Uveďte dôvod odoslania súboru a čo najpresnejší popis súboru.

Karanténa

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

antimalvérovým skenerom. Súbory z karantény môžu byť zaslané na analýzu do vírusového laboratória spoločnosti ESET.



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

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

Pridávanie súborov do karantény

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

Obnovenie z karantény

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

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

Poslanie na analýzu

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

Odstránenie objektu z karantény

Kliknite pravým tlačidlom na položku v karanténe a vyberte možnosť **Odstrániť z karantény** alebo stlačte kláves **Delete**.

Nastavenia ochrany servera

Ide o hlavnú možnosť integrácie. Pomocou prepínača môžete zapnúť alebo vypnúť integráciu Ochrany databáz e-mailových schránok, Ochrany prenosu e-mailov alebo podpisovania DKIM do svojho Exchange Servera. Po zapnutí si môžete nastaviť podrobnejšie nastavenia pre každý typ ochrany v sekcii jej určenej. Môžete taktiež upraviť prioritu agenta (uistite sa, že priorita ESET DKIM agenta bude na poslednom mieste).

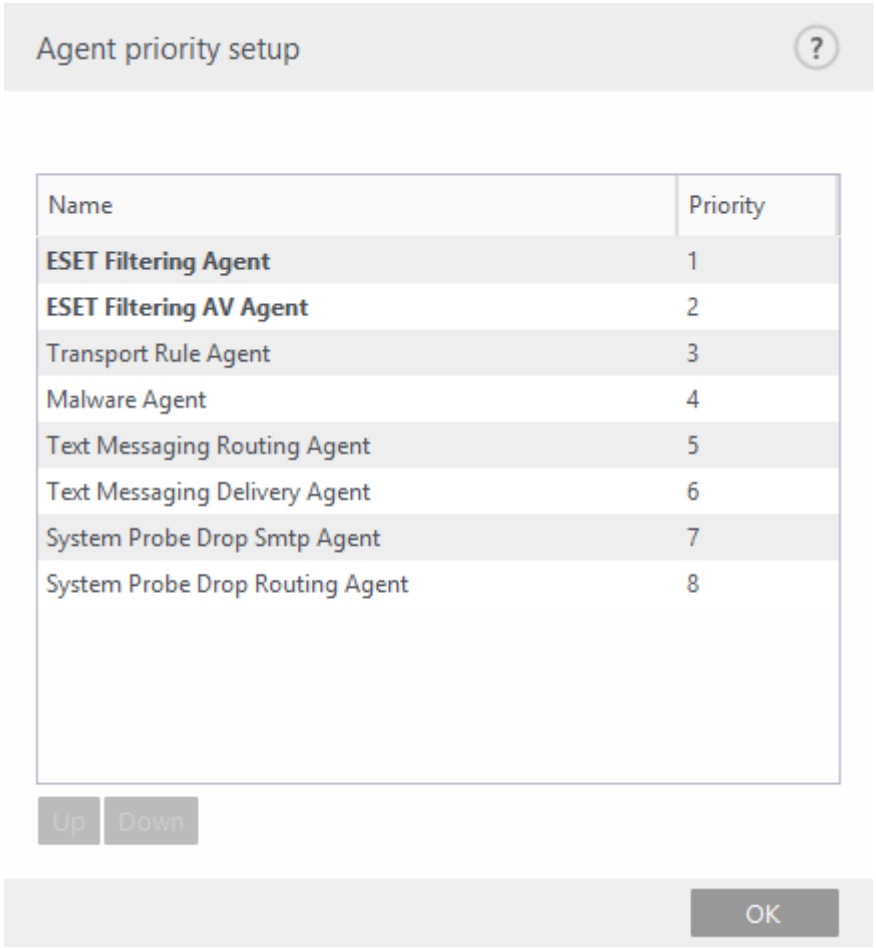
Ak používate Microsoft Exchange Server 2007 alebo 2010, môžete si vybrať medzi Ochranou databáz e-mailových schránok a Manuálnou kontrolou databáz e-mailových schránok, nie je však možné mať aktivované oba tieto typy ochrany súčasne. Ak sa rozhodnete pre Manuálnu kontrolu databáz e-mailových schránok, integrácia Ochrany databáz e-mailových schránok musí byť vypnutá. V opačnom prípade nebude Manuálna kontrola databáz e-mailových schránok dostupná.

ESET Mail Security zabezpečuje ochranu pre váš Microsoft Exchange Server pomocou nasledujúcich funkcionalít:

- Antivírusová a antispyvérová ochrana
- Antispamová ochrana
- Antiphishingová ochrana
- Pravidlá
- Ochrana prenosu e-mailov (Exchange Server 2007, 2010, 2013, 2016, 2019)
- Ochrana databáz e-mailových schránok (Exchange Server 2007, 2010)
- Manuálna kontrola databáz e-mailových schránok (Exchange Server 2007, 2010, 2013, 2016, 2019)
- E-mailová karanténa (nastavenie typu e-mailovej karantény)
- Podpisovanie DKIM

Nastavenie priority agenta

V prípade potreby môžete pre ESET Mail Security agenty nastaviť poradie, v akom sa budú aktivovať po spustení Microsoft Exchange Servera. Hodnota čísla udáva prioritu. Čím nižšia je hodnota čísla, tým vyššia je priorita. Toto platí pre Microsoft Exchange Server 2007 a novšie verzie.



Hore/Dole

Presunutím vybraného agenta v zozname vyššie alebo nižšie zmeníte jeho prioritu. Je možné zmeniť prioritu pre relevantné agenty (zvýraznené tučným písmom).

Odporúčame, aby ste prioritu ESET DKIM agenta udržiavali na poslednom mieste na spodku, vďaka čomu zabezpečíte, že hlavičky sa podpíšu ako posledné po akýchkoľvek úpravách inými agentmi.

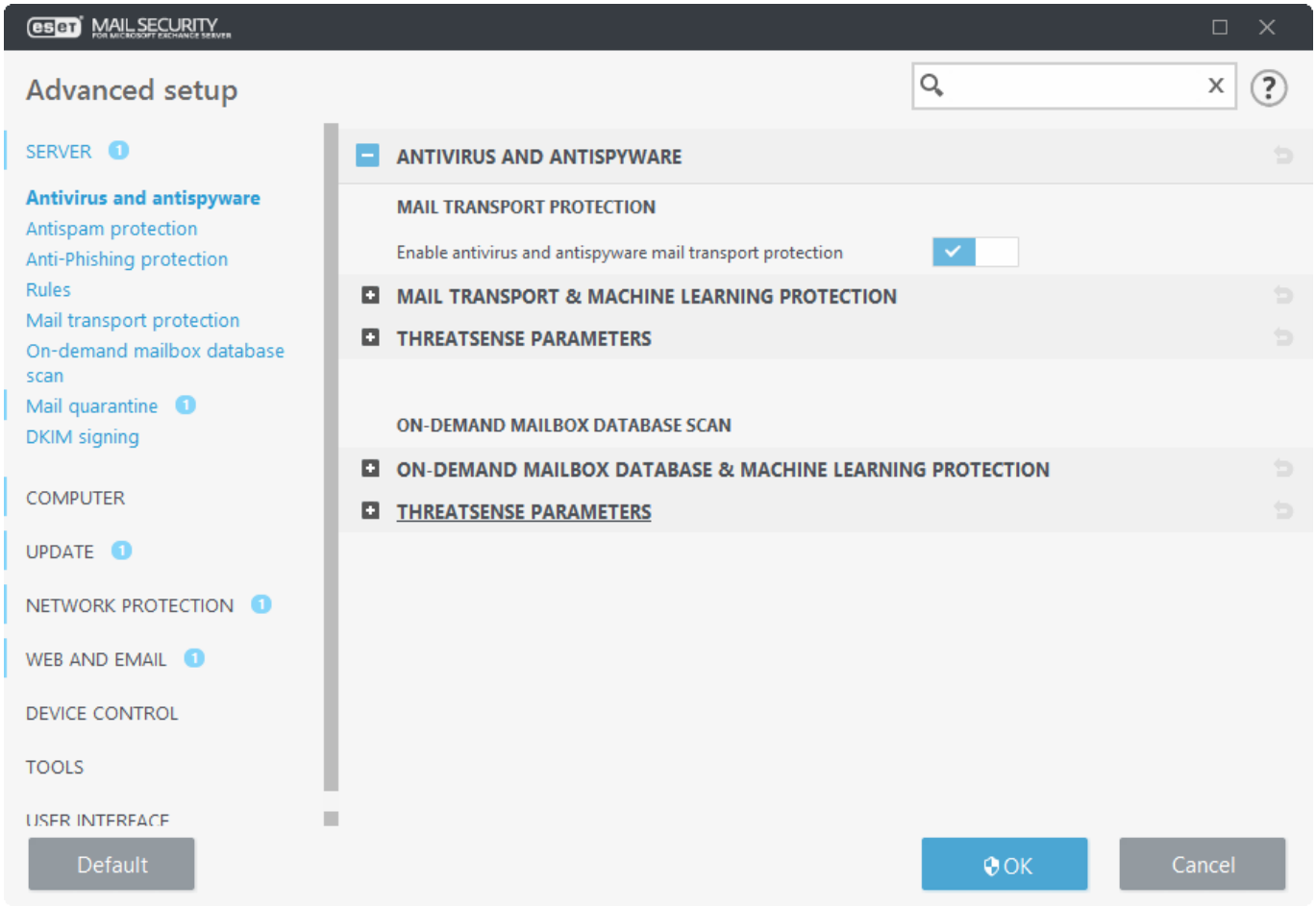
Antivírusová a antispyvérová ochrana

V tejto sekcii môžete nastaviť antivírusovú a antispyvérovú ochranu pre váš e-mailový server.

Ochrana prenosu e mailov je poskytovaná pomocou agenta prenosu. Je dostupná len pre Microsoft Exchange Server 2007 a novšie verzie. Váš Microsoft Exchange Server však musí mať rolu Edge Transport Server alebo Hub Transport Server. Toto sa vzťahuje tiež na inštaláciu, pri ktorej je použitý len jediný server s viacerými rolami Exchange servera (len ak má server rolu Edge Transport Server alebo Hub Transport Server).

Ochrana prenosu e-mailov

Ak zakážete možnosť **Zapnúť antivírusovú a antispyvérovú ochranu prenosu e-mailov**, doplnok ESET Mail Security pre Exchange Server nebude uvoľnený z procesu Microsoft Exchange Server. Zakázanie tejto možnosti bude mať za následok len to, že správy nebudú kontrolované na prítomnosť vírusov na prenosovej vrstve. Správy však budú aj naďalej kontrolované na prítomnosť vírusov a spamu na databázovej vrstve, pričom budú použité existujúce pravidlá.



Ochrana databáz e-mailových schránok

Ak zakážete možnosť **Zapnúť antivírusovú a antispyvérovú ochranu databáz e-mailových schránok**, doplnok ESET Mail Security pre Exchange Server nebude uvoľnený z procesu Microsoft Exchange Server. Zakázanie tejto možnosti bude mať za následok len to, že správy nebudú kontrolované na prítomnosť vírusov na databázovej vrstve. Správy však budú aj naďalej kontrolované na prítomnosť vírusov a spamu na prenosovej vrstve, pričom budú použité existujúce pravidlá.

Manuálna kontrola databáz e-mailových schránok

Táto funkcia je dostupná po vypnutí **Ochrany databáz e-mailových schránok** v sekcii Server.

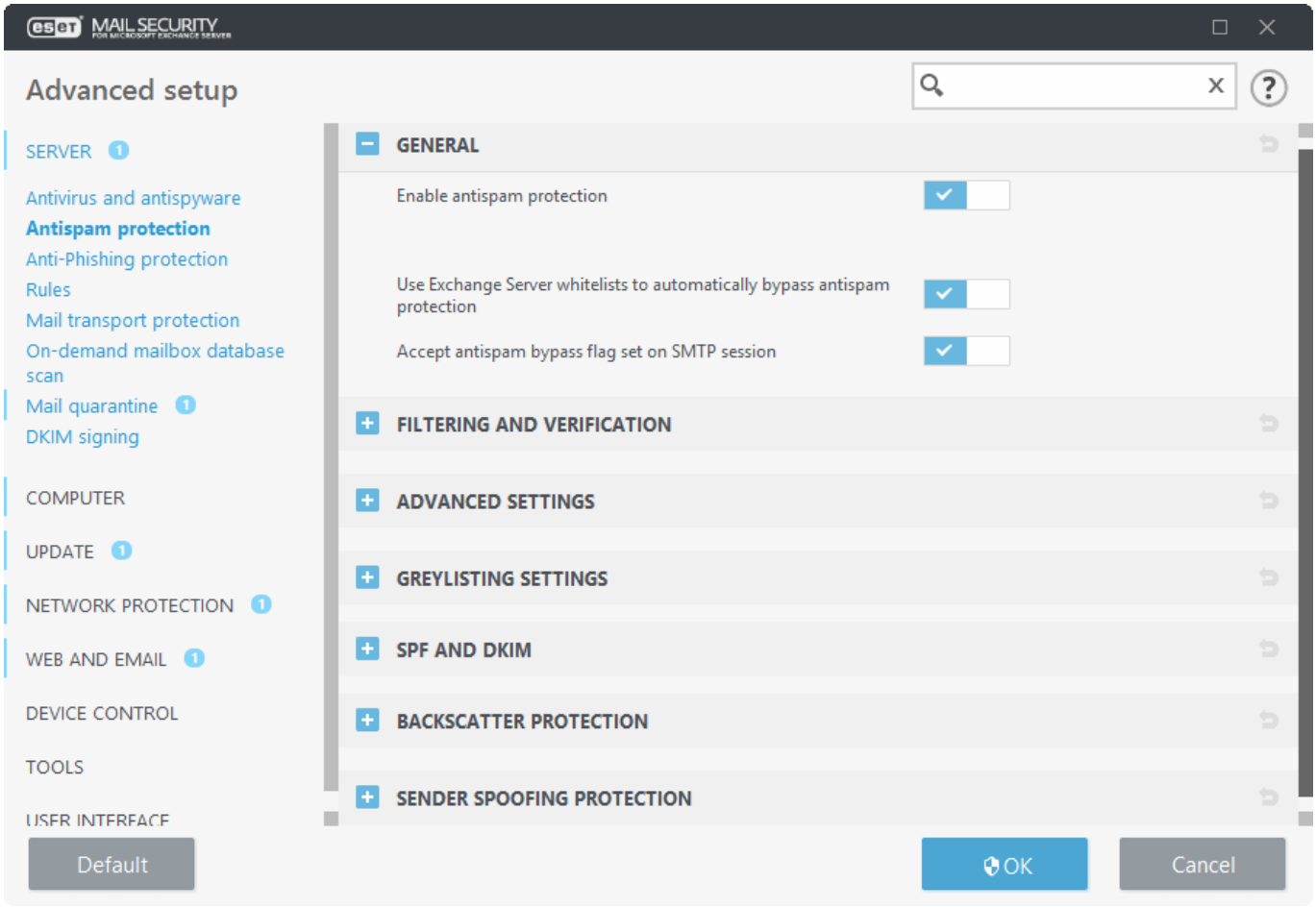
Parametre ThreatSense

V tejto sekcii môžete upraviť parametre kontroly pre Ochranu prenosu e-mailov, Ochranu databáz e-mailových schránok a Manuálnu kontrolu databáz e-mailových schránok.

Antispamová ochrana

Antispamová ochrana je pre e-mailový server štandardne povolená. Vypnúť ju môžete kliknutím na prepínač vedľa popisu **Zapnúť antispamovú ochranu**.

> Vypnutie antispamovej ochrany nezmení stav ochrany. V prípade vypnutia antispamovej ochrany sa bude aj naďalej zobrazovať zelený text **Ste chránený** v časti **Monitorovanie** nachádzajúcej sa v hlavnom menu programu. To znamená, že vypnutie antispamovej ochrany neznižuje úroveň celkovej ochrany.



Použiť whitelisty Exchange Servera pre automatické obídenie antispamovej ochrany

Povolením tejto možnosti umožníte programu ESET Mail Security používať špecifické Exchange „whitelisty“ (dôveryhodné zoznamy). Ak je táto možnosť povolená, posudzuje sa nasledovné:

- Či je IP adresa servera v zozname povolených/schválených IP adries Exchange servera.
- Či má prijímateľ správy na svojej e-mailovej schránke nastavený príznak Antispam Bypass pre vynechanie antispamovej kontroly.
- Či má prijímateľ správy adresu odosielateľa v zozname dôveryhodných odosielateľov (uistite sa, že je nastavená synchronizácia zoznamu dôveryhodných odosielateľov s vaším Exchange Server prostredím vrátane agregácie zoznamu dôveryhodných odosielateľov).

Ak ktorákoľvek z predchádzajúcich podmienok platí pre prichádzajúcu správu, správa nebude kontrolovaná na prítomnosť spamu a bude doručená do schránky prijímateľa.

Akceptovať príznak pre obídenie antispamu nastavený na SMTP relácii

Táto možnosť je užitočná pri overenej SMTP relácii medzi servermi Exchange s nastaveným antispam bypass (obídením antispamu). Napríklad, ak máte Edge server a Hub server, nie je potrebné kontrolovať komunikáciu medzi týmito servermi. Možnosť **Akceptovať príznak pre obídenie antispamu nastavený na SMTP relácii** je štandardne povolená, aplikuje sa však len ak je príznak pre obídenie antispamu nastavený pre SMTP reláciu na vašom Exchange serveri. Ak zakážete možnosť **Akceptovať príznak pre obídenie antispamu nastavený na SMTP relácii**, ESET Mail Security bude kontrolovať SMTP reláciu na prítomnosť spamu napriek tomu, že je na vašom Exchange serveri nastavené obídenie antispamu.

Pre zabezpečenie čo najlepšej možnej ochrany antispamovým modulom je dôležité, aby bola antispamová databáza pravidelne aktualizovaná. Pri povolení pravidelných aktualizácií antispamovej databázy treba dbať na to, aby mal ESET Mail Security prístup na správne IP adresy a porty. Pre podrobnejšie informácie o nastavení IP adries a portov na firewalloch tretích strán si prečítajte nasledujúci článok Databázy znalostí ESET.

Ďalšie nastavenia nájdete v príslušných podsekciách:

- Filtrovanie a overovanie
- Rozšírené nastavenia
- Nastavenia greylistingu
- SPF a DKIM
- Ochrana proti spätnému rozptylu
- Ochrana pred sfalšovaním identity odosielateľa

Filtrovanie a overovanie

Môžete nastaviť Povolené, Blokované a Ignorované zoznamy zadaním kritérií, ako napr. IP adresa alebo rozsah IP adries, názov domény atď. Pre pridanie, úpravu alebo odstránenie kritérií použite tlačidlo **Upraviť**.

IP adresy a domény zahrnuté v zoznamoch **Ignorovaných** adries/domén nebudú ďalej vyhodnocované antispamovým filtrovaním, uplatňujú sa však na ne ostatné techniky Antispamovej ochrany.
Do zoznamov ignorovaných adries/domén by ste mali pridať všetky IP adresy a názvy domén v rámci vašej internej infraštruktúry. Môžete tiež zahrnúť IP adresy alebo názvy domén vášho poskytovateľa internetových služieb, prípadne externých e-mailových serverov, ktoré sú momentálne blokované na základe RBL alebo DNSBL (cloudový blacklist – Blackhole List spoločnosti ESET alebo Blackhole List tretej strany).
Zahrnutie blokovaných zdrojov do ignorovaných zoznamov vám umožní z týchto zdrojov prijímať e□maily aj napriek tomu, že ich IP adresy sú uvedené na cloudovom blackliste. E-mailové správy prichádzajúce z týchto zdrojov budú prijaté a ich obsah bude ďalej vyhodnocovaný ostatnými antispamovými technikami.

Zoznam povolených IP adries	E-maily prichádzajúce z IP adries uvedených na tomto zozname budú automaticky doručené príjemcom. Obsah e□mailových správ nebude kontrolovaný.
Zoznam blokovaných IP adries	Automaticky zablokuje e-mailové správy prichádzajúce zo zadaných IP adries.

Zoznam ignorovaných IP adries	Zoznam IP adries, ktoré budú počas klasifikácie ignorované. Obsah e□mailových správ bude kontrolovaný. Ak chcete povoliť lokálne IP adresy svojej siete, použite prepínač Je súčasťou internej infraštruktúry (pozrite príklady nižšie).
Zoznam blokovaných domén v tele správy	Zablokuje e-mailové správy, ktoré obsahujú zadanú doménu v tele správy. Akceptované sú len domény najvyššej úrovne (TLD – top-level domain).
Zoznam ignorovaných domén v tele správy	Zadané domény nachádzajúce sa v tele správy budú počas klasifikácie ignorované. Akceptované sú len domény najvyššej úrovne (TLD – top-level domain).
Zoznam blokovaných IP adries v tele správy	Zablokuje e-mailové správy, ktoré obsahujú zadanú IP adresu v tele správy.
Zoznam ignorovaných IP adries v tele správy	Zadané IP adresy nachádzajúce sa v tele správy budú počas klasifikácie ignorované.
Zoznam povolených odosielateľov	E-maily prichádzajúce od konkrétneho odosielateľa na tomto zozname budú doručené príjemcom. Pri vyhodnotení sa použije iba jeden odosielateľ alebo celá doména podľa nižšie uvedenej priority: 1.SMTP 'MAIL FROM' adresa 2.Hlavička "Return-Path:" 3.Hlavička "X-Env-Sender:" 4.Hlavička "From:" 5.Hlavička "Sender:" 6.Hlavička "X-Apparently-From:"
Zoznam blokovaných odosielateľov	Doručenie e-mailov od konkrétneho odosielateľa na tomto zozname bude blokované. Pri vyhodnotení sa použijú všetci zistení odosielatelia alebo celé domény: SMTP 'MAIL FROM' adresa Hlavička "Return-Path:" Hlavička "X-Env-Sender:" Hlavička "From:" Hlavička "Sender:" Hlavička "X-Apparently-From:"
Zoznam povolených domén preložených na IP adresy	Automaticky povolí e-mailové správy prichádzajúce z IP adries, ktoré sú získané z domén nachádzajúcich sa v tomto zozname. Pri preklade IP adries sú rozpoznávané SPF (Sender Policy Framework) záznamy.
Zoznam blokovaných domén preložených na IP adresy	Zablokuje e-mailové správy prichádzajúce z IP adries, ktoré sú získané z domén nachádzajúcich sa v tomto zozname. Pri preklade IP adries sú rozpoznávané SPF (Sender Policy Framework) záznamy.
Zoznam ignorovaných domén preložených na IP adresy	Zoznam domén, z ktorých sú získané IP adresy, ktoré nebudú kontrolované počas klasifikácie. Pri preklade IP adries sú rozpoznávané SPF (Sender Policy Framework) záznamy.
Zoznam blokovaných krajín	Zablokuje e-mailové správy prichádzajúce zo zadaných krajín. Blokovanie je založené na GeoIP. Ak je správa odoslaná z e-mailového servera, ktorého IP adresa je podľa našej geolokalizačnej databázy priradená ku krajine nachádzajúcej sa na vami zadefinovanom Zozname blokovaných krajín, táto správa bude automaticky označená ako spam a vykoná sa akcia nastavená v roletovom menu Vykonať akciu na spamovú správu v sekcii Ochrana prenosu e-mailov.

V rámci zoznamov domén v tele správy sú akceptované iba domény najvyššej úrovne (TLD – top-level domain) podľa oficiálnej databázy Root Zone Database.

Ak chcete pridať viacero položiek, v okne **Pridať** kliknite na **Zadať viaceré hodnoty** a vyberte, aký oddeľovač by mal byť použitý. Na výber je Nový riadok, Čiarka a Bodkočiarka.

Cieľ: Vylúčiť lokálne IP adresy vašej infraštruktúry z Antispamovej ochrany ich pridaním na zoznam ignorovaných IP adries.
Prejdite do sekcie **Rozšírené nastavenia (F5)** > **Server** > **Antispamová ochrana** > **Filtrovanie a overovanie**.
Kliknite na **Upraviť** vedľa položky **Zoznam ignorovaných IP adries**.
Kliknite na **Pridať** a zadajte rozsah IP adries vašej sieťovej infraštruktúry vo formáte *1.1.1.1-1.1.1.255*. V prípade potreby môžete do zoznamu pridať viacero rozsahov alebo jednotlivých IP adries.
Použite prepínač **Je súčasťou internej infraštruktúry**.

Greylisting a SPF

Pre automatické obídenie greylistingu a SPF zadajte whitelist domén preložených na IP adresy alebo whitelist IP adries. Protokoly si môžete prezrieť v protokole SMTP ochrany. Ak chcete použiť tieto možnosti, musíte najskôr zapnúť greylisting alebo SPF. V prípade SPF je potrebné zapnúť možnosť **Automaticky odmietnuť správu, ak nebola SPF kontrola úspešná** a/alebo **Automaticky obísť greylisting, ak bola SPF kontrola úspešná**.

Použiť antispamové zoznamy pre automatické obídenie greylistingu a SPF

Ak je táto možnosť zapnutá, zoznam povolených a ignorovaných IP adries bude použitý spolu s whitelistami IP adries a domén preložených na IP adresy na automatické obídenie greylistingu a SPF.

Whitelist IP adries

V tejto časti môžete pridať IP adresu, IP adresu s maskou a rozsah IP. Zoznam môžete upraviť kliknutím na **Pridať**, **Upraviť** alebo **Odstrániť**. Môžete prípadne importovať svoj vlastný zoznam zo súboru namiesto zadávania každej položky manuálne – kliknite na **Spustiť import** a vyhľadajte súbor obsahujúci položky, ktoré chcete pridať do zoznamu. V takomto prípade vyberte z kontextového menu možnosť **Exportovať**.

Whitelisty majú prednosť pred blacklistmi. Napríklad, ak bude e-mailová správa obsahovať adresu, ktorá sa nachádza súčasne na whiteliste aj blackliste, dôjde k doručeniu správy. Voči whitelistom sa vyhodnocuje iba adresa posledného odosielateľa a ďalšie adresy do počtu definovaného v poli Maximálny počet overených adries z Received: hlavičiek. Všetky adresy sa vyhodnocujú voči lokálnym blacklistom.

Whitelist domén preložených na IP adresy

Umožňuje špecifikovať domény (napr. domainname.local). Pre úpravu zoznamu použite **Pridať**, **Odstrániť** alebo **Odstrániť všetko**. Ak chcete importovať svoj vlastný zoznam zo súboru namiesto zadávania každej položky manuálne, kliknite na **Spustiť import** a vyhľadajte súbor obsahujúci položky, ktoré chcete pridať do zoznamu. V takomto prípade vyberte z kontextového menu možnosť **Exportovať**.

Greylisting a SPF sú vyhodnocované Ochranou prenosu e-mailov a umožňujú vám používať whitelisty IP adries a domén preložených na IP adresy, ako aj zoznamy povolených a ignorovaných IP adries. Ak však používate SPF pravidlá, žiadny z týchto whitelistov nebude pre ne zohľadnený.

Antispam – Rozšírené nastavenia

Tieto nastavenia umožňujú overovanie správ pomocou externých serverov (**RBL** – Realtime Blackhole List, **DNSBL** – DNS Blocklist) podľa prednastavených kritérií.

Maximálny počet overených adries z Received: hlavičiek

Môžete obmedziť počet IP adries, ktoré sú kontrolované antispamom. Toto sa týka IP adries uvedených v

hlavičkách `Received: from`. Predvolená hodnota je 0, čo znamená, že sa skontroluje iba posledná zistená IP adresa odosielateľa.

Overiť adresu odosielateľa voči blacklistu koncového používateľa

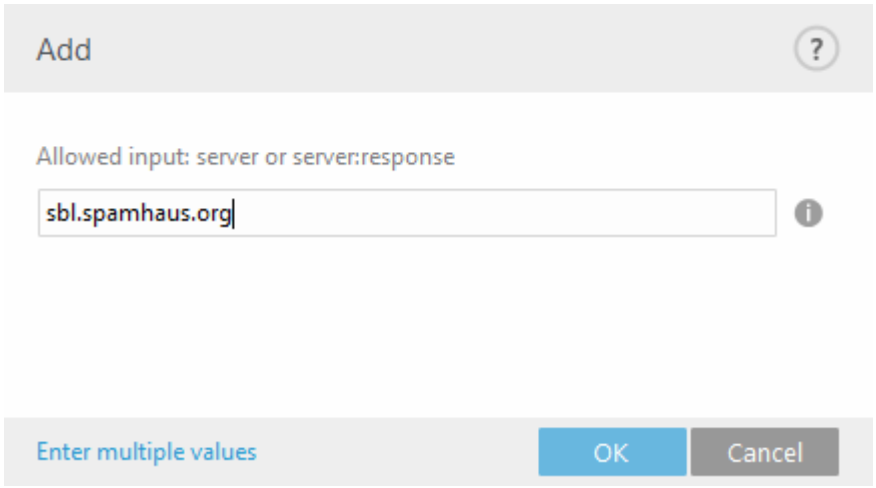
E-mailové správy, ktoré nie sú odoslané z e-mailových serverov (počítače, ktoré nie sú uvedené na zozname ako e-mailové servery), sú overované na ubezpečenie, že odosielateľ nie je na blackliste. Táto možnosť je v predvolených nastaveniach povolená. Ak je to potrebné, môžete túto možnosť vypnúť, avšak správy, ktoré nie sú odoslané z e-mailových serverov, nebudú kontrolované voči blacklistu.

> **i** V prípade IP adries z hlavičiek `Received: from` majú výsledky z blocklistov tretích strán vyššiu prioritu ako používateľské blacklisty. Na servery tretích strán sú na vyhodnotenie zasielané všetky zistené IP adresy (do stanoveného maximálneho počtu overených adries).

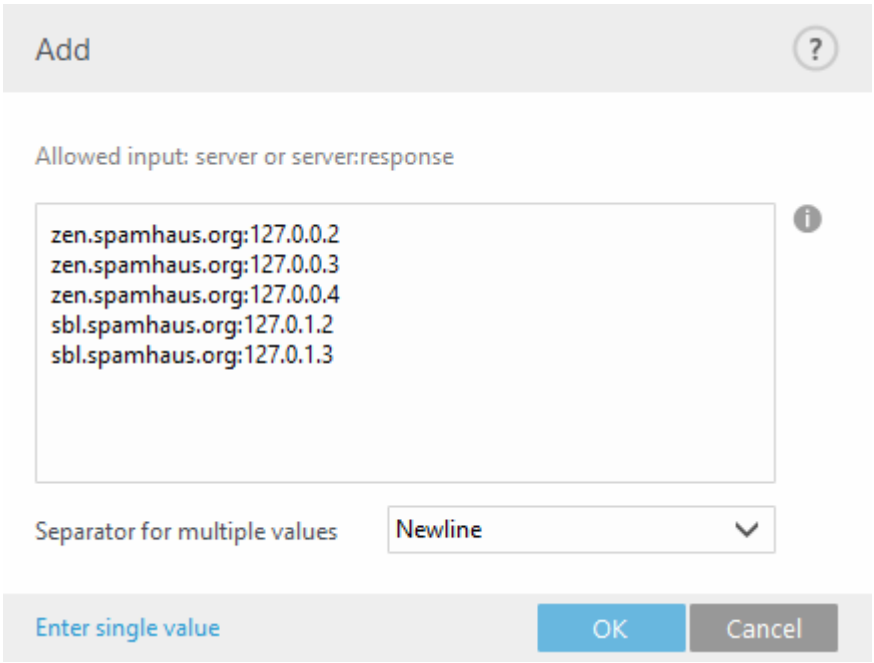
Dodatočné RBL servery

Zoznam Realtime Blackhole List (RBL) serverov, ktoré sú dopytované pri analýze správ.

> **i** Pri pridávaní dodatočných RBL serverov zadajte názov domény servera (napr. `sbl.spamhaus.org`). Toto bude fungovať s akýmkoľvek návratovým kódom, ktorý je podporovaný serverom.



Môžete tiež prípadne zadať názov servera s návratovým kódom vo formáte `server:response` (napr. `zen.spamhaus.org:127.0.0.4`). Pri použití tohto formátu odporúčame pridať každý názov servera a návratový kód osobitne tak, že budete mať kompletný zoznam. V okne **Pridať** kliknite na **Zadať viaceré hodnoty** pre upresnenie všetkých názvov serverov a ich návratových kódov. Položky by mali vyzerať ako v príklade uvedenom nižšie, avšak hostiteľské názvy RBL serverov a návratové kódy sa môžu líšiť:



Limit vykonania RBL požiadavky (v sekundách)

Táto funkcia vám umožňuje nastaviť maximálny čas pre RBL požiadavky. Budú použité len odpovede z RBL serverov, ktoré odpovedali v zadanom čase. Ak je hodnota nastavená na „0“, nie je vyžadovaný žiadny čas na odpoveď.

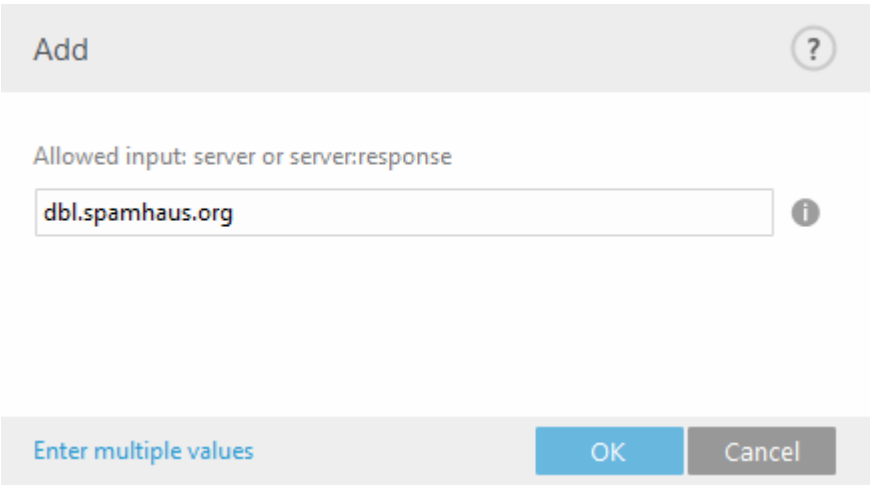
Maximálny počet overovaných IP adries voči RBL

Pomocou tejto funkcie je možné obmedziť počet IP adries dopytovaných na RBL server. Celkový počet RBL požiadaviek sa rovná počtu IP adries v hlavičkách Received: (až do maximálnej výšky RBL maxcheck IP adries), vynásobené počtom RBL serverov uvedených v zozname RBL. Ak je hodnota nastavená na „0“, počet prijatých hlavičiek nie je obmedzený. IP adresy na zozname ignorovaných IP adries sa nezapočítavajú do limitu RBL IP adries.

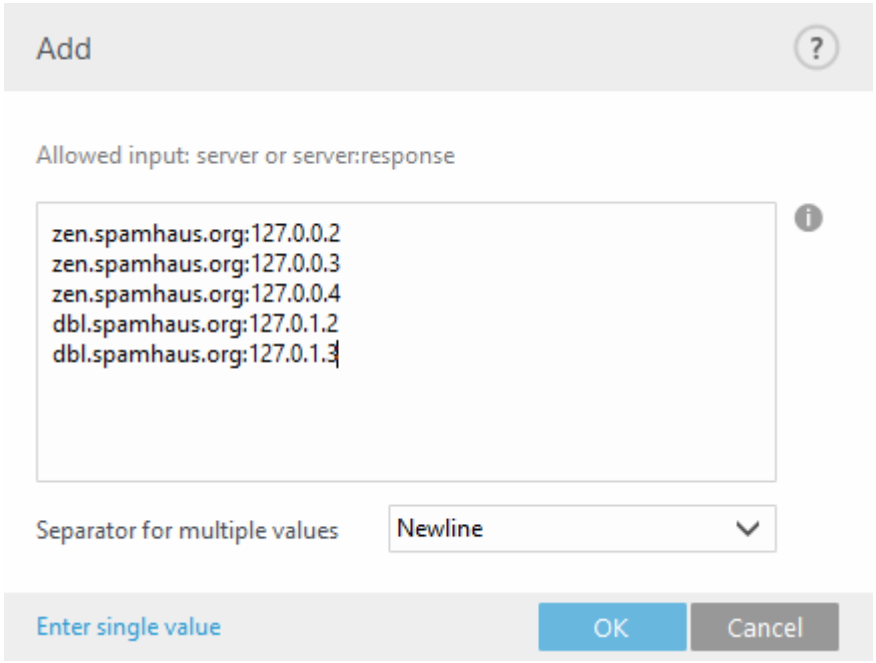
Dodatočné DNSBL servery

Zoznam DNS Blocklist (DNSBL) serverov, ktoré sú dopytované s doménami a IP adresami získanými z tela správy.

Pri pridávaní dodatočných DNSBL serverov zadajte názov domény servera (napr. `dbl.spamhaus.org`). Toto bude fungovať s akýmkoľvek návratovým kódom, ktorý je podporovaný serverom.



Môžete tiež prípadne zadať názov servera s návratovým kódom vo formáte `server:response` (napr. `zen.spamhaus.org:127.0.0.4`). V takomto prípade odporúčame pridať každý názov servera a návratový kód osobitne tak, že budete mať kompletný zoznam. V okne **Pridať** kliknite na **Zadať viaceré hodnoty** pre upresnenie všetkých názvov serverov a ich návratových kódov. Položky by mali vyzerať ako v príklade uvedenom nižšie, avšak hostiteľské názvy DNSBL serverov a návratové kódy sa môžu líšiť:



Limit vykonania DNSBL požiadavky (v sekundách)

Táto funkcia vám umožňuje nastaviť maximálny čas na dokončenie všetkých DNSBL požiadaviek.

Maximálny počet overovaných adries voči DNSBL

Pomocou tejto funkcie je možné obmedziť počet IP adries dopytovaných na DNS Blocklist server.

Maximálny počet overovaných domén voči DNSBL

Pomocou tejto funkcie je možné obmedziť počet domén dopytovaných na DNS Blocklist server.

Maximálna veľkosť kontrolovanej správy (kB)

Ide o obmedzenie antispamovej kontroly pre správy väčšie ako zadaná hodnota. Predvolená hodnota 0 znamená, že kontrolovaná správa môže mať neobmedzenú veľkosť a teda budú kontrolované všetky správy. Za normálnych okolností neexistuje dôvod na obmedzovanie antispamovej kontroly, ak ju však za určitých okolností potrebujete obmedziť, zmeňte hodnotu na požadovanú veľkosť. Ak nastavíte obmedzenie, antispamový modul spracuje správy len do nastavenej veľkosti a väčšie správy ignoruje.

Najmenšie možné obmedzenie je 12 kB. Ak nastavíte hodnotu v rozmedzí 1 až 12, antispamový modul bude stále spracovávať správy o veľkosti najmenej 12 kB.

Zapnúť dočasné odmietnutie nevyhodnotených správ

V prípade, že antispamové jadro nedokáže určiť, či správa je alebo nie je spam, čo znamená, že správa má niektoré podozrivé črty príznačné pre spam, avšak nie dostatok na to, aby bola vyhodnotená ako spam (ide napr. o prvý e□mail spamovej kampane alebo e□mail, ktorého zdroj spadá do rozsahu IP adries s pochybnou reputáciou), potom táto možnosť (ak je povolená) umožňuje programu ESET Mail Security dočasne takúto správu

zamietnuť (rovnako ako v prípade Greylistingu). Navyše, takáto správa bude zamietnutá opakovane po určitú dobu, až kým:

- Neuplynie interval a správa nie je akceptovaná pri ďalšom pokuse o doručenie. Správe bude v takomto prípade ponechaný príznak (SPAM alebo HAM) z počiatočnej analýzy.

- Antispamové jadro (cloud) nezhromaždí dostatočné množstvo dát a nedokáže správne klasifikovať správu pred uplynutím intervalu.

Zamietnutá správa nie je uchovávaná programom ESET Mail Security a musí byť opätovne odoslaná e-mailovým serverom podľa SMTP RFC.

Zapnúť odosielanie dočasne odmietnutých správ na analýzu

Obsah správy je automaticky odoslaný do spoločnosti ESET na analýzu. Toto pomáha zlepšiť klasifikáciu budúcich e-mailových správ.

Je možné, že dočasne zamietnuté správy, ktoré sú odoslané na analýzu, sú v skutočnosti HAM. V ojedinelých prípadoch môžu byť dočasne zamietnuté správy vyhodnocované manuálne. To znamená, že túto funkciu povoľte len v prípade, ak nepracujete s potenciálne citlivými dátami.

Nastavenia greylistingu

Možnosť **Zapnúť greylisting** aktivuje funkciu chrániacu používateľov pred nevyžiadanou poštou pomocou nasledujúcej techniky: Agent prenosu odošle „dočasne odmietavú“ SMTP odpoveď (štandardne je to 451/4.7.1) pre každý prijatý e-mail odosielateľa, ktorého nemôže identifikovať. Legitímny server sa v krátkej dobe pokúsi o opakované odoslanie takejto správy. Servery odosielajúce nevyžiadanú poštu sa zvyčajne nepokúšajú opakovane odoslať správu, pretože pracujú s tisíckami e-mailových adries a nemajú čas na opätovné posielanie. Greylisting je dodatočná vrstva antispamovej ochrany a nemá žiadny vplyv na vyhodnocovanie nevyžiadanej pošty pomocou antispamového modulu.

Pri vyhodnocovaní zdroja správy metóda Greylisting berie do úvahy zoznamy schválených IP adries, ignorovaných IP adries, schválených odosielateľov a povolených IP adries na Exchange serveri spoločne s nastavením pre vynechanie antispamovej kontroly konkrétnej schránky príjemcu. Pre správy z týchto IP adries/zoznamov odosielateľov alebo správy doručené do e-mailových schránok, ktoré majú povolenú možnosť pre vynechanie antispamovej kontroly, nebude použitá funkcia Greylisting.

Použiť len doménovú časť adresy odosielateľa

Ignoruje meno odosielateľa v e-mailovej adrese; berie do úvahy len doménu.

Synchronizovať databázy greylistingu naprieč klastrom ESET

Položky v databáze greylistingu sú zdieľané v reálnom čase medzi servermi v klastri ESET. Ak niektorý zo serverov dostane správu, ktorá je spracovaná greylistingom, táto informácia je odoslaná programom ESET Mail Security naprieč všetkými zostávajúcimi uzlami v klastri ESET.

Časový limit pre počiatočné odmietnutie spojenia (v minútach)

Pri prvom doručení správy a dočasnom odmietnutí definuje tento parameter časový interval, počas ktorého bude správa vždy odmietnutá (od prvého odmietnutia). Po skončení zadaného časového intervalu bude správa úspešne prijatá. Minimálna hodnota, ktorú je možné zadať, je 1 minúta.

Čas uplynutia platnosti neoverených spojení (v hodinách)

Minimálny časový interval, počas ktorého bude uchovaná trojica (tzv. triplet) základných údajov o správe. Legitímny server musí opakovane odoslať správu pred skončením tejto doby. Táto hodnota musí byť vyššia ako hodnota **Časový limit pre počiatočné odmietnutie spojenia**.

Čas uplynutia platnosti overených spojení (v dňoch)

Minimálny časový interval v dňoch, počas ktorého bude uchovaná trojica (tzv. triplet) základných údajov o správe a počas ktorého budú správy od určitého odosielateľa prijímané bez oneskorenia. Táto hodnota musí byť vyššia ako hodnota **Čas uplynutia platnosti neoverených spojení**.

SMTP odpoveď (pre dočasne zamietnuté spojenia)

Zadajte **Kód odpovede**, **Stavový kód** a **Správu odpovede**, ktoré definujú dočasne zamietnutú SMTP odpoveď odoslanú na SMTP server, z ktorého prišla zamietnutá správa. Príklad odmietavej SMTP odpovede:

Kód odpovede	Stavový kód	Správa odpovede
451	4.7.1	Please try again later

Pri definovaní odmietavej SMTP odpovede môžete tiež použiť systémové premenné.

Nesprávna syntax kódu SMTP odpovede môže spôsobiť nefunkčnosť celej Greylisting ochrany. Výsledkom môže byť, že klientom bude doručovaná nevyžiadaná pošta alebo správy nebudú doručované vôbec.

Všetky e-mailové správy, ktoré boli vyhodnocované pomocou metódy Greylisting, sú zaznamenané v protokole SMTP ochrany.

SPF a DKIM

SPF (Sender Policy Framework) a DKIM (DomainKeys Identified Mail) sú metódy používané na overovanie, či bola e-mailová správa skutočne doručená z danej domény. Tieto metódy pomáhajú chrániť príjemcov pred nevyžiadanými a podvodnými správami. ESET Mail Security využíva taktiež overovací mechanizmus DMARC (Domain-based Message Authentication, Reporting and Conformance), ktorý dopĺňa a rozširuje SPF a DKIM overovanie.

SPF

SPF kontrola overuje, či bol e-mail odoslaný legitímnym odosielateľom. Funguje tak, že sa vykoná DNS vyhľadávanie týkajúce sa SPF záznamov domény odosielateľa s cieľom získať zoznam IP adries. Ak sa ktorákoľvek z IP adries v SPF záznamoch zhoduje s IP adresou odosielateľa, výsledok SPF kontroly bude **úspešný**. Ak sa IP adresa odosielateľa nezhoduje, výsledok kontroly bude **neúspešný**. Avšak, treba mať na pamäti, že nie všetky domény majú SPF záznamy špecifikované v DNS. Ak sa v DNS nenachádzajú žiadne SPF záznamy, výsledok kontroly bude mať hodnotu **Nie je k dispozícii**. V prípade, že vyprší časový limit DNS požiadavky, výsledok kontroly bude mať taktiež hodnotu **Nie je k dispozícii**.

DKIM

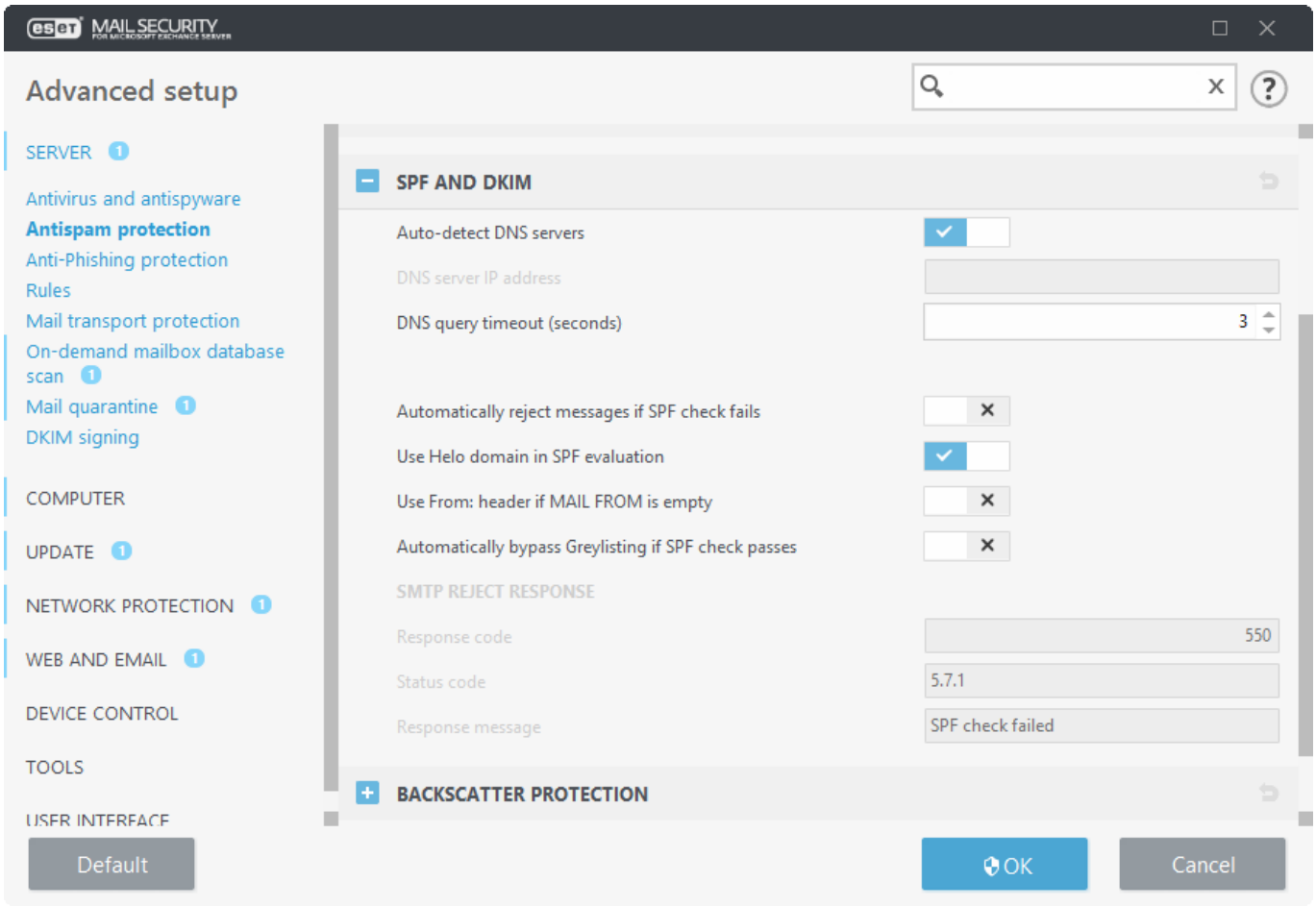
DKIM používajú organizácie na zabránenie sfalšovaniu e-mailových správ, a to tak, že do hlavičiek odchádzajúcich správ sa pridá digitálny podpis podľa štandardu DKIM. E-mailový server zašifruje súkromným doménovým kľúčom časť hlavičky správy. ESET Mail Security si následne z DNS záznamu domény stiahne verejný kľúč, dešifruje

hlavičku správy a overí, či správa skutočne pochádza z danej domény a nebola cestou zmenená.

> Exchange Server 2010 a staršie verzie nie sú plne kompatibilné s DKIM, pretože hlavičky obsiahnuté v digitálne podpísaných prichádzajúcich správach môžu byť počas DKIM overovania upravené.

DMARC

Vychádza z dvoch vyššie uvedených mechanizmov – SPF a DKIM. Môžete vytvoriť pravidlo Ochrany prenosu e-mailov, ktoré bude vyhodnocovať **výsledok DMARC**, prípadne použiť akciu **Aplikovať politiku DMARC**.



Automaticky zisťovať DNS servery

Budú použité nastavenia vášho sieťového adaptéra.

IP adresa DNS servera

Ak chcete použiť konkrétne DNS servery pre SPF a DKIM, zadajte IP adresu (vo formáte IPv4 alebo IPv6) DNS servera, ktorý chcete použiť.

Časový limit DNS požiadavky (v sekundách)

Zadajte časový limit pre DNS odpoveď.

Automaticky odmietnuť správu, ak nebola kontrola SPF úspešná

V prípade, že kontrola SPF pre konkrétnu e-mailovú správu vyjde negatívne, táto správa bude odmietnutá ešte pred jej prevzatím.

Kontrola SPF prebieha na SMTP vrstve. Správa však môže byť odmietnutá buď automaticky na SMTP vrstve, alebo počas vyhodnocovania pravidiel.
Pokiaľ máte aktivované automatické odmietnutie správ na SMTP vrstve, odmietnuté správy nebudú zaznamenávané do protokolu udalostí. Dôvod je taký, že zapisovanie do protokolu je vyvolané akciou nastavenou pre určité pravidlo, avšak k automatickému odmietnutiu správy dôjde už na SMTP vrstve, teda ešte pred tým, ako by mohlo prebehnúť samotné vyhodnocovanie pravidiel. Keďže správa je odmietnutá už pred vyhodnocovaním pravidiel, neexistuje žiadna informácia o tom, že na správu by bolo aplikované akékoľvek pravidlo, a teda ani nemôže dôjsť k zápisu do protokolu.
Odmietnuté správy je možné zaznamenávať do protokolu len v tom prípade, že boli odmietnuté na základe nastaveného pravidla. Ak si prajete, aby e-mailové správy, ktoré neprešli kontrolou SPF, boli odmietnuté, no zároveň boli po odmietnutí zaznamenané do protokolu, deaktivujte možnosť **Automaticky odmietnuť správu, ak nebola kontrola SPF úspešná**, a vytvorte nasledujúce pravidlo **Ochrany prenosu e-mailov**:
Podmienka
- Typ: Výsledok SPF
- Operácia: je
- Parameter: Fail

Akcie
- Typ: Odmietnuť správu
- Typ: Zapísať do protokolu udalostí

Použiť doménu z reťazca HELO pri vyhodnocovaní SPF

Používa doménu HELO pre vyhodnotenie SPF. Ak doména HELO nie je špecifikovaná, použije sa názov hostiteľa počítača.

Použiť From: hlavičku, ak je MAIL FROM prázdny

Hlavička MAIL FROM môže byť prázdna a môže byť tiež ľahko sfalšovaná. Ak je táto možnosť povolená a hlavička MAIL FROM je prázdna, správa sa stiahne a bude použitá hlavička From:.

Automaticky obísť greylisting, ak bola kontrola SPF úspešná

Nie je dôvod používať metódu greylisting pre správy, ktoré úspešne prešli kontrolou SPF.

Zamietavá SMTP odpoveď

Môžete zadať **Kód odpovede**, **Stavový kód** a **Správu odpovede**, ktoré definujú dočasne zamietnutú SMTP odpoveď odoslanú na SMTP server, z ktorého prišla zamietnutá správa. Správu odpovede môžete zadať v nasledujúcom formáte:

Kód odpovede	Stavový kód	Správa odpovede
550	5.7.1	SPF check failed

Ochrana proti spätnému rozptylu

Spätný rozptyl (backscatter) v rámci spamu je odosielanie nesprávne smerovaných správ o nedoručení e-mailovými servermi. Ide o nežiaduci vedľajší efekt spamu. Ak je spamová správa odmietnutá e-mailovým serverom príjemcu, údajnému odosielateľovi (e-mailová adresa, ktorá bola sfalšovaná ako odosielateľ pôvodnej spamovej správy) sa odošle správa o nedoručení (NDR), nie však skutočnému odosielateľovi spamu. Používateľ, ktorý je vlastníkom e-mailovej adresy, dostane správu o nedoručení, pričom v skutočnosti sa na pôvodnej spamovej správe nijakým spôsobom nepodieľal. V takejto situácii nachádza uplatnenie **Ochrana proti spätnému rozptylu**. Pomocou Ochrany proti spätnému rozptylu, ktorá je súčasťou ESET Mail Security, môžete zabrániť

doručovaniu spamových správ o nedoručení do e-mailových schránok používateľov v rámci svojej organizácie.

Ak povolíte možnosť **Zapnúť NDR kontrolu**, musíte zadať **Počiatočný podpis** (reťazec minimálne 8 znakov, môže ísť napr. o prístupovú frázu). Ochrana proti spätnému rozptylu programu ESET Mail Security zapisuje `X-Eset-NDR: <hash>` do hlavičky každej odchádzajúcej e-mailovej správy. `<hash>` je šifrovaný podpis, ktorý taktiež obsahuje **Počiatočný podpis**, ktorý ste zadali.

Ak nemohla byť doručená legitímna e-mailová správa, váš e-mailový server zvyčajne dostane správu o nedoručení, ktorá je následne skontrolovaná programom ESET Mail Security s cieľom nájsť v hlavičkách `X-Eset-NDR: <hash>`. Ak sa v hlavičke nachádza `X-Eset-NDR:` a podpis `<hash>` sa zhoduje, odosielateľovi legitímnej e-mailovej správy sa doručí správa o nedoručení, ktorá indikuje, že doručenie správy nebolo úspešné. Ak sa v hlavičke nenachádza `Eset-NDR:` alebo je podpis `<hash>` nesprávny, ide o spätný rozptyl spamu a správa o nedoručení je odmietnutá.

Automaticky odmietnuť správy o nedoručení (NDR) pri neúspešnej kontrole

V prípade, že kontrola NDR vyjde negatívne, daná správa bude odmietnutá ešte pred jej prevzatím.

Aktivitu **Ochrany proti spätnému rozptylu** si môžete pozrieť v protokole SMTP ochrany.

Ochrana pred sfalšovaním identity odosielateľa

Falšovanie identity odosielateľa (v angličtine „spoofing“) je rozšírenou technikou, pri ktorej útočník úmyselne mení meno alebo e□mailovú adresu odosielateľa v snahe oklamať príjemcu e□mailu. Riziko spočíva v tom, že pre príjemcu nie je ľahké rozoznať takýto falošný e□mail od pravého. Jedným z takýchto útokov je aj tzv. CEO podvod, pri ktorom sa útočník vydáva za generálneho riaditeľa spoločnosti.

E□maily od riaditeľa zvyknú zamestnanci otvárať bez väčších pochybností, vďaka čomu je takýto útok častokrát úspešný. Pri e□mailoch sa však nefalšuje len identita generálneho riaditeľa, útočník sa môže maskovať za akéhokoľvek skutočného odosielateľa, zvyčajne osobu v rámci služby Active Directory vašej organizácie. Sfalšovaná e□mailová správa potom vyzerá veľmi presvedčivo a u príjemcu nevyvolá žiadne podozrenie.

ESET Mail Security poskytuje ochranu pred týmto typom hrozby. Ochrana pred sfalšovaním identity odosielateľa preveruje, či sú informácie o odosielateľovi pravdivé, a to hneď niekoľkými metódami.

Ochrana pred sfalšovaním identity odosielateľa vyhľadá doménu uvedenú v hlavičke "From:" a v odosielateľovi obálky a následne porovná nájdenú doménu so zoznamami domén. Ak sa v zoznamoch nenájde zhodná doména, správa sa považuje za legitímnu (nesfalšovanú) a je ďalej spracovaná ďalšími vrstvami ochrany programu ESET Mail Security. Ak sa však doména zhoduje s niektorou z domén v zozname, môže ísť o e□mail so sfalšovaným odosielateľom a bude potrebné ďalšie preverenie.

V závislosti od nastavenia sa vykoná ďalšie overovanie. Prebehne kontrola SPF, IP adresa odosielateľa obálky sa porovná so zoznamom IP adries, prípadne sa správa automaticky vyhodnotí ako sfalšovaná. Ak e□mail úspešne prejde kontrolou SPF alebo IP adresa odosielateľa obálky zodpovedá IP adrese zo zoznamu, správa je legitímna. V opačnom prípade ide o e□mailovú správu so sfalšovaným odosielateľom. S takouto správou sa vykoná nastavená akcia.

Ochranu pred sfalšovaním identity odosielateľa je možné použiť dvoma spôsobmi:

- Zapnite **Ochranu pred sfalšovaním identity odosielateľa**, nakonfigurujte jej nastavenia a voliteľne upravte zoznamy domén a IP adries. S e□mailovými správami so sfalšovaným odosielateľom sa predvolene vykoná akcia **Presunúť správu do karantény**. Ak chcete zvoliť inú akciu, prejdite do rozšírených nastavení Ochrany

prenosu e-mailov .

• Utilize Mail transport protection rules, using **SPF result - From header** or **Envelope sender and From header comparison result** condition with an action of your choice. Prostredníctvom pravidiel je možné pri e-mailoch so sfalšovaným odosielateľom dosiahnuť špecifické správanie, keďže pravidlá poskytujú viac rôznych možností a kombinácií.

Ak sa používa Ochrana pred sfalšovaním identity odosielateľa alebo ak je nastavené pravidlo s akciou Zapísať do protokolu udalostí, všetky správy, ktoré boli vyhodnotené Ochranou pred sfalšovaním identity odosielateľa, sa zaznamenajú do Protokolov. Podobne, ak je v rámci Ochrany prenosu e-mailov alebo v pravidlách nastavená akcia **Presunúť správu do karantény**, e-maily so sfalšovaným odosielateľom nájdete v E-mailovej karanténe.

Zapnúť ochranu pred sfalšovaním identity odosielateľa

Aktivujte ochranu pred sfalšovaním identity odosielateľa, aby ste zabránili e-mailovým útokom, ktoré sa snažia oklamať príjemcu správy o pôvode správy tým, že falšujú informácie o odosielateľovi.

Povoliť prichádzajúce e-maily s mojou doménou uvedenou v adrese odosielateľa

Povoľte ďalšie preverenie prichádzajúcich správ, ktoré obsahujú vašu vlastnú doménu v hlavičke "From:" alebo v odosielateľovi obálky:

• Iba ak úspešne prejdú cez kontrolu SPF – pri tejto možnosti sa vychádza z aktívnej kontroly SPF. Ak správa úspešne prejde kontrolou SPF, považuje sa za legitímnu a je spracovaná na doručenie. Ak je výsledok kontroly SPF neúspešný, ide o sfalšovanú správu a vykoná sa nastavená akcia. Voliteľne môžete zapnúť funkciu Automaticky odmietnuť správu, ak nebola kontrola SPF úspešná.

• Iba ak je IP adresa uvedená na zozname IP adries infraštruktúry — porovná IP adresu odosielateľa obálky so zoznamami IP adries (Zoznam mojich IP adries a Zoznam ignorovaných IP adries s označením **Je súčasťou internej infraštruktúry**). Ak sa nájde zhoda s IP adresou, správa sa považuje za legitímnu a je spracovaná na doručenie. Ak sa zhoda IP adresy nenájde, ide o sfalšovanú správu a vykoná sa nastavená akcia.

• Nikdy – ak prichádzajúca správa obsahuje vašu vlastnú doménu v hlavičke "From:" alebo v odosielateľovi obálky, automaticky sa považuje za sfalšovanú bez ďalšieho overovania. S takouto správou sa vykoná nastavená akcia; dostupné akcie nájdete v kapitole Ochrana prenosu e-mailov.

Automaticky načítať moje domény zo zoznamu Akceptovaných domén

Dôrazne odporúčame mať túto možnosť zapnutú, aby ste si zachovali najvyššiu úroveň ochrany. Zabezpečí sa tým, aby boli pri posudzovaní správ Ochranou pred sfalšovaním identity odosielateľa zohľadnené domény a IP adresy z vašej infraštruktúry.

Zoznam mojich domén

Domény považované za vaše vlastné. Pridajte domény, ktoré sa použijú pri posudzovaní správ spolu s automaticky načítanými doménami zo služby Active Directory. Doména odosielateľa sa porovná s doménami uvedenými v týchto zoznamoch. Ak sa nenájde zhoda, správa je legitímna. Ak sa v zoznamoch nájde zhodná doména, vykoná sa ďalšie overenie podľa nastavenia **Povoliť prichádzajúce e-maily s mojou doménou uvedenou v adrese odosielateľa**.

Zoznam mojich IP adries

IP adresy, ktoré sa považujú za dôveryhodné. Pridajte IP adresy, ktoré sa použijú pri posudzovaní správ spolu s IP

adresami v Zozname ignorovaných IP adries s označením **Je súčasťou internej infraštruktúry**. IP adresa odosielateľa obálky sa porovná s IP adresami uvedenými v týchto zoznamoch. Ak sa nájde zhoda, správa je legitímna. Ak sa v zoznamoch nenájde zhodná IP adresa, ide o sfalšovanú správu a vykoná sa nastavená akcia.

Antiphishingová ochrana

Phishing je pokus o získanie citlivých informácií, akými sú napr. prihlasovacie mená, heslá, PIN kódy a podrobnosti o bankových účtoch a kreditných kartách prostredníctvom e-mailu alebo webových stránok, ktoré sa navonok snažia javiť ako dôveryhodné. Za touto činnosťou sa väčšinou skrývajú nekalé dôvody. Ide o tzv. sociálne inžinierstvo (manipulácia používateľov s cieľom získať od nich dôverné informácie).

ESET Mail Security obsahuje Antiphishingovú ochranu, ktorá zabraňuje používateľom v prístupe na phishingové webové stránky. V prípade e-mailových správ, ktoré môžu obsahovať odkazy smerujúce na phishingové webové stránky, používa ESET Mail Security pokročilú a sofistikovanú metódu analýzy, pomocou ktorej sú telo a predmet prichádzajúcej správy prehľadávané s cieľom identifikácie takýchto odkazov (URL).

Odkazy sú porovnávané voči databáze s phishingovým obsahom. Ak je výsledok analýzy pozitívny, e-mailová správa je považovaná za phishing a ESET Mail Security vykoná príslušnú akciu podľa možnosti zvolenej v rámci nastavenia **Vykonať akciu na phishingovú správu** pre každú vrstvu ochrany (Ochrana prenosu e-mailov, Ochrana databáz e-mailových schránok a Manuálna kontrola databáz e-mailových schránok). Vykonané budú aj akcie pravidla.

Podporované štandardy e-mailového formátu:

- Čistý text
- Iba HTML
- MIME
- Štandard MIME pozostávajúci z viacerých častí (e-mail, ktorý obsahuje aj HTML, aj čistý text)

Podporované HTML entity:

Phishingové správy môžu obsahovať HTML entity, ktorých účelom je vyhnúť sa detekcii Antiphishingovým jadrom. Antiphishingová ochrana však analyzuje a prekladá symboly HTML entít s cieľom nájsť a správne vyhodnotiť skryté URL odkazy.

Jeden konkrétny znak môže mať rôzne podoby. Napríklad, bodka môže byť vyjadrená nasledovne:

Ako sa odkazy väčšinou zobrazujú používateľovi v e-maile	Hodnota	Skryté odkazy nachádzajúce sa v tele správy	Typ
http://www.example-phishing-domain.com/Fraud	.	http://www.example-phishing-domain.com/Fraud	znak
http://www.example-phishing-domain.com/Fraud	&period;	http://www.example-phishing-domain.com/Fraud	názov entity
http://www.example-phishing-domain.com/Fraud	&#x0002E;	http://www.example-phishing-domain.com/Fraud	hexadecimálne číslo entity
http://www.example-phishing-domain.com/Fraud	&#46;	http://www.example-phishing-domain.com/Fraud	decimálne číslo entity

Ak si chcete pozrieť aktivitu antiphishingovej ochrany, prejdite do časti **Protokoly** > Protokol ochrany e-mailových serverov. Nájdete tam informácie o e-mailových správach a phishingových odkazoch, ktoré v nich boli detegované.

Nahlásiť phishingovú stránku

Kliknutím na Nahlásiť môžete nahlásiť phishingovú alebo iným spôsobom podozrivú webovú stránku spoločnosti ESET, kde následne dôjde k vykonaniu potrebnej analýzy.

Pravidlá

Pravidlá vám umožňujú manuálne definovať podmienky filtrovania e-mailových správ, ako aj akcie, ktoré budú vykonané s filtrovanými správami. Môžete tiež definovať podmienky a akcie, ktoré sú rozdielne pre pravidlá Ochrany prenosu e-mailov, Ochrany databáz e-mailových schránok a Manuálnej kontroly databáz e-mailových schránok. Je to z dôvodu, že každý typ ochrany používa pri spracovávaní e-mailových správ trochu odlišný prístup (predovšetkým Ochrana prenosu e-mailov).

Dostupnosť pravidiel pre Ochranu databáz e-mailových schránok, Manuálnu kontrolu databáz e-mailových schránok a Ochranu prenosu e-mailov závisí od toho, aká verzia Microsoft Exchange Servera je nainštalovaná na serveri, kde sa nachádza ESET Mail Security.

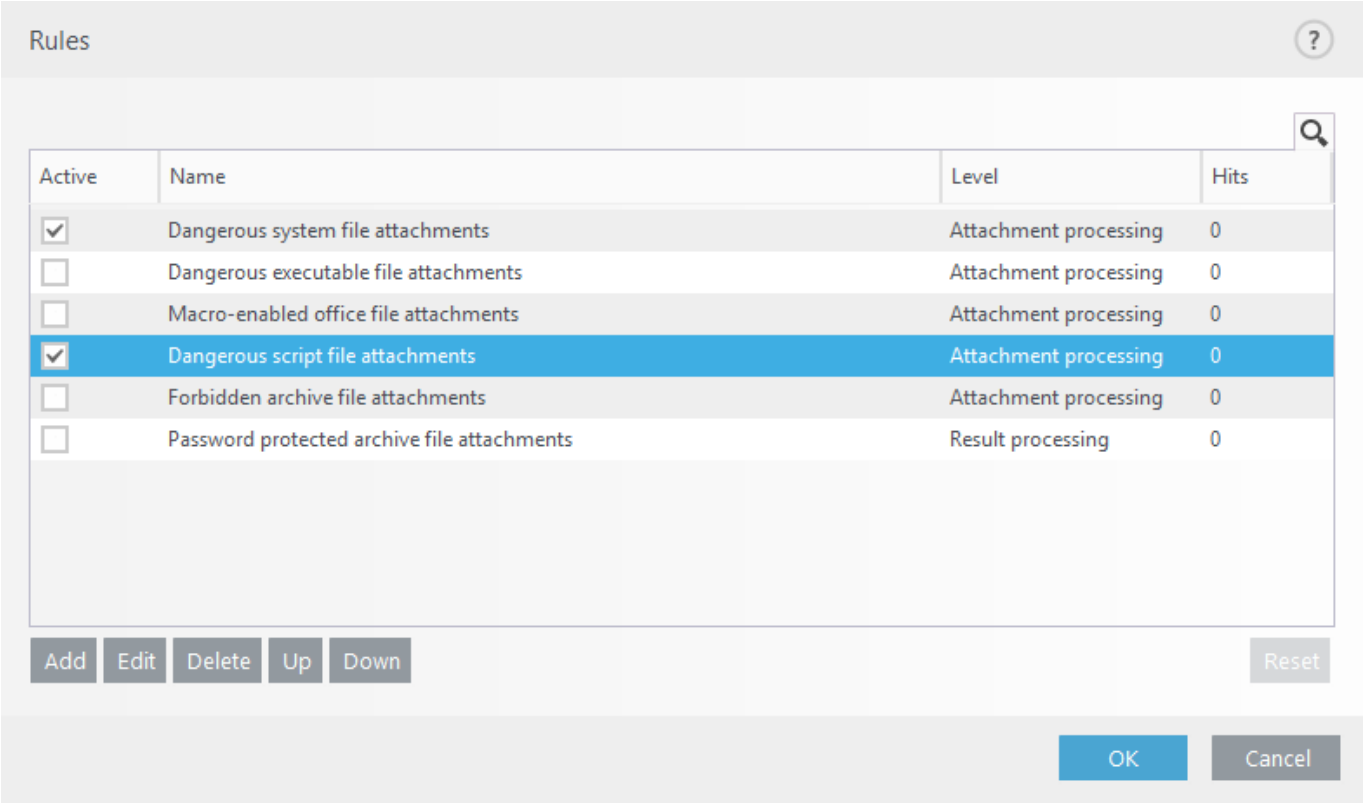
Chybne definované pravidlá pre **Manuálnu kontrolu databáz e-mailových schránok** môžu spôsobiť nezvratné zmeny v databázach e-mailových schránok. Pred prvým spustením manuálnej kontroly databáz e-mailových schránok s novonastavenými pravidlami sa preto vždy uistite, že máte vytvorenú aktuálnu zálohu vašich databáz e-mailových schránok. Taktiež vám dôrazne odporúčame overiť si, či pravidlá fungujú podľa očakávaní. Ak chcete pravidlá otestovať, nastavte pre ne v rámci želanej akcie len možnosť **Zapísať do protokolu udalostí**, pretože všetky ostatné druhy akcií môžu spôsobiť zmeny v databázach e-mailových schránok. Po overení fungovania nastavených pravidiel môžete pre tieto pravidlá pridať aj iné akcie, napríklad akciu **Odstrániť prílohu**.

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

- **Pravidlá filtrovania (1)** – pravidlá sú vyhodnocované pred antispamovou, antivírusovou a antiphishingovou kontrolou.
- **Pravidlá spracovania prílohy (2)** – pravidlá sú vyhodnocované počas antivírusovej kontroly.
- **Pravidlá spracovania výsledku (3)** – pravidlá sú vyhodnocované po antispamovej, antivírusovej a antiphishingovej kontrole.

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

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



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

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

Pravidlá sú pre e-mailovú správu vyhodnocované pri jej spracovávaní Ochranou prenosu e-mailov, Ochranou databáz e-mailových schránok alebo Manuálnou kontrolou databáz e-mailových schránok. Každá z týchto vrstiev ochrany má svoj súbor pravidiel.

Ak dôjde k splneniu podmienok pravidla Ochrany databáz e-mailových schránok alebo Manuálnej kontroly databáz e-mailových schránok, počet zásahov pre pravidlo môže byť dvojnásobný, prípadne väčší. Tieto vrstvy ochrany totiž spracovávajú telo správy a prílohy samostatne a pre každú z týchto častí aj samostatne aplikujú pravidlá. Pravidlá Ochrany databáz e-mailových schránok sú tiež aplikované pri kontrole na pozadí (napríklad, ak ESET Mail Security spustí kontrolu e-mailovej schránky po stiahnutí novej verzie vírusovej databázy), čo môže zvýšiť počet uplatnení pravidiel.

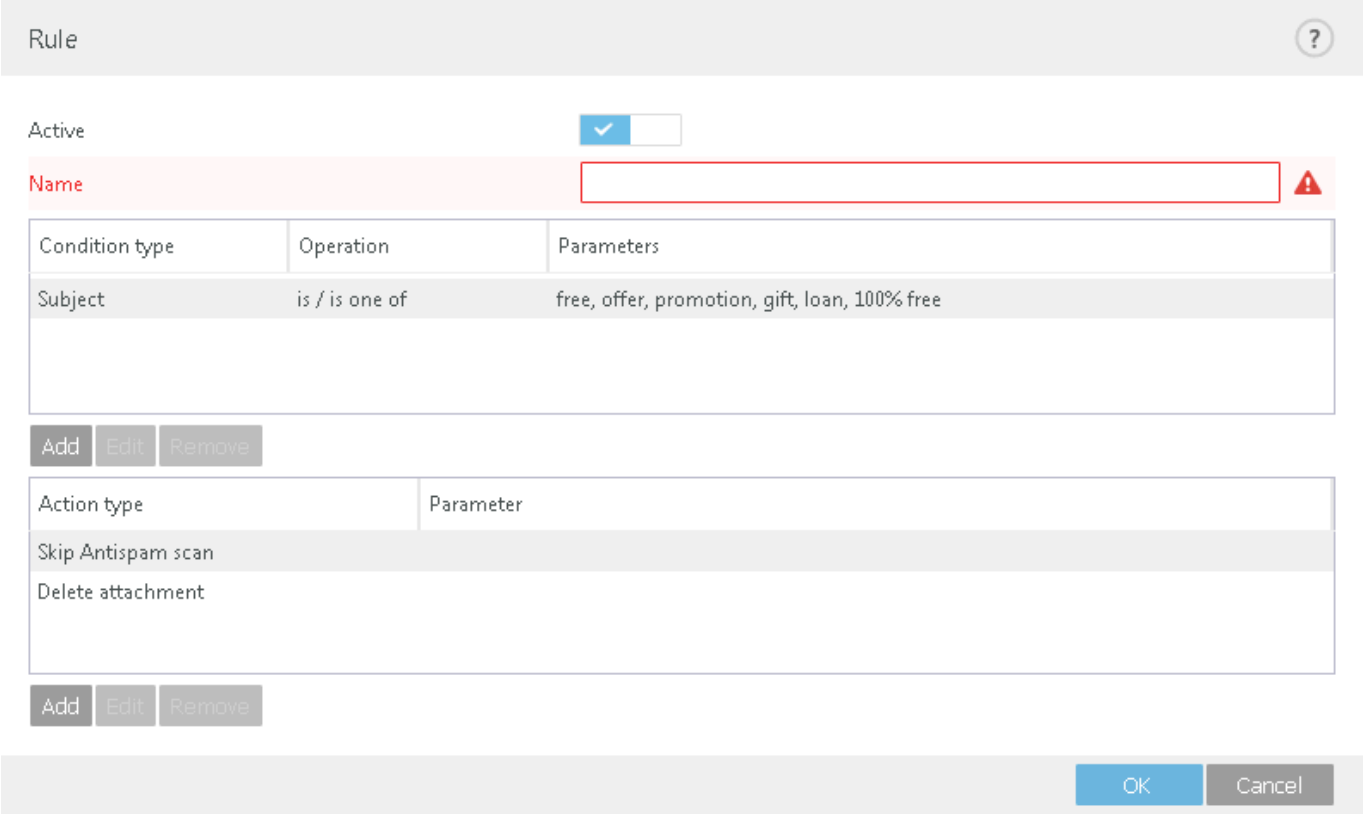
Sprievodca pravidlami

1. Kliknite na **Pridať** (v strede) a otvorí sa okno Podmienka pravidla, umožňujúce vybrať podmienku pravidla, operáciu a hodnotu. Zadávajte najprv podmienky, až potom akcie.

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

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

Pre jedno pravidlo je možné pridať viacero akcií.



3. Po zadefinovaní podmienok a akcií zadajte pre pravidlo **Názov** (názov, podľa ktorého dané pravidlo ľahko rozpoznáte). Tento názov bude zobrazený v zozname pravidiel. Názov je povinné pole, ak je zvýraznené červenou farbou, zadajte názov pravidla do textového poľa a kliknite na **OK**pre vytvorenie pravidla. Červené zvýraznenie nezmizne ani v prípade, že ste zadali názov pravidla, zmizne len ak kliknete na **OK**.

4. Ak chcete pripraviť pravidlá, ktoré budete používať neskôr, môžete kliknúť na tlačidlo prepínača vedľa popisu **Aktívne**, čím pravidlo deaktivujete. Na aktiváciu pravidla použite začiarkavacie políčko umiestnené vedľa pravidla, ktoré chcete aktivovať.

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

V kapitole Príklady pravidiel nájdete informácie o používaní pravidiel a konkrétne príklady ich využitia.

Podmienka pravidla

Tento sprievodca vám umožňuje pridať podmienky pre pravidlá. Najskôr vyberte **Typ** podmienky a **Operáciu**. Zoznam operácií sa mení v závislosti od zvoleného typu podmienky. Následne vyberte **Parameter**. Pole parametra sa mení v závislosti od zvoleného typu a operácie.

Vyberte Veľkosť súboru > je viac ako a do poľa Parameter zadajte 10 MB. Podľa týchto nastavení každý súbor väčší ako 10 MB spustí akciu, ktorú ste pre dané pravidlo nastavili. Z tohto dôvodu by ste mali určiť akciu, ktorá bude vykonaná, keď sa pravidlo aktivuje, ak ste tak ešte neurobili pri nastavovaní parametrov pre dané pravidlo.

Ak chcete importovať svoj vlastný zoznam zo súboru miesto zadávania každej položky manuálne, kliknite pravým tlačidlom v strede okna a z kontextového menu vyberte možnosť **Importovať**. Následne vyhľadajte svoj súbor

(*.xml* alebo *.txt*) obsahujúci položky (oddelené riadkami), ktoré chcete pridať do zoznamu. V takomto prípade vyberte z kontextového menu možnosť **Exportovať**.

Môžete tiež zadať **Regulárny výraz**; v tomto prípade ako Operáciu vyberte **sa zhoduje s regulárnym výrazom** alebo **sa nezhoduje s regulárnym výrazom**.

ESET Mail Security používa std::regex. Pre tvorbu regulárnych výrazov si prezrite ECMAScript syntax. Syntax regulárnych výrazov ani výsledky vyhľadávania nerozlišujú veľké a malé písmená.

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

Nasledujúce typy podmienok sú dostupné pre Ochranu prenosu e-mailov, Ochranu databáz e-mailových schránok a Manuálnu kontrolu databáz e-mailových schránok (niektoré možnosti sa nemusia zobraziť – závisí to od už vybraných podmienok):

Názov podmienky	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Predmet	✓	✓	✓	Vzťahuje sa na správy, ktorých predmet obsahuje/neobsahuje konkrétny reťazec (alebo zadaný regulárny výraz).
Odosielateľ	✓	✓	✓	Vzťahuje sa na správy odoslané konkrétnym odosielateľom.
Odosielateľ obálky (SMTP odosielateľ)	✓	☐	☐	Atribút MAIL FROM obálky použitý pri SMTP pripojení. Používa sa aj pri SPF kontrole.
IP adresa odosielateľa	✓	☐	☐	Vzťahuje sa na správy odoslané odosielateľom so zadanou IP adresou.
Doména odosielateľa obálky/Doména odosielateľa	✓	✓	✓	Vzťahuje sa na správy odoslané z konkrétnej domény.
SMTP doména odosielateľa	✓	☐	☐	Vzťahuje sa na správy odoslané z konkrétnej domény.
Hlavička From – adresa	✓	☐	☐	Hodnota „From:“ obsiahnutá v hlavičkách správ. Ide o adresu, ktorú vidí príjemca, avšak táto adresa nie je overovaná odosielacími servermi, či je odosielateľ oprávnený odosielať správy z danej adresy. Táto hlavička sa často používa na oklamanie odosielateľa.
Hlavička From – zobrazované meno	✓	☐	☐	Hodnota „From:“ obsiahnutá v hlavičkách správ. Ide o zobrazované meno, ktoré vidí príjemca, avšak odosielacie servery neoverujú, či je odosielateľ oprávnený odosielať správy z danej adresy. Táto hlavička sa často používa na oklamanie odosielateľa.
Príjemca	✓	✓	✓	Vzťahuje sa na správy odoslané konkrétnemu príjemcovi.

Názov podmienky	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Organizačné jednotky príjemcu	✓	☐	☐	Vzťahuje sa na správy odoslané príjemcovi z konkrétnej organizačnej jednotky.
Výsledok overenia príjemcu	✓	☐	☐	Vzťahuje sa na správy odoslané príjemcovi overenému v Active Directory.
Názov prílohy	✓	✓	✓	Vzťahuje sa na správy, ktoré obsahujú prílohou s konkrétnym názvom.
Veľkosť prílohy	✓	✓	✓	Vzťahuje sa na správy obsahujúce prílohu, ktorej veľkosť nemá zadanú hodnotu, je v rozmedzí zadaných hodnôt, alebo je väčšia ako zadaná hodnota.
Typ prílohy	✓	✓	✓	Vzťahuje sa na správy s prílohou, ktorá je zadaného typu. Typy súborov sú rozdelené do skupín pre zjednodušený výber, môžete označiť viacero typov súborov alebo celú kategóriu. ESET Mail Security rozpozná správny typ súboru bez ohľadu na príponu. To isté platí aj pre obsah archívu.
Veľkosť správy	✓	☐	☐	Vzťahuje sa na správy s prílohou, ktorých veľkosť nemá zadanú hodnotu, je v rozmedzí zadaných hodnôt, alebo je väčšia ako zadaná hodnota.
E-mailová schránka	☐	✓	☐	Vzťahuje sa na správy nachádzajúce sa v konkrétnej e-mailovej schránke.
Hlavičky správ	✓	✓	☐	Vzťahuje sa na správy, ktorých hlavičky obsahujú zadané dáta.
Telo správy	✓	☐	✓	V tele správy bude vyhľadaná zadaná fráza. Môžete použiť možnosť Odstraňovať HTML značky, čím odstránite HTML značky, atribúty a hodnoty, a ostane len čistý text. V texte tela správy následne prebehne vyhľadávanie.
Interná správa	✓	☐	☐	Vyhodnocuje sa, či správa je alebo nie je interná.
Odchádzajúca správa	✓	☐	☐	Vzťahuje sa na odchádzajúce správy.
Podpísaná správa	✓	☐	☐	Vzťahuje sa na podpísané správy.
Šifrovaná správa	✓	☐	☐	Vzťahuje sa na šifrované správy.
Výsledok antispamovej kontroly	✓	☐	☐	Vzťahuje sa na správy, ktoré sú alebo nie sú označené ako Ham alebo Spam (pozrite príklad).
Výsledok antivírusovej kontroly	✓	✓	✓	Vzťahuje sa na správy, ktoré sú alebo nie sú označené ako infikované.
Výsledok Anti-Phishing kontroly	✓	☐	✓	Vzťahuje sa na správy, ktoré boli vyhodnotené ako phishing.
Čas doručenia	✓	✓	✓	Vzťahuje sa na správy, ktoré boli prijaté pred alebo po zadanom čase a dátume alebo v rozmedzí zadaných dátumov.

Názov podmienky	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Obsahuje archív chránený heslom	✓	✓	☐	Vzťahuje sa na správy, ktoré majú v prílohe archív chránený heslom.
Obsahuje poškodený archív	✓	✓	☐	Vzťahuje sa na správy, ktoré obsahujú v prílohe poškodený archív (takýto archív s najväčšou pravdepodobnosťou nie je možné otvoriť).
Príloha je archív chránený heslom	☐	☐	✓	Vzťahuje sa na prílohy, ktoré sú chránené heslom.
Príloha je poškodený archív	☐	☐	✓	Vzťahuje sa na prílohy, ktoré sú poškodené (takéto prílohy s najväčšou pravdepodobnosťou nie je možné otvoriť).
Názov priečinka	☐	☐	✓	Vzťahuje sa na správy umiestnené v konkrétnom priečinku, a ak daný priečinok neexistuje, bude vytvorený. Toto sa netýka verejných priečinkov.
Výsledok DKIM	✓	☐	☐	Vyhodnocuje sa, či správa prešla alebo neprešla DKIM overením, prípadne či je výsledok dostupný.
Výsledok SPF	✓	☐	☐	Vzťahuje sa na správy, pre ktoré sú výsledky SPF kontroly nasledovné: Pass – IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "+"). Fail – SPF záznam neobsahuje odosielací server alebo IP adresu (SPF kvalifikátor "-"). Soft fail – IP adresa môže alebo nemusí byť oprávnená odosielať z domény (SPF kvalifikátor "~"). Neutral – vlastník domény uviedol v SPF zázname, že nechce prehlásiť, že IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "?"). Nie je k dispozícii – výsledok SPF kontroly None znamená, že doména nezverejnila žiadne záznamy alebo že z danej identity nemohla byť určená žiadna kontrolovateľná doména odosielateľa. Podrobnejšie informácie o SPF nájdete v dokumente RFC 4408. Ak použijete SPF výsledok, whitelisty v časti Filtrovanie a overovanie nebudú zohľadnené pre pravidlá.
Výsledok DMARC	✓	☐	☐	Vyhodnocuje sa, či správa prešla alebo neprešla kontrolou SPF/DKIM, prípadne či je výsledok dostupný.
Má reverzný DNS záznam	✓	☐	☐	Vzťahuje sa na správy s doménou odosielateľa, ktorá má reverzný DNS záznam.
Výsledok NDR	✓	☐	☐	Vzťahuje sa na správy, ktoré neprešli NDR overením.

Názov podmienky	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Výsledok SPF – Hlavička From	✓	☐	☐	Vzťahuje sa na správy, pre ktoré sú výsledky SPF kontroly nasledovné: Pass – IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "+"). Fail – SPF záznam neobsahuje odosielací server alebo IP adresu (SPF kvalifikátor "-"). Soft fail – IP adresa môže alebo nemusí byť oprávnená odosielať z domény (SPF kvalifikátor "~"). Neutral – vlastník domény uviedol v SPF zázname, že nechce prehlásiť, že IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "?"). Nie je k dispozícii – výsledok SPF kontroly None znamená, že doména nezverejnila žiadne záznamy alebo že z danej identity nemohla byť určená žiadna kontrolovateľná doména odosielateľa. Podrobnejšie informácie o SPF nájdete v dokumente RFC 4408. Ak použijete SPF výsledok, whitelisty v časti Filtrovanie a overovanie nebudú zohľadnené pre pravidlá.
Výsledok porovnania odosielateľa obálky a hlavičky From	✓	☐	☐	Porovnáva domény zahrnuté v hlavičke"From:" a v odosielateľovi obálky so zoznamami domén.
Výsledok SPF – HELO	✓	☐	☐	Vzťahuje sa na správy, pre ktoré sú výsledky HELO kontroly nasledovné: Pass – IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "+"). Fail – SPF záznam neobsahuje odosielací server alebo IP adresu (SPF kvalifikátor "-"). Soft fail – IP adresa môže alebo nemusí byť oprávnená odosielať z domény (SPF kvalifikátor "~"). Neutral – vlastník domény uviedol v SPF zázname, že nechce prehlásiť, že IP adresa je oprávnená odosielať z domény (SPF kvalifikátor "?"). Nie je k dispozícii – výsledok SPF kontroly None znamená, že doména nezverejnila žiadne záznamy alebo že z danej identity nemohla byť určená žiadna kontrolovateľná doména odosielateľa. Podrobnejšie informácie o SPF nájdete v dokumente RFC 4408. Ak použijete SPF výsledok, whitelisty v časti Filtrovanie a overovanie nebudú zohľadnené pre pravidlá.

V závislosti od typu podmienky môžete použiť nasledujúce **operácie**:

- **Reťazec:** je, nie je, obsahuje, neobsahuje, zhoduje sa, nezhoduje sa, je v, nie je v, sa zhoduje s regulárnym výrazom, sa nezhoduje s regulárnym výrazom
- **Číslo:** je menej ako, je viac ako, je medzi
- **Text:** obsahuje, neobsahuje, zhoduje sa, nezhoduje sa
- **Dátum a čas:** je menej ako, je viac ako, je medzi
- **Enumerácia:** je, nie je, je v, nie je v

> Pri spracovávaní správ podľa **Názvu prílohy** alebo **Typu prílohy** ESET Mail Security zaobchádza s Microsoft Office (2007+) súborom ako s archívom. To znamená, že jeho obsah je extrahovaný a každý súbor, ktorý je súčasťou Office archívu (napríklad `.docx`, `.xlsx`, .xltx, `.pptx`, `.ppsx`, `.potx` atď.), je skontrolovaný samostatne.

Ak vypnete **Antivírusovú ochranu** v Nastaveniach alebo v časti **Rozšírené nastavenia** (F5) > **Server** > **Antivírusová a antispyvérová ochrana** pre **Ochranu prenosu e-mailov a Ochranu databáz e-mailových schránok**, ovplyvní to nasledujúce podmienky pravidla:

- Názov prílohy
- Veľkosť prílohy
- Typ prílohy
- Výsledok antivírusovej kontroly
- Príloha je archív chránený heslom
- Príloha je poškodený archív
- Obsahuje poškodený archív
- Obsahuje archív chránený heslom

Akcia pravidla

Pri vytvorení pravidla môžete vybrať akcie, ktoré budú vykonané so správami a/alebo prílohami, ktoré spĺňajú podmienky pravidla.

> Pre jedno pravidlo je možné pridať viacero akcií.

Nasledujúce akcie sú dostupné pre Ochranu prenosu e-mailov, Ochranu databáz e-mailových schránok a Manuálnu kontrolu databáz e-mailových schránok (niektoré možnosti sa nemusia zobraziť – závisí to od už vybraných podmienok):

Názov akcie	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Presunúť správu do karantény	✓	☐	☐	Správa nebude doručená príjemcovi, ale bude presunutá do e-mailovej karantény. Používatelia, ktorí nie sú správcami, môžu e☐mailové správy presunuté do karantény týmto pravidlom uvoľňovať prostredníctvom webového prostredia karantény alebo reportov o karanténe.
Uložiť prílohu do karantény	✓	✓	✓	Uloží prílohu e-mailu do súborovej karantény. E-mail bude doručený príjemcovi bez prílohy (príloha bude mať nulovú dĺžku).
Odstrániť prílohu	✓	✓	✓	Odstráni prílohu zo správy. Správa bude doručená príjemcovi bez prílohy.
Odmietnuť správu	✓	☐	☐	Odstráni správu. Pre prichádzajúce správy prijímané prostredníctvom SMTP by mal odosielací server vygenerovať NDR (Non-Delivery Report), čiže správu o nedoručení.
Potichu odhodiť správu	✓	☐	☐	Správa bude vymazaná bez vygenerovania správy o nedoručení (NDR).
Nastaviť hodnotu SCL	✓	☐	☐	Umožňuje zmeniť alebo nastaviť konkrétnu hodnotu SCL.
Odoslať správcovi oznámenie o udalosti	✓	✓	✓	Odošle oznámenie o udalosti príjemcovi, ktorý je definovaný v sekcii E-mailové oznámenia. Je potrebné povoliť funkciu Posielať oznámenia o udalostiach e-mailom. Následne môžete pri vytváraní pravidla nastaviť formát správ o udalostiach (viac informácií nájdete v popise danej položky). Môžete tiež pozmeniť úroveň podrobnosti správ o udalostiach, výber je však ovplyvnený tým, aká minimálna úroveň podrobnosti je zvolená v nastaveniach E-mailových oznámení.
Preskočiť antispamovú kontrolu	✓	☐	☐	Správa nebude kontrolovaná antispamovým jadrom.
Preskočiť antivírusovú kontrolu	✓	✓	✓	Správa nebude kontrolovaná antivírusovým jadrom.
Preskočiť antiphishingovú kontrolu	✓	☐	✓	Správa nebude analyzovaná antiphishingovou ochranou.
Preskočiť kontrolu ESET LiveGuard Advanced	✓	☐	☐	Správa nebude vyhodnotená ochranou ESET LiveGuard Advanced.
Vyhodnotiť ďalšie pravidlá	✓	✓	✓	Umožňuje vyhodnocovanie ďalších pravidiel. Používateľ môže zadať viacero podmienok a viaceré akcie pre dané podmienky.

Názov akcie	Ochrana prenosu e-mailov	Ochrana databáz e-mailových schránok	Manuálna kontrola databáz e-mailových schránok	Popis
Zapísať do protokolu udalostí	✓	✓	✓	Umožňuje zápis informácie o vykonaní pravidla do protokolu a voľbu formátu správ o udalostiach (viac informácií nájdete v popise danej položky). Ak nastavíte akciu Zapísať do protokolu udalostí pre Ochranu databáz e-mailových schránok s parametrom %IPAddress%, typ protokolu Udalosti v časti Protokoly bude pre túto konkrétnu udalosť prázdny. Je to z dôvodu, že na úrovni ochrany databáz e-mailových schránok nie je žiadna IP adresa. Niektoré možnosti nie sú dostupné na všetkých úrovniach ochrany: %IPAddress% – ignorovaná Manuálnou kontrolou databáz e-mailových schránok a Ochranou databáz e-mailových schránok. %Mailbox% – ignorovaná Ochranou prenosu e-mailov. Nasledujúce možnosti sa vzťahujú iba na Pravidlá spracovania prílohy: %Attname% – ignorovaná Pravidlami filtrovania a Pravidlami spracovania výsledku. %Attsize% – ignorovaná Pravidlami filtrovania a Pravidlami spracovania výsledku.
Pridať hlavičku do správy	✓	☐	☐	Pridá do hlavičky správy zadaný reťazec.
Pridať predponu predmetu	✓	☐	☐	Pridá predponu do predmetu správy.
Nahradiť prílohu informáciou o akcii	☐	✓	✓	Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii.
Odstrániť polia hlavičiek	✓	☐	☐	Odstráni polia z hlavičky správy podľa zadaných parametrov.
Odstrániť správu	☐	✓	✓	Vymaže infikovanú správu.
Presunúť správu do priečinka	☐	☐	✓	Správa bude presunutá do konkrétneho priečinka.
Presunúť správu do koša	☐	☐	✓	Presunie správu do koša na strane príjemcu.
Aplikovať DMARC politiku	✓	☐	☐	Ak je splnená podmienka DMARC výsledku, e-mailová správa bude spracovaná podľa politiky špecifikovanej v DMARC DNS zázname domény odosielateľa.

Taktiež, ak vypnete **Antivírusovú ochranu** v Nastaveniach alebo v časti **Rozšírené nastavenia** (F5) > **Server** > **Antivírusová a antispyvérová ochrana** pre **Ochranu prenosu e-mailov**, ovplyvní to nasledujúce akcie pravidla:

- Uložiť prílohu do karantény
- Odstrániť prílohu

Príklady pravidiel

Presunúť do karantény správy, ktoré obsahujú malvér, alebo prílohu, ktorá je chránená heslom, zašifrovaná alebo poškodená

Cieľ: Presunúť do karantény správy, ktoré obsahujú malvér, alebo prílohu, ktorá je chránená heslom, zašifrovaná alebo poškodená
Vytvorte nasledujúce pravidlo pre **Ochranu prenosu e-mailov**:
Podmienka
- Typ: Výsledok antivírusovej kontroly
- Operácia: nie je
- Parameter: Neinfikované objekty

Akcia
Typ: Presunúť správu do karantény

Presunúť správy, ktoré neprešli SPF kontrolou, do priečinka s nevyžiadanou poštou

Cieľ: Presunúť správy, ktoré neprešli SPF kontrolou, do priečinka s nevyžiadanou poštou
Vytvorte nasledujúce pravidlo pre **Ochranu prenosu e-mailov**:
Podmienka
- Typ: Výsledok SPF
- Operácia: je
- Parameter: Fail

Akcia
- Typ: Nastaviť hodnotu SCL
- Hodnota: 5

Nastavte hodnotu podľa parametru `SCLJunkThreshold` príkazu cmdlet `Get-OrganizationConfig` vášho Exchange servera. Viac informácií nájdete v tomto článku spoločnosti Microsoft.

Overiť e-mailovú správu s podozrením na sfalšovanie identity odosielateľa

Cieľ: Overiť e-mailovú správu s podozrením na sfalšovanie identity odosielateľa. Ak je v hlavičke „From:“ alebo v odosielateľovi obálky uvedená vaša vlastná doména, preverí sa výsledok kontroly SPF. Ak je výsledok SPF neutrálny, e□mail sa presunie do karantény, zapíše sa do protokolu udalostí a správca dostane upozornenie.
Podmienka
- Typ: Výsledok porovnania odosielateľa obálky a hlavičky From
- Operácia: je
- Parameter: Zhoduje sa
- Typ: Výsledok SPF – Hlavička From
- Operácia: je
- Parameter: Neutral

Akcia
Typ: Presunúť správu do karantény, Zapísať do protokolu udalostí a Odoslať správcovi oznámenie o udalosti

Odhodiť správy od konkrétnych odosielateľov

Cieľ: Odhodiť správy od konkrétnych odosielateľov
Vytvorte nasledujúce pravidlo pre **Ochranu prenosu e-mailov**:
Podmienka
- Typ: Odosielateľ
- Operácia: je / je jedno z
- Parameter: spammer1@domain.com, spammer2@domain.com

Akcia
Typ: **Potichu odhodiť správu**

Úprava prednastaveného pravidla

Cieľ: Úprava prednastaveného pravidla
Podrobnosti: Povolenie správ, ktoré majú v prílohe archív, zo zadefinovaných IP adries (napríklad z interných systémov) v rámci pravidla blokujúceho prijímanie archívov v prílohe správ.
Otvorte súbor pravidiel pre **Ochranu prenosu e-mailov**, vyberte pravidlo **Nedovolené archívne prílohy** a kliknite na **Upraviť**.
Podmienka
- Typ: IP adresa odosielateľa
- Operácia: nie je / nie je žiadne
- Parameter: 1.1.1.2, 1.1.1.50-1.1.1.99

Telo správy

Cieľ: Presunúť do karantény správy, ktorých telo obsahuje určitý reťazec
Vytvorte nasledujúce pravidlo pre **Ochranu prenosu e-mailov**:
Podmienka
- Typ: Telo správy
- Operácia: obsahuje/obsahuje jedno z, kliknite na Pridať a zadajte URL adresu webovej stránky, prípadne časť adresy

Akcia
Typ: Presunúť správu do karantény

Ukladať správy pre neexistujúcich príjemcov

Cieľ: Ukladať správy pre neexistujúcich príjemcov
Podrobnosti: Ak chcete do karantény presúvať všetky e-mailové správy pre neexistujúcich príjemcov (bez ohľadu na výsledok Antivírusovej a Antispamovej ochrany).
Podmienka
- Typ: Výsledok overenia príjemcu
- Operácia: je
- Parameter: Obsahuje neplatného príjemcu

Akcia
Typ: Presunúť správu do karantény

Ochrana prenosu e-mailov

V tejto sekcii môžete nastaviť akcie pre zachytené hrozby na prenosovej vrstve osobitne pre každý ESET Mail Security modul (Antivírus, Anti-Phishing a Antispam). Vykonať akciu, ak nie je možné liečenie:

- **Žiadna akcia** – ponechá správy, ktoré nemôžu byť vyliečené.

- **Presunúť správu do karantény** – odošle infikované správy do e‑mailovej karantény.

- **Odmietnuť správu** – odmietne infikovanú správu.

- **Potichu odhodiť správu** – správa bude vymazaná, odosielateľovi správy však nebude zaslané NDR (Non-Delivery Report).

> Ak vyberiete možnosť **Žiadna akcia** a zároveň máte **Úroveň liečenia** nastavenú na **Neliečiť** v parametroch ThreatSense v časti Antivírusová a antispyvérová ochrana, farba stavu ochrany sa zmení na žltú. Je to preto, že ide o bezpečnostné riziko a túto kombináciu neodporúčame používať. Zmeňte niektoré z týchto nastavení pre dosiahnutie adekvátnej úrovne ochrany.

Vykonať akciu na phishingovú správu:

- **Žiadna akcia** – ponechá správy aj v prípade, že sú označené ako phishing.

- **Presunúť správu do karantény** – presunie správy, ktoré sú označené ako phishing, do e‑mailovej karantény.

- **Odmietnuť správu** – odmietne správu označenú ako phishing.

- **Potichu odhodiť správu** – správa bude vymazaná, odosielateľovi správy však nebude zaslané NDR (Non-Delivery Report).

Vykonať akciu na spamovú správu:

- **Žiadna akcia** – ponechá správy aj v prípade, že sú označené ako spam.

- **Presunúť správu do karantény** – presunie správy, ktoré sú označené ako spam, do e‑mailovej karantény.

- **Odmietnuť správu** – odmietne správu označenú ako spam.

- **Potichu odhodiť správu** – správa bude vymazaná, odosielateľovi správy však nebude zaslané NDR (Non-Delivery Report).

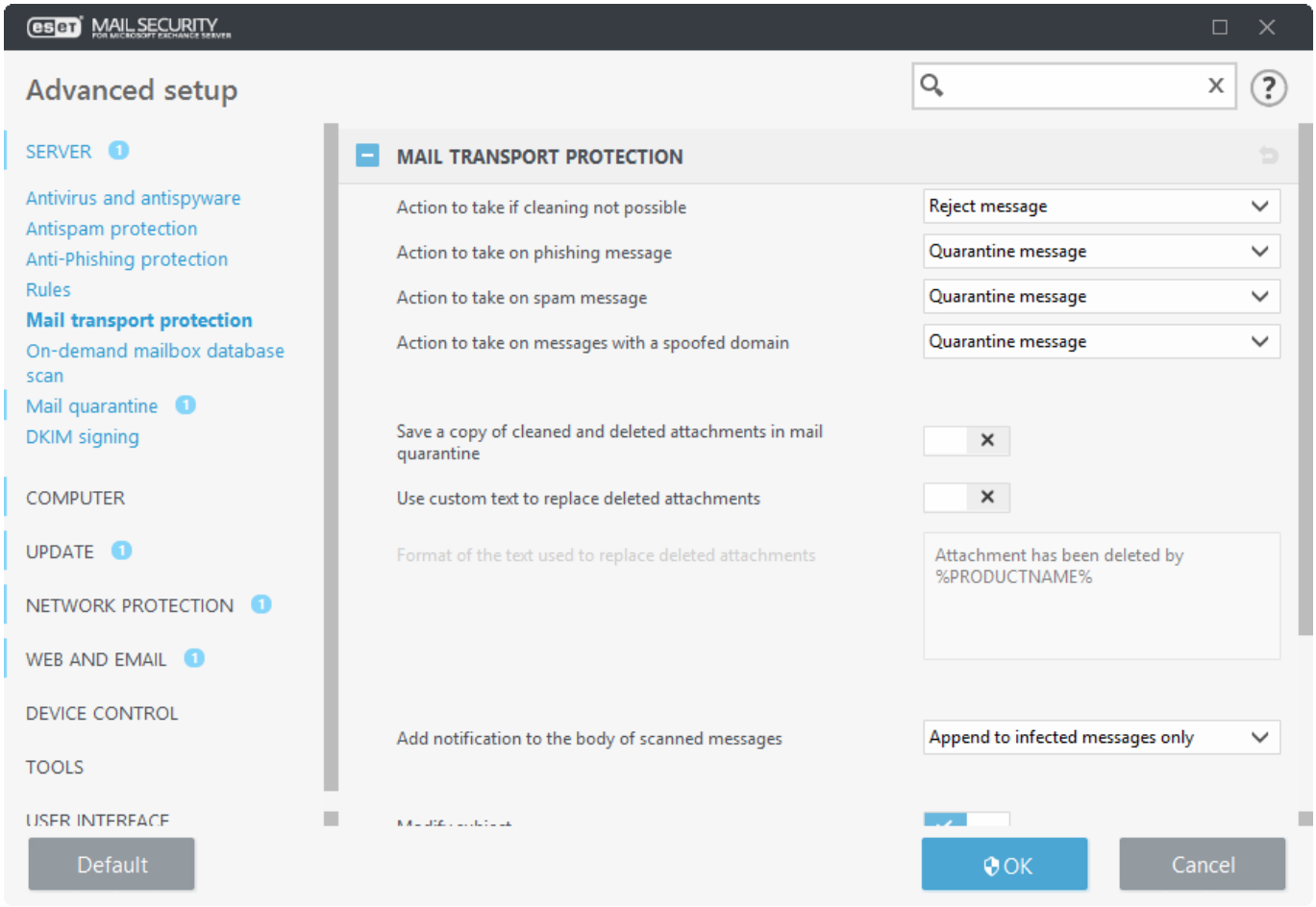
Akcia pri zachytení správy so sfalšovanou doménou:

- **Žiadna akcia** – ponechá správy, aj keď sú označené ako sfalšované.

- **Presunúť správu do karantény** – presunie správy, ktoré sú označené ako sfalšované, do e‑mailovej karantény.

- **Odmietnuť správu** – odmietne správu, ktorá je označená ako sfalšovaná.

- **Potichu odhodiť správu** – správa bude vymazaná, odosielateľovi správy však nebude zaslané NDR (Non-Delivery Report).



Uložiť kópiu vyliečených a odstránených príloh do e‑mailovej karantény

Kópia pôvodného súboru prílohy sa uloží do e‑mailovej karantény.

Nahradiť odstránené prílohy vlastným textom

Po povolení môžete upresniť vlastný text, ktorý nahradí odstránené prílohy.

Formát textu nahrádzajúceho odstránené prílohy

Nahradí prílohu textovým súborom obsahujúcim podrobné informácie o vykonanej akcii. Ak ste nastavenie vyššie povolili (**Použiť vlastný text**), môžete upraviť predvolený text s vašimi vlastnými podrobnosťami pomocou premenných.

Pomocou premenných si prispôsobte text, ktorým sa v e‑mailovej správe nahradia odstránené prílohy.
%PRODUCTNAME%
%FILENAME%
%VIRUSNAME%
%DETECTIONNAME%
%FILESIZE%
Program *%PRODUCTNAME%* odstránil prílohu %FILENAME% s veľkosťou *%FILESIZE%* z dôvodu detekcie *%DETECTIONNAME%*.
Prispôsobený formát textu sa vo výsledku zobrazí nasledovne:
Program ESET Mail Security odstránil prílohu *eicar_com.zip* s veľkosťou 184 B z dôvodu detekcie *Eicar test*.

Zamietavá SMTP odpoveď

Môžete zadať **Kód odpovede**, **Stavový kód** a **Správu odpovede**, ktoré definujú dočasne zamietnutú SMTP

odpoveď odoslanú na SMTP server, z ktorého prišla zamietnutá správa. Správu odpovede môžete zadať v nasledujúcom formáte:

Kód odpovede	Stavový kód	Správa odpovede
250	2.5.0	Requested mail action okay, completed
451	4.5.1	Requested action aborted:local error in processing
550	5.5.0	Requested action not taken:mailbox unavailable
554	5.6.0	Invalid content

Pri definovaní odmietavej SMTP odpovede môžete tiež použiť systémové premenné.

Pridať upozornenie do tela skontrolovaných správ ponúka tri možnosti:

- **Nepridávať do správ** – do správy nebudú pridané žiadne doplňujúce informácie.
- **Pridávať iba do infikovaných správ** – táto možnosť sa týka iba infikovaných správ.
- **Pridávať do všetkých správ** (neplatí pre interné správy) – označené budú všetky správy.

Upraviť predmet

Ak je táto možnosť zapnutá, môžete upraviť šablóny pridávané do predmetu infikovaných, spamových alebo phishingových správ.

Šablóna pridaná do predmetu infikovaných správ

ESET Mail Security pridá poznámku do predmetu e-mailu s hodnotou zadanou v poli **Šablóna pridaná do predmetu infikovaných správ** (predvolená hodnota je `[found threat %VIRUSNAME%]`). Táto modifikácia môže byť použitá na automatizáciu filtrovania infikovaných správ pomocou filtrovania e-mailov s určitým predmetom, napr. použitím pravidiel alebo vložením takýchto e-mailových správ na strane klienta (ak to daný e-mailový klient podporuje) do osobitného priečinka.

Šablóna pridaná do predmetu nevyžiadaných správ

ESET Mail Security pridá poznámku do predmetu e-mailu s hodnotou zadanou v poli **Šablóna pridaná do predmetu nevyžiadaných správ** (predvolená hodnota je `[SPAM]`). Táto úprava môže byť použitá na automatizáciu filtrovania nevyžiadaných správ s určitým textom v predmete správy pomocou pravidiel alebo na strane e-mailového klienta (ak je to podporované e-mailovým klientom) presunutím takejto správy do oddeleného priečinka.

Šablóna pridaná do predmetu phishingových správ

ESET Mail Security pridá poznámku do predmetu e-mailu s hodnotou zadanou v poli **Šablóna pridaná do predmetu phishingových správ** (predvolená hodnota je `[PHISH]`). Táto úprava môže byť použitá na automatizáciu filtrovania nevyžiadaných správ s určitým textom v predmete správy pomocou pravidiel alebo na strane e-mailového klienta (ak je to podporované e-mailovým klientom) presunutím takejto správy do oddeleného priečinka.

Pri upravovaní textu, ktorý bude pridaný do predmetu správy, môžete použiť aj systémové premenné.

Ochrana prenosu e-mailov – Rozšírené nastavenia

V tejto sekcii môžete bližšie špecifikovať nastavenia ochrany prenosu e-mailov.

Skontrolovať aj správy prijaté z overených alebo interných pripojení pomocou

Vyberte, ktoré typy kontrol budú vykonané na správach prijatých z overených alebo lokálnych serverov. Kontrola týchto správ je odporúčaná, keďže sa tak zvyšuje úroveň ochrany, no nevyhnutná je v tom prípade, ak používate vstavaný nástroj Microsoft SBS POP3 Connector na načítavanie e-mailových správ z externých POP3 serverov alebo e-mailových služieb (napríklad Gmail.com, Outlook.com, Yahoo.com, gmx.dem atď.). Viac informácií nájdete v časti POP3 Connector a antispam.

Z roletového menu vyberte úroveň ochrany. Odporúčame vám použiť **Antivírusovú ochranu** (predvolené nastavenie), a to najmä pre interné spojenia, pretože je nepravdepodobné, že by mohlo dôjsť k distribúcii phishingových alebo spamových správ prostredníctvom vašich lokálnych serverov. Môžete však zvýšiť úroveň ochrany pre Microsoft SBS POP3 Connector vybraním **Antivírusovej a antiphishingovej ochrany** alebo dokonca **Antivírusovej, antiphishingovej a antispamovej ochrany**.

> Toto nastavenie zapne alebo vypne Antispamovú ochranu pre overených používateľov a interné spojenia. E-maily prijaté z neoverených spojení sú kontrolované vždy, a to aj v prípade, že bola zvolená možnosť **Nekontrolovať**.

> Interné správy z nástroja Outlook sú v rámci organizácie odosielané vo formáte TNEF (Transport Neutral Encapsulation Format). Formát TNEF nie je podporovaný antispamom. To znamená, že interné e-maily vo formáte TNEF nebudú kontrolované na prítomnosť spamu bez ohľadu na nastavenie **Skontrolovať aj správy prijaté z overených alebo interných pripojení pomocou**.

Pred spustením kontroly odstrániť existujúcu SCL hlavičku

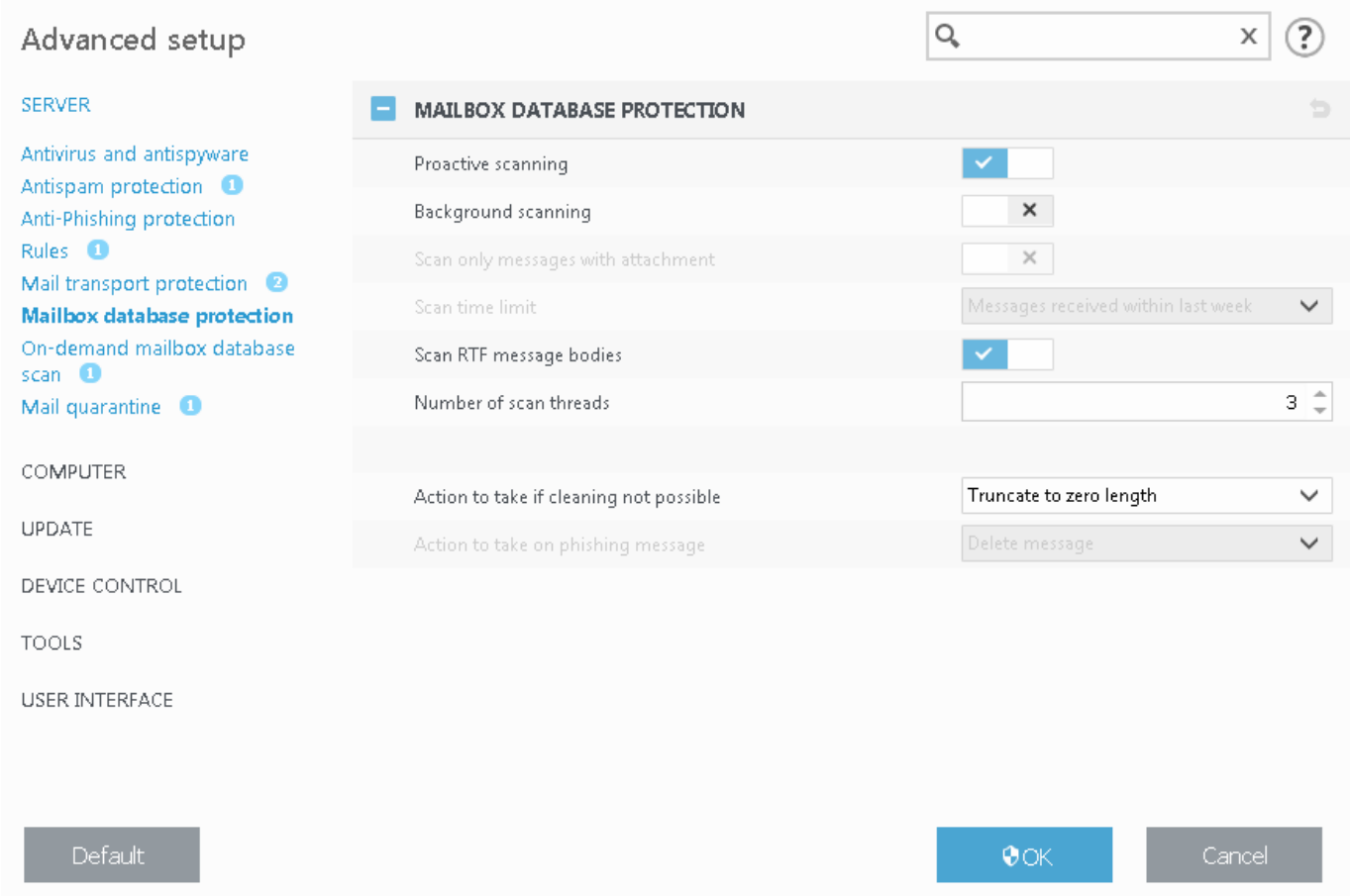
Táto možnosť je v predvolených nastaveniach zapnutá. Túto funkciu môžete vypnúť, ak potrebujete, aby bola SCL (Spam Confidence Level) hlavička zachovaná.

Zapisovať výsledky kontroly do hlavičiek správ

Ak je táto možnosť povolená, výsledky kontroly sú zapisované do hlavičiek správ. Tieto hlavičky správ sa začínajú výrazom `X_ESET`, vďaka čomu sú ľahko rozpoznateľné (napr. `X_EsetResult` alebo `X_ESET_Antispam`).

Ochrana databáz e-mailových schránok

Ak je povolená **Proaktívna kontrola**, prichádzajúce správy budú kontrolované v rovnakom poradí, v akom boli prijaté. Ak používateľ otvorí správu, ktorá ešte nebola kontrolovaná, bude táto správa skontrolovaná ihneď, a to pred ostatnými, ktoré boli na rade.



Kontrola na pozadí

Kontrola na pozadí umožňuje kontrolu všetkých správ prebiehajúcu na pozadí (kontrola prebieha v e-mailovej schránke a verejných priečinkoch, napríklad v databáze Exchange). Microsoft Exchange Server rozhoduje, či kontrolu na pozadí vykoná, alebo nie, na základe rôznych faktorov, ako je aktuálne zaťaženie systému, počet aktívnych používateľov atď. Microsoft Exchange Server si uchováva záznam o kontrolovaných správach a verzii použitého detekčného jadra.

Ak otvárate správu, ktorá nebola kontrolovaná pomocou najnovšieho detekčného jadra, Microsoft Exchange Server odošle správu do ESET Mail Security, kde musí byť skontrolovaná pred otvorením správy v e-mailovom kliente. V sekcii **Časový limit kontroly** si môžete vybrať možnosť Kontrolovať iba správy s prílohami a filtrovať správy podľa času, kedy boli prijaté:

- Všetky správy
- Správy prijaté za posledný rok
- Správy prijaté za posledných 6 mesiacov
- Správy prijaté za posledné 3 mesiace
- Správy prijaté za posledný mesiac
- Správy prijaté za posledný týždeň

Vzhľadom na to, že kontrola na pozadí môže mať vplyv na zaťaženie systému (kontrola sa vykonáva po každej aktualizácii detekčného jadra), odporúčame naplánovať spustenie kontroly počas nepracovných hodín. Naplánovanú kontrolu na pozadí je možné nastaviť pomocou špeciálnej úlohy v Plánovači.

Pri plánovaní úlohy kontroly na pozadí môžete nastaviť čas spustenia, počet opakovaní a ďalšie parametre dostupné v Plánovači. Po tom, čo bude úloha naplánovaná, sa objaví v zozname naplánovaných úloh a môžete meniť jej parametre, odstrániť ju alebo ju dočasne deaktivovať.

Počet vlákien kontroly

Počet vlákien kontroly môže byť v rozsahu od 1 do 21. Môžete nastaviť počet nezávislých vlákien kontroly používaných v rovnakom čase. Vyšší počet vlákien kontroly na multiprocesorových počítačoch môže urýchliť kontrolu. Pre čo najlepší výkon programu odporúčame použiť rovnaký počet skenovacích jadier ThreatSense a vlákien kontroly.

Kontrolovať telo správ vo formáte RTF

Povolením tejto možnosti sa aktivuje kontrola tiel správ vo formáte RTF. Telá správ vo formáte RTF môžu obsahovať macro vírusy.

Bežné textové správy nie sú kontrolované pomocou VSAPI.

Vykonať akciu, ak nie je možné liečenie:

- **Žiadna akcia** – v správe nebudú vykonané žiadne zmeny.
- **Skrátiť na nulovú dĺžku** – príloha bude skrátená na nulovú dĺžku.
- **Nahradiť obsah informáciou o akcii** – pôvodné telo správy bude nahradené informáciou o akcii. Obsah prílohy bude nahradený informáciou o akcii.
- **Odstrániť správu** – správa bude odstránená.

Vykonať akciu na phishingovú správu:

- **Žiadna akcia** – v správe nebudú vykonané žiadne zmeny.
- **Odstrániť správu** – správa bude odstránená.

K verejným priečinkom sa pristupuje rovnakým spôsobom ako k e-mailovým schránkam. Z toho vyplýva, že sú kontrolované.

Kontrola na pozadí

Tento typ úlohy umožňuje kontrolu databáz na pozadí prostredníctvom VSAPI. V podstate umožňuje vášmu Exchange serveru v prípade potreby spustiť kontrolu na pozadí. Kontrolu spúšťa samotný Exchange Server, čo znamená, že závisí od neho, či bude kontrola v povolenom čase spustená.

Odporúčame spúšťať túto úlohu mimo špičky, keď váš Exchange Server nie je zaneprázdnený, čiže napríklad v noci. Je to preto, lebo kontrola na pozadí môže do určitej miery zaťažiť váš systém. Taktiež, časový rámec kontroly by sa nemal prekrývať so žiadnymi zálohovaniami, ktoré môžu byť spustené na vašom Exchange serveri, aby sa predišlo prípadným problémom s výkonom alebo dostupnosťou.

Aby mohla byť naplánovaná úloha spustená, musí byť povolená Ochrana databáz e-mailových schránok. Tento typ ochrany je dostupný len pre Microsoft Exchange Server 2010 a 2007 pre rolu Mailbox Server (Microsoft Exchange 2010 a 2007).

Časový limit (v hodinách)

Upresnite, koľko hodín môže byť kontrola databáz na pozadí spustená vaším Exchange serverom od času spustenia naplánovanej úlohy. Po dosiahnutí časového limitu Exchange Server kontrolu na pozadí zastaví.

Manuálna kontrola databáz e-mailových schránok

Ak používate Microsoft Exchange Server 2007 alebo 2010, môžete si vybrať medzi Ochranou databáz e-mailových schránok a **Manuálnou kontrolou databáz e-mailových schránok**, nie je však možné mať aktivované oba tieto typy ochrany súčasne. Ak sa rozhodnete pre **Manuálnu kontrolu databáz e-mailových schránok**, integrácia **Ochrany databáz e-mailových schránok** musí byť vypnutá v **Rozšírených nastaveniach** (**F5**) v časti Server. V opačnom prípade nebude **Manuálna kontrola databáz e-mailových schránok** dostupná.

Adresa hostiteľa

Názov alebo IP adresa servera so spusteným procesom EWS (Exchange Web Services).

Prihlasovacie meno

Zadajte prihlasovacie údaje používateľa, ktorý má prístup do EWS (Exchange Web Services).

Prihlasovacie heslo

Kliknite na **Nastaviť** vedľa položky **Prihlasovacie heslo** a zadajte heslo pre daného používateľa.

Aby bolo možné kontrolovať verejné priečinky, používateľský účet používaný pre Manuálnu kontrolu databáz e-mailových schránok musí mať e-mailovú schránku. V opačnom prípade sa v Protokole kontroly databáz zobrazí chybové hlásenie *Failed to load public folders* (Nepodarilo sa načítať verejné priečinky), ako aj podrobnejšie hlásenie, ktoré zobrazí Exchange.

Spôsob prístupu k e-mailovej schránke

Môžete si vybrať spôsob prístupu k e-mailovej schránke:

- **Zosobnenie**

Jednoduchšia a rýchlejšia voľba je **rola ApplicationImpersonation**, ktorú je potrebné priradiť ku kontrolujúcemu účtu.

Priradiť používateľovi rolu ApplicationImpersonation

Ak táto možnosť nie je dostupná, bude potrebné najprv zadať **Prihlasovacie meno**. Pre automatické priradenie roly ApplicationImpersonation k vybranému používateľovi kliknite na **Priradiť**. Rolu ApplicationImpersonation môžete k používateľskému účtu priradiť aj manuálne. Pre používateľský účet bude vytvorená nová neobmedzená EWS Throttling politika. Viac informácií nájdete v kapitole Podrobnosti účtu kontroly databáz.

- **Delegovanie**

Pri tomto type prístupu sa vyžadujú prístupové práva na jednotlivých e-mailových schránkach, avšak poskytuje vyššie rýchlosti pri kontrole väčšieho množstva dát.

Priradiť používateľovi delegovaný prístup

Ak táto možnosť nie je dostupná, bude potrebné najprv zadať Prihlasovacie meno. Kliknutím na Priradiť automaticky pridelíte vybranému používateľovi úplný prístup ku všetkým používateľským a zdieľaným e-mailovým schránkam. Pre používateľský účet bude vytvorená nová neobmedzená EWS Throttling politika. Viac informácií nájdete v kapitole Podrobnosti účtu kontroly databáz.

Používať SSL

Túto možnosť je potrebné povoliť, ak máte EWS (Exchange Web Services) nastavené v IIS tak, aby vyžadovalo SSL protokol. Ak je SSL povolené, certifikát Exchange servera je potrebné importovať na systém, na ktorom je spustený program ESET Mail Security (v prípade, že sú roly Exchange servera na rôznych serveroch). Nastavenia pre Exchange Web Services (EWS) nájdete v IIS v sekcii Sites/Default website/EWS/SSL Settings.

Možnosť **Používať SSL** vypnite len v prípade, ak máte EWS (Exchange Web Services) nastavené v IIS tak, aby nevyžadovalo SSL protokol.

Ignorovať chyby certifikátu servera

Ak používate certifikát s vlastným podpisom, chyby certifikátu servera môžete ignorovať.

Certifikát klienta

Musí byť zadaný len v prípade, že EWS vyžaduje klientsky certifikát. Pre výber certifikátu kliknite na tlačidlo **Vybrať**.

Vykonať akciu, ak nie je možné liečenie

Toto pole vám umožňuje blokovať infikovaný obsah.

- **Žiadna akcia** – s infikovanou časťou správy nebude vykonaná žiadna akcia.
- **Presunúť správu do koša** – táto možnosť nie je podporovaná pre položky verejného priečinka. Miesto toho bude použitá akcia Odstrániť objekt.
- **Odstrániť objekt** – infikovaná časť správy bude vymazaná.
- **Odstrániť správu** – vymaže sa celá správa vrátane jej infikovanej časti.
- **Nahradiť objekt informáciou o akcii** – odstráni objekt a pridá do správy informáciu o tom, že objekt bol odstránený.

Vykonať akciu na phishingovú správu:

- **Žiadna akcia** – ponechá správy, aj keď sú označené ako phishingové.
- **Presunúť správu do koša** – táto možnosť nie je podporovaná pre položky verejného priečinka. Miesto toho bude použitá akcia Odstrániť objekt.
- **Odstrániť správu** – vymaže sa celá správa vrátane jej infikovanej časti.

Počet vlákien kontroly

Môžete definovať, koľko vlákien by mal program ESET Mail Security pri kontrole databáz využívať. Čím vyššie je číslo, tým lepší je výkon. Toto má však vplyv na to, koľko prostriedkov bude použitých. Predvolená hodnota je nastavená na 4 kontrolujúce vlákna.

Ak nakonfigurujete Manuálnu kontrolu databáz e-mailových schránok tak, že bude využívať príliš veľký počet vlákien, môže to do veľkej miery zaťažiť váš systém, čo môže následne spôsobiť spomalenie ostatných procesov alebo dokonca celého systému. Môže sa zobraziť chybové hlásenie „*Too many concurrent connections opened*“.

Účet Office 365

Táto možnosť je dostupná len v prípade, že používate hybridné prostredie Office 365.

Prihlasovacie meno

Zadajte prihlasovacie údaje používateľa, ktorý má prístup do EWS (Exchange Web Services).

Prihlasovacie heslo

Kliknite na **Nastaviť** vedľa položky **Prihlasovacie heslo** a zadajte heslo pre daného používateľa.

Priradiť používateľovi rolu ApplicationImpersonation

Ak táto možnosť nie je dostupná, bude potrebné najprv zadať **Prihlasovacie meno**. Pre automatické priradenie roly ApplicationImpersonation k vybranému používateľovi kliknite na **Priradiť**. Rolu ApplicationImpersonation môžete k používateľskému účtu priradiť aj manuálne. Pre používateľský účet bude vytvorená nová neobmedzená EWS Throttling politika. Viac informácií nájdete v kapitole Podrobnosti účtu kontroly databáz.

Kontrola databáz e-mailových schránok

Spustenie úplnej kontroly databáz vo veľkých prostrediach môže spôsobiť nežiaduce zaťaženie systému. Ak sa chcete tomuto problému vyhnúť, kontrolu spustite len na vybraných databázach alebo e-mailových schránkach. Zaťaženie systému servera pri kontrole môžete znížiť aj filtrovaním cieľov kontroly pomocou časovej pečiatky správ.

Chybne definované pravidlá pre Manuálnu kontrolu databáz e-mailových schránok môžu spôsobiť nezvratné zmeny v databázach e-mailových schránok. Pred prvým spustením manuálnej kontroly databáz e-mailových schránok s novonastavenými pravidlami sa preto vždy uistite, že máte vytvorenú aktuálnu zálohu vašich databáz e-mailových schránok. Taktiež vám dôrazne odporúčame overiť si, či pravidlá fungujú podľa očakávaní.
Ak chcete pravidlá otestovať, nastavte pre ne v rámci želanej akcie len možnosť Zapísať do protokolu udalostí, pretože všetky ostatné druhy akcií môžu spôsobiť zmeny v databázach e-mailových schránok. Po overení fungovania nastavených pravidiel môžete pre tieto pravidlá pridať aj iné akcie, napríklad akciu **Odstrániť prílohu**.

Nasledujúce typy položiek sú kontrolované vo **Verejných priečinkoch** a v **E-mailových schránkach**:

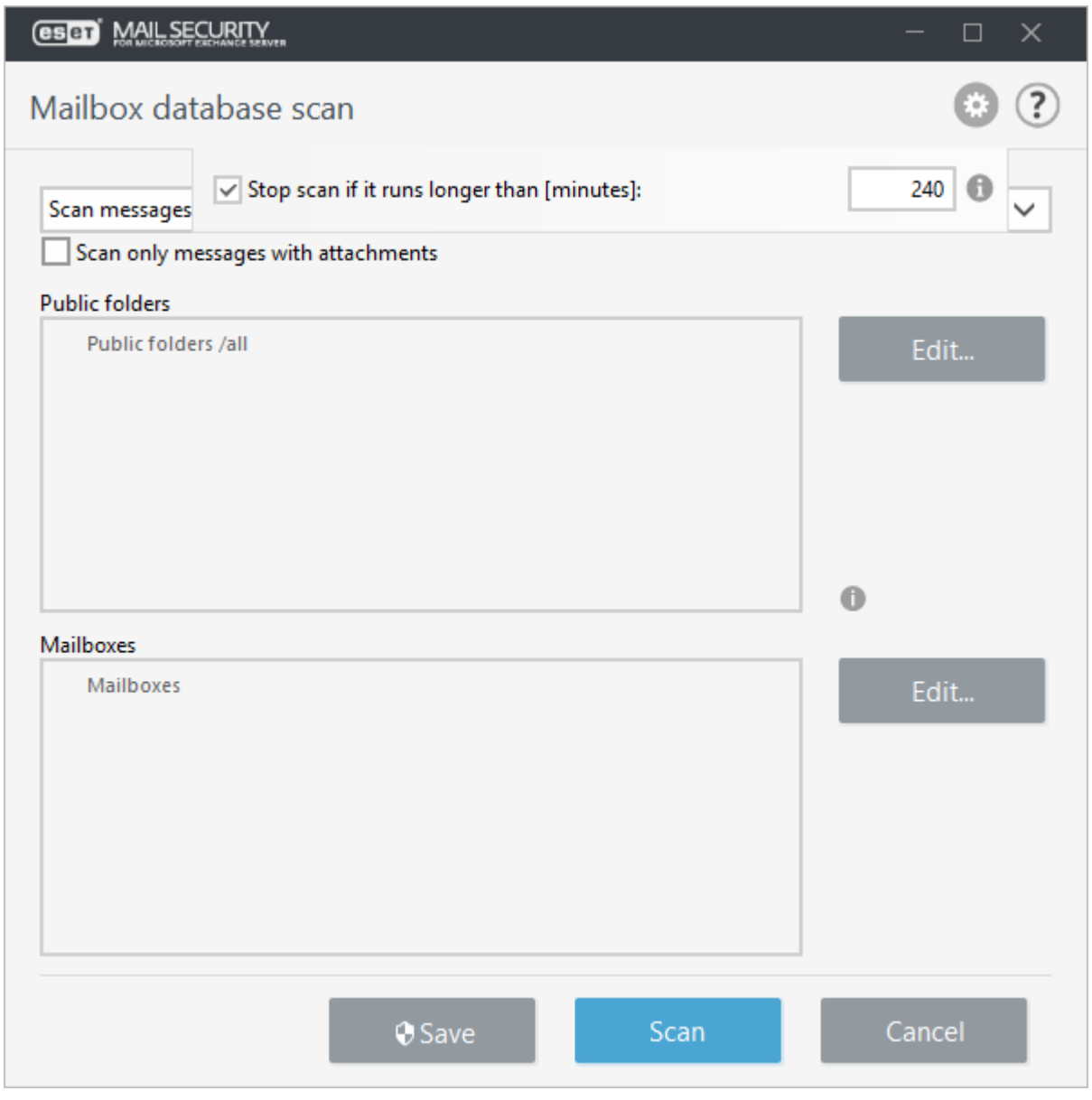
- E-mail

- Príspevky
- Položky v kalendári (schôdze/plánované činnosti)
- Úlohy
- Kontakty
- Denník

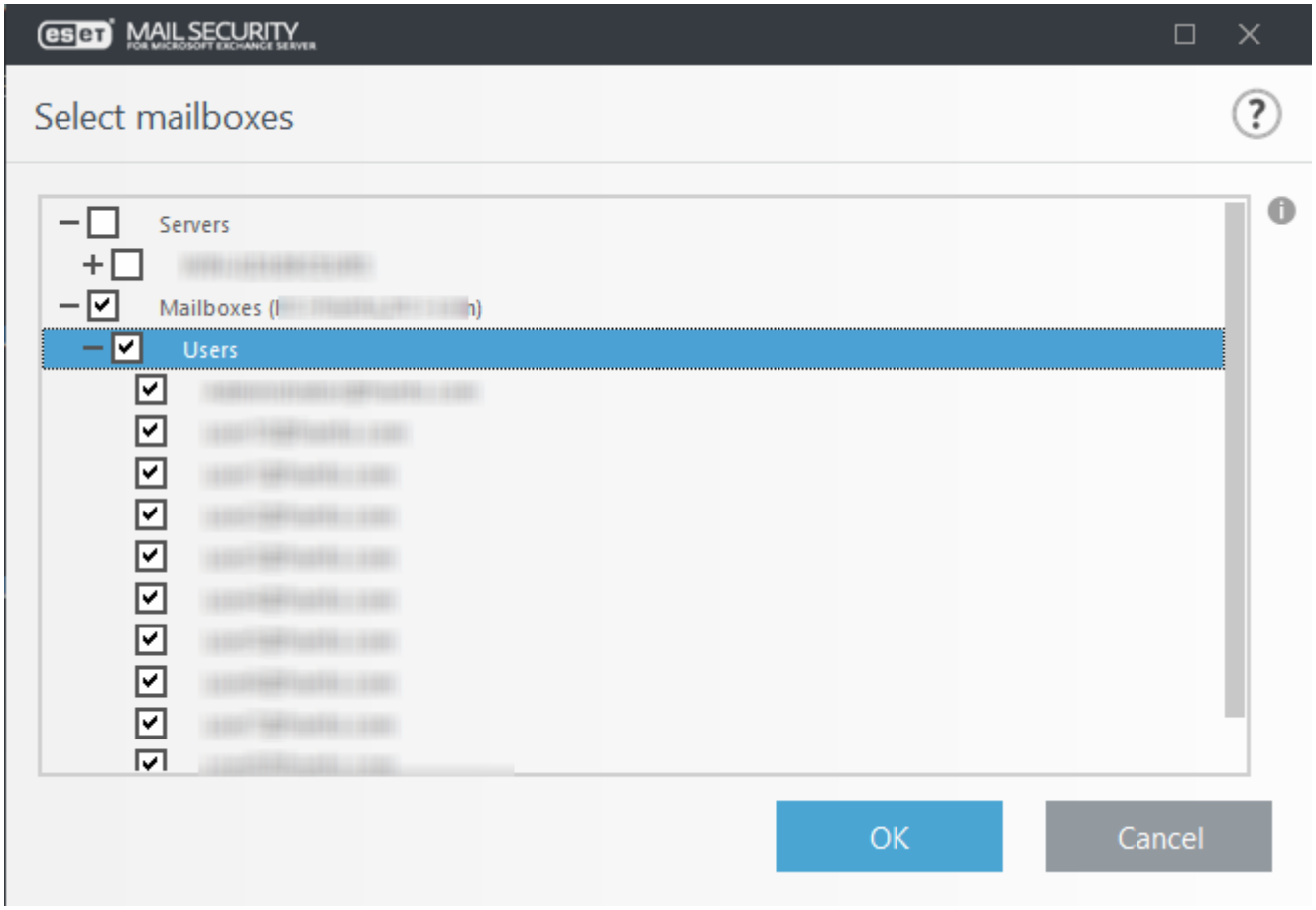
Pomocou roletového menu môžete vybrať, ktoré správy majú byť skontrolované na základe časovej pečiatky. Z roletového menu tak môžete zvoliť napríklad možnosť **Skontrolovať správy pozmenené za posledný týždeň**. V prípade potreby tiež môžete **Skontrolovať všetky správy**.

Možnosť **Kontrolovať iba správy s prílohami** vám umožňuje povoliť alebo zakázať kontrolu príloh správ. Kliknutím na možnosť **Upraviť** môžete vybrať verejné priečinky, ktoré budú kontrolované.

Kliknite na ikonu a upravte interval na možnosť **Zastaviť kontrolu, ak trvá dlhšie ako [minúty]:** a zadajte preferovaný čas (od jednej po 2880 minút).



Označte serverové databázy a e-mailové schránky, ktoré chcete skontrolovať. Filter umožňuje rýchlo vyhľadať databázy a e-mailové schránky, hlavne ak sa vo vašej infraštruktúre Exchange nachádza veľké množstvo e-mailových schránok.



Kliknite na **Uložiť** pre uloženie cieľov kontroly a ich aktuálnych nastavení v profile manuálnej kontroly. Teraz môžete kliknúť na tlačidlo **Kontrolovať**. V prípade, že ste zatiaľ nešpecifikovali podrobnosti účtu kontroly databáz, zobrazí sa dialógové okno s výzvou na zadanie prihlasovacích údajov. V opačnom prípade sa spustí manuálna kontrola databáz e-mailových schránok.

Ak nevidíte e-mailovú schránku vstavaného účtu správcu, overte si, či atribút *UserPrincipalName* nie je prázdny.

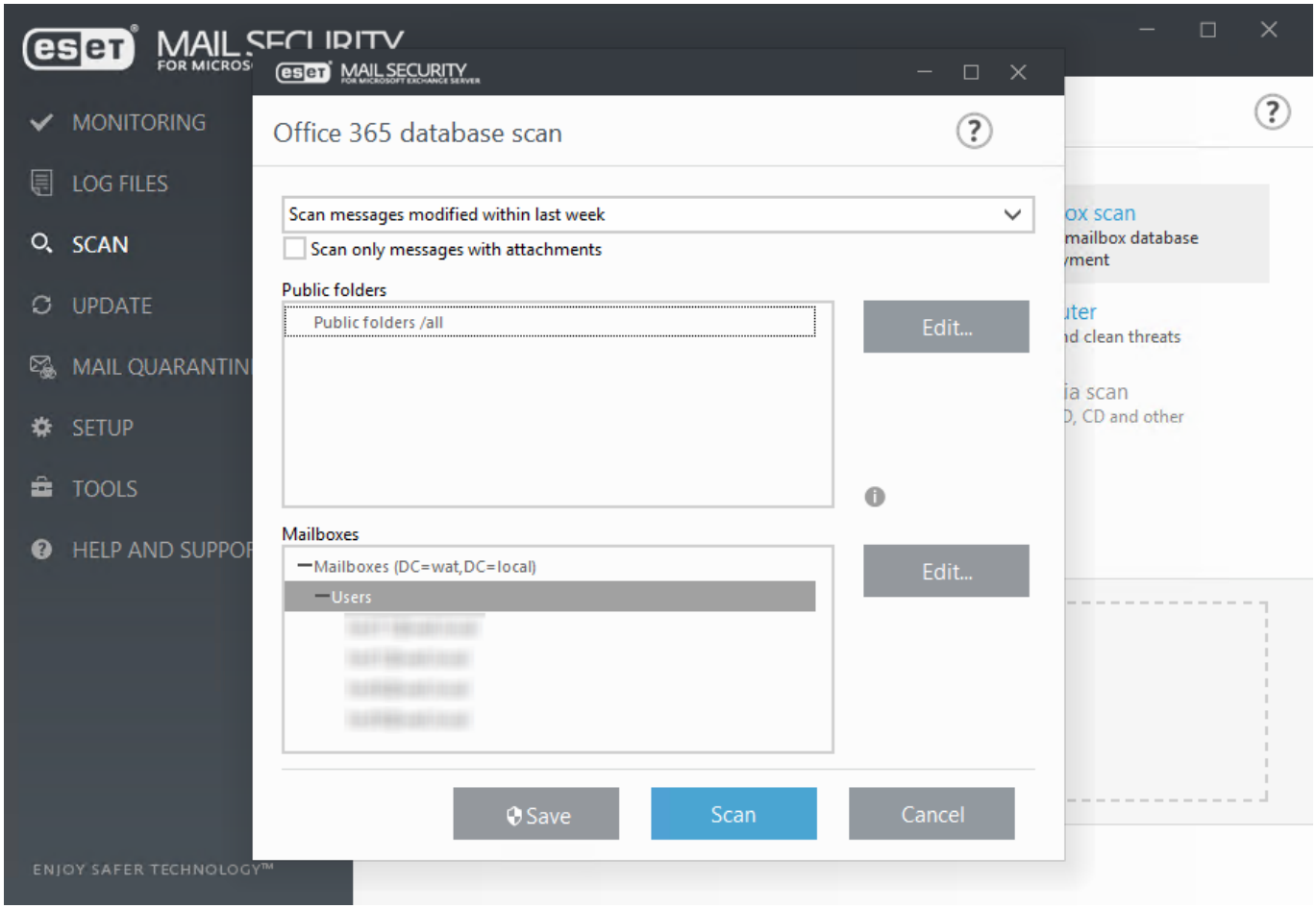
Ak používate Microsoft Exchange Server 2007 alebo 2010, môžete si vybrať medzi Ochranou databáz e-mailových schránok a Manuálnou kontrolou databáz e-mailových schránok, nie je však možné mať aktivované oba tieto typy ochrany súčasne. Ak sa rozhodnete pre **Manuálnu kontrolu databáz e-mailových schránok**, integrácia **Ochrany databáz e-mailových schránok** musí byť vypnutá v **Rozšírených nastaveniach** v časti **Server**. V opačnom prípade nebude Manuálna kontrola databáz e-mailových schránok dostupná.

Kontrola e-mailových schránok Office 365

ESET Mail Security umožňuje vykonávať kontrolu v hybridných prostrediach Office 365. Táto funkcia je dostupná v ESET Mail Security len v prípade, že používate hybridné prostredie Exchange (lokálne alebo v cloude). Podporované sú obidva scenáre smerovania správ – buď prostredníctvom **Exchange Online**, alebo **lokálne** vo vašej organizácii. Podrobnejšie informácie nájdete v tomto článku spoločnosti Microsoft.

Môžete kontrolovať vzdialené e-mailové schránky Office 365 a verejné priečinky rovnako ako pomocou

Manuálnej kontroly databáz e-mailových schránok.



Spustenie úplnej kontroly databáz vo veľkých prostrediach môže spôsobiť nežiaduce zaťaženie systému. Ak sa chcete tomuto problému vyhnúť, kontrolu spustite len na vybraných databázach alebo e-mailových schránkach. Na zníženie systémovej záťaže použite časový filter umiestnený v hornej časti okna. Z roletového menu tak môžete namiesto **Kontrolovať všetky správy** zvoliť napríklad možnosť **Kontrolovať správy zmenené za posledný týždeň**.

Odporúčame, aby ste si nastavili účet Office 365. Stlačte kláves **F5** a prejdite do sekcie **Server** > **Manuálna kontrola databáz e-mailových schránok**. Ďalšie informácie nájdete takisto v kapitole Podrobnosti účtu kontroly databáz.

Ak si chcete pozrieť aktivitu Kontroly e-mailových schránok Office 365, prejdite do časti **Protokoly** > **Kontrola databáz e-mailových schránok**.

Ďalšie položky e-mailovej schránky

Pomocou nastavení Manuálnej kontroly databáz e-mailových schránok môžete povoliť alebo zakázať kontrolu ďalších položiek e-mailovej schránky:

- Kontrolovať kalendár
- Kontrolovať úlohy
- Kontrolovať kontakty

- Kontrolovať denník

Ak sa vyskytnú pri kontrole problémy, môžete tieto položky zakázať. Pri povolení týchto položiek sa kontrola predlžuje.

Proxy server

V prípade, že používate proxy server medzi Exchange serverom s rolou CAS a Exchange serverom, kde je nainštalovaný produkt ESET Mail Security, je potrebné, aby boli v nastaveniach definované parametre proxy servera. Je to potrebné z toho dôvodu, že ESET Mail Security sa pripája na EWS (Exchange Web Services) API cez HTTP/HTTPS. V opačnom prípade karanténna e□mailová schránka ani karanténa MS Exchange nebudú funkčné.

Proxy server

Zadajte IP adresu alebo názov vášho proxy servera.

Port

Zadajte číslo portu proxy servera.

Prihlasovacie meno, heslo

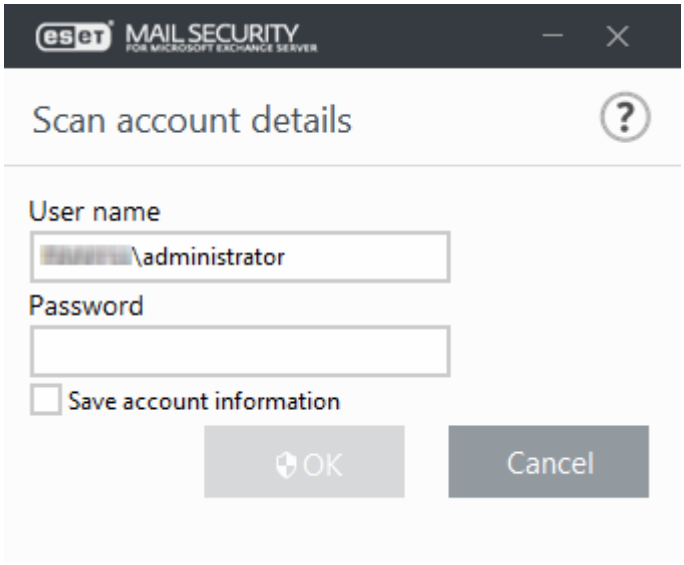
Ak váš proxy server vyžaduje overenie, zadajte príslušné prihlasovacie údaje.

Podrobnosti účtu kontroly databáz

Toto dialógové okno sa zobrazí, ak ste ešte nešpecifikovali prihlasovacie meno a heslo pre Kontrolu databáz. Zadajte prihlasovacie údaje používateľa, ktorý má prístup do EWS (Exchange Web Services), a kliknite na tlačidlo **OK**. Druhou možnosťou je otvoriť **Rozšírené nastavenia** a prejsť do sekcie **Server** > Manuálna kontrola databáz e□mailových schránok.

1. Zadajte **Prihlasovacie meno**, kliknite na **Nastaviť**, potom zadajte heslo pre daný používateľský účet a kliknite na **OK**.

2. Môžete tiež označiť možnosť **Uložiť informácie o účte** pre uloženie prístupových údajov k účtu. V opačnom prípade budete vyzvaný zadávať prístupové údaje k účtu pri každom budúcom spustení Manuálnej kontroly databáz e□mailových schránok.



Ak používateľský účet nemá dostatočné oprávnenia na prístup do EWS, môžete vybrať možnosť **Vytvoriť priradenie roly ApplicationImpersonation** pre priradenie tejto roly k používateľskému účtu. Rolu **ApplicationImpersonation** môžete priradiť aj manuálne.

Aby mohla byť vykonaná kontrola používateľských e-mailových schránok v rámci databáz e-mailových schránok Exchange, účet kontroly musí mať priradenú rolu **ApplicationImpersonation**. Ak používate Exchange Server 2010 alebo novšiu verziu, je možné nakonfigurovať EWS Throttling politiku pre každý používateľský účet.
Uistite sa, že účet kontroly má nakonfigurovanú EWS Throttling politiku, aby sa zamedzilo nadmernému množstvu požiadaviek zo strany ESET Mail Security. Ak sa chcete dozvedieť o Throttling politikách viac, prečítajte si článok EWS Best Practices a Understanding Client Throttling Policies. Ďalšie podrobnosti a príklady ďalej nájdete v článku Change user throttling settings for specific users.

Ak chcete priradiť rolu **ApplicationImpersonation** k používateľskému účtu manuálne a vytvoriť novú EWS Throttling politiku pre tento účet, môžete použiť nasledujúce príkazy (nahraďte `ESET-user` skutočným názvom účtu vo vašom systéme; môžete tiež nastaviť obmedzenia pre EWS Throttling politiku nahradením reťazca `$null` číslami):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation
Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation -User ESET-user
```

Aplikovanie môže chvíľu trvať.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -EWSFastSearchTimeoutInSeconds $null -EWSMaxConcurrency $null -EWSPercentTimeInAD $null -EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null
Set-ThrottlingPolicyAssociation -Identity user-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-Impersonation
Get-MailboxDatabase | Add-AdPermission -User ESET-user -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2013, 2016 a 2019

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation -User ESET-user
```

Aplikovanie môže chvíľu trvať.

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -EwsRechargeRate Unlimited
Set-ThrottlingPolicyAssociation -Identity ESET-user -ThrottlingPolicy ESET-ThrottlingPolicy
```

Typy e-mailovej karantény

Správca e-mailovej karantény je dostupný pre všetky tri typy karantény:

- Lokálna karanténa
- Karanténna e-mailová schránka
- Karanténa MS Exchange

Obsah e-mailovej karantény nájdete v Správcovi e-mailovej karantény pre všetky typy karantény. Lokálnu karanténu je možné zobraziť aj pomocou webového rozhrania e-mailovej karantény.

Ukladať správy pre neexistujúcich príjemcov

Toto nastavenie sa uplatňuje na správy, ktoré sú označené na presun do karantény Antivírusovou ochranou, Antispamovou ochranou alebo na základe pravidiel. Keď je táto funkcia povolená, správy, ktoré boli odoslané príjemcom, ktorí sa nenachádzajú vo vašom Active Directory, budú uchovávané v e-mailovej karanténe. Ak nechcete, aby boli takéto správy uchovávané vo vašej e-mailovej karanténe, túto funkciu vypnite. Ak je vypnutá, správy, ktoré majú neznámeho príjemcu, budú potichu zahodené.

Ak chcete do karantény presúvať všetky e-mailové správy pre neexistujúcich príjemcov, pozrite si príslušný príklad.

Vynechať vyhodnotenie pravidiel pri uvoľňovaní e-mailov

Ak chcete uvoľniť, teda doručiť správu umiestnenú v karanténe, táto správa nebude vyhodnocovaná pravidlami. Je to z dôvodu, aby sa predišlo opätovnému umiestneniu správy späť do karantény. Uvoľnená správa bude úspešne doručená príjemcovi. Táto funkcia je použitá len v prípade, že správu uvoľní správca (Administrator). Ak túto funkciu vypnete alebo ak správu uvoľňuje iný používateľ ako správca, daná správa bude vyhodnocovaná pravidlami.

> Ak používate klastrové prostredie a uvoľníte konkrétnu správu z karantény, na ďalších uzloch ESET Mail Security sa už rovnaká správa opätovne nedostane do karantény. Zabezpečuje to synchronizácia pravidiel medzi uzlami klastra.

Základný podpis správ pre prostredie s viacerými servermi

Umožňuje vám v prostredí s viacerými servermi vynechať vyhodnocovanie pravidiel pri uvoľňovaní e-mailov

z karantény. Zadajte rovnakú počiatočnú hodnotu (reťazec znakov/prístupovú frázu) na všetkých serveroch, medzi ktorými chcete vytvoriť dôveru.

Formát obálky prílohy

Pri uvoľňovaní z karantény je e-mailová správa vložená ako príloha do novej správy (obálka prílohy), ktorá je následne doručená príjemcovi. Príjemca dostane pôvodnú uvoľnenú správu v podobe prílohy. Môžete použiť predvolený formát obálky alebo ho upraviť podľa potrieb použitím dostupných premenných.

Použiť klaster ESET pre uloženie všetkých správ v karanténe na jednom uzle

Táto možnosť bude dostupná v prípade, ak používate klaster ESET. Odporúčame vám používať túto funkciu, pretože vám umožňuje uchovávať položky lokálnej karantény na jednom mieste – hlavnom uzle.

Hlavný uzol

Určite, ktorý server je hlavným uzlom vášho Klastra ESET. K lokálnej karanténe budete následne pristupovať a spravovať ju na hlavnom uzle (môžete použiť Správcu e-mailovej karantény v hlavnom okne programu alebo Webové rozhranie e-mailovej karantény).

Lokálna karanténa

Lokálna karanténa využíva na ukladanie e-mailových správ do karantény váš lokálny súborový systém a SQLite databázu na vytvorenie indexu. Súbory e-mailových správ v karanténe, ako aj súbory databázy sú z bezpečnostných dôvodov šifrované. Tieto súbory sa nachádzajú v adresári C:\ProgramData\ESET\ESET Mail Security\MailQuarantine (na systéme Windows Server 2012).

> Ak chcete mať súbory umiestnené v karanténe uložené na inom ako predvolenom disku C:, zmeňte cestu Priečinku s dátami na vašu preferovanú lokalitu počas inštalácie produktu ESET Mail Security.

Funkcie lokálnej karantény:

- Spam a e-mailové správy umiestnené v karanténe budú uložené v lokálnom súborovom systéme, nie v databáze e-mailovej schránky Exchange.
- Šifrovanie a kompresia e-mailových súborov umiestnených v lokálnej karanténe.
- Webové rozhranie e-mailovej karantény ako alternatíva k Správcovi e-mailovej karantény.
- Reporty o karanténe môžu byť odosielané na zadanú e-mailovú adresu pomocou naplánovanej úlohy.
- E-mailové súbory umiestnené v karanténe, ktoré sú odstránené z okna karantény (predvolene po 21 dňoch), sú naďalej uložené v súborovom systéme (až do automatického vymazania po nastavenom počte dní).
- Staré e-mailové súbory sú automaticky vymazávané (predvolene po 3 dňoch). Viac informácií nájdete v kapitole Súborové úložisko.
- E-mailové súbory umiestnené v karanténe, ktoré boli odstránené, môžete obnoviť pomocou nástroja eShell (v prípade, že ešte neboli odstránené zo súborového systému).
- Môžete si prezrieť e-mailové správy umiestnené v karanténe a rozhodnúť sa, či chcete odstrániť alebo

uvoľniť ktorúkoľvek z nich. Na zobrazenie a správu e-mailových správ umiestnených v lokálnej karanténe môžete použiť Správcu e-mailovej karantény v hlavnom okne programu alebo Webové rozhranie e-mailovej karantény.

> Nevýhodou používania lokálnej karantény je, že ak spustíte ESET Mail Security na viacerých serveroch so serverovou rolou Hub Transport, musíte spravovať lokálnu karanténu každého servera osobitne. Čím viac e-mailových serverov máte, tým viac karantén budete musieť spravovať.

Súborové úložisko

V tejto sekcii môžete zmeniť nastavenia pre súborové úložisko použité pre lokálnu karanténu.

Skomprimovať súbory uložené do karantény

Súbory uložené v karanténe budú po skomprimovaní zaberať menej miesta na disku. Ak si kompresiu súborov neželáte, môžete ju prostredníctvom prepínača vypnúť.

Zmazať staré súbory po (dňoch)

Správy budú odstránené z okna karantény po nastavenom počte dní. Tieto súbory však budú z disku vymazané až po uplynutí počtu dní nastavenom v časti **Zmazať odstránené súbory po (dňoch)**. Keďže súbory nie sú vymazané zo súborového systému, je možné ich obnoviť pomocou nástroja eShell.

Zmazať odstránené súbory po (dňoch)

Súbory budú vymazané z disku po nastavenom počte dní. Po vyčistení odstránených súborov už nie je možné súbory obnoviť (len v prípade zálohovania disku).

Webové rozhranie

Webové rozhranie e-mailovej karantény je alternatívou k oknu Správca e-mailovej karantény, dá sa však použiť len pre Lokálnu karanténu.

> Webové rozhranie e-mailovej karantény nie je dostupné na serveri s rolou Edge Transport. Je to zapríčinené tým, že Active Directory nie je prístupný z hľadiska autentifikácie.

Webové rozhranie e□mailovej karantény umožňuje zobraziť aktuálny stav e□mailovej karantény. Umožňuje tiež spravovať objekty v karanténe. Webové rozhranie e□mailovej karantény je prístupné buď priamo prostredníctvom odkazov v reportoch o karanténe, alebo zadaním odkazu do webového prehliadača.

Pre prístup k webovému rozhraniu je nutné zadať doménové prihlasovacie údaje. Microsoft Internet Explorer automaticky overí doménového používateľa. Musí však byť platný certifikát webovej stránky, povolená možnosť Automatické prihlásenie v prehliadači Internet Explorer a webová stránka e□mailovej karantény musí byť pridaná do zoznamu intranetových lokalít.

Akýkoľvek používateľ, ktorý existuje v Active Directory, má prístup do webového rozhrania e-mailovej karantény, avšak uvidí len tie položky uložené v karanténe, ktoré boli odoslané na jeho e-mailovú adresu (vrátane aliasov používateľa). Správca vidí všetky položky umiestnené v karanténe.

ESET Mail Security nepoužíva IIS na spúšťanie webového rozhrania e-mailovej karantény. Miesto toho využíva HTTP server API s podporou SSL pre výmenu dát prostredníctvom zabezpečených HTTP spojení.

URL webu

URL adresa, na ktorej bude dostupné webové rozhranie e-mailovej karantény. Štandardne je to FQDN servera s `/quarantine` (napr. `mailserver.company.com/quarantine`). Môžete zadať aj svoj vlastný virtuálny adresár miesto pôvodného `/quarantine`. URL webu môžete zmeniť kedykoľvek.

Hodnota URL webu musí byť zadaná bez schémy (HTTP, HTTPS) a čísla portu, použite len tvar fqdn/virtualdirectory. Miesto FQDN môžete tiež použiť zástupné symboly.

Po úprave URL webu nie je možné zmeny vrátiť späť na pôvodné nastavenia kliknutím na ikonu Vrátiť. Odstráňte položku a ponechajte textové pole prázdne. Reštartujte server. Keď sa ESET Mail Security spustí a pole URL webu je prázdne, bude automaticky vyplnené predvolenou hodnotou `fqdn/quarantine`.

ESET Mail Security podporuje url webu v štyroch rôznych formátoch:
Silný zástupný symbol (+/quarantine)
Explicitný (mydomain.com/quarantine)
Slabý zástupný symbol viažuci sa na IP adresu (192.168.0.0/quarantine)
Slabý zástupný symbol (*/quarantine)
Viac informácií nájdete v sekcii **Host-Specifier Categories** v článku UrlPrefix Strings.

Jazyk rozhrania a reportov

Môžete nastaviť jazyk webového rozhrania karantény a jazyk reportov o karanténe.

HTTPS port

HTTPS port sa používa pre webové rozhranie. Štandardný port je 443.

HTTP port

Používa sa na uvoľňovanie e-mailov z karantény prostredníctvom e-mailových reportov.

Ak nemáte v IIS nainštalovaný SSL certifikát, nakonfigurujte si HTTPS port binding. Ak zmeníte číslo portu pre HTTP alebo HTTPS, nezabudnite vytvoriť potrebnú väzbu na port v IIS.

Zaznamenávať akcie uvoľnenia do protokolu udalostí

Pri uvoľňovaní položiek z e□mailovej karantény je daná akcia zapisovaná do protokolov.

Povoliť predvolených správcov

Členovia skupiny správcov majú predvolene pridelený správcovský prístup do webového rozhrania e-mailovej karantény. Správcovský prístup nemá žiadne obmedzenia a umožňuje správcovi vidieť všetky položky (pre všetkých príjemcov) umiestnené v karanténe. Ak túto možnosť zakážete, správcovský prístup do webového rozhrania e-mailovej karantény bude možný len prostredníctvom účtu správcu (Administrator).

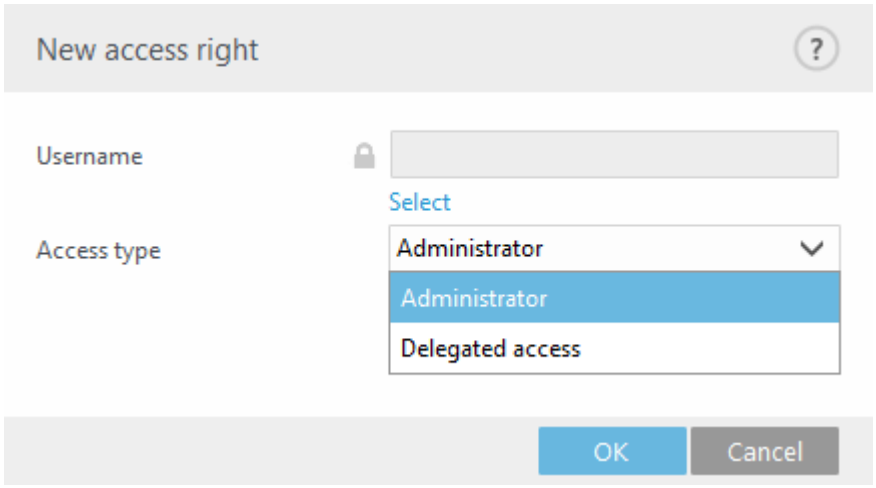
Dodatočné prístupové práva

Používateľom môžete poskytnúť dodatočné prístupové práva do webového rozhrania e□mailovej karantény a zároveň zvoliť **typ prístupu**. Kliknite na **Upraviť** pre otvorenie okna s dodatočnými prístupovými právami a

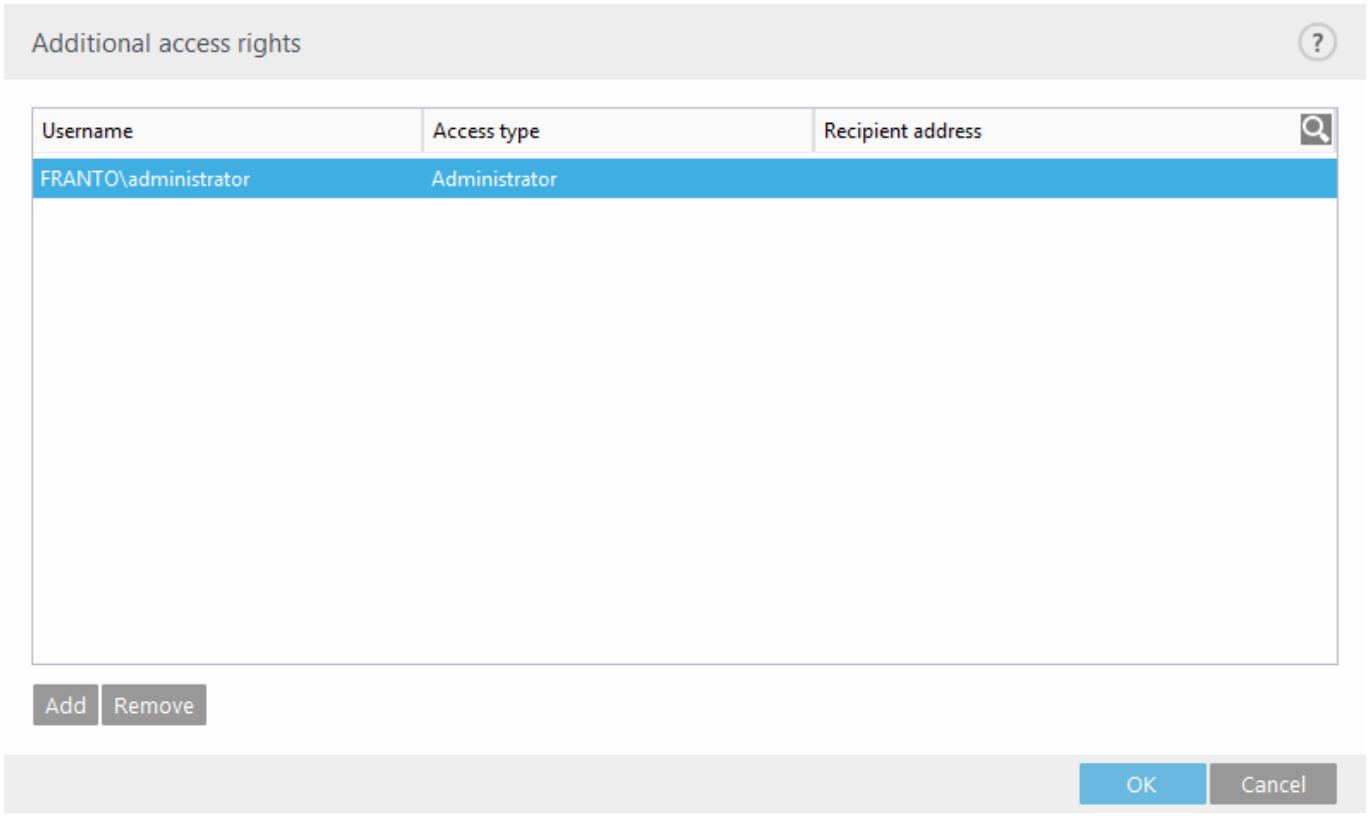
kliknite na tlačidlo Pridať pre poskytnutie prístupu používateľovi. V okne Nové prístupové práva kliknite na možnosť Vybrať, vyberte používateľa z Active Directory (môžete vybrať len jedného) a z roletového menu vyberte **Typ prístupu**:

- **Správca** – používateľ bude mať správcovský prístup do webového rozhrania e-mailovej karantény.

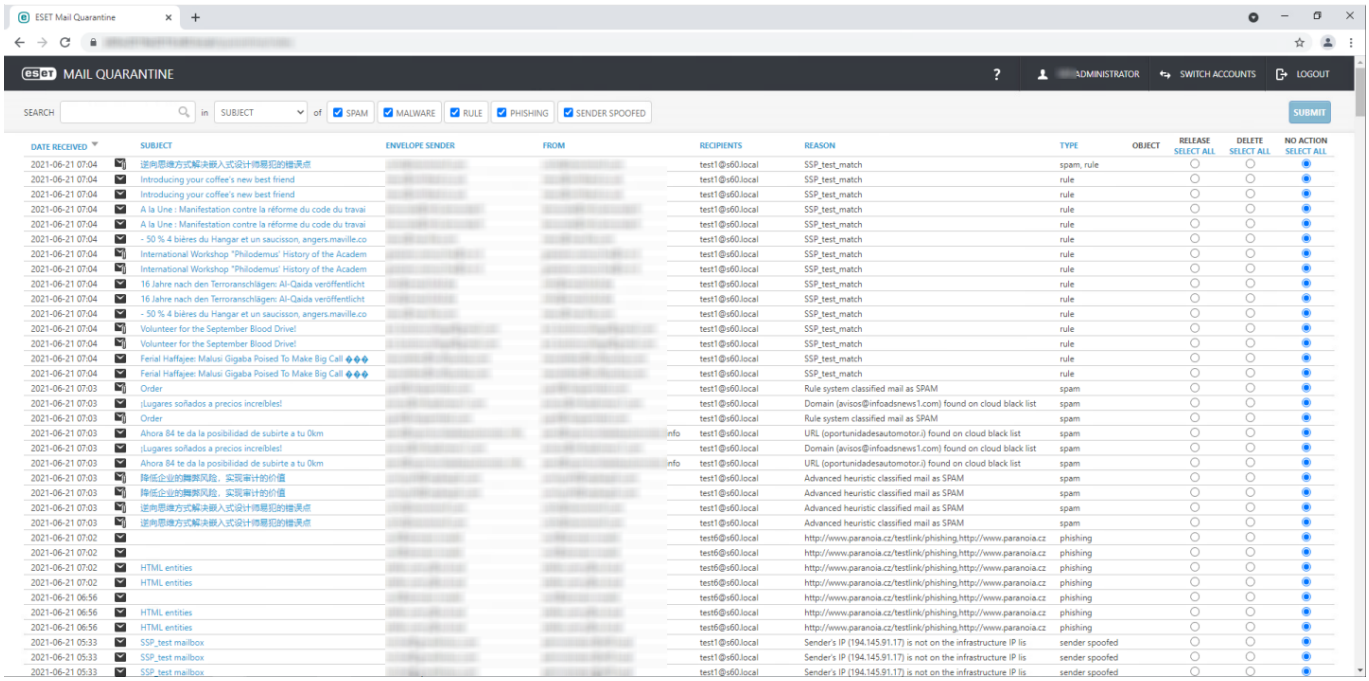
- **Delegovaný prístup** – tento typ prístupu použite vtedy, ak chcete umožniť používateľovi (delegátovi) vidieť a spravovať správy iného príjemcu uložené v karanténe. Zadajte **E-mailovú adresu príjemcu** pre používateľa, ktorého správy umiestnené v karanténe bude spravovať delegát. Ak má používateľ aliasy v Active Directory, môžete v prípade potreby pridať dodatočné prístupové práva aj pre každý alias.



Príklad používateľov, ktorým boli pridelené dodatočné prístupové práva do webového rozhrania e-mailovej karantény:



Pre prístup do webového rozhrania e-mailovej karantény otvorte svoj webový prehliadač a použite URL adresu uvedenú v časti **Rozšírené nastavenia** (**F5**) > **Server** > **E-mailová karanténa** > **Webové rozhranie** > **URL webu**.



Uvoľniť

Uvoľníte e-mail jeho pôvodnému príjemcovi prostredníctvom Replay directory a odstránite ho z karantény. Kliknutím na **Potvrdiť** potvrdíte vykonanie akcie.

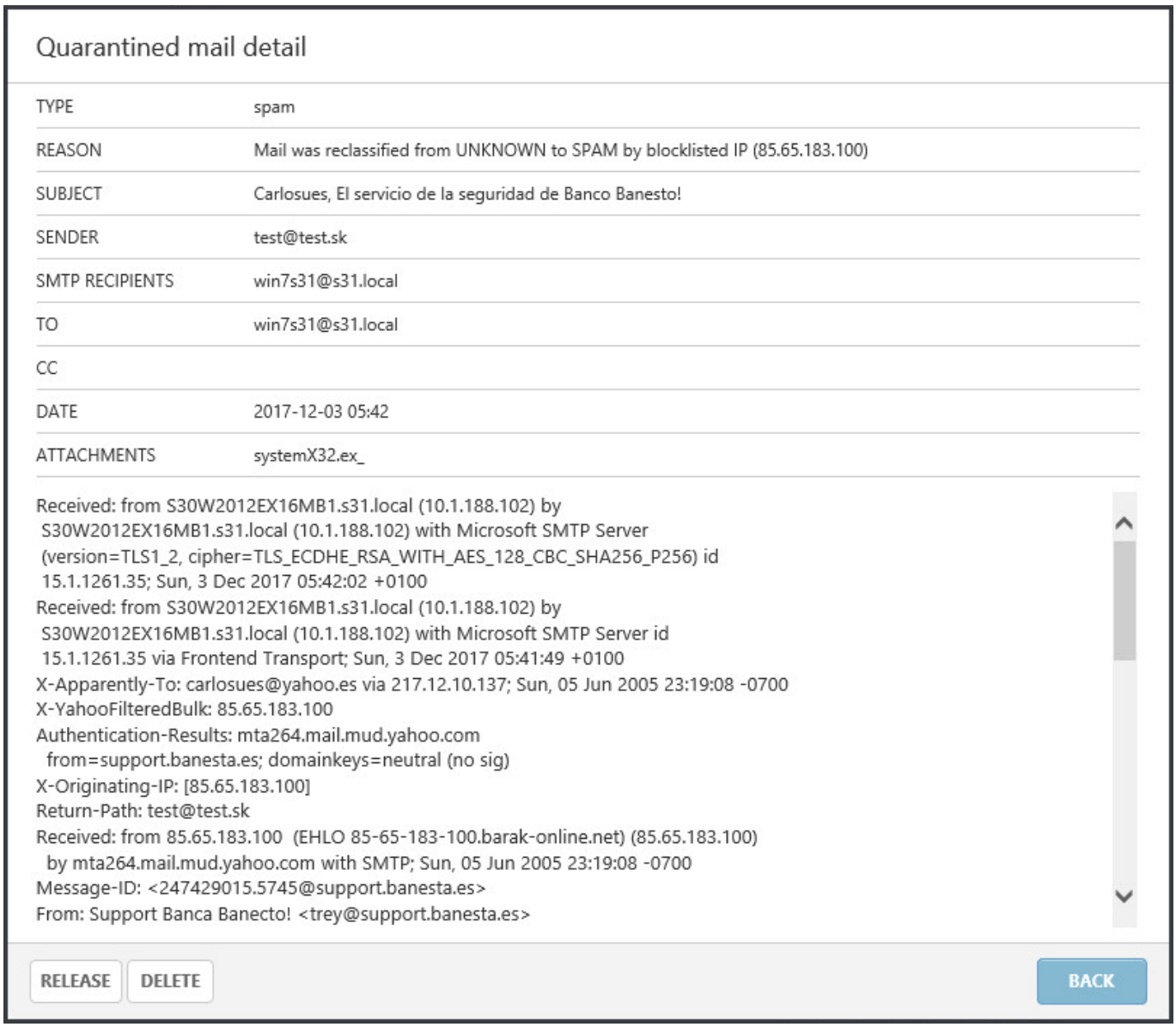
> Pri uvoľňovaní e-mailu z karantény ESET Mail Security ignoruje MIME hlavičku To: z dôvodu, že môže byť ľahko sfalšovaná. Namiesto toho sú použité informácie o pôvodnom príjemcovi z príkazu `RCPT TO:`, získané počas SMTP spojenia. Vďaka tomu sa zabezpečí, že e-mail, ktorý je uvoľnený z karantény, bude doručený správnemu príjemcovi.

Odstrániť

Odstránite položku z karantény. Kliknutím na **Potvrdiť** potvrdíte vykonanie akcie.

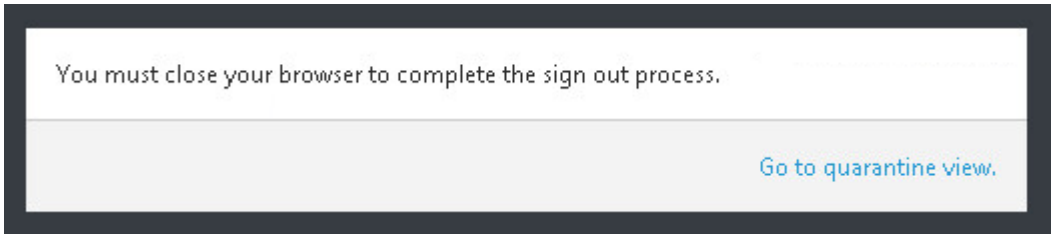
Po kliknutí na **Predmet** sa zobrazí dialógové okno s podrobnosťami o danom e-maile, ako napr. Typ, Dôvod, Odosielateľ, Dátum, Prílohy atď.

Ak kliknete na možnosť **Zobraziť hlavičky**, budú zobrazované hlavičky e-mailov v zozname.



Kliknutím na **Uvoľniť** alebo **Odstrániť** uvoľníte alebo vymažete vybrané e-mailové správy v karanténe.

Na skutočné odhlásenie z webového rozhrania e-mailovej karantény je nutné zatvoriť okno prehliadača. Prípadne kliknite na možnosť **Prejsť na zobrazenie karantény** pre návrat na predchádzajúcu obrazovku.

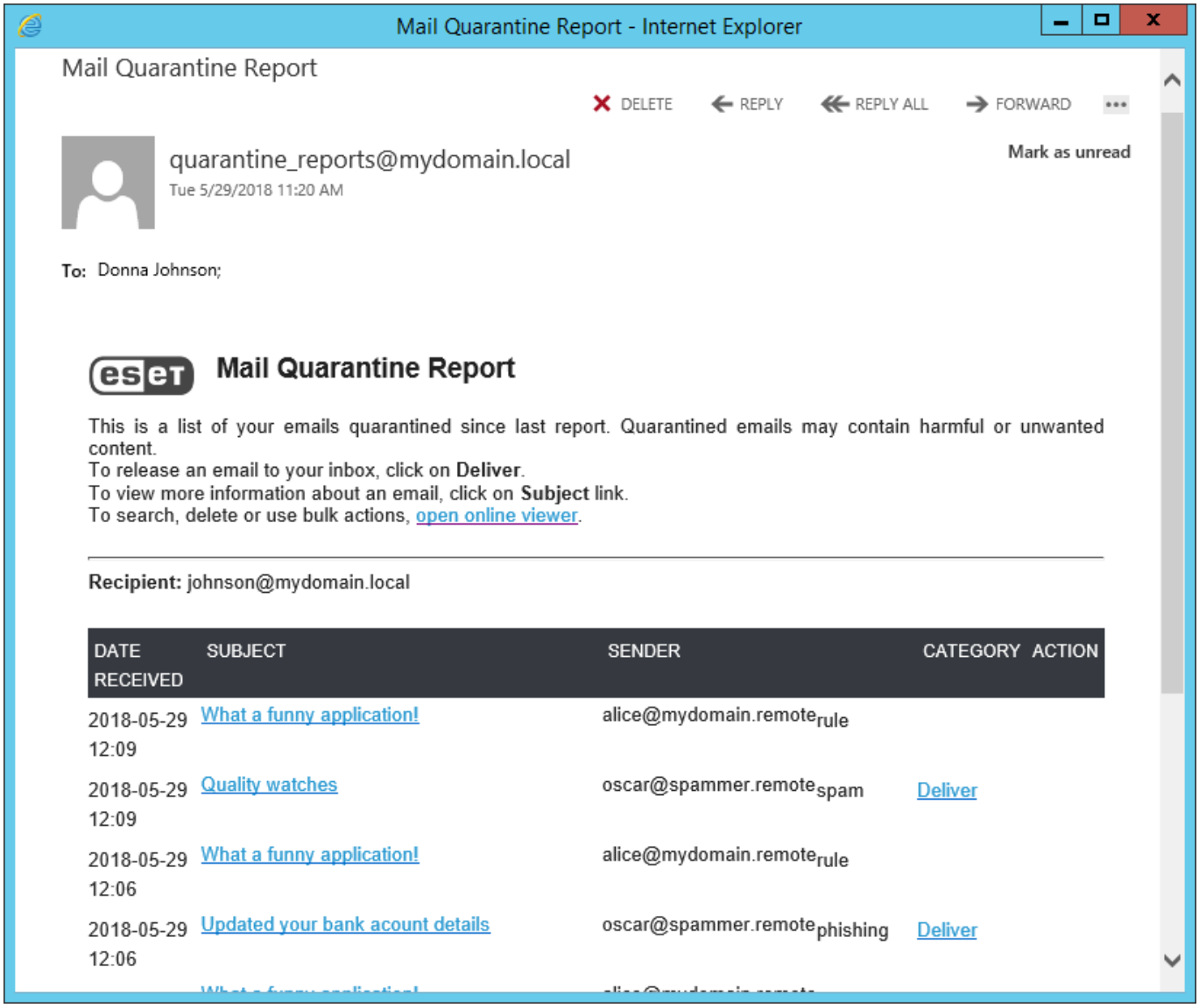


Ak máte problémy s prístupom do webového rozhrania e-mailovej karantény z vášho webového prehliadača, prípadne sa zobrazuje chybové hlásenie HTTP Error 403.4 - Forbidden alebo podobné hlásenie, skontrolujte, ktorý typ karantény je zvolený. Uistite sa, že je zvolená **Lokálna karanténa** a že je povolená možnosť **Zapnúť webové rozhranie**.

Odosielať reporty o e-mailovej karanténe – naplánovaná úloha

Reporty o e-mailovej karanténe sú notifikačné e-maily odosielané vybraným používateľom a správcom, ktoré ich informujú o e-mailoch presunutých do karantény programom ESET Mail Security. Tieto reporty obsahujú odkazy, ktoré vám a používateľom, ktorí dostávajú reporty o e-mailovej karanténe, umožňujú priamo vymazať alebo uvoľniť (doručiť) nesprávne detegovanú e-mailovú správu (false positive). Bežní používatelia nemajú povolené doručovať niektoré správy, ktoré boli odfiltrované pomocou pravidiel alebo presunuté do e-mailovej karantény antivírusovou ochranu.

Úloha Odosielať reporty o e-mailovej karanténe/Odosielať správcovské reporty o e-mailovej karanténe odosiela report o e-mailovej karanténe pomocou e-mailu podľa naplánovanej úlohy. Nižšie nájdete príklad reportu o e-mailovej karanténe určeného pre používateľa:



Report o e-mailovej karanténe tiež obsahuje odkaz na Webové rozhranie e-mailovej karantény (otvoriť online zobrazovač).

Úloha Odosielať reporty o e-mailovej karanténe je dostupná len v prípade, že používate **Lokálnu karanténu**. Túto úlohu nebudete môcť použiť s Karanténnou e-mailovou schránkou a karanténou MS Exchange.

E-mailová adresa odosielateľa

Zadajte e-mailovú adresu, ktorá bude zobrazená ako adresa odosielateľa reportu o e-mailovej karanténe.

Maximálny počet záznamov v reporte

Môžete stanoviť limit pre počet položiek v reporte. Predvolený počet je nastavený na 50.

URL webu

Táto URL adresa bude zahrnutá v reporte o e-mailovej karanténe, a tak bude môcť príjemca jednoducho kliknúť na odkaz pre prístup do webového rozhrania e-mailovej karantény.

Príjemcovia

Vyberte používateľov, ktorí budú dostávať reporty o e-mailovej karanténe. Kliknite na **Upraviť** pre výber e-

mailových schránok pre konkrétnych príjemcov.

> Prehľadný report o e-mailovej karanténe sa odošle len v prípade, že karanténa obsahuje nejaké e-mailové správy. Ak je karanténa prázdna, report sa neodošle.

Cieľ: Vytvoriť naplánovanú úlohu, ktorá bude pravidelne odosielať reporty o e-mailovej karanténe vám ako správcovi, prípadne informovať používateľov o ich spamových správach uložených v e-mailovej karanténe.
Prejdite do časti **Nástroje** > **Plánovač** > **Pridať plánovanú úlohu** a spustite sprievodcu.
Zadajte **Názov úlohy** a z roletového menu vyberte **Typ úlohy**.
Odosielať reporty o e-mailovej karanténe (report bude obsahovať len spamové správy konkrétneho používateľa) alebo **Odosielať správcovské reporty o e-mailovej karanténe** (report bude obsahovať všetky správy, čiže obsah celej karantény). Následne kliknite na **Ďalej**.
Vyberte jednu z možností načasovania podľa toho, kedy chcete úlohu spustiť. Napríklad, **Týždenne** o **10.00** v **Piatok**.
Zadajte **E-mailovú adresu odosielateľa** (administrator@mojadomena.sk).
Kliknite na **Upraviť** pre pridanie **Príjemcov** zo zoznamu. Vyberte e-mailové schránky používateľov, ktorí budú dostávať reporty o e-mailovej karanténe.

Webové rozhranie e-mailovej karantény

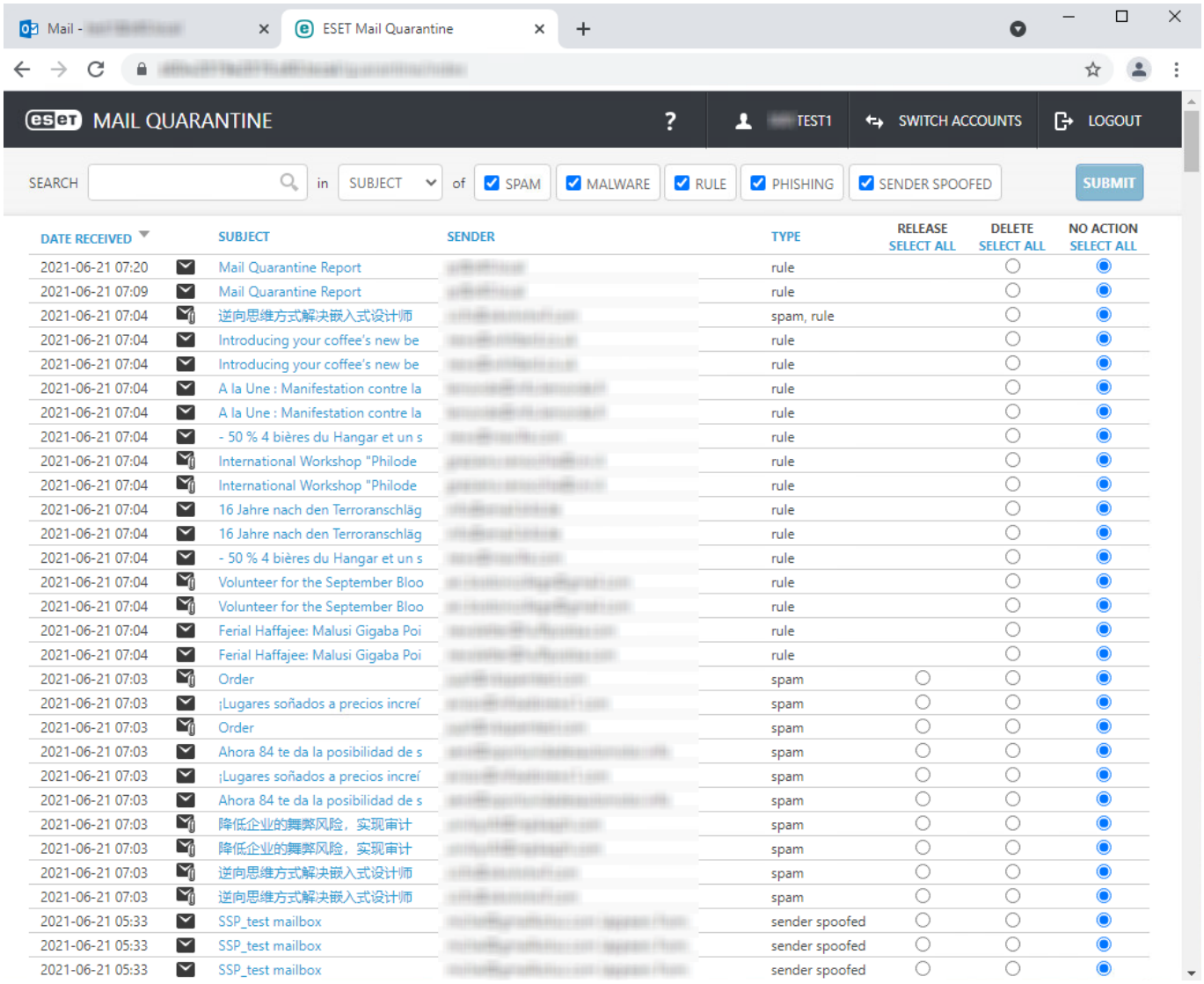
Dostali ste prístup do webového rozhrania, kde môžete spravovať správy, ktoré boli presunuté do karantény napríklad z dôvodu spamu, sfalšovaného odosielateľa alebo phishingu, ako aj správy, ktoré boli odfiltrované podľa pravidiel nastavených správcom. Štandardne môžete vidieť len tie správy, ktoré boli odoslané na vašu e-mailovú adresu a následne boli presunuté do karantény. Ak vám však bol pridelený prístup, ktorý vám umožňuje spravovať správy umiestnené v karanténe aj pre iných používateľov, uvidíte aj správy týchto používateľov. Správy môžete odlíšiť podľa príjemcov. Môžete napríklad použiť funkciu vyhľadávania a filtrovať správy podľa príjemcu.

Môžete si vybrať akciu, ktorá bude vykonaná pre správu alebo viaceré správy, ako napr. **uvoľniť**, **odstrániť** alebo **žiadna akcia**. Dostupnosť akcií závisí od úrovne prístupu a nastavení pravidiel, čiže sa napríklad môže stať, že nebudete môcť uvoľniť alebo vymazať určité typy správ.

Ak vám bol pridelený prístup správcu, uvidíte všetky správy umiestnené v karanténe pre všetkých používateľov a budete môcť vykonať akúkoľvek akciu.

Spravovanie vašich správ umiestnených v karanténe:

Pomocou webového rozhrania e-mailovej karantény si môžete prezerať položky umiestnené v karanténe. Ak máte delegovaný prístup alebo prístup správcu, uvidíte aj ostatné správy umiestnené v karanténe.



V ľavom dolnom rohu okna môžete zmeniť počet položiek zobrazovaných na jednej strane (veľkosť strany).

Ak sa zobrazuje príliš veľa správ, použite funkciu Vyhľadať nachádzajúcu sa hornom paneli na vyhľadanie konkrétnej správy alebo na filtrovanie obsahu podľa Predmetu, Odosielateľa alebo Príjemcu (príjemca je dostupný len pre používateľov, ktorí majú delegovaný prístup alebo prístup správcu). Môžete navyše použiť začiarkavacie políčka a zobraziť tak len správy určitého typu (**spam**, **malvér**, **pravidlo**, **phishing** a **sfalšovaný odosielateľ**).

Ak chcete uvoľniť (doručiť) správu, ktorá bola presunutá do karantény v dôsledku toho, že bola nesprávne detegovaná, použite prepínacie tlačidlá napravo a vyberte možnosť **Uvoľniť**. Ak chcete odstrániť správu, použite akciu **Odstrániť**.

Môžete označiť aj viacero správ naraz s príslušnou akciou. Po označení správ kliknite na **Odoslať**.

Správy, ktoré sú označené na uvoľnenie, budú doručené do vašej e-mailovej schránky alebo do schránky pôvodného adresáta v prípade, že máte delegovaný prístup a chcete uvoľniť správy iných používateľov. Správy, ktoré sú označené na vymazanie, budú natrvalo odstránené z karantény.

Akcie **Uvoľniť** a **Odstrániť** sú trvalé a po kliknutí na **Odoslať** ich nie je možné vrátiť späť.

Zobrazenie sa automaticky obnoví, keď kliknete na Odoslať, ale môžete ho obnoviť aj manuálne pomocou tlačidla obnovenia vo svojom webovom prehliadači alebo stlačením klávesu **F5**.

Uvoľnené môžu byť iba spamové správy a správy so sfalšovaným odosielateľom. Nie je možné z karantény uvoľniť správy, ktoré obsahujú malvér, phishingové správy ani správy, ktoré boli do karantény presunuté na základe pravidla. Ak potrebujete uvoľniť takéto typy správ, požiadajte o pomoc svojho správcu.

Nie je potrebné pravidelne vymazávať správy umiestnené v karanténe, sú vymazávané automaticky po uplynutí času stanoveného správcom.

Na skutočné odhlásenie z webového rozhrania e□mailovej karantény je nutné zatvoriť okno webového prehliadača. Prípadne kliknite na možnosť Prejsť na zobrazenie karantény pre návrat na predchádzajúcu obrazovku.

Karanténna e□mailová schránka a karanténa MS Exchange

Ak sa rozhodnete nepoužiť Lokálnu karanténu, máte na výber dve možnosti, a to použiť buď Karanténnu e□mailovú schránku, alebo karanténu MS Exchange. Nech si už vyberiete ktorúkoľvek možnosť, bude potrebné vytvoriť vyhradený používateľský účet s e□mailovou schránkou (napr. karantena@firma.sk), ktorá bude slúžiť na ukladanie správ v karanténe. Tento používateľský účet a e□mailovú schránku bude používať taktiež aj Správca e□mailovej karantény na zobrazenie a spravovanie objektov v karanténe. Podrobnosti o tomto účte bude preto potrebné upresniť v nastaveniach Správcu karantény.

Výhodou karanténnej e□mailovej schránky/karantény MS Exchange v porovnaní s lokálnou karanténou je, že položky e□mailovej karantény sú spravované z jedného miesta bez ohľadu na to, koľko serverov je v role Hub Transport. V prípade karanténnej e□mailovej schránky/karantény MS Exchange sú spam a e□mailové správy v karanténe (na rozdiel od lokálnej karantény) uchovávané v databázach e□mailových schránok Exchange. E-mailové správy uložené v karanténe môže spravovať ktokoľvek s prístupom ku karanténnej e-mailovej schránke.

Ak porovnáme Karanténnu e-mailovú schránku a karanténu MS Exchange, obe tieto možnosti používajú na ukladanie správ samostatnú e-mailovú schránku, avšak do určitej miery sa odlišujú v tom, ako sú e-mailové správy do tejto schránky doručované. Karanténna e-mailová schránka a karanténa MS Exchange:

Karanténna e-mailová schránka

ESET Mail Security vytvorí osobitnú obálku e-mailu s dodatočnými informáciami, pričom pôvodná e-mailová správa bude pripojená ako príloha, a následne ju doručí do definovanej e-mailovej schránky.

V tomto prípade je potrebné zadať adresu pre karanténu správ (napr. karanténa@firma.sk).

Neodporúčame používať správcovský účet (Administrator) ako karanténnu e-mailovú schránku.

Karanténa MS Exchange

Ak vyberiete možnosť Karanténa MS Exchange, za doručenie e□mailovej správy do e□mailovej schránky je zodpovedný Microsoft Exchange Server. E-mailová schránka musí byť nastavená ako Karanténa v rámci organizačnej štruktúry Active Directory (napr. pomocou príkazu PowerShell uvedeného nižšie).

Interná karanténa v rámci Microsoft Exchange servera štandardne nie je aktivovaná. Ak ju aktivovanú nemáte, bude potrebné otvoriť Exchange Management Shell a zadať nasledujúci príkaz (nahraďte `Name@domain.com` skutočnou adresou vašej vyhradenej e-mailovej schránky): `Set-ContentFilterConfig -QuarantineMailbox name@domain.com`

ESET Mail Security v tomto prípade využíva systém karantény Microsoft Exchange (podporované od verzie Microsoft Exchange Server 2007 vyššie). V tomto prípade je na uchovanie potenciálne infikovaných správ a spamu použitý interný mechanizmus Exchange.

Nastavenia správcu karantény

Adresa hostiteľa

Zobrazí sa automaticky, ak má váš lokálny Exchange Server rolu CAS (Client Access Server). V prípade, že rola CAS nie je na rovnakom serveri ako ESET Mail Security, avšak je možné ju nájsť v rámci Active Directory (AD), adresa hostiteľa sa taktiež zobrazí automaticky. Ak sa adresa nezobrazí automaticky, môžete ju zadať manuálne. Automatická detekcia nefunguje pre serverovú rolu Edge Transport. IP adresy nie sú podporované, musíte zadať názov hostiteľa CAS servera.

Prihlasovacie meno

Vyhradený používateľský účet karantény, ktorý ste vytvorili na uchovávanie správ v karanténe (alebo účet, ktorý má prístup do tejto e-mailovej schránky prostredníctvom delegácie prístupu). Pri serverovej role Edge Transport, ktorá nie je súčasťou domény, je dôležité použiť celú e-mailovú adresu (napríklad *main_quarantine@company.com*).

Heslo

Zadajte heslo pre svoj účet karantény.

Používať SSL

Túto možnosť je potrebné povoliť, ak je EWS (Exchange Web Services) nastavené na **Požadovať SSL protokol** v IIS. Ak je SSL povolené, certifikát Exchange servera je potrebné importovať na systém, na ktorom je spustený program ESET Mail Security (v prípade, že sú roly Exchange servera na rôznych serveroch). Nastavenia pre EWS nájdete v IIS v časti Sites/Default web site/EWS/SSL Settings.

Možnosť **Používať SSL** vypnite len v prípade, ak máte EWS nastavené v IIS tak, aby nevyžadovalo SSL protokol.

Ignorovať chyby certifikátu servera

Ignorované sú nasledujúce stavy: self-signed, wrong name in certificate, wrong usage, expired.

Proxy server

V prípade, že používate proxy server medzi Exchange serverom s rolou CAS a Exchange serverom, kde je nainštalovaný produkt ESET Mail Security, je potrebné, aby boli v nastaveniach definované parametre proxy servera. Je to potrebné z toho dôvodu, že ESET Mail Security sa pripája na EWS (Exchange Web Services) API cez HTTP/HTTPS. V opačnom prípade karanténna e-mailová schránka ani karanténa MS Exchange nebudú funkčné.

Proxy server

Zadajte IP adresu alebo názov vášho proxy servera.

Port

Zadajte číslo portu proxy servera.

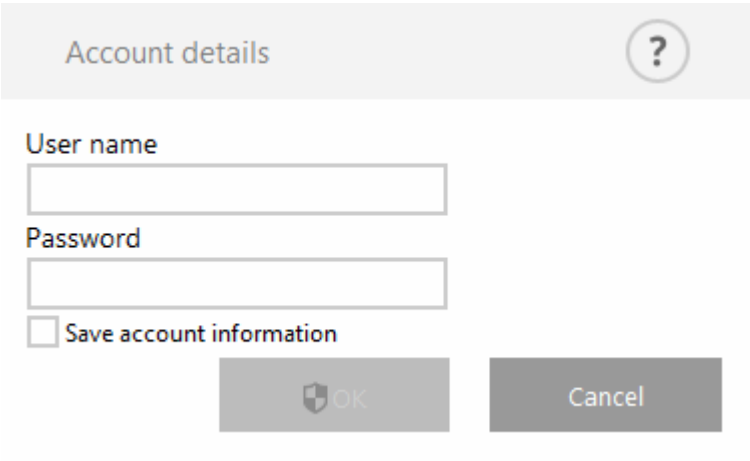
Prihlasovacie meno, heslo

Ak váš proxy server vyžaduje overenie, zadajte príslušné prihlasovacie údaje.

Podrobnosti o účte správcu karantény

Toto dialógové okno sa zobrazí v prípade, že nemáte nastavený účet (prihlasovacie meno a heslo) pre Správcu karantény. Zadajte prihlasovacie údaje používateľa s prístupom do Karanténnej e-mailovej schránky a kliknite na **OK**. Druhou možnosťou je stlačiť kláves **F5** pre zobrazenie okna **Rozšírené nastavenia**, v ktorom prejdete do sekcie **Server** > **E-mailová karanténa** > Nastavenia správcu karantény.

Zadajte **Meno používateľa** a **Heslo** pre vašu karanténnu e-mailovú schránku.



Môžete tiež označiť možnosť **Uložiť informácie o účte** pre uloženie prístupových údajov k účtu správcu karantény pre budúce použitie.

Podpisovanie DKIM

Podpisovanie DKIM (DomainKeys Identified Mail) predstavuje metódu na zaistenie dôveryhodnosti odchádzajúcich e-mailových správ a zjednodušenie ich overovania. Táto metóda poskytuje prijímajúcim e-mailovým serverom spoľahlivý spôsob, ako overiť pravosť správy a odlíšiť ju od spamu.

Overovanie na základe DKIM funguje nasledujúcim spôsobom:

- Hlavičky odchádzajúcich e-mailových správ sú podpísané súkromným kľúčom DKIM.
- Prijímajúci e-mailový server skontroluje DNS záznam domény, ktorý obsahuje verejný kľúč.
- Ak podpis DKIM so súkromným kľúčom v hlavičke správy zodpovedá verejnému kľúču v DNS zázname domény, e-mail sa vyhodnotí ako pravý a je doručený konečnému príjemcovi.

- V prípade, že sa podpis a verejný kľúč nezhodujú, na danú e-mailovú správu sa aplikuje akcia, ktorá závisí od konfigurácie prijímajúceho e-mailového servera (ten môže mať zavedené špecifické pravidlá, napríklad ESET Mail Security používa na tento účel pravidlo podmienené výsledkom DKIM).

Ak chcete používať funkciu podpisovania DKIM v programe ESET Mail Security, uistite sa, že máte pre svoju doménu nakonfigurovaný DNS záznam s DKIM. Podrobnosti o vytváraní záznamu DKIM nájdete v tomto článku. Článok obsahuje aj ukážkový príklad záznamu DKIM. Vyskúšať môžete aj online nástroj DKIM Generator na vygenerovanie súkromných a verejných kľúčov DKIM.

Nakoniec odporúčame použiť nástroj DKIM Record Checker alebo MXToolBox, aby ste si overili, či je syntax správna a verejný kľúč DKIM je naozaj uvedený v DNS zázname.

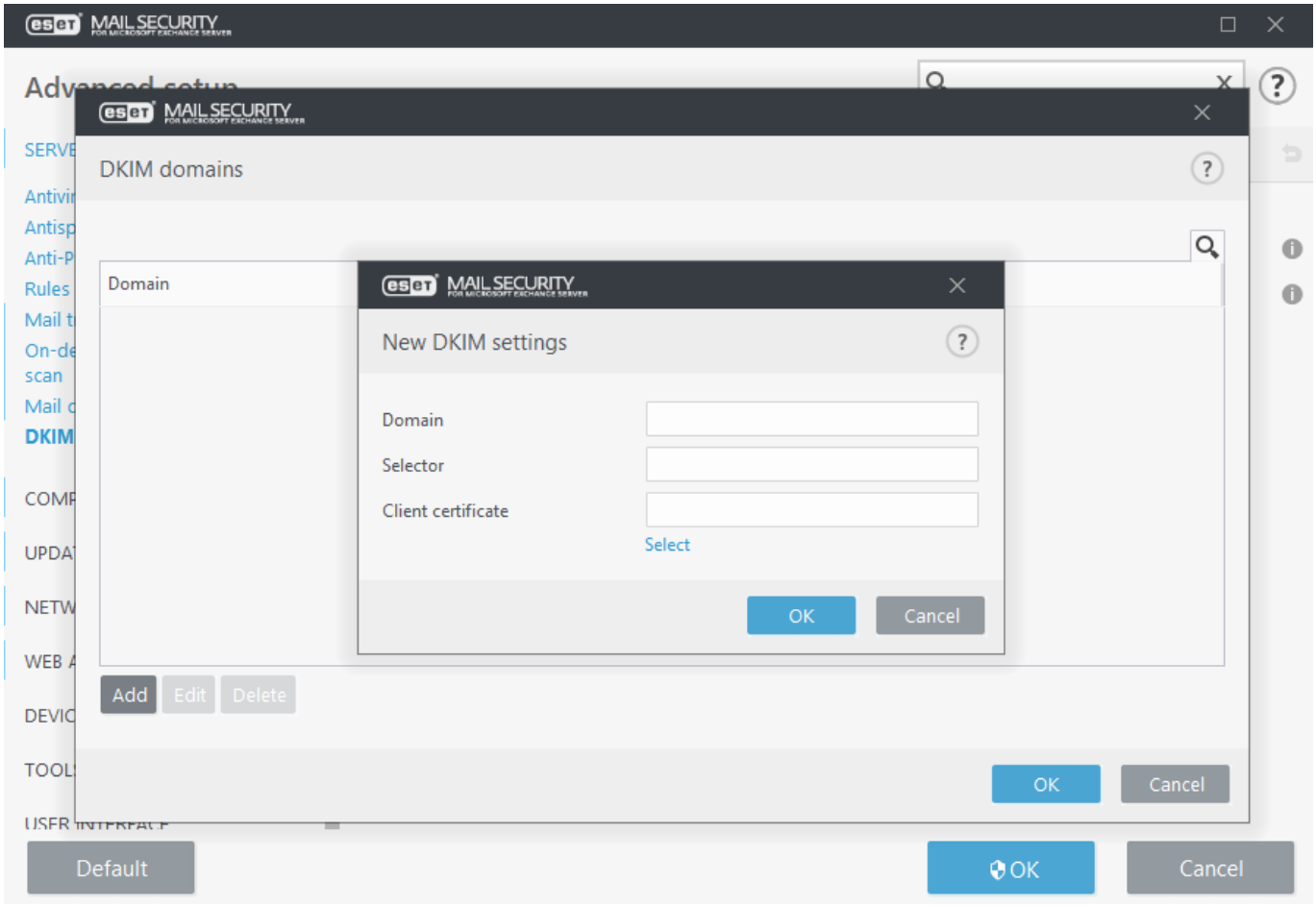
V programe ESET Mail Security nastavíte podpisovanie DKIM špecifikovaním domén DKIM a zoznamu e-mailových hlavičiek, ktoré sa majú podpísať. Podpis DKIM sa pridá do vybraných hlavičiek správ. Každý podpis DKIM obsahuje informáciu, ktorú môžu e-mailové servery použiť na overenie pravosti e-mailových správ na ich ceste k adresátovi. Ak odosielate správy z viacerých domén, môžete nastaviť podpisovanie DKIM pre každú doménu zvlášť.

Podpisovanie DKIM môžete aktivovať v **Rozšírených nastaveniach** v sekcii **Server** > Integrácia. V nastavení priorít agentov odporúčame, aby ste prioritu ESET DKIM Agenta ponechali čo najnižšie, teda na poslednom mieste v poradí, vďaka čomu zabezpečíte, že hlavičky sa podpíšu v poslednom kroku až po akýchkoľvek úpravách inými agentmi.

DKIM domény

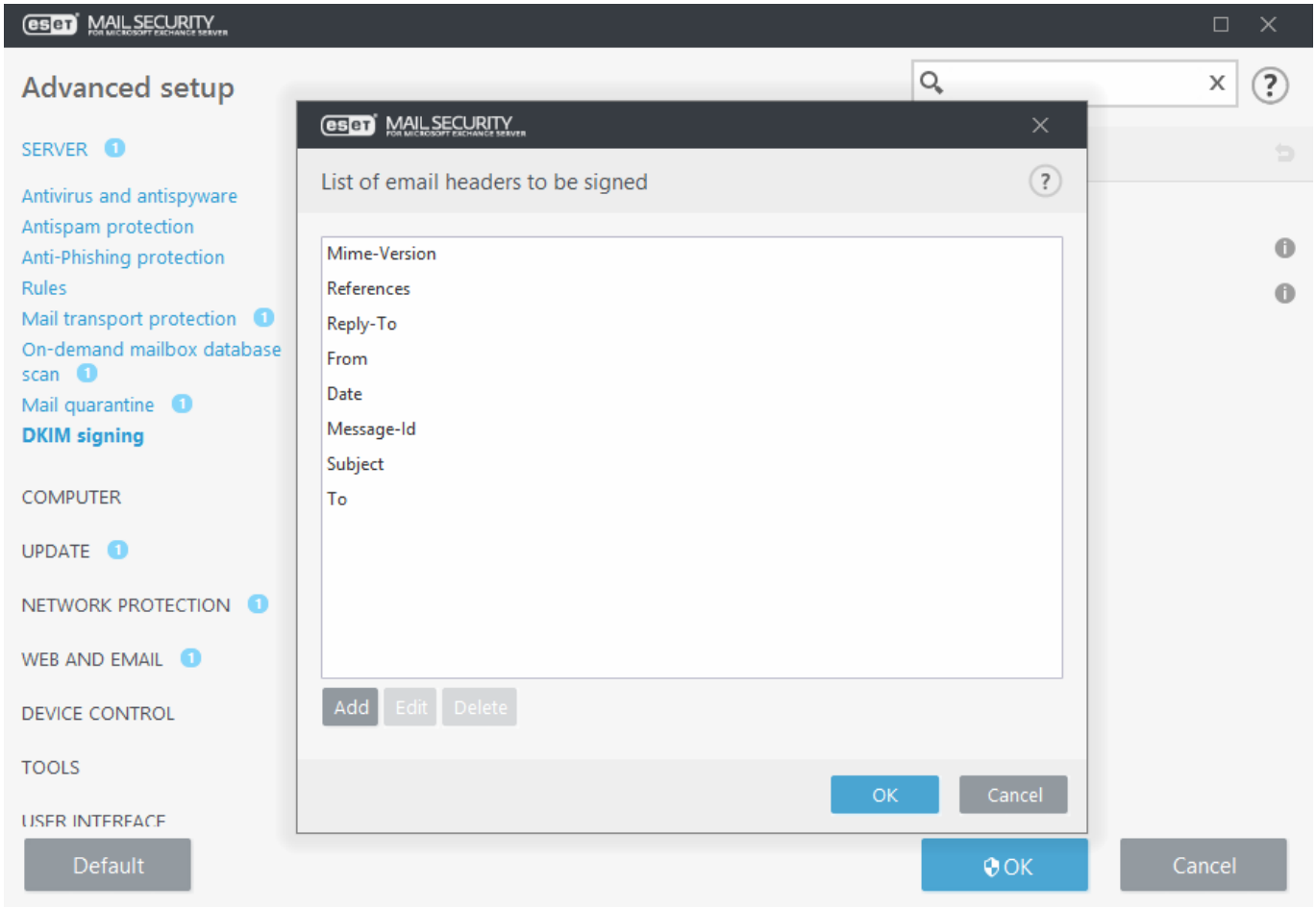
Zadefinujte nastavenia pre každú doménu, ktorá má využívať podpisovanie prostredníctvom DKIM. Ak chcete otvoriť okno domén DKIM, kliknite na **Upraviť**. Click **Add** to create **New DKIM settings** or Edit to modify existing ones.

- **Doména** – zadajte názov domény (napr. *domainname.local*).
- **Selektor** – selektor je špecifikovaný ako atribút pre podpis DKIM, ktorý je uvedený v hlavičke DKIM-Signature.
- **Certifikát klienta** – kliknite na **Vybrať** a zvoľte klientsky certifikát určený na podpisovanie DKIM.



Zoznam e-mailových hlavičiek, ktoré majú byť podpísané

Kliknutím na **Upraviť** otvorte okno zoznamu e-mailových hlavičiek na podpis, kliknite na **Pridať**, ak chcete pridať nové hlavičky, alebo na **Upraviť**, ak chcete upraviť existujúce hlavičky v zozname.



Test antivírusu

Či je rezidentná ochrana funkčná a deteguje vírusy je možné otestovať pomocou testovacieho súboru eicar.com. Ide o súbor, ktorý je detegovaný antivírusovými programami. Súbor bol vytvorený spoločnosťou EICAR (European Institute for Computer Antivirus Research) na otestovanie funkčnosti antivírusových programov.

Ak chcete otestovať svoj antivírusový program, vytvorte textový súbor, ktorý obsahuje nasledujúci reťazec:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Viac informácií, ako aj testovacie súbory v rôznych formátoch nájdete na adrese http://2016.eicar.org/85-0-Download.html.

Test antispamu

Pomocou špeciálneho testovacieho reťazca známeho pod skratkou GTUBE (Generic Test for Unsolicited Bulk Email) môžete otestovať, či antispamová funkcia programu ESET Mail Security funguje správne a deteguje spamové správy.

Pre otestovanie funkčnosti antispamu pošlite e-mail s nasledujúcim 64-bajtovým reťazcom v tele správy:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Tento reťazec nechajte v pôvodnom tvare (jeden riadok, bez medzier). Vhodnú e-mailovú správu si môžete stiahnuť vo formáte RFC-822.

Antiphishingový test

Na otestovanie funkčnosti anti-phishingu pošlite e-mail s nasledujúcim odkazom (URL) v tele alebo predmete správy:

```
https://www.amtso.org/check-desktop-phishing-page/
```

Ak si chcete pozrieť aktivitu antiphishingovej ochrany, prejdite do časti **Protokoly** > Protokol ochrany e-mailových serverov. Nájdete tam informácie o e-mailových správach a phishingových odkazoch, ktoré v nich boli detegované.

Všeobecné nastavenia

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

Computer

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

Aktualizácia

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

Web a e-mail

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

Správa zariadení

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

Konfigurácia nástrojov

Môžete si prispôsobiť nástroje, ako napr. ESET CMD, ESET RMM, poskytovateľ WMI, ESET PROTECT ciele kontroly, upozornenia o aktualizáciách systému Windows, protokoly, proxy server, e-mailové oznámenia, diagnostika, klaster atď.

Používateľské rozhranie

Táto sekcia vám umožňuje nastaviť správanie grafického používateľského rozhrania (GUI), stavy, licenčné údaje,

upozornenia a udalosti, ochranu nastavení heslom, pravidlá spúšťania nástroja eShell atď.

Computer

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

Rezidentná ochrana s využitím strojového učenia

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

Malvér

Počítačový vírus je škodlivý kód pripojený k existujúcim súborom v počítači. Termín „vírus“ sa však často používa nesprávne. Presnejším výrazom je „malvér“ (škodlivý softvér). Detekciu malvéru zabezpečuje modul detekčného jadra v kombinácii s komponentom strojového učenia. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne nechcené aplikácie

Potenciálne nechcená aplikácia je softvér, ktorého cieľ nie je jednoznačne škodlivý, avšak môže nainštalovať ďalší neželaný softvér, zmeniť správanie zariadenia, vykonávať neschválené alebo neočakávané operácie bez vedomia používateľa, prípadne mať iné nejasné ciele.

Táto kategória zahŕňa softvér zobrazujúci reklamu, softvér sťahujúci ďalší softvér, rôzne dodatočné panely s nástrojmi pre prehliadače, softvér so zavádzajúcim správaním, softvér, ktorý inštaluje ďalší softvér, softvér na sledovanie atď. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne podozrivé aplikácie

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

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

Potenciálne nebezpečné aplikácie

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

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

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

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Prah hlásení môžete nastaviť tak, aby lepšie vyhovoval vášmu prostrediu a vašim potrebám. Neexistuje len jedna správna konfigurácia. Preto vám odporúčame, aby ste monitorovali správanie vo svojom prostredí a rozhodli sa, či nie je pre vás vhodnejšie iné nastavenie Hlásení.
Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi, ale posunú informáciu príslušnej vrstve ochrany, ktorá primeraným spôsobom zakročí.

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

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

Ochrana

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

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

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

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

Ochrana využívajúca strojové učenie

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

karantény.

Rezidentná ochrana s využitím strojového učenia

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

Malvér

Počítačový vírus je škodlivý kód pripojený k existujúcim súborom v počítači. Termín „vírus“ sa však často používa nesprávne. Presnejším výrazom je „malvér“ (škodlivý softvér). Detekciu malvéru zabezpečuje modul detekčného jadra v kombinácii s komponentom strojového učenia. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne nechcené aplikácie

Potenciálne nechcená aplikácia je softvér, ktorého cieľ nie je jednoznačne škodlivý, avšak môže nainštalovať ďalší neželaný softvér, zmeniť správanie zariadenia, vykonávať neschválené alebo neočakávané operácie bez vedomia používateľa, prípadne mať iné nejasné ciele.

Táto kategória zahŕňa softvér zobrazujúci reklamu, softvér sťahujúci ďalší softvér, rôzne dodatočné panely s nástrojmi pre prehliadače, softvér so zavádzajúcim správaním, softvér, ktorý inštaluje ďalší softvér, softvér na sledovanie atď. Viac o tomto type aplikácií sa môžete dočítať v slovníku pojmov.

Potenciálne podozrivé aplikácie

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

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

Potenciálne nebezpečné aplikácie

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

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

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

Hlásenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Prah hlásení môžete nastaviť tak, aby lepšie vyhovoval vášmu prostrediu a vašim potrebám. Neexistuje len jedna správna konfigurácia. Preto vám odporúčame, aby ste monitorovali správanie vo svojom prostredí a rozhodli sa, či nie je pre vás vhodnejšie iné nastavenie Hlásení.
Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi, ale posunú informáciu príslušnej vrstve ochrany, ktorá primeraným spôsobom zakročí.

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

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

Ochrana prenosu e□mailov s využitím strojového učenia

Hlásenia
Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi (to je úloha príslušnej ochrannej vrstvy).
Ochrana
Konfiguráciou parametrov v sekcii Ochrana prenosu e‑mailov určíte, čo sa stane so zachytenými objektmi. Môžete tiež nakonfigurovať vlastné pravidlo:

Príklady príkazov pri Základnej inštalácii:
Cieľ: Presunúť do karantény správy, ktoré obsahujú malvér, alebo prílohu, ktorá je chránená heslom, zašifrovaná alebo poškodená
Vytvorte nasledujúce pravidlo pre **Ochranu prenosu e-mailov**:
Podmienka
Typ: **Výsledok antivírusovej kontroly**
Operácia: **je**
Parameter: **Infikované – nevyliečené**

Akcia
Typ: **Presunúť správu do karantény**

Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.
Nakonfigurujte ochranu využívajúcu strojové učenie pomocou eShell. Názov kontextu v eShell je **MLP**. Otvorte eShell v interaktívnom režime a prejdite na MLP:

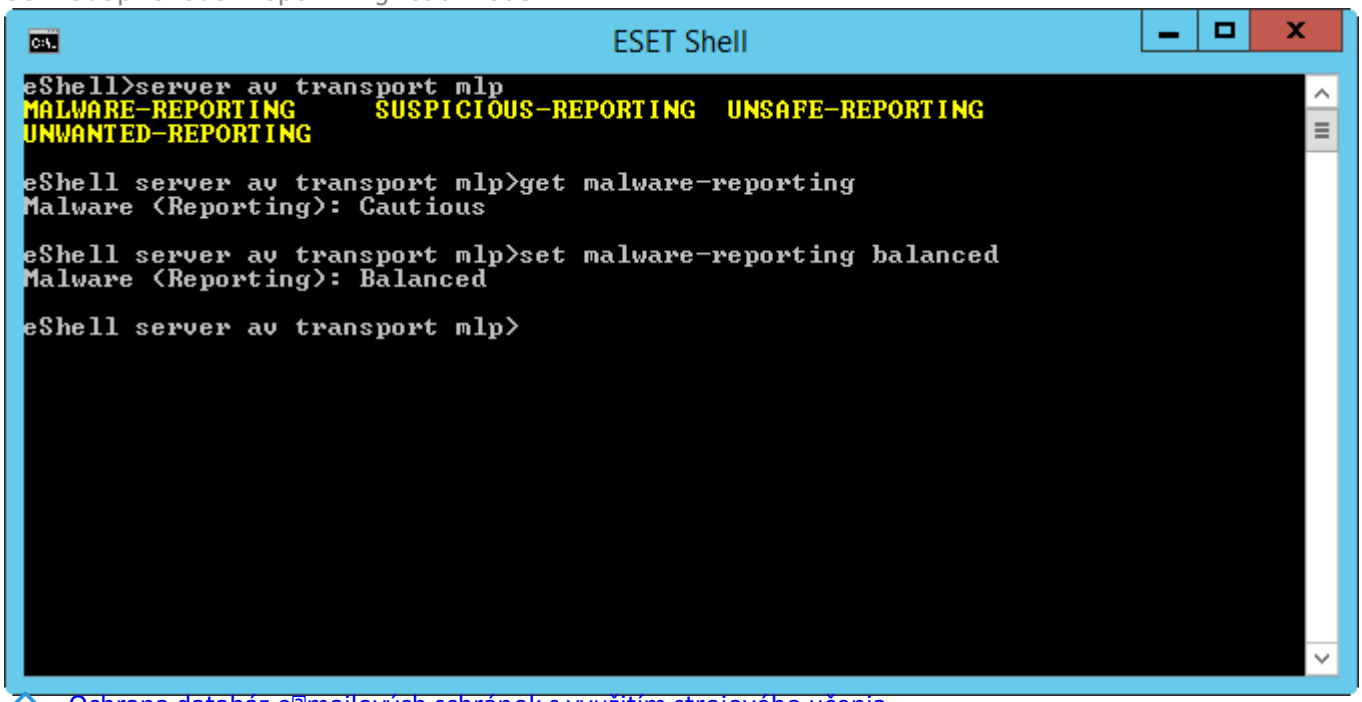
```
server av transport mlp
```

Pozrite si aktuálne nastavenie hlásení pre podozrivé aplikácie:

```
get suspicious-reporting
```

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

```
set suspicious-reporting cautious
```



Ochrana databáz e‑mailových schránok s využitím strojového učenia

Hlásenia
Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi (to je úloha príslušnej ochrannej vrstvy).
Ochrana
Konfiguráciou parametrov v sekcii Ochrana databáz e‑mailových schránok určíte, čo sa stane so zachytenými objektmi.
Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.
Nakonfigurujte ochranu využívajúcu strojové učenie pomocou eShell. Názov kontextu v eShell je **MLP**. Otvorte eShell v interaktívnom režime a prejdite na MLP:
```
server av database mlp
```
Pozrite si aktuálne nastavenie hlásení pre podozrivé aplikácie:
```
get suspicious-reporting
```
Ak chcete, aby boli hlásenia menej prísne, zmeňte nastavenia na Mierne:
```
set suspicious-reporting cautious
```

Manuálna kontrola databáz e‑mailových schránok s využitím strojového učenia

Hlásenia
Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia. Hlásenia neovplyvňujú, čo sa stane so zachytenými objektmi (to je úloha príslušnej ochrannej vrstvy).
Ochrana
Konfiguráciou parametrov v sekcii Manuálna kontrola databáz e‑mailových schránok určíte, čo sa stane so zachytenými objektmi.
Ak chcete vrátiť nastavenia v tejto sekcii na ich predvolené hodnoty, kliknite na šípku v tvare U vedľa názvu sekcie. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.
Nakonfigurujte ochranu využívajúcu strojové učenie pomocou eShell. Názov kontextu v eShell je **MLP**. Otvorte eShell v interaktívnom režime a prejdite na MLP:
```
server av on-demand mlp
```
Pozrite si aktuálne nastavenie hlásení pre podozrivé aplikácie:
```
get suspicious-reporting
```
Ak chcete, aby boli hlásenia menej prísne, zmeňte nastavenia na Mierne:
```
set suspicious-reporting cautious
```

Vylúčenia

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

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

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

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

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

umožňujú vylúčiť z kontroly konkrétne objekty.

Výkonnostné vylúčenia

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

Cesta

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

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

Poznámka

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

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

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

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

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

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

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

Cesta

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

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

Hash

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

Názov detekcie

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

Poznámka

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

ESET PROTECT umožňuje správu vylúčení detekcií, vďaka čomu môžete vytvoriť vylúčenia detekcií a aplikovať ich na viacerých počítačoch/skupinách.

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

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

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

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

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

Sprievodca vytvorením vylúčenia

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

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

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

Pokročilé možnosti

Technológia Anti-Stealth

Ide o dômyselný systém na detekciu nebezpečných programov, ako napríklad rootkitov, ktoré sú pre operačný systém v podstate neviditeľné. Tieto typy programov sa zvyčajne nedajú odhaliť pomocou štandardných techník.

AMSI

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

Automatické vylúčenia

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

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

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

Automatické vylúčenia pre Exchange servery sú založené na odporúčaniach spoločnosti Microsoft. ESET Mail Security uplatňuje len „Vylúčenia adresárov/priečinkov“ („Vylúčenia procesov“ a „Vylúčenia súborov na základe prípon“ sa neuplatňujú). Pre viac informácií prejdite na nasledujúce články znalostnej databázy spoločnosti Microsoft:

Virus scanning recommendations for Enterprise computers that are running currently supported versions of

Windows

Recommendations for troubleshooting an Exchange Server computer with antivirus software installed

File-Level Antivirus Scanning on Exchange 2007

File-Level Antivirus Scanning on Exchange 2010

Anti-Virus Software in the Operating System on Exchange Servers (Exchange 2013)

Running Windows antivirus software on Exchange 2016 servers

> Do vylúčení sú automaticky pridávané aj aktívne a pasívne databázy DAG (Database Availability Group) na lokálnom serveri. Zoznam automatických vylúčení sa aktualizuje každých 30 minút. Ak sa vytvorí nový súbor Exchange databázy, bude automaticky vylúčený bez ohľadu na jeho stav a či je aktívny alebo pasívny.

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

Zdieľaná lokálna vyrovnávacia pamäť

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

Nastavenia servera vyrovnávacej pamäte obsahujú nasledovné:

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

Našla sa infiltrácia

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

Štandardné správanie

V programe ESET Mail Security môžu byť infiltrácie zachytené prostredníctvom nasledujúcich modulov:

- Rezidentná ochrana súborového systému
- Ochrana prístupu na web

- Ochrana e-mailových klientov
- Manuálna kontrola počítača

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

Liečenie a mazanie

Ak rezidentná ochrana súborového systému nemá prednastavenú žiadnu akciu, vyzve vás pomocou výstražného okna, aby ste akciu vybrali sami. Na výber sú spravidla akcie **Liečiť**, **Odstrániť** a **Žiadna akcia**. Možnosť **Žiadna akcia** sa neodporúča, keďže infiltrácia tým pádom zostáva na svojom pôvodnom mieste a naďalej predstavuje potenciálnu hrozbu. Výnimkou je, ak máte úplnú istotu, že daný súbor bol ako infiltrácia detegovaný omylom.

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

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

Viaceré hrozby

Ak niektoré infikované súbory neboli vyliečené počas kontroly počítača (alebo úroveň liečenia bola nastavená na **Neliečiť**), zobrazí sa okno, ktoré vás vyzve, aby ste vybrali akciu pre dané súbory.

Vyberte akciu individuálne pre každú hrozbu v zozname alebo môžete tiež použiť možnosť **Vybrať akciu pre všetky hrozby v zozname** a vybrať jednu akciu, ktorá bude použitá pre všetky hrozby v zozname. Potom kliknite na **Dokončiť**.

Mazanie súborov v archívoch

Pri predvolenej úrovni liečenia je archív zmazaný iba v prípade, že obsahuje len infikované súbory. Archív nebude zmazaný, ak okrem infiltrácie obsahuje aj neškodné neinfikované súbory.

Pri nastavení prísnej úrovne liečenia treba byť opatrný – v tomto prípade bude archív vymazaný bez ohľadu na to, či jeho obsah tvoria aj neinfikované súbory.

Rezidentná ochrana súborového systému

Rezidentná ochrana súborového systému kontroluje v systéme všetky udalosti súvisiace s malvérom. Všetky súbory, ktoré sa v počítači otvárajú, vytvárajú alebo spúšťajú, sú kontrolované na prítomnosť škodlivého kódu. Rezidentná ochrana súborového systému sa predvolene spúšťa pri štarte systému a poskytuje nepretržitú kontrolu.

V špeciálnych prípadoch (napr. ak dôjde ku konfliktu s inou rezidentnou ochranou) je možné rezidentnú ochranu zastaviť zrušením výberu možnosti **Automatický štart rezidentnej ochrany súborového systému** v **Rozšírených nastaveniach** (**F5**) v sekcii **Rezidentná ochrana súborového systému** > **Základné**.

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

FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS.

Vykonávať kontrolu týchto médií

Predvolene je nastavená kontrola všetkých typov médií:

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

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

Vykonávať kontrolu pri týchto udalostiach

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

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

Vylúčenia procesov

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

Parametre ThreatSense

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

Na zabezpečenie minimálnych systémových nárokov pri použití rezidentnej ochrany nie sú súbory, ktoré už boli skontrolované, opakovane kontrolované (pokiaľ neboli zmenené). Súbory sú ihneď kontrolované znova po každej aktualizácii detekčného jadra. Toto správanie je kontrolované pomocou **Smart optimalizácie**. Pokiaľ je **Smart optimalizácia** zakázaná, všetky súbory sú kontrolované vždy, keď sa k nim pristupuje.

Ak chcete toto nastavenie zmeniť, stlačením **F5** otvorte **Rozšírené nastavenia** a kliknite na **Computer** > **Rezidentná ochrana súborového systému**. Následne kliknite na **Parametre ThreatSense** > **Iné** a zapnite alebo

vypnite možnosť **Zapnúť Smart optimalizáciu**.

Doplňujúce parametre ThreatSense

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

Parametre ThreatSense

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

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

Samotné nastavenia ThreatSense umožňujú nastaviť niekoľko parametrov kontroly:

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

Ak chcete zobraziť okno s parametrami, kliknite na **Nastavenie parametrov jadra %TS%>** v **Rozšírených nastaveniach** (**F5**) príslušných modulov využívajúcich technológiu ThreatSense (pozri ďalej). Pre rôzne druhy ochrany sa používa rôzna úroveň nastavenia. Technológia ThreatSense je osobitne nastaviteľná pre tieto moduly:

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

Parametre ThreatSense sú pre každý modul odlišné. Ich zmena môže mať značný vplyv na celkový výkon systému. Príkladom môže byť spomalenie systému pri povolení kontroly runtime packerov a pokročilej heuristiky pre rezidentnú ochranu súborového systému (týmto spôsobom sa zvyčajne kontrolujú iba novovytvorené súbory). Preto odporúčame ponechať pôvodné nastavenia ThreatSense nezmenené pre všetky moduly ochrany okrem Kontroly počítača.

Objekty na kontrolu

Táto sekcia umožňuje nastaviť, ktoré komponenty počítača a súborového systému budú testované na prítomnosť infiltrácie.

Operačná pamäť
Kontroluje prítomnosť hrozieb, ktoré útočia na operačnú pamäť systému.

Zavádzacie sektory/UEFI
Kontrola zavádzacích sektorov na prítomnosť vírusov v tzv. zavádzači operačného systému (MBR). V prípade virtuálneho počítača vytvoreného v prostredí Hyper-V bude MBR disku tohto počítača kontrolovaný v režime iba na čítanie.

Databáza WMI
Skontroluje sa celá databáza WMI s cieľom nájsť odkazy na infikované súbory alebo malvér vložený ako dáta.

Systémová databáza Registry
Skontroluje sa celá systémová databáza Registry, všetky kľúče a podkľúče s cieľom nájsť odkazy na infikované súbory alebo malvér vložený ako dáta.

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

Archívy
Program podporuje nasledujúce prípony: *ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE* a iné.

Samorozbaľovacie archívy
Archívy, ktoré nepotrebujú pre svoje rozbalenie iné programy. Ide o SFX (self-extracting) archívy.

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

> V rámci funkcie Ochrana databáz e-mailových schránok sú priložené e-mailové súbory (napr. súbory *.eml files*) kontrolované bez ohľadu na nastavenia použité v sekcii **Objekty na kontrolu**. Je to preto, lebo Exchange Server spracováva priložený súbor .eml predtým, ako je podrobený kontrole programom ESET Mail Security. Doplnok VSAPI získava extrahované súbory z prílohy .eml namiesto použitia pôvodného súboru .eml.

Možnosti kontroly

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

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

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

Liečenie

Nastavenia liečenia určujú správanie kontroly pri liečení infikovaných súborov. Rezidentná ochrana a ďalšie moduly ochrany ponúkajú nasledujúce úrovne liečenia.

Vždy vyriešiť detekciu

Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany používateľa. Výnimkou sú systémové súbory. Keď liečenie nie je možné vykonať, detegovaný objekt sa ponechá v pôvodnom umiestnení.

Vyriešiť detekciu a ak to nie je možné, ponechať ju

Program sa pokúsi o liečenie detegovaného objektu bez akéhokoľvek zásahu zo strany používateľa. Keď nie je možné vykonať liečenie na systémových súboroch alebo archívoch (s infikovanými aj neškodnými súbormi), detegovaný objekt sa ponechá v pôvodnom umiestnení.

Vyriešiť detekciu a ak to nie je možné, spýtať sa

Program sa pokúsi o liečenie detegovaného objektu. Ak ESET Mail Security nedokáže v niektorých prípadoch vykonať automatickú akciu, výber akcie (odstránenie alebo ignorovanie detekcie) sa prenechá na používateľa. Toto nastavenie sa odporúča vo väčšine prípadov.

Vždy sa spýtať koncového používateľa

ESET Mail Security nevykoná žiadnu automatickú akciu. Výber akcie sa prenechá na používateľa.

Vylúčenia

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

Iné

Pri konfigurácii parametrov ThreatSense v časti Kontrola počítača sú v sekcii **Iné** k dispozícii aj tieto možnosti:

Kontrolovať alternatívne dátové prúdy (ADS)

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

Kontroly na pozadí vykonávať s nízkou prioritou

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

Zapisovať všetky objekty do protokolu

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

Zapnúť Smart optimalizáciu

Pri zapnutej Smart optimalizácii sa použijú optimálne nastavenia pre zabezpečenie najefektívnejšej úrovne kontroly pri zachovaní najvyššej možnej rýchlosti kontroly. Moduly ochrany pri kontrole dômyselne využívajú rozdielne metódy kontroly na rôzne typy súborov. Ak je Smart optimalizácia vypnutá, pri kontrole sú použité len používateľské nastavenia jadra ThreatSense pre konkrétne moduly.

Zachovať čas posledného prístupu k súborom

Pri kontrole súboru nebude zmenený čas prístupu, ale bude ponechaný pôvodný (vhodné pri používaní zálohovacích systémov).

Obmedzenia

Obmedzenia určujúce hranice veľkostí objektov a archívov, ktoré sa budú testovať na prítomnosť vírusov:
Predvolené nastavenie objektov
Budú použité predvolené nastavenia (bez obmedzení). ESET Mail Security bude ignorovať vaše vlastné nastavenia.
Maximálna veľkosť objektu
Určuje maximálnu veľkosť kontrolovaných objektov. Daný modul ochrany bude kontrolovať len objekty s menšou veľkosťou, ako je definovaná hodnota. Tieto hodnoty odporúčame modifikovať len pokročilým používateľom, ktorí chcú veľké objekty vylúčiť z kontroly. Predvolená hodnota: neobmedzená.
Maximálny čas kontroly objektu (v sekundách)
Definuje maximálny povolený čas pre kontrolu objektov. Ak používateľ definuje určitú hodnotu, potom modul ochrany pri kontrole objektu po prekročení tejto hodnoty skončí prebiehajúcu kontrolu bez ohľadu na kompletnosť kontroly. Predvolená hodnota: neobmedzená.
Nastavenie kontroly archívov
Ak chcete robiť zmeny v nastaveniach kontroly archívov, zrušte výber možnosti **Predvolené nastavenie kontroly archívov**.
Úroveň vnorenia archívov
Určuje maximálnu hĺbku kontroly archívov. Predvolená hodnota: 10. Pre objekty detegované Ochranou prenosu e-mailov je potrebná úroveň vnorenia +1. Prvá úroveň je totiž samotný e-mail.

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

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

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

Doplňujúce parametre ThreatSense

Doplňujúce parametre ThreatSense pre vytvárané a menené súbory

Pravdepodobnosť infikovania novovytvorených alebo menených súborov je vyššia ako u existujúcich súborov. To je dôvod, prečo program tieto súbory kontroluje s prídavnými parametrami. Spolu s kontrolou založenou na porovnávaní vzoriek sa využíva pokročilá heuristika, vďaka ktorej možno zachytiť nové hrozby skôr ako vyjde aktualizácia modulov. Okrem novovytvorených súborov sa kontrolujú aj samorozbaľovacie súbory (.sfx) a runtime archívy (interne komprimované spustiteľné súbory).

Predvolene sa archívy kontrolujú do desiatej úrovne vnorenia a bez ohľadu na ich veľkosť. Pre zmenu kontroly archivovaných súborov zrušte výber možnosti **Predvolené nastavenie kontroly archívov**.

Doplňujúce parametre ThreatSense pre spúšťané súbory

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

Prípony súborov vylúčené z kontroly

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

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

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

Vylúčenia procesov

Funkcia Vylúčenia procesov umožňuje nastaviť procesy aplikácií, ktoré nemajú byť kontrolované antimalvérovou kontrolou. Vzhľadom na mimoriadne dôležitú úlohu jednoúčelových serverov (application server, storage server atď.) sú nevyhnutnosťou pravidelné zálohy pre zabezpečenie včasnej obnovy pri rôznych typoch incidentov.

Pre zlepšenie rýchlosti zálohovania, integrity procesov a dostupnosti služieb sa pri zálohovaní používajú niektoré techniky, ktoré sa dostávajú do konfliktu s ochranou pred malvérom. Podobné konflikty môžu nastať aj pri živej migrácii virtuálnych počítačov.

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

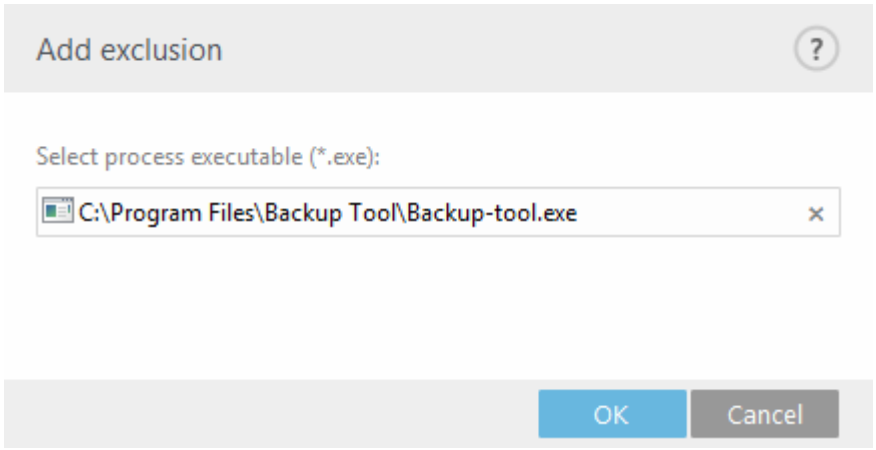
Vylúčenia procesov znižujú riziko potenciálnych konfliktov a zvyšujú výkon vylúčených aplikácií, čo má pozitívny vplyv na celkový výkon a stabilitu operačného systému. Vylúčenie procesu/aplikácie je vylúčenie samotného spustiteľného súboru (*.exe*).

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

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

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

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



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

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

Ochrana s podporou cloudu

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

Pri inštalácii ESET Mail Security označte jednu z nasledujúcich možností:

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

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

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

Štandardne ESET Mail Security odosiela podozrivé vzorky do vírusového laboratória spoločnosti ESET na analýzu. Súbory s niektorými príponami, napríklad .docx alebo .xlsx, sa nikdy neodosielajú. Ak nechcete odosielať aj nejaké iné súbory, môžete doplniť ďalšie prípony.

Zapnúť reputačný systém ESET LiveGrid® (odporúčané)

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

Zapnúť systém spätnej väzby ESET LiveGrid®

Dáta budú odoslané do ESET Research Lab na ďalšiu analýzu.

Odosielať správy o zlyhaniach a diagnostické dáta

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

Odosielať anonymné štatistiky

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

Kontaktný e-mail (nepovinný údaj)

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

Odosielanie vzoriek

Automatické odosielanie infikovaných vzoriek
Týmto sa pošlú všetky infikované vzorky do spoločnosti ESET na analýzu, čo zároveň pomôže vylepšiť ich detekciu v budúcnosti.
- Všetky infikované vzorky
- Všetky vzorky okrem dokumentov
- Neposielať

Automatické odosielanie podozrivých vzoriek
Podozrivé vzorky pripomínajúce hrozby a/alebo vzorky s neobvyklými vlastnosťami alebo správaním sú posielané spoločnosti ESET na analýzu.
- **Spustiteľné súbory** – zahŕňa typy spustiteľných súborov ako .exe, .dll, .sys.
- **Archívy** – zahŕňa typy archívnych súborov ako .zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab.
- **Skripty** – zahŕňa typy skriptov, ako sú .bat, .cmd, .hta, .js, .vbs, .js, .ps1.
- **Iné** – zahŕňa typy súborov ako .jar, .reg, .msi, .swf, .lnk.
- **Potenciálne spamové e-maily** – zlepšuje globálnu detekciu spamu.
- **Dokumenty** – zahŕňa dokumenty aplikácií Microsoft Office a PDF dokumenty s aktívnym obsahom.

Vylúčenia
Kliknite na Zmeniť vedľa vylúčení v sekcii ESET LiveGrid®, ak chcete nastaviť spôsob odosielania vzoriek do vírusových laboratórií spoločnosti ESET.
Maximálna veľkosť vzoriek (MB)
Určuje maximálnu veľkosť kontrolovaných vzoriek.

ESET LiveGuard Advanced

Službu ESET LiveGuard Advanced na klientskom počítači zapnete pomocou ESET PROTECT Web Console. V ESET PROTECT Web Console vytvorte novú politiku, prípadne si otvorte niektorú z existujúcich, a po vykonaní požadovaných zmien túto politiku priraďte k zariadeniam, na ktorých chcete službu ESET LiveGuard Advanced používať.

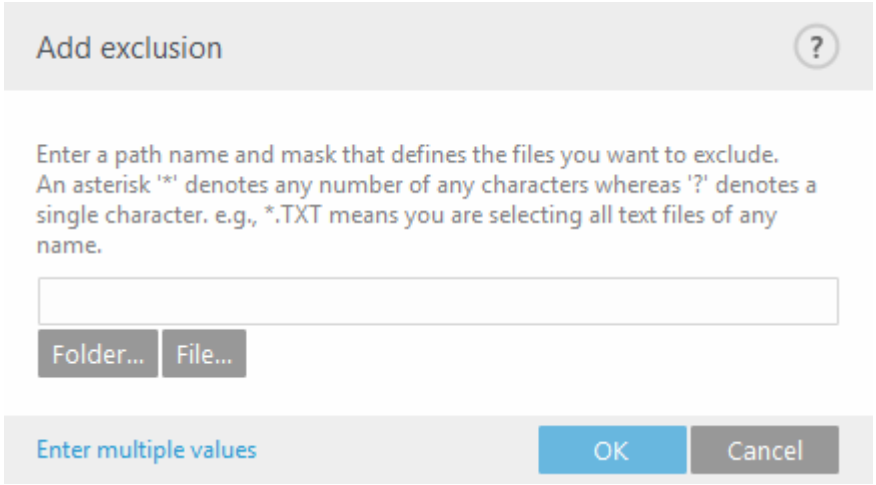
Filter vylúčení

Filter vylúčení vám umožňuje vylúčiť z ochrany súbory alebo adresáre (môže to byť užitočné pri dokumentoch obsahujúcich dôverné informácie).

Súbory pridané do vylúčení nebudú odoslané na analýzu do vírusových laboratórií spoločnosti ESET, a to ani za predpokladu, že obsahujú podozrivý kód.

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

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



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

Detekcia malvéru

V tejto časti môžete nastaviť parametre kontroly počítača.

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

Aktívny profil

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

Zoznam profilov

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

Ciele kontroly

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

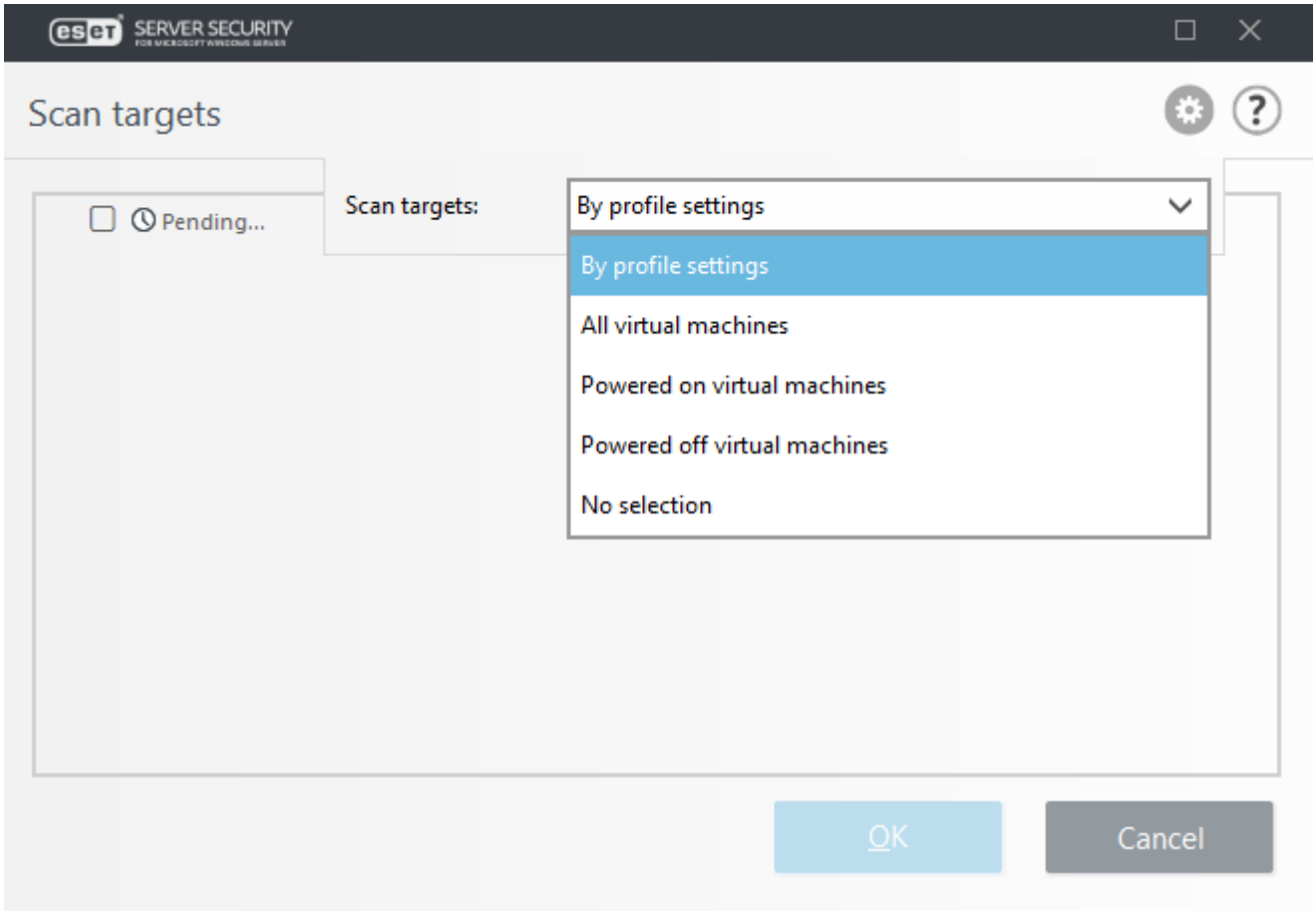
Parametre ThreatSense

V tejto sekcii môžete upraviť parametre manuálnej kontroly.

Manuálna kontrola s využitím strojového učenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia.

V okne Kontrola Hyper‑V:



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

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

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

Manažér profilov

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

- Smart kontrola
- Kontrola z kontextového menu
- Hĺbková kontrola

- Môj profil (vzťahuje sa na Kontrolu Hyper-V a Aktualizačné profily))

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

Manažér profilov sa používa v rámci ESET Mail Security na troch miestach.

Manuálna kontrola počítača

Obľúbené nastavenia kontroly počítača sa dajú uložiť do profilov. Odporúčame vytvoriť viacero profilov s rôznymi cieľmi a metódami kontroly, prípadne ďalšími nastaveniami pre často používané kontroly.

Aktualizácia

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

Kontrola Hyper-V

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

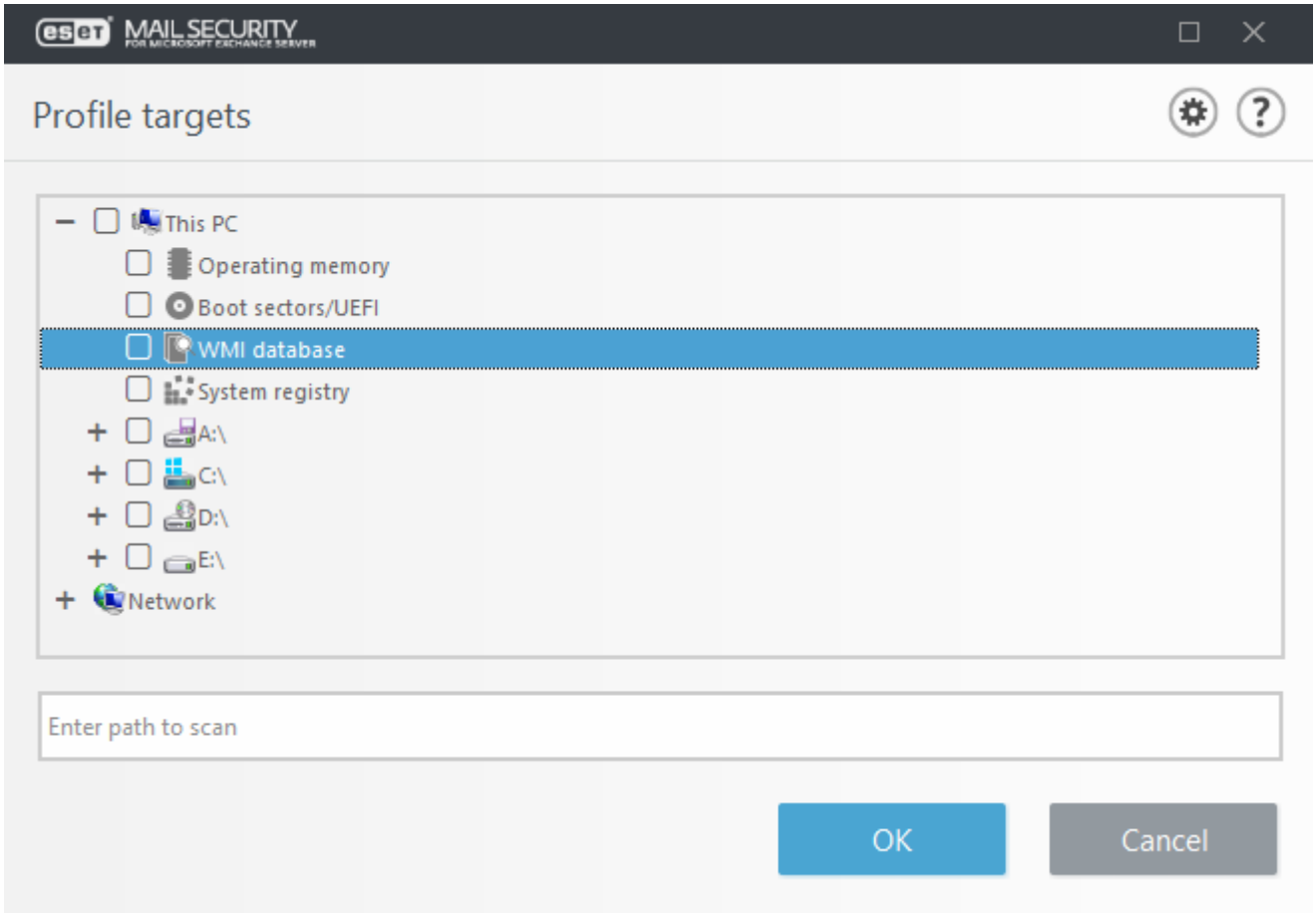
Ciele profilu

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

Tento výber profilu sa vzťahuje na manuálnu kontrolu a kontrolu Hyper-V.

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

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



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

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

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

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

- Smart kontrola
- Kontrola z kontextového menu
- Hĺbková kontrola

Tieto profily používajú rôzne nastavenia parametrov ThreatSense.

Kontrolovať bez liečenia

Ak chcete spustiť kontrolu systému bez liečenia, označte možnosť **Kontrolovať bez liečenia**. Toto je užitočné v prípade, že chcete mať iba prehľad o tom, či sa v systéme vyskytujú infikované položky, prípadne o nich získať

ďalšie podrobnosti. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na možnosť **Nastaviť...** v časti **Parametre ThreatSense** > **Liečenie**. Informácie o kontrole sa zobrazia po skončení kontroly a budú zapísané do protokolu.

Ignorovať vylúčenia

Ak použijete možnosť Ignorovať vylúčenia, umožní vám to vykonať kontrolu, pri ktorej budú ignorované vylúčenia.

Ciele kontroly

Ak chcete skontrolovať len konkrétne súbory na disku, môžete použiť **Vlastnú kontrolu**. Kliknite na **Kontrola počítača** > Vlastná kontrola a z roletového menu Ciele kontroly vyberte príslušnú možnosť, resp. príslušné cieľové umiestnenie z adresárovej (stromovej) štruktúry.

Roletové menu Ciele kontroly sa vzťahuje na nasledujúce typy kontroly:

- Manuálna kontrola
- Kontrola Hyper-V

Ak chcete rýchlo prejsť k cieľu kontroly alebo pridať nový cieľový súbor či priečinok, zadajte jeho názov do prázdneho poľa pod stromovou štruktúrou. Toto je možné len v tom prípade, ak nie sú v stromovej štruktúre vybrané žiadne ciele a v roletovom menu **Ciele kontroly** je nastavená možnosť **Bez výberu**.

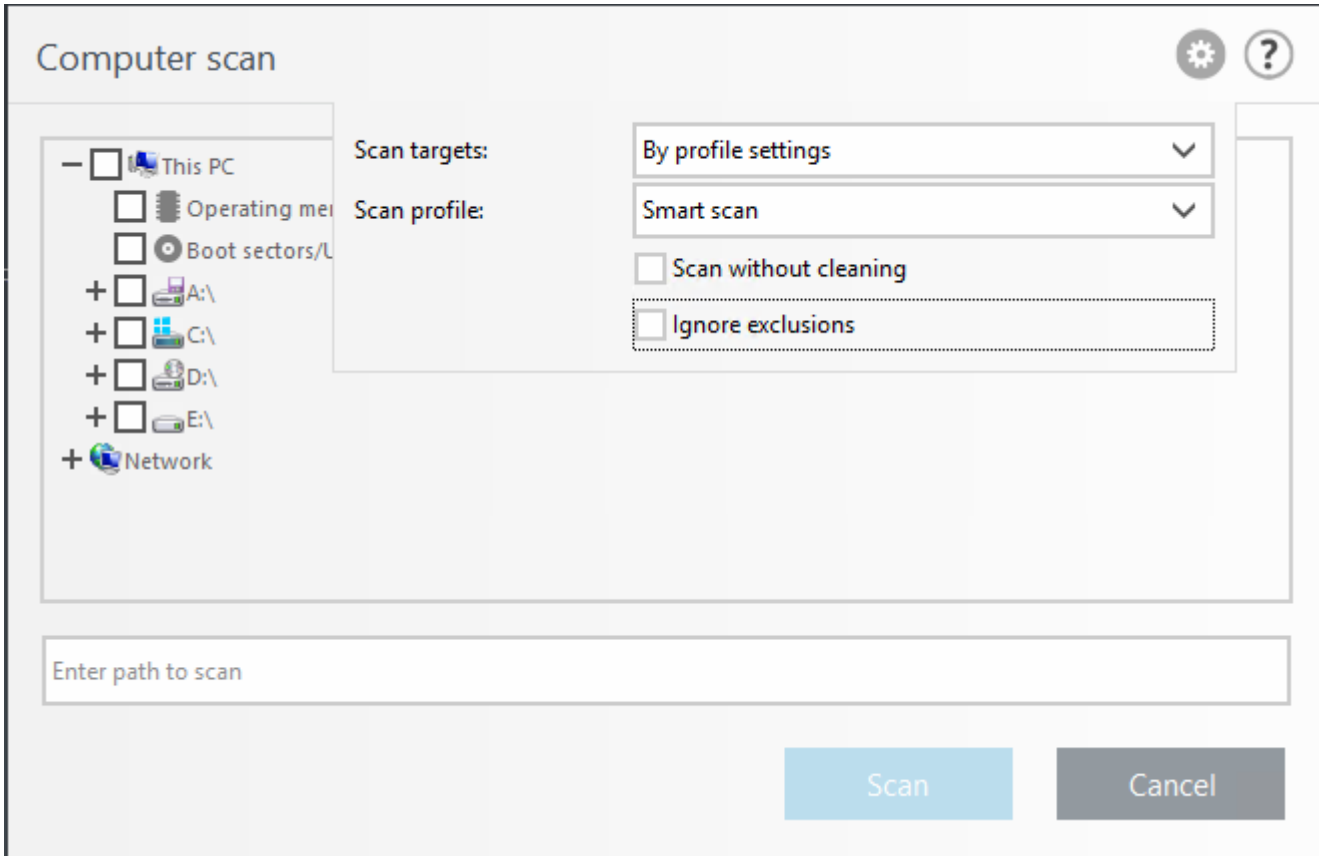
Operačná pamäť	Skontrolujú sa všetky procesy a dáta aktuálne používané v operačnej pamäti.
Zavádzacie sektory/UEFI	Vykoná sa kontrola prítomnosti škodlivého kódu v zavádzacích sektoroch a UEFI. Viac o kontrole UEFI sa dočítate v slovníku pojmov.
Databáza WMI	Skontroluje sa celá databáza Windows Management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

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

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

Profil, s ktorým bude vykonaná kontrola zvolených cieľov, môžete vybrať z roletového menu Profil kontroly. Predvolený profil je **Smart kontrola**. K dispozícii sú ešte ďalšie dva preddefinované profily kontroly: hĺbková kontrola a **kontrola z kontextového menu**. Tieto profily používajú rôzne nastavenia parametrov ThreatSense.

V okne **Vlastná kontrola**:



Kontrolovať bez liečenia

Ak chcete spustiť kontrolu systému bez liečenia, označte možnosť **Kontrolovať bez liečenia**. Toto je užitočné v prípade, že chcete mať iba prehľad o tom, či sa v systéme vyskytujú infikované položky, prípadne o nich získať ďalšie podrobnosti. Máte na výber tri úrovne liečenia, ktoré je možné nastaviť po kliknutí na možnosť **Nastaviť...** v časti **Parametre ThreatSense** > **Liečenie**. Informácie o kontrole sa zobrazia po skončení kontroly a budú zapísané do protokolu.

Ignorovať vylúčenia

Môžete vykonať kontrolu, pri ktorej budú ignorované vylúčenia.

Kontrola

Spustenie kontroly počítača s parametrami, ktoré sú nastavené.

Kontrolovať ako správca

Spustenie kontroly počítača pod účtom správcu. Túto možnosť je vhodné použiť, ak prihlásený používateľ nemá dostatočné oprávnenia na prístup k príslušným súborom, ktoré sa majú kontrolovať. Táto možnosť nie je dostupná, ak používateľ nemôže vyvolať operácie UAC (kontroly používateľských kont) ako správca.

Kontrola v nečinnosti

Ak je počítač v stave nečinnosti, na pozadí sa spúšťa kontrola všetkých diskov počítača. **Kontrola v nečinnosti** sa spustí, ak je zistený jeden z nasledujúcich stavov nečinnosti:

- vypnutá obrazovka alebo aktívny šetrič obrazovky,

- uzamknutý počítač,
- odhlásený používateľ.

Spustiť, aj keď je počítač napájaný z batérie

V predvolených nastaveniach programu sa kontrola nečinnosti nespúšťa, ak je počítač (notebook) napájaný z batérie.

Vytvárať protokol

Túto možnosť môžete použiť v prípade, ak chcete z kontroly v nečinnosti vytvárať protokol, ktorý nájdete v časti Protokoly (v hlavnom okne programu kliknite na Protokoly a potom z roletového menu vyberte možnosť Kontrola počítača).

Parametre ThreatSense

V tejto sekcii môžete upraviť parametre kontroly (napr. metódy detekcie) pre kontrolu v nečinnosti.

Kontrola pri štarte

Pri predvolených nastaveniach programu bude po štarte systému (prihlásení používateľa) a po úspešnej aktualizácii modulov vykonaná kontrola súborov spúšťaných pri štarte. Táto kontrola je riadená nastavením plánovača a úlohami.

Nastavenia kontroly pri štarte sú súčasťou plánovanej úlohy nazvanej **Kontrola súborov spúšťaných pri štarte počítača**.

Pre zmenu/zobrazenie týchto nastavení kliknite na **Nástroje** > **Plánovač**, potom vyberte jednu z úloh pod názvom **Kontrola súborov spúšťaných pri štarte počítača** (prihlásenie používateľa alebo aktualizácia modulov) a kliknite na **Upraviť**. Prejdite sprievodcom a v poslednom kroku budete môcť zmeniť podrobné nastavenia kontroly súborov spúšťaných pri štarte počítača.

Kontrola súborov spúšťaných pri štarte počítača

Pri vytváraní úlohy Kontrola súborov spúšťaných po štarte v plánovači máte na výber nasledujúce možnosti:

V roletovom menu Cieľ kontroly sa určuje hĺbka kontroly súborov spúšťaných pri štarte operačného systému. Ich poradie je určené podľa počtu kontrolovaných súborov:

- Všetky registrované súbory (najviac kontrolovaných súborov)
- Zriedkavo používané súbory
- Bežne používané súbory
- Často používané súbory
- Iba najčastejšie používané súbory (najmenej kontrolovaných súborov)

Patria sem aj dve špecifické skupiny Cieľov kontroly:

Súbory spustené pred prihlásením používateľa

Ide o súbory z umiestnení, z ktorých sa môžu spúšťať súbory bez toho, aby bol používateľ prihlásený (ide takmer o všetky startup umiestnenia, ako napr. služby, vyhľadávanie objektu pomocníka, winlogon notify, položky plánovača systému Windows, známe dll súbory atď.).

Súbory spustené po prihlásení používateľa

Ide o súbory z umiestnení, z ktorých sa spúšťajú súbory po prihlásení používateľa (súbory, ktoré sa spúšťajú iba pre daného používateľa, napr. *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Zoznamy súborov na kontrolu sú pre každú skupinu pevne definované.

Priorita kontroly

Ide o prioritu, s ktorou bude spustená kontrola:

- **Normálna** – zaťaženie systému je normálne,
- **Nižšia** – zaťaženie systému je nižšie,
- **Najnižšia** – zaťaženie systému je najnižšie možné,
- **Počas nečinnosti** – v momente, keď nie sú vykonávané žiadne iné činnosti.

Vymeniteľné médiá

ESET Mail Security poskytuje automatickú kontrolu externých vymeniteľných médií (CD/DVD/USB). Tento modul vám umožňuje skontrolovať vymeniteľné médiá. Môže to byť užitočné v prípade, ak správca chce zabrániť používateľom v používaní externých médií s nežiaducim obsahom.

Vykonať akciu po vložení alebo pripojení vymeniteľného média

Vyberte akciu, ktorá bude vykonaná pri pripojení vymeniteľného média do počítača (CD/DVD/USB).

- **Nekontrolovať** – nebude vykonaná žiadna akcia a okno Rozpoznané nové zariadenie sa zatvorí.
- **Automaticky skontrolovať zariadenie** – spustí sa kontrola vymeniteľného zariadenia.
- **Zobraziť možnosti kontroly** – zobrazenie podrobných nastavení vymeniteľných médií.

Po pripojení vymeniteľného média k počítaču sa zobrazí nasledujúce okno:

- **Kontrolovať teraz** – spustí sa kontrola vymeniteľného média.
- **Kontrolovať neskôr** – kontrola vymeniteľného média bude odložená.
- **Nastavenia** – otvorí Rozšírené nastavenia.
- **Vždy použiť zvolenú možnosť** – vyberte predvolenú akciu, ktorá bude vykonaná po pripojení vymeniteľného média do počítača.

ESET Mail Security ponúka tiež možnosť správy zariadení, ktorá umožňuje používateľom definovať pravidlá pre

používanie externých zariadení na počítači. Viac informácií nájdete v kapitole Správa zariadení.

Ochrana dokumentov

Modul ochrany dokumentov kontroluje dokumenty Microsoft Office pred ich otvorením a kontroluje objekty pri automatickom sťahovaní pomocou programu Internet Explorer, napríklad prvky Microsoft ActiveX. Ochrana dokumentov môže byť zakázaná na účely zvýšenia výkonu na operačných systémoch Windows, ktoré nie sú vystavované veľkým počtom dokumentov balíka Microsoft Office.

Integrácia do systému

Táto možnosť vylepšuje ochranu dokumentov Microsoft Office (za normálnych okolností sa nevyžaduje).

Parametre ThreatSense

V tejto sekcii môžete upraviť parametre Ochrany dokumentov.

> Tento modul pracuje iba s aplikáciami, ktoré podporujú rozhranie Microsoft Antivirus API (napríklad Microsoft Office 2000 od verzie 9.0 a Microsoft Internet Explorer od verzie 5.0).

Kontrola Hyper-V

Aktuálna verzia kontroly Hyper-V podporuje kontrolu online alebo offline virtuálneho systému v Hyper-V. Podporované typy kontroly podľa hostiteľského systému Windows Hyper-V a stavu virtuálneho systému sú uvedené nižšie:

Virtuálne systémy s funkciou Hyper-V	Online virtuálny počítač	Offline virtuálny počítač
Windows Server 2022 Hyper-V	iba na čítanie	iba na čítanie/liečenie
Windows Server 2019 Hyper-V	iba na čítanie	iba na čítanie/liečenie
Windows Server 2016 Hyper-V	iba na čítanie	iba na čítanie/liečenie
Windows Server 2012 R2 Hyper-V	iba na čítanie	iba na čítanie/liečenie
Windows Server 2012 Hyper-V	iba na čítanie	iba na čítanie/liečenie
Windows Server 2008 R2 SP1 Hyper-V	žiadna kontrola	iba na čítanie/liečenie

Hardvérové požiadavky

Server by nemal mať žiadne problémy s výkonom a zaťažením pri chode na virtuálnom počítači. Kontrola využíva prevažne prostriedky procesora. Kontrola spusteného virtuálneho počítača vyžaduje dostatok voľného miesta na disku. Voľné miesto na disku musí predstavovať aspoň dvojnásobok miesta použitého pre kontrolné body/snímky a virtuálne disky.

Špecifické obmedzenia

- Kontrola úložiska RAID, rozložených zväzkov a dynamických diskov nie je podporovaná z dôvodu povahy dynamických diskov. Odporúčame teda nepoužívať dynamické disky na vašich virtuálnych počítačoch, ak je to možné.

- Kontrola vždy prebieha na aktuálnom virtuálnom počítači a nemá vplyv na kontrolné body alebo snímky (snapshot).

- Hyper-V spustený na hostiteľovi v klastri momentálne nie je podporovaný produktom ESET Mail Security.

- Virtuálne počítače na hostiteľovi Hyper-V bežiacom na systéme Windows Server 2008 R2 SP1 môžu byť kontrolované v režime iba na čítanie (Neliečiť) bez ohľadu na to, aká úroveň liečenia je vybraná v časti parametre ThreatSense.

Kým ESET Security podporuje kontrolu MBR virtuálnych diskov, podporovaná je len kontrola v režime iba na čítanie. Toto nastavenie je možné zmeniť v sekcii **Rozšírené nastavenia** (**F5**) > **Computer** > **Kontrola Hyper-V** > Parametre ThreatSense > **Zavádzacie sektory**.

Virtuálny počítač, ktorý má byť kontrolovaný, je offline (vypnutý)

ESET Mail Security využíva nástroj Hyper-V Management na detekciu a pripojenie k virtuálnym diskom. ESET Mail Security má takto rovnaký prístup k obsahu virtuálnych diskov ako v prípade štandardných diskov.

Virtuálny počítač, ktorý má byť kontrolovaný, je online (spustený, pozastavený, uložený)

ESET Mail Security využíva nástroj Hyper-V Management na detekciu virtuálnych diskov. Pripojenie k týmto diskom nie je možné. ESET Mail Security tým pádom vytvára kontrolné body/snímky virtuálneho počítača a potom sa k nim pripája. Po dokončení kontroly sa kontrolný bod/snímka vymaže. To znamená, že kontrola v režime iba na čítanie môže byť vykonávaná, pretože na spustené virtuálne počítače vplyv nemá.

Počkajte približne minútu, kým ESET Mail Security vytvorí počas kontroly snímku alebo kontrolný bod. Toto je potrebné mať na pamäti v prípade spustenia kontroly Hyper-V na väčšom množstve virtuálnych počítačov.

Názvová konvencia

Modul kontroly Hyper-V používa nasledujúcu konvenciu vytvárania názvov:

```
VirtualMachineName\DiskX\VolumeY
```

kde X je číslo disku a Y je číslo zväzku. Napríklad:

```
Computer\Disk0\Volume1
```

Číselná prípona sa pridá na základe poradia detekcie diskov a je totožná s poradím diskov v Správcovi virtuálnych diskov. Táto konvencia pomenovávania je použitá v strome cieľov kontroly na indikátore priebehu kontroly, ako aj v protokoloch kontroly.

Spustenie kontroly

- Manuálne – kliknite na **Kontrola Hyper-V** pre zobrazenie zoznamu virtuálnych počítačov a zväzkov, pre ktoré môže byť vykonaná kontrola. Označte virtuálne počítače, disky alebo zväzky, ktoré chcete kontrolovať a kliknite na **Kontrolovať**.

- Vytvorením naplánovanej úlohy.

- Pomocou nástroja ESET PROTECT, použitím klientskej úlohy nazvanej Kontrola servera.

- Kontrolu Hyper-V je možné spravovať a spúšťať pomocou rozhrania eShell.

Môžete spustiť viacero kontrol Hyper-V súčasne. Po dokončení kontroly sa zobrazí oznámenie s odkazom na súbory protokolov.

Možné problémy

- Pri spustení kontroly online virtuálneho počítača sa vytvorí kontrolný bod/snímka daného počítača, pričom pri vytváraní kontrolného bodu/snímky môžu byť základné funkcie virtuálneho počítača obmedzené alebo úplne znemožnené.
- Ak je kontrolovaný vypnutý virtuálny počítač, nemôže byť zapnutý až do dokončenia kontroly.
- Nástroj Hyper-V Manager vám umožňuje nazvať dva rozdielne virtuálne počítače identicky, čo predstavuje problém pri rozlišovaní počítačov v protokoloch kontroly.

Kontrola Hyper-V s využitím strojového učenia

Hlásenia zabezpečuje detekčné jadro a komponent strojového učenia.

Parametre ThreatSense

Táto možnosť slúži na zmenu parametrov kontroly Hyper-V.

HIPS

HIPS (Host-based Intrusion Prevention System) chráni váš systém pred škodlivým kódom a eliminuje aktivity ohrozujúce bezpečnosť vášho počítača. Používa pokročilú analýzu správania kódu, ktorá spolu s detekčnými schopnosťami sieťového filtra zabezpečuje sledovanie spustených procesov, súborov a záznamov v databáze Registry. HIPS pracuje oddelene od firewallu aj od rezidentnej ochrany, sleduje len procesy spustené v rámci operačného systému.

Ak nie ste skúsený používateľ, neodporúčame meniť nastavenia systému HIPS. Nesprávne nastavenia v sekcii HIPS môžu spôsobiť nestabilitu systému.

Zapnúť Self-Defense

ESET Mail Security má vstavanú technológiu Self-Defense, ktorá slúži na to, aby zabránila pokusom škodlivého softvéru o narušenie alebo zablokovanie antimalvérovej ochrany. Zmeny v nastaveniach Zapnúť HIPS a Zapnúť SD (Self-Defense) sa prejavia až po reštarte systému Windows. Z tohto dôvodu sa aj vypnutie celého systému HIPS prejaví až po reštarte.

Zapnúť ako chránenú službu

Microsoft predstavil uvedením systému Microsoft Windows Server 2012 R2 koncept chránených služieb. Ide o ochranu služieb pred malvérovými útokmi. Je to vďaka tomu, že jadro programu ESET Mail Security automaticky beží ako chránená služba. Táto funkcia je dostupná na systéme Microsoft Windows Server 2012 R2 a novších operačných systémoch určených pre servery.

Zapnúť pokročilú kontrolu pamäte

V kombinácii s technológiou Exploit Blocker zvyšuje ochranu proti malvéru, ktorý bol navrhnutý tak, aby maskovaním alebo šifrovaním obišiel detekciu antimalvérových produktov. Táto možnosť je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov.

Zapnúť Exploit Blocker

Slúži na ochranu najčastejšie zneužívaných aplikácií, ako sú internetové prehliadače, prehliadače PDF dokumentov, e-mailové klienty a súčasti balíka Microsoft Office. Táto možnosť je v predvolených nastaveniach povolená. Viac o tomto type ochrany sa môžete dočítať v slovníku pojmov.

Zapnúť Ransomware Shield

Ak chcete použiť túto funkciu, je potrebné zapnúť HIPS a ESET Live Grid. Viac o malvéri typu ransomware nájdete v slovníku pojmov.

Režim filtrovania

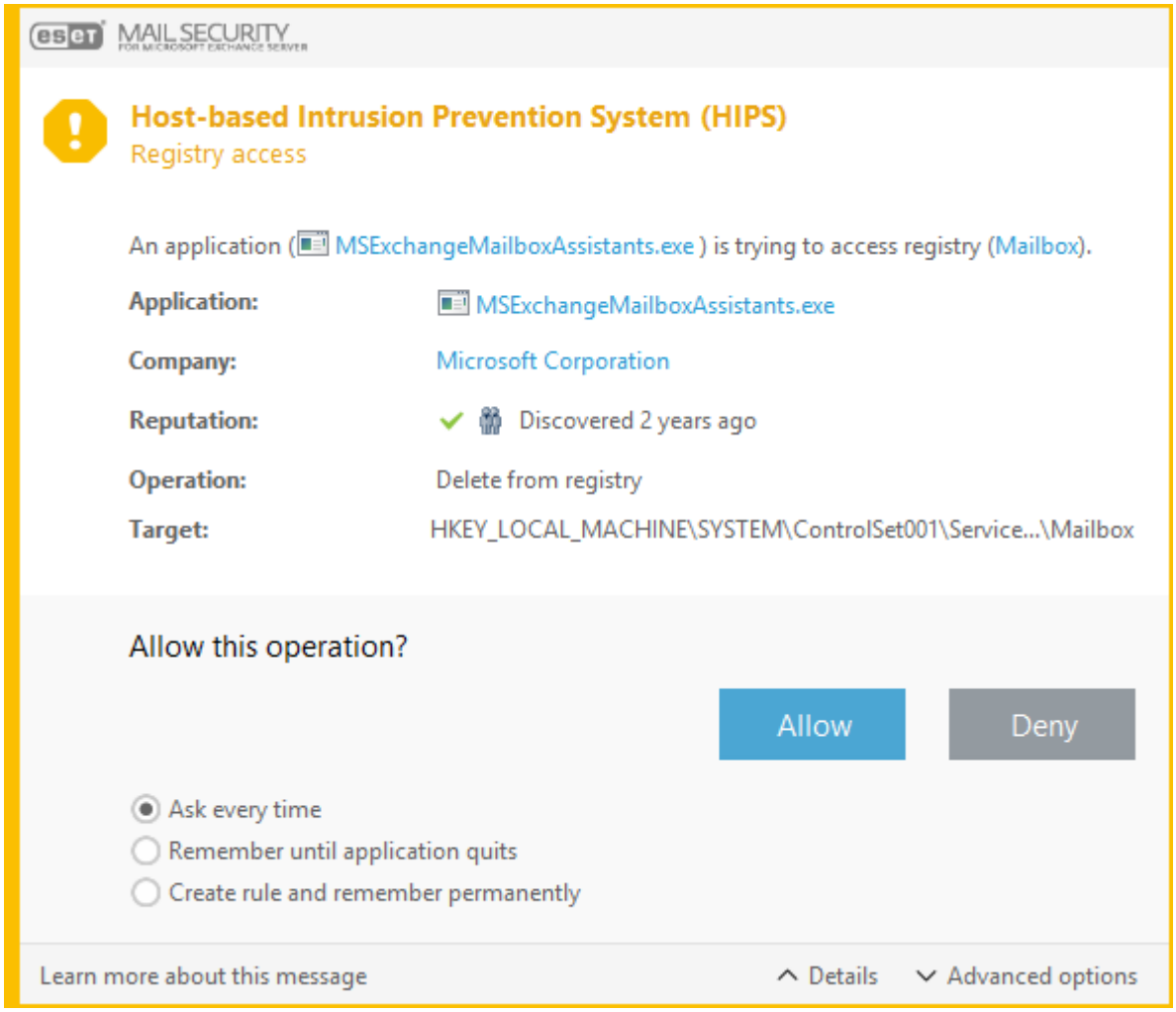
Môžete si vybrať jeden zo štyroch režimov filtrovania:

- **Automatický režim** – operácie budú povolené s výnimkou operácií blokovaných preddefinovanými pravidlami, ktoré chránia váš systém. Povolené je všetko okrem akcií, ktoré sú zakázané pravidlom.
- **Smart režim** – používateľ bude upozornený na podozrivé udalosti v systéme.
- **Interaktívny režim** – používateľ bude vyzvaný na povolenie operácií. Dostupné sú nasledujúce možnosti: Povoliť/zakázať prístup, Vytvoriť pravidlo, Dočasne si zapamätať akciu pre tento proces.
- **Režim politík** – operácie budú blokované. Akceptované sú len preddefinované pravidlá alebo pravidlá definované používateľom.
- **Učiaci sa režim** – operácie sú povolené a zároveň je vytvorené pravidlo, ktoré ich povoľuje. Pravidlá vytvorené týmto režimom sú viditeľné v editore pravidiel, ale majú nižšiu prioritu ako pravidlá vytvorené manuálne alebo pravidlá vytvorené v automatickom režime. Ak vyberiete možnosť Učiaci sa režim z roletového menu Režim filtrovania, sprístupní sa možnosť Učiaci sa režim skončí. Nastavte obdobie, počas ktorého bude zapnutý učiaci sa režim (maximálne 14 dní). Po uplynutí nastaveného obdobia, budete vyzvaný na upravenie pravidiel, ktoré boli vytvorené počas učiaceho sa režimu HIPS. Môžete tiež zvoliť iný režim filtrovania alebo oddialiť vaše rozhodnutie a používať učiaci sa režim aj naďalej.

Pravidlá

Pravidlá definujú, ktoré aplikácie môžu pristupovať ku ktorým súborom, databáze Registry a iným aplikáciám. Systém HIPS monitoruje udalosti vo vnútri operačného systému a reaguje na ne podľa pravidiel, ktoré sú štruktúrou podobné pravidlám firewallu. Ak chcete otvoriť okno správy pravidiel systému HIPS, kliknite na Upraviť. Ak je akcia v pravidle nastavená na **Spýtať sa**, po spustení pravidla sa zobrazí dialógové okno s výberom možností. Môžete si vybrať, či má byť operácia **povolená** alebo **blokovaná**. Ak používateľ nevyberie akciu vo vyhradenom čase, bude na základe pravidiel vytvorená nová akcia.

Dialógové okno umožňuje vytvorenie pravidla podľa akejkoľvek novej akcie detegovanej modulom HIPS a následné definovanie podmienok, ktoré musia byť splnené pre **povolenie** alebo **blokovanie** danej akcie. Bližšie informácie zobrazíte kliknutím na **Podrobnosti**. Takto vytvorené pravidlá sa vyhodnocujú rovnako, ako keby boli zadané ručne, teda pravidlo vytvorené z dialógového okna môže byť menej špecifické ako pravidlo, ktoré tento dialóg vyvolalo. To znamená, že po vytvorení takéhoto pravidla sa môže pri rovnakej udalosti zobraziť ďalšie dialógové okno, ak parametre z predchádzajúcej situácie nevyhovujú pre novú situáciu.



Vždy sa spýtať

Pri každom spustení pravidla sa zobrazí dialógové okno. Môžete si vybrať, či má byť operácia **povolená** alebo **zakázaná**.

Zapamätať si do ukončenia aplikácie

Výberom akcie **Zakázať** alebo **Povoliť** sa vytvorí dočasné pravidlo HIPS, ktoré bude použité, až kým nedôjde k zatvoreniu príslušnej aplikácie. Ak zmeníte režim filtrovania, upravíte pravidlá, prípadne dôjde k aktualizácii modulu HIPS alebo reštartujete systém, dočasné pravidlá budú vymazané.

Vytvoriť pravidlo a zapamätať natrvalo

Umožňuje vytvorenie nového pravidla HIPS. Toto pravidlo môžete neskôr upraviť v sekcii určenej na správu pravidiel HIPS.

Nastavenie pravidla HIPS

V tomto okne sa zobrazuje prehľad pravidiel HIPS.

Pravidlo	Názov pravidla určený používateľom alebo automaticky.
Zapnuté	Túto možnosť je vhodné deaktivovať v prípade, ak si želáte ponechať dané pravidlo v zozname pravidiel, avšak nechcete ho používať.

Pravidlo	Názov pravidla určený používateľom alebo automaticky.
Akcia	Pravidlo špecifikuje (práve jednu) akciu (Povoliť, Blokovať, Spýtať sa), ktorú je potrebné vykonať, ak sú všetky podmienky splnené.
Zdroje	Pravidlo sa uplatní len v prípade, že udalosť vyvolajú konkrétne aplikácie.
Ciele	Pravidlo sa uplatní, len ak sa operácia týka konkrétneho súboru, aplikácie alebo položky databázy Registry.
Závažnosť zapisovania do protokolu	Po zapnutí tejto možnosti budú informácie o danom pravidle zapisované do protokolu HIPS.
Oznamovať	Po spustení udalosti sa v oblasti oznámení systému Windows zobrazí malé okno.

Kliknutím na **Pridať** môžete vytvoriť nové pravidlo HIPS, prípadne kliknite na **Upraviť**, ak chcete upraviť označené položky.

Názov pravidla

Názov pravidla určený používateľom alebo automaticky.

Akcia

Pravidlo špecifikuje (práve jednu) akciu (**Povoliť**, **Blokovať**, **Spýtať sa**), ktorú je potrebné vykonať, ak sú všetky podmienky splnené.

Ovplyvnené operácie

Vyberte typy operácií, na ktoré bude pravidlo aplikované. Pravidlo sa uplatní len na tento typ operácie a na zvolený cieľ. Pravidlo pozostáva z častí, ktoré popisujú podmienky, za ktorých sa pravidlo spustí:

Zdrojové aplikácie

Pravidlo sa uplatní, len ak udalosť vyvolajú dané aplikácie. Vyberte možnosť **Špecifické aplikácie** z roletového menu a kliknite na **Pridať**, ak chcete pridať jednotlivé súbory alebo priečinky konkrétnej aplikácie, prípadne označte v roletovom menu možnosť **Všetky aplikácie** a pridajú sa všetky aplikácie.

> Niektoré operácie určitých pravidiel preddefinovaných modulom HIPS nemôžu byť blokované a sú predvolene povolené. Navyše, nie všetky systémové operácie sú monitorované modulom HIPS. Modul HIPS monitoruje operácie, ktoré možno považovať za nebezpečné.

Popis niektorých dôležitých aplikácií:

Súborové operácie

Vymazať súbor	Aplikácia žiada o povolenie zmazať cieľový súbor.
Zapísať do súboru	Aplikácia žiada o povolenie zapisovať do cieľového súboru.
Priamy prístup na disk	Aplikácia sa snaží čítať z disku alebo naň zapisovať neštandardným spôsobom, ktorý obchádza štandardné procedúry systému Windows. Výsledkom môže byť zmena súboru bez aplikácie príslušného pravidla. Táto operácia môže byť spôsobená škodlivým kódom, ktorý sa snaží vyhnúť detekcii, ďalej zálohovacím programom, ktorý kopíruje celý obsah pevného disku, alebo správcom oblastí disku, ktorý reorganizuje diskové zväzky.
Nainštalovať globálny hook	Ide o volanie funkcie SetWindowsHookEx z knižnice MSDN.

Vymazať súbor	Aplikácia žiada o povolenie zmazať cieľový súbor.
Načítať ovládač	Inštalácia a načítanie ovládačov v systéme.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické súbory** a kliknutím na **Pridať** pridajte nové súbory alebo priečinky. Prípadne môžete v roletovom menu vybrať možnosť **Všetky súbory** a pridať tak všetky aplikácie.

Operácie s aplikáciou

Ladiť inú aplikáciu	Pripojí ladiaci nástroj (debugger) k procesu. Pri ladení aplikácie je možné pozorovať alebo meniť jej správanie. Tiež je možné pristupovať k jej dátam.
Zachytávať udalosti inej aplikácie	Zdrojová aplikácia sa pokúša zachytiť udalosti cieľovej aplikácie (napríklad, ak sa keylogger snaží zachytiť aktivitu webového prehliadača).
Ukončiť/pozastaviť inú aplikáciu	Pozastavenie, obnovenie alebo ukončenie procesu (môže byť vyvolané priamo z nástroja Process Explorer alebo z okna Procesy).
Spustiť novú aplikáciu	Spúšťanie nových aplikácií alebo procesov.
Zmeniť stav inej aplikácie	Zdrojová aplikácia sa pokúša zapisovať do pamäte cieľovej aplikácie, prípadne sa snaží spustiť kód v jej mene. Táto funkcia je užitočná na ochranu dôležitej aplikácie, ak ju nastavíte ako cieľovú aplikáciu pri pravidle, ktoré blokuje tieto operácie.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické aplikácie** a kliknutím na **Pridať** pridajte jednotlivé súbory alebo priečinky konkrétnej aplikácie. Prípadne môžete v roletovom menu vybrať možnosť **Všetky aplikácie** a pridať tak všetky aplikácie.

Operácie s databázou Registry

Zmena nastavení spustenia	Ide o akékoľvek zmeny v nastaveniach definujúcich, ktoré aplikácie budú spúšťané pri štarte operačného systému Windows. Môžu byť vyhľadané napríklad pri zadaní kľúča Run do vyhľadávania v databáze Registry systému Windows.
Vymazanie z databázy Registry	Zmazanie kľúča alebo hodnoty v danom kľúči.
Premenovanie kľúča databázy Registry	Premenovanie konkrétneho kľúča.
Úprava v databáze Registry	Vytváranie nových hodnôt kľúčov alebo zmena dát asociovaných s hodnotou, zmena umiestnenia dát v rámci stromu databázy a nastavovanie používateľských alebo skupinových práv daného kľúča.

Pravidlo sa uplatní, len ak sa operácia týka tohto cieľa. V roletovom menu vyberte možnosť **Špecifické položky** a kliknutím na **Pridať** pridajte nové súbory alebo priečinky. Prípadne môžete v roletovom menu vybrať možnosť **Všetky položky** a pridať tak všetky aplikácie.

Pri zadávaní cieľa je povolené používať zástupné znaky s istými obmedzeniami. Pri cestách k databáze Registry sa dá namiesto konkrétneho kľúča v ceste použiť symbol hviezdičky (*) vo význame „ľubovoľný jeden kľúč“. Napríklad *HKEY_USERS*\software can mean HKEY_USER\.default\software* nepredstavuje *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** je nesprávne uvedená cesta kľúča databázy Registry. Cesta kľúča databázy Registry obsahujúca *** má špeciálny význam, znamená „tento kľúč alebo ľubovoľný podkľúč ľubovoľne hlboko“. Pri súborových cieľoch sa dajú používať zástupné znaky len týmto spôsobom. Pri vyhodnocovaní platí, že vždy sa hľadá najprv cieľ, ktorý popisuje danú cestu presne, až potom cieľ, ktorý ju popisuje s hviezdičkou (*).

Pri vytvorení príliš všeobecného pravidla sa môže zobraziť upozornenie.

Rozšírené nastavenia HIPS

Nasledujúce možnosti sú užitočné pre ladenie (debugging) a analýzu správania aplikácií.

Ovládače s povolením vždy sa načítať

Vybrané ovládače majú vždy povolenie sa načítať bez ohľadu na filtrovací režim, okrem prípadu, kedy sú zablokované používateľským pravidlom. Ovládače v tomto zozname majú vždy povolené načítanie bez ohľadu na zvolený HIPS režim filtrovania, pokiaľ nie sú blokované konkrétnym používateľským pravidlom. Môžete **Pridať** nový ovládač, prípadne **Upraviť** alebo **Odstrániť** zvolený ovládač zo zoznamu.

Kliknite na **Obnoviť** pre odstránenie ovládačov pridaných používateľom. Táto možnosť je užitočná, ak ste pridali väčšie množstvo ovládačov a nie je možné ich zmazať zo zoznamu.

Zapisovať všetky zablokované operácie do protokolu

Všetky zablokované operácie sa zapíšu do HIPS protokolu.

Upozorniť na zmeny v zozname aplikácií automaticky spúšťaných pri štarte

Ak pribudne alebo ubudne aplikácia zo zoznamu aplikácií spúšťaných po štarte, zobrazí sa upozornenie.

Nastavenia aktualizácie

Nastavenie aktualizácie pozostáva zo špecifikácie zdroja aktualizácie, teda z nastavenia aktualizačných serverov a autentifikácie voči týmto serverom.

Pre bezproblémové fungovanie aktualizácie je nevyhnutné mať všetky parametre nastavené správne. Ak používate firewall, treba zaistiť, aby mal program povolenú komunikáciu cez internet (napríklad HTTP komunikáciu).

Základné

Vybrať predvolený aktualizačný profil
Vyberte si z existujúcich profilov alebo vytvorte nový profil, ktorý sa bude predvolene vzťahovať na aktualizácie.
Vyčistiť aktualizačnú vyrovnávaciu pamäť
Ak máte problém s aktualizáciami, kliknite na tlačidlo **Vyčistiť** pre zmazanie obsahu adresára s dočasnými aktualizačnými súbormi.
Aktualizácie produktu/Automatické aktualizácie
Táto možnosť je v predvolených nastaveniach zapnutá. Prepínacie tlačidlo môžete použiť na dočasné vypnutie automatických aktualizácií produktu ESET Mail Security. Túto možnosť však odporúčame nechať zapnutú, aby si produkt ESET Mail Security mohol inštalovať aktualizácie programových súčastí (PCU) a mikroaktualizácie programových súčastí (µPCU) vo chvíli, keď budú dostupné.

Aktualizácie sa aplikujú po najbližšom reštarte servera.

Upozornenia na neaktuálne detekčné jadro

Automaticky nastaviť maximálny vek detekčného jadra / Maximálny vek detekčného jadra (v dňoch)
Pomocou prepínacieho tlačidla môžete vypnúť automatické nastavenie maximálneho veku detekčného jadra a následne manuálne nastaviť vlastný maximálny počet dní, po uplynutí ktorých bude detekčné jadro považované za neaktuálne a zobrazí sa upozornenie. Predvolená hodnota je 7.
Vrátenie zmien modulov
Ak máte podozrenie, že nová aktualizácia detekčného jadra alebo programových súčastí môže byť nestabilná alebo poškodená, môžete vrátiť detekčné jadro do predchádzajúceho stavu a zakázať aktualizácie na určený časový interval. Prípadne môžete povoliť predtým zakázané aktualizácie. ESET Mail Security poskytuje zálohu a obnovu detekčného jadra a programových súčastí (tzv. rollback). Na vytvorenie snímok detekčného jadra ponechajte povolenú možnosť Vytvárať snímky modulov.
Počet záložných snímok
Určuje, koľko predošlých snímok modulov má program lokálne ukladať do zálohy.
Vrátenie na predošlé moduly
Kliknutím na možnosť Vrátenie zmien vrátite programové moduly na predchádzajúcu verziu a dočasne zakážete ich aktualizáciu.

Profily
Vytvoriť si vlastný aktualizačný profil je možné prostredníctvom tlačidla **Upraviť** vedľa položky **Zoznam profilov**. Zadajte **Názov profilu** a kliknite na **Pridať**. V roletovom menu Vyberte profil na úpravu zvoľte príslušný profil a upravte parametre pre typy aktualizácie modulov alebo použite možnosť **Aktualizačný mirror**.

Aktualizácie

Z roletového menu vyberte typ aktualizácie, ktorý bude použitý:
• **Priebežné aktualizácie** – predvolene je ako typ aktualizácie nastavená priebežná aktualizácia, ktorá zabezpečuje priebežné sťahovanie aktualizácií zo serverov spoločnosti ESET tak, aby pritom čo najmenej zaťažovala sieť.
• **Predbežné aktualizácie** – aktualizácie, ktoré prešli dôkladným interným testovacím procesom a čoskoro budú dostupné pre verejnosť. Výhodou povolenia predbežných aktualizácií je možnosť prístupu k najnovším metódam detekcie a rôznym opravám. Treba však mať na pamäti, že predbežné aktualizácie nemusia byť vždy dostatočne stabilné a v žiadnom prípade by NEMALI byť používané na serveroch výroby a pracovných staniciach, kde sa vyžaduje maximálna stabilita a dostupnosť.
• **Oneskorené aktualizácie** – umožňuje aktualizovanie zo špeciálnych aktualizačných serverov poskytujúcich nové verzie vírusových databáz s oneskorením aspoň X hodín (tzn. databázy testované v reálnom prostredí a teda považované za stabilné).

Zapnúť optimalizáciu doručovania aktualizácií
Ak je táto možnosť povolená, aktualizačné súbory je možné sťahovať z CDN (sieť na doručovanie obsahu). Vypnutie tohto nastavenia môže spôsobiť prerušenie a spomalenie pri sťahovaní v prípade, že sú vyhradené aktualizačné servery ESET preťažené. Vypnutie je užitočné, ak je firewall nastavený na prístup výhradne k IP adresám aktualizačného servera ESET alebo ak pripojenie k CDN službám nefunguje.

Upozorniť pred sťahovaním aktualizácií
V prípade dostupnosti aktualizácie sa miesto automatického stiahnutia zobrazí okno s potvrdením.

Upozorniť, ak veľkosť aktualizácie presiahne (kB)
V prípade, že aktualizačný súbor prekročí definovanú veľkosť, zobrazí sa upozornenie.

Aktualizácie modulov
Pre aktualizácie modulov je predvolene nastavená možnosť **Automatický výber servera**. Aktualizačný server je umiestnenie, v ktorom sú uložené aktualizácie. Ak pre aktualizáciu používate servery spoločnosti ESET, odporúčame ponechať predvolené nastavenia.

Ak používate mirror ako lokálny HTTP server, zadajte aktualizačný server v tomto formáte: http://computer_name_or_its_IP_address:2221
Ak používate mirror ako lokálny HTTP server s SSL, zadajte aktualizačný server v tomto formáte: https://computer_name_or_its_IP_address:2221
Ak používate mirror ako zdieľaný sieťový súbor, zadajte aktualizačný server v tomto formáte: \\computer_name_or_its_IP_address\shared_folder

Povoliť častejšie aktualizácie detekčných vzoriek
Detekčné jadro bude aktualizované v kratších intervaloch. Vypnutie tohto nastavenia môže mať negatívny dopad na účinnosť detekcie.

Povoliť aktualizáciu modulov z vymeniteľných médií
Táto funkcia vám umožňuje vykonávať aktualizáciu z vymeniteľného média za predpokladu, že dané médium obsahuje vytvorený mirror. Ak je zvolená **automatická** aktualizácia, aktualizácia bude prebiehať na pozadí. Ak chcete, aby sa zobrazovali aktualizačné okná, označte možnosť **Vždy sa spýtať**.

Aktualizácie produktu
Pozastavenie automatických aktualizácií pre konkrétne aktualizačné profily dočasne vypne funkciu automatickej aktualizácie produktu pri pripojení na internet prostredníctvom iných sietí alebo pripojenia účtovaného podľa objemu údajov. Ak chcete mať neustály prístup k najnovším funkciám a najvyššej úrovni ochrany, ponechajte toto nastavenie zapnuté.

V niektorých prípadoch môže byť po vykonaní aktualizácie potrebný reštart servera.

Možnosti pripojenia

Proxy server

Pre prístup k nastaveniam proxy servera pre daný aktualizačný profil kliknite na Režim proxy a vyberte jednu z troch nasledujúcich možností:

- **Nepoužívať proxy server** – ESET Mail Security pri aktualizácii nepoužije žiadny proxy server.
- **Použiť globálne nastavenie proxy servera** – budú použité globálne nastavenia proxy servera, ktoré sú už definované v Rozšírených nastaveniach (F5) v sekcii Nástroje > Proxy server.
- **Pripojenie prostredníctvom proxy servera** – túto možnosť použite v nasledujúcich prípadoch:

Na aktualizáciu ESET Mail Security je potrebné použiť proxy server, ktorý je odlišný od proxy servera zadaného v globálnych nastaveniach (Nástroje > Proxy server). V takomto prípade je však potrebné definovať nasledujúce nastavenia: adresa Proxy servera, komunikačný Port (predvolene 3128) a v prípade potreby aj Prihlasovacie meno a Heslo pre proxy server.

Proxy server používaný pri aktualizácii ESET Mail Security je iný než globálne nastavený proxy server.

Váš počítač je pripojený na internet cez proxy server. Nastavenia sú prevzaté z prehliadača Internet Explorer počas inštalácie programu, no ak dôjde po čase k zmene v nastaveniach proxy servera (napríklad v dôsledku zmeny sprostredkovateľa internetového pripojenia – ISP), bude potrebné skontrolovať nastavenia HTTP Proxy v tejto sekcii. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií z aktualizačných serverov.

Overovacie údaje, ako **Prihlasovacie meno** a **Heslo**, sú určené pre prístup k proxy serveru. Príslušné polia vyplňte len v prípade, že sa tieto údaje vyžadujú. Berte na vedomie, že tieto polia nie sú určené pre vaše prihlasovacie meno a heslo pre ESET Mail Security a mali by byť vyplnené len v prípade, ak je na pripojenie na internet cez proxy server potrebné heslo.

Použiť priame pripojenie, ak nie je dostupný proxy server

Ak je produkt nakonfigurovaný tak, aby používal HTTP Proxy a proxy nie je k dispozícii, produkt obíde proxy a bude komunikovať priamo so servermi spoločnosti ESET.

Zdieľané lokality systému Windows

Pri aktualizácii z lokálneho servera s operačným systémom Windows sa na vytvorenie spojenia štandardne vyžaduje overenie.

Pre pripojenie do LAN vystupovať ako

Pre nastavenie svojho účtu vyberte jednu z nasledujúcich možností:

- **Systémový účet (predvolený)** – na účely overenia použite systémový účet. Za normálnych okolností overenie nebude vykonané, ak nie sú nastavené overovacie údaje v hlavných nastaveniach aktualizácie.
- **Aktuálne prihlásený používateľ** – ak sa použije táto možnosť, program sa bude overovať pod účtom aktuálne prihláseného používateľa. Nevýhodou v prípade tohto nastavenia je absencia možnosti pripojenia na server a následnej aktualizácie, ak nie je na počítači prihlásený žiadny používateľ.
- **Určený používateľ** – táto možnosť umožňuje vybrať na účely overenia konkrétneho používateľa. Túto možnosť odporúčame v prípade, že zlyhá spojenie pod lokálnym systémovým účtom. Je však potrebné dbať na to, aby mal určený používateľský účet práva na prístup k adresáru s aktualizačnými súbormi, ktorý sa nachádza na lokálnom serveri. V opačnom prípade sa spojenie nepodarí vytvoriť a aktualizácia nebude stiahnutá.

Pri použití možností **Aktuálne prihlásený používateľ** a **Určený používateľ** môže nastať chyba pri zmene identity programu na požadovaného používateľa. Z toho dôvodu odporúčame pri pripojení do LAN nastaviť overovacie údaje v hlavných nastaveniach aktualizácie. V týchto nastaveniach je potrebné uviesť údaje v nasledujúcom tvare: domain_name\user (v prípade pracovnej skupiny je to workgroup_name\name) a heslo. Pri aktualizácii cez HTTP nie je štandardne potrebné zadávať overovacie údaje.

Po dokončení aktualizácie odpojiť zo servera

Táto možnosť slúži na zrušenie spojenia so serverom a môže byť použitá v prípade, keď po stiahnutí aktualizácie ostáva spojenie nadalej aktívne.

Aktualizačný mirror

Možnosti konfigurácie pre lokálny mirror server sa nachádzajú v strome **Rozšírených nastavení** (F5) v časti **Aktualizácia** > **Profily** > karta Aktualizačný mirror.

Vrátenie zmien aktualizácií

Ak kliknete na **Vrátenie zmien**, bude potrebné vybrať čas z roletového menu Časový interval, ktorý určuje, na ako dlho budú aktualizácie detekčného jadra a programových súčastí zastavené.

Ak si želáte neskôr manuálne zapnúť pravidelné aktualizácie, vyberte možnosť **Do odvolania**. Pretože táto možnosť predstavuje potenciálne bezpečnostné riziko, označenie tejto možnosti neodporúčame.

Detekčné jadro je znížené na verziu, ktorá je uložená na disku počítača ako obraz a je najstaršia.

Naplánovaná úloha – Aktualizácia

Nastavenie hlavného a alternatívneho aktualizačného profilu umožňuje vykonávať aktualizáciu z dvoch serverov. Alternatívny profil bude použitý v prípade, že z prvého sa aktualizáciu nepodarí vykonať. Túto možnosť je možné využiť napríklad pre notebooky, ktoré sú používané v lokálnej LAN sieti a zároveň aj v iných sieťach s pripojením na internet. V prípade neúspešnej aktualizácie z hlavného profilu s nastavením na lokálnu LAN bude aktualizácia vykonaná z alternatívneho profilu, ktorý bude nastavený pre aktualizáciu priamo zo serverov spoločnosti ESET.

Nižšie spomenutý postup vám pomôže pri upravovaní úlohy určenej na zmenu **pravidelnej automatickej aktualizácie**.
1. V hlavnom okne **Plánovača** vyberte úlohu **Aktualizácia** s názvom **Pravidelná automatická aktualizácia** a kliknite na **Upraviť**, čím sa otvorí sprievodca nastavením.
2. Vyberte naplánovanú úlohu a jednu z možností načasovania podľa toho, kedy chcete danú úlohu spustiť
3. Ak chcete zabrániť tomu, aby sa úloha vykonala, ak je systém napájaný z batérie (napr. UPS), kliknite na tlačidlo vedľa možnosti **Nespúšťať úlohu, ak je počítač napájaný z batérie**.
4. Vyberte aktualizačný profil, ktorý bude použitý pri aktualizácii. Vyberte akciu, ktorá bude vykonaná v prípade zlyhania úlohy.
5. Kliknite na **Dokončiť** pre dokončenie nastavenia úlohy.

Aktualizačný mirror

ESET Mail Security umožňuje vytváranie kópie aktualizácie, z ktorej sa môžu aktualizovať ďalšie stanice nachádzajúce sa v sieti. Použitie funkcie „mirror“ – vytváranie kópie aktualizačných súborov na lokálnej sieti je výhodné použiť hlavne pri väčších sieťach, kde by množstvo dát pri aktualizovaní každého počítača cez internet spôsobovalo veľký prenos a vyťaženie kapacít liniek. Preto sa odporúča aktualizovať len jeden objekt v sieti priamo z aktualizačných serverov cez internet a následne aktualizáciu sprístupniť pomocou mirror servera ostatným objektom v lokálnej sieti. Aktualizáciou klientskych pracovných staníc z mirroru sa zabezpečí rozloženie zaťaženia siete a tiež zníženie prenosu dát.

Aktualizačný mirror

Vytvárať kópie aktualizácií
Sprístupnia sa nastavenia mirroru.
Úložný priečinok
Kliknite na **Odstrániť**, ak chcete zmeniť prednastavený priečinok na ukladanie aktualizačných súborov C:\ProgramData\ESET\ESET Security\mirror. Ak chcete vyhľadať priečinok na lokálnom počítači alebo chcete vyhľadať zdieľaný sieťový priečinok, kliknite na **Upraviť**. V prípade, že sa na prístup k priečinku vyžaduje overenie, je potrebné do príslušných polí zadať Prihlasovacie meno a Heslo. Ak je zvolený priečinok umiestnený na sieťovom disku spustenom pod operačným systémom Windows NT/2000/XP, je potrebné zadať prihlasovacie meno a heslo používateľa s oprávnením na zápis do zvoleného priečinka.
Meno používateľa zadávajte vo formáte Domain/User alebo Workgroup/User. Zároveň je potrebné zadať príslušné heslá.

Aktualizácia programových súčastí

Súbory
Pri nastavovaní mirroru môžete špecifikovať jazykové verzie aktualizácií, ktoré budú stiahnuté. Jazyk musí byť podporovaný mirror serverom nastaveným používateľom.
Automaticky aktualizovať programové súčasti
Povolí inštaláciu nových a aktualizáciu existujúcich programových súčastí. Aktualizácia môže prebiehať automaticky bez zásahu používateľa alebo s informovaním a výzvou na jej potvrdenie od používateľa. Aktualizácia samotného produktu si zvyčajne vyžaduje reštart počítača.
Aktualizovať programové súčasti
Aktualizuje programové súčasti na najnovšiu verziu.

HTTP server

Port servera
V rámci predvolených nastavení je port servera preddefinovaný na 2221. Ak používate iný port, zmeňte túto hodnotu.
Overenie
Zvoľte metódu overenia, ktorá bude použitá na prístup k aktualizačným súborom. Na výber sú tieto možnosti: **Žiadna**, **Základná** a **NTLM**.
• Zvolením možnosti **Základná** zabezpečíte, že prihlasovacie meno a heslo bude šifrované jednoduchou metódou kódovania base64.
• Možnosť **NTLM** zabezpečí kódovanie prostredníctvom bezpečnej metódy kódovania. Pri overovaní sa používajú používatelia vytvorení na stanici zdieľajúcej aktualizáciu.
• Prednastavená je možnosť **Žiadna**, ktorá sprístupňuje aktualizačné súbory bez potreby overenia.

Pri sprístupnení aktualizačných súborov prostredníctvom HTTP servera musí byť mirror priečinok umiestnený na rovnakom počítači ako ESET Mail Security, ktorý mirror vytvára.

SSL pre HTTP server
Ak chcete prevádzkovať HTTP server s podporou HTTPS (SSL), pripojte **súbor obsahujúci reťazec certifikátov** alebo vygenerujte certifikát s vlastným podpisom. Sú dostupné tieto typy certifikátov: PEM, PFX a ASN. Pre dodatočné zabezpečenie môžete použiť na sťahovanie súborov protokol HTTPS. Pri použití tohoto protokolu je takmer nemožné vystopovať prihlasovacie údaje a inú komunikáciu na sieti.
Typ súkromného kľúča je predvolene nastavený ako **Integrovaný** (preto nie je dostupná možnosť Súbor obsahujúci súkromný kľúč). To znamená, že súkromný kľúč je súčasťou zvoleného reťazca certifikátov.

Možnosti pripojenia

Zdieľané lokality systému Windows
Pri aktualizácii z lokálneho servera s operačným systémom Windows sa na vytvorenie spojenia štandardne vyžaduje overenie.
Pre pripojenie do LAN vystupovať ako
Pre nastavenie svojho účtu vyberte jednu z nasledujúcich možností:
• **Systémový účet** (predvolené) – na účely overenia použite systémový účet. Za normálnych okolností overenie nebude vykonané, ak nie sú nastavené overovacie údaje v hlavných nastaveniach aktualizácie.
• **Aktuálne prihlásený používateľ** – ak sa použije táto možnosť, program sa bude overovať pod účtom aktuálne prihláseného používateľa. Nevýhodou v prípade tohto nastavenia je absencia možnosti pripojenia na server a následnej aktualizácie, ak nie je na počítači prihlásený žiadny používateľ.
• **Určený používateľ** – táto možnosť umožňuje vybrať na účely overenia konkrétneho používateľa. Túto možnosť odporúčame v prípade, že zlyhá spojenie pod lokálnym systémovým účtom. Je však potrebné dbať na to, aby mal určený používateľský účet práva na prístup k adresáru s aktualizačnými súbormi, ktorý sa nachádza na lokálnom serveri. V opačnom prípade sa spojenie nepodarí vytvoriť a aktualizácia nebude stiahnutá.

⚠ Pri použití možností **Aktuálne prihlásený používateľ** a **Určený používateľ** môže nastať chyba pri zmene identity programu na požadovaného používateľa. Z toho dôvodu odporúčame pri pripojení do LAN nastaviť overovacie údaje v hlavných nastaveniach aktualizácie. V týchto nastaveniach je potrebné uviesť údaje v nasledujúcom tvare: *domain_name**user* (v prípade pracovnej skupiny je to *workgroup_name**name*) a heslo. Pri aktualizácii cez HTTP nie je štandardne potrebné zadávať overovacie údaje.

Po dokončení aktualizácie odpojiť zo servera
Táto možnosť slúži na zrušenie spojenia so serverom a môže byť použitá v prípade, keď po stiahnutí aktualizácie ostáva spojenie naďalej aktívne.

Ochrana siete

Ak chcete spravovať ochranu siete, kliknite na Upraviť a následne si vytvorte novú alebo upravte už existujúce:

• Známe siete – zoznam známych sietí môžete konfigurovať manuálne v Rozšírených nastaveniach v sekcii Ochrana siete > Základné > Známe siete > Upraviť

• Zóny – zoznam zón môžete konfigurovať manuálne v Rozšírených nastaveniach v sekcii Ochrana siete > Základné > Zóny > Upraviť

Známe siete

Ak počítač často pripájate k verejným sieťam alebo sieťam mimo vašej bežnej pracovnej siete, odporúčame vám overovať dôveryhodnosť nových sietí, ku ktorým sa pripájate. Po zadefinovaní sietí dokáže ESET Mail Security rozpoznávať dôveryhodné (domáce/pracovné) siete na základe rôznych sieťových parametrov nastavených v časti Identifikácia siete.

Počítače sa často pripájajú do sietí s IP adresami podobnými dôveryhodnej sieti. V takých prípadoch môže ESET Mail Security označiť neznámu sieť ako dôveryhodnú (domácu alebo pracovnú). Aby ste takéto prípady eliminovali, odporúčame vám používať Overenie siete.

Keď sa sieťový adaptér počítača pripojí na sieť alebo dôjde k zmene sieťových nastavení, ESET Mail Security sa pokúsi v zozname známych sietí vyhľadať záznam zodpovedajúci novej sieti. V prípade, že Identifikácia siete a Overenie siete (nepovinné) budú vyhovovať záznamu, sieť bude označená ako pripojená.

Ak nebola nájdená žiadna zhoda so známou sieťou, vytvorí sa nové sieťové pripojenie na základe zistenej konfigurácie siete, aby bolo možné sieť identifikovať, keď sa na ňu znova pripojíte. Pre nové siete sa predvolene použije typ ochrany Verejná sieť.

Zobrazí sa dialógové okno s oznámením Zistené pripojenie do novej siete, v ktorom budete mať možnosť zvoliť pre sieť jeden z nasledujúcich typov ochrany: Verejná sieť, Domáca alebo pracovná sieť a Použiť nastavenia Windows. Ak sa sieťový adaptér pripojí na známu sieť, ktorá je označená ako Domáca alebo pracovná, budú do dôveryhodnej zóny automaticky pridané lokálne podsiete.

Typ ochrany nových sietí

Vyberte niektorú z nasledujúcich možností: **Použiť nastavenia Windows**, **Spýtať sa používateľa** alebo **Označiť ako verejné**, ktorá bude predvolene použitá pre nové siete. Ak zvolíte možnosť **Použiť nastavenia Windows**, dialógové okno na výber typu siete sa nezobrazí a sieť, ku ktorej ste pripojený, bude automaticky označená podľa vašich nastavení Windows. V dôsledku toho budú niektoré funkcie (napr. zdieľanie súborov a vzdialená plocha) dostupné z nových sietí.

Nastavenia známych sietí sú dostupné v okne Editor známych sietí.

Pridať sieť

Nastavenie siete je rozložené do nasledujúcich záložiek:

Sieť

V tejto sekcii môžete zadať **Názov siete** a vybrať **Typ ochrany** pre danú sieť. Adresy, ktoré pridáte do **Dodatočných dôveryhodných adries**, budú vždy pridané do dôveryhodnej zóny adaptéra pripojeného do tejto siete (bez ohľadu na typ ochrany siete).

- Upozorniť na slabé šifrovanie siete Wi-Fi – ESET Mail Security vás upozorní na možné bezpečnostné riziko, ak sa pripojíte do nezabezpečenej alebo slabo zabezpečenej bezdrôtovej siete.
- Profil firewallu sa prevezme zo sieťového adaptéra.
- Aktualizačný profil – vyberte aktualizačný profil, ktorý sa použije pri pripojení k danej sieti.

Identifikácia siete

Prebieha na základe parametrov lokálneho sieťového adaptéra. Všetky nastavené parametre sú porovnávané so skutočnými parametrami aktívneho sieťového pripojenia. Podporované sú IPv4 aj IPv6 adresy.

Overenie siete

V sieti sa vyhľadá špecifický server a na overenie sa použije asymetrické šifrovanie (RSA). Názov siete, ktorá je overovaná, musí byť zhodný s názvom zóny nastaveným v nastaveniach autentifikačného servera. Názov rozlišuje veľké a malé písmená. Zadajte názov servera, port, na ktorom server počúva, a verejný kľúč zodpovedajúci súkromnému kľúču servera. Za názvom servera vo forme IP adresy, DNS alebo NetBios názvu môže nasledovať cesta upresňujúca umiestnenie kľúča na serveri (napr. *server_name_/directory1/directory2/authentication*). Môžete zadať alternatívne servery oddelené bodkočiarkou.

Verejný kľúč môže byť naimportovaný pomocou nasledujúcich typov súborov:

- PEM šifrovaný verejný kľúč (.pem) – tento typ kľúča je možné vygenerovať prostredníctvom ESET Authentication Servera.
- Šifrovaný verejný kľúč

- Verejný kľúč certifikátu (.crt)

Kliknutím na **Testovať** overte nastavenia. Ak bola autentifikácia úspešná, objaví sa oznámenie Overenie so serverom bolo úspešné. Ak nie je autentifikácia nastavená správne, zobrazí sa jedno z nasledujúcich chybových hlásení:

Overenie so serverom nebolo úspešné. Neplatný alebo nezhodujúci sa podpis.	**Podpis servera sa nezhoduje so zadaným verejným kľúčom.**
Overenie so serverom nebolo úspešné. Názov siete sa nezhoduje.	Túto možnosť je vhodné deaktivovať v prípade, ak si želáte ponechať dané pravidlo v zozname pravidiel, avšak nechcete ho používať.
Overenie so serverom nebolo úspešné. Neplatná alebo žiadna odpoveď zo servera.	Nie je prijatá žiadna odpoveď zo servera, server nie je spustený alebo je nedostupný. Neplatná odpoveď môže byť spôsobená iným HTTP serverom spusteným na nastavenej adrese.
Zadaný verejný kľúč je neplatný.	Uistite sa, že zadaný súbor verejného kľúča nie je poškodený.

Zóny

Zóna predstavuje zoskupenie sieťových adries, ktoré spolu tvoria jednu logickú skupinu IP adries. Zóny sú užitočné, ak potrebujete použiť rovnakú skupinu IP adries vo viacerých pravidlách. Na každú adresu danej skupiny sa následne aplikujú rovnaké pravidlá definované spoločne pre celú skupinu. Príkladom takejto skupiny je napríklad Dôveryhodná zóna. Dôveryhodná zóna predstavuje skupinu sieťových adries bez akéhokoľvek blokovania firewallom.

Kliknite na tlačidlo **Pridať**, zadajte **Názov** a **Popis** novej zóny a do poľa Vzdialená adresa počítača (IPv4, Ipv6, rozsah, maska) zadajte vzdialenú IP adresu.

Ochrana pred sieťovými útokmi

Zapnúť ochranu pred sieťovými útokmi (IDS)

Umožňuje vám nastaviť prístup k niektorým službám bežiacim na vašom počítači z dôveryhodnej zóny a zapnúť alebo vypnúť detekciu viacerých typov útokov a zneužití, ktoré môžu poškodiť váš počítač.

Zapnúť ochranu pred botnetmi

Odhaľuje a blokuje komunikáciu spojenú s nebezpečnými riadiacimi C&C servermi rozpoznávaním charakteristík, ktoré naznačujú, že počítač je infikovaný a bot sa snaží komunikovať s riadiacim serverom.

IDS výnimky

IDS výnimky si môžete predstaviť ako pravidlá ochrany siete. Kliknutím na Upraviť ich môžete definovať.

> V prípade prostredia s vysokovýkonnou sieťou (10GbE a viac) si prečítajte náš článok Databázy znalostí venovaný výkonu siete pri používaní ESET Mail Security.

Ochrana pred útokmi hrubou silou

ESET Mail Security kontroluje obsah sieťovej komunikácie a blokuje pokusy o uhádnutie hesiel.

Pokročilé možnosti

Nastavte pokročilé možnosti filtrovania pre lepšiu detekciu rôznych typov útokov a zraniteľností, ktoré môžu ohroziť váš počítač.

Detekcia útokov:

Protokol SMB – odhaľuje a blokuje rôzne zraniteľnosti v SMB protokole.
Protokol RPC – odhaľuje a blokuje rôzne zraniteľnosti (CVE) v RPC protokole, ktorý bol navrhnutý pre Distributed Computing Environment (DCE).
Protokol RDP – odhaľuje a blokuje rôzne zraniteľnosti (CVE) v RDP protokole (pozri popis vyššie v tejto kapitole).
Blokovať nebezpečnú adresu po detekcii útoku – IP adresy, ktoré boli zachytené ako zdroj útokov, sú pridané na blacklist a komunikácia z nich bude na určitý čas blokovaná.
Zobraziť oznámenie po detekcii útoku – pri zachytení útoku program zobrazí upozornenie v oblasti oznámení systému Windows v pravom dolnom rohu obrazovky.
Zobraziť upozornenie pri pokusoch o zneužitie bezpečnostných dier – program zobrazí upozornenie, ak bude zachytený útok na bezpečnostné diery alebo pokus o preniknutie do systému týmto spôsobom.

Kontrola paketov:

Povoliť prichádzajúce spojenie k správcovským zdieľaným položkám cez SMB protokol – správcovské zdieľané položky (admin shares) sú predvolené zdieľané položky na sieti, ktoré zdieľajú oddiely pevného disku (C$, D$ atď.) spolu so systémovým priečinkom (ADMIN$) Zakázanie prístupu k správcovským zdieľaným položkám výrazne znižuje bezpečnostné riziká. Napríklad červ Conficker vykonáva slovníkové (dictionary) útoky v snahe získať prístup k týmto položkám.
Zakázať staré (nepodporované) SMB dialekty – zakáže SMB reláciu so starým dialektom SMB, ktorý nepodporuje IDS. Najnovšie operačné systémy Windows podporujú staré dialekty SMB kvôli spätnej kompatibilite so staršími operačnými systémami, ako napríklad Windows 95. Útočník môže použiť starší dialekt SMB s úmyslom vyhnúť sa kontrole packetov. Zakážte staré SMB dialekty, ak váš počítač nepotrebuje zdieľať súbory so staršími verziami operačného systému Windows.
Zakázať relácie SMB bez bezpečnostných rozšírení – bezpečnostné rozšírenia môžu byť použité počas nadväzovania relácie SMB na zaistenie bezpečnejšieho mechanizmu autentifikácie než v prípade LAN Manager Challenge/Response (LM). Schéma LM je považovaná za slabú a neodporúča sa ju používať.
Povoliť komunikáciu so službou Správca zabezpečenia kont – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SAMR].
Povoliť komunikáciu so službou Lokálna autorita zabezpečenia – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-LSAD] a [MS-LSAT].
Povoliť komunikáciu so službou Vzdialená databáza Registry – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-RRP].
Povoliť komunikáciu so službou Správca riadenia služieb – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SCMR].
Povoliť komunikáciu so službou Server – viac informácií o tejto službe nájdete v databáze znalostí spoločnosti Microsoft [MS-SRVS].
Povoliť komunikáciu s ostatnými službami – ostatné služby MSRPC.

IDS výnimky

IDS (Intrusion Detection System) výnimky sú v podstate pravidlá ochrany siete. Jednotlivé výnimky sú vyhodnocované smerom zhora nadol. Editor IDS výnimiek vám umožňuje prispôsobiť správanie ochrany siete podľa rôznych IDS výnimiek. Aplikuje sa prvá zhodná výnimka, a to osobitne pre každý typ akcie (Blokovať,

Oznámiť, Zapísať do protokolu). Pomocou tlačidiel **Začiatok**/**Hore**/**Dole**/**Koniec** môžete upraviť prioritu výnimiek. Pre vytvorenie novej IDS výnimky kliknite na **Pridať**. Kliknutím na **Upraviť** môžete zmeniť existujúcu IDS výnimku a kliknutím na **Odstrániť** môžete výnimku odstrániť.

Z roletového menu vyberte typ **Upozornenia**. Zadajte **Názov hrozby** a vyberte **Smer**. Vyhľadajte **Aplikáciu**, pre ktorú chcete vytvoriť výnimku. Zadajte zoznam IP adries (IPv4 alebo IPv6) alebo podsietí. Ak zadávate viacero položiek, použite ako oddeľovač čiarku.

Nastavte **Akciu** pre IDS výnimku výberom jednej z možností nachádzajúcich sa v roletovom menu (**Predvolená**, **Áno**, **Nie**). Tento postup zopakujte pre každý typ akcie (**Blokovať**, **Oznámiť**, **Zapísať do protokolu**).

Ak chcete, aby sa zobrazilo oznámenie v prípade, že dôjde k výskytu IDS výnimky, a zároveň chcete, aby bol do protokolu zapísaný čas výskytu danej udalosti, ponechajte pre typ akcie **Blokovať** aktívnu možnosť **Predvolené hodnoty** a pre ostatné dva typy akcie (**Oznámiť** a **Zapísať do protokolu**) vyberte z roletového menu možnosť **Áno**.

Zablokovaná podozrivá hrozba

Táto situácia môže nastať v prípade, ak sa niektorá aplikácia na vašom počítači pokúša neštandardne komunikovať s iným počítačom v sieti, zneužiť bezpečnostnú dieru alebo sa niekto pokúša skenovať porty vo vašej sieti.

- Hrozba – názov hrozby.
- Zdroj – zdrojová sieťová adresa.
- Cieľ – cieľová sieťová adresa.
- Zastaviť blokovanie – vytvorí sa IDS pravidlo pre podozrivú hrozbu s nastaveniami povoľujúcimi danú komunikáciu.
- Pokračovať v blokovaní – detegovaná hrozba bude blokovaná. Ak chcete vytvoriť IDS pravidlo s nastaveniami blokujúcimi komunikáciu danej hrozby, vyberte možnosť Viac neupozorňovať.

Informácia zobrazená v okne oznámení sa môže líšiť v závislosti od typu zachytenej hrozby. Viac informácií o hrozbách a ďalších súvisiacich pojmoch nájdete v kapitole Typy vzdialených útokov alebo Typy detekcií.

Dočasný blacklist IP adries

Zobrazte si zoznam IP adries, ktoré boli zachytené ako zdroj útokov a pridané na blacklist s cieľom istý čas (do jednej hodiny) blokovať pripojenia. Zobrazuje zablokované **IP adresy**.

Dôvod blokovania

Zobrazuje typ zablokovaného útoku prichádzajúceho z konkrétnej adresy (napr. útok súvisiaci so skenovaním TCP portov).

Časový limit

Zobrazuje čas a dátum, keď bude adresa odstránená z blacklistu.

Odstrániť/Odstrániť všetky

Odstráni označenú IP adresu z dočasného blacklistu predtým, ako dôjde k automatickému odstráneniu, prípadne ihneď odstráni z blacklistu všetky adresy.

Pridať výnimku

Pridá výnimku firewallu do filtrovania IDS pre vybrané IP adresy.

Ochrana pred útokmi hrubou silou

Ochrana pred útokmi hrubou silou blokuje pokusy o uhádnutie prístupových hesiel k službám RDP a SMB. Útok hrubou silou je metóda systematického testovania možných kombinácií písmen, číslic a symbolov s cieľom prelomiť heslo.

- **Zapnúť ochranu pred útokmi hrubou silou** – ESET Mail Security kontroluje obsah sieťovej komunikácie a blokuje pokusy o uhádnutie hesiel.
- Pravidlá – editor pravidiel umožňuje vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia.
- Vylúčenia – zoznam vylúčených detekcií definovaných na základe IP adresy alebo cesty k aplikácii. Vylúčenia môžete vytvárať a upravovať cez ESET PROTECT Web Console.

Pravidlá ochrany pred útokmi hrubou silou

V okne s pravidlami ochrany pred útokmi hrubou silou môžete vytvárať, upravovať a zobrazovať pravidlá pre prichádzajúce a odchádzajúce sieťové pripojenia. Prednastavené pravidlá nie je možné upraviť ani odstrániť.

Kliknutím na **Pridať** môžete vytvoriť nové pravidlo ochrany pred útokmi hrubou silou, prípadne kliknite na **Upraviť**, ak chcete upraviť označené položky.

Toto okno poskytuje prehľad o existujúcich pravidlách ochrany pred útokmi hrubou silou.

Názov	Názov pravidla určený používateľom alebo automaticky.
Zapnuté	Túto možnosť je vhodné deaktivovať v prípade, ak si želáte ponechať dané pravidlo v zozname pravidiel, avšak nechcete ho používať.
Akcia	Pravidlo špecifikuje akciu Povoliť alebo Zakázať, ktorú je potrebné vykonať, ak sú všetky podmienky splnené.
Protokol	Komunikačný protokol, pre ktorý má pravidlo platiť.
Profil	Pre každý profil je možné nastaviť vlastné pravidlá.
Maximálny počet pokusov	Maximálny povolený počet pokusov o opakovanie útoku, pokým IP adresa nebude zablokovaná a pridaná na blacklist.
Obdobie uchovávania na blackliste (min)	Nastaví čas odstránenia IP adresy z blacklistu. Časové obdobie, za ktoré sa ráta počet pokusov, je predvolene nastavené na 30 minút.
Zdrojová IP adresa	Zoznam IP adries, rozsahov alebo podsietí. Ak chcete zadať viacero adries, musia byť oddelené čiarkou.
Zdrojové zóny	Po kliknutí na Pridať si môžete vybrať z preddefinovaných zón alebo si vytvoriť novú zónu so zvoleným rozsahom IP adries.

Vylúčenia z ochrany pred útokmi hrubou silou

Vylúčenia útokov hrubou silou možno použiť na potlačenie detekcií útokov hrubou silou podľa konkrétnych kritérií. Tieto vylúčenia sa vytvárajú cez konzolu ESET PROTECT na základe detekcií útokov hrubou silou. Vylúčenia sa zobrazia v tom prípade, že správca vytvorí vylúčenia útokov hrubou silou v ESET PROTECT Web Console. Vylúčenia môžu obsahovať iba povoľujúce pravidlá a sú vyhodnocované ešte pred IDS pravidlami.

- **Detekcia** – typ detekcie.
- **Aplikácia** – nastavte cestu k vylúčenej aplikácii kliknutím na ... (napríklad *C:\Program Files\Firefox\Firefox.exe*). Nezadávajte názov aplikácie.
- **Vzdialená IP** – zoznam vzdialených IPv4 alebo IPv6 adries/rozsahov/podsietí. Ak chcete zadať viacero adries, musia byť oddelené čiarkou.

Web a e-mail

V tejto sekcii môžete nakonfigurovať filtrovanie protokolov, ochranu e-mailových klientov, ochranu prístupu na web a antiphishingovú ochranu a zabezpečiť tak svoj server počas pripojenia na internet.

Ochrana e-mailových klientov

Kontroluje e-mailovú komunikáciu, chráni pred škodlivým kódom a umožňuje vám zvoliť si akciu, ktorá bude vykonaná v prípade zistenia infiltrácie.

Ochrana prístupu na web

Spočíva hlavne v monitorovaní komunikácie prehliadačov internetových stránok so servermi, ktorá prebieha podľa pravidiel protokolu HTTP a HTTPS. Táto funkcia vám tiež umožňuje blokovať, povoliť alebo vylúčiť z kontroly konkrétne URL adresy.

Filtrovanie protokolov

Ide o pokročilú ochranu pre aplikačné protokoly, ktorá je vykonávaná prostredníctvom jadra ThreatSense. Táto kontrola pracuje automaticky bez ohľadu na to, či je používaný webový prehliadač alebo e-mailový klient. Pracuje tiež so šifrovanou (SSL/TLS) komunikáciou.

Antiphishingová ochrana

Umožňuje vám blokovať webové stránky známe týmto typom obsahu.

Filtrovanie protokolov

Antimalvérová ochrana aplikačných protokolov je vykonávaná prostredníctvom jadra ThreatSense, v ktorom sú sústredené viaceré pokročilé metódy detekcie škodlivého softvéru. Filtrovanie protokolov pracuje automaticky bez ohľadu na používaný webový prehliadač alebo e-mailový klient. Ak je filtrovanie protokolov povolené, ESET Mail Security bude kontrolovať komunikáciu, ktorá využíva SSL/TLS protokol. Túto funkciu môže povoliť v sekcii **Web a e-mail** > SSL/TLS.

Zapnúť kontrolu obsahu aplikačných protokolov

Moduly ESET Mail Security (Ochrana prístupu na web, Ochrana e-mailových protokolov a Antiphishingová ochrana) sú závislé od tohto nastavenia a nebudú bez neho funkčné.

Vylúčené aplikácie

Pre vylúčenie aplikácií z kontroly ich označte v zozname. HTTP či POP3 komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu. Umožňuje vylúčiť konkrétne aplikácie z filtrovania protokolov. Kliknite na **Upraviť** a **Pridať** pre ich výber zo zoznamu aplikácií.

Vylúčenie aplikácie z kontroly odporúčame iba vo výnimočných prípadoch, napr. ak aplikácia v dôsledku kontroly jej komunikácie nepracuje správne a pod.

Vylúčené IP adresy

Umožňuje vylúčiť konkrétne adresy z filtrovania protokolov. IP adresy uvedené v zozname budú vylúčené z filtrovania protokolov. Obojstranná HTTP, POP3, či IMAP komunikácia označených aplikácií nebude kontrolovaná na prítomnosť škodlivého kódu.

Túto možnosť odporúčame používať iba v prípade dôveryhodných IP adries.

Kliknite na **Upraviť** a **Pridať** pre zadanie IP adries, rozsahu adries alebo podsiete, na ktorú sa bude vzťahovať vylúčenie. Ak označíte možnosť **Zadať viaceré hodnoty**, môžete do textového poľa zadať viacero IP adries oddelených riadkami, čiarkami alebo bodkočiarkami. Ak je povolený hromadný výber, adresy sa zobrazia v zozname vylúčených IP adries.

Túto možnosť odporúčame použiť v prípade, že filtrovanie protokolov obmedzuje spojenie.

Webové a e-mailové klienty

Bezpečnosť pri prehliadaní internetu je vzhľadom na veľké množstvo škodlivého kódu dôležitou súčasťou ochrany počítača. Zraniteľnosti prehliadačov a rôzne klamlivé odkazy dokážu zaviesť škodlivý kód do systému bez vedomia používateľa. Z tohto dôvodu je v ESET Mail Security venovaná pozornosť internetovým prehliadačom. Každá aplikácia, ktorá pristupuje k sieti, sa môže považovať za webový prehliadač. Aplikácie, ktoré už používajú protokoly na komunikáciu, alebo aplikácie z vybranej cesty môžu byť pridané do zoznamu Webových a e□mailových klientov.

SSL/TLS

ESET Mail Security umožňuje kontrolu na prítomnosť hrozieb v komunikáciách využívajúcich protokol SSL (Secure Sockets Layer) / TLS (Transport Layer Security).

Kontrolu možno prispôsobiť podľa toho, či certifikát využívaný danou SSL komunikáciou je dôveryhodný, neznámy, alebo je v zozname certifikátov, pre ktoré sa nebude vykonávať kontrola obsahu v protokole SSL.

Zapnúť filtrovanie protokolu SSL/TLS

Ak je táto možnosť vypnutá, nebude sa používať filtrovanie komunikácie cez protokol SSL. Režim filtrovania protokolu SSL/TLS je dostupný v nasledujúcich režimoch:

• **Automatický režim** – bude vykonávaná kontrola každej komunikácie cez protokol SSL/TLS, okrem komunikácie využívajúcej certifikáty vylúčené z kontroly. Pri komunikácii využívajúcej nový - zatiaľ neznámy certifikát, ktorý je dôveryhodne podpísaný, nebude používateľ upozornený a komunikácia sa bude automaticky filtrovať. Ak používateľ pristupuje na server používajúci nedôveryhodne podpísaný certifikát, pričom bol tento používateľom označený ako dôveryhodný (zaradený do zoznamu dôveryhodných certifikátov), prístup bude povolený a komunikácia bude filtrovaná.

• **Interaktívny režim** – v prípade, že zadáte novú stránku chránenú protokolom SSL/TLS (s neznámym certifikátom), zobrazí sa okno s možnosťou výberu akcie. Tento režim umožňuje vytvoriť zoznam certifikátov, pre ktoré sa nebude vykonávať kontrola v protokole SSL/TLS.

• **Režim politiky** – v režime politiky budú všetky SSL/TLS pripojenia okrem vylúčení filtrované.

Zoznam SSL/TLS-filtrovaných aplikácií

Môžete pridať filtrovanú aplikáciu a nastaviť jednu z akcií kontroly. Pomocou zoznamu SSL/TLS-filtrovaných aplikácií môžete prispôsobiť správanie ESET Mail Security pre konkrétne aplikácie, ako aj nastaviť zapamätanie zvolených akcií v prípade, že je pre **Režim filtrovania protokolu SSL/TLS** vybraná možnosť **Interaktívny režim**.

Zoznam známych certifikátov

Umožňuje vám nastaviť správanie programu ESET Mail Security pre konkrétne SSL certifikáty. Tento zoznam je možné zobraziť a spravovať kliknutím na Upraviť vedľa **Zoznamu známych certifikátov**.

Vylúčiť komunikáciu s dôveryhodnými doménami

Umožňuje vylúčiť komunikáciu využívajúcu SSL certifikát s rozšíreným overením (EV, Extended Validation) z kontroly protokolu.

Blokovať šifrovanú komunikáciu používajúcu zastaraný protokol SSLv2

Komunikácia využívajúca túto staršiu verziu SSL protokolu bude automaticky blokovaná.

Koreňový certifikát

Pre správne fungovanie SSL/TLS komunikácie v danom prehliadači/e-mailovom kliente je nevyhnutné, aby do jeho zoznamu známych koreňových certifikátov (vydavateľov) bol pridaný aj certifikát spoločnosti ESET. Možnosť Pridať koreňový certifikát do známych prehliadačov by teda mala ostať označená.

Voľba zabezpečuje jeho automatické pridanie do známych prehliadačov (napr. Opera, Firefox). Prehliadače používajúce ukladací priestor systémových certifikátov pridaný automaticky (napr. Internet Explorer).

Pre nepodporované prehliadače môže byť certifikát exportovaný cez tlačidlo **Zobraziť certifikát** > **Podrobnosti** > **Kopírovať do súboru...** a následne manuálne importovaný do prehliadača.

Platnosť certifikátu

Ak sa nedá overiť platnosť certifikátu pomocou certifikačného úložiska TRCA

V niektorých prípadoch nie je možné overiť platnosť certifikátu webovej stránky pomocou certifikačných autorít (**Trusted Root Certification Authorities** – TRCA). To znamená, že certifikát je niekým samostatne podpísaný (napr. správcom webového servera alebo malou firmou) a považovanie tohto certifikátu za dôveryhodný nemusí vždy predstavovať riziko. Väčšina veľkých obchodných spoločností (napr. banky) používajú certifikát podpísaný

certifikačnou autoritou (TRCA – Trusted Root Certification Authorities).

Ak je označená možnosť**Spýtať sa používateľa na platnosť certifikátu** (predvolená), používateľ bude v prípade nadviazania šifrovanej komunikácie upozornený na výber akcie. Pomocou možnosti **Zablokovať komunikáciu využívajúcu daný certifikát** sa vždy zablokuje komunikácia s webovou stránkou využívajúcou neoverený certifikát.

Ak je certifikát neplatný alebo poškodený

Znamená to, že mu vypršala platnosť alebo bol nesprávne podpísaný. V tomto prípade sa odporúča ponechať možnosť **Zablokovať komunikáciu využívajúcu daný certifikát** označenú.

Zoznam známych certifikátov

Pomocou zoznamu známych certifikátov môžete prispôsobiť správanie ESET Mail Security pre konkrétne SSL/TLS certifikáty, ako aj nastaviť zapamätanie zvolených akcií v prípade, že je pre Režim filtrovania protokolu SSL/TLS vybraná možnosť **Interaktívny režim**. Môžete nastaviť zvolený certifikát alebo použiť možnosť **Pridať** pre pridanie certifikátu z URL adresy alebo súboru.

Keď sa nachádzate v okne **Pridať certifikát**, kliknite na **URL** alebo **Súbor** a upresnite URL adresu certifikátu alebo vyhľadajte súbor certifikátu. Nižšie nájdete zoznam polí, ktoré sú automaticky vyplnené pomocou údajov z certifikátu:

- **Názov certifikátu** – názov certifikátu.
- **Vydavateľ certifikátu** – meno autora certifikátu.
- **Predmet certifikátu** – identifikácia entity spojenej s verejným kľúčom uloženým v poli predmet verejného kľúča.

Akcia prístupu

- **Automaticky** – povolenie dôveryhodných a pýtanie sa na nedôveryhodné certifikáty.
- **Povoliť alebo Blokovať** – povolenie alebo blokovanie komunikácie zabezpečenej týmto certifikátom bez ohľadu na jeho dôveryhodnosť.
- **Spýtať sa** – zobrazí sa výzva s výberom akcie pre konkrétny certifikát.

Akcia kontroly

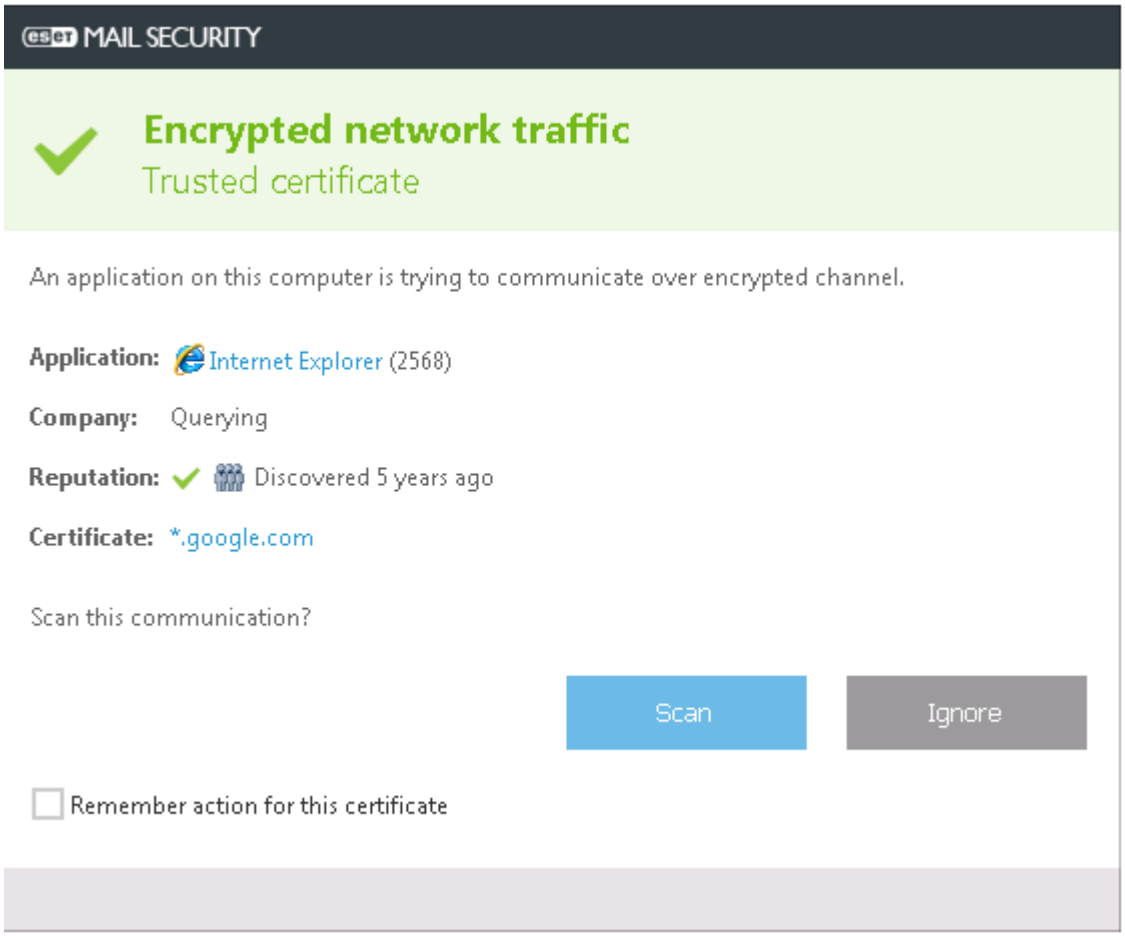
- **Automaticky** – kontrola v automatickom režime a pýtanie sa v interaktívnom režime.
- **Kontrolovať alebo Ignorovať** – kontrola alebo ignorovanie komunikácie zabezpečenej týmto certifikátom.
- **Spýtať sa** – zobrazí sa výzva s výberom akcie pre konkrétny certifikát.

Šifrovaná SSL komunikácia

Ak je počítač nastavený na kontrolu protokolu SSL, môže sa pri pokuse o šifrovanú komunikáciu zobraziť výstražné okno s možnosťami výberu, a to v dvoch situáciách:

Prvá situácia nastáva, ak stránka používa neoveriteľný alebo neplatný certifikát a program ESET Mail Security je nastavený tak, aby sa v takýchto prípadoch pýtal používateľa (predvolene len pri neoveriteľných). Zobrazí sa dialógové okno s možnosťami **Blokovať** alebo **Povoliť** spojenie.

Druhá situácia nastáva, ak je **Režim filtrovania protokolu SSL** nastavený na **Interaktívny režim**. V tom prípade sa zobrazí dialógové okno pre každú webovú stránku s možnosťami **Kontrolovať** alebo **Ignorovať** spojenia. Niektoré aplikácie kontrolujú, či ich SSL komunikácia nie je zmenená alebo sledovaná inou aplikáciou. V takomto prípade musí ESET Mail Security **Ignorovať** komunikáciu týchto aplikácií, aby nedošlo k obmedzeniu ich funkčnosti.



V oboch hore uvedených prípadoch zobrazenia výstražných okien je možné zapamätať danú akciu. Zapamätané akcie sú uložené v Zozname známych certifikátov.

Ochrana e-mailových klientov

Integrácia ESET Mail Security a e-mailových klientov zlepšuje možnosť aktívnej ochrany pred škodlivým kódom v e-mailových správach. V prípade, že je daný e-mailový klient podporovaný, je vhodné povoliť jeho integráciu s ESET Mail Security. Pri integrácii dochádza k vloženiu panela nástrojov ESET Mail Security priamo do e-mailového klienta (okrem novších verzií Windows Live Mail), čo prispieva k efektívnejšej kontrole e-mailových správ.

Integrácia s e-mailovými klientmi

V tomto okne je možné aktivovať integráciu s podporovanými poštovými klientmi, ktorými v súčasnej verzii sú: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail. E-mailová ochrana funguje v rámci týchto klientov prostredníctvom doplnku. Hlavnou výhodou je nezávislosť od použitého protokolu. V prípade šifrovanej komunikácie program takto od e-mailového klienta dostáva už dešifrované správy na kontrolu. V prípade, že integráciu nepovolíte, bude e-mailová komunikácia chránená modulom ochrany e-mailových klientov (POP3,

IMAP).

Kompletný zoznam podporovaných e-mailových klientov a ich verzií nájdete v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Vypnúť kontrolu pri zmene obsahu priečinka s doručenou poštou

Túto možnosť odporúčame použiť v prípade, ak pozorujete spomalenie pri práci s e-mailovým klientom (platí len pre Microsoft Outlook). Uvedená situácia môže nastať napríklad v prípade prijímania správ z úložiska správ prostredníctvom Kerio Outlook Connector Store.

Zapnúť e-mailovú ochranu prostredníctvom pluginov klienta

Pomocou tejto možnosti môžete vypnúť ochranu e-mailových klientov bez odstránenia integrácie so svojím e-mailovým klientom. Doplnky môžete vypnúť všetky naraz alebo môžete osobitne vypnúť nasledovné:

- **Prijaté e-maily** – zapnutie/vypnutie kontroly prijatých správ.
- **Odoslané e-maily** – zapnutie/vypnutie kontroly odosielaných správ.
- **Prečítané e-maily** – zapnutie/vypnutie kontroly čítaných správ.

Pri e-mailoch obsahujúcich detekcie vykonať nasledujúcu akciu

- **Žiadna akcia** – ak je táto možnosť povolená, program nájde e-mailové správy s infikovanými prílohami, no nevykoná s nimi žiadnu akciu.
- **Odstrániť e-mail** – program upozorní na infikované prílohy a odstráni celú správu.
- **Presunúť e-mail do priečinka vymazaných správ** – program bude automaticky presúvať infikované správy do priečinka Vymazané správy.
- **Presunúť e-mail do priečinka** – program bude automaticky presúvať infikované správy do zadaného priečinka.
- **Priečinok** – priečinok, do ktorého bude program presúvať správy, v ktorých boli zachytené infiltrácie.

Opakovať kontrolu po aktualizácii

Zapína opätovnú kontrolu po aktualizácii detekčného jadra.

Zohľadniť výsledky kontroly z iných modulov

Zohľadnenie výsledku kontroly vykonanej iným modulom (kontrola protokolov POP3, IMAP).

E-mailové protokoly

Zapnúť e-mailovú ochranu prostredníctvom filtrovania protokolov

IMAP a POP3 sú najrozšírenejšie protokoly slúžiace na príjem e-mailovej komunikácie prostredníctvom e-mailového klienta. ESET Mail Security poskytuje pre tieto protokoly ochranu bez ohľadu na používaný e-mailový klient.

ESET Mail Security podporuje kontrolu protokolov IMAPS a POP3S, ktoré používajú šifrovaný kanál na výmenu informácií medzi klientom a serverom. ESET Mail Security kontroluje aj komunikáciu šifrovanú pomocou šifrovacích metód SSL (Secure Socket Layer) a TLS (Transport Layer Security). Kontrolované sú len porty používané **protokolom IMAPS/POP3S**, pričom nezáleží na operačnom systéme.

Nastavenie kontroly protokolu IMAPS/POP3S

Šifrovaná komunikácia nie je kontrolovaná, ak sú použité predvolené nastavenia. Pre povolenie kontroly šifrovanej komunikácie prejdite do sekcie Kontrola protokolu SSL/TLS.

Číslo portu určuje, o aký port ide. Nižšie nájdete predvolené e-mailové porty pre:

Názov portu	Číslo portu	Popis
POP3	110	Predvolený POP3 nešifrovaný port.
IMAP	143	Predvolený IMAP nešifrovaný port.
Zabezpečený IMAP (IMAP4-SSL)	585	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.
IMAP4 cez SSL (IMAPS)	993	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.
Zabezpečený POP3 (SSL-POP)	995	Filtrovanie SSL/TLS protokolu. Viaceré čísla portov musia byť oddelené čiarkou.

Upozornenia a udalosti

Ochrana e-mailových klientov zabezpečuje kontrolu e-mailovej komunikácie prijímanej prostredníctvom protokolov POP3 a IMAP. Pomocou pluginu pre Microsoft Outlook a ďalšie e□mailové klienty zabezpečuje ESET Mail Security kontrolu všetkej komunikácie daného klienta (POP3, MAPI, IMAP, HTTP).

Pri kontrole prijímaných správ sú použité všetky pokročilé metódy kontroly obsiahnuté v skenovacom jadre ThreatSense. Tým je zabezpečená detekcia nebezpečných programov ešte pred aktualizáciou detekčného jadra. Kontrola protokolov POP3 a IMAP je nezávislá od typu e-mailového klienta.

Program umožňuje do kontrolovaných správ pridávať poznámku s informáciou o výsledku kontroly. Používateľ môže **Pridávať poznámku do prijatých a čítaných e-mailov**, **Pridávať do predmetu prijatých a čítaných infikovaných e-mailov** alebo tiež **Pridávať poznámku do odosielaných e-mailov**.

Na tieto poznámky sa nemožno úplne spoliehať, keďže nemusia byť doplnené do problematických HTML správ a taktiež môžu byť sfalšované malvérom. Pridávanie poznámok možno nastaviť zvlášť pre prijaté a prečítané e□maily a zvlášť pre odosielané e□maily, prípadne pre všetky e□maily.

Sú dostupné tieto možnosti:

- **Nikdy** – do správ nebudú pridávané žiadne poznámky s informáciou o výsledku kontroly.
- **Pridávať len do infikovaných e-mailov** – program bude pridávať poznámky len do infikovaných správ (predvolené nastavenie).
- **Do všetkých skontrolovaných e□mailov** – program bude pridávať poznámky do všetkých skontrolovaných e□mailov.

Pridávať do predmetu odosielaných infikovaných e-mailov

Túto možnosť vypnite v prípade, ak nechcete, aby bolo do predmetu infikovanej správy pridávané upozornenie týkajúce sa vírusu. Táto funkcia sa dá využiť pre jednoduché filtrovanie infikovaných správ podľa predmetu, pokiaľ to e-mailový klient umožňuje. Reťazec tiež vzbudzuje dôveryhodnosť u adresáta správy a poskytuje hodnotnú informáciu o bezpečnosti správy.

Šablóna pridávaná do predmetu infikovaných e-mailov

Túto šablónu upravte v prípade, ak chcete zmeniť formát predpony predmetu infikovanej správy. Táto funkcia doplní predmet správy, ktorý znie napríklad „Ahoj“, príponou „[virus]“ na nasledujúci formát: „[virus] Ahoj“. Premenná %VIRUSNAME% predstavuje typ nájdenej hrozby.

Panel nástrojov Microsoft Outlook

Ochrana programu Microsoft Outlook je vykonávaná prostredníctvom doplnku. Po nainštalovaní ESET Mail Security je do programu Microsoft Outlook pridaný panel obsahujúci nastavenia ochrany:

ESET Mail Security

Kliknutím na ikonu otvoríte hlavné okno programu ESET Mail Security.

Opätovná kontrola správ

Umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete tiež vybrať správy, ktoré budú kontrolované, a aktivovať opakovanú kontrolu prijatých správ. Viac informácií sa nachádza v kapitole Ochrana e-mailových klientov.

Nastavenia antivírusu

Otvorí okno s nastaveniami Ochrany e-mailových klientov.

Panel nástrojov v Outlook Express a Windows Mail

Ochrana programu Outlook Express alebo Windows Mail je vykonávaná prostredníctvom doplnku. Po nainštalovaní ESET Mail Security je do programu Outlook Express alebo Windows Mail pridaný panel s nastaveniami ochrany:

ESET Mail Security

Kliknutím na ikonu otvoríte hlavné okno programu ESET Mail Security.

Opätovná kontrola správ

Umožní vám manuálne spustiť kontrolu e-mailových správ. Môžete tiež vybrať správy, ktoré budú kontrolované, a aktivovať opakovanú kontrolu prijatých správ. Viac informácií sa nachádza v kapitole Ochrana e-mailových klientov.

Nastavenia antivírusu

Otvorí okno s nastaveniami Ochrany e-mailových klientov.

Prispôsobiť vzhľad

Môžete si prispôsobiť vzhľad panela pre svojho e-mailového klienta. Označte túto možnosť pre prispôsobenie vzhľadu panela.

- **Zobrazovať text** – zobrazuje popis pod ikonami.
- **Text vpravo** – popisy sú presunuté na pravú stranu vedľa ikony.
- **Veľké ikony** – zobrazí veľké ikony pre položky menu.

Potvrdzovacie dialógové okno

Dialógové okno s možnosťou potvrdenia alebo zamietnutia zvolenej akcie slúži ako ubezpečenie sa, že používateľ chce danú akciu naozaj vykonať, čo slúži na obmedzenie možných omylov. Dialógové okno ponúka aj možnosť vypnúť zobrazovanie potvrdzovacích správ úplne.

Opätovná kontrola správ

Integrovaný ovládací panel produktu ESET Mail Security v e-mailovom kliente umožňuje používateľom nastaviť rôzne druhy kontroly e-mailových správ. Prostredníctvom možnosti **Opätovná kontrola správ** je možné spustiť dva režimy kontroly:

- **Všetky správy v aktuálnom priečinku** – budú kontrolované všetky správy v priečinku, ktorý je aktuálne zobrazený.
- **Iba označené správy** – kontrole budú podliehať len správy, ktoré používateľ priamo označil.
- **Kontrolovať aj správy, ktoré už boli prekontrolované** – táto možnosť zabezpečí, aby sa do kontroly zahrnuli aj správy, ktoré už boli v minulosti kontrolované.

Ochrana prístupu na web

Ochrana prístupu na web spočíva hlavne v monitorovaní komunikácie prehliadačov webových stránok so servermi, ktorá prebieha podľa pravidiel protokolu HTTP a HTTPS.

Prístup na web stránky, ktoré sú známe ich nebezpečným obsahom, je vždy blokovaný skôr ako je obsah stiahnutý. Všetky ostatné webové stránky sú kontrolované technológiou ThreatSense pri ich načítaní a ak obsahujú škodlivý obsah, sú zablokované. Ochrana prístupu na web obsahuje dve vrstvy ochrany, blokovanie na základe blacklistu a blokovanie podľa obsahu.

Základné

Odporúčame ponechať **Ochranu prístupu na web** zapnutú. Nastavenia ochrany prístupu na web sú dostupné takisto z hlavného okna ESET Mail Security v sekcii **Nastavenia** > **Web a e-mail** > **Ochrana prístupu na web**.
Zapnúť rozšírenú kontrolu skriptov prehliadača
V rámci predvolených nastavení sú všetky JavaScript programy spúšťané webovými prehliadačmi kontrolované detekčným jadrom.

Webové protokoly

Môžete nastaviť monitorovanie pre štandardné protokoly používané väčšinou webových prehliadačov. Predvolene je ESET Mail Security nakonfigurovaný na monitorovanie HTTP protokolu používaného väčšinou webových prehliadačov.
ESET Mail Security tiež podporuje šifrovanú komunikáciu HTTPS. Pri tejto komunikácii sú údaje prenášané medzi serverom a klientom šifrované. ESET Mail Security kontroluje aj komunikáciu šifrovanú pomocou šifrovacích metód SSL (Secure Socket Layer) a TLS (Transport Layer Security). Kontrolované sú len **porty používané protokolom HTTPS**, pričom nezáleží na operačnom systéme.
Šifrovaná komunikácia nie je kontrolovaná, ak sú ponechané predvolené nastavenia. Ak chcete povoliť kontrolu šifrovanej komunikácie, použite možnosť **Rozšírené nastavenia** (**F5**) > **Web a e-mail** > SSL/TLS.

Parametre ThreatSense

V tejto sekcii nájdete podrobnejšie nastavenia kontroly, ako napr. typy kontroly (e-maily, archívy, vylúčenia, obmedzenia atď.) a metódy detekcie pre Ochranu prístupu na web.

Manažment URL adries

Manažment URL adries umožňuje definovať zoznamy adries HTTP, ktoré budú blokované, povolené alebo vylúčené z kontroly. Webové adresy na zozname blokovaných adries nebudú prístupné, pokiaľ nebudú uvedené aj v zozname povolených adries. Webové adresy na zozname adries vylúčených z kontroly sú prístupné, ale nie sú kontrolované na prítomnosť škodlivého kódu. Filtrovanie protokolu SSL/TLS musí byť povolené, ak chcete okrem HTTP adries filtrovať aj adresy HTTPS. V opačnom prípade budú pridané len domény HTTPS adries, ktoré ste navštívili, a nie celé URL adresy.

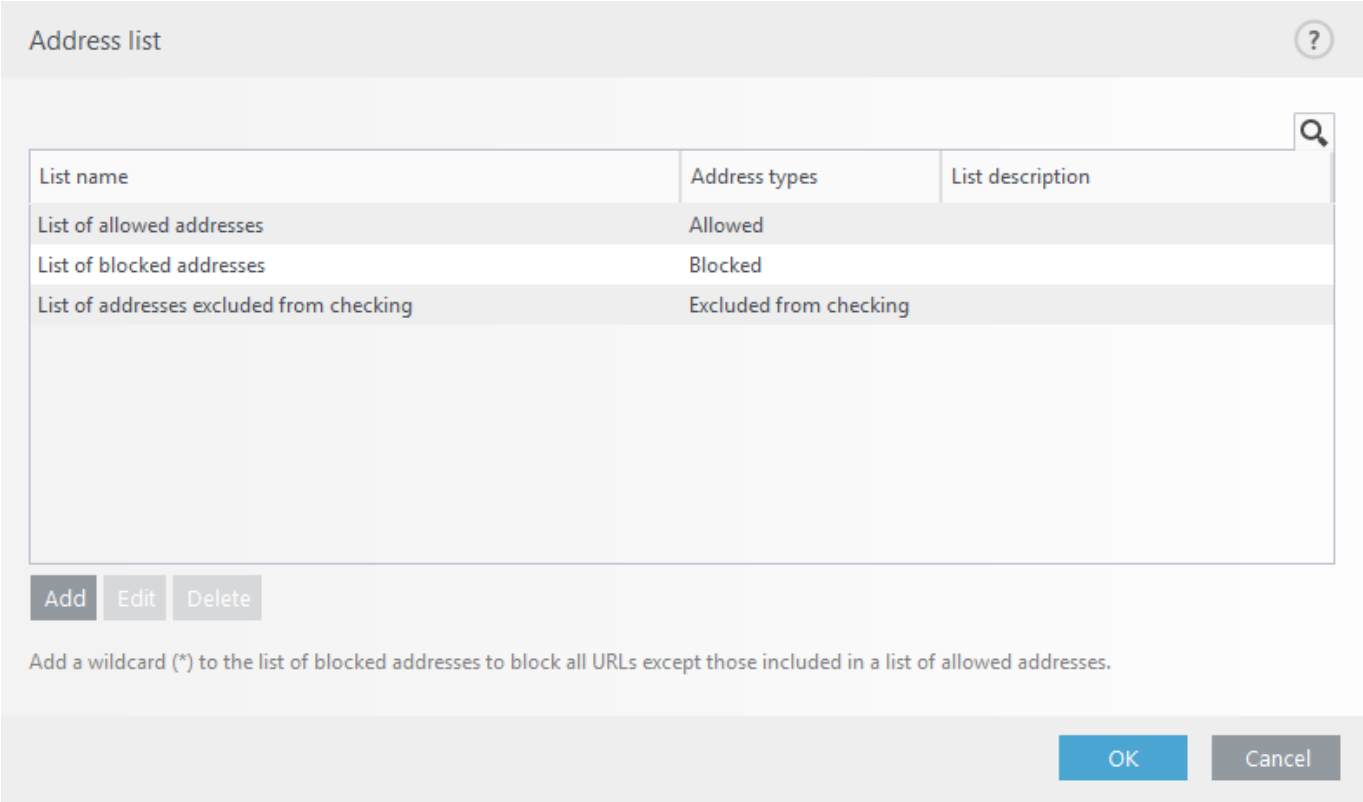
Jeden zoznam blokovaných adries môže obsahovať adresy z externého verejného blacklistu a ďalší zoznam môže obsahovať váš vlastný blacklist, čo uľahčuje aktualizáciu externých zoznamov, pričom váš používateľský zoznam nebude narušený.

Kliknutím na **Upraviť** a **Pridať** vytvoríte nový zoznam adries k vopred zadefinovaným zoznamom. Toto môže byť užitočné, ak chcete logicky rozdeliť niekoľko skupín adries. Na základe predvolených nastavení sú k dispozícii tri zoznamy:

- **Zoznam adries vylúčených z kontroly** – adresy uvedené v tomto zozname nebudú kontrolované na prítomnosť škodlivého kódu.

- **Zoznam povolených adries** – ak je aktívna možnosť Povoliť prístup iba na HTTP adresy uvedené v zozname povolených adries a zoznam blokovaných adries obsahuje znak * (všetko), používateľovi bude umožnený prístup iba na adresy uvedené v zozname povolených adries. Adresy v tomto zozname budú povolené aj vtedy, keď sa nachádzajú v zozname blokovaných adries.

- **Zoznam blokovaných adries** – na adresy v tomto zozname nebude používateľom povolený prístup, ak sa súčasne nenachádzajú aj v zozname povolených adries.



Do zoznamu môžete **pridať** novú URL adresu. Zadať môžete aj viaceré hodnoty použitím oddeľovača. Kliknutím na **Upraviť** môžete zmeniť existujúcu adresu v zozname a kliknutím na **Odstrániť** môžete adresu odstrániť. Vymazať je možné len adresy pridané pomocou funkcie **Pridať**, nie je možné vymazať adresy, ktoré boli importované.

Vo všetkých zoznamoch je možné používať špeciálne znaky * (hviezdička) a ? (otáznik). Hviezdička nahrádza ľubovoľný reťazec a otáznik nahrádza ľubovoľný znak. Pri pridávaní adries vylúčených z kontroly treba byť opatrný, pretože tento zoznam by mal obsahovať iba overené a dôveryhodné adresy. Rovnako je potrebné dbať na správne používanie špeciálnych znakov * a ? v tomto zozname.

Ak chcete zablokovať všetky HTTP adresy okrem adries zaradených na zoznam povolených adries, pridajte znak * do zoznamu blokovaných adries.

Vytvorenie nového zoznamu

Tento zoznam bude obsahovať požadované URL adresy/masky domén, ktoré budú blokované, povolené alebo vylúčené z kontroly. Pri vytváraní nového zoznamu je potrebné zadať nasledovné:

- **Typ zoznamu adries** – vyberte typ (Vylúčené z kontroly, Blokované alebo Povolené) z roletového menu.
- **Názov zoznamu** – názov nového zoznamu. Toto pole bude neprístupné, ak meníte nastavenia predvoleného zoznamu.
- **Popis zoznamu** – podrobné informácie k vytváranému zoznamu (nepovinné). Toto pole bude neprístupné, ak meníte nastavenia predvoleného zoznamu.
- **Zoznam je aktívny** – použite prepínač na deaktiváciu zoznamu. V prípade potreby ho môžete aktivovať neskôr.
- **Upozorniť pri použití adresy zo zoznamu** – označte túto možnosť, ak chcete dostať upozornenie

na použitie konkrétneho zoznamu pri vyhodnocovaní HTTP/HTTPS stránky, ktorú ste navštívili. Pri prístupe na blokovanú alebo povolenú stránku zo zoznamu sa zobrazí oznámenie na ploche. Oznámenie bude obsahovať názov zoznamu, v ktorom sa stránka nachádza.

• **Závažnosť zapisovania do protokolu** – z roletového menu vyberte závažnosť zapisovania do protokolu (Žiadne, Diagnostické, Informácie alebo Upozornenie). Záznamy so závažnosťou Upozornenie môžu byť zozbierané nástrojom ESET PROTECT.

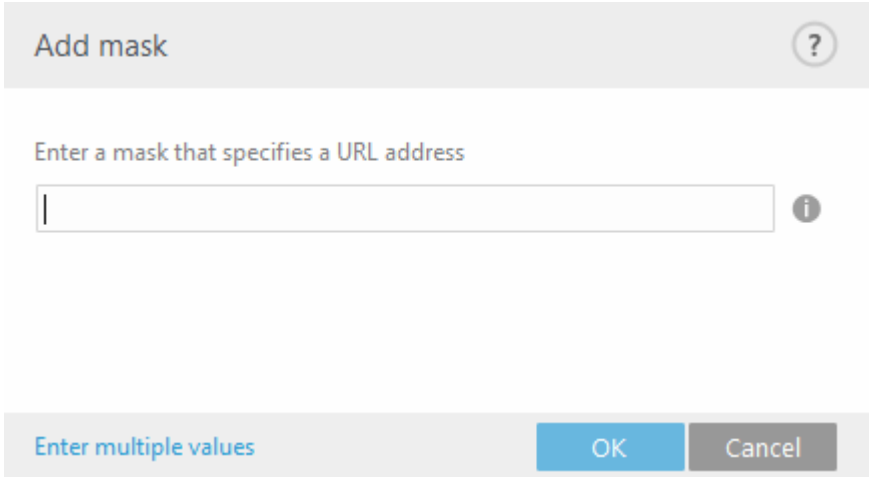
ESET Mail Security umožňuje používateľovi zablokovať prístup ku konkrétnej webovej stránke a zabrániť webovému prehliadaču v zobrazení jej obsahu. Navyše, používateľ môže definovať adresy, ktoré by mali byť z kontroly vylúčené. Ak úplný názov vzdialeného servera nie je známy alebo chce používateľ špecifikovať celú skupinu vzdialených serverov, na identifikovanie takejto skupiny možno použiť tzv. masky.

Masky obsahujú symboly ? a *:

- použite znak ? ako náhradu symbolu
- použite znak * ako náhradu textového reťazca

.c?m sa vzťahuje na všetky adresy, kde posledná časť začína písmenom c, končí písmenom m a obsahuje neznámy symbol medzi týmito dvoma znakmi (*.com*, *.cam* atď.).

Zástupné znaky *. môžete použiť výhradne na začiatku domény. Je potrebné mať na pamäti, že hviezdička * nenahrádza lomku (/) preto, aby sa napr. pomocou masky *.domena.sk nevyhodnocovala adresa *https://akakolvekdomena.sk/cesta#.domena.com* (ako prípona môže byť pripojená k akejkoľvek URL adrese bez toho, aby došlo k obmedzeniu sťahovania). Hviezdička *. ďalej predstavuje v tomto konkrétnom prípade prázdny znak. To umožňuje použiť pre celú doménu vrátane jej subdomén jednotnú masku. Napríklad maska *.domena.sk sa použije aj na vyhodnotenie adresy *https://domena.sk*. To znamená, že použitie masky *domena.sk by bolo nesprávne, pretože maska by bola použitá aj na vyhodnotenie adresy https://inadomena.sk.



Zadať viaceré hodnoty

Ak označíte túto možnosť, môžete do textového poľa zadať viacero URL adries oddelených novými riadkami, čiarkami alebo bodkočiarkami. Ak je povolený hromadný výber, adresy sa zobrazia v zozname.

Importovať

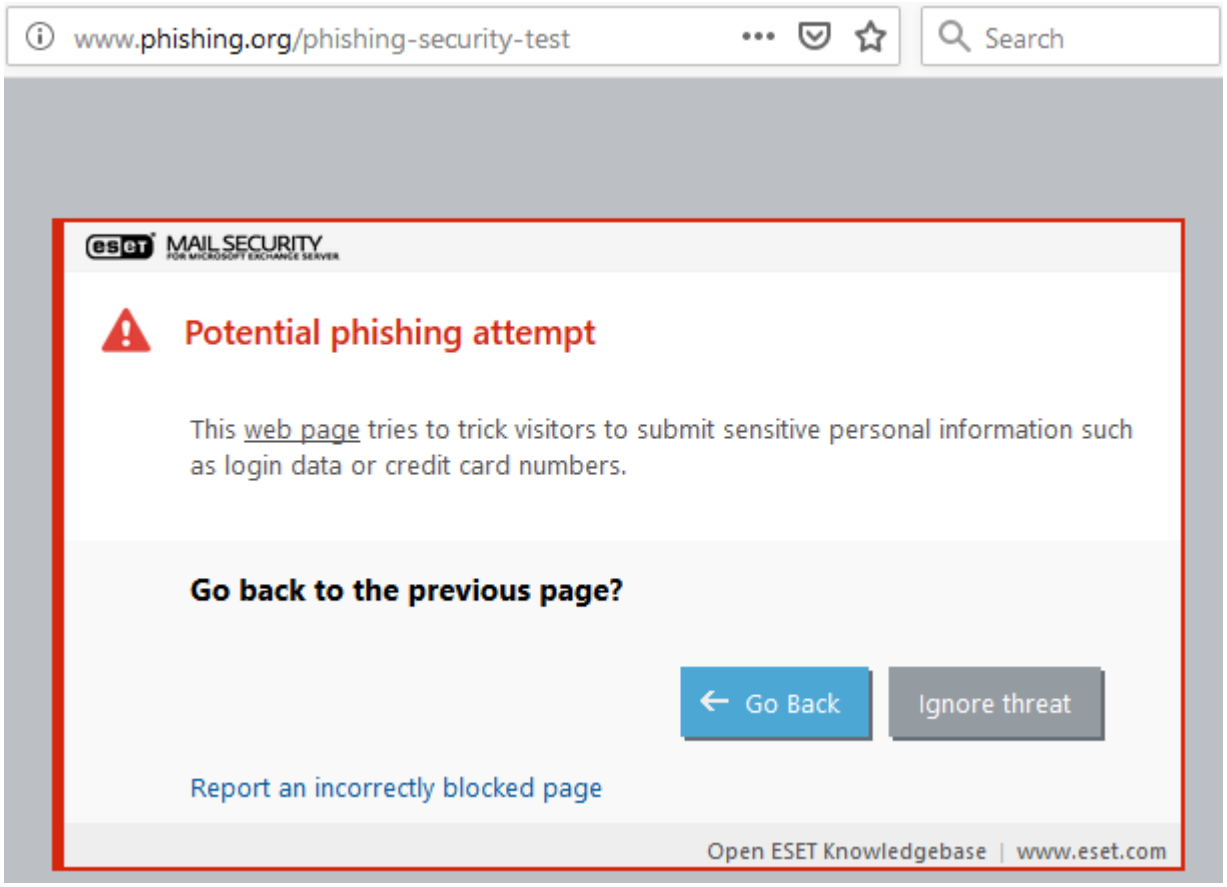
URL adresy môžete naimportovať z textového súboru (formát súboru `*.txt` v kódovaní UTF-8, kde budú jednotlivé adresy oddelené novým riadkom).

Antiphishingová ochrana

Pojem phishing označuje kriminálnu činnosť využívajúcu metódy tzv. sociálneho inžinierstva (manipulačné techniky na získanie dôverných informácií). Cieľom je získať citlivé údaje, ako napríklad heslá k bankovým účtom, PIN kódy a pod.

ESET Mail Security má zabudovanú antiphishingovú ochranu, ktorá blokuje webové stránky známe týmto typom obsahu. Odporúčame, aby ste povolili Anti‑Phishing v programe ESET Mail Security. Viac informácii o antiphishingovej ochrane v rámci produktu ESET Mail Security nájdete v našom článku databázy znalostí.

Ak otvoríte phishingovú stránku, otvorí sa vám v prehliadači nasledujúce upozornenie. Ak aj napriek tomu chcete prejsť na stránku, kliknite na možnosť **Ignorovať hrozbu** (neodporúča sa).



Potenciálne phishingové stránky, ktoré boli horeuvedeným spôsobom pridané na whitelist, vypršia v produkte po niekoľkých hodinách. Pre trvalé povolenie konkrétnej webovej stránky použite nástroj Manažment URL adries.

Nahlásiť phishingovú stránku

V prípade, že sa stretnete s podozrivou webovou stránkou, môžete ju odoslať do spoločnosti ESET na analýzu. Predtým, ako webovú stránku odošlete, sa však uistite, že spĺňa nasledujúce podmienky:

- webová stránka ešte nie je v programe detegovaná,
- webová stránka sa nesprávne deteguje ako hrozba. V takomto prípade kliknite na odkaz Toto nie je phishingová stránka.

Webovú stránku môžete odoslať na analýzu aj prostredníctvom e-mailu. V takom prípade ju pošlite na adresu samples@eset.com. Nezabudnite uviesť výstižný predmet správy a čo najviac informácií o webovej stránke (napr. URL adresa, z ktorej ste sa na túto stránku dostali, ako ste sa o nej dozvedeli a pod.).

Správa zariadení

ESET Mail Security poskytuje automatickú správu externých zariadení (CD/DVD/USB atď.). Tento modul umožňuje kontrolovať (skenovať), blokovať a nastavovať rozšírené prístupové práva a pravidlá filtrovania, ako aj nastavovať prístup konkrétneho používateľa k zariadeniu. Toto môže byť užitočné v prípade, že správca chce, aby používatelia nemohli používať externé zariadenia s nežiaducim obsahom.

Ak povolíte správu zariadení pomocou možnosti **Integrácia do systému**, v ESET Mail Security sa aktivuje funkcia Správa zariadení. Aby sa táto zmena prejavila, je nutné reštartovať počítač.

Správa zariadení sa stane aktívnou a vy budete môcť upravovať príslušné nastavenia. Ak je detegované zariadenie, ktoré je blokované existujúcim pravidlom, v pravom dolnom rohu sa zobrazí príslušné oznámenie a prístup k zariadeniu bude zamietnutý.

Pravidlá

Pravidlo správy zariadení definuje akciu, ktorá bude vykonaná pri pripojení zariadenia spĺňajúceho kritériá v pravidle.

Skupiny

Kliknutím na možnosť Upraviť môžete spravovať skupiny zariadení. Pridať alebo odstrániť zariadenia zo zoznamu môžete vytvorením novej skupiny zariadení alebo vybraním existujúcej.

V sekcii Protokoly si môžete prezrieť záznamy protokolu správy zariadení.

Pravidlá zariadení

Zariadenia môžu byť povolené alebo blokované vzhľadom na používateľa, skupinu používateľov alebo podľa vybraných parametrov nastavených v pravidle. Zoznam pravidiel pozostáva z niekoľkých parametrov, akými sú názov, typ externého zariadenia, akcia vykonaná po zistení zariadenia a rozsah vytvorených protokolov.

Môžete **pridať** nové pravidlo alebo upraviť nastavenia existujúceho pravidla. Do poľa **Názov** zadajte popis pravidla pre jeho lepšiu identifikáciu. Tlačidlom **Pravidlo je zapnuté** aktivujete alebo deaktivujete konkrétne pravidlo, čo je užitočné v prípade, že si neželáte vymazať pravidlo natrvalo.

Uplatňovať v intervale

Pravidlá môžete obmedziť pomocou časových intervalov. Najprv vytvorte časový interval, ktorý sa následne zobrazí v roletovom menu.

Typ zariadenia

Z roletového menu vyberte typ externého zariadenia (disk, prenosné zariadenie, Bluetooth, Fireware atď.). Typ zariadenia je prevzatý od operačného systému a je uvedený v systémovej Správe zariadení (Device manager), ak je zariadenie pripojené k počítaču. Úložné zariadenia môžu byť externé disky alebo čítačky pamäťových kariet pripojené cez USB alebo FireWire. Čítačky Smart kariet zahŕňajú všetky čítačky kariet s integrovaným obvodom, ako sú SIM karty alebo overovacie karty. Medzi zobrazovacie zariadenia patria napríklad skenery alebo digitálne fotoaparáty, ktoré neposkytujú informácie o používateľovi, iba o jeho akciách. Z toho vyplýva, že môžu byť blokované len globálne pre všetkých používateľov.

Akcia

Prístupové práva k zariadeniam bez úložiska môžu byť povolené/blokované. Prístupové práva k zariadeniam s úložiskom môžu byť nasledovné:

- **Čítanie/Zápis** – všetky práva nad zariadením.
- **Blokovať** – prístup k zariadeniu nebude povolený.
- **Iba na čítanie** – používateľovi bude umožnený prístup k zariadeniu v režime „iba na čítanie“.
- **Upozorniť** – pri každom pripojení zariadenia k počítaču bude používateľ informovaný, či bolo zariadenie povolené alebo zablokované, a zároveň bude daná udalosť zaznamenaná do protokolu. Program si zariadenia nepamätá, čo znamená, že príslušné oznámenie sa zobrazí aj pri opätovnom pripojení rovnakého zariadenia.

> Niektoré akcie nemusia byť dostupné pre niektoré typy zariadení. Ak má však zariadenie úložisko, všetky štyri akcie sú dostupné. Pre zariadenia bez úložiska sú dostupné len dve akcie (napríklad akcia **Iba na čítanie** nie je dostupná pre zariadenia s technológiou Bluetooth; tieto zariadenia sa dajú len povoliť alebo blokovať).

Nasledujúce parametre môžu byť použité na vyladenie pravidla pre čo najlepšie prispôsobenie pravidla danému zariadeniu. Všetky parametre rozlišujú malé a veľké písmená:

- **Výrobca** – filtrovanie podľa výrobcu alebo ID.
- **Model** – názov daného zariadenia.
- **Sériové číslo** – externé zariadenia majú zvyčajne svoje vlastné sériové číslo. V prípade CD/DVD ide o sériové číslo daného média, nie CD mechaniky.

> Ak sú hore spomenuté popisy prázdne, pravidlo bude tieto polia počas filtrovania ignorovať. Parametre vo všetkých poliach okna rozlišujú malé a veľké písmená a nepoužívajú zástupné znaky (*, ?).

Na zistenie parametrov zariadenia najprv vytvorte pravidlo pre povolenie daného typu zariadení. Po pripojení zariadenia k počítaču nájdete jeho parametre v Protokole správy zariadení.

Z roletového menu vyberte **Závažnosť zapisovania do protokolu**:

- **Vždy** – do protokolu budú zaznamenávané všetky udalosti.
- **Diagnostické** – do protokolu budú zaznamenávané informácie potrebné pre ladenie programu.
- **Informácie** – zaznamenáva informatívne správy, napríklad o úspešnej aktualizácii, ako aj udalosti s vyššou závažnosťou.
- **Upozornenie** – zaznamenávané budú varovné správy a kritické chyby.
- **Žiadne** – nebudú vytvárané žiadne protokoly.

Pravidlo môže byť obmedzené len na určitých používateľov alebo skupiny používateľov ich pridaním do Zoznamu používateľov. Kliknutím na **Upraviť** vykonáte zmeny v **Zozname používateľov**.

- **Pridať** – otvorí sa okno Typy objektov: Používatelia alebo Skupiny, kde je možné vybrať konkrétnych používateľov.
- **Odstrániť** – vybraný používateľ bude odstránený z filtra.

> Nie všetky typy zariadení je možné filtrovať pomocou používateľských pravidiel (napríklad zobrazovacie zariadenia neposkytujú informácie o používateľoch, ale iba o vykonaných akciách).

Na výber sú tieto funkcie:

Upraviť

Môžete zmeniť názov zvoleného pravidla alebo parametre zariadení nachádzajúcich sa v danej skupine (výrobca, model a sériové číslo zariadenia).

Kopírovať

Táto funkcia slúži na vytvorenie nového pravidla s parametrami označeného pravidla.

Odstrániť

Slúži na vymazanie označeného pravidla. Ak chcete pravidlo zakázať, môžete tiež prípadne použiť začiarkavacie políčko vedľa daného pravidla. Táto možnosť je užitočná, ak nechcete pravidlo zmazať, ale len dočasne zakázať.

Načítať

Zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné. Po výbere zariadenia zo zoznamu nájdených zariadení a kliknutí na **OK** sa zobrazí okno editora pravidiel s vopred definovanými údajmi (všetky nastavenia môžete meniť).

Pravidlá, ktoré sú v zozname vyššie, majú vyššiu prioritu. Pravidlá môžete hromadne označiť a aplikovať akcie; môžete ich napríklad vymazať alebo presunúť nižšie/vyššie pomocou šípok – **Začiatok**/**Hore**/**Dole**/**Koniec**.

Skupiny zariadení

Okno Skupiny zariadení je rozdelené na dve časti. Na ľavej strane okna je zoznam existujúcich skupín a po pravej strane sa nachádza zoznam zariadení patriacich do konkrétnej skupiny. Vyberte skupinu, ktorej zariadenia chcete zobraziť.

Môžete vytvoriť viaceré skupiny zariadení, na ktoré sa budú aplikovať rôzne pravidlá. Môžete vytvoriť aj jedinú skupinu zariadení, na ktorú sa bude vzťahovať nastavenie, resp. režim **Čítanie/Zápis** alebo **Iba na čítanie**. Týmto docielite, že nerozpoznané zariadenia budú po pripojení k vášmu počítaču blokované.

⚠ Externé zariadenia pripojené k vášmu počítaču môžu predstavovať bezpečnostné riziko.

Na výber sú tieto funkcie:

Pridať

Vytvorenie novej skupiny zariadení zadaním jej názvu alebo pridanie zariadenia do existujúcej skupiny (môžete upresniť aj podrobnosti, ako napr. názov výrobcu, model a sériové číslo).

Upraviť

Môžete zmeniť názov vybranej skupiny alebo parametre zariadení nachádzajúcich sa v danej skupine (výrobca, model a sériové číslo zariadenia).

Odstrániť

Odstránenie vybranej skupiny alebo zariadenia. Ak chcete pravidlo zakázať, môžete tiež prípadne použiť začiarkavacie políčko vedľa daného pravidla. Táto možnosť je užitočná, ak nechcete pravidlo zmazať, ale len dočasne zakázať.

Spustiť import

Importuje zo súboru zoznam sériových čísel zariadení.

Načítať

Zobrazí okno so zoznamom práve pripojených zariadení s nasledujúcimi informáciami: typ zariadenia, výrobca, model a sériové číslo v prípade, že je dostupné. Po výbere zariadenia zo zoznamu nájdených zariadení a kliknutí na **OK** sa zobrazí okno editora pravidiel s vopred definovanými údajmi (všetky nastavenia môžete meniť).

Po dokončení úprav kliknite na **OK**. Ak chcete opustiť okno **Skupiny zariadení** bez zmeny nastavení, kliknite na **Zrušiť**.

ℹ Niektoré akcie nemusia byť dostupné pre niektoré typy zariadení. Ak má však zariadenie úložisko, všetky štyri akcie sú dostupné. Pre zariadenia bez úložiska sú dostupné len dve akcie (napríklad akcia Iba na čítanie nie je dostupná pre zariadenia s technológiou Bluetooth; tieto zariadenia sa dajú len povoliť alebo blokovať).

Konfigurácia nástrojov

V sekcii Nástroje môžete zmeniť rozšírené nastavenia pre nasledujúce položky:

- Časové intervaly
- Microsoft Windows Update
- ESET CMD
- ESET RMM
- Licencia
- Poskytovateľ WMI
- Ciele kontroly pre konzolu na správu produktov ESET
- Protokoly
- Proxy server
- Oznámenia
- Prezentačný režim
- Diagnostika
- Klaster

Časové intervaly

Časové intervaly sa používajú v rámci pravidiel správy zariadení a slúžia na obmedzovanie pravidiel v prípade, že sú aplikované. Môžete vytvoriť časový interval a použiť ho pri pridávaní nových pravidiel alebo pri úprave existujúcich pravidiel (parameter **Uplatňovať v intervale**). Toto vám umožní definovať bežne používané časové intervaly (pracovný čas, víkend atď.) a následne ich jednoducho opäť použiť bez potreby opätovného definovania časových rozsahov pre každé pravidlo. Časový interval by sa mal vzťahovať na akýkoľvek relevantný typ pravidla, ktoré podporuje ovládanie pomocou času.

Microsoft Windows® Update

Aktualizácie systému poskytujú dôležité opravy potenciálnych zraniteľností v systéme a pomáhajú zabezpečiť maximálnu úroveň ochrany vášho počítača. Preto je vhodné nainštalovať aktualizácie systému Microsoft Windows hneď ako sú dostupné. ESET Mail Security vás informuje o chýbajúcich systémových aktualizáciách na úrovni, ktorú je možné nastaviť. Sú dostupné tieto úrovne:

- **Žiadne aktualizácie** – nebudú ponúkané žiadne aktualizácie.
- **Voliteľné aktualizácie** – budú ponúkané aktualizácie s nízkou prioritou a všetky nasledovné.

- **Odporúčané aktualizácie** – budú ponúkané bežné aktualizácie a všetky nasledovné.
- **Dôležité aktualizácie** – budú ponúkané dôležité aktualizácie a všetky nasledovné.
- **Kritické aktualizácie** – budú ponúkané len kritické aktualizácie.

Kliknite na **OK** pre uloženie zmien. Zobrazenie okna dostupných aktualizácií prebehne po overení stavu na aktualizačnom serveri. Samotné zobrazenie dostupných aktualizácií preto nemusí nutne prebehnúť hneď po uložení zmien.

Modul kontroly cez príkazový riadok

Manuálnu kontrolu môžete okrem eShell spustiť aj prostredníctvom príkazového riadka pomocou nástroja `ecls.exe`, ktorý je umiestnený v inštalačnom priečinku produktu ESET Mail Security.

Nižšie je uvedený zoznam parametrov a prepínačov:

Možnosti:

`/base-dir=FOLDER`	načítať moduly z PRIEČINKA
`/quar-dir=FOLDER`	umiestniť PRIEČINOK do karantény
`/exclude=MASK`	vylúčiť z kontroly súbory zodpovedajúce MASKE
`/subdir`	kontrolovať podpriečinky (predvolené)
`/no-subdir`	nekontrolovať podpriečinky
`/max-subdir-level=LEVEL`	podpriečinky kontrolovať len do úrovne
`/symlink`	sledovať symbolické prepojenia (predvolené)
`/no-symlink`	preskočiť symbolické prepojenia
`/ads`	kontrolovať ADS (predvolené)
`/no-ads`	nekontrolovať ADS
`/log-file=FILE`	zapísať výstup do SÚBORU
`/log-rewrite`	prepísať výstupný súbor (predvolene sa dopíše)
`/log-console`	zapísať výstup do konzoly (predvolené)
`/no-log-console`	nezapisovať výstup do konzoly
`/log-all`	zapisovať do protokolu aj neinfikované súbory
`/no-log-all`	nezapisovať do protokolu neinfikované súbory (predvolené)
`/aind`	zobraziť indikátor aktivity
`/auto`	skontrolovať a automaticky vyliečiť všetky lokálne disky

Možnosti kontroly:

`/files`	kontrolovať súbory (predvolené)
`/no-files`	nekontrolovať súbory
`/memory`	kontrolovať pamäť
`/boots`	kontrolovať zavádzacie sektory
`/no-boots`	nekontrolovať zavádzacie sektory (predvolené)

/arch	kontrolovať archívy (predvolené)
/no-arch	nekontrolovať archívy
/max-obj-size=SIZE	kontrolovať len súbory menšie ako VEĽKOSŤ MB (predvolene 0 = neobmedzené)
/max-arch-level=LEVEL	podradené archívy kontrolovať len do úrovne
/scan-timeout=LIMIT	archívy kontrolovať najviac LIMIT s
/max-arch-size=SIZE	kontrolovať len súbory v archíve menšie ako VEĽKOSŤ MB (predvolene 0 = neobmedzené)
/max-sfx-size=SIZE	kontrolovať len súbory v samorozbaľovacích archívoch menšie ako VEĽKOSŤ MB (predvolene 0 = neobmedzené)
/mail	kontrolovať e-mailové súbory (predvolené)
/no-mail	nekontrolovať e-mailové súbory
/mailbox	kontrolovať e-mailové schránky (predvolené)
/no-mailbox	nekontrolovať e-mailové schránky
/sfx	kontrolovať samorozbaľovacie archívy (predvolené)
/no-sfx	nekontrolovať samorozbaľovacie archívy
/rtp	kontrolovať runtime archívy (predvolené)
/no-rtp	nekontrolovať runtime archívy
/unsafe	kontrolovať potenciálne nebezpečné aplikácie
/no-unsafe	nekontrolovať potenciálne nebezpečné aplikácie (predvolené)
/unwanted	kontrolovať potenciálne nechcené aplikácie
/no-unwanted	nekontrolovať potenciálne nechcené aplikácie (predvolené)
/suspicious	kontrolovať podozrivé aplikácie (predvolené)
/no-suspicious	nekontrolovať podozrivé aplikácie
/pattern	používať signatúry (predvolené)
/no-pattern	nepoužívať signatúry
/heur	zapnúť heuristiku (predvolené)
/no-heur	vypnúť heuristiku
/adv-heur	zapnúť pokročilú heuristiku (predvolené)
/no-adv-heur	vypnúť pokročilú heuristiku
/ext-exclude=EXTENSIONS	vylúčiť z kontroly súborové PRÍPONY oddelené dvojbodkou
/clean-mode=MODE	použiť REŽIM liečenia infikovaných objektov Na výber sú tieto možnosti: • none (predvolené) – nenastane žiadne automatické liečenie. • standard – ecls.exe sa pokúsi o automatické vyliečenie alebo odstránenie infikovaných súborov. • strict – ecls.exe sa pokúsi o automatické vyliečenie alebo odstránenie infikovaných súborov bez zásahu používateľa (pred odstránením súborov sa vám nezobrazí výzva na potvrdenie akcie). • rigorous – ecls.exe odstráni súbory bez pokusu o vyliečenie, a to bez ohľadu na to, o aké súbory ide. • delete – ecls.exe odstráni súbory bez pokusu o vyliečenie, ale nepristúpi k odstráneniu citlivých súborov, ako sú systémové súbory vo Windows.
/quarantine	uložiť kópie infikovaných súborov (pri liečení) do karantény (doplnková akcia pri liečení súborov)

`/no-quarantine`	neukladať kópie infikovaných súborov do karantény

Všeobecné možnosti:

`/help`	zobraziť pomocníka a ukončiť
`/version`	zobraziť informáciu o verzii a ukončiť
`/preserve-time`	zachovať čas posledného prístupu k súborom

Návratové hodnoty:

`0`	nenašla sa žiadna infekcia
`1`	našla sa infekcia, ale bola odstránená
`10`	niektoré súbory nemohli byť skontrolované (a môžu obsahovať infekciu)
`50`	našla sa infekcia
`100`	chyba (návratové hodnoty väčšie ako 100 znamenajú, že súbor nebol skontrolovaný a nemožno ho považovať za čistý)

ESET CMD

Táto funkcia umožňuje používať pokročilé príkazy ecmd. Umožňuje vám importovať a exportovať nastavenia pomocou príkazového riadka (ecmd.exe). Doposiaľ bolo možné importovať a exportovať nastavenia len prostredníctvom grafického používateľského rozhrania. ESET Mail Security nastavenia môžu byť exportované ako súbor *.xml*.

Po povolení ESET CMD sú k dispozícii dve metódy autorizácie:

- **Žiadna** – žiadna autorizácia. Túto metódu neodporúčame, pretože umožňuje importovanie akejkoľvek nepodpísanej konfigurácie, čo môže predstavovať potenciálne riziko.

- **Heslo pre prístup k rozšíreným nastaveniam** – na import konfigurácie zo súboru .xml sa vyžaduje heslo. Tento súbor musí byť podpísaný (bližšie informácie o podpisovaní konfiguračného súboru .xml nájdete nižšie). Predtým, ako môže byť importovaná nová konfigurácia, musí byť zadané heslo špecifikované v Nastaveniach prístupu. Ak nemáte nastavenú ochranu heslom, heslá sa nezhodujú alebo konfiguračný súbor .xml nie je podpísaný, konfigurácia nebude importovaná.

Po povolení ESET CMD môžete používať príkazový riadok na import/export konfigurácie programu ESET Mail Security. Môžete to vykonávať manuálne alebo si vytvoriť skript na účely automatizácie.

Pre použitie pokročilých ecmd príkazov ich budete musieť spúšťať s oprávneniami správcu alebo spustením príkazového riadku systému Windows pomocou možnosti **Spustiť ako správca**. V opačnom prípade sa zobrazí chybové hlásenie **Chyba pri vykonávaní príkazu (Error executing command)**. Pri exportovaní konfigurácie musí tiež existovať cieľový priečinok. Príkaz pre export funguje aj v prípade, že je vypnutá možnosť ESET CMD.

Príkaz pre export nastavení:
```
ecmd /getcfg c:\config\settings.xml
```

Príkaz pre import nastavení:
```
ecmd /setcfg c:\config\settings.xml
```

Pokročilé ecmd príkazy môžu byť spúšťané len lokálne. Spustenie klientskej úlohy **Spustiť príkaz** pomocou nástroja ESET PROTECT nebude fungovať.

Podpisovanie konfiguračných súborov *.xml*:

1. Stiahnite si XmlSignTool.

2. Otvorte príkazový riadok systému Windows použitím možnosti **Spustiť ako správca**.

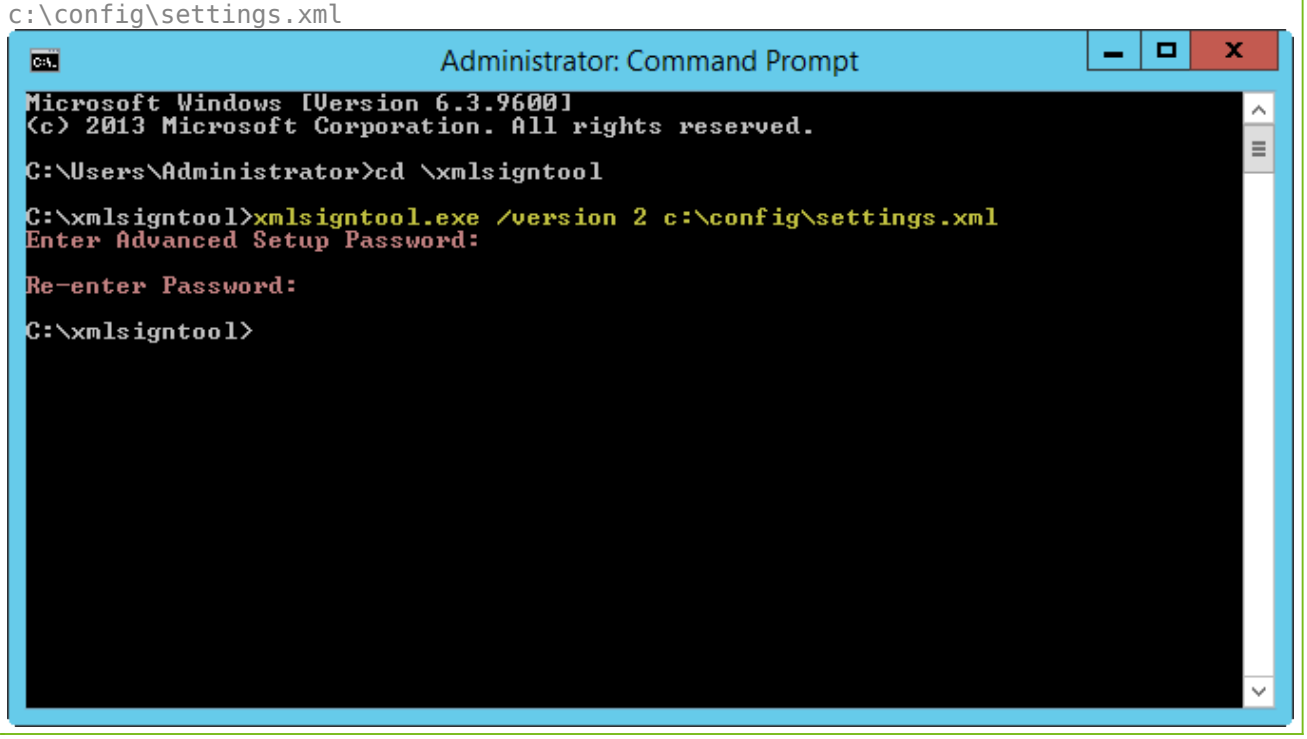
3. Prejdite do priečinka, kde sa nachádza nástroj `xmlsigntool.exe`.

4. Konfiguračný súbor *.xml* podpíšte nasledujúcim príkazom: `xmlsigntool /version 1|2 <xml_file_path>`.

Hodnota parametra `/version` závisí od verzie vášho produktu ESET Mail Security. Pre ESET Mail Security 7 a novšie verzie použite `/version 2`.

5. Po výzve nástroja XmlSignTool zadajte heslo, ktoré máte nastavené v produkte pre ochranu prístupu do Rozšírených nastavení. Váš konfiguračný súbor *.xml* je teraz podpísaný a môže byť pomocou ESET CMD použitý na importovanie v rámci ďalšej inštalácie ESET Mail Security.

Príkaz na podpísanie exportovaného konfiguračného súboru: `xmlsigntool /version 2 c:\config\settings.xml`



Ak sa zmení heslo v rámci Nastavení prístupu a chcete importovať konfiguráciu, ktorá bola podpísaná skôr prostredníctvom starého hesla, môžete podpísať konfiguračný súbor *.xml* znova, a to použitím aktuálneho hesla. Tento postup vám umožní použiť starší konfiguračný súbor bez potreby jeho exportovania na iný počítač, na ktorom je spustený program ESET Mail Security.

ESET RMM

Vzdialený monitoring a správa (RMM) slúži na spravovanie a riadenie softvérových systémov (napr. na stolových počítačoch, serveroch a mobilných zariadeniach) pomocou lokálne nainštalovaného agenta, ktorý je dostupný prostredníctvom MSP (Managed Service Provider).

Zapnúť RMM

Zapne vzdialený monitoring a správu. Nato, aby ste mohli používať nástroj RMM, musíte mať oprávnenia správcu.

Pracovný režim

Z roletového menu vyberte pracovný režim pre RMM:

- **Iba bezpečné operácie** – zapne rozhranie RMM iba pre bezpečné operácie a operácie len na čítanie
- **Všetky operácie** – zapne rozhranie RMM pre všetky operácie

Spôsob overenia

Z roletového menu vyberte spôsob overenia RMM:

- **Žiadne** – nebude vykonaná žiadna kontrola cesty k aplikácii, *ermm.exe* môžete spustiť pomocou akejkoľvek aplikácie.
- **Cesta k aplikácii** – vyberte aplikáciu, ktorá bude mať povolené spúšťať *ermm.exe*.

Súčasťou predvolenej inštalácie ESET Mail Security je súbor *ermm.exe*, ktorý sa nachádza v adresári produktu ESET Mail Security (predvolené umiestnenie je *c:\Program Files\ESET\ESET Mail Security*). *ermm.exe* zabezpečuje výmenu dát s pluginom RMM, ktorý komunikuje s agentom RMM prepojeným so serverom RMM.

- *ermm.exe* – nástroj príkazového riadka vyvinutý spoločnosťou ESET, ktorý umožňuje správu produktov určených pre koncové zariadenia a zároveň komunikáciu s akýmkoľvek pluginom RMM.
- Plugin RMM – aplikácia tretej strany, ktorá beží lokálne na koncovom zariadení so systémom Windows. Tento plugin bol navrhnutý tak, aby komunikoval s konkrétnym agentom RMM (napr. Kaseya) a s *ermm.exe*.
- Agent RMM – aplikácia tretej strany (napr. Kaseya), ktorá beží lokálne na koncovom zariadení so systémom Windows. Agent komunikuje s pluginom RMM a serverom RMM.
- Server RMM – beží ako služba na serveri tretej strany. Medzi podporované systémy RMM patria Kaseya, Labtech, Autotask, Max Focus a Solarwinds N able.

Viac informácií o ESET RMM v produkte ESET Mail Security nájdete v našom článku Databázy znalostí spoločnosti ESET.

Plugin ESET Direct Endpoint Management pre riešenia RMM tretích strán

Server RMM beží ako služba na serveri tretej strany. Viac informácií nájdete v online používateľských príručkách ESET Direct Endpoint Management:

- Plugin ESET Direct Endpoint Management pre ConnectWise Automate
- Plugin ESET Direct Endpoint Management pre DattoRMM
- ESET Direct Endpoint Management pre Solarwinds N-Central
- ESET Direct Endpoint Management pre NinjaRMM

Licencia

ESET Mail Security sa pripája na licenčný server ESET niekoľkokrát za hodinu s cieľom vykonať kontrolu. Parameter **Interval kontroly** je predvolene nastavený ako **Automatický**. Ak chcete znížiť objem sieťovej komunikácie v dôsledku kontrol licencií, zmeňte Interval kontroly na **Obmedzený** a kontrola licencií sa bude vykonávať iba raz denne (a tiež po reštarte servera).

Ak je Interval kontroly nastavený ako **Obmedzený**, všetky zmeny ESET Mail Security, ktoré súvisia s licenciou a boli uskutočnené prostredníctvom nástrojov ESET Business Account a ESET MSP Administrator, sa môžu prejaviť až po jednom dni.

Poskytovateľ WMI

Funkcia Windows Management Instrumentation (WMI) je implementáciou Web-Based Enterprise Management (WBEM) od spoločnosti Microsoft, ktorá je snahou o vytvorenie technologického štandardu pre prístup k informáciám na vzdialenú správu softvéru vo firemnom prostredí.

Viac informácií nájdete na webovej stránke http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx.

ESET Poskytovateľ WMI

Účel funkcie poskytovateľa WMI je povolenie vzdialeného sledovania produktov spoločnosti ESET vo firemnom prostredí bez nutnosti inštalácie ďalšieho softvéru od spoločnosti ESET. Sprístupnením základných informácií o produkte ako napr. stavu ochrany, štatistík cez WMI rozširuje možnosti správy pre správcov firemných sietí.

Správca môže na sledovanie stavu produktov spoločnosti ESET využiť niekoľko metód prístupu, ktoré WMI ponúka (príkazový riadok, skripty, monitorovacie nástroje tretích strán).

Súčasná implementácia poskytuje len prístup na čítanie k základným informáciám, akými sú nainštalované súčasti programu, stav ochrany, štatistiky kontroly, protokoly.

WMI poskytovateľ vám umožňuje použitie infraštruktúry a nástrojov Windows WMI na sledovanie stavu a protokolov bezpečnostných produktov.

Poskytnuté údaje

Všetky triedy WMI týkajúce sa produktov ESET sa nachádzajú na adrese „root\ESET“. Podporované sú nasledujúce triedy:

Všeobecné

- ESET_Product
- ESET_Features
- ESET_Statistics

Protokoly

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_HIPSLog
- ESET_URLLog
- ESET_DevCtrlLog
- ESET_GreylistLog
- ESET_MailServeg
- ESET_HyperVScanLogs
- ESET_HyperVScanLogRecords

ESET_Product

Trieda ESET_Product môže mať len jednu inštanciu. Vlastnosti tejto triedy popisujú základné informácie o nainštalovanom produkte ESET:

- ID – skratka (identifikátor) vyjadrujúca typ produktu, napríklad „emsl“.
- Name – názov produktu, napríklad „ESET Mail Security“.
- FullName – úplný názov produktu, napríklad „ESET Mail Security pre IBM Domino“.
- Version – verzia produktu, napríklad „6.5.14003.0“.
- VirusDBVersion – verzia detekčného jadra, napríklad „14533 (20161201)“.
- VirusDBLastUpdate – dátum a čas poslednej aktualizácie detekčného jadra. Reťazec obsahuje časovú pečiatku vyjadrenú vo WMI formáte, napríklad „20161201095245.000000+060“.
- LicenseExpiration – dátum skončenia platnosti licencie. Reťazec obsahuje časovú pečiatku vyjadrenú vo WMI formáte.
- KernelRunning – hodnota typu boolean vyjadrujúca, či je služba „ekrn“ spustená na počítači (napr. „TRUE“).
- StatusCode – číslo vyjadrujúce stav ochrany produktu: 0 – Zelený (V poriadku), 1 – Žltý (Varovanie), 2 – Červený (Chyba)
- StatusText – správa vyjadrujúca dôvod zmeneného stavu ochrany, ak je stav ochrany iný ako 0.

ESET_Features

Počet inštancií sa rovná počtu funkcií produktu ESET. Každá inštancia obsahuje:

- Name – názov funkcie (zoznam názvov je k dispozícii nižšie).
- Status – stav funkcie: 0 – neaktívna, 1 – vypnutá, 2 – zapnutá

Zoznam reťazcov predstavujúcich funkcionality produktu:

- CLIENT_FILE_AV – rezidentná ochrana súborového systému.
- CLIENT_WEB_AV – ochrana prístupu na web.
- CLIENT_DOC_AV – ochrana dokumentov.
- CLIENT_NET_FW – firewall.
- CLIENT_EMAIL_AV – antivírusová ochrana e-mailového klienta.
- CLIENT_EMAIL_AV – antispamová ochrana e-mailového klienta.
- SERVER_FILE_AV – rezidentná ochrana súborov na chránenom serveri, napríklad súborov v databázach obsahu SharePointu v prípade programu ESET Mail Security.
- SERVER_EMAIL_AV – antivírusová ochrana e□mailov na chránenom serveri, napríklad e□maily na serveri Microsoft Exchange alebo IBM Domino.
- SERVER_EMAIL_AV – antispamová ochrana e□mailov na chránenom serveri, napríklad e□maily na serveri Microsoft Exchange alebo IBM Domino.
- SERVER_GATEWAY_AV – antivírusová ochrana sieťových protokolov v bráne.
- SERVER_GATEWAY_AS – antispamová ochrana sieťových protokolov v bráne.

ESET_Statistics

Počet inštancií sa rovná počtu typov kontroly v produkte ESET. Každá inštancia obsahuje:

- Scanner – reťazec pre každý druh kontroly v programe, napríklad „CLIENT_FILE“.
- Total – celkový počet skontrolovaných súborov.
- Infected – počet nájdených infikovaných súborov.
- Cleaned – počet vyliečených súborov.
- Timestamp – čas poslednej zmeny štatistík. Je vyjadrený vo WMI formáte, napríklad „20130118115511.000000+060“.
- ResetTime – čas posledného vynulovania počítadla štatistík. Je vyjadrený vo WMI formáte, napríklad „20130118115511.000000+060“.

Zoznam reťazcov predstavujúcich typy kontroly v produkte:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

ESET_ThreatLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Zachytené infiltrácie“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Scanner – typ kontroly, pri ktorej bol protokol vytvorený.
- ObjectType – typ objektu, ktorý vytvoril tento protokol.
- ObjectName – názov objektu, ktorý vytvoril tento protokol.
- Threat – názov hrozby/infiltrácie, ktorá bola odhalená v objekte pomocou vlastností ObjectName a ObjectType.
- Action – akcia vykonaná po identifikovaní hrozby.
- User – používateľský účet, v ktorom bol protokol vytvorený.
- Information – dodatočné informácie o udalosti.
- Hash – hash objektu, ktorý vytvoril tento protokol.

ESET_EventLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Udalosti“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Module – názov modulu, ktorý vytvoril tento protokol.

- Event – popis udalosti.
- User – používateľský účet, v ktorom bol protokol vytvorený.

ESET_ODFileScanLogs

Počet inštancií sa rovná počtu záznamov v protokole typu „Kontrola počítača“. Ide o ekvivalent protokolov kontroly počítača v používateľskom prostredí. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- Targets – cieľové priečinky/objekty kontroly.
- TotalScanned – celkový počet skontrolovaných objektov.
- Infected – počet nájdených infikovaných objektov.
- Cleaned – počet vyliečených objektov.
- Status – stav procesu kontroly.

ESET_ODFileScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_ODFileScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol počítača. Pri filtrovaní inštancie konkrétneho protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- LogID – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_ODFileScanLogs).
- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Log – správa z protokolu.

ESET_ODServerScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly servera“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- Targets – cieľové priečinky/objekty kontroly.
- TotalScanned – celkový počet skontrolovaných objektov.
- Infected – počet nájdených infikovaných objektov.

- Cleaned – počet vyliečených objektov.
- RuleHits – celkový počet uplatnení pravidla.
- Status – stav procesu kontroly.

ESET_ODServerScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_ODServerScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol počítača. Pri filtrovaní inštancie konkrétneho protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- LogID – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_ ODServerScanLogs).
- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Log – správa z protokolu.

ESET_SmtpProtectionLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Protokol SMTP ochrany“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- HELODomain – názov reťazca HELO.
- IP – IP adresa zdroja.
- Sender – odosielateľ e-mailu.
- Recipient – príjemca e-mailu.
- ProtectionType – typ použitej ochrany.
- Action – vykonaná akcia.
- Reason – dôvod vykonania akcie.
- TimeToAccept – počet minút, po ktorých bude e-mail prijatý.

ESET_HIPSLog

Počet inštancií sa rovná počtu záznamov v protokole typu „HIPS“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Application – zdrojová aplikácia.
- Target – typ operácie.
- Action – akcia vykonaná modulom HIPS (napr. povolenie, zamietnutie atď.).
- Rule – názov pravidla, na základe ktorého je akcia vykonaná.
- AdditionalInfo

ESET_URLLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Filtrované webové stránky“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- URL – URL adresa.
- Status – vyjadruje, čo sa stalo s URL adresou (napr. „Blokované webovou kontrolou“).
- Application – aplikácia, ktorá sa pokúsila získať prístup k URL adrese.
- User – používateľský účet, pod ktorým bola aplikácia spustená.

ESET_DevCtrlLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Správa zariadení“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Device – názov zariadenia.

- User – názov používateľského účtu.
- UserSID – SID používateľského účtu.
- Group – názov skupiny používateľov.
- GroupSID – SID skupiny používateľov.
- Status – vyjadruje, čo sa stalo so zariadením (napr. „Blokovaný zápis“).
- DeviceDetails – dodatočné informácie o zariadení.
- EventDetails – dodatočné informácie o udalosti.

ESET_MailServerLog

Počet inštancií sa rovná počtu záznamov v protokole typu „E-mailový server“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- IPAddr – IP adresa zdroja.
- HELODomain – názov reťazca HELO.
- Sender – odosielateľ e-mailu.
- Recipient – príjemca e-mailu.
- Subject – predmet e□mailovej správy.
- ProtectionType – typ ochrany, ktorá vykonala akciu zaznamenanú v protokole (napr. antimalvérová ochrana, antispam alebo pravidlá).
- Action – vykonaná akcia.
- Reason – dôvod, prečo bola akcia vykonaná konkrétnym typom ochrany („ProtectionType“) pre daný objekt.

ESET_HyperVScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly Hyper-V“. Ide o ekvivalent protokolov kontroly Hyper-V v používateľskom prostredí. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- Targets – cieľové počítače/disky/zväzky, pre ktoré bude vykonaná kontrola.

- TotalScanned – celkový počet skontrolovaných objektov.
- Infected – počet nájdených infikovaných objektov.
- Cleaned – počet vyliečených objektov.
- Status – stav procesu kontroly.

ESET_HyperVScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_HyperVScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol Hyper-V. Pri filtrovaní inštancie konkrétneho protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- LogID – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_HyperVScanLogs).
- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Log – správa z protokolu.

ESET_NetworkProtectionLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Ochrana siete“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Event – udalosť, ktorá spúšťa akciu ochrany siete.
- Action – akcia vykonaná ochranou siete.
- Source – zdrojová adresa sieťového zariadenia.
- Target – cieľová adresa sieťového zariadenia.
- Protocol – protokol sieťovej komunikácie.
- RuleOrWormName – názov pravidla alebo červa súvisiaceho s udalosťou.
- Application – aplikácia, ktorá iniciovala sieťovú komunikáciu.
- User – používateľský účet, v ktorom bol protokol vytvorený.

ESET_SentFilesLog

Počet inštancií sa rovná počtu záznamov v protokole typu „Odoslané súbory“. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo záznamu protokolu.
- Timestamp – dátum a čas vytvorenia záznamu protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Sha1 – Sha-1 hash odoslaného súboru.
- File – odoslaný súbor.
- Size – veľkosť odoslaného súboru.
- Category – kategória odoslaného súboru.
- Reason – dôvod odoslania súboru.
- SentTo – oddelenie spoločnosti ESET, kde bol súbor odoslaný.
- User – používateľský účet, v ktorom bol protokol vytvorený.

ESET_OneDriveScanLogs

Počet inštancií sa rovná počtu spustení „Kontroly OneDrive“. Ide o ekvivalent protokolov kontroly OneDrive v používateľskom prostredí. Každá inštancia obsahuje:

- ID – jedinečné identifikačné číslo protokolu OneDrive.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- Targets – cieľové priečinky/objekty kontroly.
- TotalScanned – celkový počet skontrolovaných objektov.
- Infected – počet nájdených infikovaných objektov.
- Cleaned – počet vyliečených objektov.
- Status – stav procesu kontroly.

ESET_OneDriveScanLogRecords

Počet inštancií sa rovná počtu inštancií protokolov kontroly v triede ESET_OneDriveScanLogs. Inštancie tejto triedy poskytujú záznamy protokolov všetkých kontrol OneDrive. Pri filtrovaní inštancie konkrétneho protokolu kontroly použite vlastnosť LogID. Každá inštancia obsahuje:

- LogID – identifikačné číslo protokolu kontroly, ku ktorému patrí záznam (identifikačné číslo inštancie triedy ESET_OneDriveScanLogs).

- ID – jedinečné identifikačné číslo protokolu OneDrive.
- Timestamp – dátum a čas vytvorenia protokolu (vo WMI formáte).
- LogLevel – závažnosť záznamu protokolu vyjadrená číslom [0 – 8]. Čísla vyjadrujú nasledujúce úrovne: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical.
- Log – správa z protokolu.

Prístup k poskytnutým údajom

Nasleduje niekoľko príkladov, ako pristupovať k dátam cez ESET WMI z príkazového riadka Windows PowerShell, ktoré by mali fungovať na všetkých verziách operačného systému Windows. Sú však dostupné aj iné cesty ako sa dostať k týmto dátam pomocou skriptovacích jazykov alebo iných nástrojov.

Cez príkazový riadok bez skriptov

Nástroj príkazového riadka `wmic` možno použiť na prístup k rôznym vopred definovaným WMI triedam.

Zobrazenie kompletných informácií o produkte na lokálnom počítači:

```
wmic /namespace:\\root\ESET Path ESET_Product
```

Zobrazenie čísla verzie produktu na lokálnom počítači:

```
wmic /namespace:\\root\ESET Path ESET_Product Get Version
```

Zobrazenie kompletných informácií o produkte na vzdialenom počítači s IP adresou 10.1.118.180:

```
wmic /namespace:\\root\ESET /node:10.1.118.180 /user:Administrator Path ESET_Product
```

PowerShell

Zobrazenie kompletných informácií o produkte na lokálnom počítači:

```
Get-WmiObject ESET_Product -namespace 'root\ESET'
```

Zobrazenie kompletných informácií o produkte na vzdialenom počítači s IP adresou 10.1.118.180:

```
$cred = Get-
Credential # promts the user for credentials and stores it in the variable
Get-WmiObject ESET_Product -namespace 'root\ESET' -computername '10.1.118.180' -
cred $cred
```

Ciele kontroly pre konzolu na správu produktov ESET

Táto funkcia umožňuje nástroju ESET PROTECT používať ciele kontroly (Manuálnej kontroly databáz e-mailových schránok a Kontroly Hyper-V) pri spustení klientskej úlohy Kontrola servera na serveri s nainštalovaným produktom ESET Mail Security. Nastavenie cieľov kontroly v rámci nástroja ESET PROTECT je dostupné len v prípade, že máte nainštalovaného ESET Management Agenta, v opačnom prípade bude táto možnosť nedostupná.

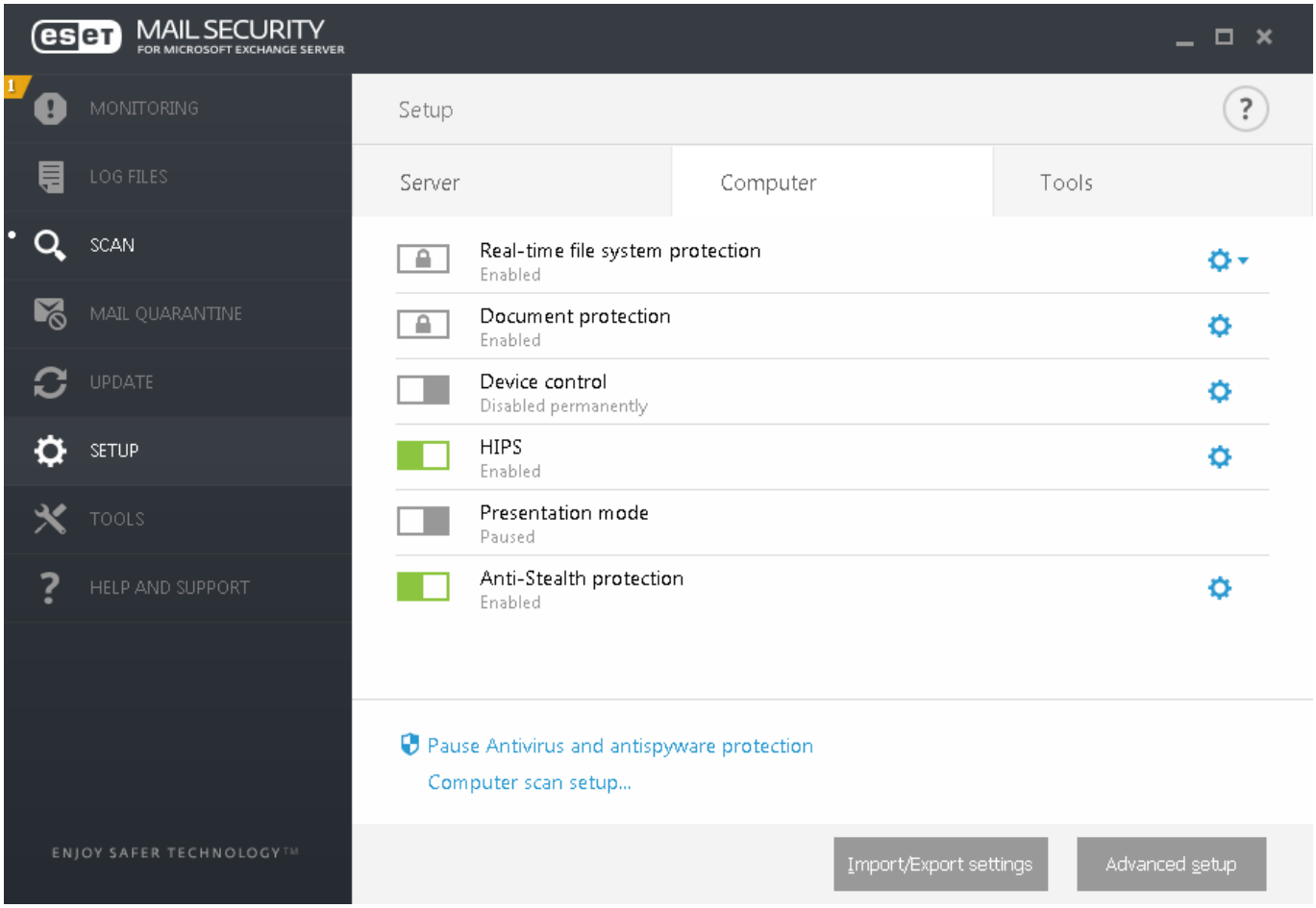
Ak povolíte **Generovanie zoznamu cieľov**, ESET Mail Security vytvorí zoznam dostupných cieľov kontroly. Tento zoznam je vytváraný v pravidelných intervaloch na základe zadaného **Intervalu aktualizácie**.

> Po prvom použití funkcie **Generovať zoznam cieľov** bude nástroju ESET PROTECT trvať približne polovicu z času zadaného pre **Interval aktualizácie**, kým si vygenerovaný zoznam cieľov preberie. Napríklad, ak je **Interval aktualizácie** nastavený na 60 minút, zoznam cieľov kontroly bude v nástroji ESET PROTECT k dispozícii približne po 30 minútach. Ak potrebujete v ESET PROTECT získať zoznam cieľov skôr, nastavte kratší interval aktualizácie. Dobu aktualizácie môžete kedykoľvek zvýšiť.

Ak chce ESET PROTECT spustiť klientsku úlohu **Kontrola servera**, vytvorí zoznam a umožní vám vybrať ciele Kontroly Hyper-V pre daný server.

Režim prepísania

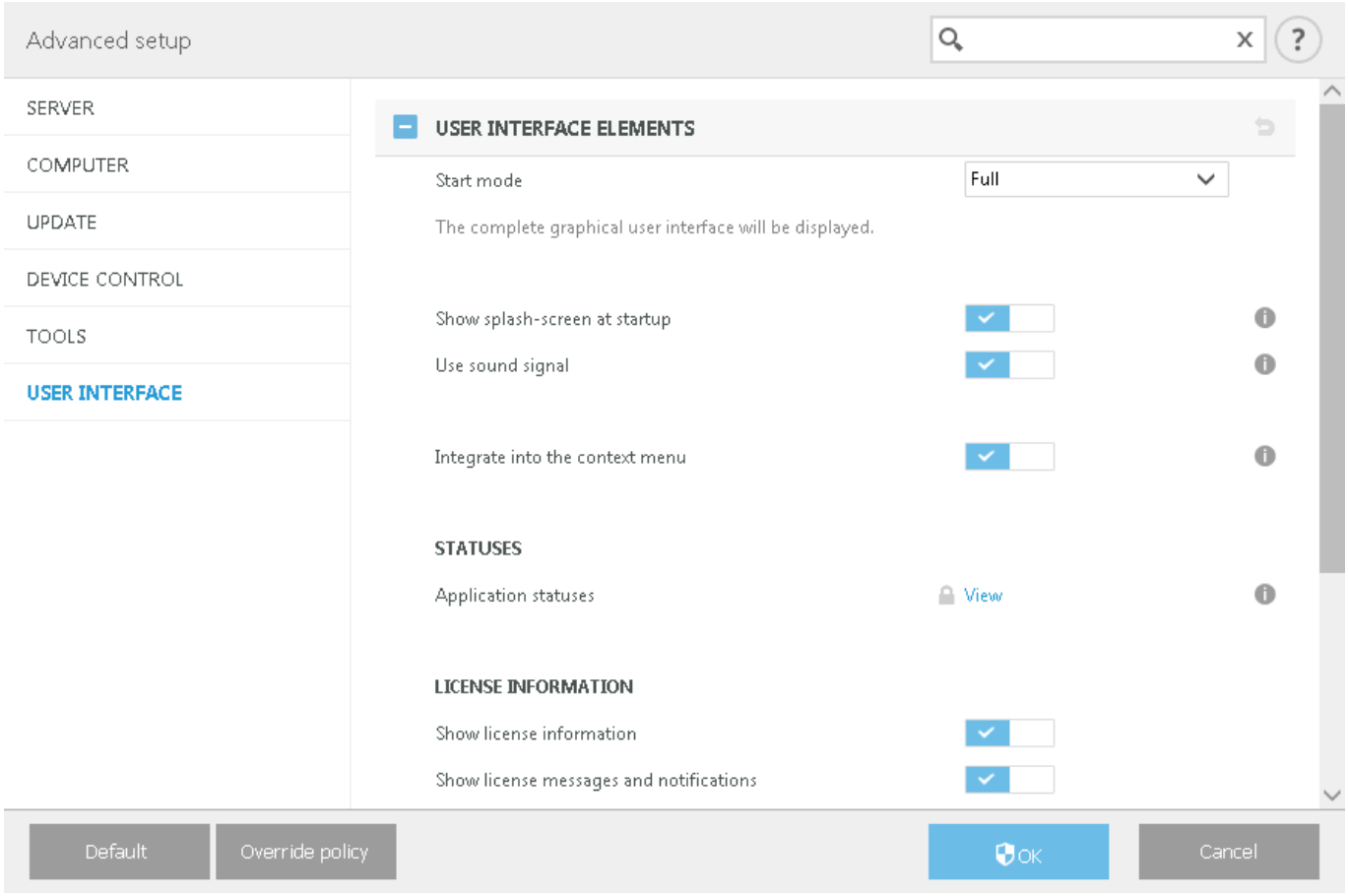
Ak máte na ESET Mail Security aplikovanú politiku ESET PROTECT, namiesto prepínača Povoliť/Zakázať v sekcii Nastavenia bude zobrazená ikona zámku  , podobne ako v prípade prepínača v okne **Rozšírené nastavenia**.



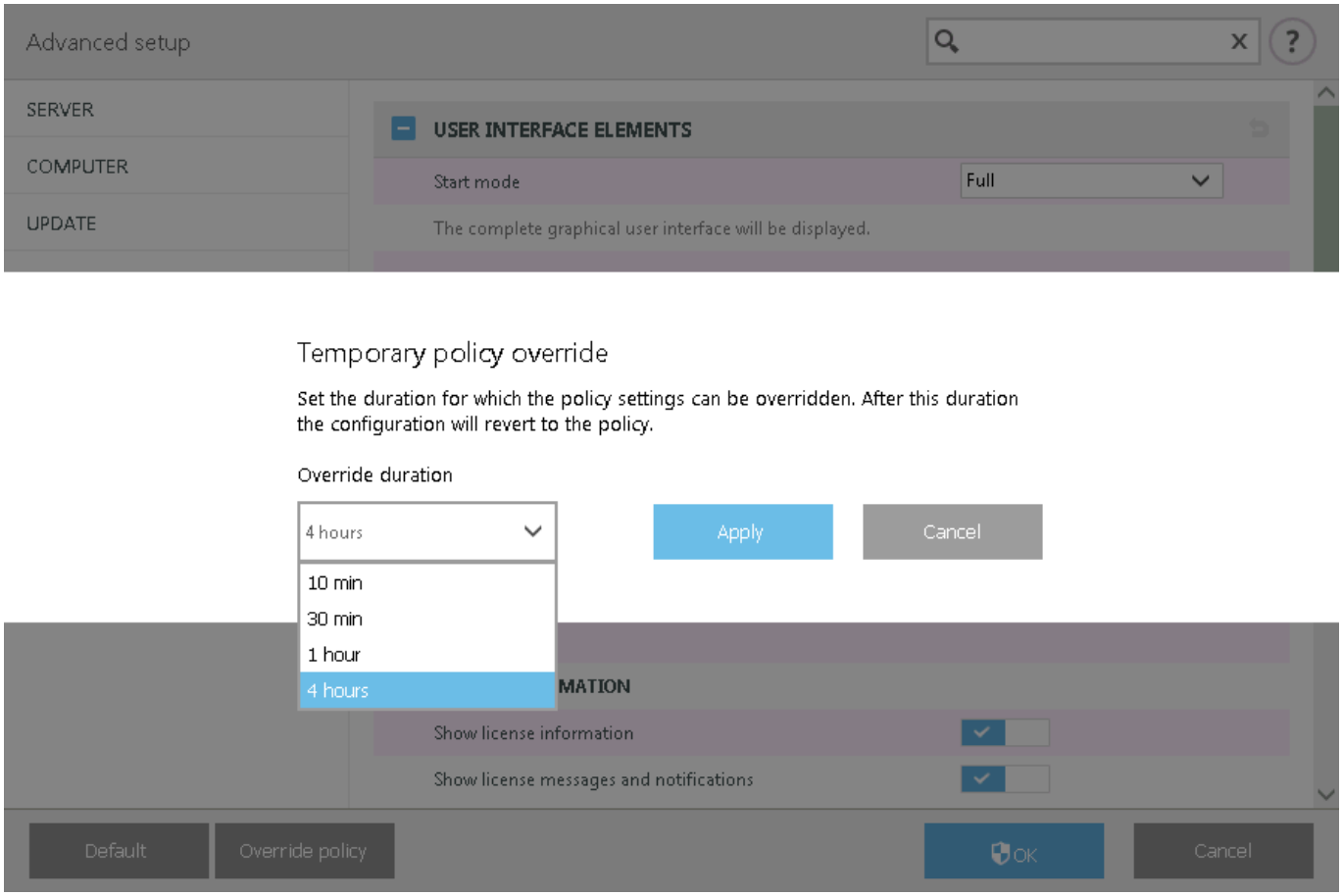
Za normálnych okolností nastavenia konfigurované prostredníctvom politiky ESET PROTECT nie je možné modifikovať. Režim prepísania vám umožňuje dočasne odomknúť tieto nastavenia. Je však potrebné povoliť **Režim prepísania** pomocou politiky ESET PROTECT.

Prihláste sa do ESET PROTECT Web Console, prejdite do sekcie **Politiky** a vyberte a upravte existujúcu politiku, ktorá je aplikovaná na ESET Mail Security, prípadne vytvorte novú politiku. V **Nastaveniach** kliknite na **Režim prepísania**, povoľte ho a dokončite konfiguráciu vrátane Typu autentifikácie (Používateľ Active Directory alebo Heslo).

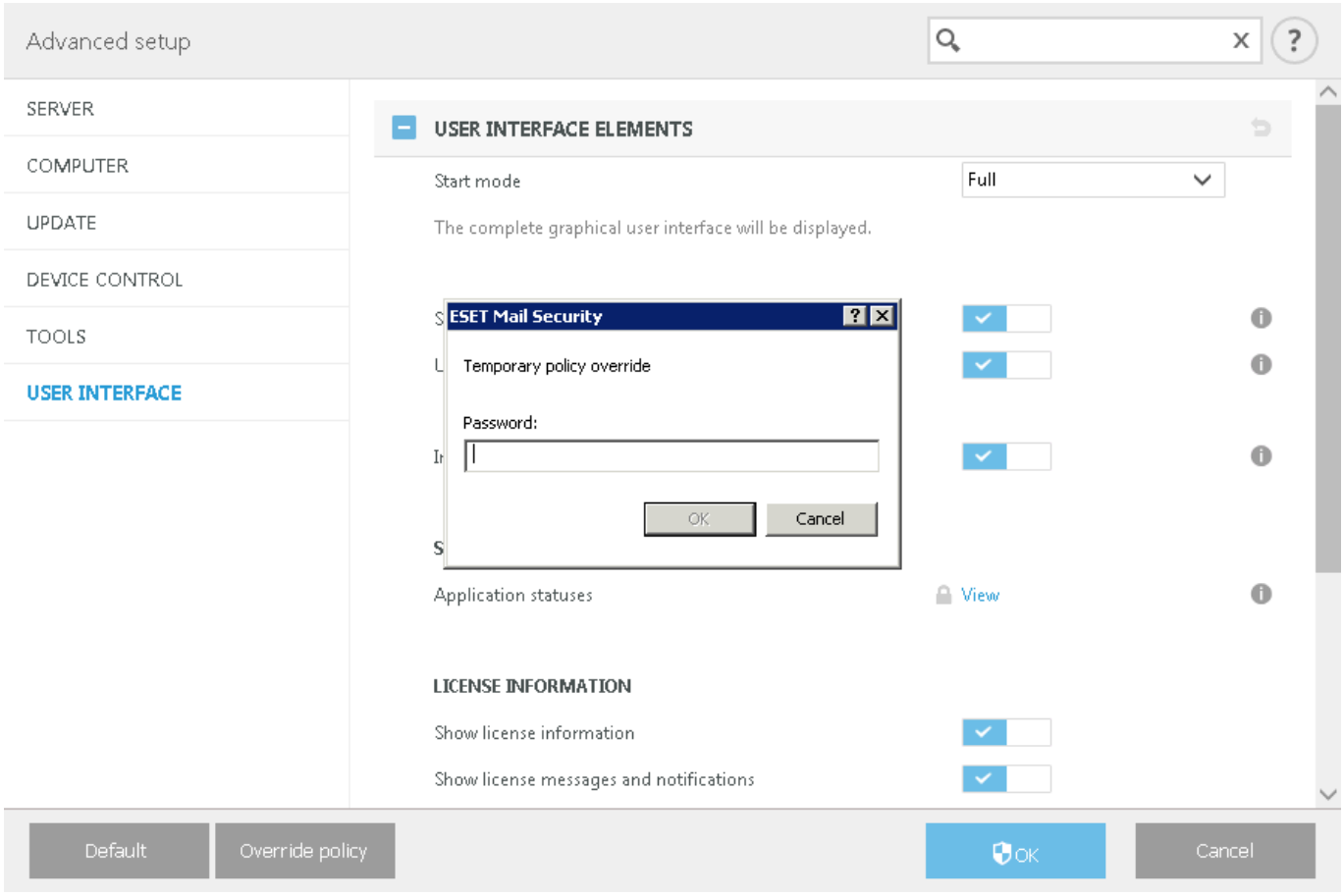
Po úprave politiky alebo aplikovaní novej politiky na ESET Mail Security sa v okne **Rozšírené nastavenia** zobrazí tlačidlo Prepísať politiku.



Kliknite na tlačidlo **Prepísať politiku**, nastavte dĺžku trvania a kliknite na **Uložiť**.



Ak ste ako typ autentifikácie vybrali možnosť **Heslo**, zadajte heslo pre prepísanie politiky.



Po uplynutí stanovenej doby trvania režimu prepísania budú akékoľvek zmeny vykonané v konfigurácii vrátené

späť na pôvodné nastavenia vynútené politikou ESET PROTECT. Pred tým, ako doba trvania režimu prepísania uplynie, sa zobrazí oznámenie.

Režim prepísania však môžete ukončiť kedykoľvek použitím možnosti **Ukončiť prepisovanie** v sekcii Monitorovanie alebo v okne Rozšírené nastavenia.

Protokoly

Táto sekcia vám umožňuje upravovať nastavenia týkajúce sa zapisovania do protokolov v rámci programu ESET Mail Security.

Zapisovať záznamy do protokolu

Záznamy sú zapisované do protokolu udalostí (*C:\ProgramData\ESET\ESET Security\Logs*) a sú zobrazené v časti Protokoly. Pomocou prepínačov povolíte alebo zakážete konkrétne funkcie:
Zaznamenávať do protokolu chyby prenosu e□mailov
Ak je táto možnosť povolená a vyskytujú sa problémy na vrstve prenosu e-mailov, chybové hlásenia budú zapisované do protokolu Udalosti.
Zaznamenávať do protokolu výnimky prenosu e□mailov
Ak sa vyskytujú akékoľvek výnimky na vrstve prenosu e-mailov, podrobnosti o tejto skutočnosti budú zapísané do protokolu Udalosti.

Filter zápisu do protokolu

Keďže sú predvolene aktivované všetky možnosti zapisovania do protokolu, bude dochádzať k vytváraniu veľkého množstva dát. Odporúčame vám deaktivovať zozbieravanie dát z tých komponentov, ktoré nesúvisia s vaším aktuálne riešeným problémom.

> Ak chcete zapnúť zapisovanie do protokolov, je potrebné najprv povoliť **Diagnostické zapisovanie do protokolu** na úrovni programu v hlavnom menu > **Nastavenia** > Nástroje. Po povolení zapisovania do protokolov bude ESET Mail Security vytvárať podrobné protokoly v závislosti od funkcií povolených v tejto sekcii.

Pomocou prepínačov povolíte alebo zakážete konkrétne funkcie. Tieto možnosti je možné aj kombinovať v závislosti od dostupnosti jednotlivých komponentov v rámci ESET Mail Security.

- Diagnostické protokoly prenosu e□mailov

> Pri riešení problémov s kontrolou databáz spustenou pri bežnej prevádzke odporúčame deaktivovať funkciu **Diagnostické protokoly prenosu e□mailov**. V opačnom prípade bude vo výslednom protokole nadmerné množstvo dát, ktoré skomplikuje jeho analýzu.

- **Diagnostické protokoly manuálnej kontroly databáz** – zapisovanie podrobných informácií do protokolov, hlavne na účely riešenia problémov.
- **Diagnostické protokoly klastra** – protokoly klastra budú súčasťou diagnostických protokolov.
- **Diagnostické protokoly antispamového jadra** – v prípade potreby riešenia problémov budú v protokoloch zahrnuté podrobné informácie o antispamovom jadre. Táto možnosť slúži na povolenie zapisovania podrobných informácií o antispamovom jadre do protokolov na účely diagnostiky. Antispamové jadro nevyužíva protokol Udalosti (súbor warnlog.dat), čiže príslušné záznamy si nie je možné prezerať v sekcii Protokoly. Záznamy sú zapisované priamo do vyhradeného textového súboru (napr. C:\ProgramData\ESET\ESET Mail Security\Logs\antispam.0.log), aby boli všetky diagnostické dáta antispamového jadra uchovávané na jednom mieste. Vďaka tomu nie je oslabený výkon ESET Mail Security v prípade zvýšeného príjmu e-mailov.

Protokoly

V tejto sekcii je možné určiť spôsob spravovania protokolov. Toto je dôležité hlavne z hľadiska šetrenia miesta na disku. Predvolené nastavenia umožňujú automatické mazanie starších protokolov s cieľom šetriť miesto na disku.

Automaticky zmazať záznamy

Protokoly staršie ako nastavená hodnota (pozri ďalej) budú automaticky zmazané.

Zmazať záznamy staršie ako (počet dní)

Zadajte počet dní.

Automaticky odstraňovať staré záznamy, ak je prekročená veľkosť protokolu

Ak veľkosť protokolu prekročí **maximálnu veľkosť protokolu [MB]**, staré protokoly budú odstránené, kým nebude dosiahnutá **redukovaná veľkosť protokolu [MB]**.

Zálohovať automaticky vymazané protokoly

Automaticky vymazané protokoly a súbory budú zálohované do vybraného adresára a komprimované do ZIP archívu, ak komprimovanie povolíte.

Zálohovať diagnostické protokoly

Diagnostické protokoly budú automaticky zálohované. Ak táto možnosť nie je povolená, diagnostické protokoly nebudú zálohované.

Priečinok na zálohy

Priečinok na ukladanie záloh protokolov. Môžete povoliť komprimovanie zálohy do ZIP archívu.

Automaticky optimalizovať protokoly

Táto možnosť slúži na automatickú defragmentáciu protokolov, ak počet nevyužitých záznamov prekročí definovaný pomer v percentách nastavený v poli **Ak počet nepoužívaných záznamov prekročí (%)**. Kliknite na **Optimalizovať** pre spustenie defragmentácie protokolov. Defragmentácia odstraňuje prázdne záznamy v protokoloch, čím sa zefektívni a zrýchli práca s nimi. Viditeľné zlepšenie práce s protokolmi po optimalizácii je očividné hlavne pri väčších množstvách záznamov v protokoloch.

Zapnúť textový protokol

Túto možnosť použite v prípade, ak chcete ukladať protokoly v odlišnom formáte ako v prípade Protokolov:

- **Cieľový adresár** – adresár, v ktorom budú uložené protokoly (platí len pre **Text**/**CSV**). Každá skupina protokolov má vlastný súbor s predvoleným názvom (napríklad *virlog.txt* sú protokoly skupiny Zachytené infiltrácie uložené vo formáte obyčajného textu).
- **Typ** – formát **Text** ukladá protokoly do textového súboru, dáta sú oddelené tabulátormi. Formát **CSV** tvoria tiež textové súbory, avšak oddelené čiarkami. Ak vyberiete možnosť **Udalosť**, protokoly budú ukladané v denníku udalostí systému Windows, ktorý je dostupný v Zobrazovači udalostí nachádzajúcom sa v Ovládacom paneli.
- **Odstrániť všetky protokoly** – vymaže všetky protokoly označené v roletovom menu **Typ**.

> Na urýchlenie riešenia problémov vás môžu pracovníci technickej podpory spoločnosti ESET požiadať o zaslanie protokolov z vášho počítača. Nástroj ESET Log Collector zjednodušuje zozbieranie potrebných údajov. Viac informácií o nástroji ESET Log Collector nájdete v našom článku Databázy znalostí spoločnosti ESET.

Protokol auditu

Umožňuje vám sledovať zmeny v konfigurácii produktu alebo v jeho stave ochrany. Keďže zmeny v konfigurácii produktu môžu výrazne ovplyvniť jeho fungovanie, sledovanie zmien môže byť užitočné z pohľadu auditu. Záznamy o zmenách nájdete v sekcii **Protokoly** > Protokol auditu.

Export protokolov

Exportovať do protokolov aplikácií a služieb Windows
Umožňuje duplikovať záznamy z protokolu ochrany e-mailových serverov do denníkov aplikácií a služieb. Pre zobrazenie protokolu ochrany e-mailových serverov otvorte **Zobrazovač udalostí** systému Windows (Event Viewer) a prejdite do sekcie **Applications and Services Logs** > **ESET** > **Security** > **ExchangeServer** > **MailProtection**. Applications and Services Logs sú podporované na systéme Microsoft Windows Server 2008 R2 SP1 a novších systémoch.
Exportovať na syslog server
Protokoly ochrany e-mailových serverov je možné duplikovať na syslog server vo formáte Common Event Format (CEF). CEF je štandardizovaný rozšíriteľný textový formát, ktorý uľahčuje zhromažďovanie a agregáciu dát na neskoršiu analýzu prostredníctvom systému na správu podniku (EMS). V tomto prípade ho môžete použiť so Security Information and Event Management (SIEM) riešeniami a riešeniami na správu protokolov, ako je napríklad Micro Focus ArcSight. Podrobnosti o exportovaných poliach udalostí vrátane ich popisu nájdete v kapitole Mapovanie udalostí syslogu.
Adresa servera
Zadajte IP adresu alebo názov hostiteľa servera. V prípade ArcSight vyberte server, kde je nainštalovaný SmartConnector.
Protokol
Vyberte protokol, ktorý bude použitý – TCP alebo UDP.
Port
Predvolená hodnota je 514 pre oba protokoly.
Exportovať do súboru
Umožňuje exportovať protokoly lokálne do súboru vo formáte CEF. Kapacita úložiska protokolov je obmedzená, preto sa používa cyklické zapisovanie do protokolu. Záznamy sa do súborov zapisujú sekvenčne (od `mailserver.0.log` po `mailserver.9.log`). Najnovší záznam je uložený v `mailserver.0.log` a hneď ako dosiahne limit veľkosti, najstarší súbor `mailserver.9.log` bude vymazaný a ostatné súbory postupne premenované (`mailserver.0.log` bude premenovaný na `mailserver.1.log` atď.).
Cesta k súboru
Predvolená cesta je C:\ProgramData\ESET\ESET Security\Logs. Toto umiestnenie môžete v prípade potreby zmeniť.

Mapovanie udalostí syslogu

Nasledujúce tabuľky ukazujú mapovanie udalostí z riešenia ESET Mail Security do dátových polí nástroja ArcSight. Tabuľky poskytujú referenčné informácie o tom, aké data sa prostredníctvom SmartConnectora prenášajú do nástroja ArcSight.

Header		
Device Vendor	"ESET"	
Device Product	"EMSX"	"EMSX" or "ESET Mail Security for MS Exchange Server"
Device Version	e.g. "7.1.10005.0"	
Device Event Class ID	e.g. "101"	Device Event Category unique identifier: 100-199 malware 200-299 phish 300-399 spam 400-499 policy
Event Name	e.g. "MailScanResult: malware"	A brief description of what happened in the event: MailScanResult: malware MailScanResult: phishing link MailScanResult: spam MailScanResult: policy

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
rt	deviceReceiptTime	Time event was generated	The time at which the event was generated, in milliseconds since Jan 1st 1970
src	sourceAddress	Sender's IP	IP address of the sending mail server
shost	sourceHostName (1023)	Sender's HELO domain	HELO domain of the sending mail server
flexString1	flexString1	Message-ID	Message-ID header from the email
dhost	destinationHostName (1023)	Receiving server	Hostname of the machine that received the communication
msg	message (1023)	Message subject	Subject of the message, from the RFC5233 header "Subject:"
suser	sourceUserName (1023)	SMTP sender	SMTP sender of the email (MAIL FROM)
duser	destinationUserName (1023)	SMTP recipient(s)	SMTP recipient(s) of the email (RCPT TO)
act	deviceAction (63)	Action taken	Action taken (cleaned, quarantined, etc.)
cat	deviceEventCategory (1023)	Detection category	Most significant detection (malware >> phish >> spam >> SPF/DKIM >> policy)
sourceServiceName	sourceServiceName	Type of protection	SMTP Transport agent, On-demand database scan.
deviceExternalId	deviceExternalId	Engine version	Anti-Malware engine version, Antispam engine version, e.g. "18620,7730"
cs1	deviceCustomString1	Anti-Malware result	Result of Anti-Malware scan, including threat name
cs1Label	deviceCustomString1Label	"Anti-Malware result"	
cs2	deviceCustomString2	Antispam result	Result of Antispam scan, including reason for marking as spam
cs2Label	deviceCustomString2Label	"Antispam result"	
cs3	deviceCustomString3	Anti-Phishing result	Result of Anti-Phishing scan, including detected URL
cs3Label	deviceCustomString3Label	"Anti-Phishing result"	
cs4	deviceCustomString4	SPF/DKIM/DMARC result	Result of SPF/DKIM/DMARC check, in RFC7601 format
cs4Label	deviceCustomString4Label	"SPF/DKIM/DMARC result"	
cs5	deviceCustomString5	"From:" sender	Sender address from RFC5322 header "From:"
cs5Label	deviceCustomString5Label	"From header"	
cs6	deviceCustomString6	"To:" and "Cc:" recipients	Recipients addresses from RFC5322 headers "To:" and "Cc:"
cs6Label	deviceCustomString6Label	"To and Cc headers"	
fname	filename (1023)	Attachment name	Name of the first detected attachment

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
fileHash	fileHash (255)	Attachment hash	Hash of the first detected attachment
fsize	fileSize	Attachment size	Size of the first detected attachment
reason	reason (1023)	Rule/policy activated	Name of the policy triggered by the email or it's content
ESETEMSXFileDetails	ESETEMSXFileDetails	File details	Information about all detected attachments, their names, hashes and sizes

Optional

CEF Key Name	CEF Key Full Name (Size)	Field Description	Detailed Field Description
end	endTime	Time event has ended	The time at which the activity ended, in milliseconds since Jan 1st 1970. Useful only if sand boxing technology is used ESET LiveGuard Advanced.
dtz	deviceTimeZone (255)	Timezone of the server	
request	requestURL	Detected URL	Malign or blacklisted URL extracted from mail body or mail headers. ESET Mail Security does not provide single URL in logs due to the fact that multiple URL's can be detected in email messages by various detection components.

Proxy server

V prostredí, kde sa používa rozsiahlejšia lokálna sieť, je väčšinou pripojenie do internetu zabezpečované cez tzv. proxy server. V takomto prípade musia byť nastavenia proxy servera správne definované. V opačnom prípade nebude automaticky prebiehať sťahovanie aktualizácií. Nastavenie proxy servera je možné v ESET Mail Security definovať na dvoch odlišných miestach v rámci štruktúry **Rozšírených nastavení** (**F5**):

1. **Rozšírené nastavenia** (F5) > **Aktualizácia** > **Profily** > **Aktualizácie** > **Možnosti pripojenia** > HTTP Proxy. Toto nastavenie je platné pre konkrétny profil aktualizácie a je ho vhodné nastaviť, ak ide o prenosný počítač, ktorý vykonáva aktualizáciu z rôznych miest.

2. **Rozšírené nastavenia** (F5) > **Nástroje** > **Proxy server**. Proxy server zadaný v tejto sekcii bude použitý programom ESET Mail Security ako globálne nastavenie proxy servera. Tieto nastavenia budú používané všetkými modulmi, ktoré sa pripájajú na internet.

Na upresnenie nastavení proxy servera na tejto úrovni povoľte možnosť **Používať proxy server**, zadajte adresu proxy servera do poľa **Proxy server** a číslo portu do poľa **Port**.

Proxy server vyžaduje overenie

Ak sieťová komunikácia cez proxy server vyžaduje overenie, povoľte túto možnosť a zadajte **Prihlasovacie meno** a **Heslo**.

Vyhľadať proxy server

Na automatické vyhľadanie nastavení proxy servera kliknite na tlačidlo **Vyhľadať**. Pomocou tlačidla sa prenesú nastavenia z programu Internet Explorer.

> Týmto spôsobom nie je možné získať overovacie údaje (prihlasovacie meno a heslo) – je potrebné ich zadať.

Použiť priame pripojenie, ak nie je dostupný proxy server

Ak je produkt nakonfigurovaný tak, aby používal HTTP Proxy a proxy nie je k dispozícii, produkt obíde proxy a bude komunikovať priamo so servermi spoločnosti ESET.

Oznámenia

Upozornenia na pracovnej ploche sú informačnými prostriedkami, ktoré neponúkajú a ani nevyžadujú interakciu používateľa. Zobrazujú sa v paneli oznámení v pravej dolnej časti obrazovky. Ďalšie možnosti (ako dĺžka zobrazenia oznámenia a priehľadnosť tohto okna) možno nastaviť nižšie.

Povolením možnosti **Nezobrazovať oznámenia pri spúšťaní aplikácií na celú obrazovku** budú pozastavené oznamovacie okná v prípade, že bude spustená aplikácia na celú obrazovku.

Zobrazovať oznámenia o úspešnej aktualizácii

Po úspešnej aktualizácii sa zobrazí príslušné oznámenie.

Posielať oznámenia o udalostiach e-mailom

Kliknutím na túto možnosť aktivujete posielanie e-mailových oznámení.

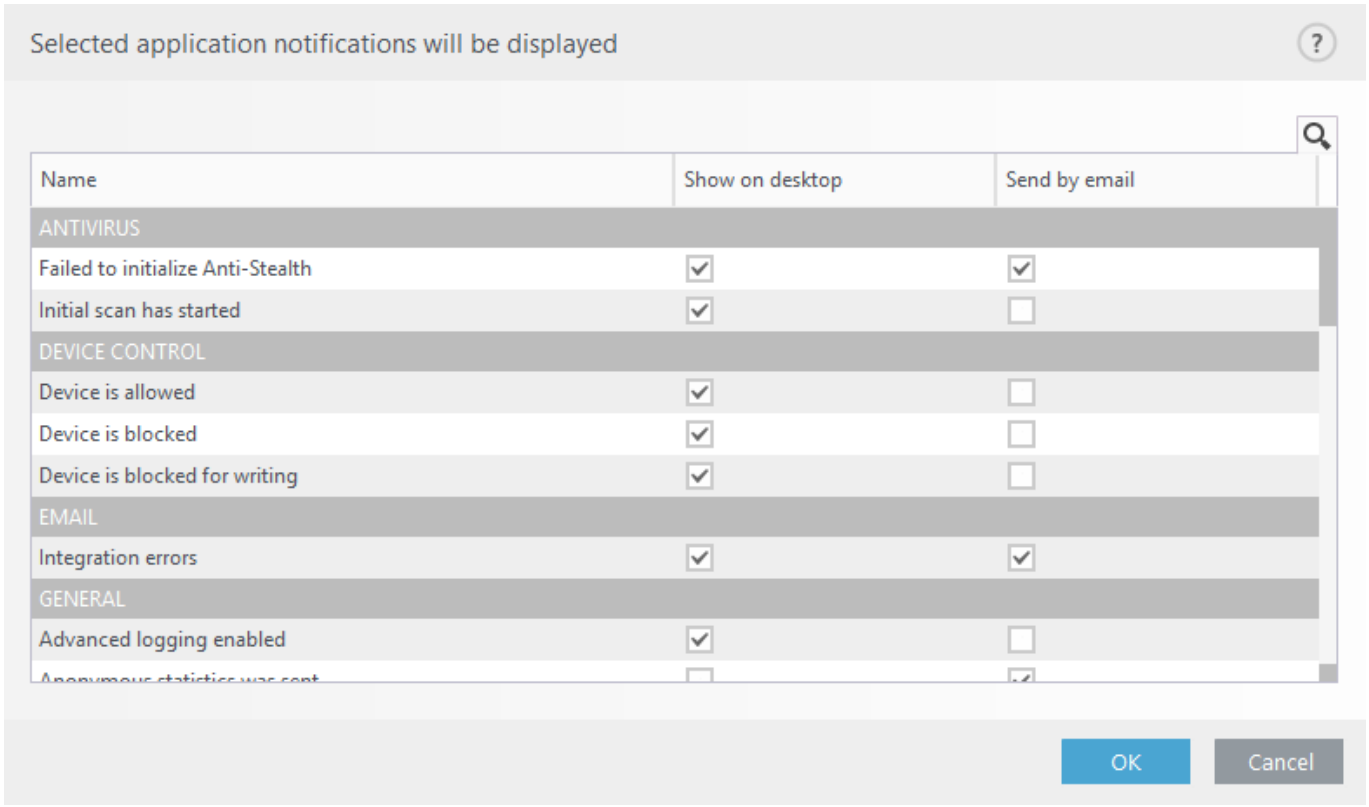
Oznámenia aplikácie

Kliknutím na Upraviť zapnete alebo vypnete zobrazovanie oznámení aplikácie.

Oznámenia aplikácie

ESET Mail Security oznámenia môžete nastaviť tak, aby sa zobrazovali na ploche alebo aby boli odosielané e-mailom.

> Ak chcete používať e-mailové oznámenia, uistite sa, že je povolená možnosť **Posielať oznámenia o udalostiach e-mailom** v sekcii **Základné** a následne nakonfigurujte SMTP server a ostatné podrobnosti podľa potreby.



Oznámenia na ploche

V tejto sekcii je možné nastaviť výstražné a informačné hlásenia programu ESET Mail Security (napr. správy o úspešnej aktualizácii). Nastaviť je možné napríklad **Trvanie** zobrazenia oznámenia, ako aj **Priehľadnosť** okna v oblasti oznámení systému Windows (len na systémoch, ktoré podporujú notifikácie).

V roletovom menu **Zobrazovať udalosti od úrovne** je možné nastaviť, aké závažné udalosti sa budú zobrazovať. Na výber sú tieto možnosti:

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

V poli s názvom **Vo viacpoužívateľskom prostredí zobrazovať oznámenia tomuto používateľovi** je špecifikovaný používateľ, ktorému sa budú zasielať dôležité systémové hlásenia na systéme umožňujúcom prihlásenie viacerých používateľov súčasne. Štandardne je týmto používateľom správca systému alebo siete. Túto možnosť je vhodné použiť na terminálovom serveri za predpokladu, že všetky systémové hlásenia budú odosielané správcovi.

Povoliť oznámeniam zobrazovať sa v popredí – oznámenia sa budú zobrazovať v popredí obrazovky a budú dostupné pomocou klávesovej skratky Alt+Tab.

E-mailové oznámenia

ESET Mail Security podporuje automatické odosielanie oznámení e□mailom, ak sa vyskytne udalosť s nastavenou úrovňou zápisu.

ESET Mail Security podporuje SMTP servery, ktoré využívajú šifrovanie TLS.

SMTP server

Názov SMTP servera použitého na odosielanie oznámení a upozornení. Zvyčajne je to názov vášho Microsoft Exchange Servera.

Prihlasovacie meno a heslo

V prípade, že SMTP server vyžaduje overenie, musí byť táto možnosť zapnutá a pre prístup k SMTP serveru musí byť nastavené správne prihlasovacie meno a heslo.

E-mailová adresa odosielateľa

Upresnite adresu odosielateľa, ktorá bude zobrazená v hlavičke e□mailovej správy obsahujúcej oznámenie. Ide o adresu, ktorú príjemca uvidí v poli **Od**.

E-mailová adresa príjemcu

Zadajte e□mailovú adresu príjemcu, pre ktorého je oznámenie určené.

Zapnúť TLS

Zapne odosielanie správ a upozornení s podporou šifrovania typu TLS.

Nastavenia e-mailu

Posielať udalosti od úrovne

Určuje minimálnu úroveň podrobností odosielaných oznámení.

Interval, v akom sa budú e□mailom posielať nové oznámenia (v minútach)

Časový interval v minútach, po ktorom sa odošle nové oznámenie prostredníctvom e□mailu. Ak chcete, aby sa e-maily odosielali okamžite, nastavte túto hodnotu na 0.

Posielať každé oznámenie v samostatnom e-maile

Každé oznámenie bude odoslané v samostatnom e-maile. Výsledkom môže byť veľký počet odosielaných e-mailov za krátky čas.

Formát správy

Komunikácia medzi programom a používateľom, správcom alebo zodpovednou osobou je zabezpečená prostredníctvom e-mailov alebo oznamovacích správ (pomocou služby Windows messenger service). Vírusové správy a upozornenia systému majú prednastavený formát, ktorý sa neodporúča meniť. V niektorých prípadoch je potrebné pozmeniť formát správ o udalostiach.

Formát správ o udalostiach

Formát správ o udalostiach zobrazovaných na vzdialenom počítači, ktorý je špecifikovaný v nastaveniach odosielania.

Formát správ o hrozbách

Správy obsahujúce upozornenia a oznámenia o hrozbách majú preddefinovaný formát. Meniť tento formát sa neodporúča. Formát môžete meniť napríklad v prípade, že používate systém na automatické spracovanie e-mailov.

Vo formáte správ sa nachádzajú kľúčové slová označené percentom („%“), ktoré sú pri vytváraní správ nahradené zodpovedajúcimi hodnotami. Sú dostupné nasledujúce kľúčové slová:

- %TimeStamp% – dátum a čas udalosti.
- %Scanner% – modul, ktorý zaznamenal udalosť.
- %ComputerName% – názov počítača, na ktorom došlo k udalosti.
- %ProgramName% – program, ktorý spôsobil udalosť.
- %InfectedObject% – názov infikovaného súboru, e-mailovej správy atď.
- %VirusName% – názov vírusu.
- %ErrorDescription% – popis chyby.

Kľúčové slová **%InfectedObject%** a **%VirusName%** sa využívajú iba v upozorneniach týkajúcich sa hrozieb, kým kľúčové slovo **%ErrorDescription%** sa využíva iba v informatívnych upozorneniach.

Znaková sada

V roletovom menu si môžete vybrať kódovanie znakov. E-mailová správa bude skonvertovaná podľa zvoleného kódovania.

Použiť Quoted-printable kódovanie

Zdroj e-mailovej správy bude zakódovaný do Quoted-printable (QP) formátu, ktorý používa ASCII znaky a vie správne preložiť špeciálne znaky do 8-bitového formátu (áéíóú).

Prispôsobenie

Táto správa bude zobrazená v päte vybraných upozornení.

Predvolená správa v oznámeniach

Predvolená správa, ktorá sa zobrazí v päte upozornenia.

Hrozby

Automaticky nezatvárať oznámenia o malvéri

Ak použijete túto možnosť, upozornenia o malvéri ostanú na obrazovke až kým ich nezatvoríte manuálne.

Použiť predvolenú správu

Môžete vypnúť odosielanie predvolenej správy a nastaviť si vlastnú správu upozorňujúcu na hrozbu, ktorá sa zobrazí v prípade, že došlo k zablokovaniu hrozby.

Správa upozorňujúca na hrozbu

Zadajte vlastnú správu, ktorá sa zobrazí v prípade, že došlo k zablokovaniu hrozby.

Prezentačný režim

Prezentačný režim je funkcia určená pre používateľov, ktorí chcú svoj softvér používať neprerušovane a neželajú si byť vyrušovaní oknami s oznámeniami, pričom taktiež požadujú minimálne vyťaženie procesora antivírusom. Prezentačný režim je možné použiť aj pri prezentáciách, ktoré nesmú byť prerušené aktivitou programu ESET Mail Security. Zapnutím prezentačného režimu budú zakázané všetky oznámenia programu a plánované úlohy. Samotná ochrana je aj naďalej spustená v pozadí, avšak nevyžaduje žiadne zásahy používateľa.

Automaticky zapnúť prezentačný režim pri spúšťaní aplikácií na celú obrazovku

Prezentačný režim sa aktivuje automaticky pri spustení aplikácie v režime na celú obrazovku. Ak je prezentačný režim aktívny, nebudú sa zobrazovať oznámenia alebo zmeny stavu vášho programu ESET Mail Security.

Automaticky vypnúť prezentačný režim po určenom čase

Môžete si tiež zvoliť túto možnosť a určiť čas v minútach, po uplynutí ktorého sa prezentačný režim automaticky vypne.

Diagnostika

Diagnostika poskytuje výpisy aplikácie pri zlyhaní procesov ESET (napr. *ekrn*). Ak aplikácia zlyhá, vygeneruje sa výpis. Výpis môže pomôcť vývojárom pri oprave rôznych problémov produktu ESET Mail Security.

Kliknite na roletové menu vedľa položky **Typ výpisu** a vyberte jednu z nasledujúcich možností:

- **Žiadny** – použitím tejto možnosti vypnete túto funkciu.
- **Skrátený** (predvolené) – zaznamená najmenšiu sadu užitočných informácií, ktoré môžu pomôcť identifikovať dôvod, prečo aplikácia nečakane zlyhala. Tento typ výpisu môže byť užitočný, keď je obmedzený priestor na disku. Pre obmedzené množstvo zahrnutých informácií však chyby, ktoré neboli priamo spôsobené vláknom (threadom) aktívnym v čase problému, nemusia byť pri analýze tohto súboru objavené.
- **Úplný** – zaznamená celý obsah systémovej pamäte, keď sa aplikácia nečakane zastaví. Kompletný výpis pamäte môže obsahovať dáta procesov, ktoré bežali v čase, keď bol výpis zozbieraný.

Cieľový priečinok

Priečinok, do ktorého sa pri zlyhaní vygeneruje výpis.

Otvoriť diagnostický priečinok

Po kliknutí na možnosť **Otvoriť** sa tento priečinok zobrazí v novom okne *Windows Prieskumníka*.

Vytvoriť diagnostický výpis

Ak chcete v cieľovom priečinku vytvoriť diagnostický výpis, kliknite na **Vytvoriť**.

Vytváranie rozšírených protokolov

Zapnúť rozšírené protokoly kontroly počítača
Zaznamenávať sa budú všetky udalosti, ku ktorým dôjde počas kontroly súborov a priečinkov Kontrolou počítača alebo Rezidentnou ochranou súborového systému.
Zapnúť rozšírené protokoly správy zariadení
Zaznamenávať sa budú všetky udalosti správy zariadení s cieľom umožniť diagnostiku a riešenie problémov.
Zapnúť rozšírené protokoly Direct Cloud
Zaznamenávať sa bude všetka komunikácia produktu so servermi Direct Cloud.
Zapnúť rozšírené protokoly ochrany dokumentov
Zaznamenávať sa budú všetky udalosti modulu Ochrana dokumentov, aby bolo možné jednoduchšie diagnostikovať a opraviť prípadné problémy.
Zapnúť rozšírené protokoly jadra
Zaznamenávať sa budú všetky udalosti v jadre ESET (ekrn) s cieľom umožniť diagnostiku a riešenie problémov.
Zapnúť rozšírené protokoly licencovania
Zaznamenávaná bude všetka komunikácia produktu s licenčným serverom.
Zapnúť sledovanie pamäte
Zaznamenávať sa budú všetky udalosti, ktoré pomôžu vývojárom diagnostikovať úniky pamäte.
Zapnúť rozšírené protokoly ochrany siete
Zaznamenávané budú všetky sieťové dáta prechádzajúce ochranou siete v PCAP formáte. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa ochrany siete.
Zapnúť protokoly operačného systému
Budú zozbierané dodatočné informácie o operačnom systéme, ako sú spustené procesy, aktivita procesora a operácie disku. Vývojárom to môže pomôcť diagnostikovať a opraviť problémy súvisiace s produktom ESET, ktorý beží na vašom operačnom systéme.
Zapnúť rozšírené protokoly filtrovania protokolov
Zaznamenávané budú všetky dáta prechádzajúce jadrom filtrovania protokolov v PCAP formáte. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa filtrovania protokolov.
Zapnúť rozšírené protokoly push správ
Zaznamenávať sa budú všetky udalosti, ktoré môžu pomôcť pri diagnostike a riešení problémov týkajúcich sa push správ.
Zapnúť rozšírené protokoly rezidentnej ochrany súborového systému
Zaznamenávať sa budú všetky udalosti modulu Rezidentná ochrana súborového systému, aby bolo možné jednoduchšie diagnostikovať a opraviť prípadné problémy.
Zapnúť rozšírené protokoly aktualizačného jadra
Zaznamenávané budú všetky udalosti, ktoré nastanú počas procesu aktualizácie. Toto môže pomôcť vývojárom diagnostikovať a opraviť problémy týkajúce sa aktualizačného jadra.
Umiestnenie protokolov
C:\ProgramData\ESET\ESET Security\Diagnostics

Technická podpora

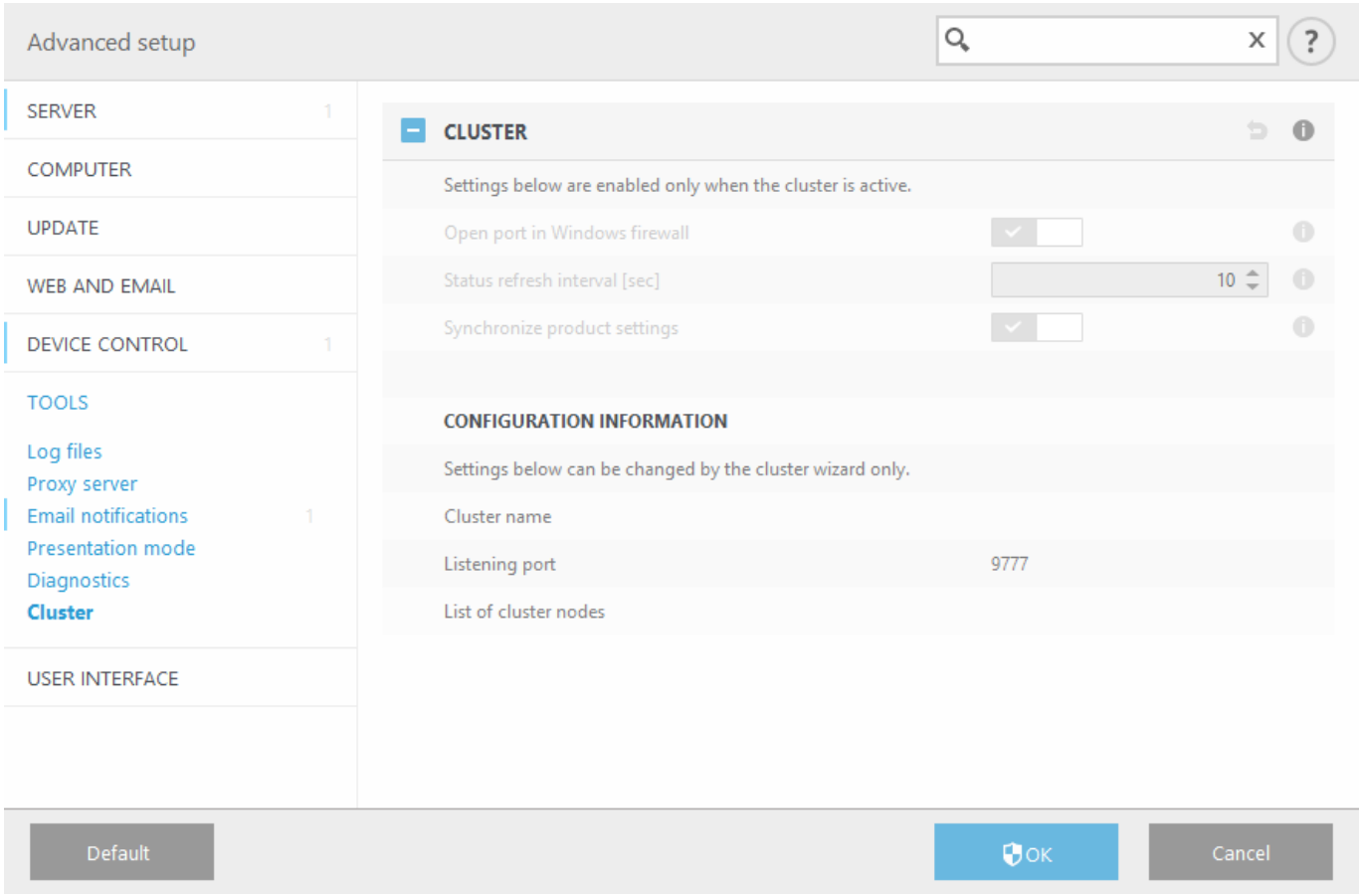
Odoslať systémové nastavenia

Z roletového menu vyberte možnosť **Vždy odosielať** (ak nechcete, aby sa vám pred odoslaním konfiguračných údajov programu ESET Mail Security technickej podpore vždy zobrazila výzva) alebo možnosť **Spýtať sa pred odoslaním**.

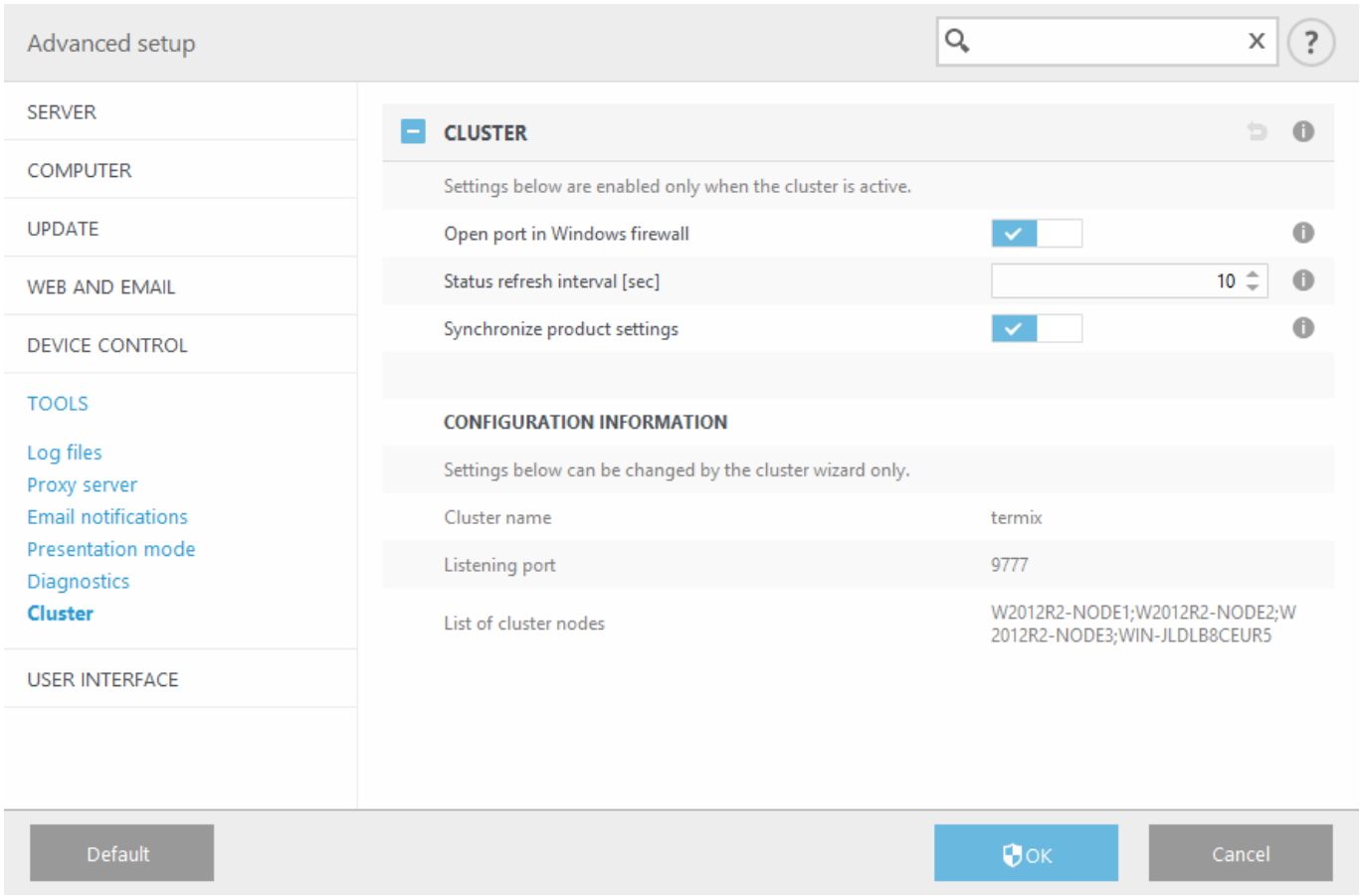
Klaster

Možnosť Povoliť klaster je automaticky zapnutá, ak je nastavený klaster ESET. Klaster môžete zakázať v okne **Rozšírené nastavenia** (F5) kliknutím na prepínač (napríklad, ak potrebujete zmeniť nastavenia bez toho, aby to ovplyvnilo ostatné uzly v klastri ESET). Prepínač slúži len na zapnutie alebo vypnutie funkcie klastra ESET. Pre nastavenie alebo odstránenie klastra je potrebné použiť Sprievodcu konfiguráciou klastra alebo **zrušiť klaster** v sekcii Nástroje > Klaster hlavného okna programu.

Klaster ESET nie je nastavený alebo je vypnutý:



Klaster ESET je nastavený:



Používateľské rozhranie

V tejto sekcii môžete nastaviť grafické používateľské rozhranie programu ESET Mail Security. Môžete si prispôsobiť vizuálnu stránku programu a použité efekty.

Prvky používateľského rozhrania

V roletovom menu Štartovací režim sú na výber nasledujúce možnosti zobrazenia grafického používateľského rozhrania:

- **Úplný** – zobrazuje sa kompletné grafické rozhranie.
- **Terminál** – nezobrazujú sa ani oznámenia ani varovania. Tento režim môže spustiť len správca. Grafické rozhranie by malo byť prepnuté na Terminál, ak zobrazovanie prvkov grafického rozhrania programu spomaľuje výkon vášho počítača alebo spôsobuje problémy. Vypnutie GUI je tiež užitočné pre terminálový server. Viac informácií o ESET Mail Security nainštalovanom na terminálovom serveri nájdete v časti Vypnutie grafického rozhrania (GUI) na terminálovom serveri.

Zobrazovať úvodný obrázok pri štarte
Vypnite túto možnosť, ak nechcete, aby sa napr. pri prihlásení do systému zobrazoval úvodný obrázok ESET Mail Security.
Používať zvukové upozornenia
ESET Mail Security prehráva pri dôležitých udalostiach zvukové efekty (napríklad pri nájdení hrozieb, kontrole počítača alebo pri dokončení kontroly), ktoré môžu byť zapnuté alebo vypnuté pomocou tejto možnosti.
Pridať do kontextového menu
Ovládacie prvky programu ESET Mail Security budú integrované do kontextového menu. Kontextové menu sa zobrazuje po kliknutí pravým tlačidlom myši na súbor v prieskumníkovi. Obsahuje zoznam akcií, ktoré možno so súborom vykonať.
Stavy aplikácie
Kliknutím na Upraviť môžete vybrať stavy aplikácie, ktoré budú zobrazované v okne Monitorovanie. Môžete tiež použiť ESET PROTECT politiky na konfiguráciu vašich stavov aplikácií. Stav aplikácie bude tiež zobrazený, ak váš produkt nie je aktivovaný alebo vypršala vaša licencia.
Zobrazovať licenčné informácie
Ak je táto možnosť povolená, budú zobrazované správy a oznámenia týkajúce sa vašej licencie.

Upozornenia a okná správ

V tejto časti môžete zmeniť správanie upozornení pri detekcii hrozieb a správanie systémových upozornení. Tie môžu byť zmenené tak, aby vyhovovali vašim požiadavkám. Ak sa rozhodnete nezobrazovať určité upozornenia, budú zobrazené v časti Vypnuté správy a stavy. Môžete kontrolovať ich stav, zobraziť viac informácií alebo ich odstrániť.

Nastavenia prístupu

Akýmkoľvek neoprávneným zmenám môžete predísť použitím Nastavení prístupu. Pomocou týchto nastavení môžete zaistiť vysokú mieru zabezpečenia.

ESET Shell

Konfigurácia prístupových práv k nastaveniam, funkciám a dátam programu prostredníctvom nástroja eShell je možná zmenou politiky spustenia nástroja ESET Shell.

Ikona v oblasti oznámení systému Windows

Vrátiť späť všetky nastavenia v tejto sekcii

Upozornenia a okná správ

V tejto sekcii je možné nastaviť výstražné a informačné hlásenia programu ESET Mail Security (napr. správy o úspešnej aktualizácii). Nastaviť je možné napríklad **Trvanie** zobrazenia oznámenia, ako aj **Priehľadnosť** okna v oblasti oznámení systému Windows (len na systémoch, ktoré podporujú notifikácie).

Zobrazovať interaktívne upozornenia

Vypnite túto funkciu, ak si neprajete, aby program ESET Mail Security zobrazoval akékoľvek upozornenia v oblasti oznámení systému Windows v pravom dolnom rohu obrazovky.

Zoznam interaktívnych upozornení

Túto možnosť využijete na automatizáciu. Ak nechcete zobraziť upozornenie a čakať na interakciu používateľa, môžete v rámci automatizácie pre konkrétne položky zrušiť výber možnosti **Spýtať sa používateľa** a vybrať požadovanú akciu, ktorú má produkt vykonať.

Okná správ sú používané na zobrazovanie krátkych textových správ alebo otázok.

Okná správ zatvárať automaticky

Okná s oznámeniami sa budú zatvárať automaticky po určitom čase. Po uplynutí nastaveného času sa okno oznámenia zatvorí automaticky, ak ho nezatvorí sám používateľ.

Potvrdzovacie správy

Po kliknutí na možnosť **Upraviť** sa zobrazí okno so zoznamom potvrdzovacích správ, ktoré ESET Mail Security zobrazí pred vykonaním konkrétnej akcie. Použitím začiarkavacích políčok môžete upraviť nastavenia pre potvrdzovacie správy.

Nastavenia prístupu

Správne nastavenie ESET Mail Security je veľmi dôležité pre zachovanie maximálnej bezpečnosti vášho systému. Neoprávnené zmeny nastavení môžu vystaviť systém nebezpečenstvu, prípadne spôsobiť stratu dát. Ak chcete zabrániť neoprávneným zmenám, môžete si v rámci ESET Mail Security nastaviť ochranu nastavení heslom.

Ak sa pokúsite odinštalovať ESET Mail Security v prípade, keď je aktívna ochrana nastavení heslom, bude potrebné zadať príslušné heslo. V opačnom prípade nebude možné ESET Mail Security odinštalovať.

Ochrana nastavení heslom

Zapína/vypína uzamknutie nastavení vami zadaným heslom. Po kliknutí sa otvorí okno **Nastavenie hesla**.

Nastaviť heslo

Pre zmenu nastaveného hesla kliknite na **Nastaviť**. Na ochranu nastavení produktu ESET Mail Security a zabránenie ich neoprávneným zmenám je potrebné nastaviť nové heslo. Pre zmenu hesla najprv zadajte staré heslo do poľa **Pôvodné heslo**, potom zadajte nové heslo do polí **Nové heslo** a **Potvrdiť heslo** a následne potvrďte zmenu hesla kliknutím na **OK**. Toto heslo bude odteraz vyžadované pre všetky ďalšie zmeny v nastaveniach ESET Mail Security.

Vyžadovať úplné práva správcu aj pre účty s obmedzenými právami

Túto možnosť použite v prípade, že chcete, aby bol aktuálny používateľ (ak nemá práva správcu) vyzvaný na zadanie prihlasovacích údajov pri pokuse o zmenu niektorých systémových parametrov (napr. vypnutie modulov ochrany).

Ak sa zmení heslo pre Nastavenie prístupu a chcete importovať existujúci konfiguračný súbor .xml (podpísaný pred zmenou hesla) pomocou príkazového riadku ESET CMD, je potrebné súbor podpísať znova pomocou vášho aktuálneho hesla. Tento postup vám umožní použiť starší konfiguračný súbor bez potreby jeho exportovania na inom počítači, na ktorom je spustený program ESET Mail Security.

ESET Shell

Konfigurácia prístupových práv k nastaveniam, funkciám a dátam programu prostredníctvom nástroja eShell je možná zmenou **politiky spustenia nástroja ESET Shell**. Predvolene je nastavené **Obmedzené skriptovanie**, pričom ďalšie možnosti sú: Vypnutý, Iba na čítanie a Úplný prístup.

Vypnutý

eShell nemôže byť použitý. Je povolená len konfigurácia samotného nástroja eShell v ui eshell kontexte. Môžete zmeniť vzhľad nástroja eShell, nemáte však prístup k bezpečnostných nastaveniam a dátam.

Iba na čítanie

Nástroj eShell môže byť použitý len na monitorovanie. Všetky nastavenia môžete zobraziť v oboch režimoch, nemôžete však zmeniť žiadne nastavenia, funkcie alebo dáta.

Obmedzené skriptovanie

V interaktívnom režime môžete zobraziť a zmeniť všetky nastavenia, funkcie alebo dáta. V Batch režime bude nástroj eShell pracovať v režime Iba na čítanie, ak však používate podpísané batch súbory, budete môcť upravovať nastavenia aj dáta.

Úplný prístup

Prístup ku všetkým nastaveniam v interaktívnom aj batch režime. Môžete zobraziť a zmeniť všetky nastavenia. eShell musíte používať s právami správcu. Taktiež musíte mať povolenú UAC (user account control) a eleváciu.

Vypnutie grafického používateľského rozhrania (GUI) na terminálovom serveri

Táto kapitola vysvetľuje, ako vypnúť grafické rozhranie (GUI) programu ESET Mail Security pre používateľov prihlásených na terminálovom serveri.

Za normálnych okolností sa grafické rozhranie (GUI) programu ESET Mail Security spustí pri každom prihlásení používateľa na terminálový server. Toto je väčšinou nežiaduce, pokiaľ ide o terminálové servery. Ak si želáte vypnúť GUI pre terminálové pripojenia, môžete to urobiť pomocou nástroja eShell spustením príkazu `set ui ui gui-start-mode none`. Tento príkaz prepne GUI do terminálu. Sú dostupné nasledujúce dve možnosti:

```
set ui ui gui-start-mode full
```

```
set ui ui gui-start-mode none
```

Ak chcete zistiť, ktorá z dvoch možností zobrazenia GUI je zapnutá, spustite príkaz `get ui ui gui-start-mode`.

Ak používate ESET Mail Security na serveri Citrix, odporúčame použiť nastavenia popísané v nasledujúcom článku Databázy znalostí spoločnosti ESET.

Vypnuté správy a stavy

Potvrdzovacie správy

Zobrazí vám zoznam potvrdzovacích správ, pre ktoré môžete zvoliť, či sa majú alebo nemajú zobrazovať.

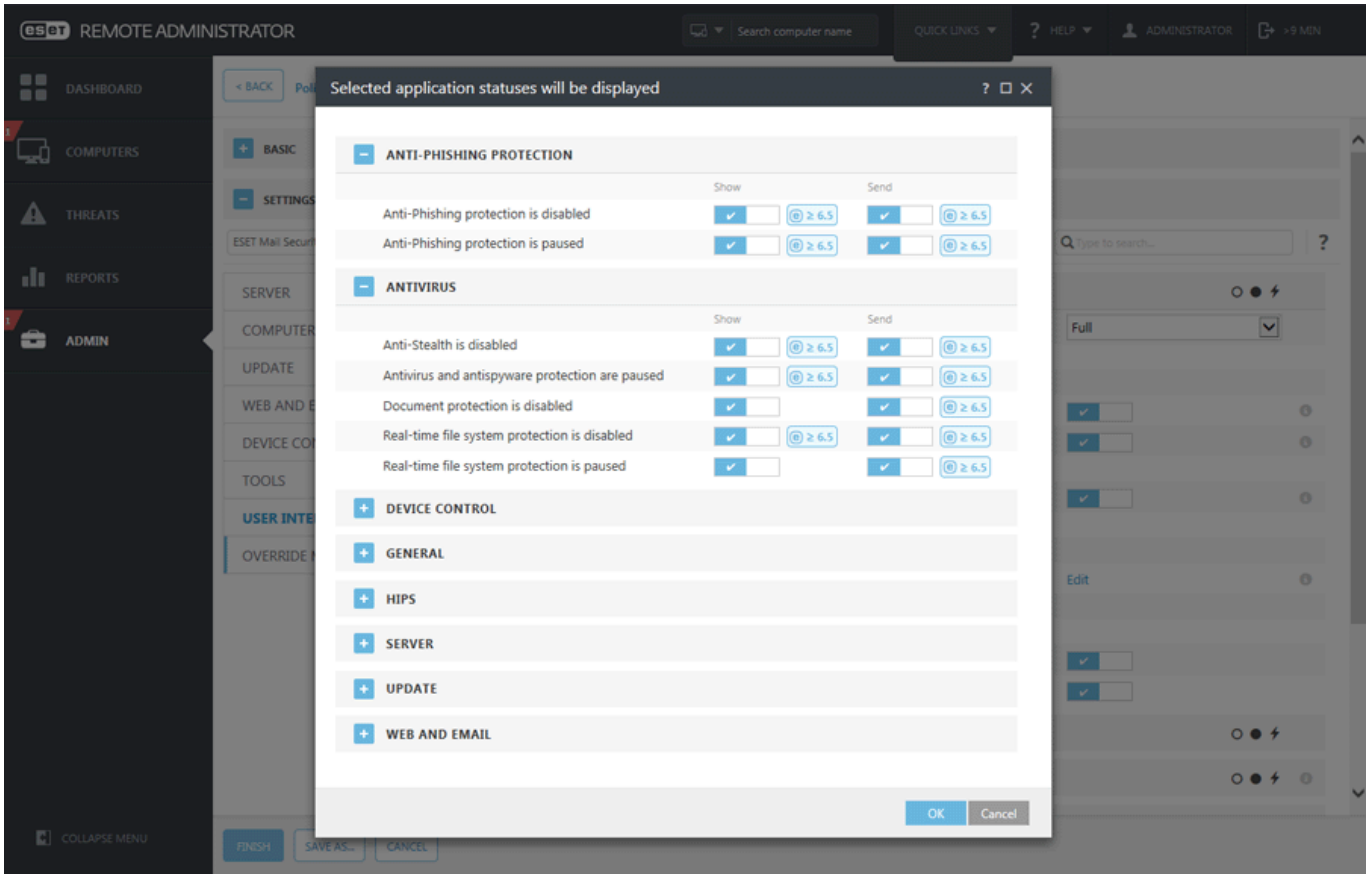
Nastavenia stavov aplikácie

Umožňuje zapnúť alebo vypnúť zobrazenie stavu v okne Monitorovanie, ktoré sa nachádza v hlavnom menu.

Nastavenia stavov aplikácie

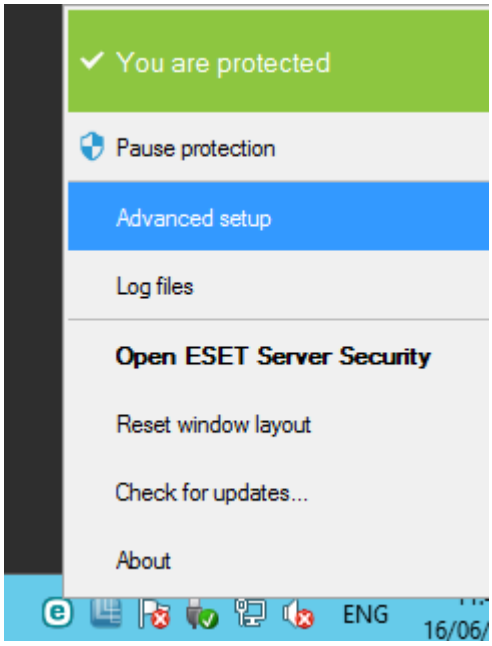
Toto dialógové okno vám umožňuje definovať, ktoré stavy aplikácie budú alebo nebudú zobrazované. Napríklad, ak pozastavíte antivírusovú a antispyvérovú ochranu, výsledkom bude zmena stavu ochrany, čo bude následne zobrazené v sekcii Monitorovanie. Stav aplikácie bude tiež zobrazený, ak váš produkt nie je aktivovaný alebo vypršala vaša licencia.

Stavy aplikácií je možné spravovať prostredníctvom ESET PROTECT politík. Kategórie a stavy sú zobrazené v zozname s dvomi možnosťami: **Zobraziť** a **Odoslať** stav. Stĺpec „Odoslať“ pre stavy aplikácií je viditeľný len v konfigurácii ESET PROTECT politiky. ESET Mail Security zobrazuje nastavenia s ikonou zámku. Pre dočasnú zmenu stavov aplikácie môžete použiť Režim prepísania.



Ikona v oblasti oznámení systému Windows

Ikona na paneli úloh slúži na rýchly prístup k často používaným funkciám programu ESET Mail Security. Tieto funkcie sú dostupné po kliknutí pravým tlačidlom myši na ikonu v oblasti oznámení systému Windows.



Viac informácií

Otvorí sa okno Monitorovanie, kde bude zobrazený aktuálny stav ochrany a súvisiace správy.

Pozastaviť ochranu

Zobrazí sa potvrdzovacie dialógové okno, ktoré vypne Antivírusovú a antispyvérovú ochranu, ktorá chráni pred škodlivými systémovými útokmi pomocou kontroly súborov, webu a e-mailovej komunikácie. Keď dočasne pozastavíte antivírusovú a antispyvérovú ochranu pomocou ikony programu v oblasti oznámení systému Windows, zobrazí sa dialógové okno **Pozastaviť ochranu**. Táto možnosť vypína ochranu systému pred malvérom na stanovený čas. Ak chcete ochranu vypnúť natrvalo, môžete to urobiť v **Rozšírených nastaveniach**. Pri vypínaní ochrany buďte opatrný, pretože váš systém bude vystavený hrozbám.

Rozšírené nastavenia

Otvorí sa okno s **Rozšírenými nastaveniami** pre daný program.

Protokoly

Protokoly obsahujú informácie o všetkých systémových udalostiach a poskytujú prehľad zistených ohrození.

Skryť ESET Mail Security

Skryje hlavné okno programu ESET Mail Security z obrazovky.

Obnoviť rozmiestnenie okien

Obnoví prednastavenú veľkosť a umiestnenie okna ESET Mail Security na obrazovke.

Overiť dostupnosť aktualizácií

Spustí aktualizáciu modulov, ktorá je dôležitou súčasťou zabezpečenia komplexnej ochrany pred škodlivým kódom.

O programe

Informácie o programe ESET Mail Security, v ktorých môžete nájsť verziu produktu, licenčné informácie a informácie o nainštalovaných moduloch. Informácie o operačnom systéme a systémových prostriedkoch sú zobrazené v dolnej časti okna.

Vrátiť späť na predvolené nastavenia

Nastavenia môžete v rámci **rozšírených nastavení** vrátiť späť na pôvodné hodnoty. Existujú dva spôsoby. Na predvolené hodnoty môžete vrátiť buď všetko, alebo iba nastavenia pre konkrétnu sekciu (nastavenia v ostatných sekciách ostanú nezmenené).

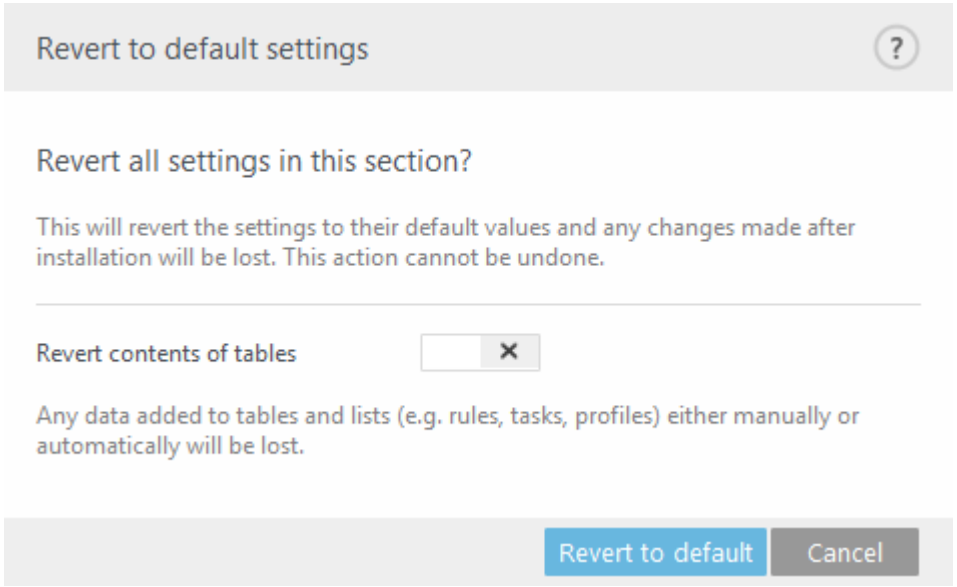
Vrátiť späť všetky nastavenia

Všetky nastavenia vo všetkých sekciách rozšírených nastavení budú obnovené do stavu po inštalácii ESET Mail Security. V podstate ide o obnovenie továrenských nastavení.

Po kliknutí na možnosť **Vrátiť späť na predvolené** budú všetky vykonané zmeny stratené. Túto akciu nie je možné vrátiť späť.

Vrátiť späť všetky nastavenia v tejto sekcii

Nastavenia modulov vo vybranej sekcii budú vrátené na pôvodné hodnoty. Akékoľvek zmeny, ktoré ste vykonali v tejto sekcii, sa stratia.



Vrátiť späť obsah tabuliek

Po povolení tejto možnosti sa stratia pravidlá, úlohy alebo profily pridané či už manuálne, alebo automaticky.

Pomocník a podpora

ESET Mail Security obsahuje nástroj poskytujúci pomoc pri riešení známych problémov, prostredníctvom ktorého možno kontaktovať technickú podporu spoločnosti ESET.

Nainštalovaný produkt

Informácie o produkte a licencii

- O ESET Mail Security – zobrazuje informácie o vašej kópii programu ESET Mail Security.
- Riešenie problémov s produktom – otvorí sa kapitola pomocníka, ktorá sa venuje riešeniu najčastejších problémov s produktom. Skôr ako kontaktujete technickú podporu, odporúčame vám prečítať si túto sekciu.
- Riešenie problémov s licenciou – otvorí sa stránka, ktorá sa venuje riešeniu problémov s aktiváciou alebo zmenou licencie.
- Zmeniť licenciu – kliknutím na túto možnosť otvoríte okno na aktiváciu produktu.

Pomocník k programu

Kliknutím na túto možnosť otvoríte online pomocníka pre ESET Mail Security.

Databáza znalostí

Hľadať v Databáze znalostí spoločnosti ESET – Databáza znalostí spoločnosti ESET obsahuje odpovede na najčastejšie kladené otázky, ako aj odporúčané riešenia rozličných problémov. Pravidelná aktualizácia databázy znalostí pracovníkmi spoločnosti ESET z nej robí najrýchlejší nástroj na riešenie rozličných druhov problémov.

Technická podpora

- Vytváranie rozšírených protokolov – umožňuje vytvorenie podrobných protokolov pre všetky dostupné funkcie programu. Takéto protokoly našim vývojárom uľahčia diagnostiku problému a jeho následné riešenie.
- Požiadať o technickú podporu – v prípade problému, na ktorý nenájdete odpoveď, je možné kontaktovať naše oddelenie technickej podpory.
- Podrobnosti pre technickú podporu – zobrazia sa podrobné informácie pre technickú podporu (názov produktu, verzia produktu atď.).
- ESET Log Collector – ESET Log Collector je nástroj určený na automatické zhromažďovanie informácií a protokolov zo servera na rýchlejšie vyriešenie problému.

Odoslať žiadosť na technickú podporu

Na čo možno najrýchlejšie a najpresnejšie poskytnutie pomoci bude od vás spoločnosť ESET vyžadovať informácie o konfigurácii vášho produktu ESET Mail Security, podrobné systémové informácie, spustené procesy (protokol nástroja ESET SysInspector) a tiež údaje databázy Registry. Spoločnosť ESET použije tieto informácie len na účely poskytnutia technickej podpory. Toto nastavenie môžete zmeniť aj v časti **Rozšírené nastavenia** (**F5**) > **Nástroje** > **Diagnostika** > **Technická podpora**.

Ak ste sa rozhodli odoslať systémové nastavenia, je potrebné vyplniť a odoslať webový formulár, v opačnom prípade vaša požiadavka na technickú podporu nebude vytvorená.

Ak odosielate webový formulár, vaše systémové nastavenia budú poskytnuté spoločnosti ESET. Zvoľte možnosť **Vždy odosielať tieto informácie**, ak chcete, aby bola akcia pre tento proces zapamätaná.

Neodoslať informácie

Túto možnosť použite v prípade, ak si neprajete odosielať údaje. Budete presmerovaný na webovú stránku technickej podpory spoločnosti ESET.

O programe ESET Mail Security

Toto okno obsahuje podrobnosti o nainštalovanej verzii produktu ESET Mail Security. Vrchná časť okna obsahuje informácie o vašom operačnom systéme a systémových prostriedkoch, ako aj o práve prihlásených používateľoch. Okrem toho tu nájdete aj úplný názov počítača.

Nainštalované súčasti

Kliknutím na túto možnosť sa zobrazí zoznam nainštalovaných súčastí a podrobnosti o nich. Kliknutím na **Kopírovať** skopírujete zoznam do schránky. Môže to byť užitočné v prípade hľadania problému alebo pri kontaktovaní technickej podpory spoločnosti ESET.

Slovník pojmov

Bližšie informácie o technických termínoch, hrozbách a internetovej bezpečnosti nájdete v Slovníku pojmov.

Licenčná dohoda s koncovým používateľom

S účinnosťou od 19. októbra 2021.

DÔLEŽITÉ: Pred stiahnutím, inštaláciou, kopírovaním alebo použitím si pozorne prečítajte nižšie uvedené podmienky používania produktu. **INŠTALÁCIOU, STIAHNUTÍM, KOPÍROVANÍM ALEBO POUŽITÍM SOFTVÉRU VYJADRUJETE SVOJ SÚHLAS S TÝMITO PODMIENKAMI A BERIETE NA VEDOMIE ZÁSADY OCHRANY OSOBNÝCH ÚDAJOV.**

Licenčná dohoda s koncovým používateľom

Podľa podmienok tejto Dohody s koncovým používateľom (Dohoda“) uzatvorenej medzi spoločnosťou ESET, spol. s r. o., so sídlom Einsteinova 24, 85101 Bratislava, Slovak Republic, zapísanej v Obchodnom registri okresného súdu Bratislava I, oddiel Sro, vložka č. 3586/B, IČO: 31333532 („ESET“ alebo „Poskytovateľ“) a vami, fyzickou alebo právnickou osobou („Vy“ alebo „Koncový používateľ“) máte právo na používanie Softvéru uvedeného v článku 1 tejto Dohody. Softvér uvedený v článku 1 tejto Dohody môže byť v súlade so zmluvnými podmienkami uvedenými nižšie uložený na dátovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov.

TOTO NIE JE KÚPNA ZMLUVA ALE DOHODA O PRÁVACH KONCOVÉHO POUŽÍVATEĽA. Poskytovateľ zostáva vlastníkom kópie Softvéru a prípadného fyzického média, na ktorom sa Softvér dodáva v obchodnom balení, ako aj všetkých kópií Softvéru, na ktoré má Koncový používateľ právo podľa tejto Dohody.

Kliknutím na položku „Súhlasím“ alebo „Súhlasím…“ pri inštalácii, sťahovaní, kopírovaní alebo používaní Softvéru vyjadrujete svoj súhlas s podmienkami a požiadavkami tejto Dohody a prijímate Zásady ochrany osobných údajov. Ak s niektorými podmienkami a požiadavkami tejto Dohody a/alebo Zásad ochrany osobných údajov nesúhlasíte, bezodkladne kliknite na možnosť zrušenia, zrušte inštaláciu alebo sťahovanie, prípadne zničte alebo vráťte Softvér, inštalačné médium, priloženú dokumentáciu a potvrdenie o platbe späť Poskytovateľovi alebo v obchode, kde ste Softvér získali.

SÚHLASÍTE S TÝM, ŽE VAŠE POUŽÍVANIE SOFTVÉRU JE ZNAKOM TOHO, ŽE STE SI PREČÍTALI TÚTO DOHODU, ROZUMIETE JEJ, A SÚHLASÍTE S TÝM, ŽE STE VIAZANÝ JEJ USTANOVENIAMI.

1. **Softvér**. Pojem „Softvér“ v tejto zmluve označuje (i) počítačový program, ku ktorému je priložená táto Zmluva, vrátane všetkých jeho súčastí, (ii) celý obsah diskov, CD-ROM, DVD médií, e-mailov a ich všetkých prípadných príloh alebo iných médií, ku ktorým je priložená táto Zmluva, vrátane Softvéru dodaného vo forme objektového kódu na dátovom nosiči, elektronickou poštou alebo stiahnutého cez internet, (iii) so Softvérom súvisiace vysvetľujúce písomné materiály a akúkoľvek dokumentáciu, najmä akýkoľvek popis Softvéru, jeho špecifikácie, popis vlastností, popis ovládania, popis operačného prostredia, v ktorom sa Softvér používa, pokyny na použitie alebo inštaláciu Softvéru alebo akýkoľvek popis používania Softvéru („Dokumentácia“), (iv) kópie Softvéru, opravy prípadných chýb Softvéru, dodatky k Softvéru, rozšírenia Softvéru, modifikované verzie Softvéru a aktualizácie súčastí Softvéru, ak sú dodané, na ktoré vám Poskytovateľ udeľuje licenciu v zmysle článku 3. tejto Zmluvy. Softvér sa dodáva výlučne vo forme spustiteľného objektového kódu.

2. **Inštalácia, počítač a licenčný kľúč**. Softvér dodaný na pamäťovom médiu, odoslaný elektronickou poštou, stiahnutý z internetu, stiahnutý zo serverov Poskytovateľa alebo získaný z iných zdrojov je nutné inštalovať. Softvér je potrebné inštalovať do správne nakonfigurovaného počítača, ktorý spĺňa minimálne požiadavky uvedené v Dokumentácii. Spôsob inštalácie je popísaný v Dokumentácii. Do počítača, do ktorého inštalujete Softvér, sa nesmú inštalovať žiadne počítačové programy ani hardvér, ktorý by mohol mať na Softvér negatívny vplyv. Počítač znamená hardvér vrátane, okrem iného, osobných počítačov, notebookov, pracovných staníc, vreckových počítačov, smartfónov, ručných elektronických zariadení a ďalších elektronických zariadení, pre ktoré je Softvér určený a v ktorých sa bude inštalovať a/alebo používať. Licenčný kľúč znamená jedinečnú postupnosť symbolov, písmen, číslic alebo špeciálnych znakov poskytnutú Koncovému používateľovi a umožňujúcu legálne používanie Softvéru, jeho konkrétnej verzie alebo predĺženie obdobia licencie v súlade s touto Dohodou.

3. **Licencia**. Za predpokladu, že ste súhlasili s podmienkami tejto zmluvy a dodržiavate všetky jej zmluvné podmienky, poskytovateľ vám udeľuje nasledujúce práva („licencia“):

a) **Inštalácia a používanie**. Máte nevýhradné a neprevoditeľné, časovo obmedzené právo inštalovať Softvér na pevný disk počítača alebo na iné podobné médium slúžiace na trvalé ukladanie dát, inštaláciu a na ukladanie Softvéru do pamäte počítačového systému, na vykonávanie, na ukladanie a na zobrazovanie Softvéru.

b) **Stanovenie počtu licencií.** Právo na použitie Softvéru sa viaže na počet Koncových používateľov. Jedným Koncovým používateľom sa pritom rozumie: (i) inštalácia Softvéru na jednom počítačovom systéme, alebo (ii) ak sa rozsah licencie viaže na počet poštových schránok, potom sa rozumie jedným Koncovým používateľom užívateľ počítača, ktorý si pomocou Mail User Agent („MUA“) preberá elektronickú poštu. Ak MUA preberá elektronickú poštu a následne ju automaticky rozdeľuje viacerým používateľom potom sa počet Koncových používateľov stanovuje podľa skutočného počtu užívateľov, pre ktorých je elektronická pošta rozdeľovaná. V prípade, že poštový server vykonáva funkciu poštovej brány, je počet Koncových používateľov zhodný s počtom užívateľov poštových serverov, pre ktoré poskytuje táto brána služby. Pokiaľ je jednému používateľovi smerovaný ľubovoľný počet adries elektronickej pošty (napríklad pomocou aliasov) a preberá si ich jeden používateľ, a správy nie sú automaticky na strane klienta rozdeľované pre viac používateľov, je potrebná licencia pre jeden počítač. Jednu licenciu nesmiete súčasne používať na viacerých počítačoch. Koncový používateľ smie zadať licenčný kľúč v Softvéri len v rozsahu, v ktorom má Koncový používateľ právo používať Softvér v súlade s obmedzením vyplývajúcim z počtu Licencií pridelených Poskytovateľom. Licenčný kľúč sa považuje za dôverný – Licenciu

nesmiete zdieľať s tretími stranami a ani nesmiete tretím stranám umožniť používať licenčný kľúč, ak to nie je povolené v tejto Dohode alebo Poskytovateľom. Ak dôjde k neoprávnenému použitiu vášho licenčného kľúča, okamžite informujte Poskytovateľa.

c) **Home/Business Edition.** Verzia Softvéru Home Edition je určená výlučne na domáce a rodinné používanie v súkromných alebo nekomerčných prostrediach. Na použitie v komerčnom prostredí, ako aj na použitie Softvéru na mailových serveroch, mail relay serveroch, mailových bránach alebo internetových bránach musíte získať Softvér vo verzii Business Edition.

d) **Trvanie Licencie.** Vaše právo používať Softvér je časovo obmedzené.

e) **OEM Softvér.** Softvér klasifikovaný ako OEM je obmedzený len na počítač, s ktorým bol získaný. Nie je ho možné preniesť na iný počítač.

f) **NFR, TRIAL Softvér.** Softvér označený ako „Nepredajný“, „Not-for-resale“, NFR alebo TRIAL nemôžete previesť za protihodnotu alebo používať na iný účel, ako na predvádzanie, testovanie jeho vlastností alebo vyskúšanie.

g) **Zánik Licencie.** Licencia zaniká automaticky uplynutím obdobia, na ktoré bola udelená. Ak nedodržíte ktorékoľvek ustanovenie tejto Dohody má Poskytovateľ právo odstúpiť od Dohody bez toho, aby bol dotknutý akýkoľvek nárok alebo prostriedok, ktorý má Poskytovateľ pre takýto prípad k dispozícii. V prípade zrušenia licencie musíte softvér a všetky záložné kópie okamžite odstrániť, zničiť alebo na svoje náklady vrátiť spoločnosti ESET alebo na miesto, kde ste softvér získali. Zánikom Licencie je tiež Poskytovateľ oprávnený ukončiť možnosť Koncového používateľa používať funkcie Softvéru, ktoré vyžadujú pripojenie k serverom Poskytovateľa alebo serverom tretích strán.

4. **Funkcie so zhromažďovaním údajov a požiadavky na pripojenie na internet.** Softvér na svoje správne fungovanie vyžaduje pripojenie na internet a musí sa v pravidelných intervaloch pripájať na servery Poskytovateľa alebo servery tretích strán. Takisto vyžaduje zhromažďovanie príslušných údajov v súlade so Zásadami ochrany osobných údajov. Pripojenie na internet a zhromažďovanie údajov je nevyhnutné na tieto funkcie Softvéru:

a) **Aktualizácia Softvéru.** Poskytovateľ môže príležitostne vydávať aktualizácie alebo inovácie Softvéru („Update“), nie je však povinný poskytovať Update. Táto funkcia je pri štandardnom nastavení Softvéru zapnutá, preto sa Update nainštaluje automaticky, okrem prípadov, keď Koncový používateľ automatickú inštaláciu Update zakázal. Pre poskytovanie aktualizácii sa vyžaduje overenie pravosti Licencie vrátane informácií o počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, v súlade so Zásadami ochrany osobných údajov.

Na poskytovanie akýchkoľvek aktualizácií sa môžu vzťahovať Zásady Ukončenia životného cyklu („Zásady Ukončenia životného cyklu“), ktoré sú k dispozícii na adrese https://go.eset.com/eol. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebudú sa poskytovať žiadne aktualizácie.

b) **Preposielanie infiltrácií a informácií Poskytovateľovi.** Softvér obsahuje funkcie, ktoré zhromažďujú vzorky počítačových vírusov a iných škodlivých počítačových programov, ako aj podozrivých, problémových, potenciálne nechcených alebo potenciálne nebezpečných objektov, ako sú napríklad súbory, URL adresy, IP pakety a ethernetové rámce („Infiltrácie“), a potom ich odosiela Poskytovateľovi vrátane, nie však výhradne, informácií o procese inštalácie, počítači a/alebo platforme, na ktorej je Softvér nainštalovaný, a/alebo informácií o prevádzke a fungovaní Softvéru („Informácie“.) Informácie a Infiltrácie môžu obsahovať údaje (vrátane náhodne alebo neúmyselne získaných osobných údajov) o Koncovom používateľovi alebo iných používateľoch počítača, v ktorom je Softvér nainštalovaný, a súboroch postihnutých Infiltráciami spolu so súvisiacimi metaúdajmi.

Informácie a Infiltrácie sa môžu zhromažďovať prostredníctvom nasledujúcich funkcií Softvéru:

i. Súčasťou funkcie LiveGrid Reputation System je zhromažďovanie a odosielanie jednosmerných hodnôt hash

súvisiacich s infiltráciami Poskytovateľovi. Táto funkcia sa zapína v štandardných nastaveniach Softvéru.

ii. Súčasťou funkcie LiveGrid Feedback System je zhromažďovanie a odosielanie Infiltrácií spolu so súvisiacimi metaúdajmi a Informáciami Poskytovateľovi. Túto funkciu môže aktivovať Koncový používateľ počas inštalácie Softvéru.

Poskytovateľ použije získané Informácie a Infiltrácie iba na účely analýzy a preskúmania Infiltrácií, vylepšenia Softvéru a overenia pravosti Licencie, pričom vykoná primerané opatrenia na zachovanie zabezpečenia získaných Infiltrácií a Informácií. Aktivovaním tejto funkcie Softvéru môže Poskytovateľ zhromažďovať a spracúvať Infiltrácie a Informácie v súlade so zásadami ochrany osobných údajov a príslušnými právnymi predpismi. Tieto funkcie môžete kedykoľvek deaktivovať.

Na účely tejto Dohody je potrebné zhromažďovať, spracúvať a ukladať údaje umožňujúce Poskytovateľovi identifikovať vás v súlade so Zásadami ochrany osobných údajov. Týmto beriete na vedomie, že Poskytovateľ kontroluje s využitím vlastných prostriedkov, či Softvér používate v súlade s ustanoveniami tejto Dohody. Zároveň týmto beriete na vedomie, že na účely tejto Dohody je počas komunikácie medzi Softvérom a počítačovými systémami Poskytovateľa alebo jeho obchodných partnerov v rámci distribučnej a podpornej siete Poskytovateľa potrebný prenos údajov na zabezpečenie funkčnosti Softvéru a oprávnenia na používanie Softvéru a na ochranu práv Poskytovateľa.

Po uzavretí tejto Dohody je Poskytovateľ alebo ľubovoľný jeho obchodný partner v rámci distribučnej a podpornej siete Poskytovateľa oprávnený na účely fakturácie, plnenia tejto Dohody a prenosu oznámení do vášho počítača v nevyhnutnom rozsahu prenášať, spracovávať a uchovávať dôležité údaje, ktoré vás umožnia identifikovať.

Podrobné informácie o ochrane súkromia, ochrane osobných údajov a vašich právach ako dotknutej osoby sú uvedené v zásadách ochrany osobných údajov dostupných na webových stránkach Poskytovateľa a prístupných priamo počas procesu inštalácie. Prístup k nim môžete získať aj v pomocníkovi softvéru.

5. **Výkon práv Koncového používateľa**. Práva Koncového používateľa musíte vykonávať osobne alebo prostredníctvom svojich prípadných zamestnancov. Softvér môžete použiť výlučne na zabezpečenie svojej činnosti a na ochranu len tých počítačových systémov, pre ktoré ste získali Licenciu.

6. **Obmedzenie práv.** Nesmiete Softvér kopírovať, šíriť, oddeľovať jeho časti alebo vytvárať od Softvéru odvodené diela. Pri používaní Softvéru ste povinný dodržiavať nasledovné obmedzenia:

a) Môžete pre seba vytvoriť jedinú kópiu Softvéru na médiu určenom na trvalé ukladanie dát ako záložnú kópiu, za predpokladu, že vaša archívna záložná kópia sa nebude inštalovať alebo používať na inom počítači. Vytvorenie akejkoľvek ďalšej kópie Softvéru je porušením tejto Dohody.

b) Softvér nesmiete používať, upravovať, prekladať, reprodukovať, alebo prevádzať práva na používanie Softvéru alebo kópií Softvéru inak, než je výslovne uvedené v tejto Dohode.

c) Softvér nesmiete predať, sublicencovať, prenajať alebo prenajať si, vypožičať si ho alebo používať na poskytovanie komerčných služieb.

d) Softvér nesmiete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsiť získať zdrojový kód Softvéru s výnimkou rozsahu, v ktorom je takéto obmedzenie výslovne zakázané zákonom.

e) Súhlasíte s tým, že budete používať Softvér iba spôsobom, ktorý je v súlade so všetkými platnými právnymi predpismi v právnom systéme, v ktorom Softvér používate, najmä v súlade s platnými obmedzeniami vyplývajúcimi z autorského práva a ďalších práv duševného vlastníctva.

f) Súhlasíte s tým, že budete používať Softvér a jeho funkcie výlučne spôsobom, ktorý neobmedzí možnosti iných Koncových používateľov na prístup k týmto službám. Poskytovateľ si vyhradzuje právo obmedziť rozsah služieb poskytovaných jednotlivým Koncovým používateľom tak, aby umožnil ich využívanie čo najväčšiemu počtu Koncových používateľov. Obmedzenie rozsahu služieb môže znamenať aj úplné zrušenie možnosti používať niektorú z funkcií Softvéru a likvidáciu Údajov a informácií na serveroch Poskytovateľa alebo serveroch tretích strán spojených danou funkciou Softvéru.

g) Súhlasíte s tým, že nebudete vykonávať žiadne činnosti zahŕňajúce použitie licenčného kľúča v rozpore s podmienkami tejto Dohody alebo vedúce k poskytnutiu licenčného kľúča akejkoľvek osobe, ktorá nie je oprávnená používať Softvér, ako napríklad prenos použitého alebo nepoužitého licenčného kľúča v akejkoľvek forme, ako aj neoprávnená reprodukcia alebo distribúcia duplikovaných alebo generovaných licenčných kľúčov alebo používanie Softvéru v dôsledku použitia licenčného kľúča získaného od iného zdroja ako od Poskytovateľa.

7. **Autorské práva**. Softvér a všetky práva, najmä vlastnícke práva a práva duševného vlastníctva k nemu, sú vlastníctvom spoločnosti ESET a/alebo jej poskytovateľov licencií. Tieto sú chránené ustanoveniami medzinárodných dohôd a všetkými ďalšími aplikovateľnými zákonmi krajiny, v ktorej sa Softvér používa. Štruktúra, organizácia a kód Softvéru sú obchodnými tajomstvami a dôvernými informáciami spoločnosti ESET a/alebo jej poskytovateľov licencií. Softvér nesmiete kopírovať, s výnimkou uvedenou v ustanovení článku 6 písmeno a). Akékoľvek kópie, ktoré smiete vytvoriť podľa tejto Zmluvy, musia obsahovať rovnaké upozornenia na autorské a vlastnícke práva, aké sú uvedené na Softvéri. V prípade, že v rozpore s ustanoveniami tejto Dohody budete spätne analyzovať, dekompilovať, prevádzať do zdrojového kódu alebo sa iným spôsobom pokúsite získať zdrojový kód, súhlasíte s tým, že takto získané informácie sa budú automaticky a neodvolateľne považovať za prevedené na Poskytovateľa a vlastnené v plnom rozsahu Poskytovateľom od okamihu ich vzniku, tým nie sú dotknuté práva Poskytovateľa spojené s porušením tejto Dohody.

8. **Výhrada práv**. Všetky práva k Softvéru, okrem práv ktoré Vám ako Koncovému používateľovi Softvéru boli výslovne udelené v tejto Dohode, si Poskytovateľ vyhradzuje pre seba.

9. **Viaceré jazykové verzie, verzie pre viac operačných systémov, viaceré kópie**. V prípade ak Softvér podporuje viaceré platformy alebo jazyky, alebo ak ste získali viac kópii Softvéru, môžete Softvér používať len na takom počte počítačových systémov a v takých verziách, na ktoré ste získali Licenciu. Verzie alebo kópie Softvéru, ktoré nepoužívate nesmiete predať, prenajať, sublicencovať, zapožičať alebo previesť na iné osoby.

10. **Začiatok a trvanie Dohody.** Táto Dohoda je platná a účinná odo dňa, kedy ste odsúhlasili túto Dohodu. Dohodu môžete kedykoľvek ukončiť tak, že natrvalo odinštalujete zničíte alebo na svoje vlastné náklady vrátite Softvér, všetky prípadné záložné kópie a všetok súvisiaci materiál, ktorý ste získali od Poskytovateľa alebo jeho obchodných partnerov. Na vaše právo používať Softvér a ktorúkoľvek z jeho funkcií sa môžu vzťahovať Zásady Ukončenia životného cyklu. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, vaše právo používať Softvér zanikne. Bez ohľadu na spôsob zániku tejto Dohody, ustanovenia jej článkov 7, 8, 11, 13, 19 a 21 zostávajú v platnosti bez časového obmedzenia.

11. **VYHLÁSENIA KONCOVÉHO POUŽÍVATEĽA**. AKO KONCOVÝ POUŽÍVATEĽ UZNÁVATE, ŽE SOFTVÉR JE POSKYTOVANÝ "AKO STOJÍ A LEŽÍ", BEZ VÝSLOVNEJ ALEBO IMPLIKOVANEJ ZÁRUKY AKÉHOKOĽVEK DRUHU A V MAXIMÁLNEJ MIERE DOVOLENEJ APLIKOVATEĽNÝMI ZÁKONMI. ANI POSKYTOVATEĽ, ANI JEHO POSKYTOVATELIA LICENCIÍ, ANI DRŽITELIA AUTORSKÝCH PRÁV NEPOSKYTUJÚ AKÉKOĽVEK VÝSLOVNÉ ALEBO IMPLIKOVANÉ PREHLÁSENIA ALEBO ZÁRUKY, NAJMÄ NIE ZÁRUKY PREDAJNOSTI ALEBO VHODNOSTI PRE KONKRÉTNY ÚČEL ALEBO ZÁRUKY, ŽE SOFTVÉR NEPORUŠUJE ŽIADNE PATENTY, AUTORSKÉ PRÁVA, OCHRANNÉ ZNÁMKY ALEBO INÉ PRÁVA TRETÍCH STRÁN. NEEXISTUJE ŽIADNA ZÁRUKA ZO STRANY POSKYTOVATEĽA ANI ŽIADNEJ ĎALŠEJ STRANY, ŽE FUNKCIE, KTORÉ OBSAHUJE SOFTVÉR, BUDÚ VYHOVOVAŤ VAŠÍM POŽIADAVKÁM, ALEBO ŽE PREVÁDZKA SOFTVÉRU BUDE NERUŠENÁ A BEZCHYBNÁ. PREBERÁTE ÚPLNÚ ZODPOVEDNOSŤ A RIZIKO ZA VÝBER SOFTVÉRU PRE DOSIAHNUTIE VAMI ZAMÝŠĽANÝCH VÝSLEDKOV A ZA INŠTALÁCIU, POUŽÍVANIE A VÝSLEDKY, KTORÉ SO

SOFTVÉROM DOSIAHNETE.

12. **Žiadne ďalšie záväzky.** Táto Dohoda nezakladá na strane Poskytovateľa a jeho prípadných poskytovateľov licencií okrem záväzkov konkrétne uvedených v tejto Dohode žiadne iné záväzky.

13. **OBMEDZENIE ZODPOVEDNOSTI**. V MAXIMÁLNEJ MIERE, AKÚ DOVOĽUJE APLIKOVATEĽNÉ PRÁVO, V ŽIADNOM PRÍPADE NEBUDE POSKYTOVATEĽ, JEHO ZAMESTNANCI ALEBO JEHO POSKYTOVATELIA LICENCIÍ ZODPOVEDAŤ ZA AKÝKOĽVEK UŠLÝ ZISK, PRÍJEM ALEBO PREDAJ, ALEBO ZA AKÚKOĽVEK STRATU DÁT, ALEBO ZA NÁKLADY VYNALOŽENÉ NA OBSTARANIE NÁHRADNÝCH TOVAROV ALEBO SLUŽIEB, ZA MAJETKOVÉ ŠKODY, ZA OSOBNÚ UJMU, ZA PRERUŠENIE PODNIKANIA, ZA STRATU OBCHODNÝCH INFORMÁCIÍ, ANI ZA AKÉKOĽVEK ŠPECIÁLNE, PRIAME, NEPRIAME, NÁHODNÉ, EKONOMICKÉ, KRYCIE, TRESTNÉ, ŠPECIÁLNE ALEBO NÁSLEDNÉ ŠKODY, AKOKOĽVEK ZAPRÍČINENÉ, ČI UŽ VYPLYNULI ZO ZMLUVY, ÚMYSELNÉHO KONANIA, NEDBALOSTI ALEBO INEJ SKUTOČNOSTI, ZAKLADAJÚCEJ VZNIK ZODPOVEDNOSTI, VZNIKNUTÉ INŠTALÁCIOU, POUŽÍVANÍM ALEBO NEMOŽNOSŤOU POUŽÍVAŤ SOFTVÉR, A TO AJ V PRÍPADE, ŽE POSKYTOVATEĽ ALEBO JEHO POSKYTOVATELIA LICENCIÍ BOLI UVEDOMENÍ O MOŽNOSTI TAKÝCHTO ŠKÔD. NAKOĽKO NIEKTORÉ ŠTÁTY A NIEKTORÉ PRÁVNE SYSTÉMY NEDOVOĽUJÚ VYLÚČENIE ZODPOVEDNOSTI, ALE MÔŽU DOVOĽOVAŤ OBMEDZENIE ZODPOVEDNOSTI, JE ZODPOVEDNOSŤ POSKYTOVATEĽA, JEHO ZAMESTNANCOV ALEBO POSKYTOVATEĽOV LICENCIÍ OBMEDZENÁ DO VÝŠKY CENY, KTORÚ STE ZAPLATILI ZA LICENCIU.

14. Žiadne ustanovenie tejto Dohody sa nedotýka práv strany, ktorej zákon priznáva práva a postavenie spotrebiteľa, pokiaľ je s nimi v rozpore.

15. **Technická podpora**. Technickú podporu poskytuje ESET alebo ním poverená tretia strana na základe vlastného uváženia bez akýchkoľvek záruk alebo prehlásení. Keď Softvér alebo ktorákoľvek z jeho funkcií dosiahne dátum Ukončenia životného cyklu stanovený v Zásadách Ukončenia životného cyklu, nebude sa poskytovať žiadna technická podpora. Koncový používateľ je povinný pred poskytnutím technickej podpory zálohovať všetky jeho existujúce dáta, softvér a programové vybavenie. ESET a/alebo ním poverená tretia strana nepreberajú zodpovednosť za poškodenie alebo stratu dát, majetku, softvéru alebo hardvéru alebo ušlý zisk pri poskytovaní technickej podpory. ESET a/alebo ním poverená tretia strana si vyhradzuje právo na rozhodnutie, že riešený problém presahuje rozsah technickej podpory. ESET si vyhradzuje právo odmietnuť, pozastaviť alebo ukončiť poskytovanie technickej podpory na základe vlastného uváženia. Informácie o Licencii, Informácie a ďalšie údaje v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely poskytovania technickej pomoci.

16. **Prevod Licencie**. Softvér môžete preniesť z jedného počítačového systému na iný počítačový systém, pokiaľ to nie je v rozpore s Dohodou. Pokiaľ to nie je v rozpore s Dohodou, Koncový používateľ môže jednorazovo trvalo previesť Licenciu a všetky práva z tejto Dohody na iného Koncového používateľa iba so súhlasom Poskytovateľa za podmienky, že (i) pôvodný Koncový používateľ si neponechá žiadnu kópiu Softvéru, (ii) prevod práv musí byť priamy, teda z pôvodného Koncového používateľa na nového Koncového používateľa, (iii) nový Koncový používateľ musí prebrať všetky práva a povinnosti, ktoré má podľa tejto Dohody pôvodný Koncový používateľa (iv) pôvodný Koncový používateľ musí odovzdať novému Koncovému používateľovi doklady umožňujúce overenie legality Softvéru ako je uvedené v článku 17.

17. **Overenie pravosti Softvéru.** Koncový používateľ musí preukázať právo na používanie Softvéru jedným z týchto spôsobov: (i) prostredníctvom osvedčenia o licencii vydaného Poskytovateľom alebo treťou stranou určenou Poskytovateľom, (ii) prostredníctvom písomnej licenčnej zmluvy, ak takáto zmluva bola uzavretá, (iii) predložením e-mailu odoslaného Poskytovateľom, ktorý obsahuje podrobnosti o licencii (meno používateľa a heslo). Informácie o Licencii a identifikačné údaje Koncového používateľa v súlade so Zásadami ochrany osobných údajov sa môžu vyžadovať na účely overenia pravosti Softvéru.

18. **Licencovanie pre štátne orgány a vládu USA**. Softvér sa poskytuje štátnym orgánom vrátane vlády Spojených štátov amerických s licenčnými právami a obmedzeniami popísanými v tejto Dohode.

19. **Súlad s kontrolou obchodu**.

a) Zaväzujete sa, že Softvér nebudete priamo alebo nepriamo vyvážať, opätovne vyvážať ani ho inak nesprístupníte žiadnej osobe, ani ho nepoužijete akýmkoľvek spôsobom, ktorý by spôsobil, že spoločnosť ESET alebo jej holdingové spoločnosti, dcérske spoločnosti alebo dcérske spoločnosti jej holdingových spoločností spolu s osobami ovládanými jej holdingovými spoločnosťami („Pobočky“) porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu, ktoré zahŕňajú:

i. všetky zákony, ktoré kontrolujú, obmedzujú alebo vynucujú licenčné podmienky vývozu, opätovného vývozu alebo prenosu výrobkov, softvéru, technológií alebo služieb vydaných alebo prijatých akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje a

ii. všetky ekonomické, finančné, obchodné alebo iné sankcie, obmedzenia, embargá, zákazy dovozu alebo vývozu, zákazy prevodu prostriedkov alebo aktív alebo poskytovania služieb alebo iné porovnateľné opatrenie prijaté akýmkoľvek vládnym, štátnym alebo regulačným úradom Spojených štátov amerických, Singapuru, Spojeného kráľovstva, Európskej únie alebo niektorým z jej členských štátov alebo ktorejkoľvek krajiny, v ktorej má byť naplnená Dohoda alebo v ktorej je spoločnosť ESET alebo niektorá z jej Pobočiek zapísaná do obchodného registra alebo v nej obchoduje.

(právne predpisy, na ktoré sa odkazuje v bodoch i. a ii. vyššie, ďalej spoločne „Zákony na kontrolu obchodu“).

b) Spoločnosť ESET si vyhradzuje právo s okamžitou platnosťou pozastaviť alebo ukončiť plnenie svojich povinností vyplývajúcich z tejto dohody v prípade, že:

i. Spoločnosť ESET rozhodne podľa svojho najlepšieho vedomia a svedomia, že Používateľ porušil alebo pravdepodobne poruší ustanovenia článku 19 bodu (a) Dohody; alebo

ii. Koncový používateľ a/alebo Softvér sa stanú predmetom zákonov na kontrolu obchodu, následkom čoho spoločnosť ESET podľa svojho najlepšieho vedomia a svedomia rozhodne, že ďalšie plnenie jej povinností vyplývajúcich z Dohody by mohlo mať za následok, že spoločnosť ESET a jej Pobočky porušia zákon alebo budú znášať postihy v rámci zákonov na kontrolu obchodu.

c) Žiadna časť Dohody nie je zamýšľaná a nesmie byť interpretovaná tak, že podnecuje niektorú zo strán či od nej vyžaduje, aby konala alebo sa zdržala konania spôsobom (či s takýmto konaním či nekonaním súhlasila), ktorý akýmkoľvek spôsobom porušuje platné zákony na kontrolu obchodu alebo sa týmito zákonmi postihuje či zakazuje.

20. **Oznámenia**. Všetky oznámenia, vrátený Softvér a Dokumentáciu je potrebné doručiť na adresu: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez toho, aby bolo dotknuté právo spoločnosti ESET oznámiť vám akékoľvek zmeny tejto Dohody, Zásad ochrany osobných údajov, Zásad Ukončenia životného cyklu a Dokumentácie v súlade s článkom 22 Dohody. Spoločnosť ESET vám môže posielať e-maily, oznámenia v aplikácii prostredníctvom Softvéru alebo uverejniť komunikáciu na svojej webovej lokalite. Súhlasíte s tým, že budete od spoločnosti ESET dostávať právnu komunikáciu v elektronickej forme vrátane akejkoľvek komunikácie o zmene podmienok, osobitných podmienok alebo zásad ochrany osobných údajov, akýchkoľvek návrhov/prijatí zmluvy alebo pozvánok, upozornení alebo inej právnej komunikácie. Takáto elektronická komunikácia sa bude považovať za prijatú v písomnej forme, pokiaľ príslušné právne predpisy osobitne nevyžadujú inú formu komunikácie.

21. **Rozhodujúce právo**. Táto Dohoda sa riadi a musí byť vykladaná v súlade so zákonmi Slovenskej republiky. Koncový používateľ a Poskytovateľ sa dohodli, že kolízne ustanovenia rozhodujúceho právneho poriadku a Dohovor OSN o zmluvách pri medzinárodnej kúpe tovarov sa nepoužijú. Výslovne súhlasíte, že riešenie akýkoľvek sporov alebo nárokov z tejto Dohody voči Poskytovateľovi alebo spory a nároky súvisiace s používaním

softvéru je príslušný Okresný súd Bratislava I a výslovne súhlasíte s výkonom jurisdikcie týmto súdom.

22. **Všeobecné ustanovenia**. V prípade, že akákoľvek ustanovenie tejto Dohody je neplatné alebo nevykonateľné, neovplyvní to platnosť ostatných ustanovení Dohody. Tie zostanú platné a vykonateľné podľa podmienok v nej stanovených. Táto Dohoda bola vyhotovená v angličtine. V prípade, že je z praktických dôvodov alebo na akýkoľvek iný účel vypracovaný akýkoľvek preklad Dohody, alebo v prípade akýchkoľvek nezrovnalostí medzi jazykovými verziami tejto Dohody platí verzia v angličtine.

Spoločnosť ESET si vyhradzuje právo kedykoľvek vykonať zmeny v Softvéri, ako aj kedykoľvek upraviť podmienky tejto Dohody, jej prílohy, dodatky, Zásady ochrany osobných údajov, Zásady Ukončenia životného cyklu a dokumentáciu, prípadne ich ľubovoľnú časť tak, že aktualizuje príslušný dokument: (i) aby zohľadňoval zmeny v Softvéri alebo v tom, ako spoločnosť ESET vykonáva podnikateľskú činnosť, (ii) z právnych, regulačných alebo bezpečnostných dôvodov alebo (iii) na zabránenie zneužitiu alebo ublíženiu. O každej úprave Dohody vás informujeme prostredníctvom e-mailu, oznámenia v aplikácii alebo iným spôsobom elektronickej komunikácie. Ak s navrhovanými zmenami Dohody nebudete súhlasiť, môžete ju v súlade s článkom 10 ukončiť do 30 dní od prijatia oznámenia o zmene. Ak Dohodu v tejto časovej lehote neukončíte, navrhované zmeny sa budú považovať za prijaté a nadobudnú voči vám účinnosť k dátumu prijatia oznámenia o zmene.

Táto Zmluva medzi Vami a Poskytovateľom predstavuje jedinú a úplnú Zmluvu vzťahujúcu sa na Softvér, a plne nahrádza akékoľvek predchádzajúce vyhlásenia, rokovania, záväzky, správy alebo reklamné informácie, týkajúce sa Softvéru.

EULAID: EULA-PRODUCT-LG; 3537.0

Zásady ochrany osobných údajov

Spoločnosť ESET, spol. s r. o. so sídlom na adrese Einsteinova 24, 851 01 Bratislava, Slovak Republic, zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sro, vložka číslo 3586/B, IČO: 31333532, ako prevádzkovateľ údajov (ďalej len „ESET“ alebo „my“) kladie veľký dôraz na ochranu osobných údajov. Chceme splniť požiadavku transparentnosti, ktorá je právne štandardizovaná vo všeobecnom nariadení EÚ o ochrane údajov (ďalej len „GDPR“). S týmto cieľom zverejňujeme tieto zásady ochrany osobných údajov, ktorých jediným účelom je informovať nášho zákazníka (ďalej len „koncový používateľ“ alebo „vy“) ako dotknutú osobu o týchto témach ochrany osobných údajov:

- právny základ spracúvania osobných údajov;
- zdieľanie a dôvernosť údajov;
- bezpečnosť údajov;
- práva, ktoré máte ako dotknutá osoba;
- spracúvanie osobných údajov;
- Kontaktné informácie.

Spracúvanie osobných údajov

Služby poskytované spoločnosťou ESET a realizované v rámci nášho produktu sa poskytujú v súlade s podmienkami dohody LICENČNÁ DOHODA (EULA), ale niektoré z nich si môžu vyžadovať osobitnú pozornosť. Chceme vám poskytnúť podrobnejšie informácie o zhromažďovaní údajov, ktoré súvisí s poskytovaním našich služieb. Poskytujeme rôzne služby, ktoré sú opísané v zmluve EULA, ako aj v produktovej dokumentácii. Poskytujeme rôzne služby opísané v dohode EULA a produktovej dokumentácii. Nato, aby všetko fungovalo, ako má, musíme zhromažďovať tieto informácie:

- Informácie o aktualizáciách a ďalšie štatistické informácie týkajúce sa procesu inštalácie a počítača vrátane

informácií o platforme, na ktorej je produkt nainštalovaný, a informácií o operáciách a funkčnosti našich produktov, napríklad informácie o operačnom systéme, hardvéri, identifikátoroch inštalácie, identifikácii licencie, IP adrese, MAC adrese a nastaveniach konfigurácie produktu.

- Jednosmerné haše súvisiace s infiltráciami, ktoré sú zhromažďované v rámci reputačného systému ESET LiveGrid® a ktorými sa zlepšuje účinnosť našich antimalvérových riešení na základe porovnávania naskenovaných súborov s databázou položiek zaradených na whitelist a blacklist v cloude.
- Prijaté podozrivé vzorky a metadáta zhromažďované v rámci systému spätnej väzby ESET LiveGrid®, ktoré umožňujú spoločnosti ESET okamžite reagovať na potreby svojich koncových používateľov, ako aj na najnovšie hrozby. Spoliehame sa na to, že nám zašlete
    - infiltrácie, ako napríklad vzorky potenciálnych vírusov a iných škodlivých a podozrivých programov; problematické, potenciálne neželané alebo potenciálne nebezpečné objekty, ako napríklad spustiteľné súbory, e-mailové správy, ktoré ste nahlásili ako spam alebo ktoré takto označil váš produkt;
    - informácie o zariadeniach v lokálnej sieti, ako napríklad typ, dodávateľ, model a/alebo názov zariadenia;
    - informácie o používaní internetu, ako napríklad IP adresu, geografické informácie, IP pakety, URL adresy a ethernetové rámce;
    - súbory výpisov pri zlyhaní a informácie, ktoré obsahujú.

Nemáme v úmysle zhromažďovať vaše údaje mimo tohto rozsahu, niekedy sa tomu však nedá zabrániť. Náhodne zhromaždené údaje môžu byť obsiahnuté v samotnom malvéri (zhromaždené bez vášho vedomia alebo súhlasu) alebo môžu byť súčasťou názvov súborov či URL adries a my nemáme v úmysle začleniť ich do našich systémov ani ich spracovať na účely uvedené v týchto zásadách ochrany osobných údajov.

- Licenčné informácie, ako napríklad identifikácia licencie, a osobné údaje, ako napríklad meno, priezvisko, adresa a e-mailová adresa, sa vyžadujú na fakturačné účely, overenie pravosti licencie a poskytovanie našich služieb.
- Kontaktné informácie a údaje obsiahnuté vo vašich žiadostiach o podporu sa vyžadujú na poskytnutie technickej alebo inej podpory spoločnosťou ESET. Podľa toho, akým spôsobom sa nás rozhodnete kontaktovať, môžeme zhromažďovať informácie, ako sú napríklad vaša e-mailová adresa, telefónne číslo, licenčné informácie, podrobnosti o produkte a popis vášho konkrétneho prípadu podpory. Na zjednodušenie poskytnutia podpory vás môžeme požiadať o poskytnutie ďalších informácií.

Zdieľanie a dôvernosť údajov

Vaše údaje nezdieľame s tretími stranami. Spoločnosť ESET však pôsobí globálne prostredníctvom pridružených spoločností alebo partnerov v rámci svojej siete predaja, služieb a podpory. Informácie o správe licencií, účtovaní a technickej podpore spracúvané spoločnosťou ESET sa môžu prenášať medzi pridruženými subjektmi alebo partnermi na účely plnenia dohody EULA, ako je napríklad poskytovanie služieb alebo podpory.

Spoločnosť ESET uprednostňuje spracúvanie údajov v krajinách Európskej únie (EÚ). V závislosti od vašej polohy (používanie našich produktov a/alebo služieb mimo EÚ) a/alebo vami vybratej služby však môže byť nevyhnutné preniesť vaše údaje do krajiny mimo EÚ. Využívame napríklad služby tretích strán spojené s cloudovou výpočtovou technikou. V týchto prípadoch si dôkladne vyberáme poskytovateľov služieb a dbáme na ochranu údajov na primeranej úrovni prostredníctvom zmluvných, ale tiež technických a organizačných opatrení. V prípade potreby sa spravidla dohodneme na štandardných zmluvných doložkách EÚ s doplnkovými zmluvnými pravidlami.

Pri niektorých krajinách mimo EÚ, ako je napríklad Spojené kráľovstvo a Švajčiarsko, už EÚ určila porovnateľnú úroveň ochrany údajov. Z dôvodu porovnateľnej úrovne ochrany údajov sa pri prenose údajov do týchto krajín nevyžaduje žiadne osobitné oprávnenie ani dohoda.

Práva dotknutej osoby

Práva každého koncového používateľa sú dôležité a chceme vás informovať, že všetci koncoví používatelia (z ktorejkoľvek krajiny EÚ aj mimo EÚ) majú práva uvedené nižšie zaručené spoločnosťou ESET. Ak chcete uplatniť svoje práva dotknutej osoby, môžete nás kontaktovať prostredníctvom formulára podpory alebo e-mailom na adrese dpo@eset.sk. Na účely identifikácie vás požiadame o tieto informácie: meno, e-mailovú adresu a (ak sú tieto informácie k dispozícii) licenčný kľúč alebo číslo zákazníka a pridruženú spoločnosť. Neodosielajte nám žiadne iné osobné údaje, napríklad dátum narodenia. Chceme zdôrazniť, že na účely spracovania vašej žiadosti, ako aj na účely identifikácie, budeme spracúvať vaše osobné údaje.

Právo na odvolanie súhlasu. Právo na odvolanie súhlasu sa uplatňuje v prípade spracúvania, ktoré je založené len na súhlase. Ak vaše osobné údaje spracúvame na základe vášho súhlasu, máte právo súhlas kedykoľvek odvolať aj bez uvedenia dôvodu. Odvolanie súhlasu je účinné len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred odvolaním.

Právo namietať. Právo namietať voči spracúvaniu sa uplatňuje v prípade spracúvania na základe oprávneného záujmu spoločnosti ESET alebo tretej strany. Ak vaše osobné údaje spracúvame na ochranu oprávneného záujmu, ako dotknutá osoba máte právo kedykoľvek namietať voči nami uvedenému oprávnenému záujmu a spracúvaniu vašich osobných údajov. Vaša námietka je účinná len pre budúcnosť a nemá vplyv na zákonnosť spracúvania údajov pred námietkou. Ak vaše osobné údaje spracúvame na účely priameho marketingu, nie je potrebné uvádzať dôvody námietky. Platí to aj pre profilovanie, pokiaľ je spojené s takýmto priamym marketingom. Vo všetkých ostatných prípadoch vás požiadame, aby ste nás stručne informovali o svojich sťažnostiach týkajúcich sa oprávneného záujmu spoločnosti ESET spracúvať vaše osobné údaje.

V niektorých prípadoch máme oprávnenie napriek vášmu odvolaniu súhlasu ďalej spracúvať vaše osobné údaje na inom právnom základe, napríklad na účely plnenia zmluvy.

Právo prístupu. Ako dotknutá osoba máte právo kedykoľvek bezplatne získať informácie o svojich údajoch, ktoré uchováva spoločnosť ESET.

Právo na opravu. Ak neúmyselne spracúvame vaše nesprávne osobné údaje, máte právo na ich opravu.

Právo na vymazanie a právo na obmedzenie spracúvania. Ako dotknutá osoba máte právo požiadať o vymazanie alebo obmedzenie spracúvania svojich osobných údajov. Ak napríklad vaše osobné údaje spracúvame s vaším súhlasom, odvoláte ho a neexistuje žiadny iný právny základ, ako je napríklad zmluva, vaše osobné údaje vymažeme okamžite. Vaše osobné údaje tiež budú vymazané, keď už nebudú potrebné na účely, ktoré sú pre ne uvedené, na konci nášho obdobia uchovávania.

Ak vaše osobné údaje používame výhradne na účely priameho marketingu a odvoláte súhlas alebo budete namietať voči existujúcemu oprávnenému záujmu spoločnosti ESET, spracúvanie vašich osobných údajov obmedzíme tak, že pridáme vaše kontaktné údaje do svojho interného blacklistu, aby nedošlo k nevyžiadanému kontaktu. V opačnom prípade sa vaše osobné údaje vymažú.

Upozorňujeme, že sa od nás môže žiadať, aby sme vaše údaje uchovávali až do uplynutia povinností a období uchovávania stanovených zákonodarcom alebo dozornými orgánmi. Povinnosti a obdobia uchovávania tiež môžu vyplývať z právnych predpisov Slovenskej republiky. Po ich uplynutí sa príslušné údaje vymažú zvyčajným spôsobom.

Právo na prenosnosť údajov. Ako dotknutej osobe vám radi poskytneme osobné údaje spracúvané spoločnosťou ESET vo formáte XLS.

Právo podať sťažnosť. Ako dotknutá osoba máte právo kedykoľvek podať sťažnosť dozornému orgánu. Spoločnosť

ESET podlieha slovenským zákonom a je viazaná právnymi predpismi Európskej únie o ochrane údajov. Príslušným dozorným orgánom na ochranu údajov je Úrad na ochranu osobných údajov Slovenskej republiky so sídlom na adrese Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Kontaktné informácie

Ak chcete využiť svoje právo dotknutej osoby alebo chcete položiť otázku či vyjadriť obavu, obráťte sa na nás na adrese:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk