SECURITY MANAGEMENT CENTER

Administrátorská príručka

Pre stiahnutie najnovšej verzie tohto dokumentu kliknite sem

ENJOY SAFER TECHNOLOGY™

ESET **SECURITY MANAGEMENT CENTER 7**

Copyright © 2018 **ESET, spol. s r.o.**
ESET Security Management Center 7 bol vyvinutý spoločnosťou ESET, spol. s r. o.

Pre viac informácií navštívte webovú stránku www.eset.sk.
Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukovaná žiadnym prostriedkom ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti ESET, spol. s r. o.
ESET, spol. s r. o. si vyhradzuje právo zmeny programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

Kontaktný formulár: http://www.eset.com/sk/podpora/formular/ tel.: +421 (2) 322 44 444

REV. 15.08.2018

Obsah

Obsah

Obsah

1. Úvod

Vitajte v príručke správcu pre produkt ESMC. Cieľom tohto dokumentu je vysvetliť, ako spravovať bezpečnostné riešenia spoločnosti ESET určené pre firmy v rámci vašej infraštruktúry. Tento dokument tiež popisuje zmeny v najnovšej verzii ESMC, ako aj scenáre pre správcov a používateľov, ktorí budú pracovať s nástrojom ESMC Web Console.

1.1 O tejto príručke

Táto príručka správcu bola napísaná tak, aby vám pomohla oboznámiť sa s produktom ESET Security Management Center a poskytla inštrukcie, ako ho správne používať.

Pre zachovanie konzistentnosti, a aby sa zabránilo zámene, je terminológia použitá v tejto príručke založená na názvoch parametrov nástroja ESET Security Management Center. Používame tiež jednotnú sadu symbolov na zvýraznenie kapitol, ktoré sú zvlášť dôležité alebo sú iným spôsobom markantné.

Poznámka:
Poznámky môžu poskytovať cenné informácie, ako napríklad špecifické funkcie alebo odkaz na súvisiacu kapitolu.

Dôležité:
Takéto označenie vyžaduje vašu pozornosť a neodporúča sa ho ignorovať. Zvyčajne poskytuje dôležité informácie.

Upozornenie:
Toto označenie obsahuje mimoriadne dôležité informácie, pri ktorých by ste mali spozornieť. Upozornenia sú umiestnené tak, aby vás včas varovali a zároveň vám pomohli predísť chybám, ktoré by mohli mať negatívne následky. Prosím, dôkladne si prečítajte text ohraničený týmto označením, pretože sa týka vysoko citlivých systémových nastavení alebo upozorňuje na riziká.

PRÍKLAD:
Toto označenie obsahuje ukážkový príklad, ktorý priamo súvisí s informáciami v príslušnej kapitole. Príklady sa využívajú hlavne pri komplikovanejších kapitolách.

Konvencia	Význam
Tučné písmo	Pomenúva položky rozhrania, ako napr. polia a tlačidlá možností.
Kurzíva	Zástupné symboly pre údaje, ktoré máte poskytnúť. Napríklad, *file name* alebo *path* znamená, že máte zadať konkrétnu cestu alebo názov súboru.
`Courier New`	Príklady kódov alebo príkazov.
Hypertextové prepojenie	Poskytuje rýchly a jednoduchý prístup k súvisiacim prepojeným kapitolám alebo externým webovým lokalitám. Hypertextové prepojenia sú zvýraznené modrou farbou a môžu byť podčiarknuté.
%ProgramFiles%	Systémový adresár Windows, kde sú uložené programy systému Windows a ďalšie programy.

- Online pomocník je hlavným zdrojom pomocného obsahu. Pri pripojení na internet je zobrazovaná vždy najnovšia verzia online pomocníka. Online pomocník pre produkt ESET Security Management Center obsahuje tri aktívne karty na vrchnej navigačnej hlavičke: Inštalácia/aktualizácia, Administrácia a Nasadenie VA.

- Táto príručka je rozdelená na niekoľko kapitol a podkapitol. Konkrétne informácie môžete vyhľadať pomocou poľa **Hľadaj** v hornej časti.

Dôležité:
Keď otvoríte používateľskú príručku z navigačného panela umiestneného vo vrchnej časti stránky, vyhľadávanie bude obmedzené len na obsah danej príručky. Napríklad, ak otvoríte časť Administrácia, kapitoly z časti Inštalácia/aktualizácia a Nasadenie VA nebudú zahrnuté do výsledkov vyhľadávania.

- 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.
- ESET fórum poskytuje používateľom produktov spoločnosti ESET jednoduchý spôsob, ako získať pomoc a zároveň pomôcť iným. Môžete tam uverejniť akúkoľvek otázku alebo sa informovať o akomkoľvek probléme v súvislosti s produktmi spoločnosti ESET.
- Môžete odoslať vaše hodnotenie alebo poskytnúť spätnú väzbu v rámci určitej kapitoly v pomocníkovi. Kliknite na odkaz **Boli tieto informácie užitočné?** alebo na **Ohodnoťte tento článok: Užitočné/Neužitočné** v spodnej časti stránky.

1.1.1 Offline pomocník

Offline pomocník pre ESET Security Management Center nie je predvolene nainštalovaný. Ak potrebujete pomocníka pre ESET Security Management Center, ktorého môžete použiť aj keď ste offline (v prípade, že nemáte prístup na internet), postupujte podľa nasledujúcich krokov.

Kliknite na jazykový kód pre stiahnutie Offline pomocníka pre nástroj ESET Security Management Center v požadovanom jazyku. Offline pomocník môže byť nainštalovaný vo viacerých jazykoch.

Pokyny na inštaláciu Offline pomocníka na systéme Windows

1. **Stiahnite si** súbor *.zip* kliknutím na jazykový kód v tabuľke nižšie, čím stiahnete Offline pomocníka pre nástroj ESET Security Management Center v požadovanom jazyku.
2. **Uložte** súbor *.zip* (napr. na USB kľúč).
3. **Vytvorte** nový priečinok s názvom **help** na vašom serveri, na ktorom beží **ESMC Web Console**, v nasledujúcom umiestnení: *%ProgramFiles%\Apache Software Foundation\Tomcat 7.0\webapps\era\webconsole* a **skopírujte** súbor *.zip* do priečinka **help**.
4. **Extrahujte** obsah súboru *.zip*, napr. *en-US.zip*, do priečinka s rovnakým názvom (v tomto prípade **en-US**), aby štruktúra priečinkov vyzerala takto: *%ProgramFiles%\Apache Software Foundation\Tomcat 7.0\webapps\era\webconsole\help\en-US*

Teraz môžete otvoriť ESMC Web Console. Vyberte požadovaný jazyk a prihláste sa. Ak kliknete na ikonu v pravom hornom rohu, zobrazí sa Offline pomocník.

Pre aktualizáciu Offline pomocníka po vykonaní migrácie zo staršej verzie (napr. z verzie 6.5) vymažte existujúci priečinok pomocníka (`...webapps\era\webconsole\help`) a vytvorte nový priečinok v rovnakom umiestnení (krok č. 3, uvedený vyššie). Po nahradení priečinka pokračujte štandardným postupom.

POZNÁMKA:
Offline pomocníka môžete v prípade potreby pridať aj vo viacerých jazykoch podľa krokov uvedených vyššie.

Dôležité:
Ak váš počítač alebo mobilné zariadenie, z ktorého sa prihlasujete do ESMC Web Console, nemá pripojenie na internet, budete musieť zmeniť nastavenia ESMC Web Console tak, aby sa pre nástroj ESMC predvolene otváral **Offline pomocník** (miesto Online pomocníka). Postupujte podľa inštrukcií uvedených pod tabuľkou.

Pokyny na inštaláciu Offline pomocníka na systéme Linux

1. **Stiahnite si** súbor `.tar` kliknutím na jazykový kód v tabuľke nižšie, čím stiahnete Offline pomocníka pre nástroj ESET Security Management Center v požadovanom jazyku.
2. **Uložte** súbor `.tar` (napr. na USB kľúč).
3. **Otvorte terminál** a prejdite do `/usr/share/tomcat/webapps/era/webconsole`.
4. **Vytvorte** nový priečinok s názvom **help** spustením príkazu `mkdir help`.
5. **Skopírujte** súbor `.tar` do priečinka **help** a extrahujte ho napr. pomocou príkazu `tar -xvf en-US.tar`.

Teraz môžete otvoriť ESMC Web Console. Vyberte požadovaný jazyk a prihláste sa. Ak kliknete na ikonu v pravom hornom rohu, zobrazí sa Offline pomocník.

Pre aktualizáciu Offline pomocníka po vykonaní migrácie zo staršej verzie (napr. z verzie 6.5) vymažte existujúci priečinok pomocníka (`...webapps\era\webconsole\help`) a vytvorte nový priečinok v rovnakom umiestnení (krok č. 3, uvedený vyššie). Po nahradení priečinka pokračujte štandardným postupom.

POZNÁMKA:
Offline pomocníka môžete v prípade potreby pridať aj vo viacerých jazykoch podľa krokov uvedených vyššie.

Dôležité:
Ak váš počítač alebo mobilné zariadenie, z ktorého sa prihlasujete do ESMC Web Console, nemá pripojenie na internet, budete musieť zmeniť nastavenia ESMC Web Console tak, aby sa pre nástroj ESMC predvolene otváral **Offline pomocník** (miesto Online pomocníka). Postupujte podľa inštrukcií uvedených pod tabuľkou.

Podporovaný jazyk	Offline HTML pomocník .zip	Offline HTML pomocník .tar
Angličtina	en-US.zip	en-US.tar
Arabčina	ar-EG.zip	ar-EG.tar
Zjednodušená čínština	zh-CN.zip	zh-CN.tar
Tradičná čínština	zh-TW.zip	zh-TW.tar
Chorvátčina	hr-HR.zip	hr-HR.tar
Čeština	cs-CZ.zip	cs-CZ.tar
Francúzština	fr-FR.zip	fr-FR.tar
Francúzština (kan.)	fr-CA.zip	fr-CA.tar
Nemčina	de-DE.zip	de-DE.tar
Gréčtina	el-GR.zip	el-GR.tar
Taliančina	it-IT.zip	it-IT.tar
Japončina	ja-JP.zip	ja-JP.tar
Kórejčina	ko-KR.zip	ko-KR.tar
Poľština	pl-PL.zip	pl-PL.tar
Portugalčina – Brazília	pt-BR.zip	pt-BR.tar
Ruština	ru-RU.zip	ru-RU.tar
Španielčina	es-ES.zip	es-ES.tar
Španielčina – Latinská Amerika	es-CL.zip	es-CL.tar
Slovenčina	sk-SK.zip	sk-SK.tar
Turečtina	tr-TR.zip	tr-TR.tar

Vynútenie Offline pomocníka na systéme Windows

1. **Otvorte** `C:\Program Files\Apache Software Foundation\Tomcat`

`7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties` v textovom editore.

2. **Vyhľadajte** riadok, v ktorom sa nachádza nastavenie `help_show_online=true`, zmeňte hodnotu tohto nastavenia na `false` a uložte zmeny.
3. **Reštartujte** službu Tomcat v rámci služieb alebo pomocou príkazového riadka.

Offline pomocník pre ESMC sa otvorí vždy, keď kliknete na ikonu v pravom hornom rohu nástroja ESMC Web Console alebo prejdete do spodnej časti okna vľavo a kliknete na možnosť **Pomocník**.

Vynútenie Offline pomocníka na systéme Linux

1. **Otvorte** konfiguračný súbor `/usr/share/tomcat/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties` v textovom editore (napr. `nano`).
2. **Vyhľadajte** riadok, v ktorom sa nachádza nastavenie `help_show_online=true`, zmeňte hodnotu tohto nastavenia na `false` a uložte zmeny.
3. Zastavte službu tomcat spustením príkazu `tomcat stop`.
4. Spustite službu tomcat spustením príkazu `tomcat start`.

Offline pomocník pre ESMC sa otvorí, keď kliknete na ikonu v pravom hornom rohu nástroja ESMC Web Console alebo prejdete do spodnej časti ľavého panela s ponukou a kliknete na možnosť **Pomocník**.

1.2 Podporované webové prehliadače, bezpečnostné produkty ESET a jazyky

V tejto časti nájdete zoznam operačných systémov, webových prehliadačov a bezpečnostných produktov spoločnosti ESET podporovaných nástrojom ESET Security Management Center.

- Windows, Linux a macOS.
- ESET Security Management Center Web Console môžete spúšťať cez nasledujúce webové prehliadače:

Webový prehliadač	Podporované od verzie
Mozilla Firefox	57.0.2
Microsoft Internet Explorer	11.64.16299.0
Microsoft Edge	41.16299.15.0
Google Chrome	63.0.3239.132
Safari	11.0.2
Opera	51.0.2830.40

Poznámka:
Odporúčame používať vždy najnovšiu verziu **webových** prehliadačov.

- ESET Security Management Center dokáže nasadiť, aktivovať a spravovať nasledujúce produkty ESET:

Najnovšie verzie produktov ESET spravovateľných prostredníctvom nástroja ESET Security Management Center 7:

Produkt	Verzia produktu
ESET Endpoint Security pre Windows	5.x, 6.x, 7.x
ESET Endpoint Antivirus pre Windows	5.x, 6.x, 7.x
ESET Endpoint Security pre macOS	6.x
ESET Endpoint Antivirus pre macOS	6.x

Produkt	Verzia produktu
ESET Endpoint Security pre Android	2.x
ESET File Security pre Windows Server	6.x, 7.x
ESET File Security pre Microsoft Azure	6.x
ESET Mail Security pre Microsoft Exchange Server	7.x
ESET Security pre Microsoft SharePoint Server	7.x
ESET Mail Security pre IBM Lotus Domino	6.x, 7.x
ESET Virtualization Security	1.x
ESET Dynamic Threat Defense	
ESET Enterprise Inspector	1.x

Staršie verzie produktov ESET spravovateľných prostredníctvom nástroja ESET Security Management Center 7:

Produkt	Verzia produktu
ESET File Security pre Microsoft Windows Server	4.5.x
ESET NOD32 Antivirus 4 Business Edition pre Mac OS X	4.x
ESET NOD32 Antivirus 4 Business Edition pre Linux Desktop	4.x
ESET Mail Security pre Microsoft Exchange Server	4.5.x
ESET Mail Security pre IBM Lotus Domino	4.5.x
ESET Security pre Microsoft Windows Server Core	4.5.x
ESET Security pre Microsoft SharePoint Server	4.5.x a 6.x
ESET Security pre Kerio	4.5.x
ESET NOD32 Antivirus Business Edition	4.2.76
ESET Smart Security Business Edition	4.2.76

Poznámka:

- Staršie verzie produktov spoločnosti ESET pre Windows Server uvedených v tabuľke vyššie momentálne nie je možné spravovať prostredníctvom nástroja *ESET Security Management Center* 7.
- Pozrite si tiež informácie o životnom cykle produktov spoločnosti ESET určených pre firmy.

Produkty podporujúce aktiváciu prostredníctvom predplatného

Produkt ESET	Dostupné od verzie
ESET Endpoint Antivirus/Security pre Windows	7.0
ESET Endpoint Antivirus/Security pre macOS	6.6.x
ESET Endpoint Security pre Android	2.0.158
ESET Mobile Device Management pre Apple iOS	7.0
ESET Virtualization Security pre VMware	1.7
ESET File Security pre Microsoft Windows Server	7.0
ESET Security Management Center	7.0
ESET Mail Security pre Microsoft Exchange	7.0
ESET File Security pre Windows Server	7.0
ESET Mail Security pre IBM Domino	7.0
ESET Security pre Kerio	7.0
ESET Security pre Microsoft SharePoint Server	7.0

Podporované jazyky

Jazyk	Kód
English (United States)	en-US
Arabic (Egypt)	ar-EG
Chinese Simplified	zh-CN
Chinese Traditional	zh-TW
Croatian (Croatia)	hr-HR
Czech (Czech Republic)	cs-CZ
French (France)	fr-FR
French (Canada)	fr-CA
German (Germany)	de-DE
Greek (Greece)	el-GR
Hungarian (Hungary)*	hu-HU
Italian (Italy)	it-IT
Japanese (Japan)	ja-JP
Korean (Korea)	ko-KR
Polish (Poland)	pl-PL
Portuguese (Brazil)	pt-BR
Russian (Russia)	ru-RU
Spanish (Chile)	es-CL
Spanish (Spain)	es-ES
Slovak (Slovakia)	sk-SK
Turkish (Turkey)	tr-TR

* V maďarčine je dostupný len samotný produkt, nie Online pomocník.

1.3 Legenda ikon

Táto časť popisuje a vysvetľuje význam všetkých ikon, ktoré sa vyskytujú v ESMC Web Console. Niektoré ikony znázorňujú akciu, typ položky alebo súčasný stav. Väčšina ikon je zobrazená v jednej z troch farieb, ktoré slúžia na označenie dostupnosti daného prvku:

- Štandardná ikona – akcia je dostupná.
- Modrá ikona – zvýraznený prvok pri ukázaní na položku kurzorom myši.
- Sivá ikona – akcia nie je dostupná.

Ikona stavu	Popis
	Zobraziť podrobnosti – zobrazia sa podrobné informácie o klientskom zariadení.
	Pridať nové – budú pridané nové zariadenia. **Nová úloha** – bude pridaná nová úloha. **Nové oznámenie** – bude pridané nové oznámenie. **Nové statické/dynamické skupiny** – budú pridané nové skupiny.
	Upraviť – môžete upravovať vytvorené úlohy, oznámenia, šablóny správ, skupiny, politiky atď.
	Duplikovať – umožňuje vytvoriť novú politiku založenú na už existujúcej politike, ktorú ste vybrali. Duplikovaná politika si vyžaduje nový názov.

Ikona stavu	Popis
	**Presunúť** – umožňuje presunúť počítače, politiky, statické alebo dynamické skupiny. **Prístupová skupina** – umožňuje presunúť položku do inej statickej skupiny.
	**Vymazať** – úplne odstráni zvoleného klienta, skupinu atď.
	**Premenovať viaceré položky** – pokiaľ vyberiete viacero položiek, môžete ich premenovať po jednom alebo môžete použiť Regex vyhľadávanie (na základe regulárnych výrazov) a naraz premenovať viaceré položky.
	**Kontrolovať** – táto funkcia spustí úlohu Manuálna kontrola na kliente, ktorý nahlásil hrozbu.
	**Aktualizovať moduly** – táto funkcia spustí úlohu Aktualizácia modulov (aktualizácia bude spustená manuálne).
	**Spustiť úlohu** – spustenie úlohy na mobilných zariadeniach.
	**Znovu registrovať** – otvorí sa okno Pridať mobilné zariadenie prostredníctvom e-mailu.
	**Odomknúť** – zariadenie bude odomknuté.
	**Zamknúť** – zariadenie bude uzamknuté po zachytení podozrivej aktivity alebo v prípade, že zariadenie je označené ako stratené.
	**Hľadať** – vyžiadanie GPS súradníc vášho mobilného zariadenia.
	**Siréna** – vzdialené spustenie hlučnej sirény aj pokiaľ je na zariadení vypnutý zvuk.
	**Vymazať** – všetky dáta uložené na zariadení budú natrvalo vymazané.
	**Reštartovať** – ak vyberiete počítač a použijete možnosť **Reštartovať**, zariadenie sa reštartuje. **Obnoviť** – obnoviť súbor presunutý do karantény späť do jeho pôvodného umiestnenia.
	**Vypnutie** – ak vyberiete počítač a použijete možnosť **Reštartovať** > **Vypnutie**, zariadenie sa vypne. **Deaktivácia produktov** – licencia bude odstránená zo všetkých zvolených zariadení cez licenčný server spoločnosti ESET. Produkt bude deaktivovaný aj v prípade, že nebol aktivovaný prostredníctvom nástroja ESMC, ako aj v prípade, že jeho licencia nie je nástrojom ESMC spravovaná.
	**Spustiť úlohu** – vyberte úlohu a nastavte pre ňu spúšťač a obmedzenie (voliteľné). Úloha bude zaradená do poradia úloh čakajúcich na vykonanie podľa jej nastavení. Táto možnosť okamžite spustí úlohu, ktorú vyberiete zo zoznamu dostupných úloh.
	**Naposledy použité úlohy** – zobrazia sa naposledy použité úlohy. Môžete kliknúť na požadovanú úlohu a opätovne ju spustiť.
	**Priradiť používateľa** – môžete priradiť používateľa k zariadeniu. Používateľov môžete spravovať v sekcii Používatelia počítača.
	**Spravovať politiky** – politika môže byť tiež priradená priamo ku klientu (viacerým klientom), nie len ku skupine. Vyberte túto možnosť, ak si želáte priradiť politiku k označeným klientom.
	**Odoslať volanie na prebudenie** – ESMC Server spustí okamžitú replikáciu ESET Management Agenta na klientskom počítači prostredníctvom služby EPNS. Toto je užitočné, ak nechcete čakať na pravidelný interval pripojenia ESET Management Agenta na ESMC Server. Ak napríklad chcete, aby bola úloha pre klienta spustená na klientoch okamžite alebo chcete, aby bola politika aplikovaná ihneď.
	**Nasadiť agenta** – pomocou tejto možnosti môžete vytvoriť novú úlohu pre server.

Ikona stavu	Popis
	Pripojiť – môžete vygenerovať a stiahnuť *.rdp* súbor, ktorý vám umožní pripojiť sa na cieľové zariadenie cez protokol RDP (Remote Desktop Protocol).
	Potlačiť – ak vyberiete počítač a použijete možnosť **Potlačiť**, agent daného klienta sa prestane hlásiť do ESMC. Bude len agregovať informácie. Ikona potlačenia bude zobrazená vedľa názvu počítača v stĺpci „Potlačený“. Po vypnutí potlačenia kliknutím na **Zrušiť potlačenie** sa potlačený počítač bude znova prihlasovať (hlásiť) a komunikácia medzi ESMC a klientom bude obnovená.
	Vypnúť – vypnutie alebo odstránenie nastavenia, prípadne výberu.
	Priradiť – táto funkcia slúži na priradenie politiky ku klientu alebo skupine.
	Importovať – môžete importovať správy, politiky alebo verejný kľúč.
	Exportovať – môžete exportovať správy, politiky alebo partnerský certifikát.
	Počítač
	Virtuálny počítač (bez agenta)
	Mobil
	Server
	Súborový server
	Poštový server
	Server brány
	Server pre spoluprácu
	Agent
	Mobile Device Connector
	Rogue Detection Sensor
	Hostiteľ virtuálneho agenta
	Proxy
	ESMC Server
	Zdieľaná lokálna vyrovnávacia pamäť
	Virtual Security Appliance
	Enterprise Inspector Agent
	Enterprise Inspector Server

2. Začíname s nástrojom ESMC Web Console

ESET Security Management Center je možné konfigurovať a spravovať pomocou **ESMC Web Console**. Po úspešnej inštalácii nástroja ESET Security Management Center alebo nasadení virtuálneho zariadenia ESMC sa môžete pripojiť na váš ESMC Server pomocou ESMC Web Console.

V nasledujúcich kapitolách sú popísané funkcie a používanie nástroja ESMC Web Console. Môžete vytvoriť inštalátory a nasadiť ESET Management Agenta, prípadne bezpečnostné produkty spoločnosti ESET, na klientske počítače. Po nasadení ESET Management Agenta môžete spravovať skupiny, vytvárať a priraďovať politiky a nastavovať oznámenia a správy. Môžete kliknúť na jednu z nasledujúcich tém a prejsť priamo do príslušnej kapitoly:

- Otvorenie ESMC Web Console
- Používanie sprievodcu spustením
- ESMC Web Console
- Prehľad stavu

2.1 Predstavenie programu ESET Security Management Center

Vitajte v programe ESET Security Management Center (ESMC) verzie 7.0. ESET Security Management Center vám umožňuje spravovať v sieťovom prostredí z jedného miesta všetky produkty spoločnosti ESET na pracovných staniciach, serveroch a mobilných zariadeniach. Pomocou nástroja ESET Security Management Center Web Console (ESMC Web Console) môžete nasadiť bezpečnostné riešenia spoločnosti ESET, spravovať úlohy, vynucovať bezpečnostné politiky, sledovať stav systému a pohotovo reagovať na problémy alebo hrozby na vzdialených počítačoch. ESMC pozostáva z nasledujúcich komponentov:

- ESMC Server – ESMC Server môže byť nainštalovaný na Windows a Linux servery a môže mať tiež podobu virtuálneho zariadenia. Riadi komunikáciu s agentmi a zhromažďuje a uchováva dáta aplikácií v databáze.
- ESMC Web Console – ESMC Web Console nahrádza ERA Console, ktorá bola súčasťou starších verzií (v5) programu, a je hlavným rozhraním, ktoré vám umožňuje spravovať klientske počítače vo vašej sieti. Poskytuje prehľad klientov v sieti a dá sa použiť na vzdialenú inštaláciu produktov spoločnosti ESET na nespravované počítače. Po inštalácii komponentu ESET Security Management Center Server (ESMC Server) máte prístup do Web Console prostredníctvom vášho webového prehliadača. Ak sa rozhodnete sprístupniť webový server na internete, budete môcť používať ESMC z akéhokoľvek miesta a zariadenia pripojeného na internet.
- ESET Management Agent – ESET Management Agent sprostredkúva komunikáciu medzi ESMC Serverom a klientskymi počítačmi. Agent musí byť nainštalovaný na každom klientskom počítači, ktorý bude komunikovať s ESMC Serverom. Keďže sa agent nachádza na klientskom počítači a dokáže uchovávať viaceré bezpečnostné scenáre, používanie ESET Management Agenta skracuje čas reakcie na nové hrozby. Pomocou ESMC Web Console môžete nasadiť ESET Management Agenta na nespravované počítače, ktoré boli identifikované prostredníctvom vášho Active Directory alebo nástrojom ESET RD Sensor. V prípade potreby je možná aj manuálna inštalácia ESET Management Agenta.
- Rogue Detection Sensor – ESMC Rogue Detection Sensor deteguje nespravované počítače, ktoré sa nachádzajú v sieti. Informácie o týchto počítačoch sú odosielané na ESMC Server. To umožňuje jednoducho pridať nové klientske počítače do vašej zabezpečenej siete. RD Sensor si pamätá počítače, ktoré už boli nájdené a nebude odosielať rovnaké informácie dvakrát.
- Apache HTTP Proxy – je to služba, ktorá môže byť použitá v kombinácii s nástrojom ESET Security Management Center na:
    - distribúciu aktualizácií na klientske počítače a distribúciu inštalačných balíkov na ESET Management Agenta,
    - presmerovanie komunikácie s ESET Management Agentmi na ESMC Server.
- Mobile Device Connector – komponent, ktorý umožňuje správu mobilných zariadení pomocou nástroja ESET Security Management Center. Umožňuje vám spravovať mobilné zariadenia (Android a iOS) a bezpečnostný produkt ESET Endpoint Security pre Android.

- Virtuálne zariadenie ESMC (ESMC VA) je určené pre používateľov, ktorí chcú spúšťať ESET Security Management Center vo virtualizovanom prostredí.

- ESET Security Management Center Virtual Agent Host – komponent programu ESET Security Management Center, ktorý vytvára virtuálnych agentov, a umožňuje tak správu virtuálnych zariadení bez klasického agenta. Toto riešenie umožňuje automatizáciu, použitie dynamických skupín a správu úloh na rovnakej úrovni ako tomu je pri klasických ESET Management Agentoch na fyzických počítačoch. Virtuálny agent zbiera informácie na virtuálnych zariadeniach a odosiela ich na ESMC Server.

- Mirror Tool – tento nástroj sa používa na aktualizovanie programových modulov v offline prostredí. V prípade, že bezpečnostné produkty ESET na vašich klientskych počítačoch nemajú pripojenie na internet, môžete použiť nástroj Mirror Tool, ktorý sťahuje aktualizačné súbory z aktualizačných serverov spoločnosti ESET a ukladá ich lokálne.

- Asistent migrácie – tento nástroj je určený na pomoc pri migrácii z nástroja ERA 5 na ESMC 7. Asistent migrácie je samostatný nástroj, ktorý vás prostredníctvom prehľadného sprievodcu prevedie celým procesom migrácie dát z ERA 5.x do prechodnej databázy, ktorú je následne možné importovať do ESMC 7.

- Deployment Tool – tento nástroj slúži na nasadenie all-in-one inštalačných balíkov vytvorených pomocou nástroja ESMC Web Console. Ponúka tak pohodlný spôsob distribúcie ESET Management Agenta s bezpečnostným produktom ESET na klientske počítače v sieti.

- ESET Business Account – nový licenčný portál určený pre firemné produkty ESET vám umožňuje spravovať licencie. Bližšie informácie o aktivácii vášho produktu nájdete v kapitole ESET Business Account, prípadne si môžete prečítať používateľskú príručku portálu ESET Business Account, kde nájdete podrobnejšie informácie o jeho používaní. Ak už máte prihlasovacie meno a heslo, ktoré vám boli vydané spoločnosťou ESET, môžete ich konvertovať na licenčný kľúč. Viac informácií nájdete v časti Konvertovanie licenčných prihlasovacích údajov na licenčný kľúč.

- ESET Enterprise Inspector (EEI) – komplexný systém detekcie a reakcie na hrozby v koncových bodoch (Endpoint Detection and Response – EDR), ktorý zahŕňa funkcie, ako napr. detekcia incidentov, manažment a reakcia na incidenty, zozbieravanie údajov, detekcia indikátorov ohrozenia, detekcia anomálií, detekcia správania, detekcia porušenia pravidiel atď.

2.2 Otvorenie ESMC Web Console

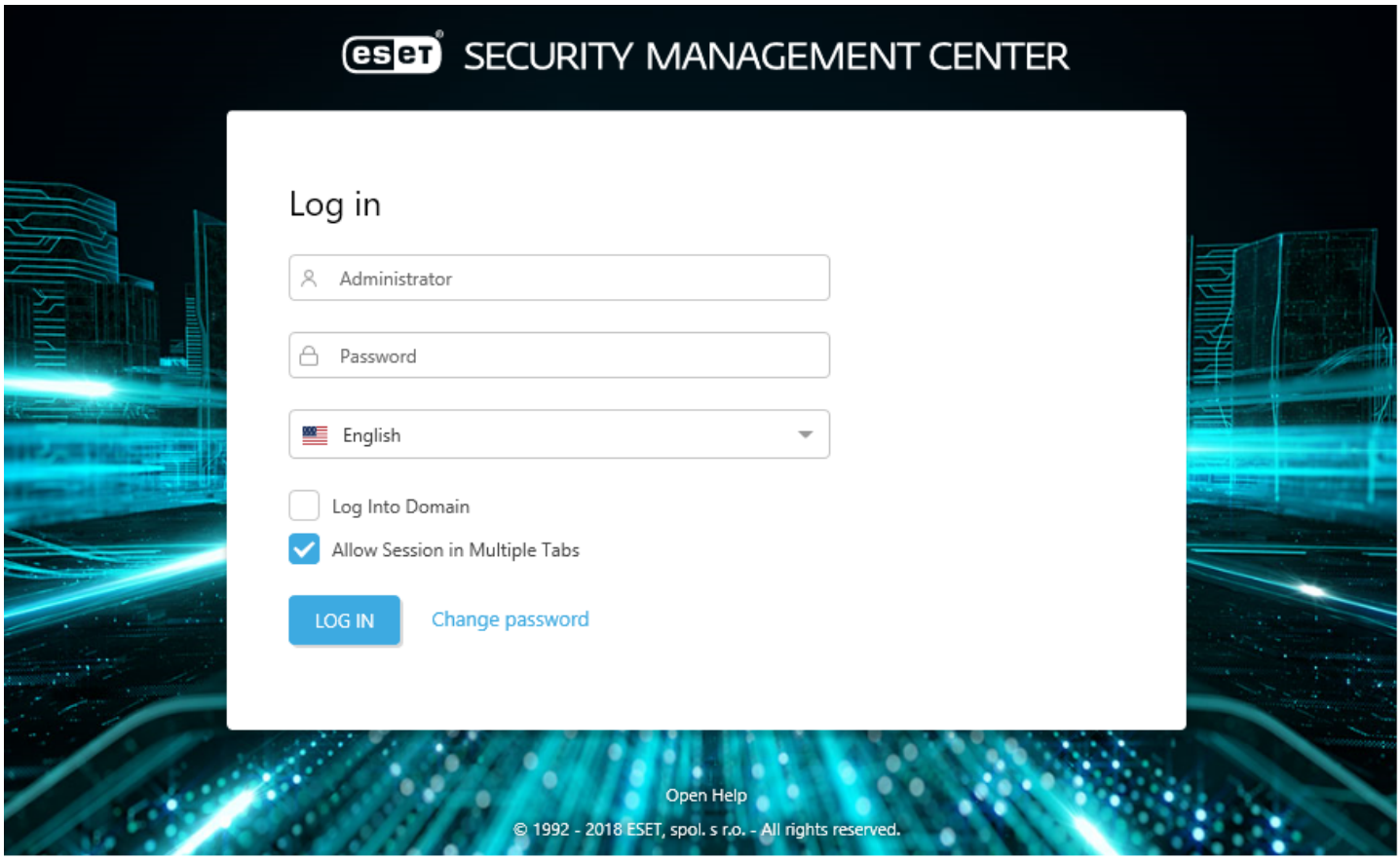
ESET Security Management Center Web Console je hlavné používateľské rozhranie používané na komunikáciu s ESMC Serverom. Je to v podstate ovládací panel a tiež centrálne miesto, z ktorého môžete spravovať všetky bezpečnostné riešenia spoločnosti ESET. Je to webové rozhranie, ktoré je dostupné pomocou webového prehliadača z akéhokoľvek miesta a zariadenia s prístupom na internet.

Existuje niekoľko možností otvorenia rozhrania ESMC Web Console.

- Na vašom **lokálnom serveri** (počítači s Web Console) otvorte nasledujúcu URL adresu vo webovom prehliadači: *https://localhost/era/*
- Z **akéhokoľvek miesta s prístupom na internet** zadajte do webového prehliadača URL adresu v nasledujúcom formáte:
  https://yourservername/era/
  Nahraďte „yourservername“ skutočným názvom alebo IP adresou svojho webového servera.

- Pre prihlásenie do **virtuálneho zariadenia ESMC** použite nasledujúcu URL adresu:
  https://[IP address]/
  Nahraďte „[IP address]“ IP adresou vášho virtuálneho počítača ESMC. Ak si nepamätáte IP adresu, postupujte podľa kroku č. 9 v časti obsahujúcej inštrukcie nasadenia virtuálneho zariadenia.
- Na vašom lokálnom serveri (počítač, na ktorom beží Web Console) kliknite na **Štart** > **Všetky programy** > **ESET** > **ESET Security Management Center** > **ESET Security Management Center Web Console** – otvorí sa prihlasovacie okno vo vašom predvolenom webovom prehliadači. Toto sa nevzťahuje na virtuálne zariadenie ESMC.

Ak na webovom serveri beží ESMC Web Console, zobrazí sa nasledujúca obrazovka:



POZNÁMKA:
Ak sa vám nedarí prihlásiť sa do Web Console alebo sa pri prihlasovaní zobrazí chybové hlásenie, pozrite si kapitolu Riešenie problémov – Web Console.

2.3 Používanie sprievodcu spustením

Keď sa po prvýkrát prihlásite do Web Console, zobrazí sa **Sprievodca spustením** pre ESET Security Management Center. Tento sprievodca vám poskytne základné vysvetlenie dôležitých častí nástroja ESMC Web Console, ako aj stručné vysvetlenie ESET Management Agenta a bezpečnostných produktov spoločnosti ESET. Dozviete sa o počítačoch, skupinách, úlohách pre klienta, ako aj o ESET Management Agente.

Posledný krok v Sprievodcovi nazvaný **Nasadenie** vám pomôže vytvoriť all-in-one inštalátor (obsahujúci ESET Management Agenta a bezpečnostný produkt ESET).

Dôležité:
Inštalačný balík je v podobe súboru `.exe` a je platný len pre systém Windows.

Ak si neželáte použiť sprievodcu, kliknite na **Zatvoriť sprievodcu spustením**. Otvorí sa rozhranie nástroja ESMC Web Console. Tento sprievodca sa už pri ďalšom prihlásení do ESMC Web Console nezobrazí. Sprievodcu spustením však môžete opätovne zobraziť kliknutím na **Pomocník** > **Sprievodca spustením**.

Na vytvorenie all-in-one inštalátora agenta nepotrebujete použiť sprievodcu, je možné vytvoriť ho aj manuálne kliknutím na **Iné možnosti nasadenia** v časti **Rýchle odkazy**.

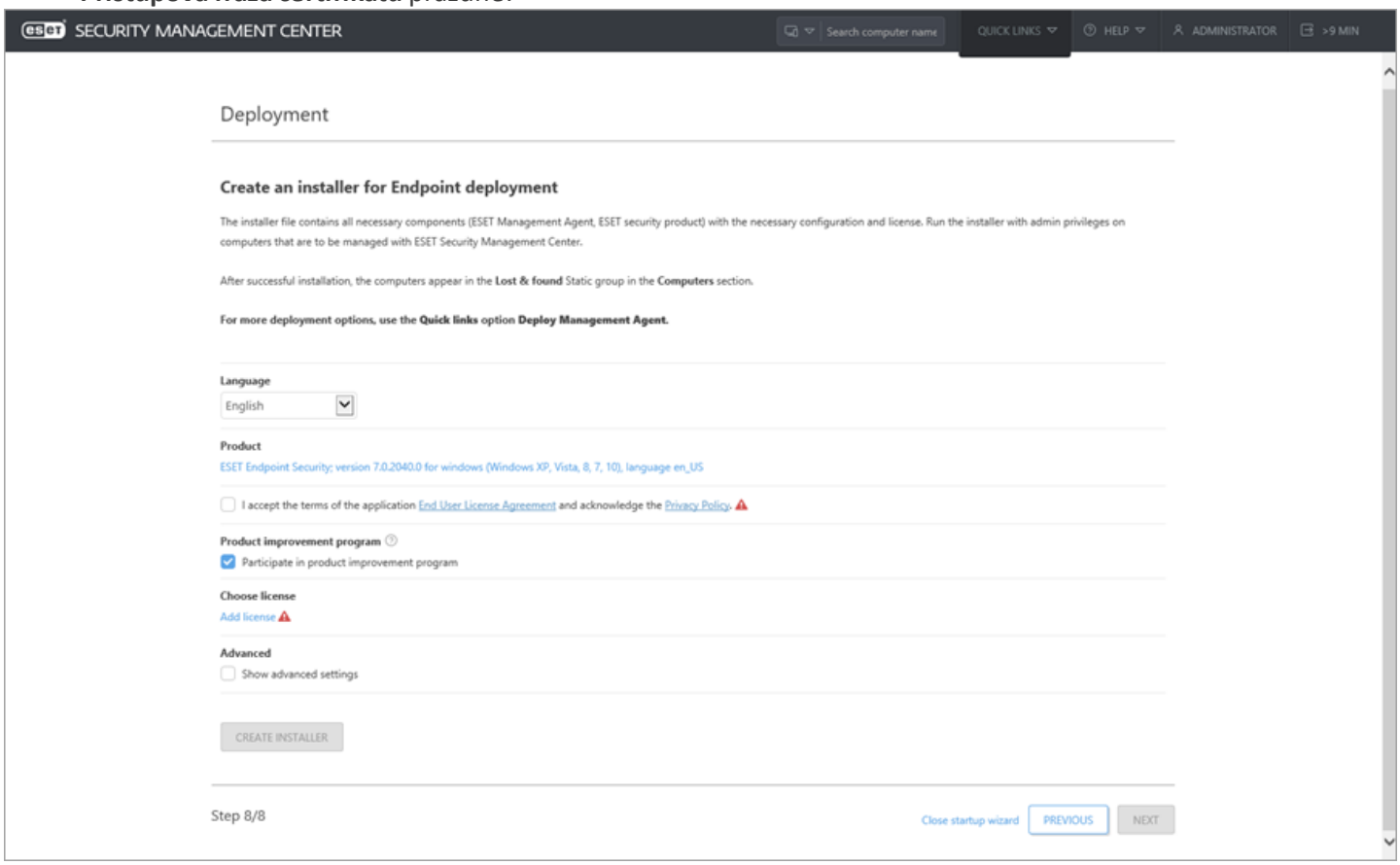
Dôležité:
Ak chcete vytvoriť inštalačný balík, váš používateľský účet musí mať pridelené **povolenie pre nasadenie agenta**. Ak používateľský účet toto povolenie nemá, v Sprievodcovi spustením sa nezobrazí krok **Nasadenie**, čo znamená, že používateľ nebude mať možnosť vytvoriť inštalačný balík.

Pre vytvorenie inštalačného balíka postupujte podľa krokov uvedených nižšie:

1. **Jazyk** – vyberte jazyk inštalátora zo zoznamu podporovaných jazykov.
2. **Produkt** – zo zoznamu vyberte inštalačný súbor bezpečnostného produktu ESET. Ak vyberiete verziu 6.3 alebo staršiu, automatická aktivácia produktu nebude fungovať. Produkt budete musieť aktivovať neskôr. Bezpečnostné produkty ESET vo verzii 6.4 a novších budú pri inštalácii aktivované automaticky.

Poznámka:
Ak sa nezobrazujú žiadne inštalačné súbory produktu, uistite sa, že máte repozitár nastavený na *AUTOSELECT*. Podrobnosti nájdete v **Pokročilých nastaveniach** časti Nastavenia servera.

3. Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.
4. Ak nesúhlasíte so zasielaním správ o zlyhaní programu a telemetrických údajov spoločnosti ESET, zrušte označenie možnosti **Zúčastnite sa programu zlepšovania produktov**. Ak ponecháte túto možnosť označenú, telemetrické údaje a správy o zlyhaní programu budú odosielané spoločnosti ESET.
5. **Vyberte licenciu** (povinné) – licenciu je potrebné pridať pomocou jednej z metód popísaných v časti Licencie. Ak už máte existujúce licencie v Správe licencií, jednoducho vyberte licenciu, ktorá bude použitá na aktiváciu bezpečnostného produktu ESET počas inštalácie. Ak nevyberiete licenciu, môžete vytvoriť inštalátor bez nej a aktivovať produkt neskôr. Pridať či odobrať licenciu môže len správca, ktorý má ako domácu skupinu nastavenú skupinu **Všetko** a má oprávnenie na **zápis** pre licencie v danej skupine.
6. Ak označíte možnosť **Pokročilé**, budete môcť vybrať **Certifikát agenta** a v prípade potreby zadať aj **Prístupovú frázu certifikátu**. Prístupovú frázu certifikátu zadajte v prípade, ak ste ju špecifikovali počas inštalácie svojho ESMC alebo používate vlastný certifikát s prístupovou frázou certifikátu. V opačnom prípade ponechajte pole **Prístupová fráza certifikátu** prázdne.



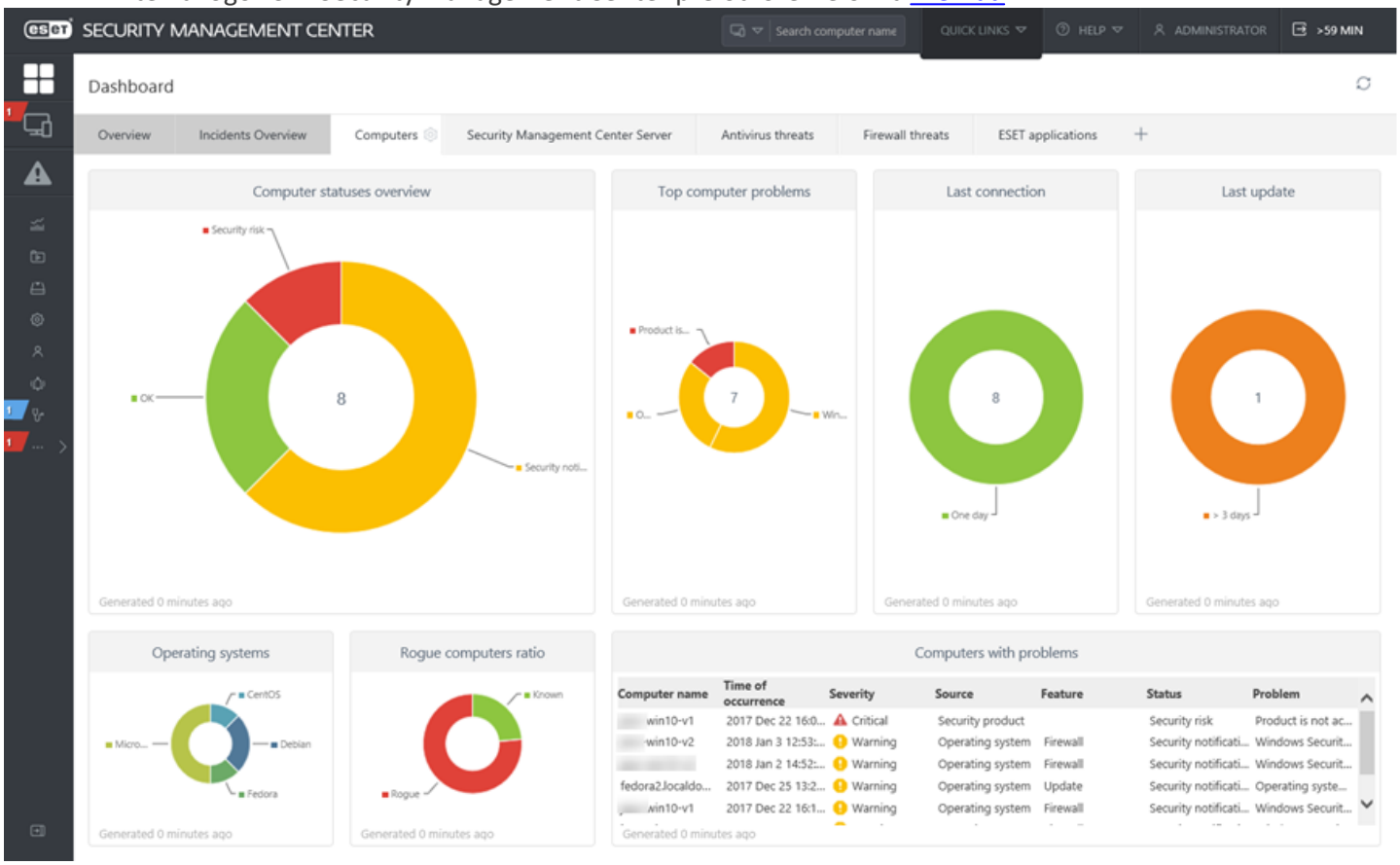
7. Kliknite na **Vytvoriť inštalátor**. Súbory all-in-one inštalátora budú vygenerované pre 32-bitové a 64-bitové operačné systémy. Kliknite na požadovanú verziu a začne sa sťahovanie. Po dokončení sťahovania budete vyzvaný na zadanie umiestnenia, kde bude súbor uložený (napr. *ESMC_Installer_x32_en_US.exe* alebo *ESMC_Installer_x64_en_US.exe*). Kliknite na **Uložiť súbor**.
8. **Spustite** súbor all-in-one inštalačného balíka na klientskom počítači. Podrobné inštrukcie nájdete v kapitole All-in-one sprievodca inštaláciou agenta.

2.4 ESMC Web Console

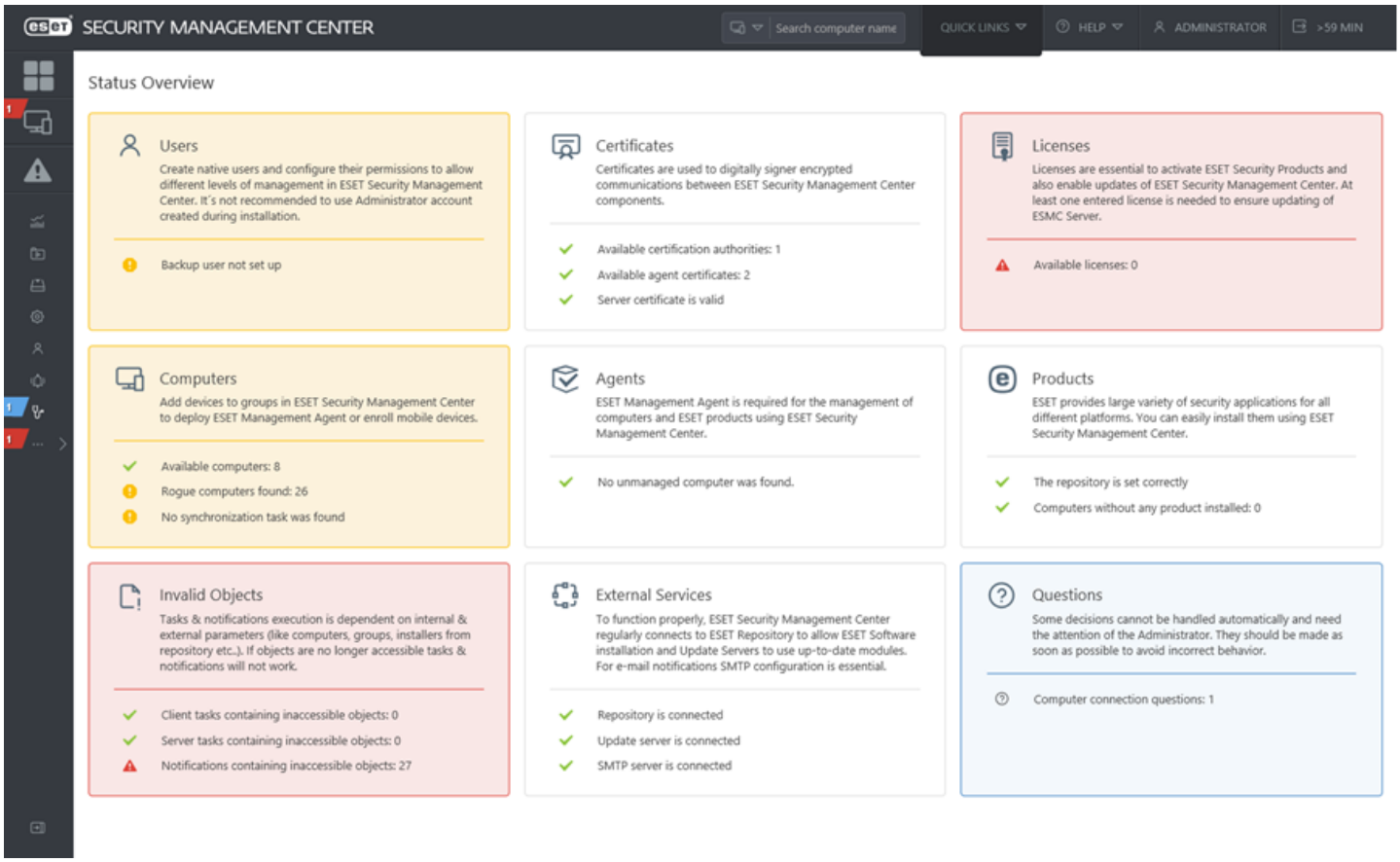
ESMC Web Console je hlavné používateľské rozhranie používané na komunikáciu s ESMC Serverom. Je to v podstate ovládací panel a tiež centrálne miesto, z ktorého môžete spravovať všetky bezpečnostné riešenia spoločnosti ESET. Web Console je webové rozhranie, ktoré sa používa prostredníctvom webového prehliadača (pozrite si časť Podporované webové prehliadače) z akéhokoľvek miesta a zariadenia, ktoré má prístup na internet.

Štandardné rozloženie ESMC Web Console:

- Prihlásený používateľ je zobrazený v pravom hornom rohu obrazovky, kde je tiež počítadlo automatického odhlásenia, na ktorom sa odpočítava čas. Ak sa chcete odhlásiť, kliknite na tlačidlo **Odhlásiť** a budete okamžite odhlásený. Po vypršaní relácie (v prípade, že používateľ je neaktívny) sa musí používateľ znova prihlásiť.
- Ak chcete zmeniť Nastavenia používateľa, kliknite na svoje prihlasovacie meno v pravom hornom rohu rozhrania ESMC Web Console.
- Kedykoľvek môžete kliknúť na ikonu v pravej hornej časti obrazovky pre zobrazenie ponuky **Pomocníka**. Po kliknutí na prvý odkaz v tejto ponuke sa vždy zobrazí kapitola Online pomocníka, ktorá popisuje aktuálne prehliadanú časť rozhrania Web Console.
- **Menu** je dostupné vždy na ľavej strane obrazovky okrem prípadu, keď používate sprievodcu. Kliknite na pre rozbalenie menu na ľavej strane obrazovky. **Zbaliť menu** je možné kliknutím na .
- Ikona vždy predstavuje dostupnosť kontextového menu.
- Kliknite na možnosť **Obnoviť**, ak chcete znova obnoviť/načítať zobrazené informácie.
- Kliknite na logo ESET Security Management Center pre otvorenie okna Prehľad.

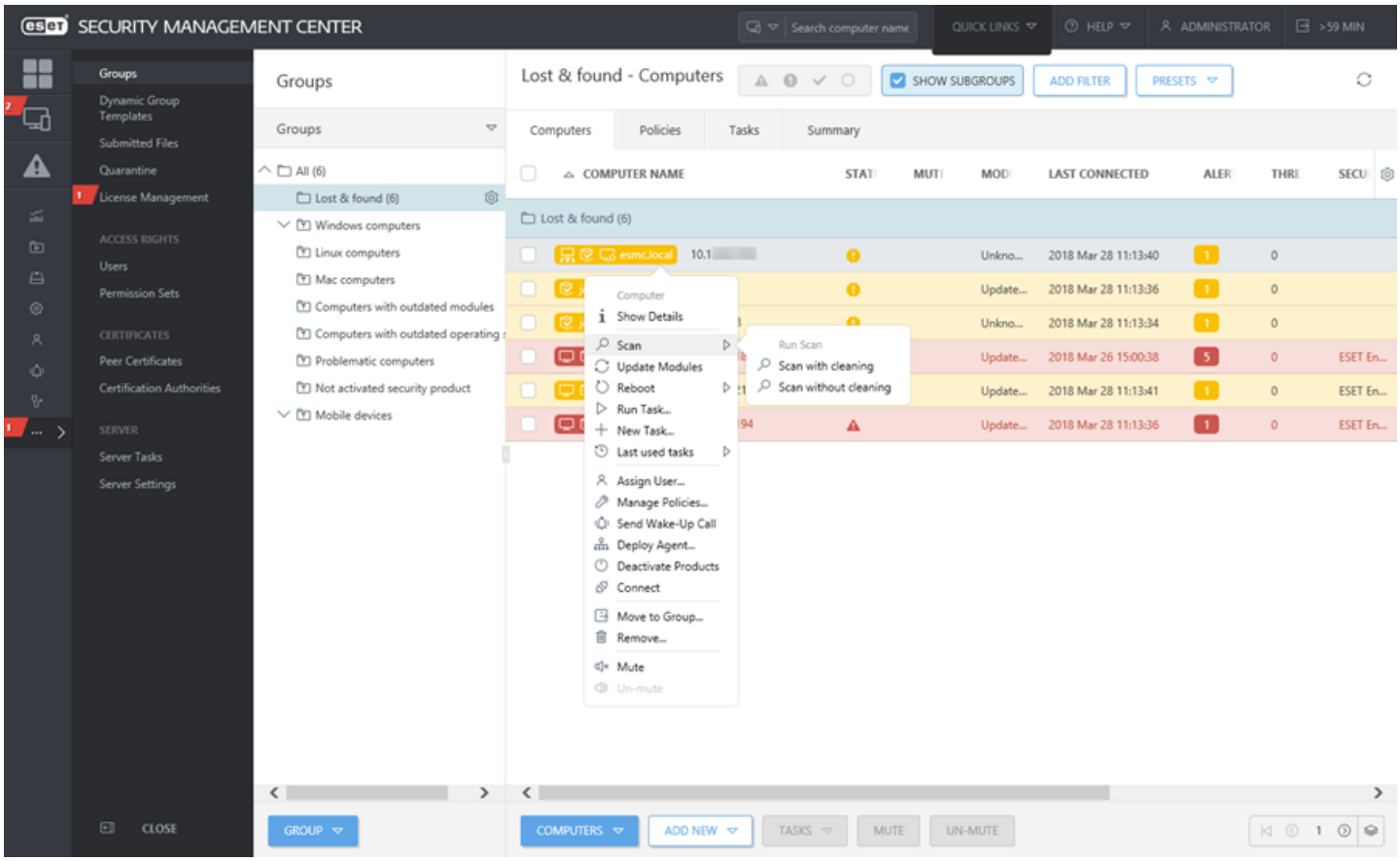


Prehľad stavu vám ukáže, ako čo najlepšie využiť nástroj ESET Security Management Center. Položky, ktoré sa tu nachádzajú, vás prevedú jednotlivými krokmi odporúčaných nastavení.



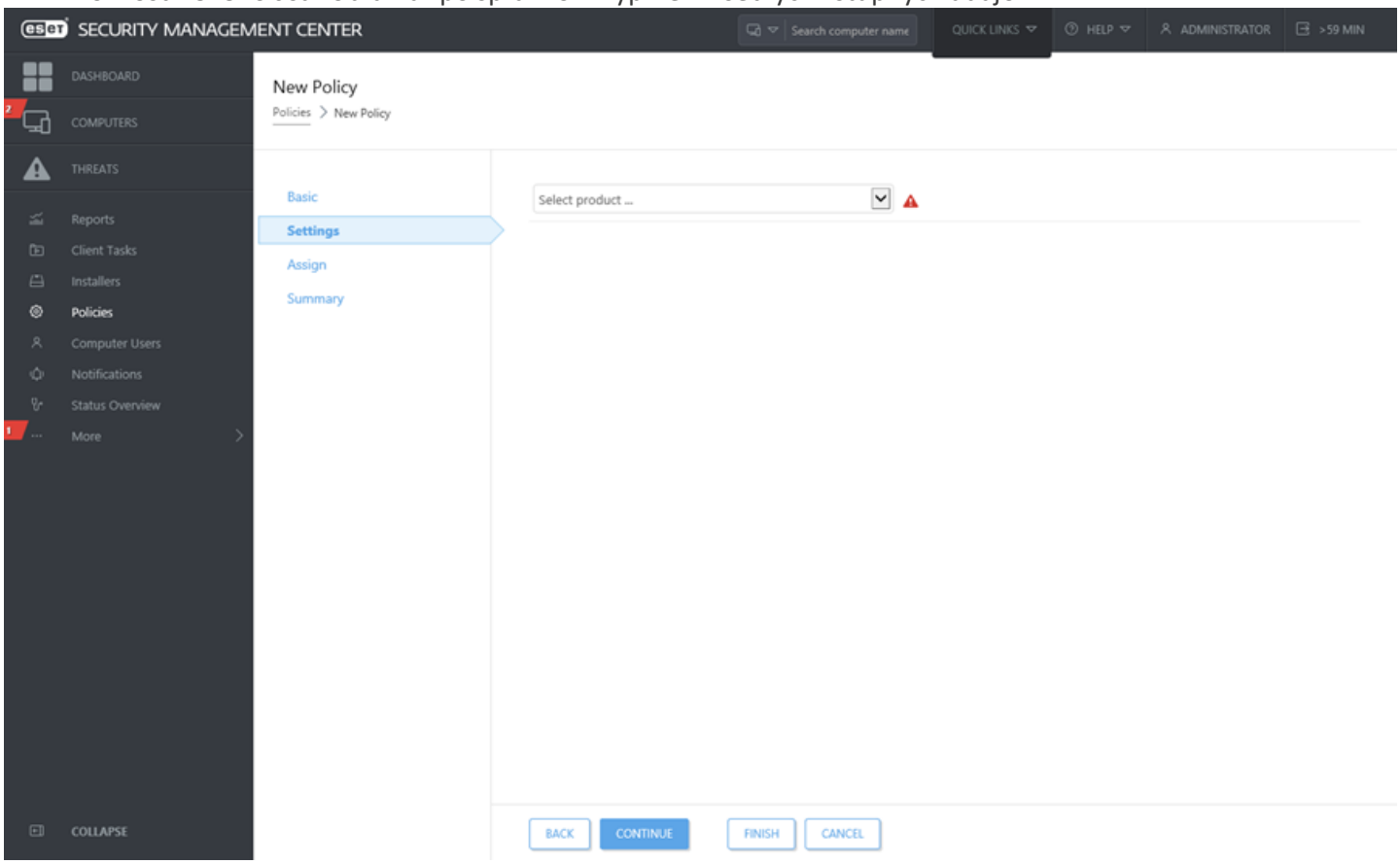
Zobrazenie stromovej štruktúry má špecifické ovládanie. Stromová štruktúra sa nachádza na ľavej strane, dostupné akcie nájdete v dolnej časti. Kliknutím na položku v stromovej štruktúre sa zobrazia nastavenia pre príslušnú položku.

Tabuľky vám umožňujú spravovať jednotky pomocou riadkov individuálne alebo v skupinách (ak je označených viac riadkov). Kliknutím na riadok sa zobrazia nastavenia dostupné pre jednotky v danom riadku. Údaje v tabuľkách môžu byť filtrované a zoraďované.



Objekty v ESMC môžu byť upravené pomocou sprievodcu. Používanie sprievodcu je vždy rovnaké:

- Jednotlivé kroky sú orientované vertikálne, čiže zhora nadol.
- K jednotlivým krokom sa môžete kedykoľvek vrátiť.
- Nesprávne vyplnené údaje budú označené, ak prejdete kurzorom myši na ďalšie pole. Kroky sprievodcu s nesprávne vyplnenými údajmi budú takisto označené.
- Možnosť **Dokončiť** sa zobrazí až po správnom vyplnení všetkých vstupných údajov.



2.5 Ako spravovať produkty spoločnosti ESET určené pre koncové zariadenia prostredníctvom nástroja ESET Security Management Center?

Správca môže cez ESMC Web Console vykonávať rôzne úlohy s cieľom nainštalovať na klientske zariadenia bezpečnostné produkty a následne tieto klientske zariadenia kontrolovať. Na nižšie uvedených odkazoch nájdete viac informácií o jednotlivých témach.

Inštalácia ESET Management Agenta a bezpečnostných produktov ESET určených pre koncové zariadenia

Na správu klientskych počítačov v sieti prostredníctvom nástroja ESET Security Management Center je potrebné mať na každom kliente nainštalovaného ESET Management Agenta. ESET Management Agenta je možné nainštalovať na klienta spolu s bezpečnostným produktom ESET určeným pre koncové zariadenia použitím nástroja na nasadenie (Deployment Tool) alebo all-in-one inštalátora. Pred samotnou inštaláciou vám odporúčame do nástroja ESET Security Management Center importovať vašu licenciu, aby bolo možné túto licenciu použiť pri nasledujúcich inštaláciách. Produkt určený pre koncové zariadenia môžete nainštalovať dvoma spôsobmi:

- Pokiaľ chcete nainštalovať súčasne produkt pre koncové zariadenia aj ESET Management Agenta, použite nástroj na nasadenie alebo all-in-one inštalátor.
- Pokiaľ sú ESET Management Agenty na klientoch už nainštalované, použite úlohu pre klienta určenú na inštaláciu produktu ESET pre koncové zariadenia.

Spravovanie bezpečnostných produktov ESET určených pre koncové zariadenia cez ESET Security Management Center

Všetky bezpečnostné produkty ESET určené pre koncové zariadenia je možné spravovať prostredníctvom ESMC Web Console. Pomocou politík sa na jednotlivé zariadenia alebo skupiny zariadení aplikujú konkrétne nastavenia. Môžete napríklad vytvoriť politiku, ktorá bude blokovať prístup k určitým webovým stránkam alebo meniť rôzne iné nastavenia v produkte. Politiky je možné zlučovať, ako ukazuje tento príklad. Politiky, ktoré boli nastavené prostredníctvom nástroja ESMC, nie je používateľ na klientskom zariadení schopný prepísať. Správca však môže použiť funkciu Režim prepísania, čím používateľovi dočasne umožní robiť v bezpečnostnom produkte na klientskom zariadení zmeny. Po dokončení všetkých zmien môžete vyžiadať finálnu konfiguráciu z klienta a uložiť ju ako novú politiku.

Na správu klientov je tiež možné použiť úlohy pre klienta. Úlohy pre klienta sa nasadzujú z Web Console a na kliente sú vykonávané ESET Management Agentom. Najčastejšie používanými úlohami pre klienty s operačným systémom Windows sú:

- Aktualizovať moduly (aktualizuje aj vírusový databázu)
- Spustiť manuálnu kontrolu
- Spustiť vlastný príkaz
- Vyžiadať konfiguráciu produktu a počítača

Správy o stave počítača a získavanie informácií z klientov do ESET Security Management Center

Každý klientsky počítač je pripojený k nástroju ESET Security Management Center prostredníctvom ESET Management Agenta. Agent zbiera všetky požadované informácie o klientskom zariadení a softvéri a odosiela ich na ESMC Server. Na základe predvolených nastavení sa agent pripája na server každú minútu. Túto hodnotu je však možné zmeniť v politike ESET Management Agenta. Všetky protokoly z produktov ESET určených pre koncové zariadenia alebo iných bezpečnostných produktov spoločnosti ESET sú zasielané na ESMC Server.

Informácie o nainštalovaných produktoch ESET, ako aj o operačnom systéme a stave klienta nájdete v sekcii **Počítače**. Vyberte klienta a kliknite na **Zobraziť podrobnosti**. V časti **Konfigurácia** môže používateľ vyhľadať staršie konfigurácie alebo vyžiadať súčasnú konfiguráciu. V časti **SysInspector** môže používateľ vyžiadať protokoly (len z počítačov s operačným systémom Windows).

Prostredníctvom Web Console sa tiež dostanete k zoznamu všetkých hrozieb nájdených na klientskych zariadeniach (prejdite do sekcie **Hrozby**). Hrozby nájdené na jednotlivých zariadeniach je možné zobraziť po kliknutí na sekciu **Počítače**. Zvoľte klienta a kliknite na **Zobraziť podrobnosti > Hrozby a karanténa**. Ak na klientskom počítači beží ESET Enterprise Inspector, budú zobrazené aj hrozby hlásené týmto nástrojom, ktoré je zároveň možné spravovať.

Prostredníctvom vlastných správ môžete získať potrebné informácie o klientskych zariadeniach vo vašej sieti. Správy môžete vygenerovať manuálne alebo pomocou plánovanej úlohy. Prednastavené šablóny správ ponúkajú rýchly spôsob zozbieravania dôležitých dát, máte však rovnako možnosť vytvoriť si vlastné nové šablóny. Správy obsahujú súhrnné informácie napríklad o počítačoch, hrozbách, karanténe a dôležitých aktualizáciách.

Dôležité:
Používateľ môže použiť len tie šablóny správ, pre ktoré má dostatočné povolenia. Všetky šablóny sú štandardne uložené v skupine **Všetko**. Správa môže obsahovať len informácie o počítačoch a udalostiach, ktoré spadajú do rozsahu povolení daného používateľa. Dokonca i v prípade zdieľania šablóny správ medzi viacerými používateľmi sa budú jednotlivým používateľom zobrazovať v správe len informácie o tých zariadeniach, ku ktorým má daný používateľ pridelené povolenia. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

2.6 Zmeny po aktualizácii zo staršej verzie ERA

Ak ste vykonali aktualizáciu z ERA 6.4 alebo staršej verzie, je potrebné skontrolovať nastavenia používateľov, povolenia a nastavenia servera a uistiť sa, že vyhovujú vylepšenému bezpečnostnému modelu, ktorý poskytuje nástroj ESET Security Management Center.

Používatelia a sady povolení

Správca by mal skontrolovať všetkých používateľov a sady povolení. Nový bezpečnostný model je založený hlavne na statických skupinách, takže vám odporúčame si najskôr rozvrhnúť štruktúru skupín a až potom vytvárať sady povolení. Správca môže vytvárať aj nových natívnych používateľov.

Dôležité:
Nezabudnite ku každému používateľovi priradiť domácu skupinu a sadu povolení, ktorá používateľovi poskytne prístupové práva pre túto skupinu. Všetky objekty vytvorené používateľom budú vždy automaticky zahrnuté do domácej skupiny daného používateľa.

Po vykonaní aktualizácie budú používatelia rozdelení do dvoch kategórií:

- Používatelia, ktorým nebola pridelená sada povolení na prístup ku skupine *Všetko* v staršej verzii ERA, nebudú mať domácu skupinu v novej verzii ESMC. Títo používatelia nebudú mať prístupové práva ku **Skupinám a počítačom**, čo znamená, že sa im nebudú zobrazovať žiadne zariadenia.
- Používatelia, ktorým bola pridelená sada povolení na prístup ku skupine *Všetko* v staršej verzii ERA, budú mať tieto povolenia ponechané. Títo používatelia navyše získajú aj povolenia na prístup ku **Skupinám a počítačom**.

Úlohy pre server a spúšťače

Od verzie ERA 6.5 je povolený pre každú úlohu pre server len jeden spúšťač. Počet spúšťačov je po aktualizácii na verziu 6.5 automaticky upravený tak, aby sa zhodoval s počtom úloh pre server. V sekcii **Viac** > **Úlohy pre server** zvoľte konkrétnu úlohu pre zobrazenie podrobností o jej spúšťači.

Správy, šablóny a ostatné objekty

Po aktualizácii zo staršej verzie budú všetky objekty zahrnuté v statickej skupine *Všetko*. Správca môže jednotlivé objekty zdieľať medzi používateľmi rozličnými spôsobmi:

- duplikovaním objektov, čím sa tieto objekty sprístupnia používateľom bez administrátorských oprávnení,
- presunutím objektov do zdieľaných skupín, kde k nim má prístup viac používateľov,
- používateľom je možné prideliť dodatočné sady povolení, ktoré im umožnia obmedzený prístup k určitým objektom (napríklad k **Politikám**) cez skupinu *Všetko*.

Statické a dynamické skupiny

Statické skupiny sú základom bezpečnostného modelu v ESMC 7, kde je každý objekt umiestnený v jednej statickej skupine. Štruktúra statických aj dynamických skupín zostáva rovnaká aj po vykonaní aktualizácie. Používatelia musia mať pridelené povolenia pre svoju skupinu, aby bolo umožnené zobrazovanie a interakcia s ostatnými členmi skupiny.

2.7 ESET Push Notification Service

Služba **ESET Push Notification Service** (EPNS) dokáže odosielať pokyny na prebudenie medzi ESMC Serverom a ESET Management Agentmi verzie 7. Každý pokyn na prebudenie zároveň odosiela pokyn **Wake-on-LAN**. Rozosielacie adresy (multicast addresses) pre **Wake-on-LAN** môžete nastaviť v nastaveniach servera.

Podrobnosti o pripojení

Nato, aby bolo možné odosielať pokyny na prebudenie prostredníctvom EPNS, sa musia ESET Management Agent a ESMC Server vedieť pripojiť k EPNS serveru.

Podrobnosti o pripojení	
Zabezpečenie prenosu	SSL
Protokol	MQTT (protokol pripojenia machine-to-machine)
Port	8883
Adresa hostiteľa	epns.eset.com
Kompatibilita proxy	HTTP Proxy neumožňuje preposielanie protokolu MQTT. Agenty, ktoré používajú proxy, nemôžu dostávať pokyny na prebudenie.

Kompatibilita s nástrojom ERA 6.x

Nástroj ERA používal na odosielanie pokynov na prebudenie UDP pripojenie.

- ERA Agenty verzie 6.x môžu dostávať pokyny na prebudenie iba prostredníctvom UDP.
- ESET Management Agenty môžu dostávať pokyny na prebudenie iba prostredníctvom EPNS.

Z toho vyplýva, že ERA Agenty verzie 6.x nie sú kompatibilné s PRODUCT_NAME Serverom verzie 7.

Riešenie problémov

- Uistite sa, že váš firewall je nastavený tak, aby umožňoval pripojenie k EPNS serveru (podrobnejšie informácie nájdete v tabuľke vyššie).
- Uistite sa, že agent aj server majú priamu viditeľnosť na EPNS server.

2.8 Používanie softvéru od spoločnosti Safetica

Čo je Safetica

Safetica je softvérová spoločnosť tretej strany a člen Technologickej aliancie ESET. Spoločnosť Safetica poskytuje riešenie v oblasti IT bezpečnosti zamerané na prevenciu straty dát a dopĺňa bezpečnostné riešenia ESET. Medzi hlavné funkcie softvéru Safetica patria:

- Prevencia straty dát – monitorovanie všetkých pevných diskov, USB diskov, prenosov súborov po sieti, e-mailov a tlačiarní, ako aj prístupu k súborom aplikácií.
- Hlásenie a blokovanie aktivít – pre operácie so súbormi, webové stránky, e-maily, odosielanie okamžitých správ, použitie aplikácií a vyhľadávané kľúčové slová.

Ako funguje Safetica

Safetica nasadí na želané koncové pracovné stanice agenta (Safetica Endpoint Client) a udržiava s nimi pravidelné spojenie prostredníctvom servera (Safetica Management Service). Tento server vytvára databázu informácií o dianí na pracovných staniciach a distribuuje nové bezpečnostné politiky a nariadenia ochrany dát na jednotlivé pracovné stanice.

Integrácia softvéru Safetica s ESMC

ESET Management Agent deteguje a hlási softvér Safetica ako softvér spoločnosti ESET v sekcii **Podrobnosti o počítači** > **Nainštalované aplikácie**. ESMC Web Console aktualizuje Safetica agenta v prípade, že je dostupná novšia verzia. Safetica agent môže byť aktualizovaný priamo z ESMC Web Console prostredníctvom repozitára softvéru spoločnosti ESET.

3. Počiatočná konfigurácia, nasadenie produktu ESMC a VDI

Predtým, ako začnete spravovať bezpečnostné riešenia spoločnosti ESET, musíte najprv vykonať počiatočnú konfiguráciu. Odporúčame vám použiť Prehľad stavu, a to obzvlášť v prípade, ak ste preskočili Sprievodcu spustením.

Používatelia Web Console

Po prihlásení do ESMC Web Console vytvorte jeden alebo viacero **Natívnych používateľských účtov** a nastavte pre ne **Sady povolení** pre umožnenie rôznych úrovní správy v nástroji ESET Security Management Center.

Dôležité:
Neodporúčame používať prednastavený účet **správcu** nástroja ESMC (účet Administrator) ako štandardný používateľský účet. Tento účet slúži ako záloha v prípade, že sa vyskytnú problémy s bežnými používateľskými účtami. V takom prípade môžete použiť účet správcu a odstrániť dané problémy.

Čo sú certifikáty?

Certifikáty sú dôležitou súčasťou nástroja ESET Security Management Center, pretože sú potrebné pre umožnenie bezpečnej komunikácie súčastí ESMC s ESMC Serverom. Pre správnu komunikáciu súčastí ESMC musia byť všetky partnerské certifikáty platné a podpísané rovnakou certifikačnou autoritou.

Dôležité:
Budú sa vám zobrazovať len tie certifikáty, ktoré sú umiestnené vo vašej domácej skupine (za predpokladu, že máte pridelené povolenia na **čítanie** certifikátov). Certifikáty vytvorené počas inštalácie ESMC sú zahrnuté v skupine **Všetko** a prístup k nim tak majú iba správcovia.

V rámci certifikátov máte na výber niekoľko možností:

- Môžete používať certifikáty, ktoré boli automaticky vytvorené pri inštalácii nástroja ESMC.
- Môžete vytvoriť novú Certifikačnú autoritu (CA) alebo importovať verejný kľúč, ktorý použijete pri podpisovaní Partnerského certifikátu pre každý komponent (ESET Management Agent, ESMC Server, ESMC MDM alebo Virtual Agent Host).
- Môžete používať vlastnú Certifikačnú autoritu a certifikáty.

Poznámka:
Ak sa chystáte migrovať ESMC Server na iný počítač, musíte exportovať/zálohovať všetky certifikačné autority, ktoré používate, ako aj certifikát ESMC Servera. V opačnom prípade súčasti ESMC nebudú komunikovať s vaším novým ESMC Serverom.

Správa licencií

ESET Security Management Center má svoju vlastnú Správu licencií, ktorá je dostupná z hlavného menu v sekcii **Viac** > **Správa licencií**.

Pridať licenciu môžete troma metódami: môžete zadať **Licenčný kľúč**, zadať prihlasovacie údaje **Bezpečnostného správcu** alebo odovzdať **Offline licenčný súbor**.

Dôležité:
Pridávať a odstraňovať licencie môžu len správcovia, ktorých domácou skupinou je skupina **Všetko** a ktorí majú pridelené povolenia na **zápis** pre licencie (umiestnené v skupine Všetko). Každá licencia je identifikovaná **Verejným ID** a môže obsahovať jednu alebo viacero jednotiek. Licencie môže ostatným používateľom (tým, ktorí majú dostatočné povolenia) distribuovať len správca. Licenciu nie je možné rozdeliť.

Spôsoby nasadenia

ESET Security Management Center ponúka viacero spôsobov, ako na zariadenie nasadiť ESET Management Agenta a bezpečnostné produkty ESET. Podrobnejšie informácie nájdete v nasledujúcich kapitolách.

3.1 Nasadenie

Po úspešnej inštalácii nástroja ESET Security Management Center je potrebné nasadiť **ESET Management Agenta** na klientske počítače vo vašej sieti. Táto časť popisuje všetky dostupné metódy nasadenia ESET Management Agenta. Agent je veľmi dôležitý, pretože bezpečnostné riešenia spoločnosti ESET spustené na klientskych počítačoch komunikujú s ESMC Serverom výhradne pomocou agenta.

Po úspešnej inštalácii nástroja ESET Security Management Center a jeho počiatočnej konfigurácii sa proces nasadenia skladá z nasledujúcich krokov:

1. Pridanie klientskych počítačov do skupinovej štruktúry ESMC – je potrebné nasadiť ESET Management Agenta a nainštalovať bezpečnostný produkt spoločnosti ESET na počítače v sieti.
2. Proces nasadenia agenta – môžete si vybrať medzi lokálnym nasadením a vzdialeným nasadením.
3. Vytvorenie politiky na aplikovanie vašich vlastných nastavení – táto politika bude vynútená agentom akonáhle bude nainštalovaný softvér. Pre viac informácií si pozrite krok č. 4.
4. Inštalácia bezpečnostného produktu spoločnosti ESET – použitie úlohy inštalácia softvéru na inštaláciu bezpečnostných produktov spoločnosti ESET.

Pri problémoch so vzdialeným nasadením ESET Management Agenta (napríklad zlyhá úloha pre server **Nasadenie agentov**) si prezrite informácie na nasledujúcich odkazoch:

Riešenie problémov – nasadenie agenta

Riešenie problémov – pripojenie agenta

Ukážkové scenáre nasadenia ESET Management Agenta

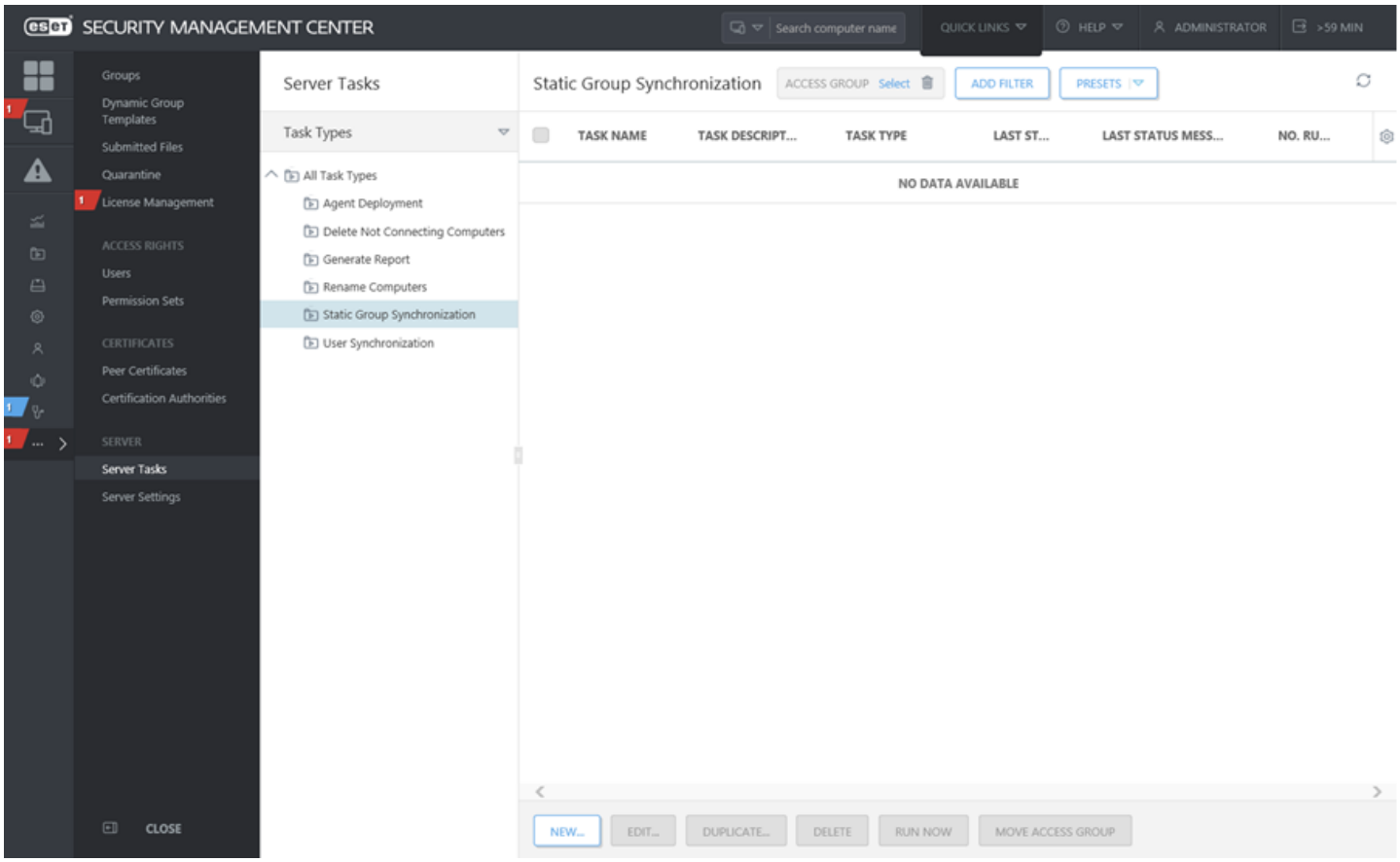
3.1.1 Pridanie klientskeho počítača do štruktúry ESMC

Predtým, ako začnete spravovať klientske počítače vo vašej sieti, musíte ich pridať do nástroja ESET Security Management Center. Pre pridanie počítačov do ESMC použite jednu z nasledujúcich metód:

- Synchronizácia s Active Directory
- Použitie nástroja RD Sensor
- Manuálne pridanie nových zariadení
- Lokálna inštalácia ESET Management Agenta

3.1.1.1 Synchronizácia s Active Directory

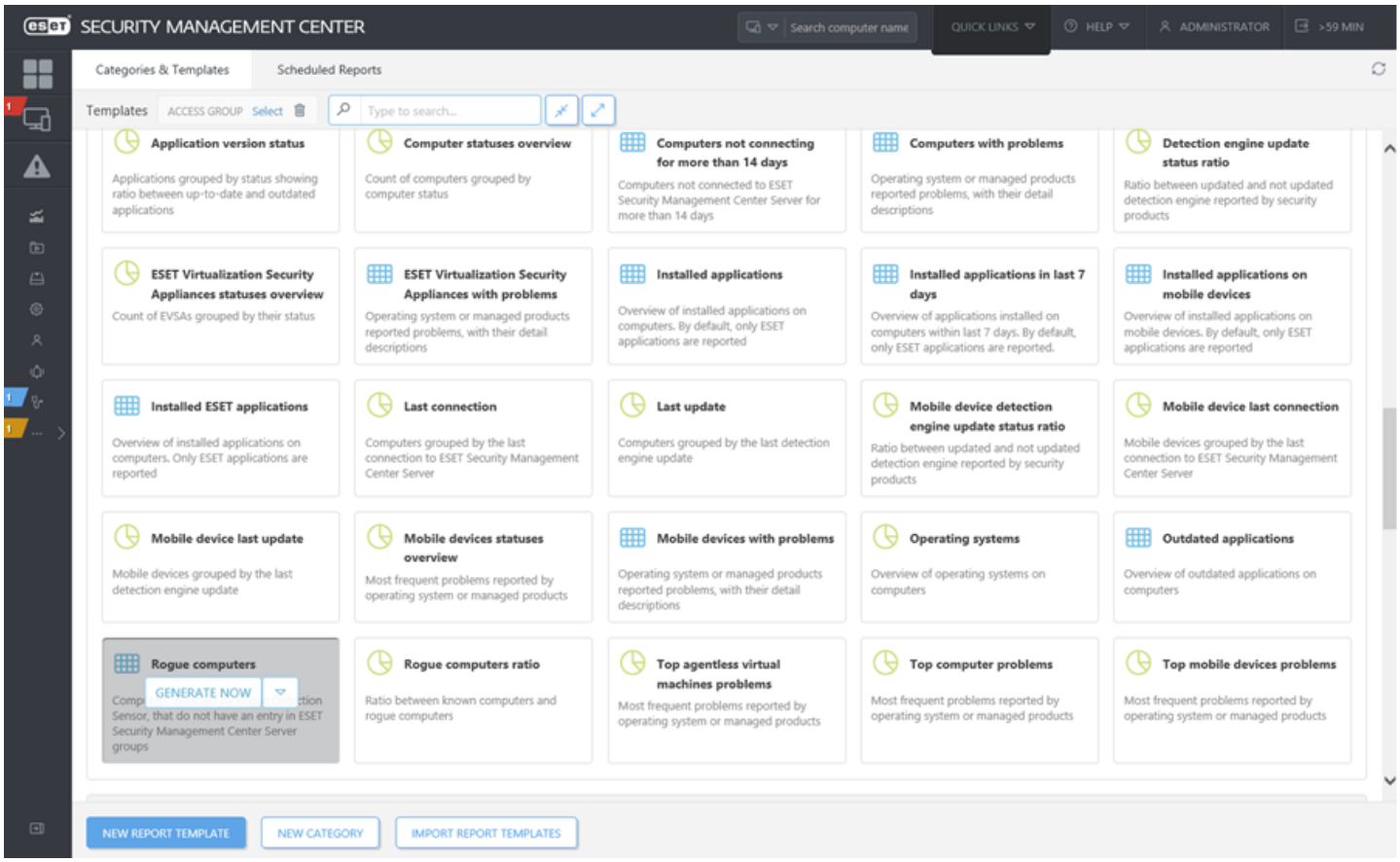
AD synchronizácia je vykonávaná pomocou úlohy pre server **Synchronizácia statickej skupiny**. Ide o prednastavenú úlohu, ktorá môže byť spustená automaticky už počas inštalácie produktu ESET Security Management Center. Ak je počítač v doméne, prebehne synchronizácia a počítače z AD budú pridané do predvolenej skupiny **Všetko**.



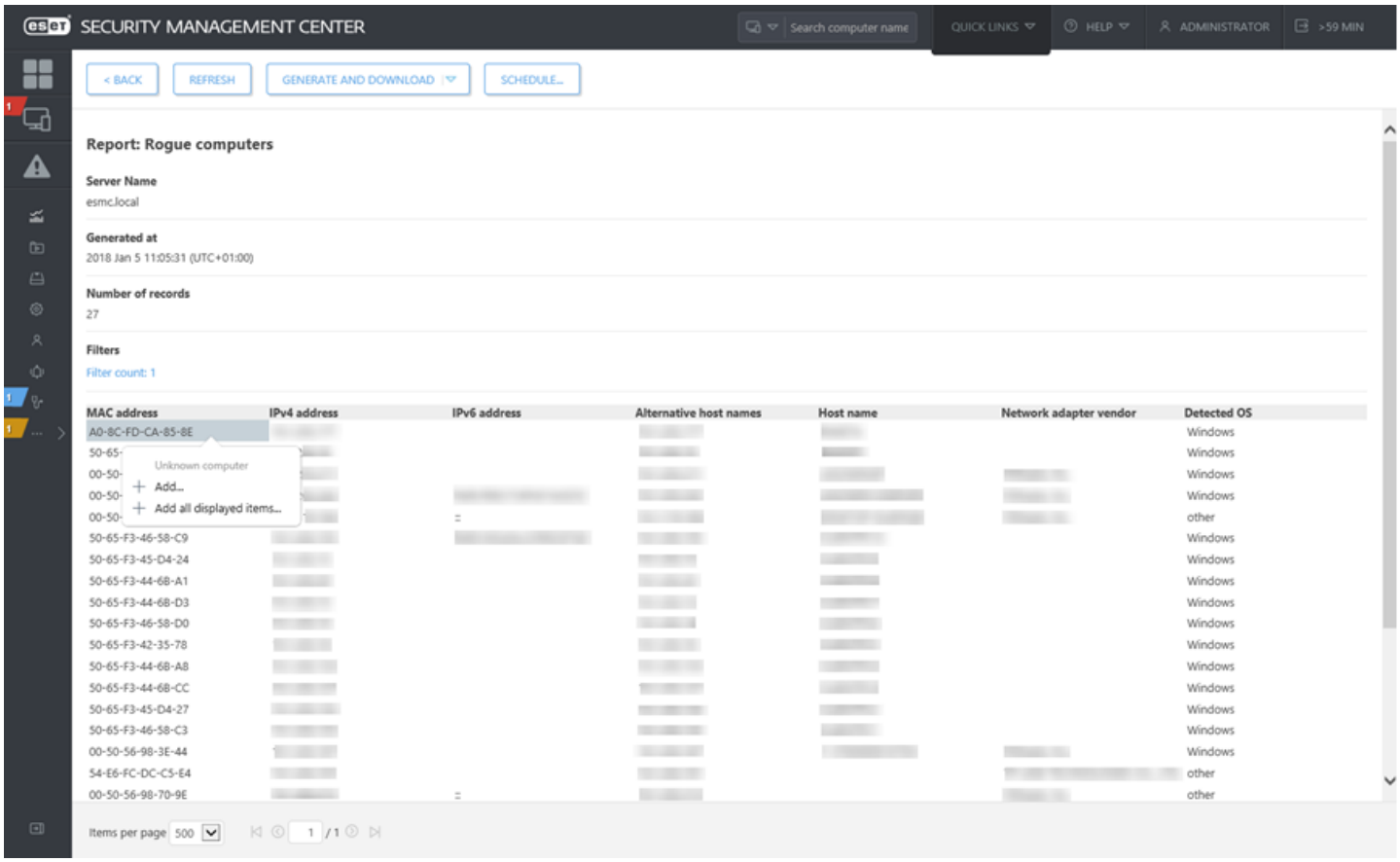
Ak chcete spustiť synchronizáciu, kliknite na úlohu a vyberte možnosť **Vykonať teraz**. Ak potrebujete vytvoriť novú úlohu pre synchronizáciu s AD, označte skupinu, do ktorej chcete pridať nové počítače zo služby Active Directory. Taktiež vyberte objekty v AD, ktoré chcete synchronizovať a nastavte, čo sa má stať v prípade výskytu duplikátov. Nastavte parametre pripojenia k Active Directory a režim synchronizácie nastavte na **Active Directory/Open Directory/LDAP**. Postupujte podľa podrobných inštrukcií nachádzajúcich sa v nasledujúcom článku databázy znalostí spoločnosti ESET.

3.1.1.2 Používanie nástroja RD Sensor

Ak nepoužívate synchronizáciu s Active Directory, najjednoduchším spôsobom, ako pridať počítač do ESMC štruktúry, je použitie nástroja **RD Sensor**. Nástroj RD Sensor je súčasťou inštalačného balíka. V časti **Správy** prejdite do sekcie **Počítače**, vyberte správu s označením **Neautorizované počítače** a kliknite na **Vygenerovať**.

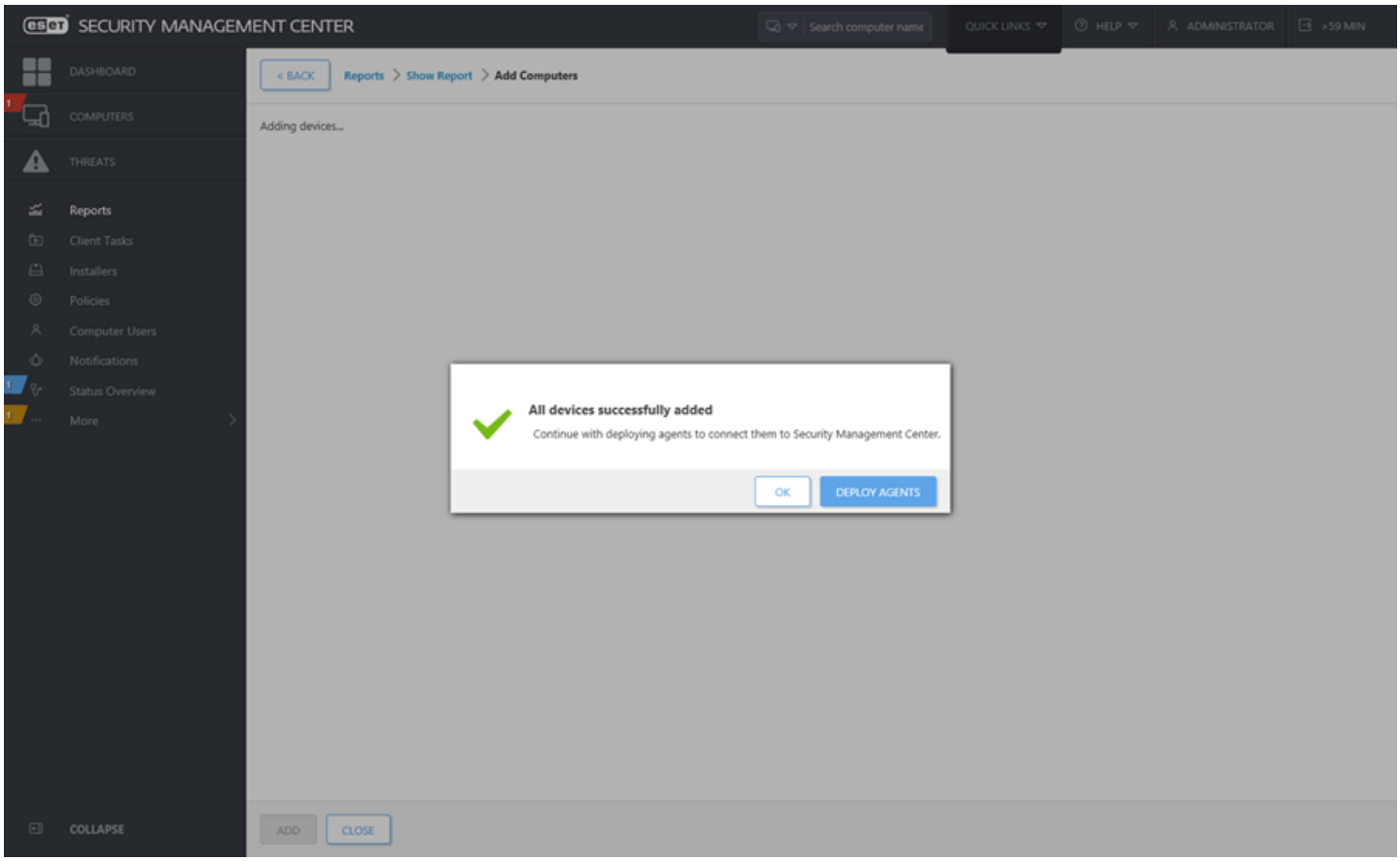


Správa **Neautorizované počítače** teraz zobrazuje počítače nájdené nástrojom RD Sensor. Počítače môžu byť pridané kliknutím na počítač, ktorý chcete pridať a kliknutím na **Pridať**, prípadne môžete kliknúť na **Pridať všetky zobrazené položky**.



Ak pridávate jeden počítač, môžete použiť preddefinovaný názov alebo zadať vlastný (ide len o zobrazovaný názov, ktorý bude použitý iba v ESMC Web Console, nie ako názov hostiteľa). Môžete tiež pridať popis. Ak sa už tento počítač nachádza v ESMC adresári, budete na to upozornený a môžete sa rozhodnúť, ako pokračovať. Sú dostupné tieto možnosti: **Nasadiť agenta**, **Vynechať**, **Opakovať**, **Presunúť**, **Duplikovať** alebo **Zrušiť**. Po pridaní počítača sa zobrazí okno s možnosťou **Nasadiť agenta**.

Po kliknutí na možnosť **Pridať všetky zobrazené položky** sa zobrazí zoznam počítačov, ktoré budú pridané. Kliknite na vedľa názvu konkrétneho počítača, ak ho nechcete pridať do ESMC štruktúry. Po odstránení neželaných počítačov zo zoznamu kliknite na **Pridať**. Po kliknutí na **Pridať** označte akciu, ktorá bude vykonaná pri nájdení duplikátov (pri veľkom počte počítačov môže nastať oneskorenie): **Vynechať, Opakovať, Presunúť**, **Duplikovať** alebo **Zrušiť**. Následne sa zobrazí okno s možnosťou **Nasadiť agentov**.



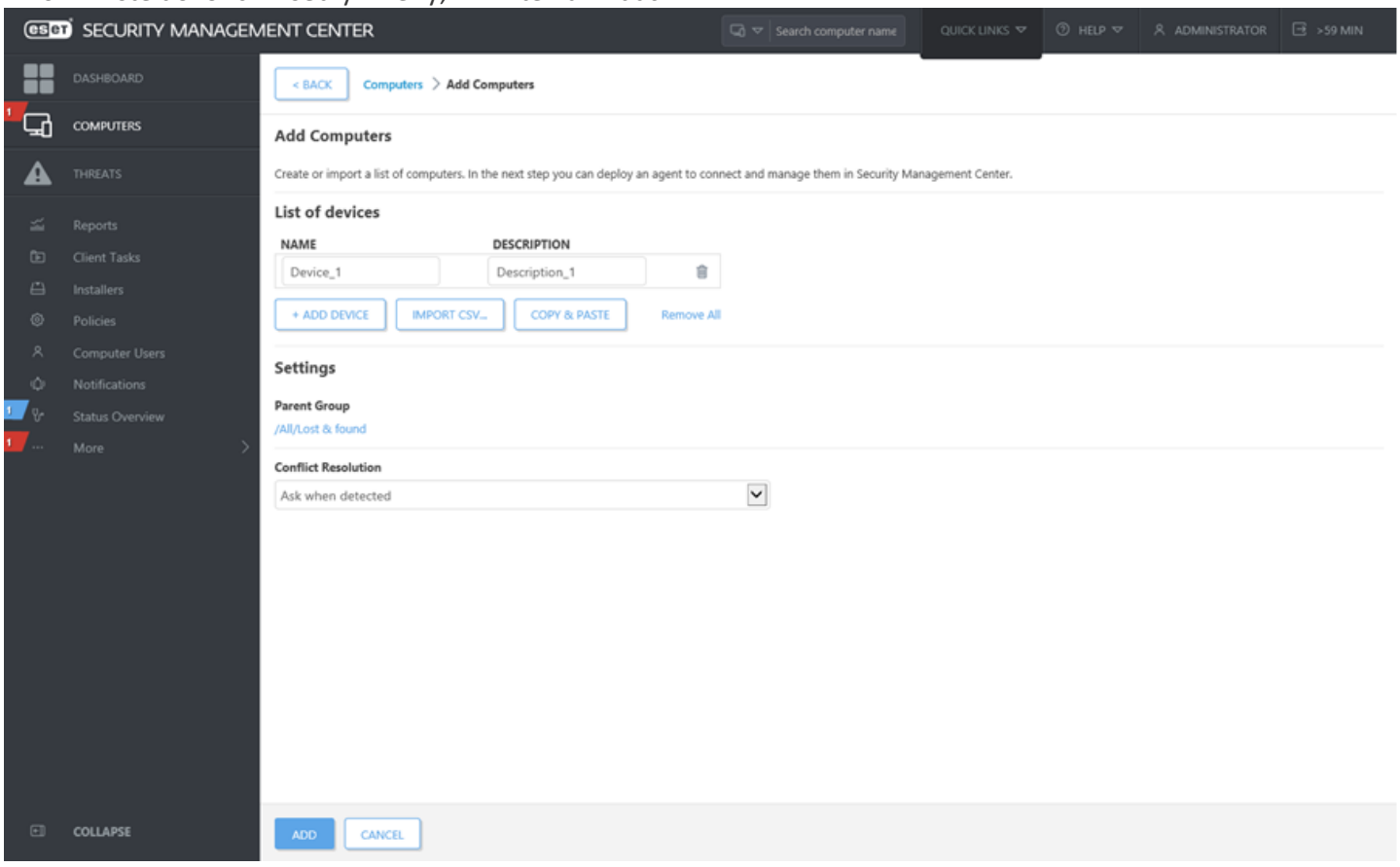
Výsledky vyhľadávania nástroja RD Sensor sú zapísané do protokolu `detectedMachines.log`. Tento protokol obsahuje zoznam počítačov nájdených vo vašej sieti. Protokol `detectedMachines.log` sa nachádza v nasledujúcich umiestneniach:

- Windows
  C:\ProgramData\ESET\Rogue Detection Sensor\Logs\detectedMachines.log
- Linux
  /var/log/eset/RogueDetectionSensor/detectedMachines.log

3.1.1.3 Pridávanie počítačov

Táto funkcia umožňuje manuálne pridávanie **počítačov** alebo mobilných zariadení, ktoré neboli nájdené alebo pridané automaticky. Karta **Počítače** alebo **Skupiny** vám umožňuje pridať nové počítače alebo mobilné zariadenia.

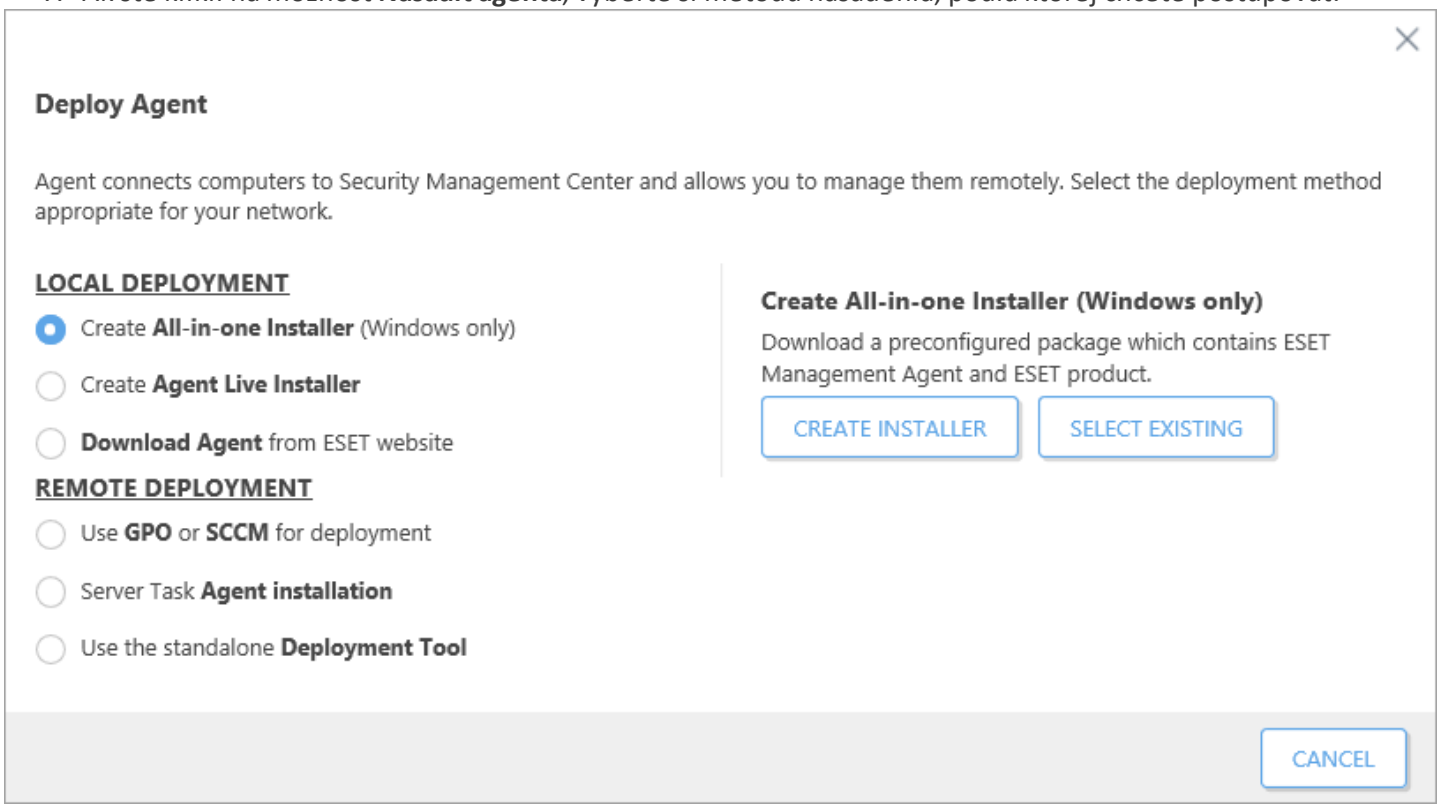
1. Pre pridanie nového počítača prejdite do sekcie **Počítače**, kliknite na tlačidlo **Pridať nový** a následne vyberte možnosť **Počítače** (prípadne kliknite na ikonu ozubeného kolesa vedľa už existujúcej **Statickej skupiny** a potom kliknite na **Pridať nové**).
2. Zadajte **IP adresu** alebo **názov hostiteľa** pre počítač, ktorý chcete pridať a ESET Security Management Center vyhľadá tento počítač v sieti. V prípade potreby môžete pre počítače môžete zadať aj **Popis**.
3. **Nadradená skupina** – vyberte existujúcu nadradenú skupinu a následne kliknite na **OK**.
4. Z roletového menu **Riešenie konfliktov** vyberte akciu, ktorá bude vykonaná, ak sa už počítač, ktorý chcete pridať, nachádza v ESMC:
   - **Spýtať sa pri zachytení:** Ak nastane konflikt, program sa spýta, akú akciu má vykonať (pozrite možnosti nižšie).
   - **Preskočiť duplicitné zariadenia:** Počítače, ktoré sa už nachádzajú v ESMC, nebudú pridané.
   - **Presunúť duplicitné zariadenia do skupiny... :** Konfliktné počítače budú presunuté do **Nadradenej skupiny**.
   - **Vytvárať duplicitné zariadenia:** Budú pridané nové počítače, avšak s odlišnými názvami.
5. Môžete použiť nasledujúce možnosti:
   a. Možnosť **+ Pridať zariadenie** pre pridanie ďalších počítačov. Ak chcete odstrániť počítač zo zoznamu zariadení, kliknite na ikonu **Odpadkového koša** alebo kliknite na možnosť **Odobrať všetky**.
   b. Možnosť **Import CSV** pre odovzdanie `.csv` súboru obsahujúceho zoznam počítačov, ktoré majú byť pridané. Viac informácií nájdete v časti Import CSV.
   c. **Skopírovať a vložiť** vlastný zoznam adries oddelených vlastnými oddeľovačmi. Táto funkcia funguje podobne ako CSV import.
6. Ak ste dokončili všetky zmeny, kliknite na **Pridať**.



Poznámka:
Pridávanie viacerých počítačov môže trvať dlhšie (môže byť uskutočnené reverzné vyhľadávanie DNS záznamov).

Po kliknutí na tlačidlo **Pridať** sa zobrazí nové okno so zoznamom zariadení, ktoré majú byť pridané. Môžete kliknúť na **OK** alebo nasadiť agenta.

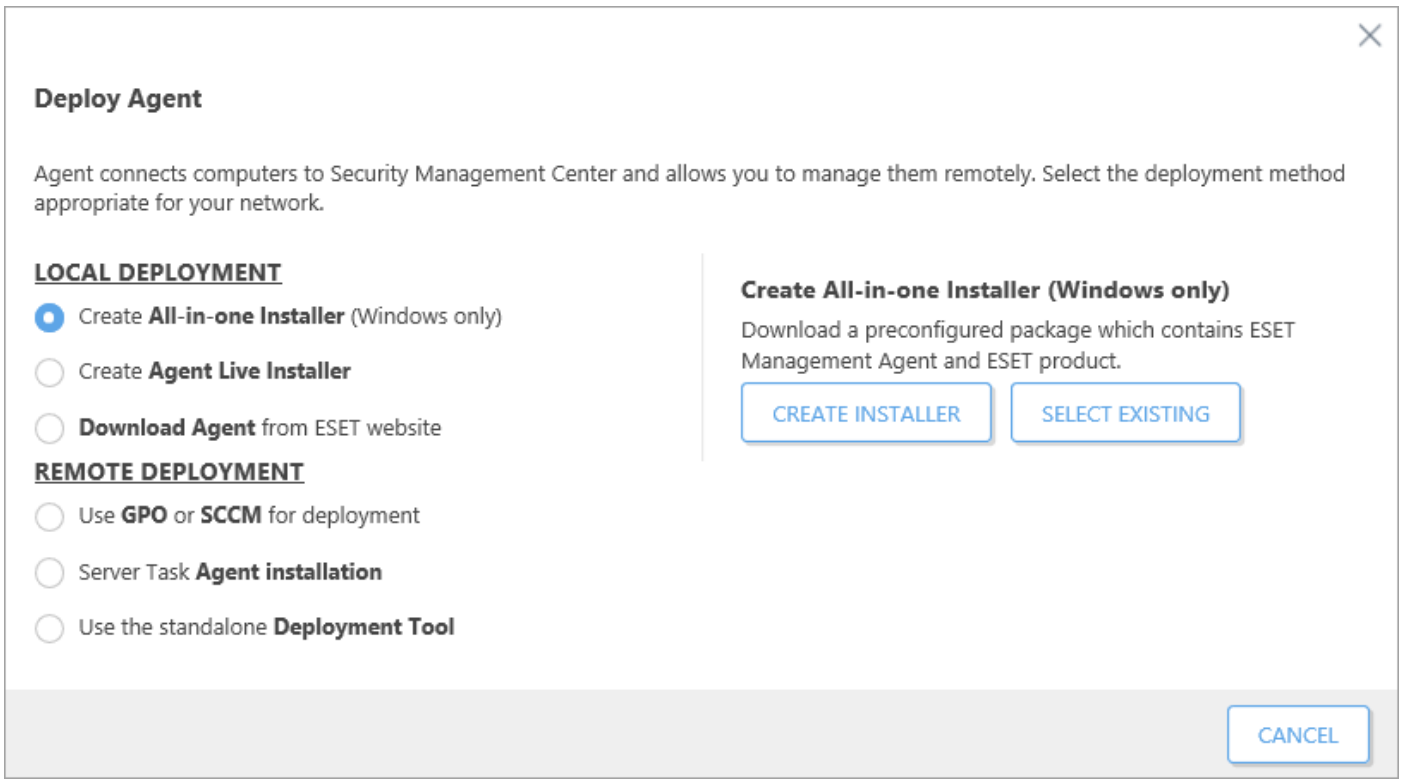
7. Ak ste klikli na možnosť **Nasadiť agenta**, vyberte si metódu nasadenia, podľa ktorej chcete postupovať:



3.1.2 Proces nasadenia agenta

Nasadenie ESET Management Agenta je možné vykonať troma rôznymi spôsobmi. Agenta môžete nasadiť lokálne alebo vzdialene:

- Lokálne nasadenie – pomocou all-in-one inštalačného balíka (ESET Management Agent a bezpečnostný produkt ESET), live inštalátorov agenta alebo stiahnutím ESET Management Agenta z webovej stránky spoločnosti ESET.
- Vzdialené nasadenie – túto metódu odporúčame použiť v prípade nasadenia ESET Management Agenta na väčší počet klientskych počítačov.



3.1.2.1 Lokálne nasadenie

Táto metóda nasadzovania je určená na lokálne inštalácie. Prvým krokom je vytvorenie alebo stiahnutie inštalačného balíka. Tento balík je následne sprístupnený pomocou zdieľaného priečinka alebo je distribuovaný použitím USB kľúča (prípadne prostredníctvom e-mailu). Inštalačný balík musí byť na klientskom zariadení nainštalovaný správcom alebo používateľom s oprávneniami správcu.

Poznámka:
Lokálne nasadenie odporúčame použiť len v prípade malých sietí (do 50 počítačov). Vo väčších sieťach môžete nasadiť ESET Management Agenta pomocou GPO alebo SCCM.

Sú dostupné tri spôsoby lokálneho nasadenia:

Vytvorenie all-in-one inštalátora agenta (iba Windows)

Vytvorenie Live inštalátora agenta

Stiahnutie agenta z webovej stránky spoločnosti ESET (Windows, Linux, macOS)

Povolenia na lokálne nasadenie agenta

Podrobný postup, ako používateľovi udeliť povolenia na lokálne nasadenie ESET Management Agenta, nájdete v tomto príklade.

Poznámka:
Pri vytváraní inštalátorov agenta bude používateľ pracovať s certifikátmi. Používateľ musí mať povolenie na **použitie Certifikátov** s prístupom k statickej skupine, kde sa nachádzajú certifikáty. Používateľ bude môcť nasadzovať ESET Management Agenta len v prípade, že mu bolo pridelené povolenie na **použitie** certifikačnej autority, ktorou je podpísaný samotný certifikát servera. Informácie o tom, ako udeliť prístupové práva k certifikátom bez možnosti prístupu k certifikačným autoritám, nájdete v tomto príklade. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

3.1.2.1.1 Vytvorenie all-in-one inštalátora agenta

Proces tvorby all-in-one inštalátora (obsahujúceho ESET Management Agenta a bezpečnostný produkt ESET) je podobný ako Sprievodca spustením, avšak all-in-one inštalátor ponúka pokročilé možnosti nastavenia. Tieto možnosti zahŕňajú nastavenia **Politiky** pre ESET Management Agenta a bezpečnostné produkty ESET, **Názov hostiteľa** ESMC Servera a **Port**, ako aj možnosť zvoliť **Nadradenú skupinu**.

Dôležité:
Inštalačný balík je v podobe súboru `.exe` a je platný len pre operačné systémy Microsoft Windows.

Kliknite na **Iné možnosti nasadenia** v časti **Rýchle odkazy** na paneli s ponukami. V okne **Nasadiť agenta** kliknite na **Vytvoriť inštalátor** pod možnosťou **Vytvoriť all-in-one inštalátor (iba Windows)**. Otvorí sa okno **Vytvoriť all-in-one inštalátor**.

Vytvorenie inštalačného balíka

Ak nesúhlasíte so zasielaním správ o zlyhaní programu a telemetrických údajov spoločnosti ESET, zrušte označenie možnosti **Zúčastnite sa programu zlepšovania produktov**. Ak ponecháte túto možnosť označenú, telemetrické údaje a správy o zlyhaní programu budú odosielané spoločnosti ESET.

Obsah balíka – vyberte si jednu z nasledujúcich možností:

- **Bezpečnostný produkt + agent** – obsahuje bezpečnostný produkt ESET s ESET Management Agentom. Túto možnosť vyberte v prípade, že na klientskom počítači nie je nainštalovaný žiadny bezpečnostný produkt ESET a chcete ho nainštalovať pomocou ESET Management Agenta.

Produkt – rozbaľte túto sekciu a zo zoznamu dostupných produktov spoločnosti ESET vyberte požadovaný inštalačný súbor. Ak vyberiete verziu 6.3 alebo staršiu, automatická aktivácia produktu nebude fungovať. Produkt budete musieť aktivovať neskôr. Bezpečnostné produkty ESET verzie 6.4 a novších verzií budú pri inštalácii aktivované automaticky.

Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.

Poznámka:
Ak sa nezobrazujú žiadne inštalačné súbory produktu, uistite sa, že máte repozitár nastavený na **AUTOSELECT**. Podrobnosti nájdete v Nastaveniach servera v časti **Pokročilé nastavenia**.

Jazyk – vyberte jazyk inštalátora zo zoznamu podporovaných jazykov.
Licencia (povinné) – túto možnosť použite na pridanie licencie pomocou jednej z metód popísaných v časti Licencie. Ak už máte existujúce licencie v Správe licencií, vyberte licenciu, ktorá bude použitá na aktiváciu bezpečnostného produktu ESET počas inštalácie. Ak nevyberiete licenciu, môžete vytvoriť inštalátor bez nej a aktivovať produkt neskôr.

- **Iba agent** – obsahuje iba ESET Management Agenta. Túto možnosť vyberte v prípade, že chcete nainštalovať bezpečnostný produkt ESET na klientsky počítač neskôr alebo na klientskom počítači už bezpečnostný produkt nainštalovaný je.

Certifikát

Partnerský certifikát a certifikačná autorita ESMC sú zvolené automaticky podľa dostupných certifikátov. Ak chcete použiť iný certifikát ako ten, ktorý bol zvolený automaticky, kliknite na **ESMC Certifikát**. Zobrazí sa zoznam dostupných certifikátov, z ktorého môžete vybrať vami požadovaný certifikát. Ak chcete používať **Vlastný certifikát**, kliknite na prepínacie tlačidlo a odovzdajte certifikačný súbor `.pfx`. Bližšie inštrukcie nájdete v časti Vlastné certifikáty pre ESMC.

V prípade potreby zadajte vašu **Prístupovú frázu certifikátu**. Je potrebné ju zadať napríklad vtedy, ak ste prístupovú frázu špecifikovali počas inštalácie ESMC alebo ak používate vlastný certifikát s prístupovou frázou. V opačnom prípade ponechajte pole **Prístupová fráza certifikátu** prázdne.

Dôležité:
Prístupovú frázu certifikátu je možné extrahovať, pretože je vložená v súbore `.exe`.

Rozšírené

Táto sekcia vám umožňuje upraviť all-in-one balík inštalátora podľa vlastných potrieb:

1. V prípade potreby môžete zmeniť **Názov** inštalačného balíka a zadať preň **Popis**.
2. **Nadradená skupina (voliteľná)** – vyberte **Nadradenú skupinu**, do ktorej bude počítač po inštalácii umiestnený. Ak chcete vytvoriť novú nadradenú statickú skupinu, kliknite na tlačidlo **Nová statická skupina** a použite sprievodcu. Novovytvorená skupina bude automaticky zvolená.
3. Nástroj **ESET AV Remover** vám pomôže odinštalovať alebo úplne odstrániť iné antivírusové programy. Ak chcete tento nástroj použiť, označte príslušné začiarkavacie políčko.
4. **Počiatočná konfigurácia inštalátora** – môžete si vybrať z dvoch typov konfigurácie:
   - **Nekonfigurovať** – budú aplikované iba politiky, ktoré sú zlúčené do nadradenej statickej skupiny.
   - **Vybrať konfiguráciu zo zoznamu politík** – túto možnosť použite, ak chcete aplikovať konfiguračnú politiku na ESET Management Agenta a/alebo bezpečnostný produkt ESET. Kliknite na **Vybrať** a vyberte si zo zoznamu dostupných politík. Ak vám nevyhovuje žiadna z preddefinovaných politík, môžete vytvoriť novú politiku alebo najprv upraviť už existujúcu politiku. Ak potom znova skúsite vybrať politiku, v zozname už bude zobrazená vaša nová politika.
     a. V prípade potreby môžete špecifikovať **Názov hostiteľa ESMC Servera** a číslo **Portu**. V opačnom prípade predvolené hodnoty nemeňte.
6. Kliknite na **Dokončiť**. Súbory all-in-one inštalačného balíka budú vygenerované pre 32-bitové a 64-bitové operačné systémy. Kliknite na požadovanú verziu a začne sa sťahovanie. Po dokončení sťahovania budete vyzvaný na výber umiestnenia, kde bude súbor uložený (napr. *ESMC_Installer_x32_en_US.exe* alebo *ESMC_Installer_x64_en_US.exe*). Kliknite na **Uložiť súbor**.
7. Spustite súbor all-in-one inštalačného balíka na klientskom počítači. Podrobné inštrukcie týkajúce sa sprievodcu inštaláciou balíka nájdete v tejto príručke.

3.1.2.1.2 Vytvorenie Live inštalátora agenta

Tento typ nasadenia agenta je užitočný v prípade, že vám nevyhovuje vzdialené ani lokálne nasadenie. V takomto prípade môžete odoslať Live inštalátor agenta prostredníctvom e-mailu a nasadenie ponechať na používateľovi. Live inštalátor agenta môžete tiež spustiť z vymeniteľného média (napr. z USB kľúča).

> **Poznámka:**
> Klientske zariadenie musí mať internetové pripojenie, aby bolo možné stiahnuť inštalačný balík pre agenta. Klient sa tiež musí vedieť pripojiť na ESMC Server.

Kliknite na **Iné možnosti nasadenia** v časti **Rýchle odkazy** na paneli s ponukami. V okne **Nasadiť agenta** kliknite na tlačidlo **Vytvoriť inštalátor**, ktoré sa nachádza pod možnosťou **Vytvoriť Live inštalátor agenta**. Otvorí sa okno s Live inštalátormi agenta.

Vytvorenie inštalačného balíka

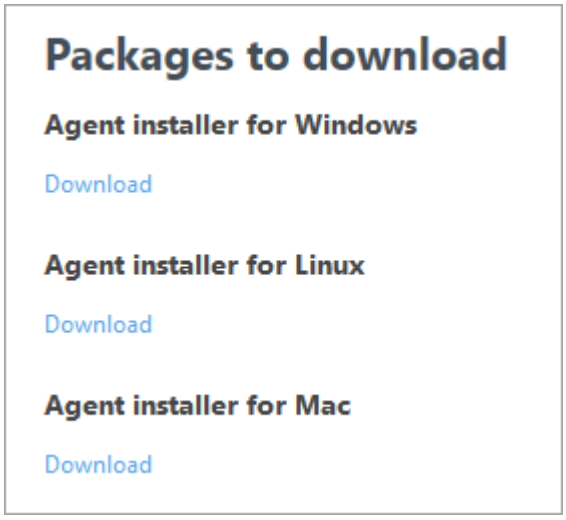
Ak nesúhlasíte so zasielaním správ o zlyhaní programu a telemetrických údajov spoločnosti ESET, zrušte označenie možnosti **Zúčastnite sa programu zlepšovania produktov**. Ak ponecháte túto možnosť označenú, telemetrické údaje a správy o zlyhaní programu budú odosielané spoločnosti ESET.

Certifikát – partnerský certifikát a certifikačná autorita ESMC sú zvolené automaticky podľa dostupných certifikátov. Ak chcete použiť iný certifikát ako ten, ktorý bol automaticky zvolený, kliknite na ESMC Certifikát. Zobrazí sa zoznam dostupných certifikátov, z ktorého môžete vybrať vami požadovaný certifikát. Ak chcete používať **Vlastný certifikát**, kliknite na prepínacie tlačidlo a odovzdajte certifikačný súbor `.pfx`. Viac informácií nájdete v časti Vlastné certifikáty pre ESMC.

V prípade potreby zadajte **Prístupovú frázu certifikátu**. Je potrebné ju zadať napríklad vtedy, ak ste prístupovú frázu špecifikovali počas inštalácie ESMC alebo ak používate vlastný certifikát s prístupovou frázou. V opačnom prípade ponechajte pole **Prístupová fráza certifikátu** prázdne.

Konfigurácia – táto sekcia vám umožňuje upraviť nastavenia inštalátora podľa vlastných potrieb:

1. V prípade potreby môžete zmeniť **Názov** inštalátora a zadať preň **Popis**.
2. **Názov hostiteľa servera** – v prípade potreby môžete špecifikovať **Názov hostiteľa** ESMC **Servera** a číslo **Portu**. V opačnom prípade predvolené hodnoty nemeňte.
3. **Nadradená skupina (voliteľná)** – vyberte **Nadradenú skupinu**, do ktorej bude počítač po inštalácii umiestnený. Ak chcete vytvoriť novú nadradenú statickú skupinu, kliknite na tlačidlo **Nová statická skupina** a použite sprievodcu. Novovytvorená skupina bude automaticky zvolená.
4. Kliknite na **Dokončiť** pre vytvorenie odkazov na súbory inštalátora agenta pre operačné systémy Windows, Linux a macOS.



5. Kliknite na **Stiahnuť** pod súborom inštalátora, ktorý chcete stiahnuť, a príslušný súbor **.zip** uložte. Rozbaľte .zip súbor na klientskom počítači, na ktorý chcete nasadiť ESET Management Agenta, a spustite skript `ESMCAgentOnlineInstaller.bat` (Windows) alebo skript `ESMCAgentOnlineInstaller.sh` (Linux a macOS) pre spustenie inštalácie. Viac informácií o nasadení ESET Management Agenta na klienta pomocou Live inštalátora nájdete v našom článku databázy znalostí.

Poznámka:
Ak chcete spustiť daný skript na systéme Windows XP SP2, musíte si nainštalovať Microsoft Windows Server 2003 Administration Tools Pack. V opačnom prípade sa Live inštalátor agenta nespustí správne. Po nainštalovaní balíka Administration Tools Pack môžete spustiť skript Live inštalátora agenta.

Poznámka:
Stav klientskeho počítača sa zaznamenáva do protokolu *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*, pomocou ktorého sa môžete uistiť, či ESET Management Agent pracuje správne. V prípade, že sa vyskytnú problémy s agentom (napríklad sa nepripája na ESMC Server), pozrite si kapitolu Riešenie problémov.

Nasadenie z vlastného vzdialeného umiestnenia

Ak chcete nasadiť agenta z iného umiestnenia ako je ESET repozitár, upravte inštalačný skript tak, aby obsahoval novú URL adresu, kde sa nachádza balík agenta. Môžete tiež použiť IP adresu nového balíka.

Nájdite a upravte nasledujúce riadky:

- Inštalátor systému Windows:
  `set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7.../Agent_x64.msi`
  `set url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7.../Agent_x86.msi`

- Inštalátor systému Linux:
  `eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7.../Agent-Linux-i386.sh`
  `eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7.../Agent-Linux-x86_64.sh`

- Inštalátor systému macOS:
  `eraa_installer_url=http://repository.eset.com/v1/com/eset/apps/business/era/agent/v7.../Agent-MacOSX-x86_64.dmg`

Nasadenie z lokálneho zdieľaného priečinka

Ak chcete nasadiť ESET Management Agenta pomocou Live inštalátora agenta zo svojho lokálneho zdieľaného priečinka bez použitia ESET repozitára, postupujte nasledovne:

Windows

1. Upravte súbor `ESMCAgentOnlineInstaller.bat`.
2. Zmeňte riadky 30 a 33 tak, aby odkazovali na lokálne stiahnuté súbory. Pôvodný súbor vyzerá nasledovne:

```
30 set url=http://h3-externtest-v.eset.com/repository_devel/com/eset/apps/business/era/agent/v7/7.0.261.0/agent_x64.msi
31 set checksum=302f8e5a0cc45639c1a20cc44896a870c1b8ba80
32 if defined IsArch_x86 (
33   set url=http://h3-externtest-v.eset.com/repository_devel/com/eset/apps/business/era/agent/v7/7.0.261.0/agent_x86.msi
34   set checksum=f64cce26499d15d717e62a219305bfe9d2a91f1d
```

3. Použite vlastnú URL adresu (lokálny zdieľaný priečinok), nie tú, ktorá je zobrazená na obrázku:

```
30 set url=\\server\share\Agent_x64.msi
31 set checksum=67e2c3c29633548daad2a8f6c59045d11d538b42
32 if defined IsArch_x86 (
33   set url=\\server\share\Agent_x86.msi
34   set checksum=0f80b4e9dc22ae4192601c335b6b6a76a79f5255
```

Poznámka:
Live inštalátor agenta overuje integritu inštalačných súborov na základe kontrolného súčtu checksum (pozrite si riadky 31 a 34). Ide o jedinečný reťazec generovaný pre každý súbor. V prípade, že sa zmení súbor, zmení sa zároveň aj jeho checksum.

Dôležité:
Uistite sa, že používateľský účet, pod ktorým je inštalačný balík spúšťaný, má pridelené povolenie na zápis pre zvolený lokálny zdieľaný priečinok. Zadaná cesta môže obsahovať medzery, napríklad `\\server\shared folder\Agent_x64.msi` (nepoužívajte úvodzovky "").

4. Do riadku 76 namiesto **" echo.packageLocation = DownloadUsingHTTPProxy^("!url!", "!http_proxy_hostname!", "!http_proxy_port!", "!http_proxy_username!", "!http_proxy_password!"^) "**

```
75 echo.On Error Resume Next
76 echo.packageLocation = DownloadUsingHTTPProxy^("!url!", "!http_proxy_hostname!","!http_proxy_port!", "!http_proxy_username!", "!http_proxy_password!"^)
77 echo.If packageLocation = "" Then
78 echo.    packageLocation = DownloadUsingHTTPProxy^("!url!", "", "", "", ""^)
79 echo.    If packageLocation = "" Then
80 echo.        Wscript.Quit 30
81 echo.    End If
82 echo.End If
83 echo.On Error GoTo 0
```

zadajte **echo.packageLocation = "!url!"**

```
75  echo.On Error Resume Next
76  echo.packageLocation = "!url!"
77  echo.If packageLocation = "" Then
78  echo.    packageLocation = DownloadUsingHTTPProxy^("!url!", "", "", "", ""^)
79  echo.    If packageLocation = "" Then
80  echo.        Wscript.Quit 30
81  echo.    End If
82  echo.End If
83  echo.On Error GoTo 0
```

5. Uložte súbor.

macOS

1. Otvorte skript `ESMCAgentOnlineInstaller.sh` v textovom editore.
2. Vymažte nasledujúce riadky: 52, 53 a 56 – 68.

```
50  eraa_product_uuid=""
51
52  eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.5.376.0/agent-macosx-i386.dmg"
53  eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
54  eraa_initial_sg_token="MDAwMDAwMDAtMDAwMC0wMDAwLTcwMDEtMDAwMDAwMDAwMDAyyV+3a+e2RtKK4qtJHgJO3zW9ioNnokabqhsC6n+Ek80sRQ6CtUGFHuETqOREOB462cUJ1Q=="
55
56  arch=$(uname -m)
57  if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)
58  then
59      eraa_installer_url="http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.5.376.0/agent-macosx-i386.dmg"
60      eraa_installer_checksum="9b28a28ea75d0325f1b3f56661e747bbe84ba895"
61  fi
62
63  if test -z $eraa_installer_url
64  then
65    echo "No installer available for '$arch' arhitecture. Sorry :/"
66    exit 1
67  fi
68
69  local_params_file="/tmp/postflight.plist"
70  echo "$local_params_file" >> "$files2del"
```

3. Nahraďte riadky 138 – 159 cestou k svojmu lokálnemu inštalátoru. Pozrite si zvýraznenú časť na obrázku. Použite vlastnú URL adresu (lokálny zdieľaný priečinok), nie tú, ktorá je zobrazená na obrázku.

```
136   done < "$local_migration_list"
137
138   local_dmg="$(mktemp -q -u /tmp/EraAgentOnlineInstaller.dmg.XXXXXXXX)"
139   echo "Downloading installer image '$eraa_installer_url':"
140
141   eraa_http_proxy_value=""
142   if test -n "$eraa_http_proxy_value"
143   then
144     export use_proxy=yes
145     export http_proxy="$eraa_http_proxy_value"
146     (curl --connect-timeout 300 --insecure -o "$local_dmg" "$eraa_installer_url" || curl --connect-timeout 300 --noproxy
       "*" --insecure -o "$local_dmg" "$eraa_installer_url") && echo "$local_dmg" >> "$files2del"
147   else
148     curl --connect-timeout 300 --insecure -o "$local_dmg" "$eraa_installer_url" && echo "$local_dmg" >> "$files2del"
149   fi
150
151   os_version=$(system_profiler SPSoftwareDataType | grep "System Version" | awk '{print $6}' | sed
      "s:.[[:digit:]]*.$::g")
152   if test "10.7" = "$os_version"
153   then
154     local_sha1="$(mktemp -q -u /tmp/EraAgentOnlineInstaller.sha1.XXXXXXXX)"
155     echo "$eraa_installer_checksum  $local_dmg" > "$local_sha1" && echo "$local_sha1" >> "$files2del"
156     /bin/echo -n "Checking integrity of of downloaded package " && shasum -c "$local_sha1"
157   else
158     /bin/echo -n "Checking integrity of of downloaded package " && echo "$eraa_installer_checksum  $local_dmg" | shasum
      -c
159   fi
160
161   local_mount="$(mktemp -q -d /tmp/EraAgentOnlineInstaller.mount.XXXXXXXX)" && echo "$local_mount" | tee "$dirs2del" >>
      "$dirs2umount"
162   echo "Mounting image '$local_dmg':" && sudo -S hdiutil attach "$local_dmg" -mountpoint "$local_mount" -nobrowse
```

```
117             break
118           fi
119         fi
120       fi
121   done < "$local_migration_list"
122
123   local_dmg="/path/to/local/agent-macosx-i386.dmg"
124
125   local_mount="$(mktemp -q -d /tmp/EraAgentOnlineInstaller.mount.XXXXXXXX)" && echo "$local_mount" | tee "$dirs2del" >> "$dirs2umount"
126   echo "Mounting image '$local_dmg':" && sudo -S hdiutil attach "$local_dmg" -mountpoint "$local_mount" -nobrowse
```

4. Uložte súbor.

Linux

1. Otvorte skript `ESMCAgentOnlineInstaller.sh` v textovom editore.
2. Vymažte riadky 27 a 28.

```
26  eraa_product_uuid=""
27  eraa_installer_url="
    http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.5.417.0/agent-linux-i386.sh"
28  eraa_installer_checksum="ff606fd0e4fb5f5de88bebf722667f85a0516ff5"
29  eraa_initial_sg_token=
    "MDAwMDAwMDAtMDAwMC0wMDAwLTcwMDEtMDAwMDAwMDAwMDAxw6ZurvQmQbeHPN8jAJdWSn9cBGxaDkK8oriZj/dFXrkzoPm
    YLFYVeHqFV+R7fHvFBA0Mkw=="
```

3. Vložte nasledujúci riadok, ktorý obsahuje cesty k vášmu lokálnemu `i386` inštalátoru.

```
26  eraa_product_uuid=""
27  eraa_initial_sg_token=
    "MDAwMDAwMDAtMDAwMC0wMDAwLTcwMDEtMDAwMDAwMDAwMDAxw6ZurvQmQbeHPN8jAJdWSn9cBGxaDkK8oriZj/dFXrkzoPm
    YLFYVeHqFV+R7fHvFBA0Mkw=="
28  local installer="/path/to/local/agent-linux-i386.sh"
29  arch=$(uname -m)
```

4. Nahraďte riadky 34 – 41 cestou k svojmu lokálnemu `x86_64` inštalátoru. Pozrite si zvýraznenú časť na obrázku. Použite vlastnú URL adresu (lokálny zdieľaný priečinok), nie tú, ktorá je zobrazená na obrázku.

```
31  arch=$(uname -m)
32  if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)
33  then
34      eraa_installer_url="
        http://repository.eset.com/v1/com/eset/apps/business/era/agent/v6/6.5.417.0/agent-linux-x86_
        64.sh"
35      eraa_installer_checksum="e9b2f43f0fad23100eb0b5ea5c3ba6e14240aaae"
36  fi
37
38  if test -z $eraa_installer_url
39  then
40    echo "No installer available for '$arch' arhitecture. Sorry :/"
41    exit 1
42  fi
43
44  local_cert_path="$(mktemp -q -u)"
45  echo $eraa_peer_cert_b64 | base64 -d > "$local_cert_path" && echo "$local_cert_path" >>
    "$cleanup_file"
```

```
30  if $(echo "$arch" | grep -E "^(x86_64|amd64)$" 2>&1 >> /dev/null)
31  then
32  local installer="/path/to/local/agent-linux-x86_64.sh"
33  fi
34
35  local_cert_path="$(mktemp -q -u)"
36  echo $eraa_peer_cert_b64 | base64 -d > "$local_cert_path" && echo "$local_cert_path" >>
    "$cleanup_file"
37
38  if test -n "$eraa_ca_cert_b64"
39  then
40    local_ca_path="$(mktemp -q -u)"
41    echo $eraa_ca_cert_b64 | base64 -d > "$local_ca_path" && echo "$local_ca_path" >>
      "$cleanup_file"
42  fi
```

5. Vymažte riadky 53 – 65.

```
47  if test -n "$eraa_ca_cert_b64"
48  then
49    local_ca_path="$(mktemp -q -u)"
50    echo $eraa_ca_cert_b64 | base64 -d > "$local_ca_path" && echo "$local_ca_path" >>
      "$cleanup_file"
51  fi
52
53  local_installer="$(mktemp -q -u)"
54
55  eraa_http_proxy_value=""
56  if test -n "$eraa_http_proxy_value"
57  then
58    export use_proxy=yes
59    export http_proxy="$eraa_http_proxy_value"
60    (wget --connect-timeout 300 --no-check-certificate -O "$local_installer"
      "$eraa_installer_url" || wget --connect-timeout 300 --no-proxy --no-check-certificate -O
      "$local_installer" "$eraa_installer_url" || curl --connect-timeout 300 -k
      "$eraa_installer_url" > "$local_installer") && echo "$local_installer" >> "$cleanup_file"
61  else
62    (wget --connect-timeout 300 --no-check-certificate -O "$local_installer"
      "$eraa_installer_url" || curl --connect-timeout 300 -k "$eraa_installer_url" >
      "$local_installer") && echo "$local_installer" >> "$cleanup_file"
63  fi
64
65  echo -n "Checking integrity of installer script " && echo "$eraa_installer_checksum
    $local_installer" | sha1sum -c
```

6. Uložte súbor.

3.1.2.1.3 Stiahnutie agenta z webovej stránky spoločnosti ESET

Stiahnite si inštalačný balík ESET Management Agenta z webovej stránky spoločnosti ESET. Zvoľte inštalačný balík podľa operačného systému klientskeho počítača, na ktorý chcete nainštalovať agenta:

- Linux (serverom asistovaná inštalácia a offline inštalácia)
- macOS
- Windows
  - Serverom asistovaná inštalácia – pri použití inštalačného balíka agenta sa v priebehu inštalácie certifikáty stiahnu z ESMC Servera automaticky (odporúčaná metóda pre lokálne nasadenie).

> **Poznámka:**
> Ak chcete, aby serverom asistovanú inštaláciu agenta mohol vykonať iný používateľ, musia byť nastavené nasledujúce povolenia:
>
> - Používateľ musí mať pridelené povolenie na použitie certifikačnej autority, ktorá podpísala partnerský certifikát servera, a taktiež mať povolenie na použitie aspoň jedného partnerského certifikátu. Ak žiadny takýto certifikát ešte vytvorený nebol, používateľ bude potrebovať povolenie na zápis, aby mohol vytvoriť nový certifikát.
> - Povolenie na **zápis** pre statickú skupinu, do ktorej chce používateľ pridať počítač.

  - Offline inštalácia – použitím inštalačného balíka agenta. Certifikáty je potrebné manuálne vyexportovať a následne použiť pri tejto metóde nasadenia.

Ak sa počas inštalácie ESET Management Agenta vyskytnú problémy, prezrite si protokol stavu na klientskom zariadení a skontrolujte, či ESET Management Agent pracuje správne. V prípade problémov s agentom (napríklad ak sa nepripája na ESMC Server) si pozrite kapitolu Riešenie problémov – nasadenie agenta.

> **Poznámka:**
> Pomocou protokolu stavu (umiestnený v *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html alebo C:\Documents and Settings\All Users\Application Data\Eset\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.hmtl)* môžete na klientskom počítači skontrolovať, či ESET Management Agent pracuje správne. V prípade problémov s agentom (napríklad ak sa nepripája na ESMC Server) si pozrite kapitolu Riešenie problémov – nasadenie agenta.

3.1.2.2 Vzdialené nasadenie agenta

Sú dostupné dva spôsoby vzdialeného nasadenia:

- Group Policy Object (GPO) a Software Center Configuration Manager (SCCM) – túto metódu odporúčame používať pri hromadnom nasadení ESET Management Agenta na klientske počítače.
- Úloha pre server Nasadenie agentov – alternatíva k metódam GPO a SCCM.
- Deployment Tool – tento nástroj slúži na nasadenie all-in-one inštalačných balíkov vytvorených cez ESMC Web Console.

Dôležité:
Vzdialené nasadenie agenta je možné len na klientskych počítačoch, ktoré sú pripojené na internet.

Povolenia na vzdialené nasadenie agenta

Ak chcete používateľovi povoliť vytvárať GPO inštalátory a SCCM skripty, nastavte pre daného používateľa povolenia podľa nášho príkladu.

V rámci používania úlohy pre server „Nasadenie agentov“ je nevyhnutné používateľovi prideliť nasledujúce povolenia:

- povolenie na **zápis** v rámci skupín a počítačov, na ktorých má prebehnúť nasadenie (kategória povolení **Skupiny a počítače**),
- povolenie na **použitie** certifikátov (kategória povolení **Certifikáty**) s prístupom k statickej skupine, kde sa nachádzajú certifikáty,
- povolenie na **použitie** úlohy pre server **Nasadenie agentov** (v rámci kategórie povolení **Úlohy a spúšťače servera**).

3.1.2.2.1 Nasadenie agenta pomocou GPO a SCCM

Okrem lokálneho nasadenia a vzdialeného nasadenia pomocou úlohy pre server môžete použiť aj nástroje na správu, ako napr. Group Policy Object (GPO), Software Center Configuration Manager (SCCM), Symantec Altiris alebo Puppet.

Pre nasadenie ESET Management Agenta na klientske počítače prostredníctvom GPO alebo SCCM postupujte podľa nasledujúcich krokov:

Stiahnite si inštalátor ESET Management Agenta v podobe súboru `.msi` z webovej stránky spoločnosti ESET.

Kliknite na možnosť **Iné možnosti nasadenia** v časti **Rýchle odkazy** na paneli s ponukami. Zobrazí sa kontextové okno, kde budete mať možnosť **Pre nasadenie použiť GPO alebo SCCM**. Kliknite na možnosť **Vytvoriť skript**.

Certifikát

Ak nesúhlasíte so zasielaním správ o zlyhaní programu a telemetrických údajov spoločnosti ESET, zrušte označenie možnosti **Zúčastnite sa programu zlepšovania produktov**. Ak ponecháte túto možnosť označenú, telemetrické údaje a správy o zlyhaní programu budú odosielané spoločnosti ESET.

Partnerský certifikát a certifikačná autorita ESMC sú zvolené automaticky podľa dostupných certifikátov. Ak chcete použiť iný certifikát ako ten, ktorý bol zvolený automaticky, kliknite na popis pre **ESMC Certifikát**. Zobrazí sa zoznam dostupných certifikátov, z ktorého vyberte certifikát, ktorý chcete používať. Ak chcete používať **Vlastný certifikát**, kliknite na prepínacie tlačidlo a odovzdajte certifikačný súbor `.pfx`. Viac informácií nájdete v časti Vlastné certifikáty pre ESMC.

V prípade potreby zadajte **Prístupovú frázu certifikátu**. Prístupovú frázu certifikátu zadajte v prípade, ak ste ju špecifikovali počas inštalácie svojho ESMC alebo používate vlastný certifikát s prístupovou frázou certifikátu. V opačnom prípade ponechajte pole **Prístupová fráza certifikátu** prázdne.

Rozšírené

Môžete si prispôsobiť inštalačný balík ESET Management Agenta:

- Pre inštalačný balík vyplňte polia **Názov** a **Popis** (voliteľné).
- **Nadradená skupina (voliteľná)** – môžete buď vybrať existujúcu statickú skupinu, alebo vytvoriť novú. Kliknite na **Vybrať** a vyberte nadradenú statickú skupinu pre klientsky počítač, na ktorom použijete all-in-one balík inštalátora. Ak chcete vytvoriť novú nadradenú statickú skupinu, kliknite na tlačidlo **Nová statická skupina** a použite sprievodcu. Novovytvorená skupina bude automaticky zvolená.
- **Počiatočná konfigurácia inštalátora** – môžete si vybrať z dvoch typov konfigurácie:
  - **Nekonfigurovať** – budú aplikované iba politiky, ktoré sú zlúčené s nadradenou statickou skupinou.
  - **Vybrať konfiguráciu zo zoznamu politík** – túto možnosť použite, ak chcete aplikovať konfiguračnú politiku na ESET Management Agenta. Kliknite na **Vybrať** v časti **Konfigurácia agenta (voliteľná)** a vyberte si zo zoznamu dostupných politík. Ak vám nevyhovuje žiadna z preddefinovaných politík, môžete vytvoriť novú politiku alebo najprv upraviť už existujúce politiky.
- V prípade potreby môžete upresniť **Názov hostiteľa ESMC Servera (voliteľné)** a číslo **Portu**. V opačnom prípade predvolené hodnoty nemeňte.

Kliknite na **Dokončiť** a keď sa otvorí okno so súborom `install_config.ini`, vyberte možnosť **Uložiť súbor**.

Ak chcete, aby bola komunikácia ESET Management Agenta preposielaná na ESMC Server pomocou proxy, pridajte nasledujúce parametre do súboru `install_config.ini`:

```
P_USE_PROXY=1
P_PROXY_HTTP_HOSTNAME=
P_PROXY_HTTP_PORT=
P_PROXY_HTTP_USERNAME=
P_PROXY_HTTP_PASSWORD=
```

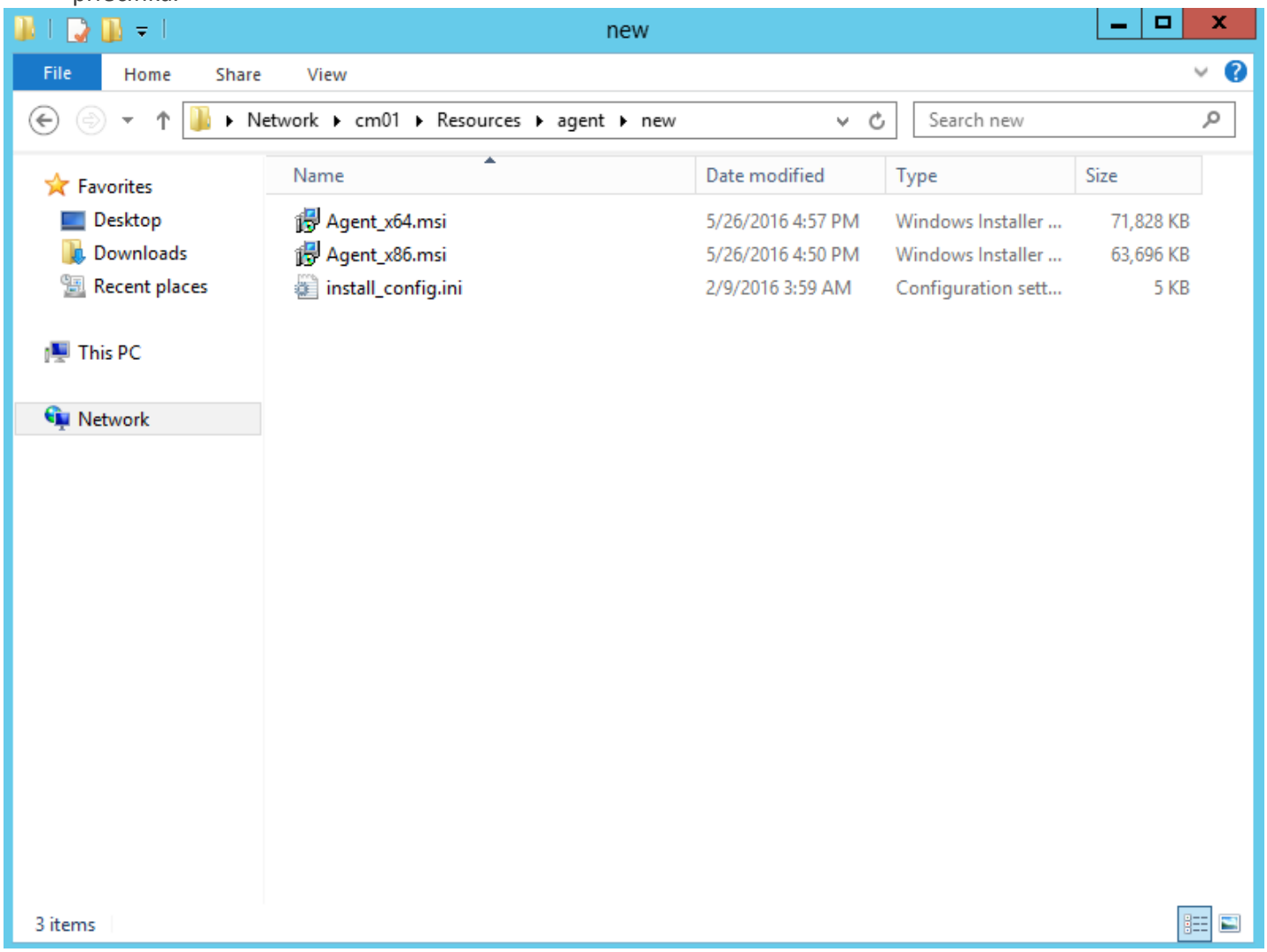
Kliknutím na príslušný odkaz nižšie zobrazíte postup pre dve populárne metódy nasadenia ESET Management Agenta:

1. Postup nasadenia ESET Management Agenta pomocou GPO
2. Postup nasadenia ESET Management Agenta pomocou SCCM

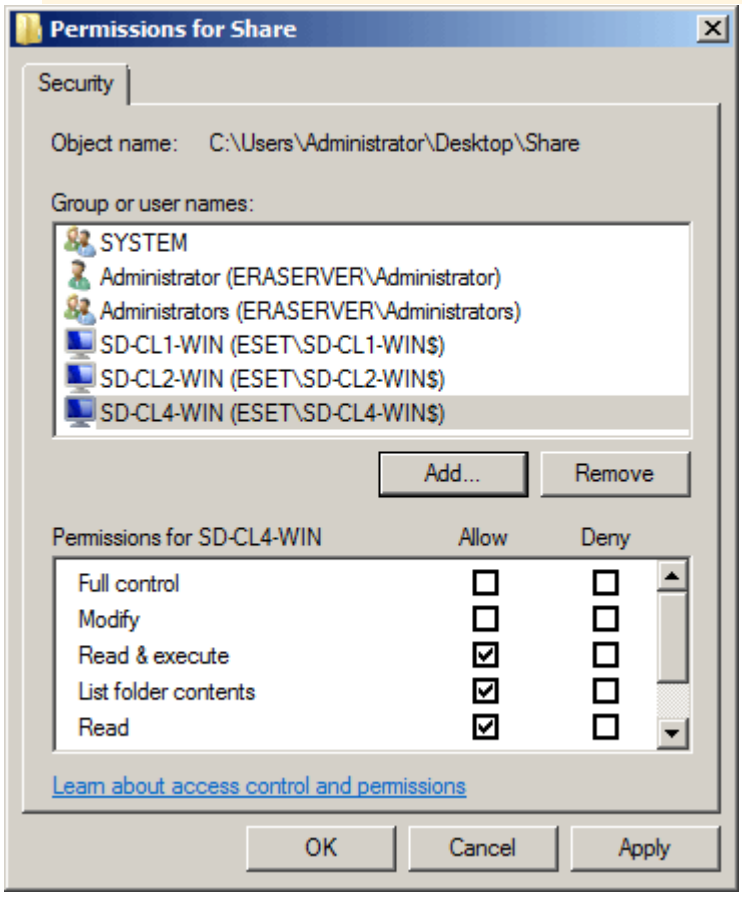
3.1.2.2.2 Nasadenie agenta prostredníctvom SCCM

Ak chcete nasadiť ESET Management Agenta pomocou SCCM, pokračujte podľa nasledujúcich krokov:

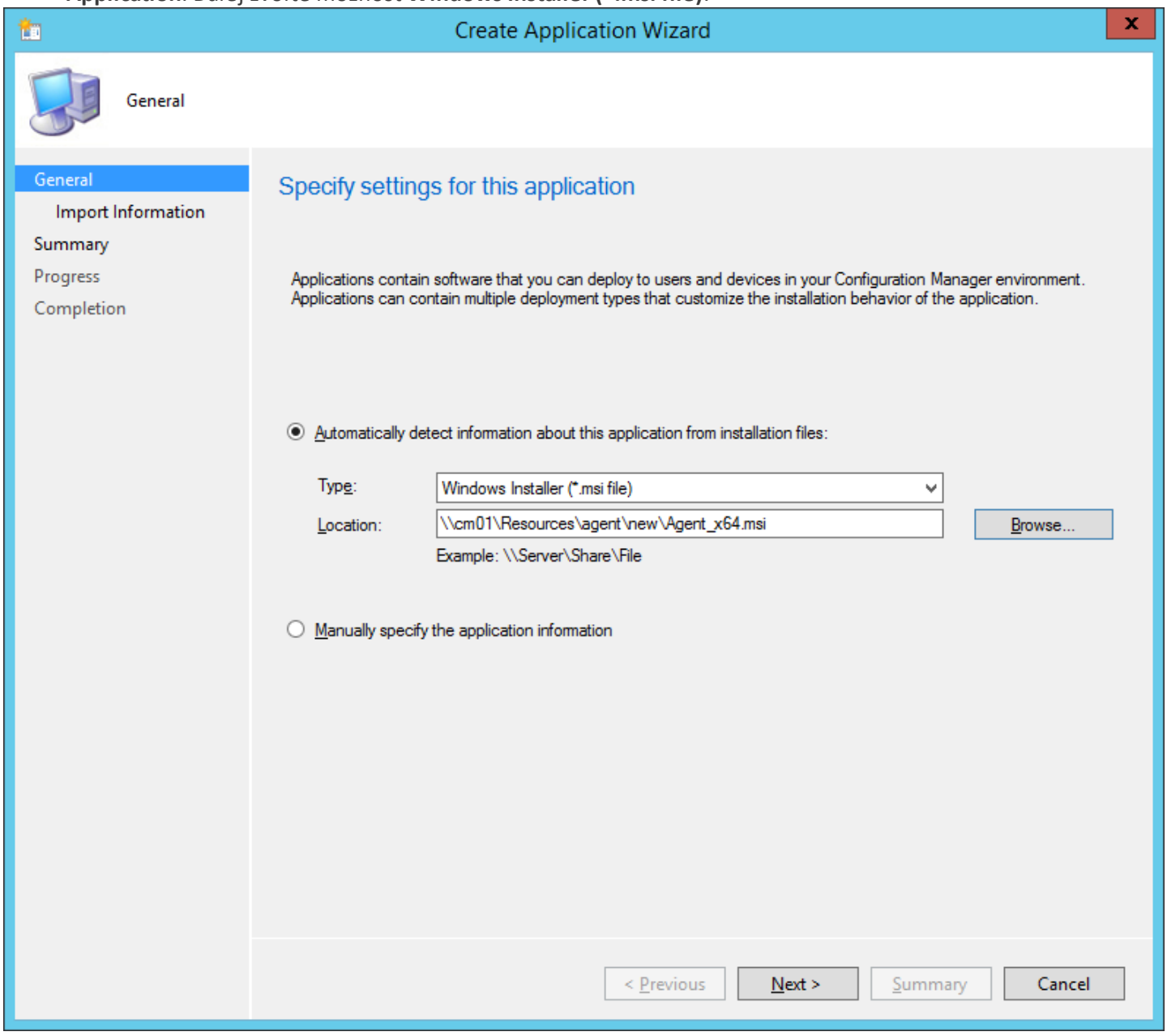
1. Umiestnite `.msi` súbory inštalátora ESET Management Agenta a súbor *install_config.ini* do zdieľaného priečinka.



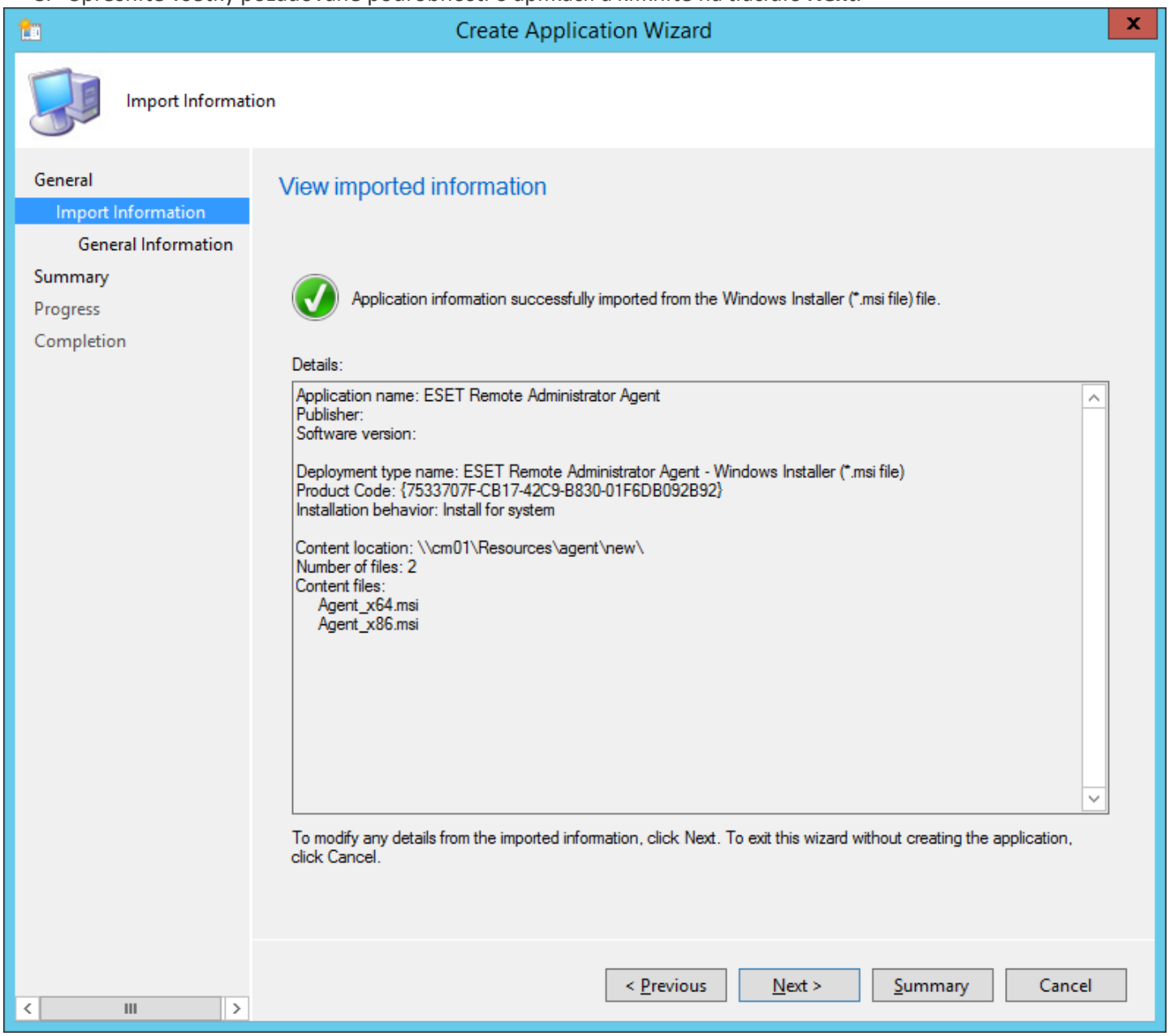
Dôležité:
Klientske počítače budú potrebovať prístup k tomuto zdieľanému priečinku s oprávneniami čítania/zapisovania.



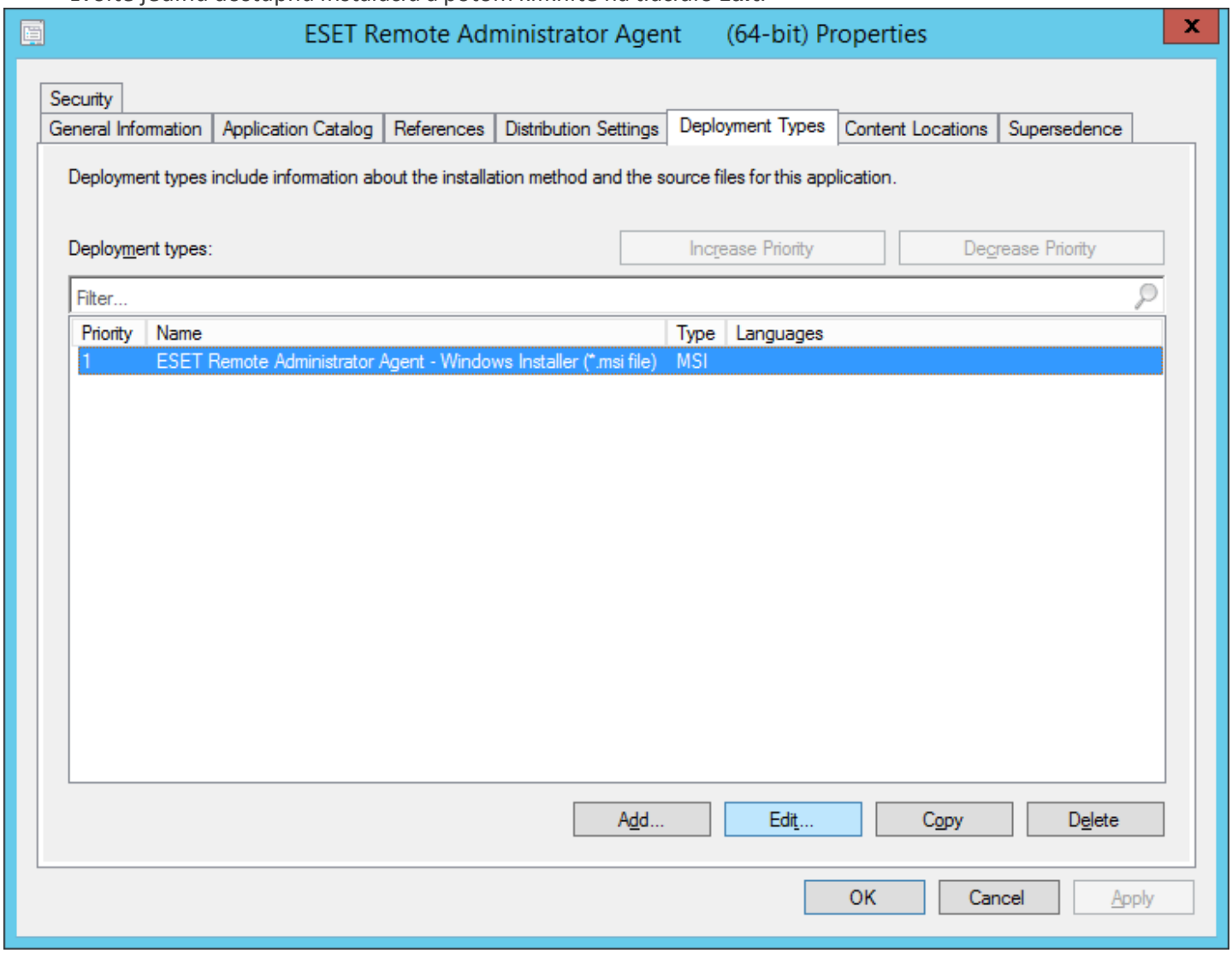
2. Otvorte SCCM (System Center Configuration Manager) konzolu a kliknite na **Software Library**. V sekcii **Application Management** kliknite pravým tlačidlom myši na **Applications** a vyberte možnosť **Create Application**. Ďalej zvoľte možnosť **Windows Installer (*.msi file)**.



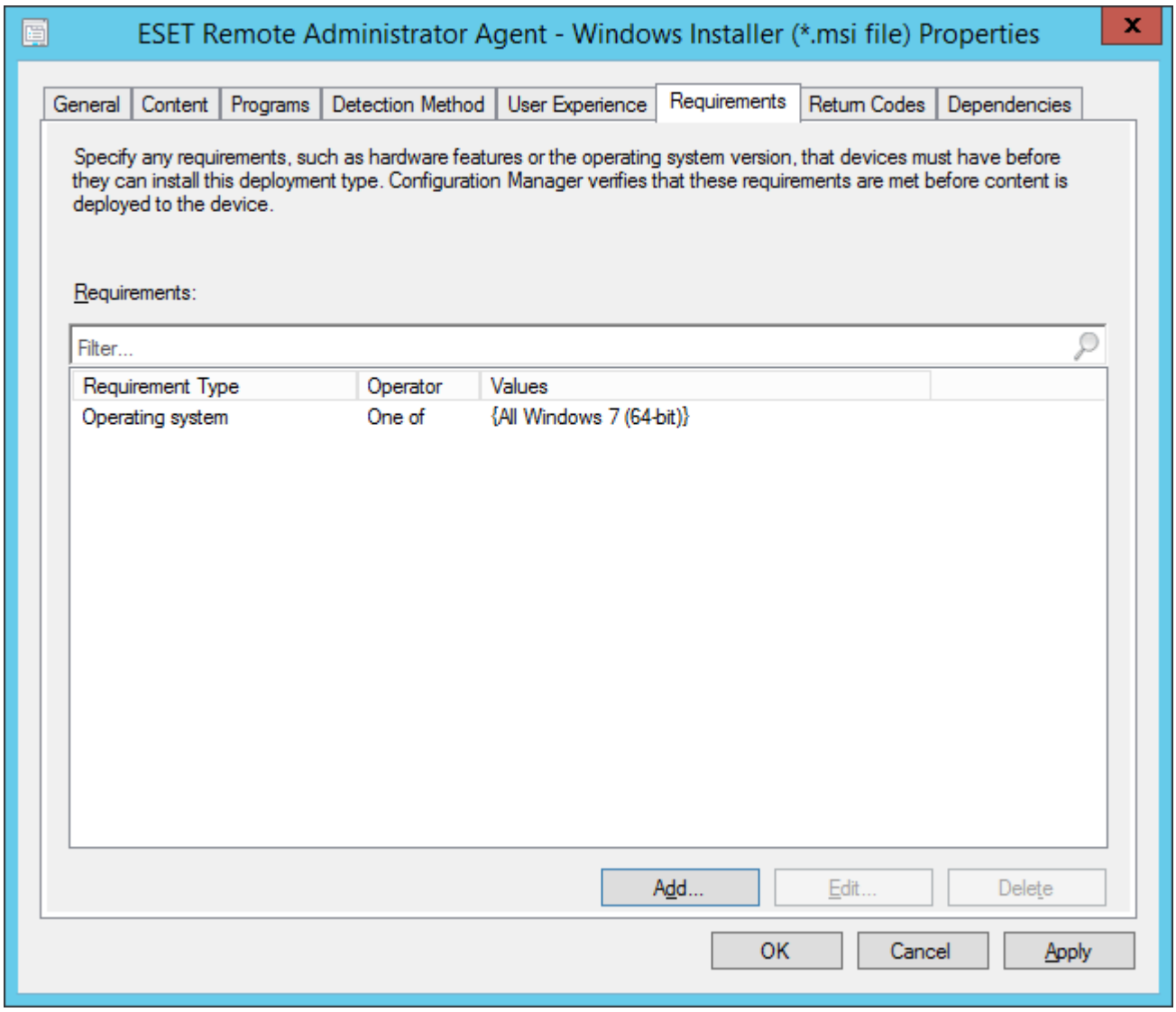
3. Upresnite všetky požadované podrobnosti o aplikácii a kliknite na tlačidlo **Next**.

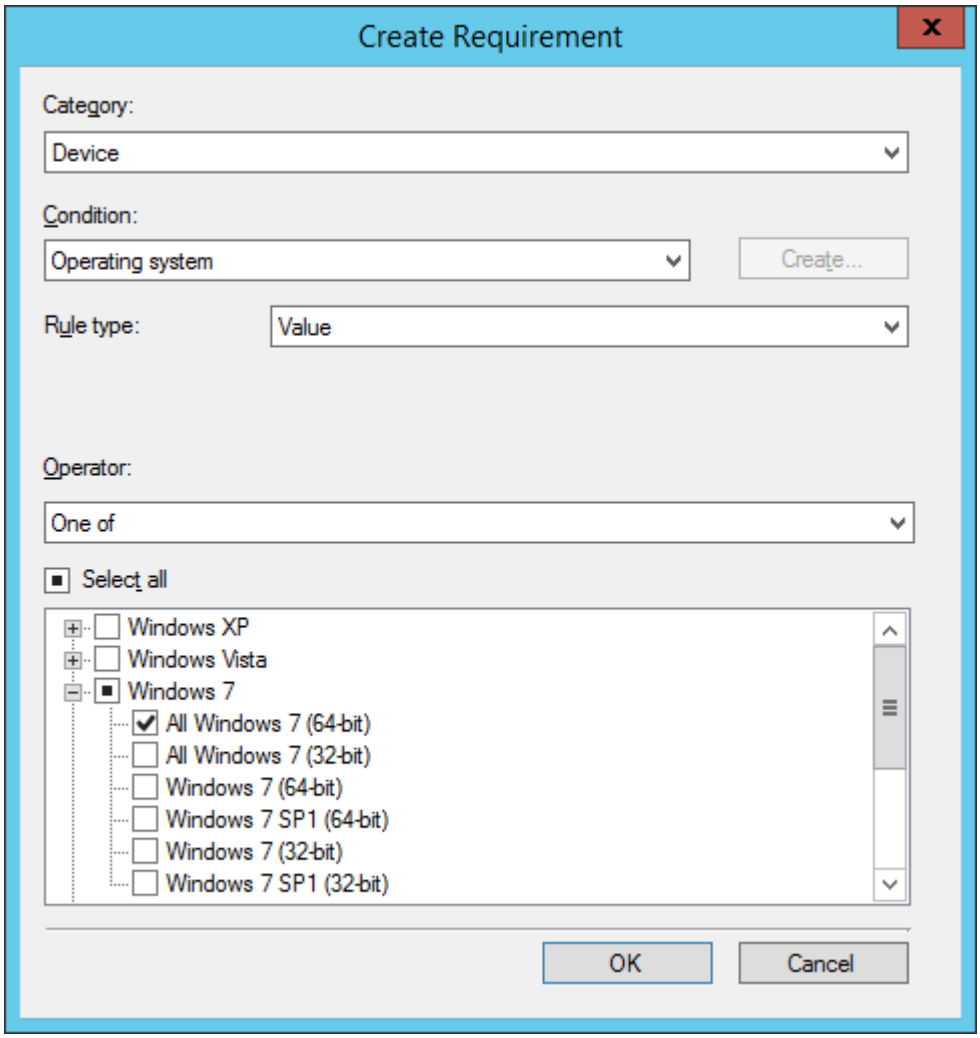


4. Pravým tlačidlom myši kliknite na aplikáciu ESET Management Agent, kliknite na kartu **Deployment Types**, zvoľte jedinú dostupnú inštaláciu a potom kliknite na tlačidlo **Edit**.

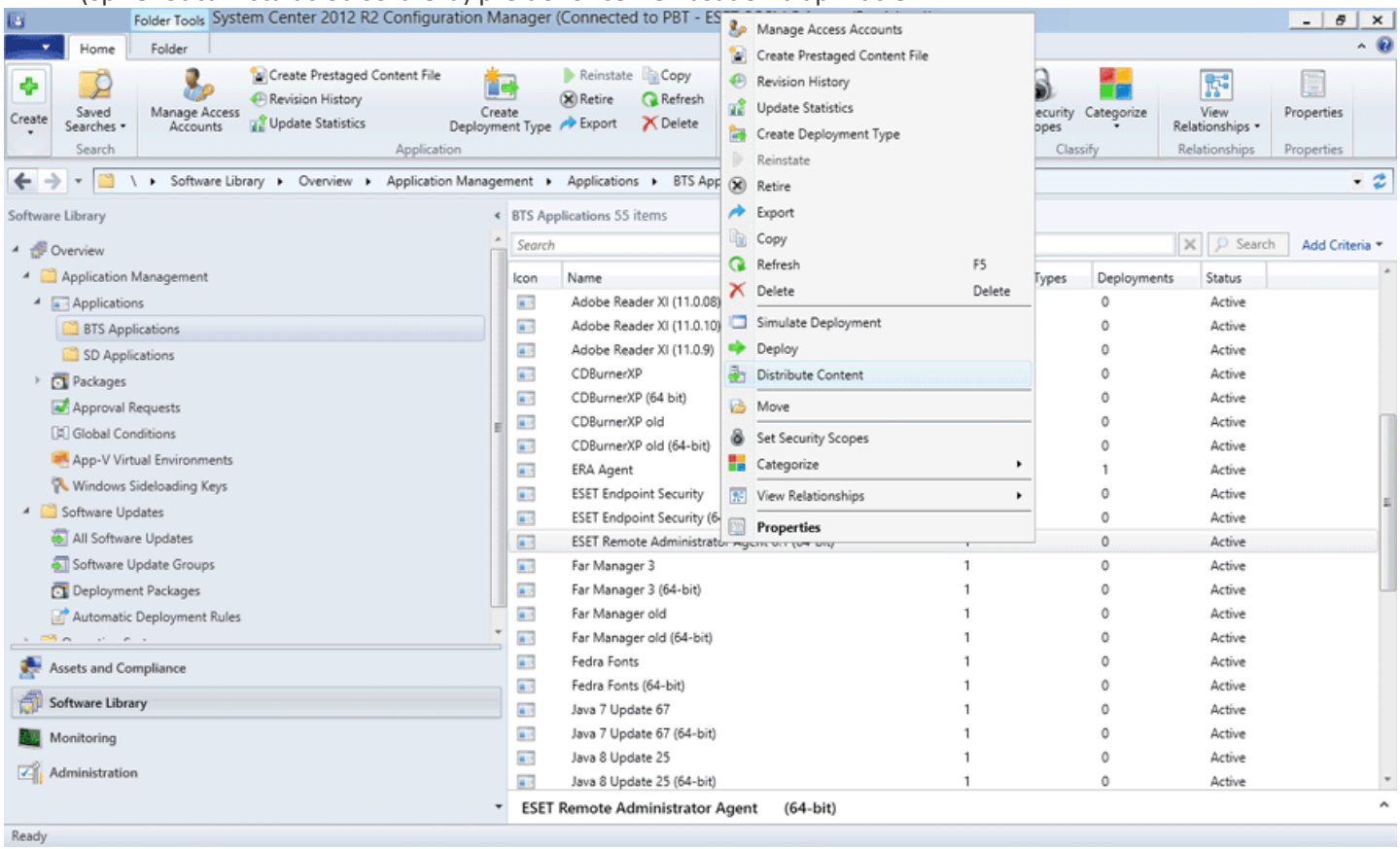


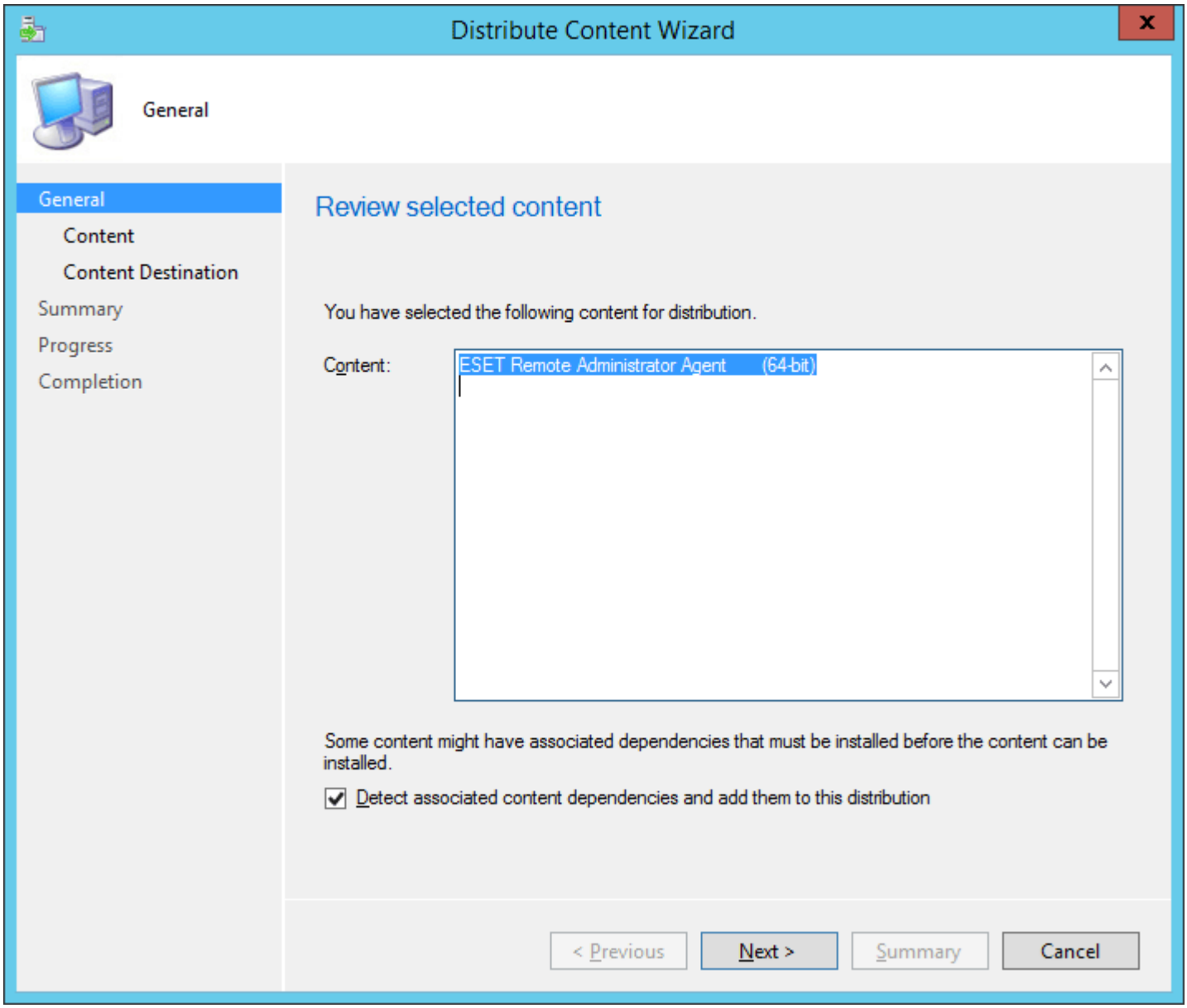
5. Kliknite na kartu **Requirements** a potom na tlačidlo **Add**. Zvoľte možnosť **Operating system** z roletového menu **Condition**, ďalej zvoľte možnosť **One of** z roletového menu **Operator** a nakoniec upresnite zoznam operačných systémov, na ktoré budete inštalovať, pomocou príslušných začiarkavacích políčok. Po dokončení tohto kroku kliknite na tlačidlo **OK** a následne kliknite na **OK** znova pre zatvorenie všetkých okien a uloženie zmien.

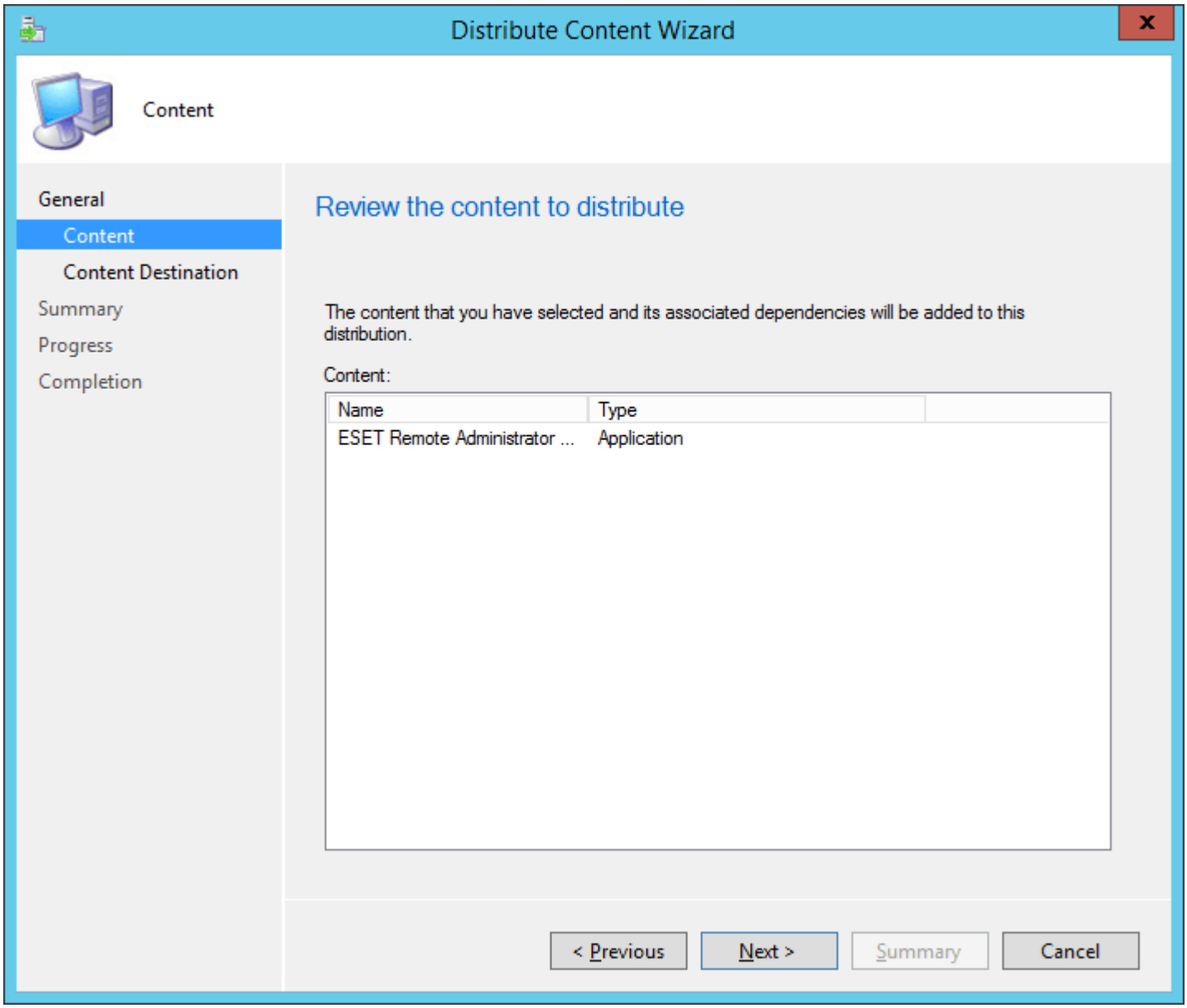




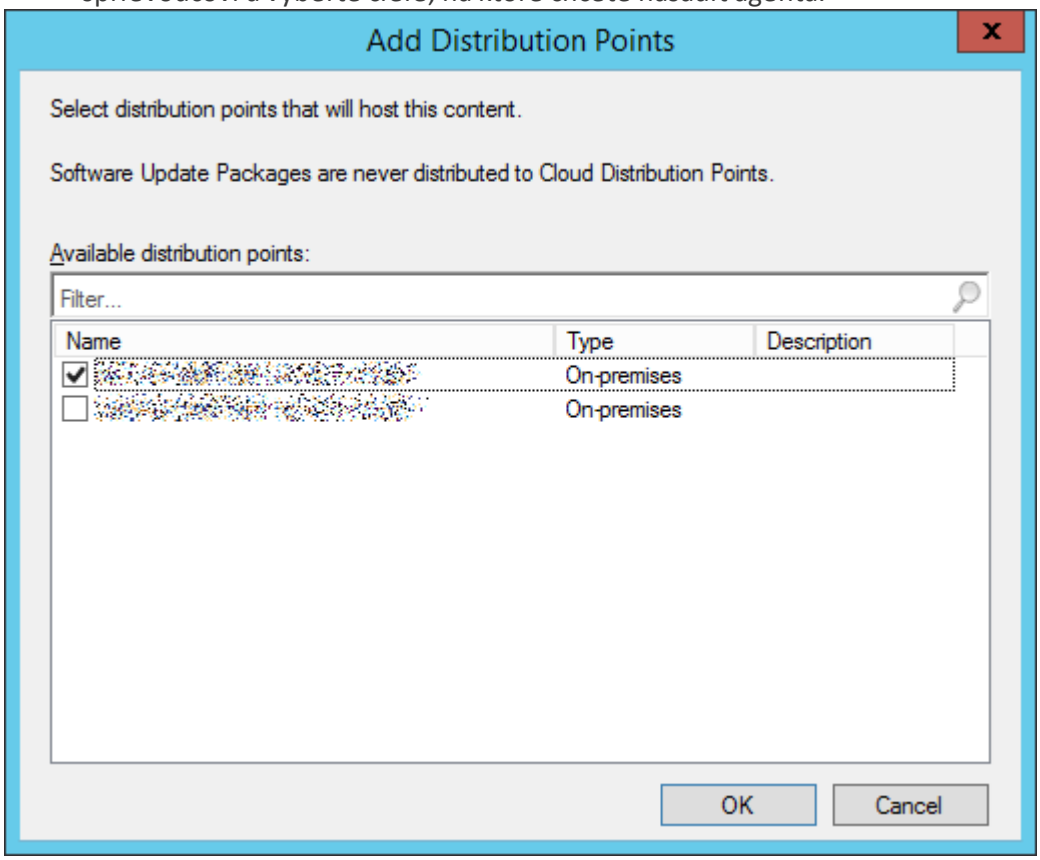
6. V „System Center Software Library“ kliknite pravým tlačidlom myši na vašu novú aplikáciu a v kontextovom menu zvoľte možnosť **Distribute Content**. Postupujte podľa inštrukcií v nástroji Deploy Software Wizard (sprievodca inštaláciou softvéru) pre dokončenie nasadenia aplikácie.

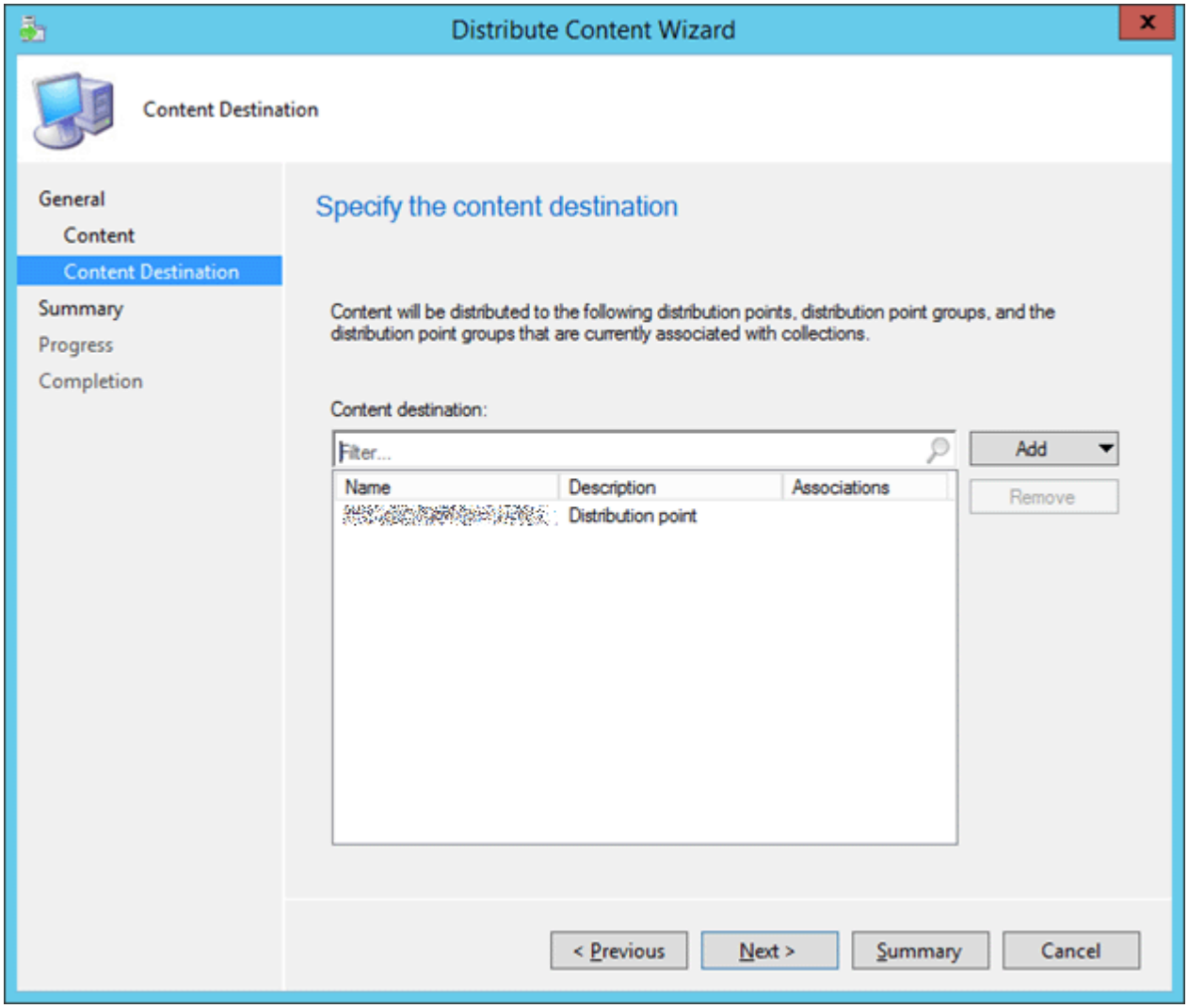


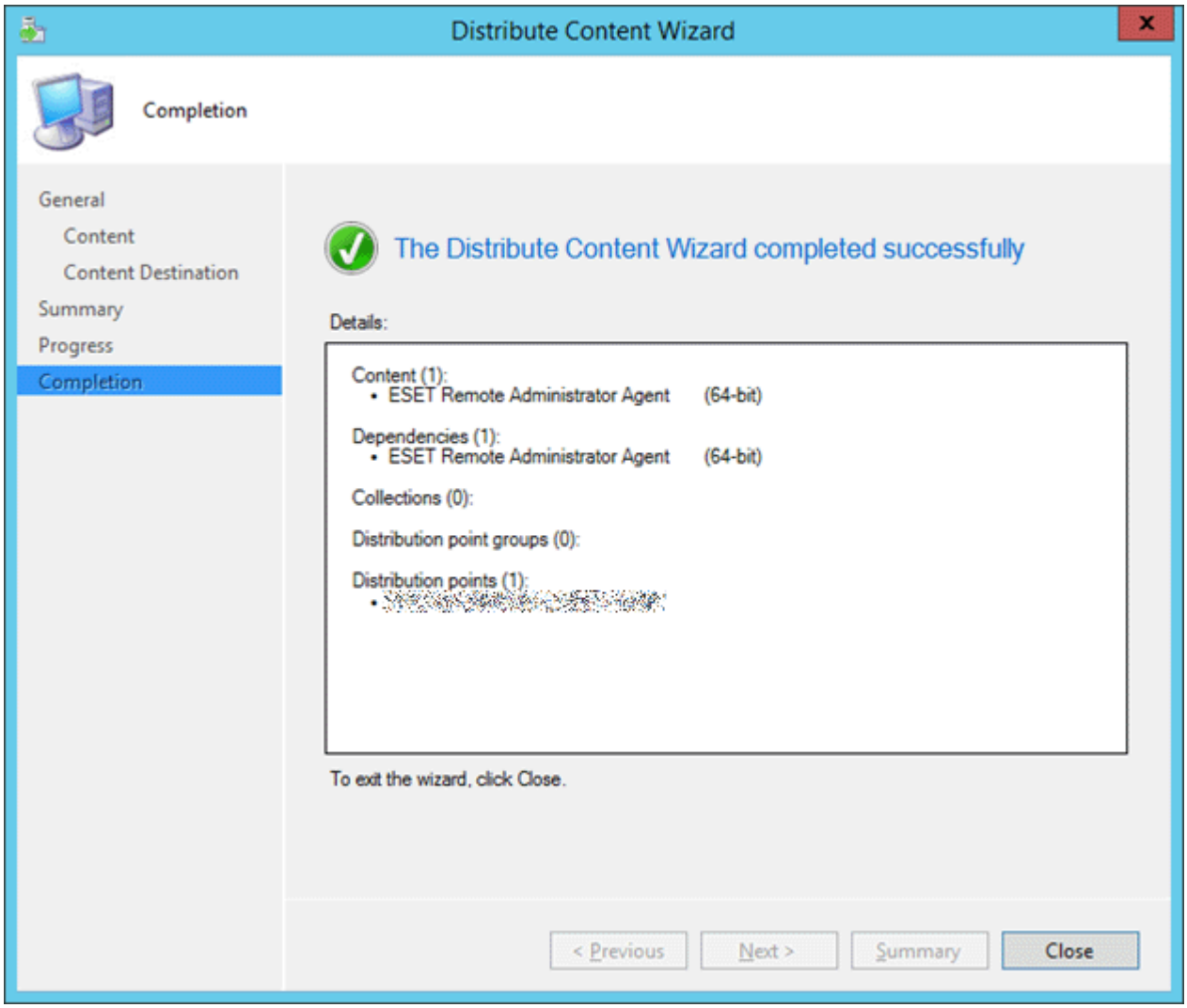

Distribute Content Wizard
General
General
Content
Content Destination
Summary
Progress
Completion
Review selected content
You have selected the following content for distribution.
Content:
ESET Remote Administrator Agent (64-bit)
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
< Previous
Next >
Summary
Cancel

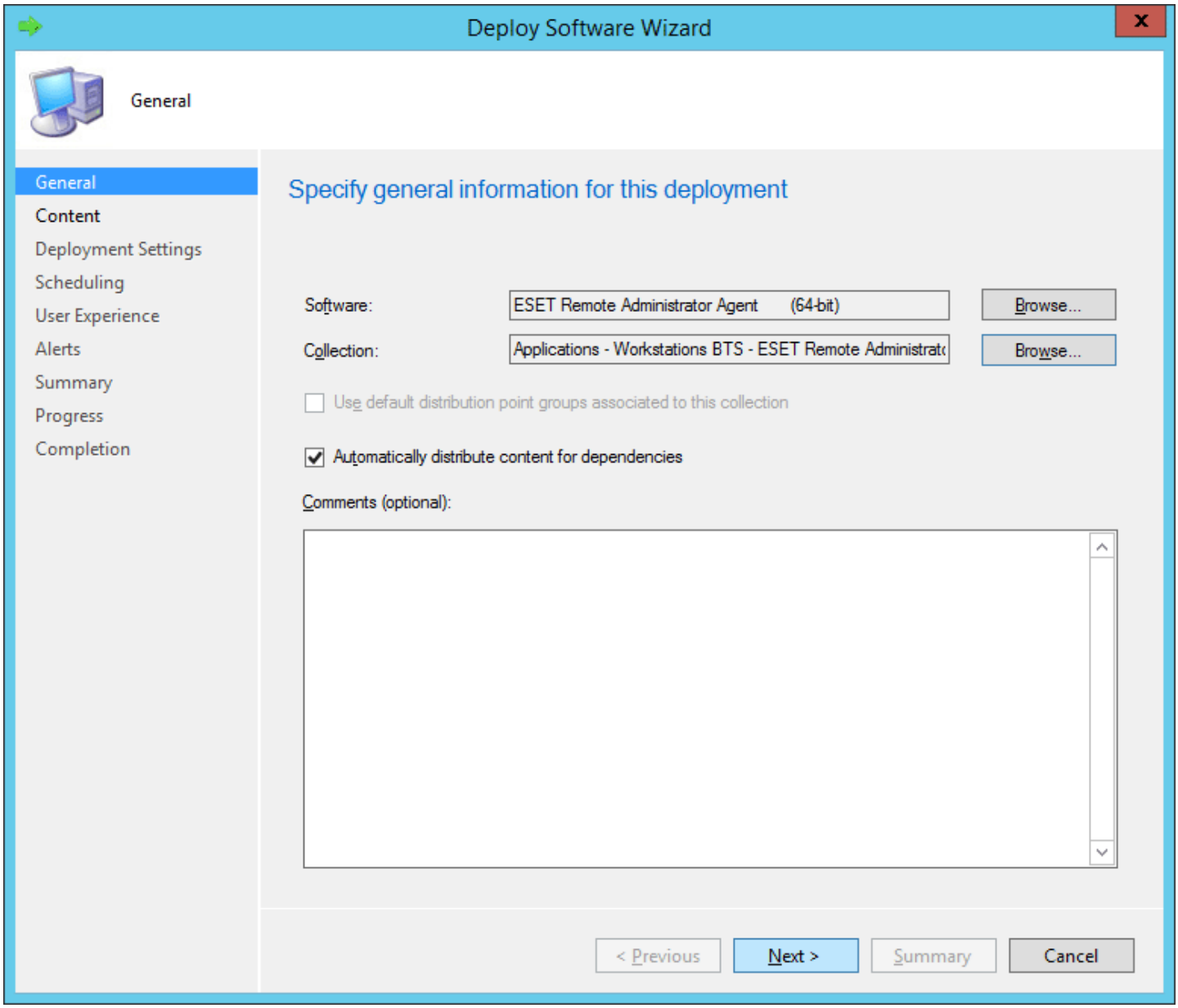

Distribute Content Wizard
Content
General
Content
Content Destination
Summary
Progress
Completion
Review the content to distribute
The content that you have selected and its associated dependencies will be added to this distribution.
Content:
Name
Type
ESET Remote Administrator ...
Application
< Previous
Next >
Summary
Cancel

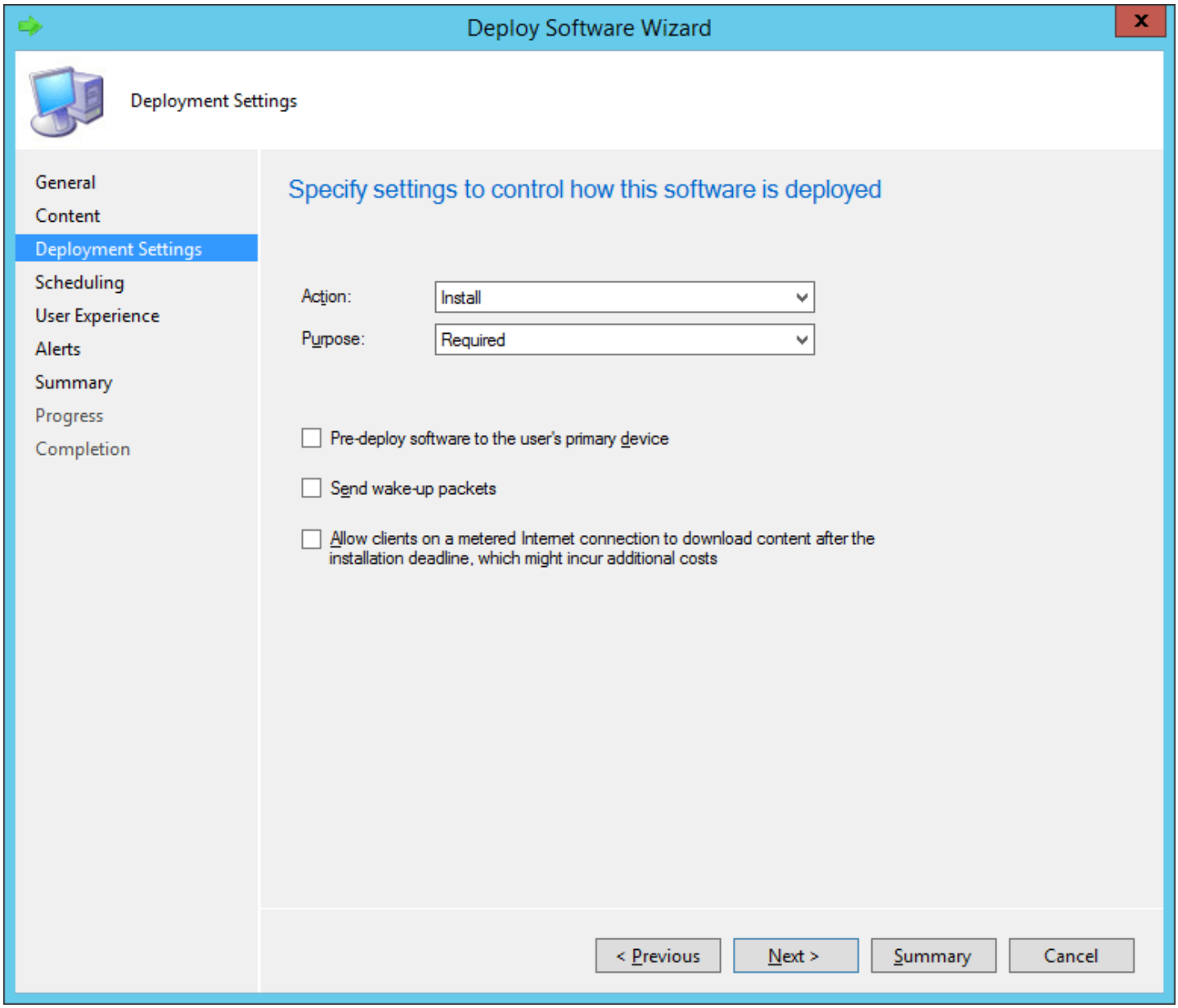
7. Pravým tlačidlom myši kliknite na aplikáciu a zvoľte možnosť **Deploy**. Postupujte podľa inštrukcií v sprievodcovi a vyberte ciele, na ktoré chcete nasadiť agenta.

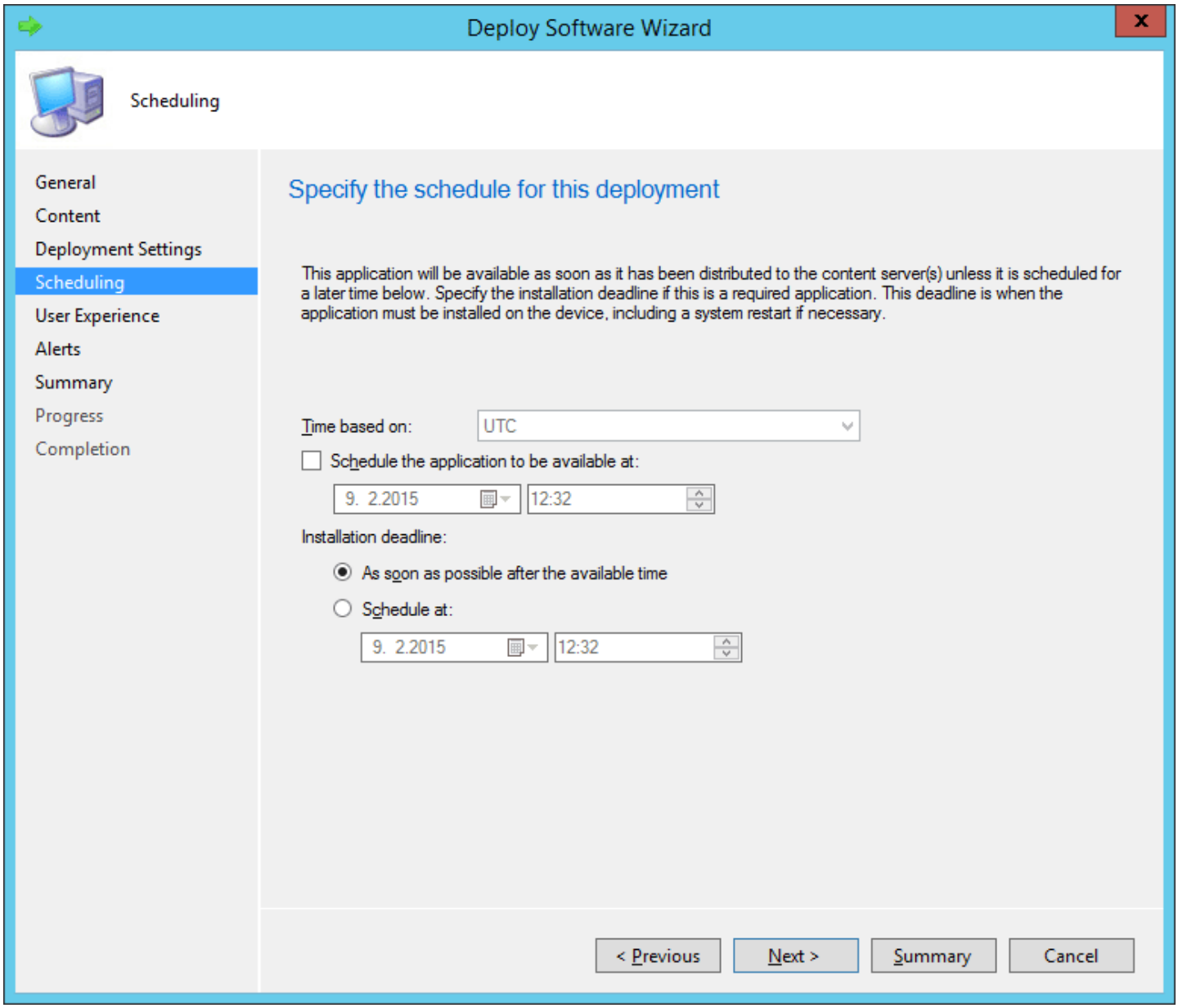


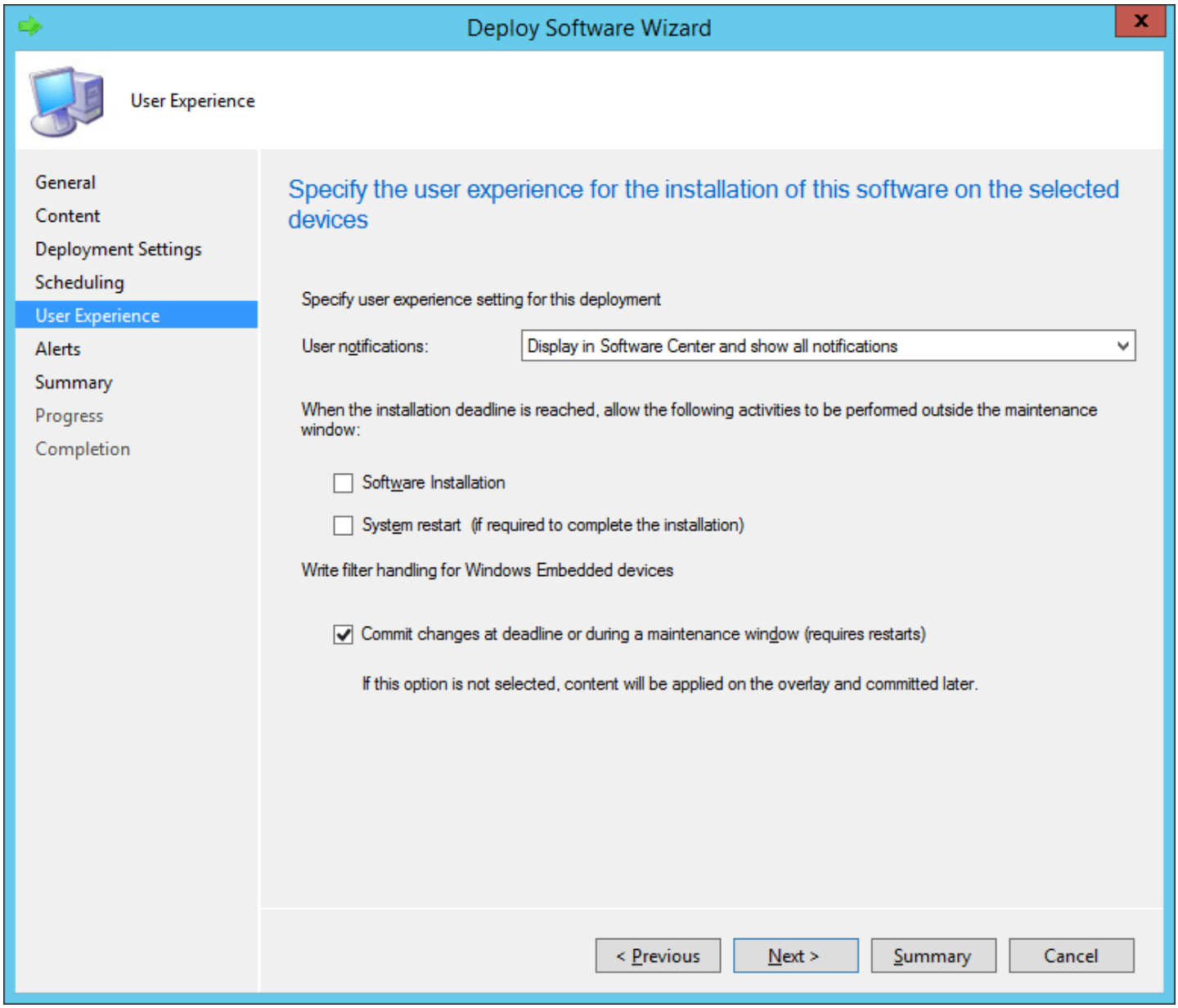


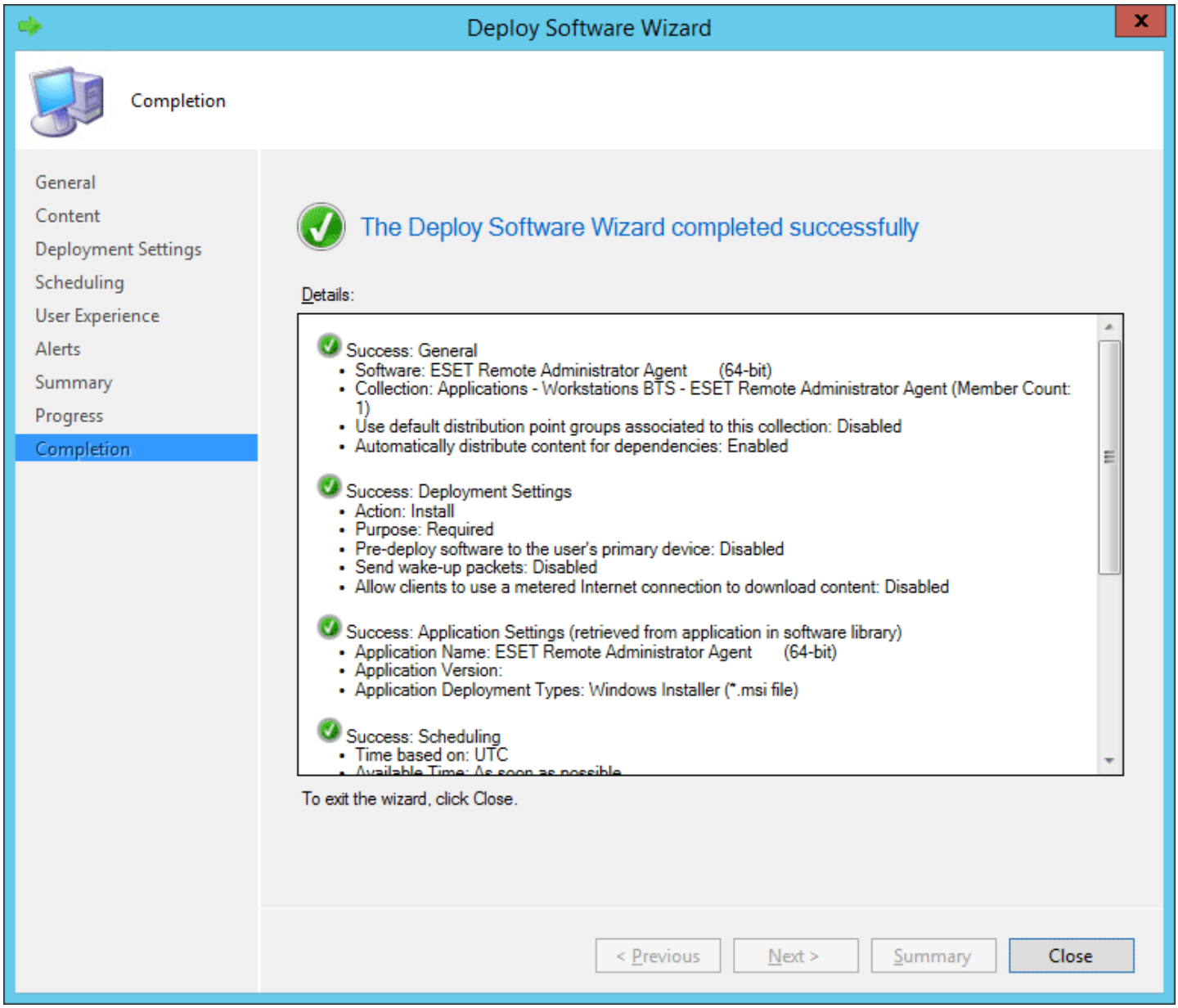

Distribute Content Wizard
Completion
General
Content
Content Destination
Summary
Progress
Completion
The Distribute Content Wizard completed successfully
Details:
Content (1):
• ESET Remote Administrator Agent (64-bit)
Dependencies (1):
• ESET Remote Administrator Agent (64-bit)
Collections (0):
Distribution point groups (0):
Distribution points (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Deploy Software Wizard
General
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Software:
ESET Remote Administrator Agent (64-bit)
Browse...
Collection:
Applications - Workstations BTS - ESET Remote Administrat
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
9. 2.2015
12:32
Installation deadline:
As soon as possible after the available time
Schedule at:
9. 2.2015
12:32
< Previous
Next >
Summary
Cancel

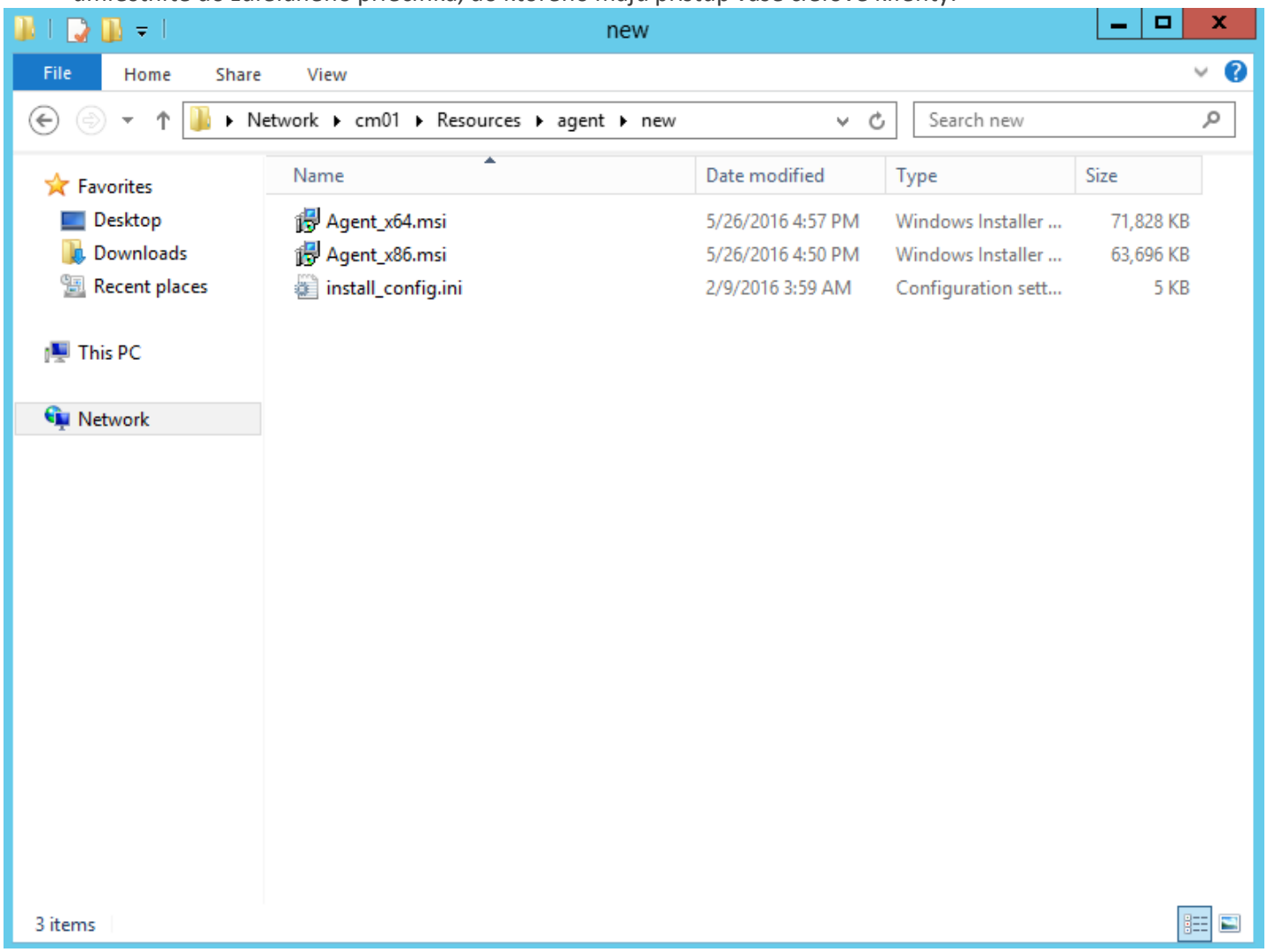

Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
Software: ESET Remote Administrator Agent (64-bit)
Collection: Applications - Workstations BTS - ESET Remote Administrator Agent (Member Count: 1)
Use default distribution point groups associated to this collection: Disabled
Automatically distribute content for dependencies: Enabled
Success: Deployment Settings
Action: Install
Purpose: Required
Pre-deploy software to the user's primary device: Disabled
Send wake-up packets: Disabled
Allow clients to use a metered Internet connection to download content: Disabled
Success: Application Settings (retrieved from application in software library)
Application Name: ESET Remote Administrator Agent (64-bit)
Application Version:
Application Deployment Types: Windows Installer (*.msi file)
Success: Scheduling
Time based on: UTC
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

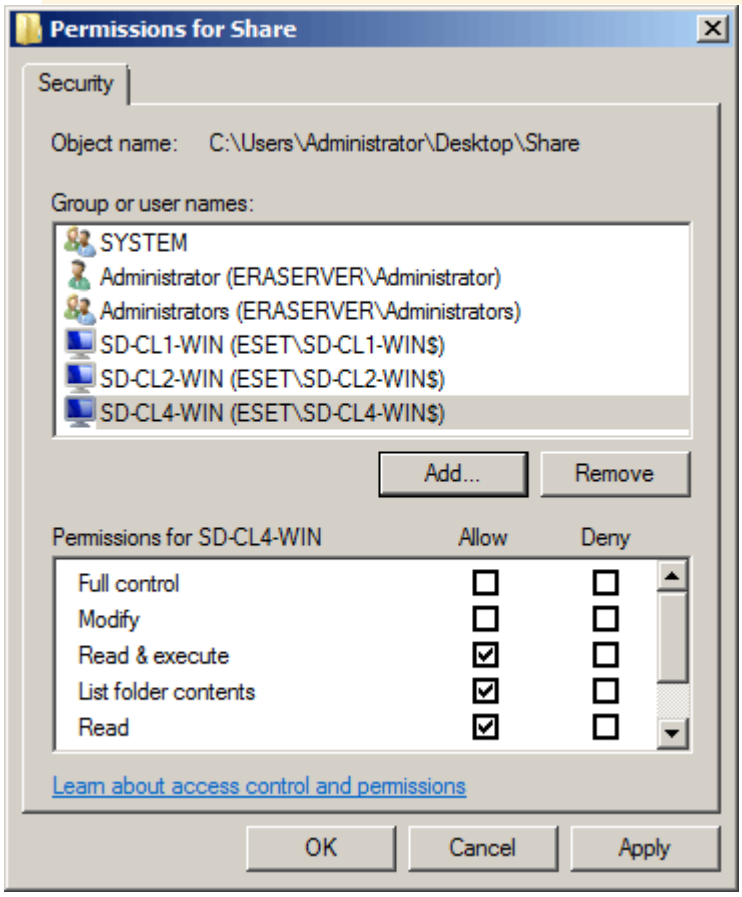
3.1.2.2.3 Nasadenie agenta prostredníctvom GPO

Ak chcete nasadiť ESET Management Agenta pomocou GPO, pokračujte podľa nasledujúcich krokov:

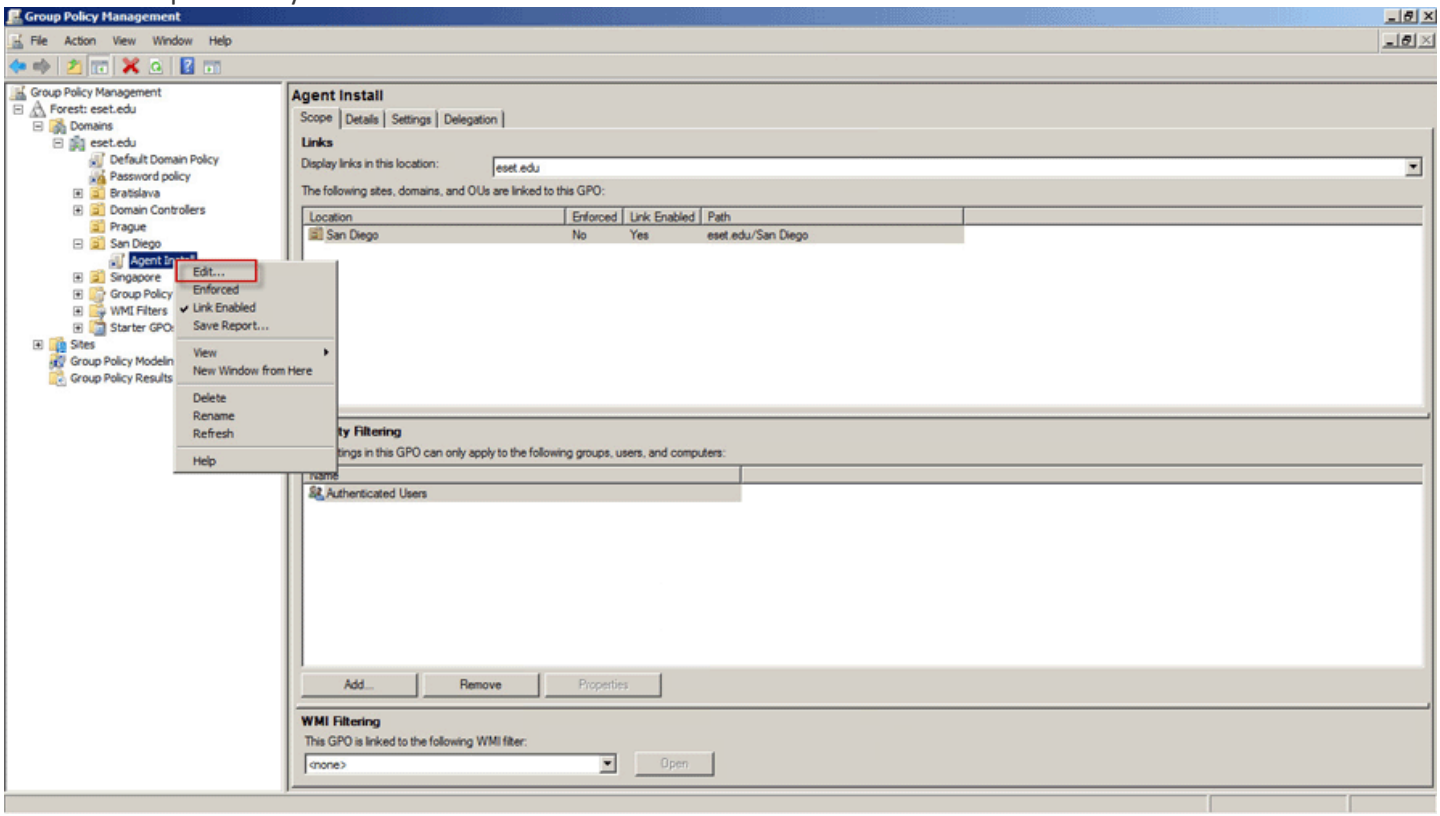
1. Inštalátor ESET Management Agenta v podobe súboru `.msi` a vytvorený súbor `install_config.ini` umiestnite do zdieľaného priečinka, do ktorého majú prístup vaše cieľové klienty.



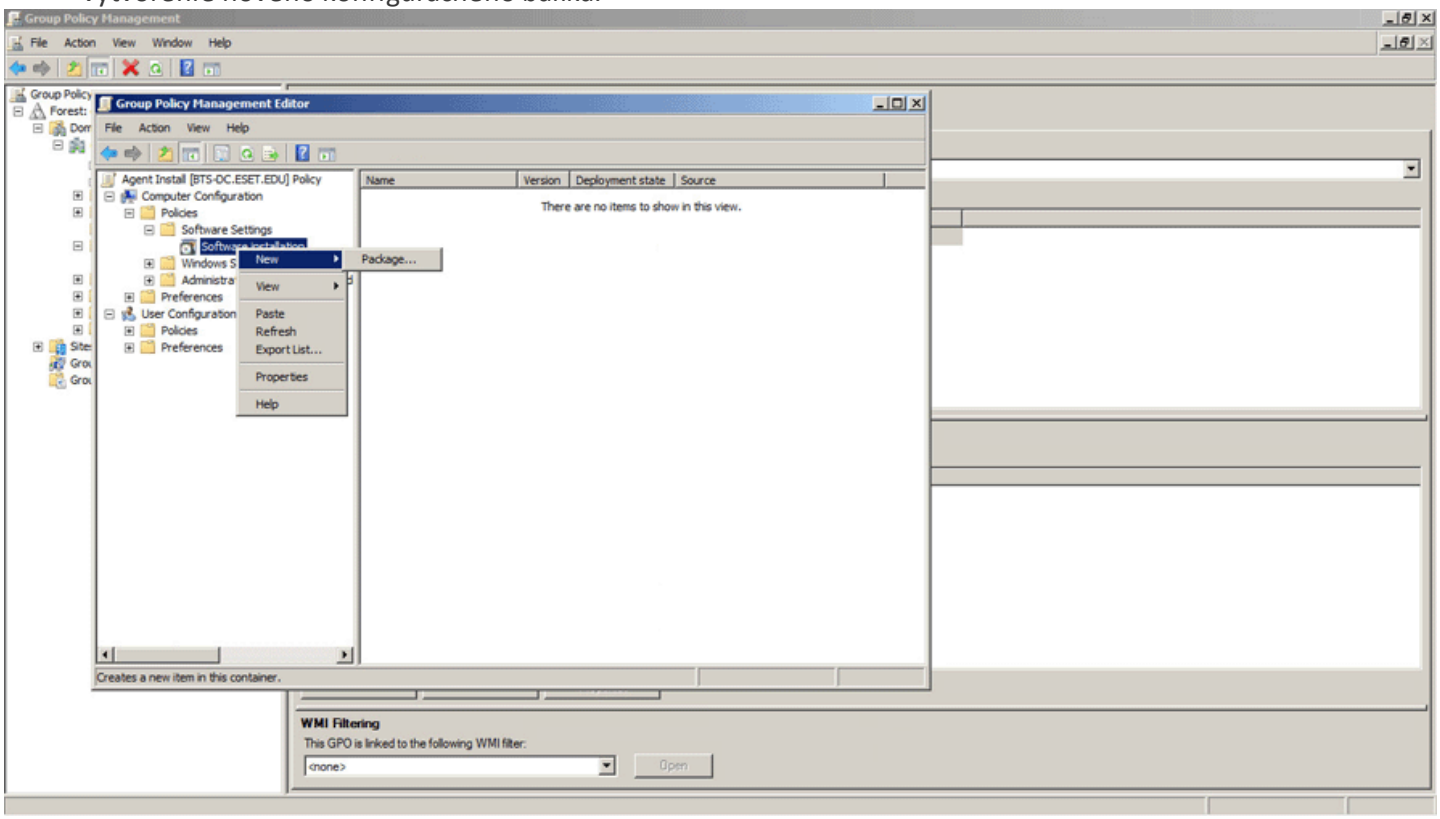
Dôležité:
Klientske počítače budú potrebovať prístup k tomuto zdieľanému priečinku s oprávneniami čítania/zapisovania.



2. Použite existujúci objekt Group Policy alebo vytvorte nový (kliknite pravým tlačidlom na GPO a kliknite na New). V strome GPMC (Group Policy Management Console) kliknite pravým tlačidlom myši na GPO, ktoré chcete použiť a vyberte možnosť Edit.

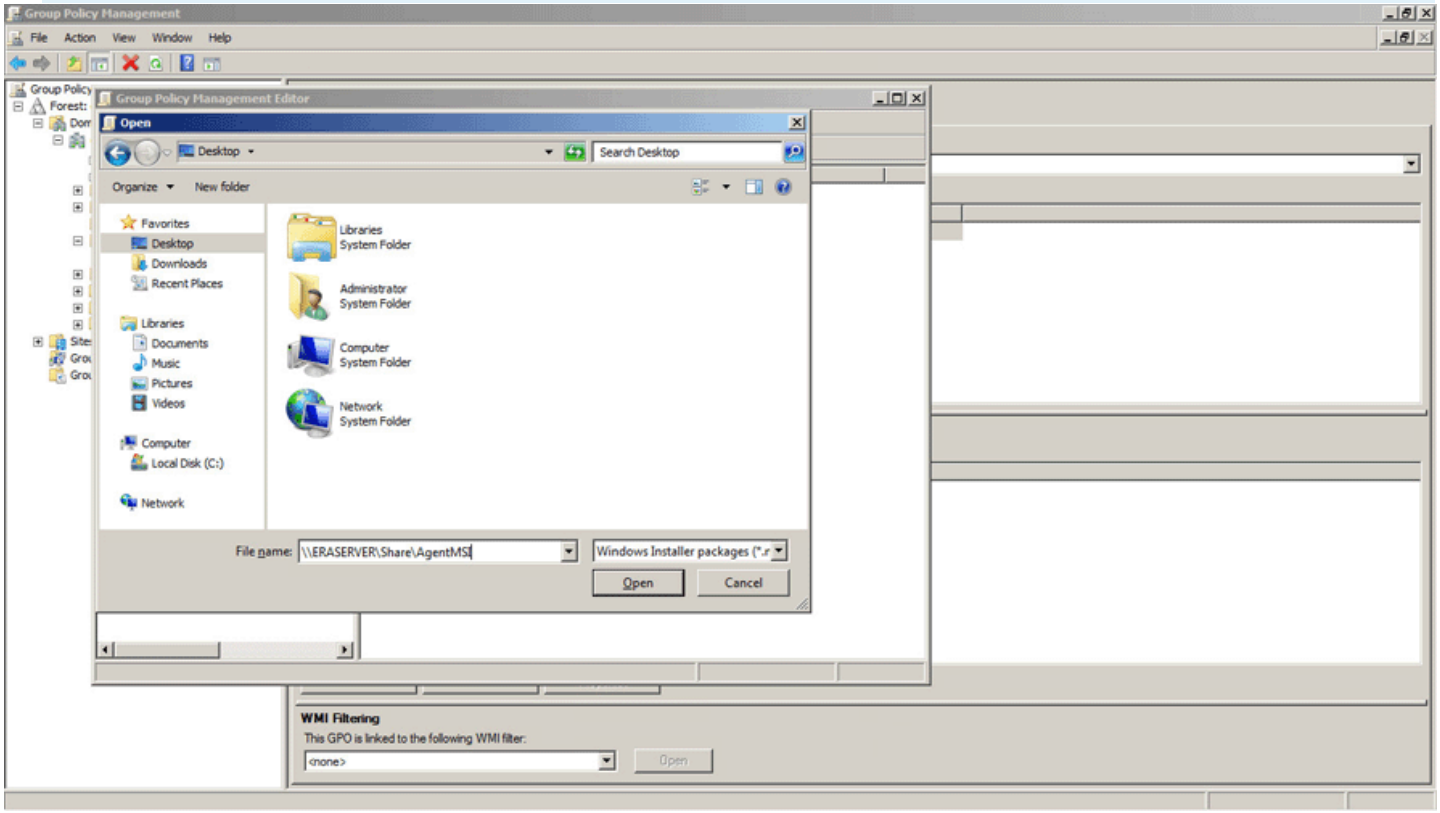


3. V časti **Computer Configuration** prejdite do vetvy **Policies** > **Software Settings**.
4. Kliknite pravým tlačidlom myši na **Software installation**, vyberte možnosť **New** a kliknite na **Package** pre vytvorenie nového konfiguračného balíka.

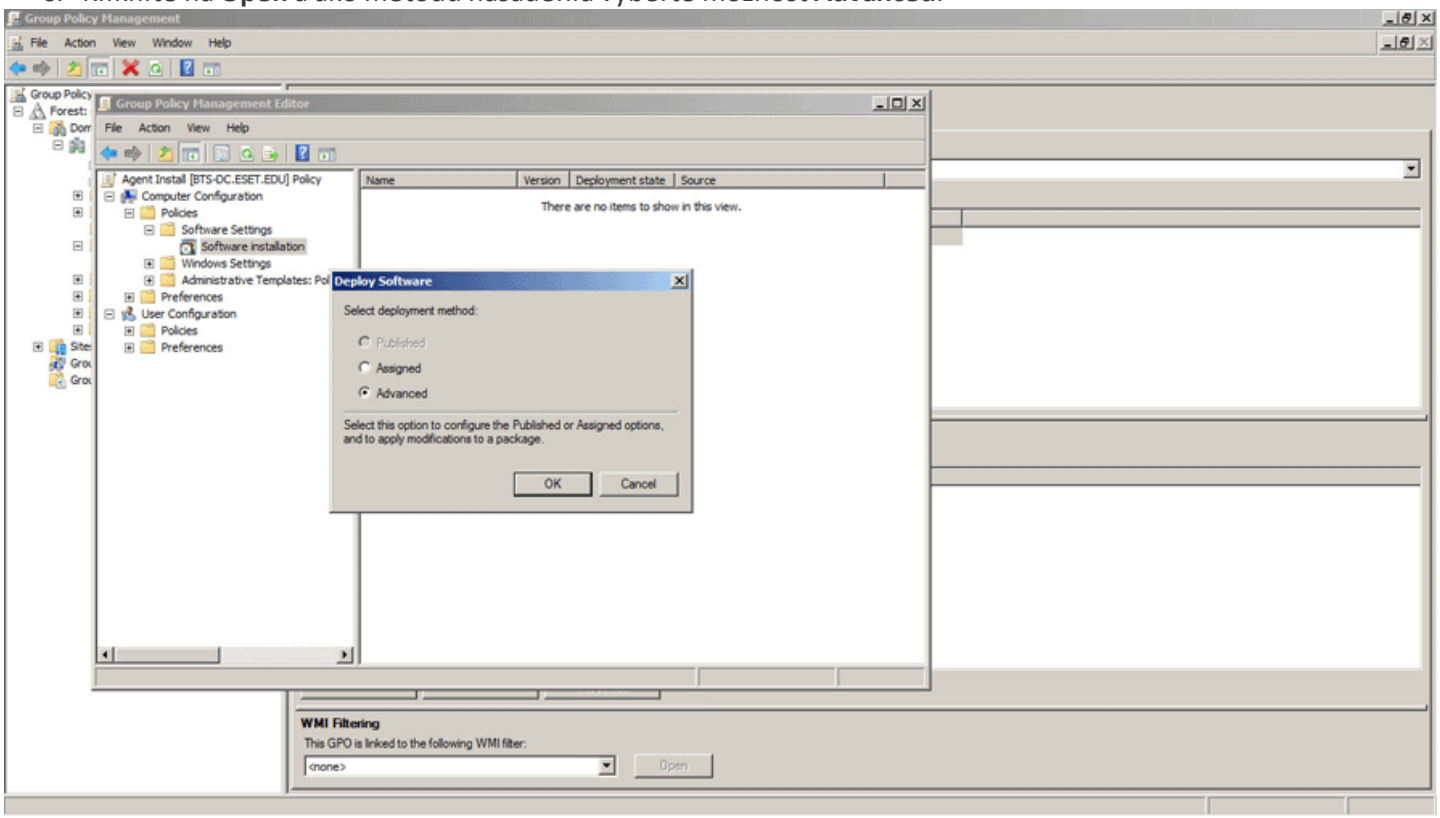


5. Vyberte cestu k `.msi` súboru ESET Management Agenta. V dialógovom okne **Open** zadajte úplnú sieťovú cestu (UNC) zdieľaného balíka inštalátora, ktorý chcete použiť. Napríklad `\\fileserver\share\filename.msi`.

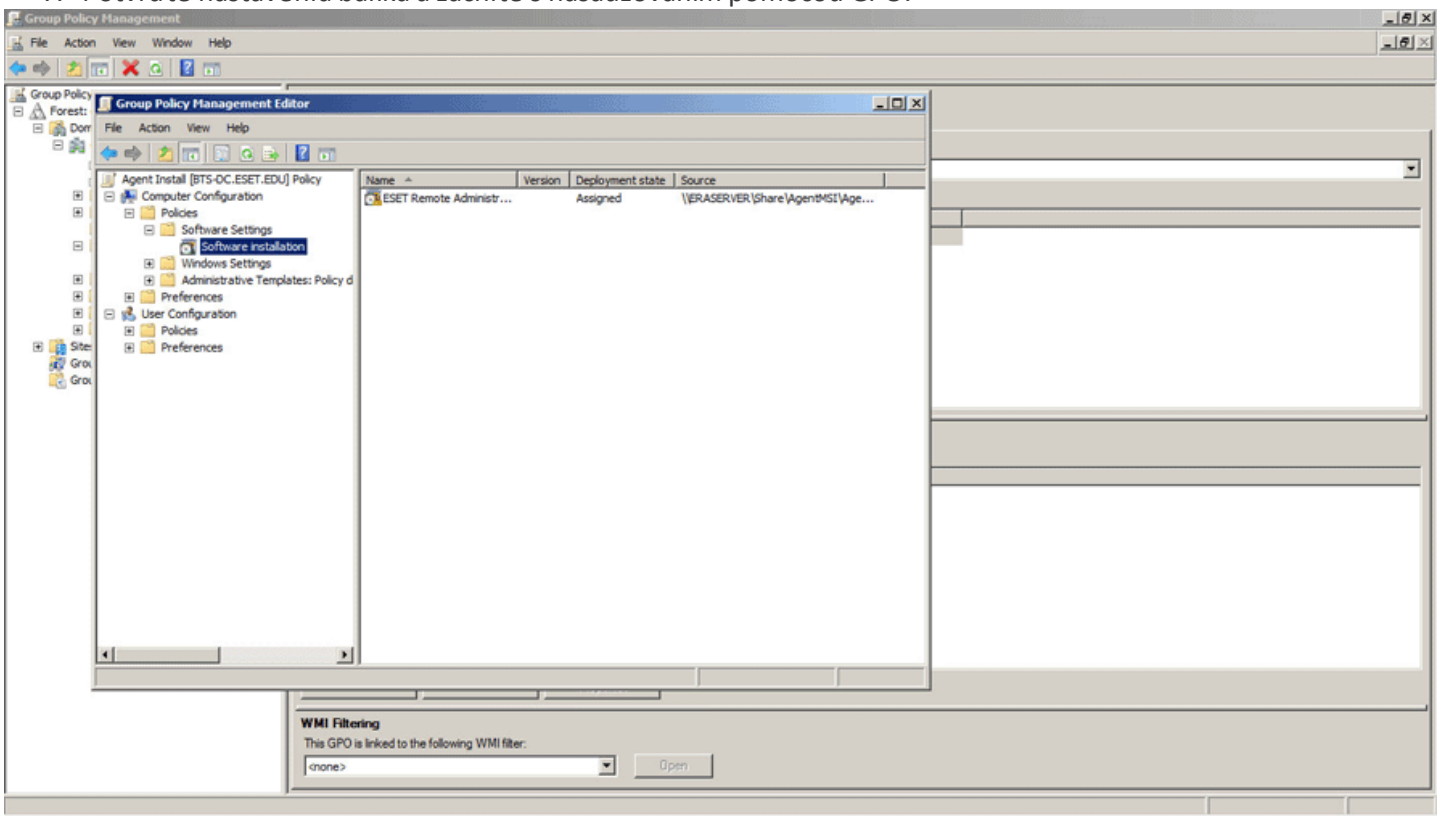
Poznámka:
Uistite sa, že ste zadali UNC cestu k zdieľanému balíku inštalátora.



6. Kliknite na **Open** a ako metódu nasadenia vyberte možnosť **Advanced**.



7. Potvrďte nastavenia balíka a začnite s nasadzovaním pomocou GPO.



3.1.2.2.4 Nástroj na nasadenie (Deployment Tool)

Nástroj na nasadenie (Deployment Tool) ponúka pohodlný spôsob distribúcie ESET Management Agenta spoločne s bezpečnostným produktom ESET na klientske počítače v sieti. Umožňuje vám tiež použiť vlastné inštalátory, ktoré ste si vytvorili. Tento nástroj si môžete zadarmo stiahnuť z webovej stránky spoločnosti ESET ako samostatný ESMC komponent. Nástroj na nasadenie je určený predovšetkým na nasadenie v malých a stredne veľkých sieťach. Je dostupný len pre operačné systémy Windows.

Viac informácií o prerekvizitách a použití nástroja nájdete v kapitole Nástroj na nasadenie v Inštalačnej príručke.

3.1.2.3 Nastavenia ESET Management Agenta

Použitím politiky môžete upraviť nastavenia ESET Management Agenta. Pre ESET Management Agenta existuje niekoľko prednastavených politík, napríklad **Pripojenie – Pripojiť každých...** (časový interval pripájania agenta k serveru) alebo **Hlásenia aplikácií – Hlásiť všetky inštalované aplikácie** (nielen aplikácie spoločnosti ESET). Postup ako vynútiť konkrétnu politiku len na určitú podsieť je uvedený v tomto príklade.

Kliknite na **Politiky** a rozbaľte sekciu **Vstavané politiky > ESET Management Agent**, kde môžete upravovať existujúce alebo vytvárať nové politiky.

Pripojenie

- **Servery pre pripojenie** – kliknite na **Upraviť zoznam serverov** pre upresnenie podrobností pripojenia na ESMC Server (názov hostiteľa/IP a číslo portu). Je možné zadať viacero ESMC Serverov. Politiku s týmto nastavením môžete využiť napríklad pri zmene IP adresy vášho ESMC Servera alebo v prípade, že vykonávate migráciu.
- **Dátový limit** – vyberte maximálny počet bajtov pre odosielanie dát.
- **Interval pripojenia** – zvoľte pravidelný interval a upresnite časovú hodnotu intervalu pripojenia na ESMC Server (prípadne použite CRON výraz).
- **Certifikát** – môžete spravovať partnerské certifikáty pre ESET Management Agenta. Kliknite na **Zmeniť certifikát** a vyberte, ktorý certifikát by mal byť používaný ESET Management Agentom. Viac informácií nájdete v kapitole Partnerské certifikáty.

Aktualizácie

- **Interval aktualizácie** – časový interval, v ktorom budú prijímané aktualizácie. Môžete zvoliť pravidelný interval a upresniť nastavenia alebo môžete použiť CRON výraz.
- **Aktualizačný server** – aktualizačný server, z ktorého bude ESMC Server sťahovať aktualizácie pre bezpečnostné produkty a komponenty ESMC.
- **Typ aktualizácie** – vyberte požadovaný typ aktualizácie. Môžete si vybrať pravidelnú, predbežnú alebo oneskorenú aktualizáciu. Neodporúčame výber predbežnej aktualizácie pre produkčné systémy, pretože to môže predstavovať bezpečnostné riziko.

Pokročilé nastavenia

- **HTTP Proxy** – môžete použiť proxy server, ktorý bude slúžiť na sprostredkovanie internetového pripojenia klientom vo vašej sieti, ako aj na komunikáciu agenta s ESMC Serverom.
  - **Typ konfigurácie proxy**
    - **Globálne proxy** – túto možnosť použite v prípade, ak chcete, aby bol na replikáciu agenta a ukladanie ESET služieb do vyrovnávacej pamäte (napr. aktualizácie) použitý rovnaký proxy server.
    - **Rôzne proxy pre každú službu** – túto možnosť použite v prípade, ak chcete, aby jeden proxy server slúžil na replikáciu agenta a druhý na ukladanie služieb ESET do vyrovnávacej pamäte (napr. aktualizácie).
  - **Globálne proxy** – táto možnosť je dostupná len v prípade, že ju vyberiete v sekcii **Typ konfigurácie proxy**. Kliknite na **Upraviť** a nastavte svoje proxy.

Dve možnosti spomenuté nižšie sú dostupné len ak vyberiete možnosť **Rôzne proxy pre každú službu**. Môžete tiež nastaviť proxy napr. len pre **ESET služby** a ponechať **Replikáciu** vypnutú. Použitím možnosti **Použite priame pripojenie, ak nie je k dispozícii HTTP proxy** vyriešite situáciu, keby bol klient mimo dosah proxy.

- **Replikácia (na ESMC Server)** – nastavte proxy, pomocou ktorého sa bude agent pripájať na server.
- **ESET služby** – nastavte proxy, pomocou ktorého sa budú ESET služby ukladať do vyrovnávacej pamäte.

- **Volanie na prebudenie** – ESMC Server dokáže spustiť okamžitú replikáciu ESET Management Agenta na klientskom počítači prostredníctvom služby EPNS. Toto je užitočné, ak nechcete čakať na pravidelný interval pripojenia ESET Management Agenta na ESMC Server. Ak napríklad chcete, aby bola úloha pre klienta spustená na klientoch okamžite alebo chcete, aby bola politika aplikovaná ihneď.
- **Kompatibilita** – pre umožnenie správy bezpečnostných produktov spoločnosti ESET verzie 5 alebo staršej prostredníctvom ESET Management Agenta musí byť nastavený špecifický prijímajúci port. Bezpečnostné produkty ESET musia byť nakonfigurované tak, aby boli nasmerované na tento port a adresa ESET Security Management Center Servera musí byť nastavená na **localhost**.
- **Operačný systém** – použite prepínače pre hlásenie určitých informácií alebo problémov na klientskom počítači.
- **Repozitár** – umiestnenie repozitára, kde sú uložené všetky inštalačné súbory.

Poznámka:
Pre repozitár je prednastavená možnosť **AUTOSELECT**.

- **Program zlepšovania produktov** – môžete zapnúť alebo vypnúť odosielanie správ o zlyhaní programu a anonymných telemetrických údajov do spoločnosti ESET.
- **Zapisovanie do protokolov** – môžete nastaviť úroveň podrobnosti protokolov, čím určíte úroveň informácií, ktoré budú zhromažďované a zapisované do protokolov – od úrovne **Sledovanie** (informačné) až po **Závažné** (najdôležitejšie, kritické informácie). Aktuálny súbor protokolu ESET Management Agenta sa nachádza na klientskom počítači v nasledujúcom umiestnení: *C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* alebo *C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*
- **Nastavenie** – Inštalácia chránená heslom je funkcia, ktorá slúži na ochranu ESET Management Agenta (iba na systéme Windows). Pre povolenie ochrany ESET Management Agenta je potrebné nastaviť heslo. Po aplikovaní politiky ESET Management Agent nemôže byť odinštalovaný ani na ňom nemôže byť vykonaná oprava, ak nie je zadané heslo.

Dôležité:
V prípade, že zabudnete heslo, nebudete môcť odinštalovať ESET Management Agenta z cieľového počítača.

Priradiť

Vyberte klientske zariadenia, pre ktoré má byť daná politika určená. Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte zariadenie, na ktoré chcete politiku aplikovať, a kliknite na **OK**.

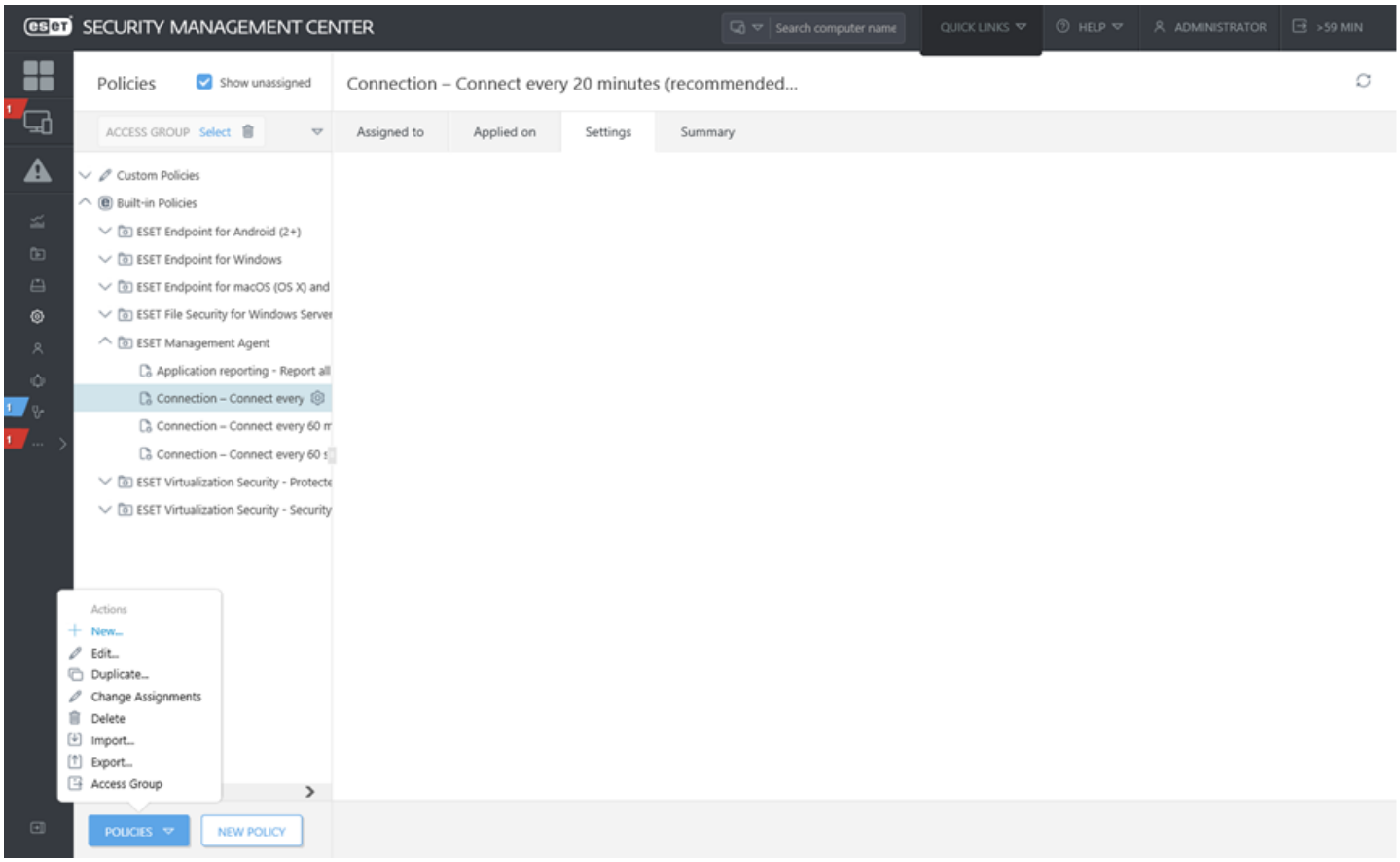
Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

3.1.2.3.1 Vytvorenie politiky pre úpravu intervalu pripájania ESET Management Agenta

V nasledujúcom príklade si ukážeme, ako vytvoriť politiku pre ESET Management Agenta a upraviť jeho interval pripájania na ESMC Server. Odporúčame vykonať tieto kroky pred samotným testovaním hromadného nasadenia agenta vo vašom prostredí.

Vytvorte novú statickú skupinu. Pridajte novú politiku kliknutím na **Politiky**. Kliknite na **Politiky** v spodnej časti a kliknite na možnosť **Nová**.

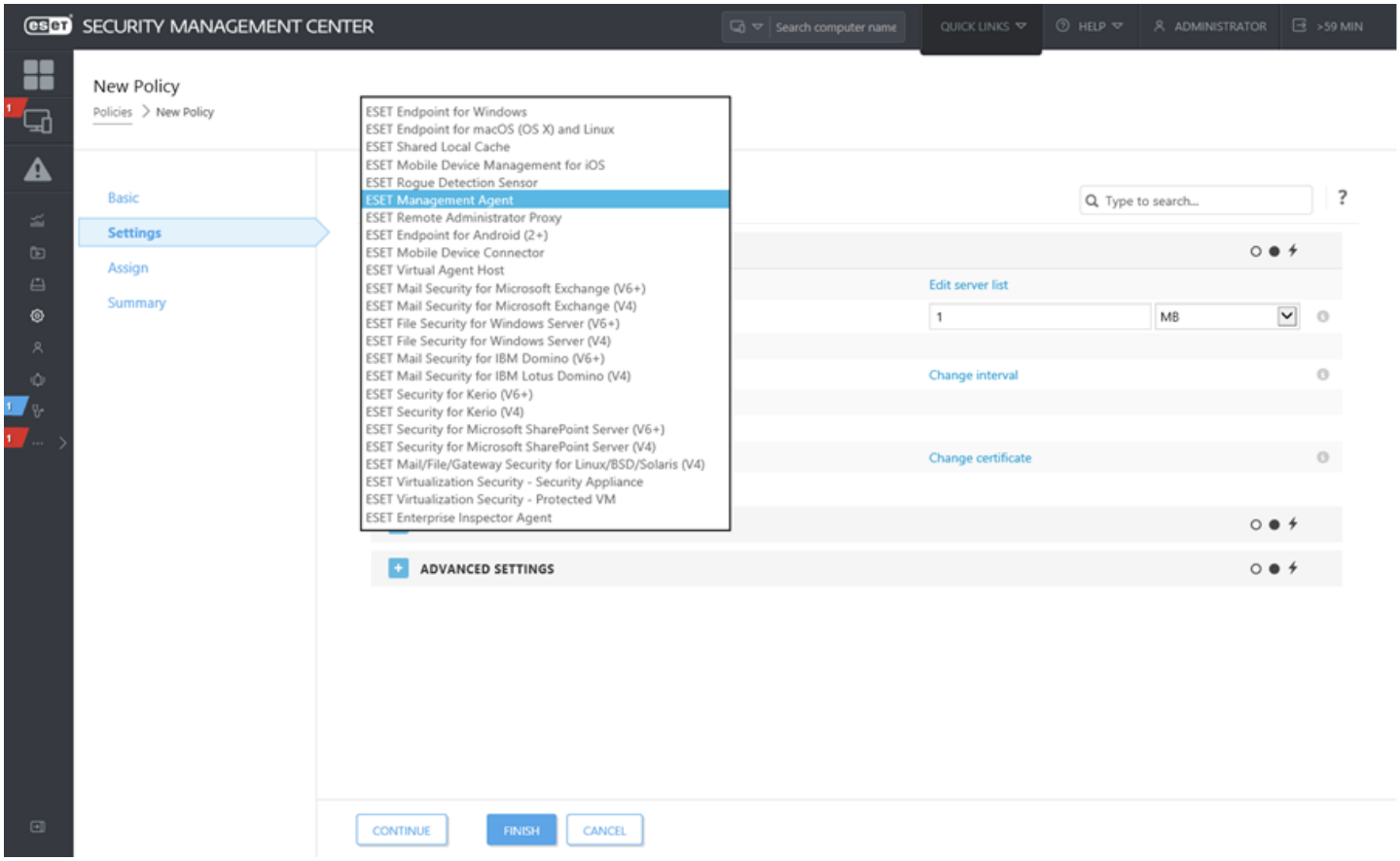


Základné

Zadajte **Názov** pre novú politiku (napr. „Interval pripojenia agenta“). Pole **Popis** je voliteľné.

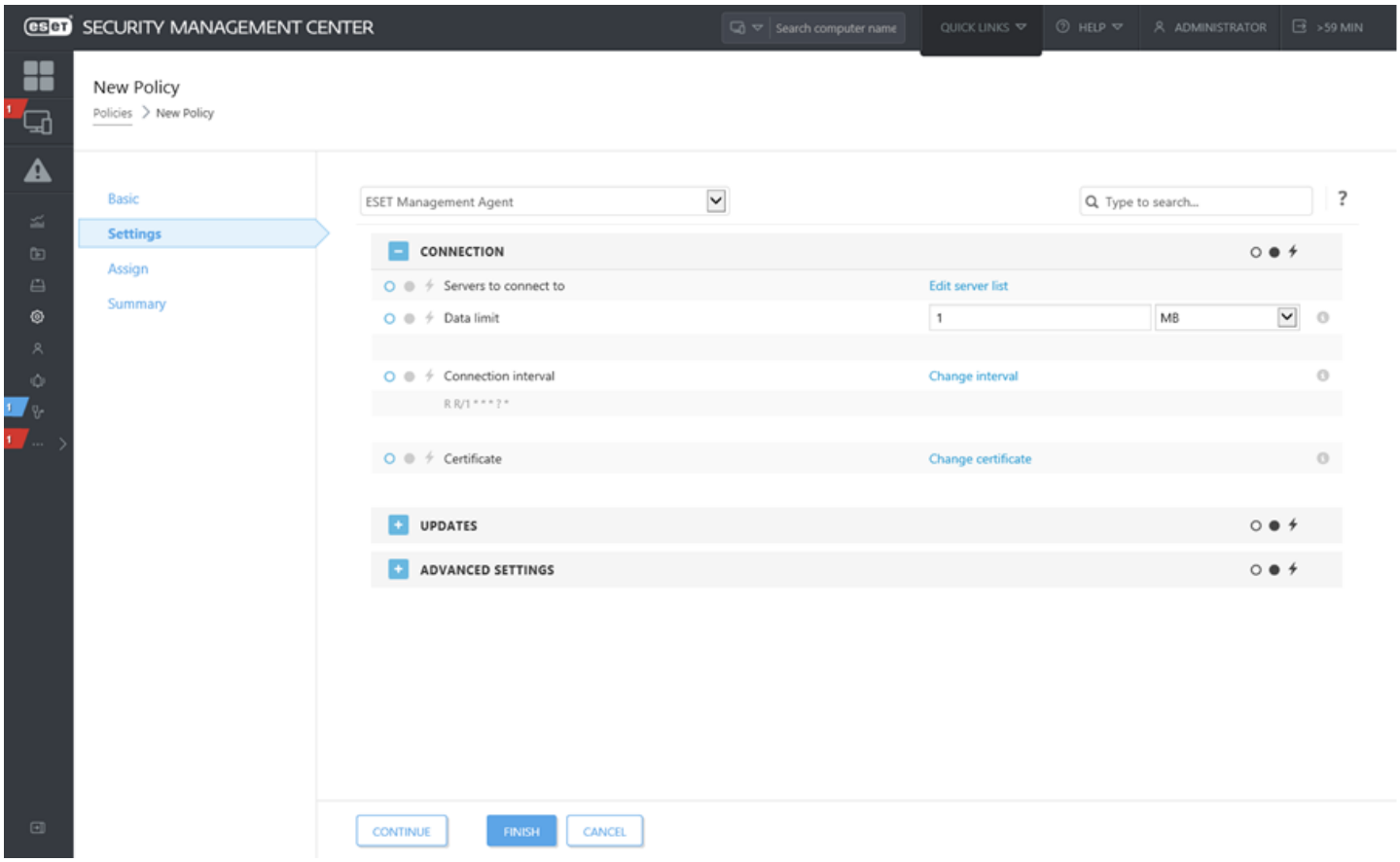
Nastavenia

Z roletového menu **Produkt** vyberte možnosť **ESET Management Agent**.

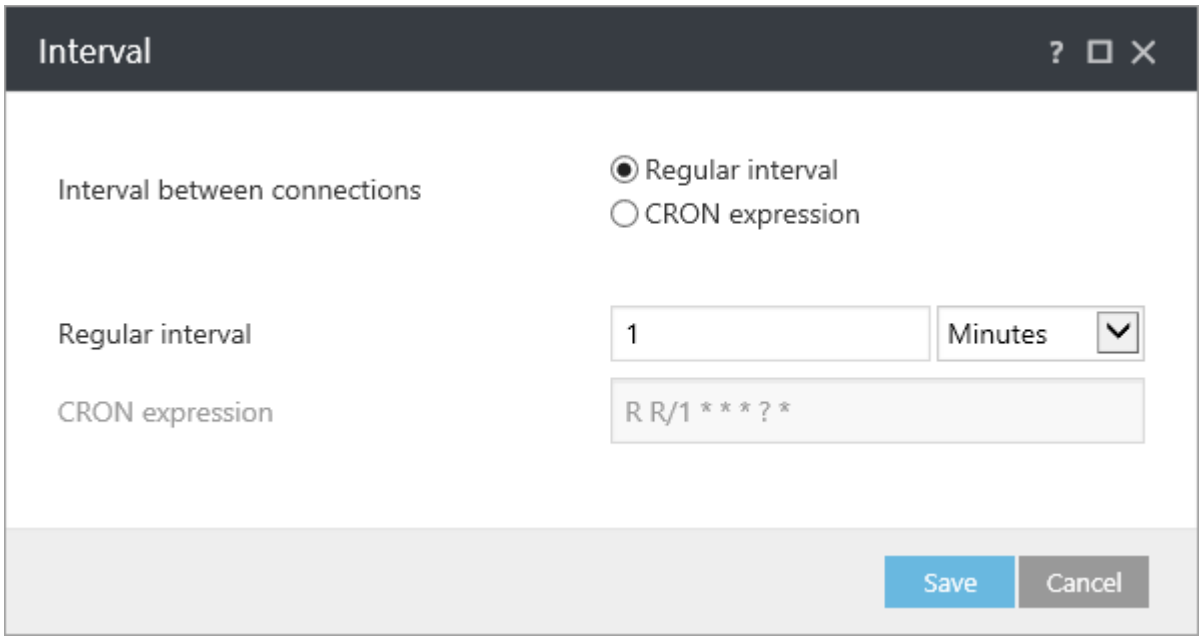


Pripojenie

V zozname na ľavej strane vyberte kategóriu. Na pravej strane upravte požadované nastavenia. Každé nastavenie je pravidlo, pre ktoré môžete určiť príznak. Kliknite na položku **Zmeniť interval**.

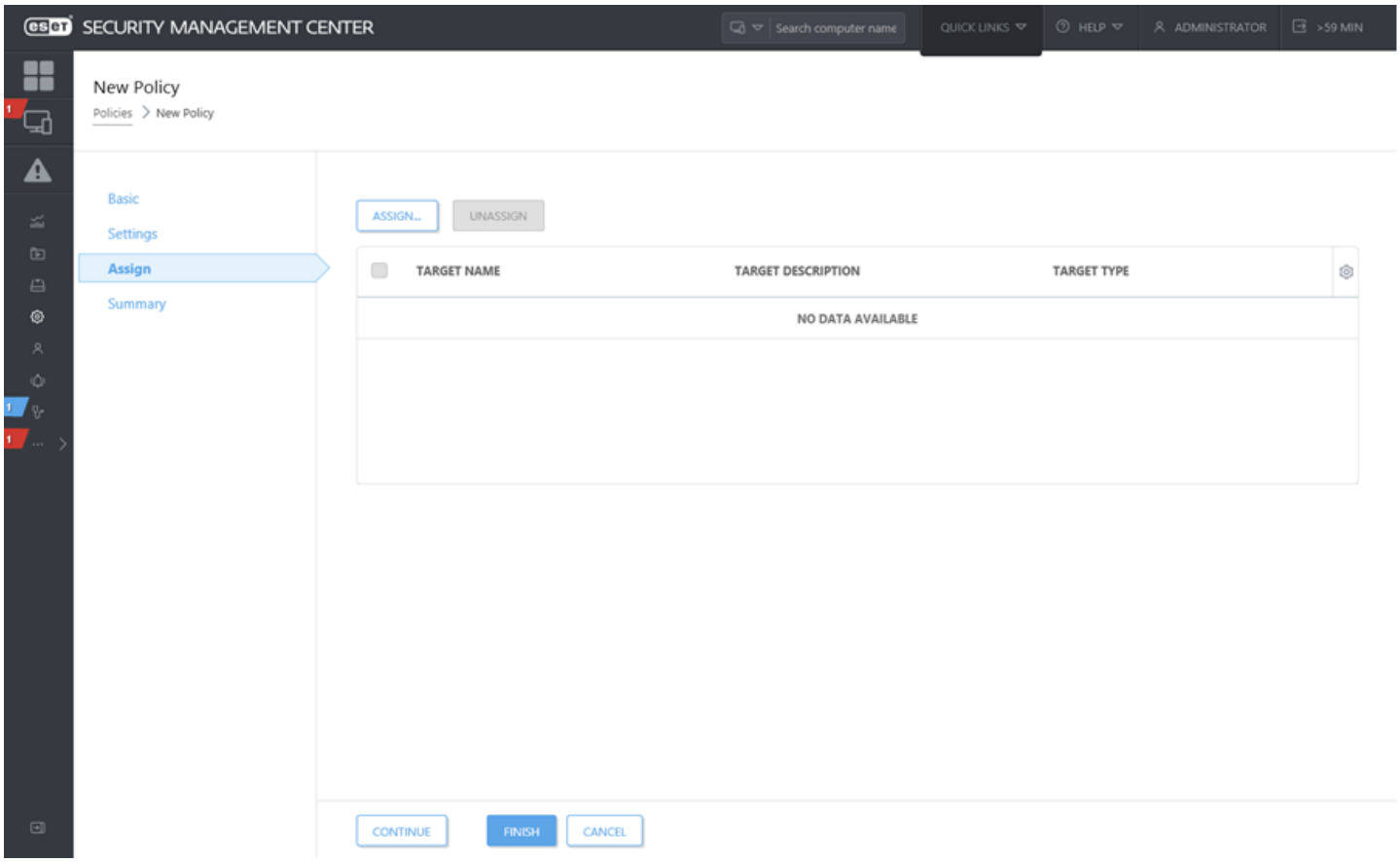


V poli **Pravidelný interval** zmeňte hodnotu na vami preferovaný časový interval (odporúčame 60 sekúnd) a kliknite na **Uložiť**.

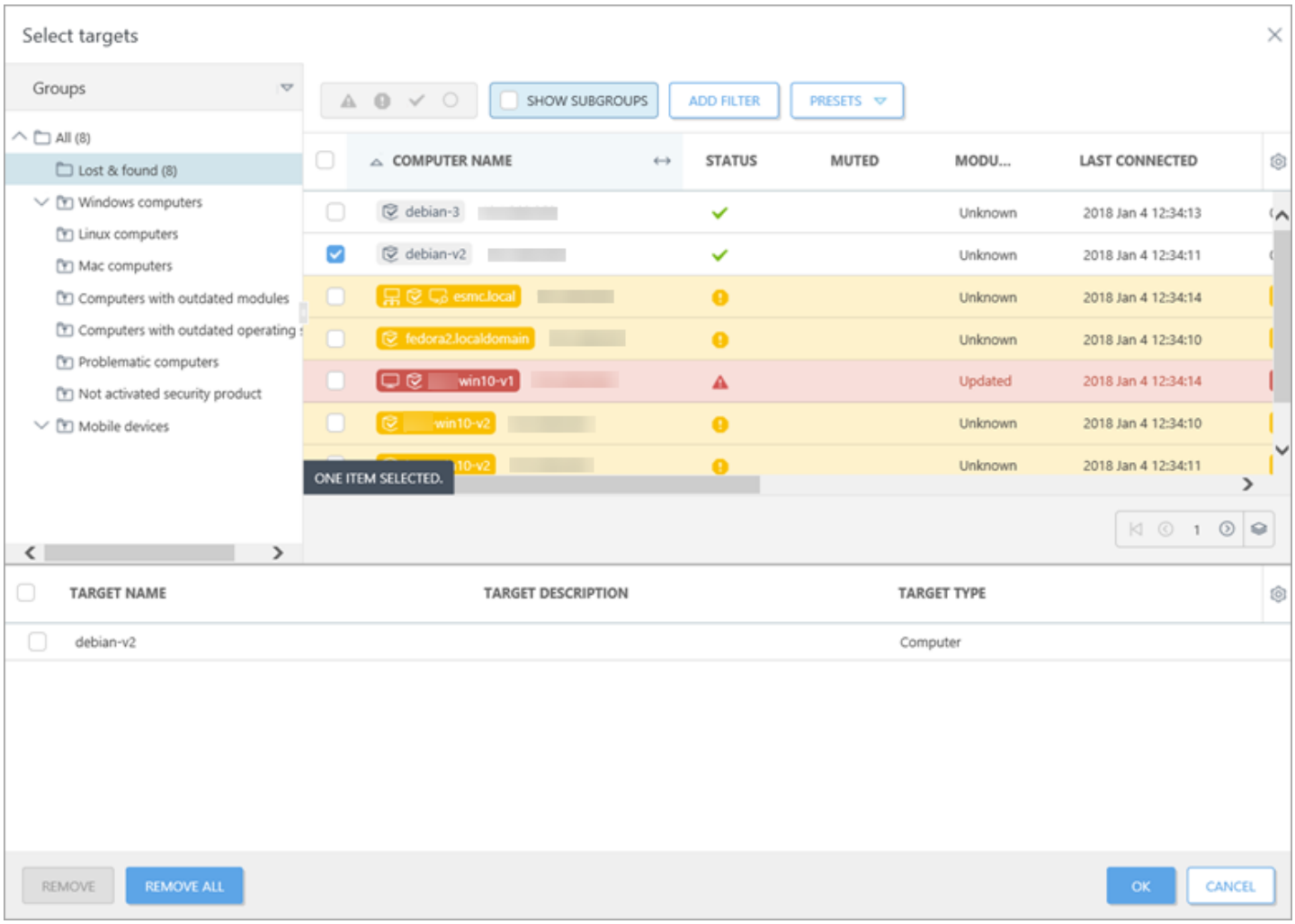


Priradiť

Zvoľte klientov (individuálne počítače/mobilné zariadenia alebo celé skupiny), ku ktorým bude priradená daná politika.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte požadované klientske zariadenia a kliknite na **OK**.



Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

3.1.2.3.2 Vytvorenie politiky pre pripájanie ESET Management Agenta na nový ESMC Server

Táto politika umožňuje upraviť správanie ESET Management Agenta zmenou nastavení. Je to užitočné hlavne pri migrácii klientskych počítačov na nový ESMC Server.

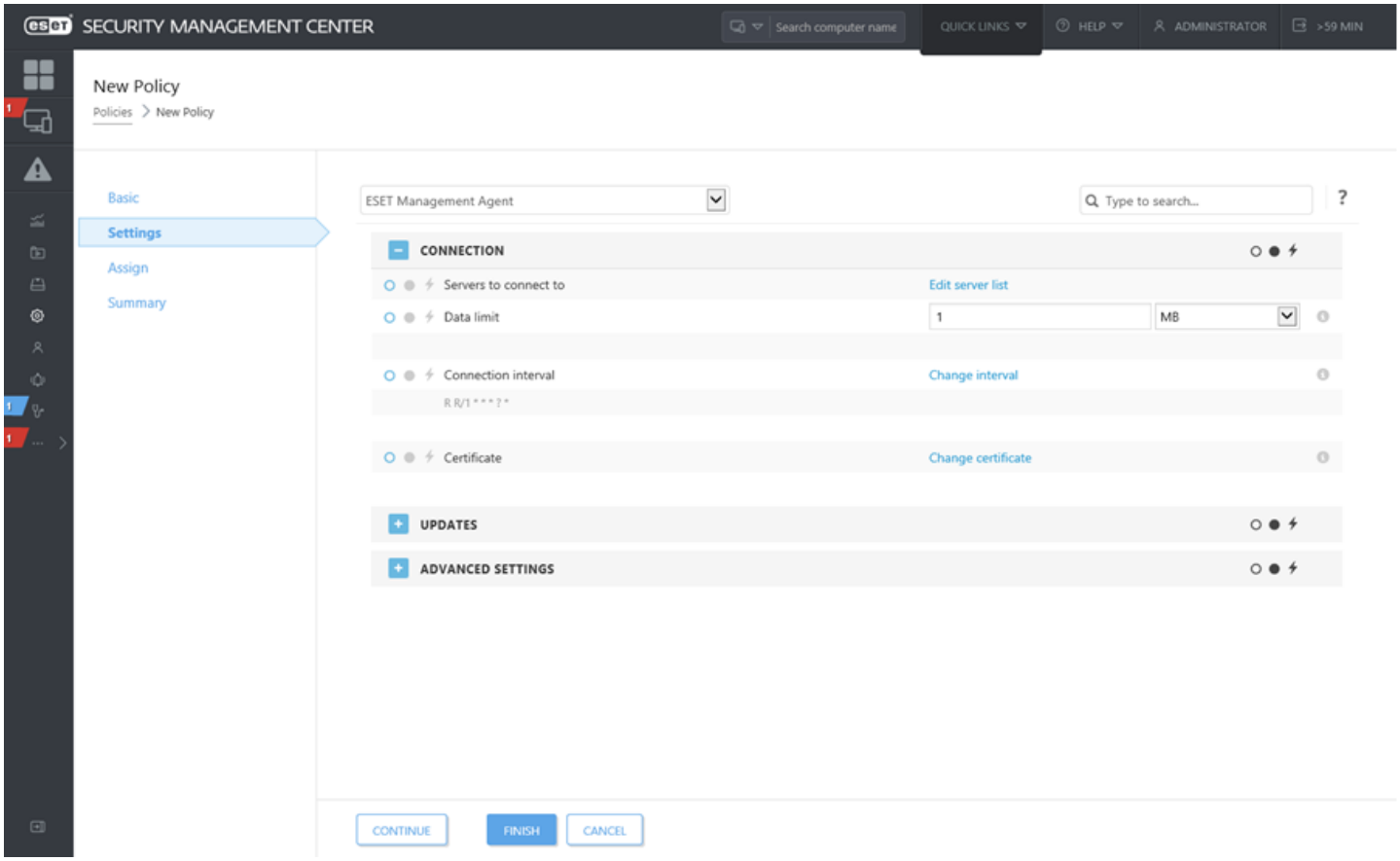
Vytvorte novú politiku, pomocou ktorej bude nastavená nová IP adresa ESMC Servera, a priraďte ju k všetkým klientskym počítačom. Kliknite na **Politiky** > **Vytvoriť novú politiku**.

Základné

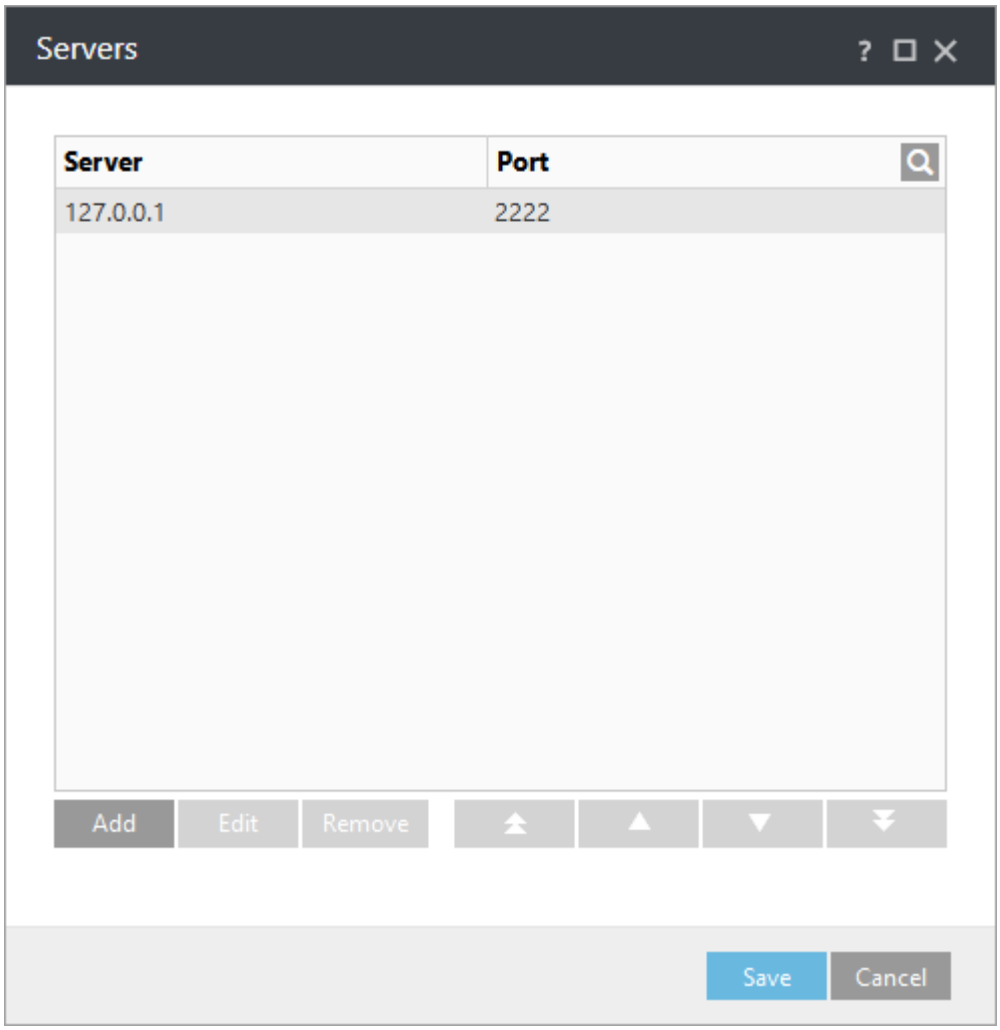
Do poľa **Názov** zadajte názov vašej politiky. Pole **Popis** je voliteľné.

Nastavenia

Z roletového menu vyberte možnosť **ESET Management Agent**, rozbaľte sekciu **Pripojenie** a kliknite na možnosť **Upraviť zoznam serverov** vedľa položky **Servery pre pripojenie**.



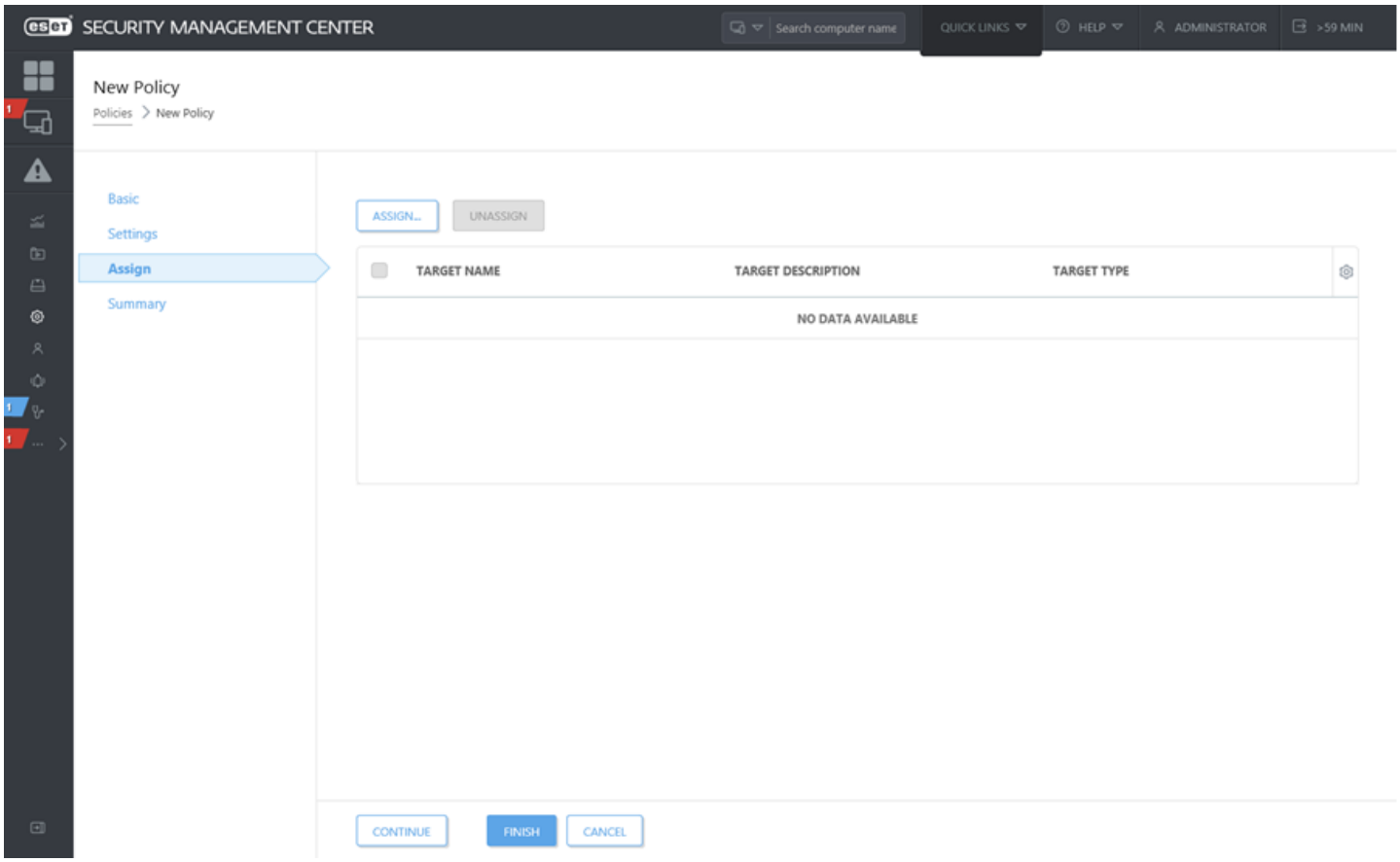
Otvorí sa okno so zoznamom ESMC Serverov, na ktoré sa ESET Management Agent môže pripojiť. Kliknite na možnosť **Pridať** a zadajte IP adresu nového ESMC Servera do poľa **Hostiteľ**. Ak používate iný ako štandardný port ESMC Servera 2222, zadajte svoje číslo portu.



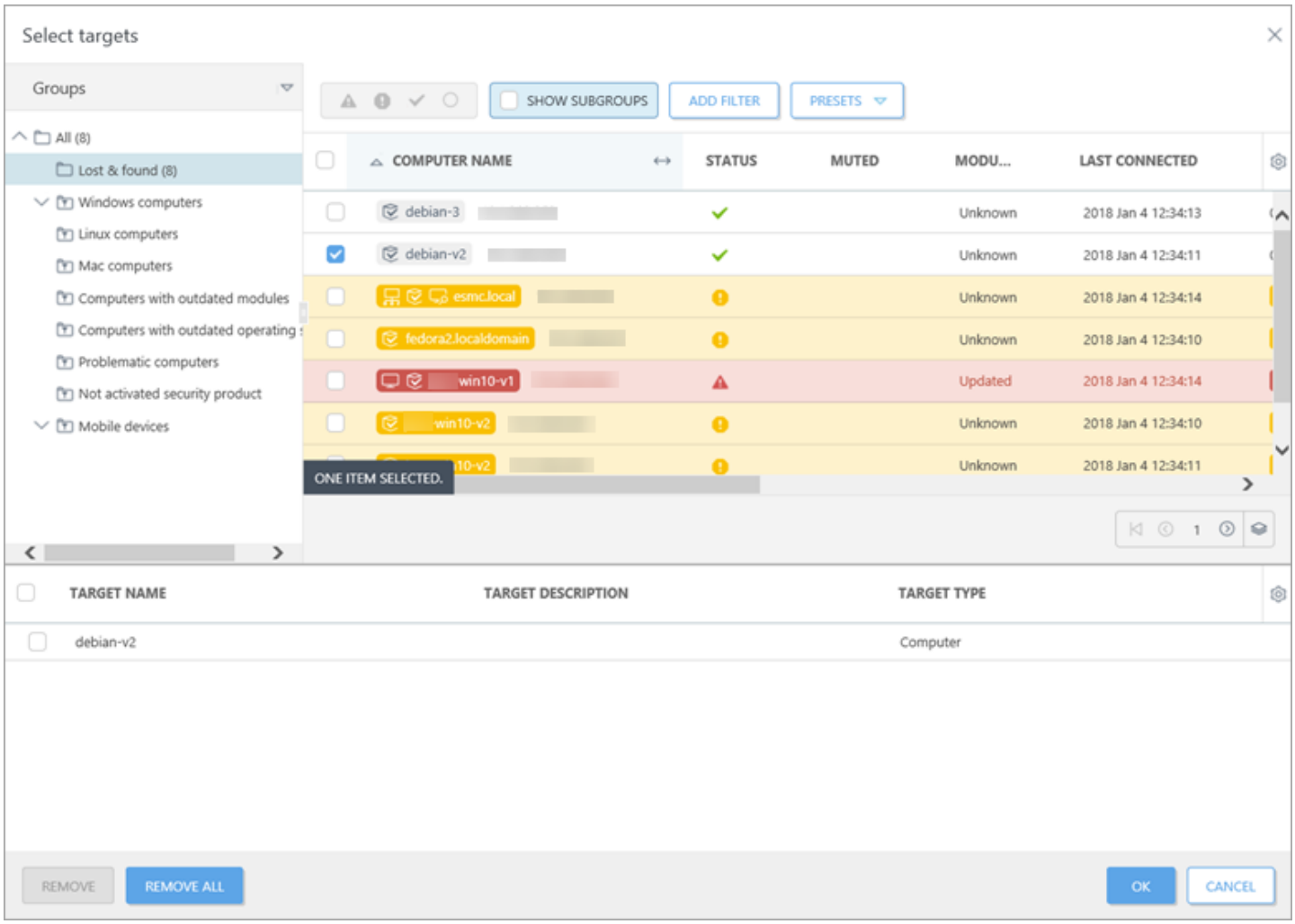
Pomocou tlačidiel so šípkami môžete zmeniť prioritu ESMC Serverov v zozname. Uistite sa, že váš nový ESMC Server je na najvyššom mieste v zozname kliknutím na **dvojitú šípku** a potom kliknite na tlačidlo **Uložiť**.

Priradiť

Zvoľte klientov (individuálne počítače/mobilné zariadenia alebo celé skupiny), ku ktorým bude priradená daná politika.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte požadované klientske zariadenia a kliknite na **OK**.



Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

3.1.2.3.3 Vytvorenie politiky na ochranu ESET Management Agenta heslom

Postupujte podľa nasledujúcich krokov, ak chcete vytvoriť politiku, pomocou ktorej nastavíte heslo chrániace ESET Management Agenta pred neoprávnenými pokusmi o odinštalovanie alebo zmenu nastavení. Ak sa použije **Ochrana nastavení heslom**, bude možné ESET Management Agenta odinštalovať alebo meniť jeho nastavenia len po zadaní príslušného hesla. Viac informácií nájdete v časti Ochrana agenta.

Základné

Zadajte **Názov** politiky. Pole **Popis** je voliteľné.

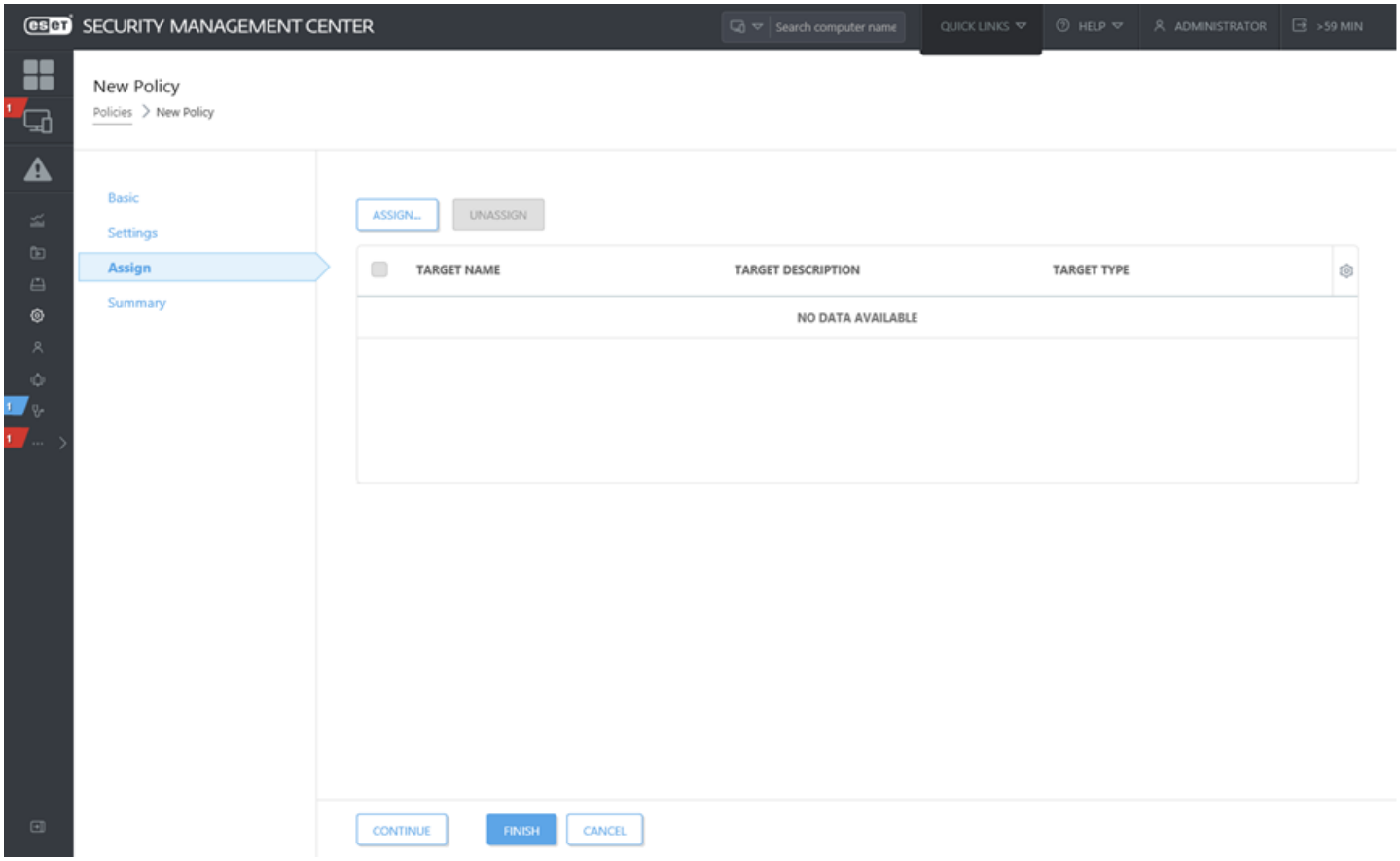
Nastavenia

Z roletového menu vyberte možnosť **ESET Management Agent**, rozbaľte ponuku **Pokročilé nastavenia**, prejdite do časti **Nastavenie** a zadajte heslo do poľa **Ochrana nastavení heslom**. Toto heslo bude vyžadované, ak sa niekto bude pokúšať na klientskom počítači odinštalovať ESET Management Agenta alebo meniť jeho nastavenia.

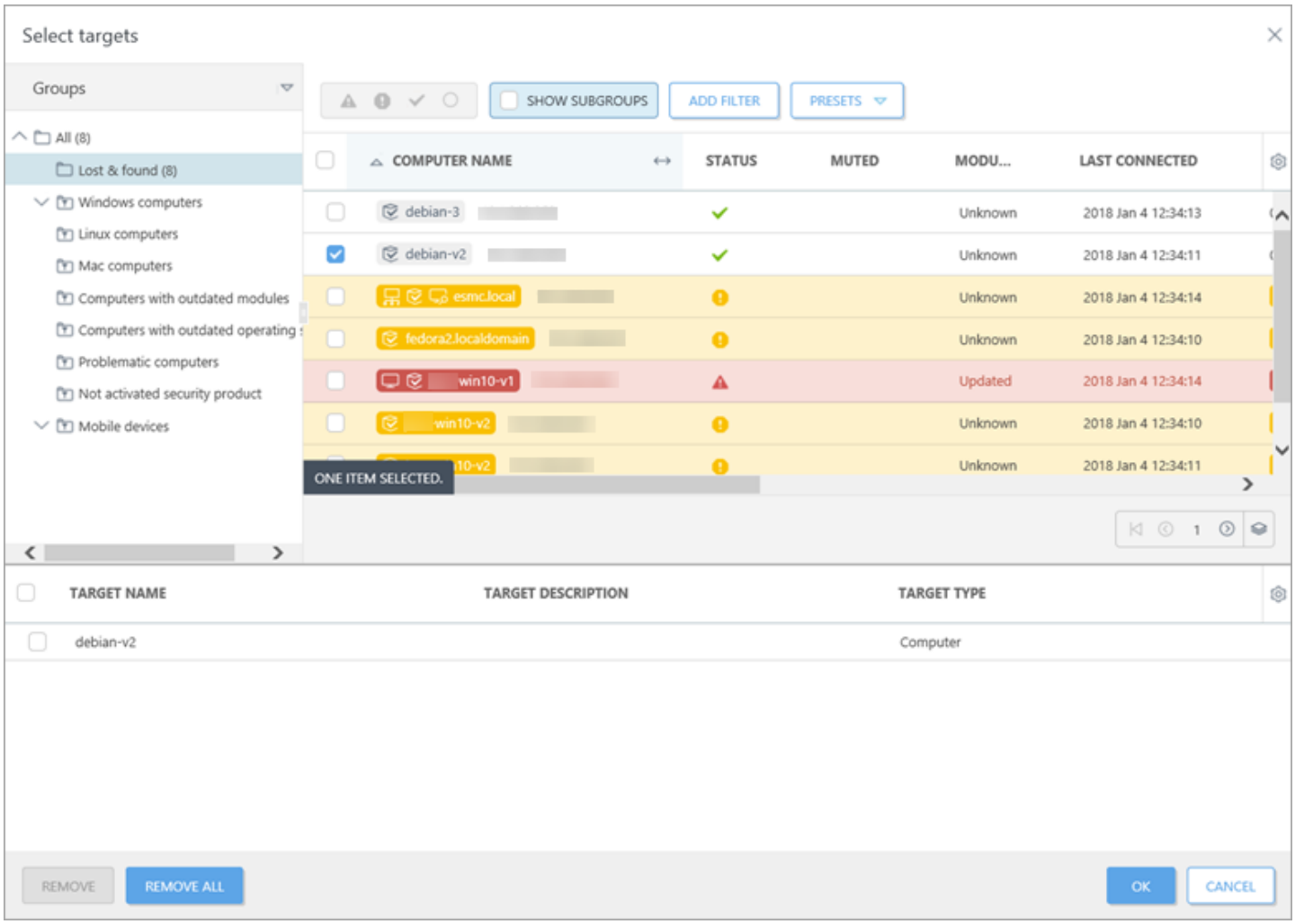
Dôležité:
Toto heslo si dôkladne uložte, pretože je nevyhnutné pre odinštalovanie ESET Management Agenta z klientskeho počítača. V prípade použitia politiky na ochranu heslom, je zadanie správneho hesla jediným konvenčným spôsobom odinštalovania ESET Management Agenta.

Priradiť

Zvoľte klientov (individuálne počítače/mobilné zariadenia alebo celé skupiny), ku ktorým bude priradená daná politika.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte požadované klientske zariadenia a kliknite na **OK**.



Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

3.1.2.4 Ochrana agenta

ESET Management Agent je chránený vstavaným sebaobranným mechanizmom. Táto funkcia poskytuje nasledovné:

- Ochrana proti úpravám registrov ESET Management Agenta (HIPS).
- Súbory patriace ESET Management Agentu nemôžu byť modifikované, nahradzované, vymazané alebo iným spôsobom pozmenené (HIPS).
- Proces ESET Management Agenta nemôže byť ukončený.
- Služba ESET Management Agenta nemôže byť zastavená, pozastavená, zakázaná, odinštalovaná alebo iným spôsobom narušená.

O časť tejto ochrany sa stará funkcia HIPS, ktorá je súčasťou vášho bezpečnostného produktu ESET.

Poznámka:
Pre zaistenie kompletnej ochrany ESET Management Agenta musí byť HIPS na klientskom počítači povolený.

Ochrana nastavení heslom

Okrem spomínaného sebaobranného mechanizmu je možné posilniť ochranu agenta aj nastavením hesla určeného na ochranu prístupu k ESET Management Agentu (dostupné len pre Windows). Pokiaľ je heslo na ochranu agenta nastavené, bude možné ESET Management Agenta odinštalovať alebo meniť jeho nastavenia len po zadaní správneho hesla. Pre nastavenie hesla pre ESET Management Agenta musíte vytvoriť príslušnú politiku.

3.1.3 Riešenie problémov – pripojenie agenta

Ak sa počítač nepripája na ESMC Server, odporúčame riešiť problémy s ESET Management Agentom lokálne na klientskom počítači.

Štandardne sa ESET Management Agent synchronizuje s ESMC Serverom každú minútu. Toto nastavenie môžete zmeniť vytvorením novej politiky na úpravu intervalu pripojenia ESET Management Agenta.

Skontrolujte najnovší protokol ESET Management Agenta. Súbor sa nachádza v nasledujúcom umiestnení:

Windows	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* *C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*
Linux	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
macOS	*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/* */Users/%user%/Library/Logs/EraAgentInstaller.log*

Poznámka:
Pre povolenie úplného zapisovania do protokolov vytvorte prázdny súbor s názvom *traceAll* bez prípony v rovnakom priečinku ako *trace.log* a reštartujte službu ESET Management Agent. Táto možnosť aktivuje úplné zapisovanie do protokolu *trace.log*.

- **last-error.html** – protokol (tabuľka) zobrazujúci posledný chybový kód zaznamenaný počas toho, ako je ESET Management Agent spustený.
- **software-install.log** – textový protokol poslednej vzdialenej inštalácie vykonanej pomocou ESET Management Agenta.
- **status.html** – tabuľka zobrazujúca aktuálny stav komunikácie (synchronizácie) medzi ESET Management Agentom a ESMC Serverom.
- **trace.log** – podrobná správa o celkovej aktivite ESET Management Agenta vrátane chýb, ktoré boli zaznamenané.

Medzi najčastejšie chyby, ktoré môžu brániť komunikácii ESET Management Agenta s ESMC Serverom, patria:

- Vaša sieť nie je nastavená správne. Uistite sa, že počítač, na ktorom je nainštalovaný ESMC Server, môže komunikovať s pracovnými stanicami, kde je nainštalovaný ESET Management Agent.
- Pre váš ESMC Server nie je nastavený port 2222.
- DNS nepracuje správne alebo sú porty blokované firewallom. Pozrite si náš zoznam portov používaných nástrojom ESET Security Management Center alebo si prečítajte náš článok databázy znalostí: Ktoré porty a adresy treba povoliť, ak používam firewall od iného výrobcu?
- Je použitý chybne vygenerovaný certifikát obsahujúci nesprávne alebo neúplné údaje, ktoré nezodpovedajú verejnému kľúču certifikačnej autority ESMC Servera. Pre vyriešenie tohto problému vytvorte nový certifikát ESET Management Agenta.

3.1.4 Riešenie problémov – nasadenie agenta

Pri nasadzovaní ESET Management Agenta sa môžu vyskytnúť určité problémy. Zlyhanie nasadenia môže mať niekoľko príčin. Táto kapitola vám pomôže:

- zistiť príčinu zlyhania nasadenia ESET Management Agenta,
- skontrolovať možné príčiny zlyhania podľa nižšie uvedenej tabuľky,
- vyriešiť problém a následne vykonať úspešné nasadenie agenta.

Windows

1. Aby ste zistili, prečo zlyhalo nasadenie agenta, prejdite do sekcie **Správy** > **Automatizácia**, vyberte možnosť **Informácie o úlohách nasadenia agenta za posledných 30 dní** a kliknite na **Generovať teraz**.
Zobrazí sa tabuľka s informáciami o nasadení. V stĺpci **Priebeh** sú zobrazené chybové hlásenia nasadenia agenta obsahujúce informácie o tom, prečo nasadenie zlyhalo.

Ak potrebujete podrobnejšie informácie, môžete zmeniť úroveň podrobnosti protokolov ESMC Servera. Prejdite do sekcie **Viac** > Nastavenia servera > **Pokročilé nastavenia** > **Zapisovanie do protokolov** a z roletového menu vyberte možnosť **Chyba**. Spustite nasadenie agenta znova a ak zlyhá, skontrolujte najnovšie položky v protokole ESMC Servera, ktoré nájdete v dolnej časti protokolu. Správa bude obsahovať návrhy riešenia daného problému.

Najnovší súbor nájdete v nasledujúcom umiestnení:

Protokol ESMC Servera	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\trace.log*
Protokol ESET Management Agenta	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* *C:\Documents and Settings\All Users\Application Data\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs*

Pre povolenie úplného zapisovania do protokolov vytvorte prázdny súbor s názvom *traceAll* bez prípony v rovnakom umiestnení ako *trace.log*. Reštartujte službu ESET Security Management Center Server a úplné zapisovanie do protokolov v rámci súboru *trace.log* bude povolené.

Poznámka:
V prípade problémov s pripojením ESET Management Agenta si pozrite časť Riešenie problémov – pripojenie Agenta.

Poznámka:
Ak inštalácia skončí chybou 1603, skontrolujte súbor *ra-agent-install.log*. Súbor sa nachádza v nasledujúcom umiestnení: *C:\Users\%user%\AppData\Local\Temp\ra-agent-install.log* na cieľovom počítači.

2. Nasledujúca tabuľka obsahuje viaceré možné príčiny zlyhania nasadenia agenta:

Chybové hlásenie	Možné príčiny
Nedarí sa pripojiť	• Klient nie je dostupný v sieti, firewall blokuje komunikáciu. • Prichádzajúca komunikácia na portoch 135, 137, 138, 139 a 445 nie je povolená vo firewalle. Nie je použitá výnimka povoľujúca prichádzajúce požiadavky na zdieľanie súborov a tlačiarní. • Hostiteľský názov klienta sa nepodarilo rozpoznať. Použite platný FQDN názov počítača (úplný názov domény).
Prístup odmietnutý	• Ak je aj server, aj klient pripojený k doméne, použite prihlasovacie údaje používateľa, ktorý je doménovým správcom, a to vo formáte **doména\používateľ**. • Ak je aj server, aj klient pripojený k doméne, službu ESMC Server môžete dočasne spustiť pod účtom doménového správcu. • Pri nasadzovaní zo servera na klienta, ktorý nie je v rovnakej doméne, vypnite na cieľovom počítači vzdialenú správu používateľských účtov. • Pri nasadzovaní zo servera na klienta, ktorý nie je v rovnakej doméne, použite prihlasovacie údaje lokálneho používateľa, ktorý je členom skupiny správcov. Názov cieľového počítača bude automaticky vložený na začiatok prihlasovacieho mena. • Účet správcu nemá nastavené heslo. • Nedostatočné prístupové práva. • Správcovské zdieľanie ADMIN$ nie je dostupné. • Správcovské zdieľanie IPC$ nie je dostupné. • Je aktívne zjednodušené zdieľanie súborov.
Balík nebol nájdený v repozitári	• Odkaz na repozitár je nesprávny. • Repozitár je nedostupný. • Repozitár neobsahuje požadovaný balík.

3. Pre riešenie problémov postupujte podľa príslušných krokov v závislosti od možnej príčiny zlyhania:

- **Klient nie je dostupný v sieti** – z ESMC Servera vyskúšajte príkaz ping na klienta. Ak sa zobrazí odozva, pokúste sa na klienta prihlásiť vzdialene (napríklad cez vzdialenú pracovnú plochu).
- **Firewall blokuje komunikáciu** – skontrolujte nastavenia firewallu na serveri aj na kliente a taktiež akýkoľvek iný firewall tretej strany, ktorý figuruje medzi týmito dvoma počítačmi.
- **Hostiteľský názov klienta sa nepodarilo rozpoznať** – medzi možné riešenia problémov s DNS môže patriť:
  - Použitie príkazu `nslookup` pre IP adresu a názov hostiteľa servera a/alebo klienta, ktorý má problém s nasadením agenta. Výsledok by sa mal zhodovať s informáciami z počítača. Napríklad, `nslookup` pre názvov hostiteľa by mal byť preložený na IP adresu, ktorú zobrazí príkaz `ipconfig` na danom hostiteľovi. Príkaz `nslookup` bude potrebné spustiť na klientskych počítačoch a na serveri.
  - Manuálne skontrolovať DNS záznamy pre duplikáty.
- **Porty 2222 a 2223 nie sú otvorené vo firewalle** – uistite sa, že tieto porty sú otvorené na oboch stranách (vo firewalle na serveri aj na kliente).
- **Účet správcu nemá nastavené heslo** – nastavte heslo pre účet správcu (nepoužívajte prázdne heslo).
- **Nedostatočné prístupové práva** – pri vytváraní úlohy pre nasadenie agenta skúste použiť prihlasovacie údaje doménového správcu. Ak je klientsky počítač v pracovnej skupine, použite na danom počítači lokálny účet správcu.

POZNÁMKA:
Po úspešnom nasadení nie sú porty 2222 s 2223 otvorené vo firewalle. Povoľte tieto porty vo všetkých firewall riešeniach medzi klientom a serverom.

- **Aktivácia** účtu správcu:
  1. Otvorte príkazový riadok.
  2. Zadajte nasledujúci príkaz:

```
net user administrator /active:yes
```

- **Správcovské zdieľanie ADMIN$ nie je dostupné** – klientsky počítač musí mať povolené zdieľanie zdroja *ADMIN$*. Uistite sa, že je toto zdieľanie povolené (**Štart** > **Ovládací panel** > **Nástroje na správu** > **Správa počítača** > **Zdieľané priečinky** > **Shares**).
- **Správcovské zdieľanie IPC$ nie je dostupné** – skontrolujte, či má server prístup do *IPC$* pomocou nasledujúceho príkazu spúšťaného v príkazovom riadku na serveri:

`net use \\clientname\IPC$` , kde `clientname` je názov cieľového počítača.

- **Je aktívne zjednodušené zdieľanie súborov** – ak sa vám zobrazuje chybové hlásenie **Prístup odmietnutý** a používate zmiešané prostredie (obsahuje aj doménu, aj pracovnú skupinu), vypnite **Zjednodušené zdieľanie súborov** alebo použite **Sprievodcu zdieľaním** na všetkých počítačoch, ktoré majú problém s nasadením agenta. Napríklad, na operačnom systéme Windows 7 vykonajte nasledovné:
  - Kliknite na **Štart**, do vyhľadávacieho poľa napíšte `priečinok` a kliknite na **Možnosti priečinka**. Ďalej kliknite na kartu **Zobrazenie** a v dolnej časti sekcie **Rozšírené nastavenia** zrušte označenie možnosti **Použiť Sprievodcu zdieľaním**.
- **Odkaz na repozitár je nesprávny** – v nástroji ESMC Web Console prejdite do časti **Viac** > Nastavenia servera, kliknite na **Pokročilé nastavenia** > **Repozitár** a uistite sa, že URL adresa repozitára je správna.
- **Balík nebol nájdený v repozitári** – toto chybové hlásenie sa zvyčajne zobrazuje vtedy, keď nie je dostupné pripojenie k ESMC repozitáru. Skontrolujte vaše pripojenie na internet.

Linux a macOS

Ak nasadenie agenta zlyhá na operačných systémoch macOS, problém sa väčšinou týka SSH. Skontrolujte klientske počítače a uistite sa, že SSH daemon je spustený. Znova spustite nasadenie agenta.

3.1.5 Ukážkové scenáre nasadenia ESET Management Agenta

Táto časť obsahuje štyri overené scenáre nasadenia ESMC Agenta.

1. Nasadenie zo zariadenia ESMC Server alebo z ESMC Servera bežiaceho na systéme Linux na cieľové počítače Windows nepripojené k doméne.
2. Nasadenie z ESMC Servera bežiaceho na Windows serveri nepripojenom k doméne na cieľové počítače Windows nepripojené k doméne.
3. Nasadenie zo zariadenia ESMC Server alebo z ESMC Servera bežiaceho na systéme Linux na cieľové počítače Windows pripojené k doméne.
4. Nasadenie z ESMC Servera bežiaceho na Windows serveri pripojenom k doméne na cieľové počítače Windows pripojené k doméne.

3.1.5.1 Ukážkové scenáre nasadenia ESET Management Agenta na ciele nepripojené k doméne

1. Nasadenie zo zariadenia ESMC Server alebo z ESMC Servera bežiaceho na systéme Linux na cieľové počítače Windows **nepripojené k doméne**.
2. Nasadenie z ESMC Servera bežiaceho na Windows serveri nepripojenom k doméne na cieľové počítače Windows **nepripojené k doméne**.

Prerekvizity:

- Rovnaká lokálna sieť.
- Funkčné názvy FQDN, napr. desktop-win7.test.local sa viaže k 192.168.1.20 a naopak.
- Čistá inštalácia operačného systému z MSDN s predvolenými nastaveniami.

Ciele:

Windows 10 Enterprise
Windows 8.1 Enterprise
Windows 7 Enterprise

1. Vytvorte používateľa s heslom, ktorý bude členom skupiny správcov, napr. „Admin“. Otvorte **Microsoft Management Console** kliknutím na **Spustiť** v ponuke Štart, zadaním príkazu „mmc“ a následným stlačením tlačidla **OK**.
2. Kliknutím na **Súbor** > **Pridať alebo odstrániť modul** v konzole MMC pridajte modul **Lokálni používatelia a skupiny**. Do priečinka**Používatelia** pridajte nového používateľa a vyplňte požadované informácie do príslušných polí (nezabudnite zadať heslo). V sekcii **Skupiny** otvorte **Vlastnosti** skupiny **Administrators** a kliknutím na tlačidlo **Pridať** pridajte novovytvoreného používateľa do skupiny. V rámci možnosti **Zadajte názvy objektov, ktoré chcete vybrať** vyplňte prihlasovacie údaje novovytvoreného používateľa a overte ich kliknutím na tlačidlo **Skontrolovať názvy**.
3. V **Centre sietí a zdieľania** zmeňte nastavenie siete z **Verejnej siete** na **Súkromnú sieť** kliknutím na možnosť **Verejná sieť** v ľavej časti sekcie **Zobrazenie aktívnych sietí**.
4. Pre **Súkromnú sieť** vypnite **Windows Firewall** – kliknite na **Zapnúť alebo vypnúť bránu Windows Firewall** a zvoľte možnosť **Vypnúť bránu Windows Firewall** v nastaveniach domácej alebo pracovnej siete.
5. V **Centre sietí a zdieľania** kliknite na **Zmeniť rozšírené nastavenie zdieľania** a skontrolujte, či je pre **Súkromnú sieť** povolené **Zdieľanie súborov a tlačiarní**.
6. Kliknutím na **Spustiť** z ponuky Štart a zadaním príkazu „regedit“ otvorte **Editor databázy Registry**. Prejdite do `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
7. V súbore **System** vytvorte novú **hodnotu DWORD** s názvom „LocalAccountTokenFilterPolicy“ a **hodnotu** nastavte na „1“.
8. V ESET Security Management Center Web Console vytvorte úlohu pre server „Nasadenie agentov“ a priraďte ju k FQDN názvu počítača (ak chcete zistiť FQDN názov počítača, kliknite pravým tlačidlom myši na ikonu **Počítač** a zvoľte možnosť **Vlastnosti**. FQDN názov sa zobrazí vedľa popisu **Úplný názov počítača**).
9. Nastavte **Názov hostiteľa servera (voliteľný)** tak, aby odkazoval na FQDN názov alebo IP adresu ESMC Servera.
10. Nastavte používateľské meno na „Admin“ (bez uvádzania názvu domény alebo názvu počítača) a zadajte príslušné heslo.
11. Vyberte certifikát agenta.
12. Vytvorenú úlohu spustite.

Pre Windows XP Professional

1. Vytvorte používateľa s heslom, ktorý bude členom skupiny správcov, napr. „Admin“. Otvorte **Microsoft Management Console** kliknutím na **Spustiť** v ponuke Štart, zadaním príkazu „mmc“ a následným stlačením tlačidla **OK**.
2. Kliknutím na **Súbor** > **Pridať alebo odstrániť modul** pridajte modul **Lokálni používatelia a skupiny**. Do priečinka**Používatelia** pridajte nového používateľa a vyplňte požadované informácie do príslušných polí (nezabudnite zadať heslo). V sekcii **Skupiny** otvorte **Vlastnosti** skupiny **Administrators** a kliknutím na tlačidlo **Pridať** pridajte novovytvoreného používateľa do skupiny. V rámci možnosti **Zadajte názvy objektov, ktoré chcete vybrať** vyplňte prihlasovacie údaje novovytvoreného používateľa a overte ich kliknutím na tlačidlo **Skontrolovať názvy**.
3. Na karte **Windows Firewall** > **Všeobecné** vypnite **Windows Firewall**.
4. Na karte **Windows Firewall** > **Výnimky** skontrolujte, či je povolené **Zdieľanie súborov a tlačiarní**.
5. Otvorte **Lokálne nastavenie zabezpečenia** kliknutím na **Spustiť** z ponuky Štart, zadaním príkazu „secpol.msc“ a stlačením tlačidla **OK**.
6. Zvoľte **Lokálne politiky** > **Možnosti zabezpečenia** > **Prístup na sieť: Model zdieľania a zabezpečenia lokálnych kont** a pravým tlačidlom myši kliknite na možnosť **Vlastnosti**.
7. Nastavte zvolenú politiku na **Klasický – lokálni používatelia sú overovaní ako oni sami**.

8. V ESET Security Management Center Web Console vytvorte novú úlohu pre server „Nasadenie agentov“ a priraďte ju k FQDN názvu počítača (ak chcete zistiť FQDN názov počítača, kliknite pravým tlačidlom myši na ikonu **Počítač** a zvoľte možnosť **Vlastnosti**. FQDN názov sa zobrazí vedľa popisu **Úplný názov počítača**).
9. Nastavte **Názov hostiteľa servera (voliteľný)** tak, aby odkazoval na FQDN názov alebo IP adresu ESMC Servera.
10. Nastavte používateľské meno na „Admin“ (bez uvádzania názvu domény alebo názvu počítača) a zadajte príslušné heslo.
11. Vyberte certifikát agenta.
12. Vytvorenú úlohu spustite.

3.1.5.2 Ukážkové scenáre nasadenia ESET Management Agenta na ciele pripojené k doméne

1. Nasadenie zo zariadenia ESMC Server alebo z ESMC Servera bežiaceho na systéme Linux na cieľové počítače Windows **pripojené k doméne**.
2. Nasadenie z ESMC Servera bežiaceho na Windows serveri pripojenom k doméne na cieľové počítače Windows **pripojené k doméne**.

Prerekvizity:

- Rovnaká lokálna sieť.
- Funkčné názvy FQDN, napr. desktop-win10.esmc.local sa viaže k 10.0.0.2 a naopak.
- Čistá inštalácia operačného systému z MSDN s predvolenými nastaveniami.
- Vytvorená doména „esmc.local“ s netbios názvom „ESMC“.
- Vytvorený používateľský účet doménového administrátora („DomainAdmin“), ktorý je členom bezpečnostnej skupiny „Domain Admins“ v doménovom radiči.
- Každý počítač je pripojený k doméne „esmc.local“ s používateľom „DomainAdmin“, pričom tento používateľ musí byť správca (Windows 10, 8.1, 7) alebo štandardný používateľ (pokročilý používateľ na Windows XP).
- Doménový správca „DomainAdmin“ sa môže prihlásiť do každého počítača a vykonávať lokálne správcovské úlohy.
- Služba ESMC Server na systéme Windows je dočasne spustená pod účtom doménového správcu „ESMC\DomainAdmin“. Po nasadení stačí službu spustiť ako sieťovú službu „Network Service“ (pre virtuálne zariadenie alebo Linux nie sú potrebné žiadne zmeny).

Ciele:

Windows 10 Enterprise
Windows 8.1 Enterprise
Windows 7 Enterprise

1. Otvorte **Centrum sietí a zdieľania**.
2. V sekcii **Zobrazenie aktívnych sietí** skontrolujte, či je vaša sieť nastavená ako **Doménová sieť**.
3. Pre **Doménovú sieť** vypnite **Windows Firewall** – kliknite na **Zapnúť alebo vypnúť bránu Windows Firewall** a zvoľte možnosť **Vypnúť bránu Windows Firewall** v časti **Nastavenia umiestnenia doménovej siete**.
4. V **Centre sietí a zdieľania** kliknite na **Zmeniť rozšírené nastavenie zdieľania** a skontrolujte, či je pre **Doménovú sieť** povolené **Zdieľanie súborov a tlačiarní**.
5. V ESET Security Management Center Web Console vytvorte novú úlohu pre server „Nasadenie agentov“ a priraďte ju k FQDN názvu počítača (ak chcete zistiť FQDN názov počítača, kliknite pravým tlačidlom myši na ikonu **Počítač** a zvoľte možnosť **Vlastnosti**. FQDN názov sa zobrazí vedľa popisu **Úplný názov počítača**).
6. Nastavte **Názov hostiteľa servera (voliteľný)** tak, aby odkazoval na FQDN názov alebo IP adresu ESMC Servera.
7. Do poľa Používateľské meno zadajte „ESMC\DomainAdmin“ (je dôležité zahrnúť názov domény) a do ďalšieho poľa zadajte heslo tohto doménového správcu.
8. Vyberte certifikát agenta.
9. Vytvorenú úlohu spustite.

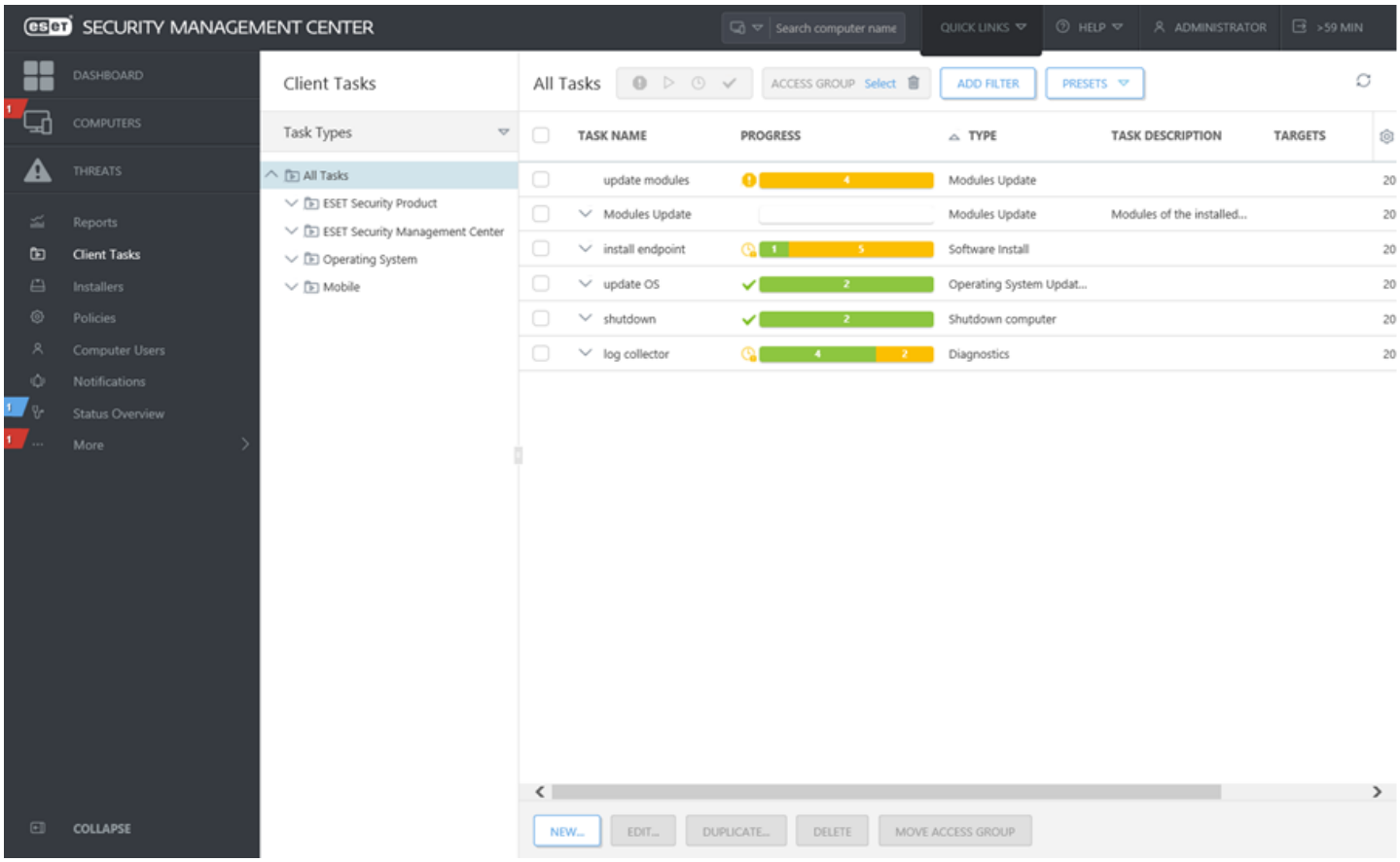
Pre Windows XP Professional

1. Na karte **Windows Firewall** > **Všeobecné** vypnite **Windows Firewall**.
2. Na karte **Windows Firewall** > **Výnimky** skontrolujte, či je povolené **Zdieľanie súborov a tlačiarní**.
3. V ESET Security Management Center Web Console vytvorte novú úlohu pre server „Nasadenie agentov“ a priraďte ju k FQDN názvu počítača (ak chcete zistiť FQDN názov počítača, kliknite pravým tlačidlom myši na ikonu **Počítač** a zvoľte možnosť **Vlastnosti**. FQDN názov sa zobrazí vedľa popisu **Úplný názov počítača**).
4. Nastavte **Názov hostiteľa servera (voliteľný)** tak, aby odkazoval na FQDN názov alebo IP adresu ESMC Servera.
5. Do poľa Používateľské meno zadajte „ESMC\DomainAdmin“ (je dôležité zahrnúť názov domény) a do ďalšieho poľa zadajte heslo tohto doménového správcu.
6. Vyberte certifikát agenta.
7. Vytvorenú úlohu spustite.

3.1.6 Inštalácia bezpečnostných produktov

Bezpečnostné produkty spoločnosti ESET môžu byť nainštalované vzdialene, a to kliknutím na požadovaný klientsky počítač a zvolením možnosti **Nová...** alebo vytvorením novej úlohy pre klienta **Inštalácia softvéru** v časti > **Úlohy pre klienta**. Kliknite na možnosť **Nová...** a môžete začať nastavovať úlohu.

Časť Vykonania úloh pre klienta vám zobrazí aktuálny stav úlohy pre klienta a obsahuje aj indikátor priebehu pre označenú úlohu.

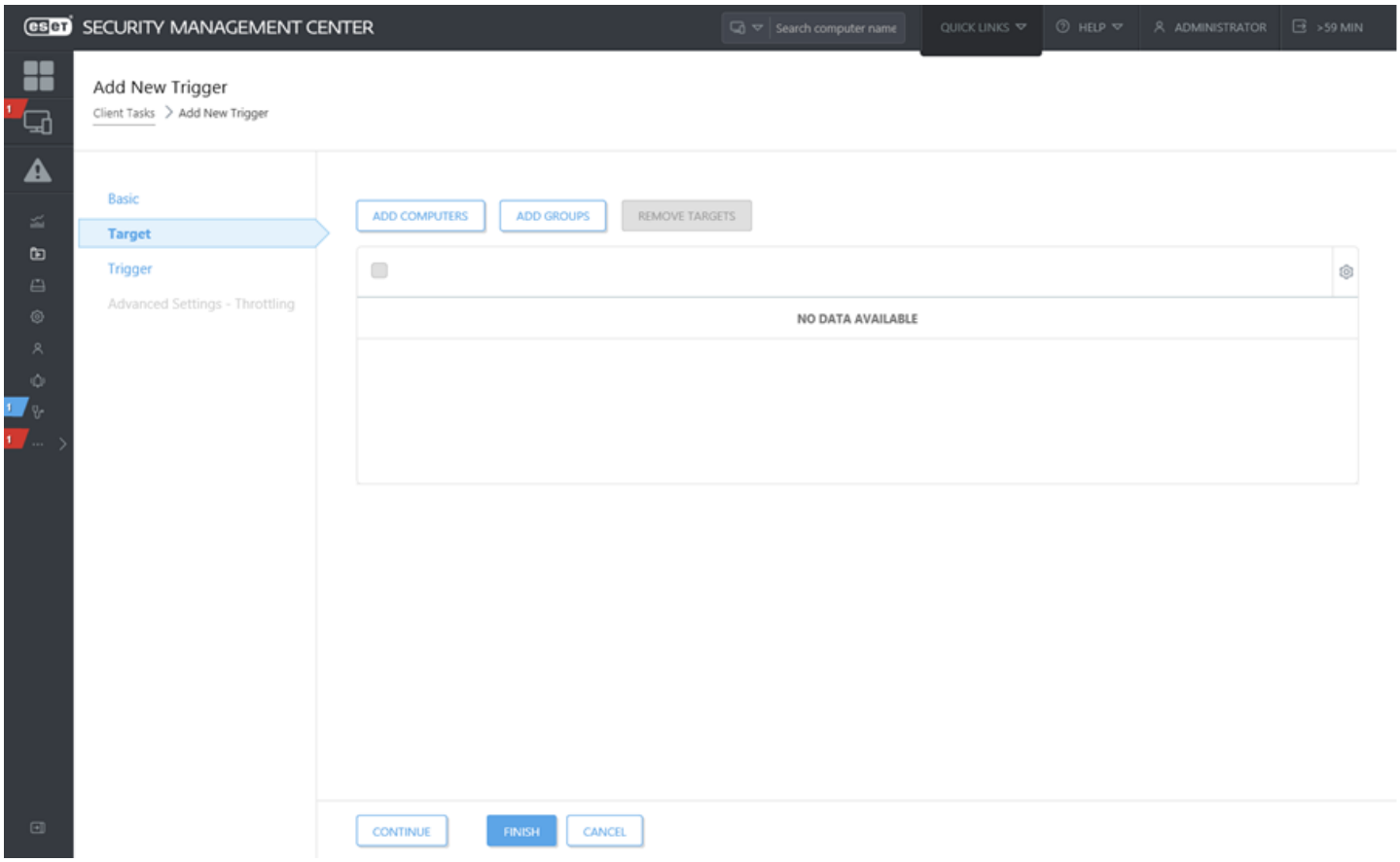


Základné

Zadajte základné informácie o úlohe, ako napr. **Názov**, prípadne popis do poľa **Popis** a typ úlohy do poľa **Typ úlohy**. **Typ úlohy** (pozrite si zoznam vyššie) definuje nastavenia a správanie danej úlohy.

Cieľ

Dôležité:
Ciele nie je možné pridať pri vytváraní úlohy pre klienta. Ciele môžete pridať až vtedy, keď je už úloha vytvorená. Upresnite **Nastavenia** úlohy a kliknite na **Dokončiť** pre vytvorenie úlohy. Potom vytvorte Spúšťač a zvoľte ciele, na ktoré má byť daná úloha aplikovaná.



Nastavenia

Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.

Kliknite na možnosť **<Vyberte ESET licenciu>** a zo zoznamu dostupných licencií vyberte licenciu pre inštalovaný produkt.

V sekcii **<Vyberte balík>** vyberte príslušný inštalačný balík z repozitára alebo zadajte URL adresu balíka. Zobrazí sa zoznam dostupných balíkov, kde si môžete vybrať produkt spoločnosti ESET, ktorý chcete nainštalovať (napr. ESET Endpoint Security). Vyberte požadovaný inštalačný balík a kliknite na **OK**. Ak chcete zadať URL adresu inštalačného balíka, napíšte ju alebo skopírujte do textového poľa (napr. *file://\\pc22\install\ees_nt64_ENU.msi*). Nepoužívajte URL adresu, ktorá vyžaduje autorizáciu.

http://server_address/ees_nt64_ENU.msi – ak inštalujete z verejného webového servera alebo vášho vlastného HTTP servera.
file://\\pc22\install\ees_nt64_ENU.msi – ak inštalujete z lokality vo vašej sieti.
file://C:\installs\ees_nt64_ENU.msi – ak inštalujete z lokálneho disku.

Poznámka:

- ESMC Server a ESET Management Agent musia mať prístup na internet, aby sa mohli pripojiť na repozitár a vykonať inštaláciu. Ak nemáte prístup na internet, musíte nainštalovať klientsky softvér lokálne. V opačnom prípade vzdialená inštalácia zlyhá.
- Pri vykonávaní úlohy Inštalácia softvéru na počítačoch v doméne s bežiacim ESET Management Agentom musí mať používateľ pridelené povolenie na *čítanie* pre priečinok, v ktorom sú uložené inštalátory. V prípade, že je nutné prideliť tieto povolenia, postupujte podľa krokov uvedených nižšie:

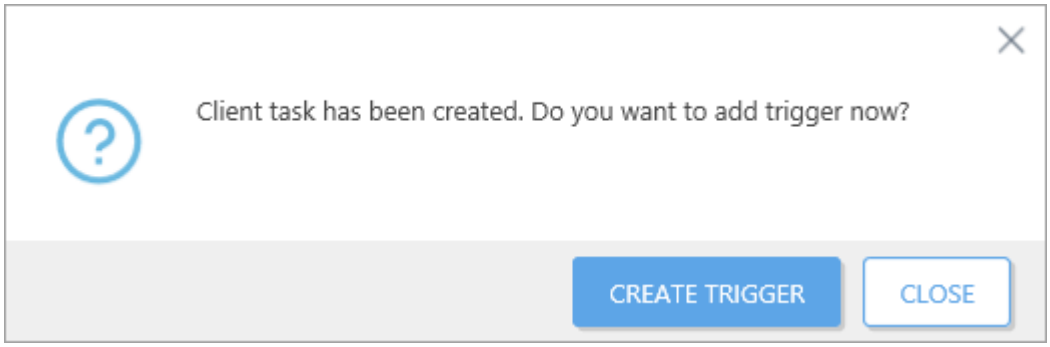
1. Pridajte konto počítača pre službu Active Directory do počítača, na ktorom je daná úloha spustená (napr. *NewComputer$*).
2. Počítaču *NewComputer$* prideľte povolenie na **čítanie** pre priečinok s inštalátormi – kliknite pravým tlačidlom myši na priečinok, z kontextového menu zvoľte možnosť Vlastnosti, prejdite na kartu **Zdieľanie** a stlačte **Zdieľať**.Znak „$“ je na konci názvu počítača nutné uviesť.

Inštalácia zo zdieľaného umiestnenia je možná len v prípade, ak je klientsky počítač v doméne.

V prípade potreby môžete zadať parametre inštalácie. Za iných okolností ponechajte toto pole prázdne. Vyberte možnosť **Automaticky reštartovať, keď je to potrebné** pre vynútenie automatického reštartovania počítača po inštalácii. Túto možnosť však môžete vynechať, pretože klientsky počítač môže byť reštartovaný aj manuálne.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



3.1.6.1 Inštalácia produktu pomocou príkazového riadka

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 nástroja **msiexec**.

Podporované parametre:

APPDIR=<path>
- path – platná cesta k adresáru
- Adresár, do ktorého bude aplikácia nainštalovaná.
- Napríklad: `ees_nt64_ENU.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.

ADDEXCLUDE=<list>
- Zoznam ADDEXCLUDE je čiarkami oddelený zoznam všetkých funkcií, ktoré nebudú nainštalované. Tento parameter nahrádza parameter REMOVE zo starších verzií.
- 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: `ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network`

Poznámka:
Parameter Parameter **ADDEXCLUDE** nemôže byť používaný spolu s parametrom **ADDLOCAL**.

ADDLOCAL=<list>
- Inštalácia komponentov – zoznam nepovinných funkcií, ktoré budú nainštalované lokálne.
- Použitie s ESET inštalačnými balíkmi .msi: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Viac informácii o parametri **ADDLOCAL** nájdete na webovej stránke http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx.

Pravidlá

- Príkaz **ADDLOCAL list** je zoznam funkcií, ktoré budú nainštalované, pričom názvy týchto funkcií sú oddelené čiarkou.
- Pri výbere funkcie, ktorá má byť nainštalovaná, musí byť v zozname uvedená celá cesta (vrátane všetkých nadradených funkcií).
- Pre správne použitie pozrite ostatné pravidlá.

Prítomnosť funkcie

- **Povinné** – táto funkcia bude nainštalovaná vždy.
- **Voliteľné** – výber tejto funkcie môžete zrušiť.
- **Neviditeľné** – funkcia je povinná pre správne fungovanie inej funkcie.
- **Zástupný symbol** – funkcia, ktorá neovplyvňuje produkt, ale musí byť uvádzaná s podfunkciami.

Nižšie nájdete zoznam funkcií produktu ESET určeného pre koncové zariadenia:

Strom funkcií	Názov funkcie	Prítomnosť funkcie
Počítač	Computer	Povinné
Počítač > Antivírus a antispyware	Antivirus	Povinné
Počítač > Antivírus a antispyware > Rezidentná ochrana	RealtimeProtection	Povinné
Počítač > Antivírus a antispyware > Kontrola počítača	Scan	Povinné
Počítač > Antivírus a antispyware > Ochrana dokumentov	DocumentProtection	Voliteľné
Počítač > Správa zariadení	DeviceControl	Voliteľné

Sieť	Sieť	Zástupný symbol
Sieť > Personálny firewall	Firewall	Voliteľné
Web a mail	WebAndEmail	Zástupný symbol
Web a mail > Filtrovanie protokolov	ProtocolFiltering	Neviditeľné
Web a mail > Ochrana prístupu na web	WebAccessProtection	Voliteľné
Web a mail > Ochrana poštových klientov	EmailClientProtection	Voliteľné
Web a mail > Ochrana poštových klientov > Poštové doplnky	MailPlugins	Neviditeľné
Web a mail > Ochrana poštových klientov > Antispamová ochrana	Antispam	Voliteľné
Web a mail > Webová kontrola	WebControl	Voliteľné
Aktualizačný mirror	UpdateMirror	Voliteľné
Podpora Microsoft NAP	MicrosoftNAP	Voliteľné

Ostatné pravidlá

- Ak je na inštaláciu vybraná akákoľvek funkcia v kategórii **Web a mail**, v zozname musí byť zahrnutá aj funkcia **Filtrovanie protokolov**.
- Ak je na inštaláciu vybraná akákoľvek z podfunkcií sekcie **Ochrana poštových klientov**, v zozname musí byť zahrnutá aj funkcia **Poštové doplnky**.

Príklady:

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Zoznam vlastností CFG_ properties:

CFG_POTENTIALLYUNWANTED_ENABLED=	0 – vypnuté, 1 – zapnuté	Detekcia potenciálne nechcených aplikácií (PUA)
CFG_LIVEGRID_ENABLED=	0 – vypnuté, 1 – zapnuté	LiveGrid®
CFG_EPFW_MODE=	0 – Automatický 1 – Interaktívny 2 – Politika 3 – Učiaci sa	Režim firewallu
CFG_PROXY_ENABLED=	0 – vypnuté, 1 – zapnuté	Nastavenie proxy
CFG_PROXY_ADDRESS=	<ip>	IP adresa proxy
CFG_PROXY_PORT=	<port>	Číslo portu proxy
CFG_PROXY_USERNAME=	<user>	Overenie používateľa
CFG_PROXY_PASSWORD=	<pass>	Heslo pre overenie

3.1.6.2 Zoznam problémov pri zlyhaní inštalácie

- Inštalačný balík nebol nájdený.
- Vyžaduje sa novšia verzia služby Inštalátor systému Windows.
- Je nainštalovaná iná verzia alebo konfliktný produkt.
- Prebieha iná inštalácia. Skôr ako budete pokračovať v tejto inštalácii, musíte dokončiť prebiehajúcu inštaláciu.
- Inštalácia alebo odinštalovanie skončilo úspešne, avšak vyžaduje sa reštart počítača.
- Úloha zlyhala – vyskytla sa chyba, otvorte si protokol agenta a nájdite návratový kód inštalátora.

3.1.7 Desktop Provisioning

Viac informácií nájdete v tejto časti.

3.2 Ďalšie nastavenia

Po dokončení počiatočnej konfigurácie odporúčame venovať pozornosť aj nižšie uvedeným možnostiam:

Vytvorenie a úprava skupín

Odporúčame rozdeliť klienty do statických a dynamických Skupín na základe rôznych kritérií. Uľahčuje to správu klientov a správca má väčší prehľad o sieti.

Vytvorenie novej politiky

Politiky sú užitočné v prípade, ak chcete nasadiť špecifickú konfiguráciu na bezpečnostné produkty spoločnosti ESET nainštalované na klientskych pracovných staniciach. Môžete sa tým vyhnúť potrebe nastaviť každý nainštalovaný bezpečnostný produkt spoločnosti ESET manuálne na každom počítači. Po vytvorení novej politiky, ktorá obsahuje vaše nastavenia, ju môžete priradiť ku skupine (statickej alebo dynamickej) pre aplikovanie vašich nastavení na všetky počítače v skupine.

Priradenie politiky ku skupine

Aby bolo možné konkrétnu politiku aplikovať, musí byť priradená k určitej skupine. Politika bude aplikovaná na počítače, ktoré patria do danej skupiny. Politika bude aplikovaná a aktualizovaná vždy, keď sa agent pripojí na ESMC Server.

Nastavenie Oznámenia a vytvorenie Správy

Odporúčame používať oznámenia a správy na sledovanie stavu klientskych počítačov vo vašej sieti. Napríklad, ak chcete byť upozornený v prípade výskytu určitej udalosti, alebo si chcete pozrieť alebo stiahnuť správu.

3.3 VDI, klonovanie a detekcia hardvéru

Produkt ESET Security Management Center od verzie 7 podporuje VDI prostredia, klonovanie počítačov a neperzistentné ukladacie systémy. Táto funkcia vyžaduje, aby bol niektorý počítač označený ako predloha, prípadne sa vyžaduje vyriešenie otázky, ktorá sa objavuje pri klonovaní alebo zmene hardvéru.

- Kým nie je otázka vyriešená, klientsky počítač sa nebude môcť pripojiť k ESMC Serveru.
- Vypnutie detekcie hardvéru nie je možné vrátiť späť, preto odporúčame používať túto možnosť čo najopatrnejšie a iba na fyzických počítačoch!
- Pri riešení viacerých otázok použite dlaždicu Prehľad Stavu – **Otázky**.

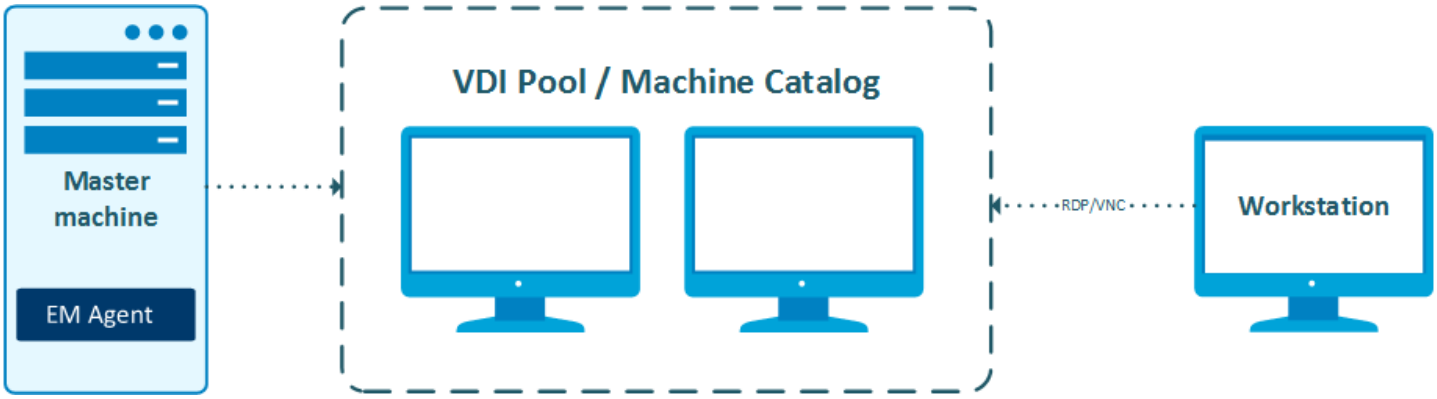
Ktoré operačné systémy a nástroje hypervisor sú podporované?

- Podporované sú iba operačné systémy Windows od verzie XP SP2 x64.
- Komponenty ESET Virtual Agent Host nie sú podporované.
- Mobilné zariadenia spravované pomocou MDM nie sú podporované.
- Prepojené klonované zariadenia vo Virtual Box nie je možné rozlíšiť.
- V ojedinelých prípadoch môže byť detekcia hardvéru vypnutá automaticky nástrojom ESMC. Môže k tomu dôjsť v prípade, ak ESMC nedokáže spoľahlivo analyzovať hardvér zariadenia.
- Citrix, Hyper-V, VMware, VMware Workstation sú podporované.

VDI prostredia

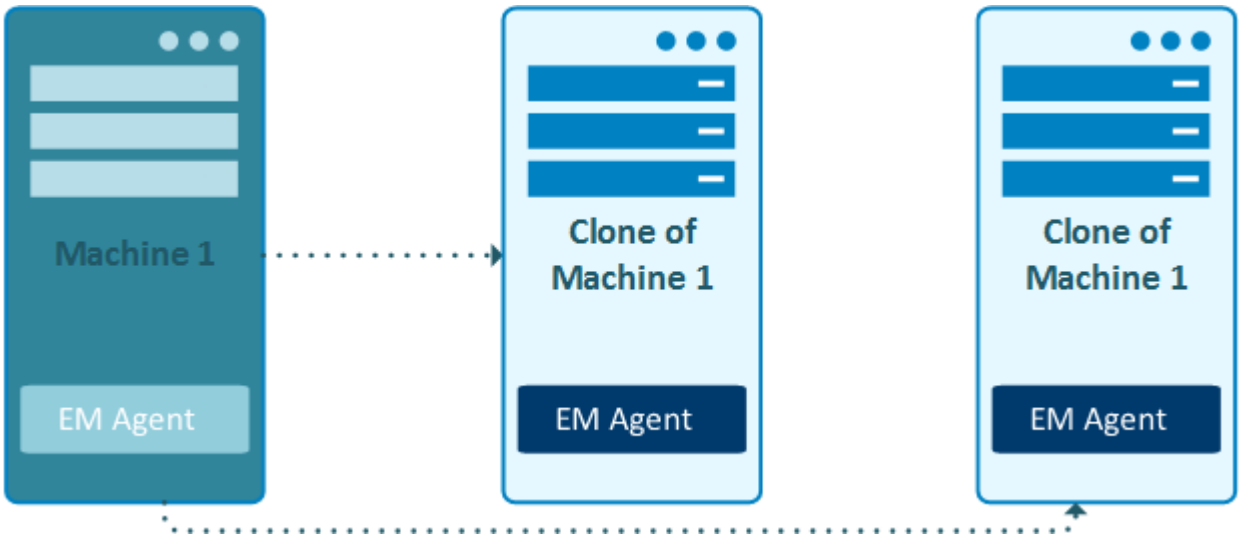
V rámci fondu VDI môžete použiť počítač slúžiaci ako predloha, kde je zároveň nainštalovaný ESET Management Agent. Nevyžaduje sa žiadny VDI konektor, pretože všetku komunikáciu zabezpečuje ESET Management Agent. ESET Management Agent verzie 7 musí byť však na počítači slúžiacom ako predloha nainštalovaný predtým, ako bude nastavený fond VDI (katalóg zariadení).

- Ak chcete vytvoriť fond VDI, označte najprv počítač ako predlohu v sekcii Podrobnosti o počítači – **Hardvér**. Vyberte možnosť **Označiť ako predloha pre klonovanie (porovnať s existujúcim počítačom)**.
- Ak dôjde k odstráneniu počítača označeného ako predloha z ESMC, obnova jeho identity (klonovanie) nebude povolená. Nové počítače z fondu dostanú vždy novú identitu (vo Web Console sa vytvorí záznam o novom počítači).
- Ak sa počítač z fondu VDI pripojí po prvýkrát, má povinný 1-minútový interval pripojenia. Po niekoľkých počiatočných pripojeniach sa interval pripojenia nastaví podľa počítača označeného ako predloha.
- Nikdy nevypínajte detekciu hardvéru pri používaní fondu VDI.
- Počítač označený ako predloha môže byť spustený spolu s klonovanými počítačmi, čiže je možné udržiavať ho vždy aktuálny.



Klonovanie počítačov prostredníctvom nástroja hypervisor

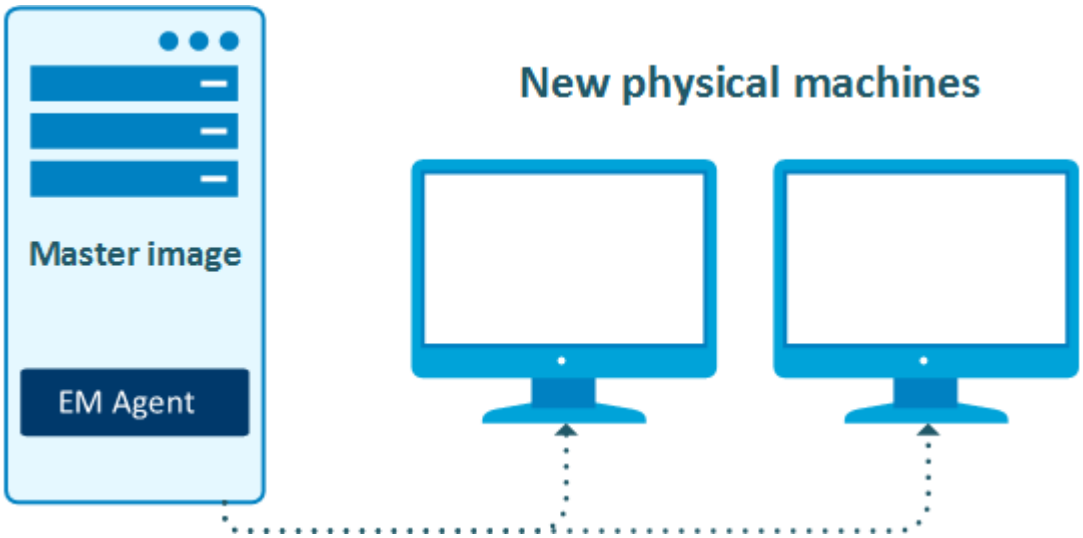
Môžete vytvoriť klon bežného počítača. Stačí počkať, kým sa zobrazí otázka, a potom ju vyriešte vybraním možnosti **Vytvoriť počítač iba teraz**.



Zavádzanie systémov na fyzické počítače z predpripravených obrazov

Pri inštalácii nových počítačov môžete použiť obraz počítača slúžiaceho ako predloha, na ktorom je už nainštalovaný ESET Management Agent verzie 7. Existujú dva spôsoby:

1. Systém vytvorí nový počítač v ESMC po každom nasadení obrazu.
   - Pri pripojení pracovnej stanice vyriešte otázku manuálne a vyberte možnosť **Vždy vytvoriť nový počítač**.
   - Predtým, ako začnete s klonovaním, označte počítač v ESMC ako predlohu. Vyberte možnosť **Označiť ako predloha pre klonovanie (vytvoriť nový počítač)**.
2. Systém vytvorí nový počítač v ESMC v prípade, ak došlo k nasadeniu obrazu na novú pracovnú stanicu. Ak sa obraz opätovne nasadí na pracovnú stanicu, ktorú už ESMC pozná (bol na nej nainštalovaný ESET Management Agent verzie 7), jej identita bude v ESMC priradená k už existujúcemu záznamu.
   - Pri pripojení pracovnej stanice vyriešte otázku manuálne a vyberte možnosť **Vždy porovnať s existujúcim počítačom**.
   - Predtým, ako začnete s klonovaním, označte počítač v ESMC ako predlohu. Vyberte možnosť **Označiť ako predloha pre klonovanie (porovnať s existujúcim počítačom)**.



Paralelná replikácia

ESMC Server dokáže rozpoznať a vyriešiť paralelnú replikáciu viacerých počítačov v ESMC pod jednou identitou. Takáto udalosť je hlásená v sekcii Podrobnosti o počítači – **Upozornenia**. Existujú dva spôsoby riešenia tejto situácie:

- Kliknite na zobrazené upozornenie a vyberte príslušnú akciu. Počítače budú rozdelené na jednotlivé identity a dôjde k trvalému vypnutiu detekcie hardvéru.
- V ojedinelých prípadoch môžu spôsobovať konflikt aj počítače, pre ktoré je detekcia hardvéru vypnutá. V takýchto prípadoch je jediným riešením spustenie úlohy pre klienta Obnoviť klonovaného agenta.
- Spustite na príslušnom počítači úlohu pre klienta Obnoviť klonovaného agenta. Vďaka tomu nebude nutné vypínať detekciu hardvéru.

3.3.1 Riešenie otázok na klonovanie

Otázka na klonovanie sa zobrazí v prípade, že ESMC Server deteguje jedno z nasledovného:

- pripájajúci sa klonovaný počítač,
- zmena hardvéru existujúceho zariadenia s nainštalovaným ESET Management Agentom.

Vždy, keď sa zariadenie pripojí k ESMC Serveru, vytvorí sa záznam z jeho hardvérového odtlačku. Tento odtlačok ostáva rovnaký aj po preinštalovaní zariadenia, čo znamená, že môže byť použitý na vyhodnotenie zhody medzi novopripojeným zariadením a zariadením pripojeným v minulosti.

Dôležité:
Detekcia hardvérového odtlačku nie je podporovaná na:

- systémoch Linux, macOS, Android a iOS,
- systémoch spravovaných pomocou komponentov ESET Virtual Agent Host (ESET Virtualization Security),
- počítačoch, na ktorých nie je nainštalovaný ESET Management Agent verzie 7.

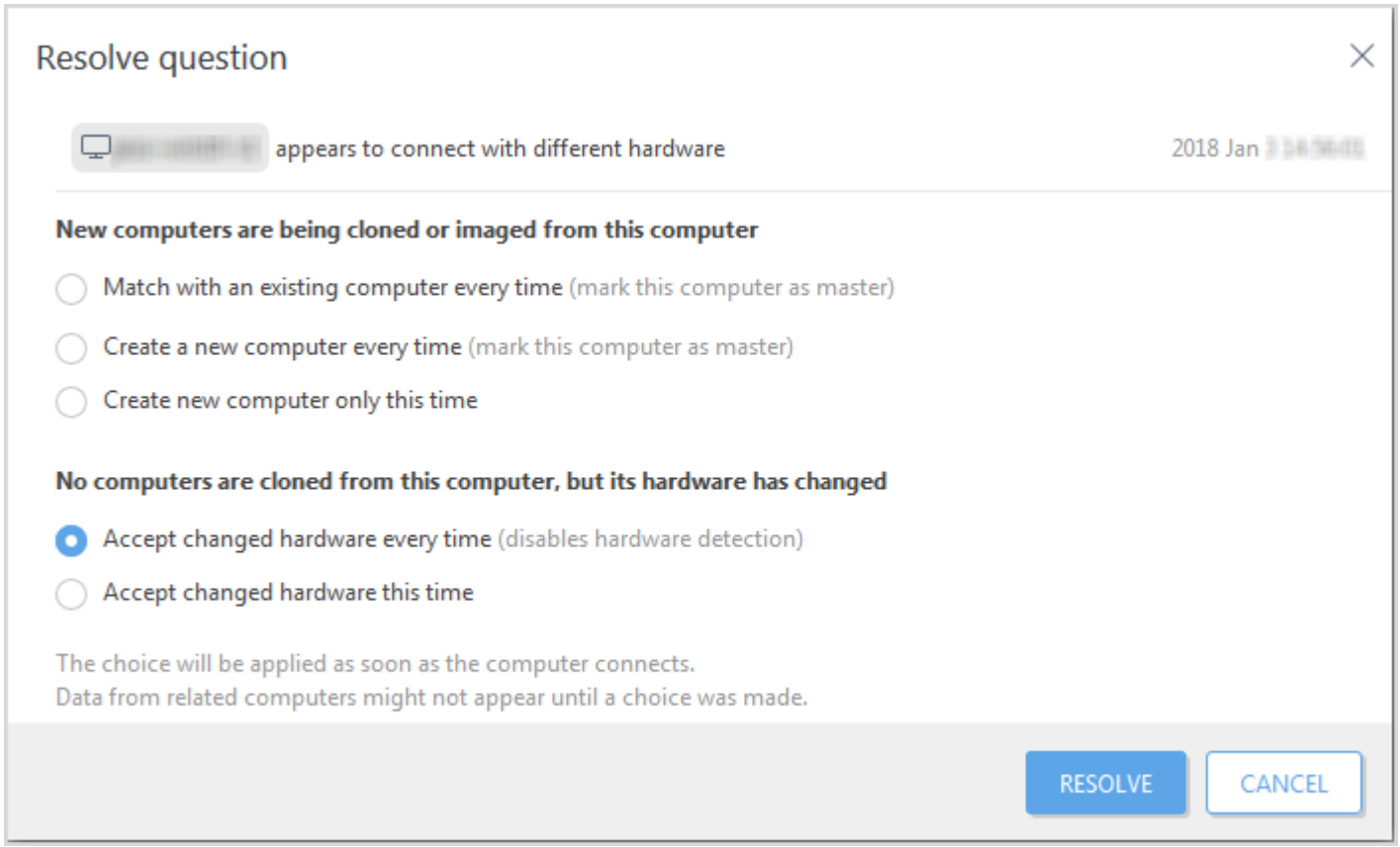
Kliknutím na otázku a označením možnosti **Vyriešiť otázku** zobrazíte ponuku s nasledujúcimi možnosťami:

Nové počítače sú klonované alebo sú vytvárané ich obrazy z tohto počítača		
Vždy porovnať s existujúcim počítačom	Túto možnosť použite v prípade, že: • používate počítač ako predlohu a všetky jeho obrazy by sa mali pripájať k existujúcemu záznamu daného počítača v ESMC, • používate počítač ako predlohu na nastavenie VDI prostredia, počítač sa nachádza vo fonde VDI a očakáva sa, že bude obnovená jeho identita na základe ID hardvérového odtlačku.	Článok databázy znalostí
Vždy vytvoriť nový počítač	Túto možnosť použite v prípade, že tento počítač používate ako obraz predlohy a chcete, aby nástroj ESMC automaticky rozpoznával všetky jeho klony ako nové počítače. Nepoužívajte túto možnosť v rámci VDI prostredí.	Článok databázy znalostí
Vytvoriť počítač iba teraz	Počítač je klonovaný iba raz. Vyberte túto možnosť, ak chcete vytvoriť novú inštanciu pre klonované zariadenie.	Článok databázy znalostí

Žiadne počítače nie sú klonované z tohto počítača, avšak jeho hardvér sa zmenil		
Vždy prijať zmeny hardvéru	Použitím tejto možnosti dôjde k permanentnému vypnutiu detekcie hardvéru na danom zariadení. Túto možnosť použite len v prípade, ak sú hlásené neexistujúce zmeny hardvéru. Túto akciu nie je možné vrátiť späť!	

Prijať zmeny hardvéru iba teraz	Vyberte túto možnosť, ak chcete obnoviť hardvérový odtlačok zariadenia. Použite ju po vykonaní zmien v hardvéri klientskeho počítača. Budúce zmeny hardvéru budú znova hlásené.

Kliknite na **Vyriešiť** pre potvrdenie zvolenej možnosti.



Situácia s dvoma agentmi

Ak je ESET Management Agent odinštalovaný (avšak počítač nie je odstránený z Web Console) na klientskom počítači a následne znova nainštalovaný, vo Web Console sa budú nachádzať dva rovnaké počítače. Na server sa však pripája len jeden z nich. Takúto situáciu nie je možné riešiť pomocou dialógového okna **Otázky**. Daná situácia je zapríčinená nesprávnym odstránením agenta. Jediným riešením je manuálne odstrániť z Web Console ten počítač, ktorý sa nepripája. História a protokoly vytvorené pred preinštalovaním budú následne stratené.

Oznámenia pre klonované počítače

Existujú tri preddefinované oznámenia, ktoré môže používateľ použiť pre zmenu hardvéru alebo akcie týkajúce sa klonovania, pričom používateľ si môže vytvoriť aj nové vlastné oznámenie pomocou udalostí súvisiacich s klonovaním. Pre nastavenie oznámenia prejdite do ponuky **Oznámenia** v rozhraní Web Console.

- **Nový počítač bol pripojený po prvýkrát** – upozornenie v prípade, že sa počítač po prvýkrát pripojil k vybranej statickej skupine (štandardne je zvolená skupina **Všetko**). Tento typ oznámenia funguje len pre ESET Management Agenty verzie 7.
- **Identita počítača obnovená** – upozornenie v prípade, že počítač bol identifikovaný na základe hardvéru. Počítač bol klonovaný zo zariadenia označeného ako predloha alebo iného známeho zdroja.
- **Bolo zachytené potenciálne klonovanie počítača alebo zmena hardvéru** – upozornenie týkajúce sa významnej zmeny hardvéru alebo klonovania v prípade, že zdrojové zariadenie nebolo v minulosti označené ako predloha.

3.3.2 Identifikácia hardvéru

ESMC zozbierava z každého zariadenia podrobnosti o jeho hardvéri a pokúša sa daný hardvér identifikovať. Každé zariadenie pripojené k ESMC patrí do jednej z nasledujúcich kategórií, ktoré sú zobrazené v stĺpci **Identifikácia hardvéru** v okne **Počítače**.

Detekcia hardvéru je zapnutá – detekcia je zapnutá a pracuje správne.

Detekcia hardvéru je vypnutá – detekcia bola vypnutá používateľom alebo automaticky ESMC Serverom.

Žiadne informácie o hardvéri – nie sú k dispozícii žiadne informácie o hardvéri, čo znamená, že na klientskom zariadení je buď nepodporovaný operačný systém, alebo stará verzia agenta.

Detekcia hardvéru je nespoľahlivá – detekcia bola nahlásená používateľom ako nespoľahlivá a bude vypnutá. Tento stav môže nastať len počas jediného intervalu replikácie pred vypnutím detekcie.

4. Používateľské rozhranie ESMC

Všetky klientske počítače sú spravované pomocou **ESMC Web Console**. Prístup do ESMC Web Console je možný z akéhokoľvek zariadenia, ktoré používa kompatibilný webový prehliadač. Rozhranie ESMC Web Console je rozdelené na niekoľko hlavných častí:

1. V hornej časti ESMC Web Console sa nachádza nástroj na **Rýchle vyhľadávanie**. Vyberte cieľ vyhľadávania kliknutím na ikonu:
   - **Názov počítača**, **Popis** a **IP adresa** – zadajte **Názov klienta** alebo **IPv4/IPv6 adresu** a stlačte **Enter**. Budete presmerovaný do sekcie Počítače, kde budú zobrazené výsledky.
   - **Názov hrozby** – budete presmerovaný do sekcie Hrozby, kde budú zobrazené výsledky.
   - **Meno používateľa** – môžete vyhľadávať importovaných používateľov AD, pričom výsledky sa zobrazia v sekcii Používatelia počítača.
2. Kliknite na tlačidlo **Rýchle odkazy** pre zobrazenie ponuky:

Rýchle odkazy
Nastaviť počítače
• Pridať počítač
• Pridať mobilné zariadenie
• Iné možnosti nasadenia
• Pridať používateľa počítača
Spravovať počítače
• Vytvoriť úlohu pre klienta
• Vytvoriť novú politiku
• Priradiť politiku
Skontrolovať stav
• Generovať správu

3. Menu na ľavej strane obsahuje hlavné sekcie nástroja ESET Security Management Center a nasledujúce položky:
   - Riadiaci panel
   - Počítače
   - Hrozby
   - Správy
   - Úlohy pre klienta
   - Inštalátory
   - Politiky
   - Používatelia počítača
   - Oznámenia
   - Prehľad stavu
   - Viac
4. Tlačidlá nachádzajúce sa v dolnej časti sú individuálne pre každú sekciu a funkciu a sú podrobne popísané v ich príslušných kapitolách.

Základné pravidlá

- Povinné nastavenia sú vždy označené červeným výkričníkom.
- Ak potrebujete pomoc pri práci s nástrojom ESET Security Management Center, kliknite na ikonu v pravom hornom rohu a následne kliknite na **<Aktuálna téma> – Pomocník**. Zobrazí sa Pomocník programu pre sekciu programu, ktorú máte otvorenú.

- Bližšie informácie nájdete v sekcii Viac.

4.1 Prihlasovacia obrazovka ESMC Web Console

Na prihlásenie do ESMC Web Console musí používateľ zadať prihlasovacie údaje (prihlasovacie meno a heslo). Je tiež možné sa prihlásiť ako doménový používateľ označením možnosti **Prihlásiť do domény** (doménový používateľ sa nevzťahuje na žiadnu namapovanú skupinu domény). Pri prihlasovaní do domény je nevyhnutné dodržať nasledujúci tvar prihlasovacieho mena: `domain\user.name`.

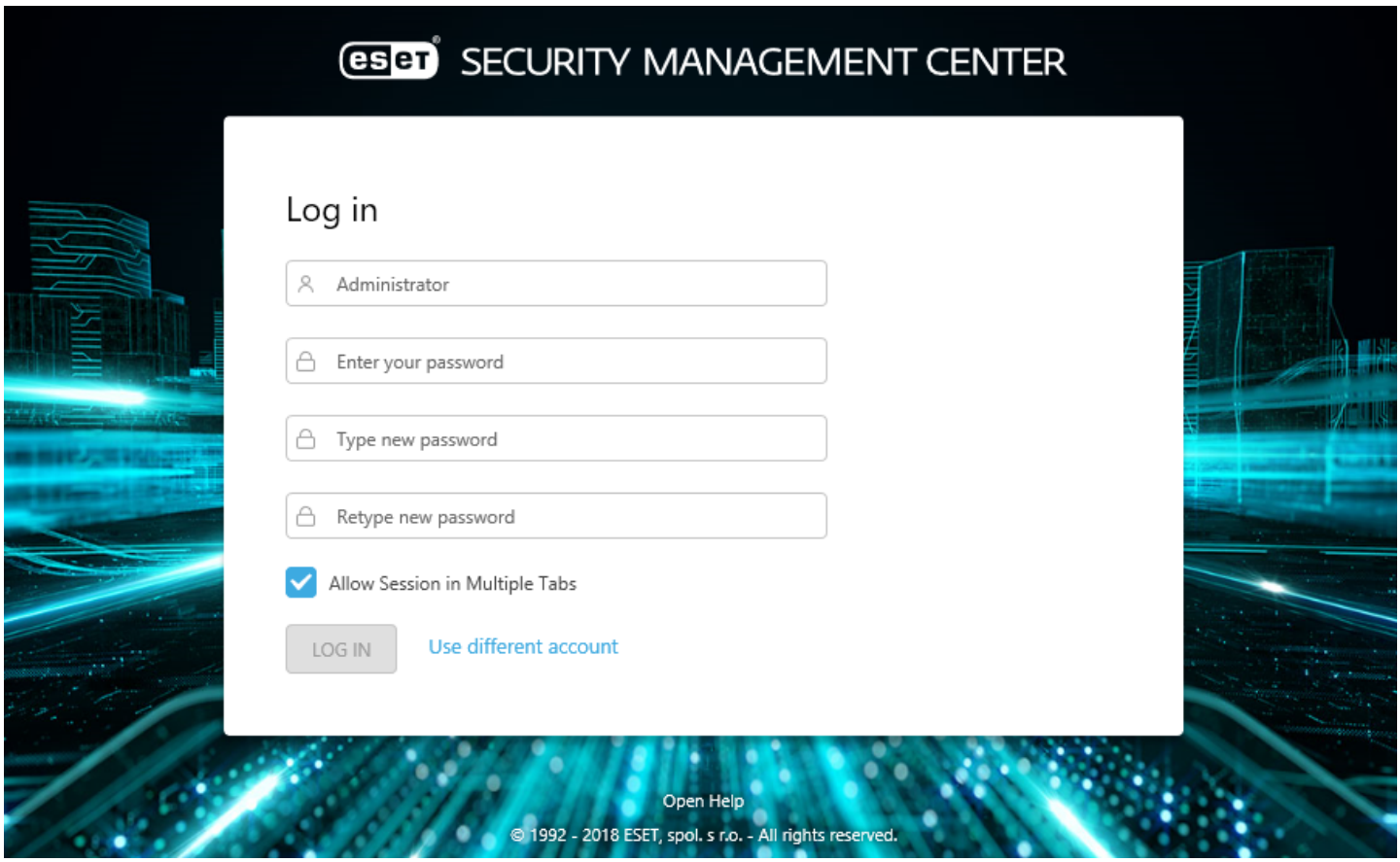
Poznámka:
Ak sa vám nedarí prihlásiť sa do ESMC Web Console alebo sa pri prihlasovaní zobrazí chybové hlásenie, pozrite si kapitolu Riešenie problémov – ESMC Web Console, kde nájdete navrhované riešenie daného problému.

Môžete si **vybrať jazyk** kliknutím na šípku roletového menu vedľa aktuálne zvoleného jazyka. Viac informácií nájdete v našom článku databázy znalostí.

Povoliť reláciu vo viacerých kartách – Web Console je možné otvoriť vo webovom prehliadači na viacerých kartách.

- Po označení tejto možnosti bude každá karta s otvorenou Web Console reláciou v jednom prehliadači pripojená k tej istej relácii. Ak sa otvorí nová karta, všetky ostatné karty pripojené s rovnakým nastavením sa pripoja k tejto novej relácii. Pri odhlásení a ukončení relácie na ktorejkoľvek karte prebehne súčasne odhlásenie aj na všetkých ostatných kartách.
- Ak daná možnosť označená nie je, na každej novej karte bude možné otvoriť samostatnú ESMC Web Console reláciu.

Zmeniť heslo/Použiť iný účet – umožňuje zmenu hesla alebo návrat späť do prihlasovacieho okna.



Správa relácií a bezpečnostné opatrenia:

Zablokovanie IP adresy po neúspešnom prihlásení

Po 10 neúspešných pokusoch o prihlásenie z rovnakej IP adresy bude ďalší prístup z tejto IP adresy dočasne zablokovaný na 10 minút. Zablokovanie IP adresy nemá vplyv na spustené relácie.

Zablokovanie IP adresy používajúcej neplatné ID relácie

Ak je 15-krát zaznamenaná nesprávna identifikácia relácie z rovnakej IP adresy, bude prístup z tejto IP adresy zablokovaný na 15 minút. Toto sa nevzťahuje na relácie, ktorých platnosť vypršala. Ak sa vo webovom prehliadači vyskytne relácia, ktorej platnosť vypršala, nie je to považované za útok. Zablokovanie IP adresy na 15 minút platí pre všetky akcie (vrátane platných požiadaviek). Zablokovanie môže byť zrušené pomocou reštartovania nástroja Web Console (`tomcat` služba).

4.1.1 Riešenie problémov – Web Console

Táto kapitola obsahuje informácie o bežných chybových hláseniach týkajúcich sa prihlasovania a zároveň poskytuje informácie o tom, ako tieto problémy riešiť.

Chybové hlásenie	Možná príčina
⚠ Prihlásenie zlyhalo: Neplatné používateľské meno alebo heslo	Uistite sa, že ste svoje prihlasovacie meno a heslo zadali správne.
⚠ Prihlásenie zlyhalo: Pripojenie zlyhalo so stavom „Nepripojený“	Skontrolujte, či je spustená služba ESMC Server a služba databázy. Podrobnejšie informácie nájdete v nasledujúcom článku databázy znalostí.
⚠ Prihlásenie zlyhalo: Chyba komunikácie	Overte si, či je služba ESMC Server spustená. Taktiež skontrolujte, či je spustená a správne funguje služba Apache Tomcat.
⚠ Prihlásenie zlyhalo: Pripojeniu vypršal časový limit	Skontrolujte sieťové pripojenie a nastavenia firewallu a uistite sa, že ESMC Web Console má prístup na ESMC Server. Môže sa tiež stať, že ESMC Server je preťažený. Skúste preto reštart. Tento problém môže nastať aj v prípade, že používate rozličné verzie ESMC Servera a ESMC Web Console.
⚠ Prihlásenie zlyhalo: Používateľ nemá priradené žiadne prístupové práva	Používateľovi neboli pridelené žiadne prístupové práva. Prihláste sa ako správca a upravte účet používateľa tak, aby mal priradenú aspoň jednu sadu povolení.
⚠ Prihlásenie zlyhalo: Chyba parsovania odpovede	Verzia nástroja Web Console a verzia ESMC Servera nie sú kompatibilné. K tomuto problému môže dôjsť počas alebo po vykonaní aktualizácie niektorého z komponentov. Ak tento problém pretrváva, nasaďte správnu verziu nástroja Web Console manuálne.
⚠ Používate nešifrované pripojenie! Upravte, prosím, konfiguráciu webového servera tak, aby používal HTTPS	Z bezpečnostných dôvodov vám odporúčame nastaviť nástroj ESMC Web Console tak, aby používal HTTPS.
JavaScript je vypnutý. Povoľte, prosím, JavaScript vo svojom prehliadači.	Povoľte JavaScript alebo aktualizujte svoj webový prehliadač.
Nezobrazuje sa prihlasovacie okno alebo sa nepretržite načítava.	Reštartujte službu ESET Security Management Center *Server*. Hneď ako sa služba ESET Security Management Center *Server* znova spustí, reštartujte službu *Apache Tomcat*. Po reštartovaní oboch služieb už bude možné načítať prihlasovacie okno ESET Security Management Center Web Console.
„Nastala neočakávaná chyba“ alebo „Vyskytla sa nezachytená výnimka“	Tento problém zvyčajne nastane vtedy, keď vstupujete do ESMC Web Console. Prečítajte si informácie

Chybové hlásenie	Možná príčina
	obsiahnuté v časti Podporované webové prehliadače a bezpečnostné produkty spoločnosti ESET.

Poznámka:
Pretože Web Console používa protokol HTTPS, môže sa vo vašom webovom prehliadači zobraziť správa o bezpečnosti certifikátu alebo nedôveryhodnom pripojení (presné znenie správy závisí od typu prehliadača). Váš webový prehliadač chce, aby ste skontrolovali identitu stránky, na ktorú sa snažíte pripojiť. Kliknite na **Pokračovať v používaní tejto webovej lokality (neodporúča sa)** (Internet Explorer) alebo **Rozumiem možným rizikám**. Kliknite na **Pridať výnimku** a potom na **Potvrdiť bezpečnostnú výnimku** (Firefox) pre umožnenie prístupu do prostredia ESMC Web Console. Toto sa vzťahuje len na situáciu, kde sa snažíte pripojiť na adresu rozhrania ESET Security Management Center Web Console.

Viac informácií o nastavení HTTPS/SSL pripojenia nájdete v našom článku databázy znalostí.

Poznámka:
Ak sa vám v niektorých častiach ESMC Web Console (napr. kontextové menu a menu Rýchle odkazy) nezobrazia všetky texty, môže to byť spôsobené doplnkom webového prehliadača, ktorý je určený na blokovanie reklamy. Pre vyriešenie tohto problému vypnite tento doplnok pre adresu ESMC Web Console.

4.2 Nastavenia používateľa

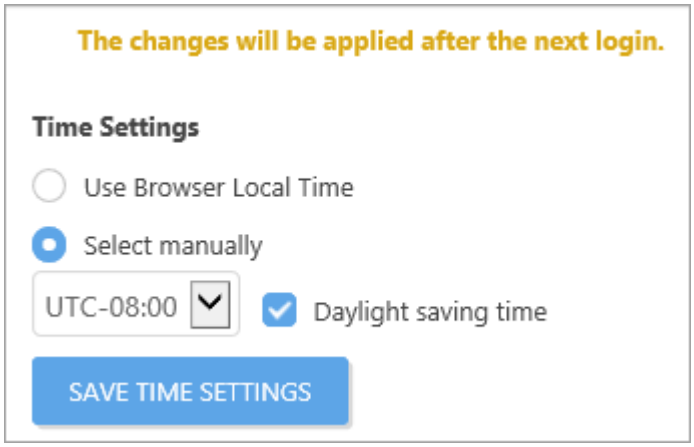
V tejto časti môžete upravovať používateľské nastavenia. Kliknutím na **Používateľský účet** v pravom hornom rohu ESMC Web Console (naľavo od tlačidla **Odhlásenie**) zobrazíte všetkých aktívnych používateľov. Do ESMC Web Console môžete byť prihlásený z rôznych webových prehliadačov, počítačov alebo mobilných zariadení súčasne. Tu uvidíte všetky svoje aktuálne relácie.

Poznámka:
Používateľské nastavenia sa vzťahujú iba na používateľa, ktorý je aktuálne prihlásený. Každý používateľ môže v rámci ESMC Web Console používať vlastné nastavenia času. Preferované nastavenia času konkrétneho používateľa sa aplikujú pre daného používateľa bez ohľadu na to, odkiaľ sa do ESMC Web Console prihlasuje.

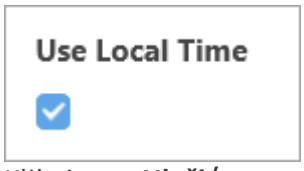
Nastavenia času:

Všetky informácie sú v rámci nástroja ESET Security Management Center uchovávané interne pomocou časového štandardu UTC (Coordinated Universal Time). Čas je z UTC formátu automaticky konvertovaný na časové pásmo používané nástrojom ESMC Web Console (pričom ohľad sa berie aj na letný čas). ESMC Web Console zobrazuje lokálny čas systému, kde je konzola spustená (nezobrazuje UTC). Nastavenie zobrazeného času môžete tiež zmeniť manuálne podľa vašich požiadaviek.

Ak chcete prepísať predvolené nastavenie **Použiť miestny čas prehliadača**, zvoľte možnosť **Vybrať manuálne**, následne manuálne zadajte časové pásmo konzoly a zvoľte, či sa má používať letný čas.



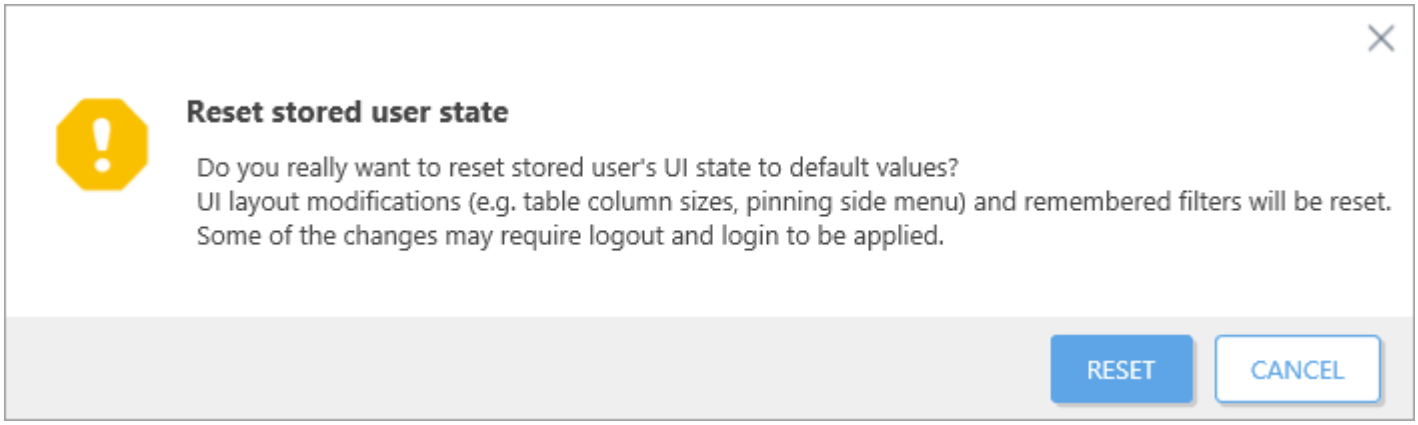
Dôležité:
V niektorých prípadoch môže byť k dispozícii aj možnosť použiť iné časové pásmo (napríklad lokálny čas klientskeho počítača, na ktorom beží ESMC). Toto nastavenie je dôležité predovšetkým pri konfigurácii spúšťačov. Ak je táto možnosť dostupná, bude zobrazená v ESMC Web Console a vy si budete môcť vybrať, či chcete **Použiť miestny čas**.



Kliknite na **Uložiť nastavenia času** pre potvrdenie zmien.

Uložený stav používateľa

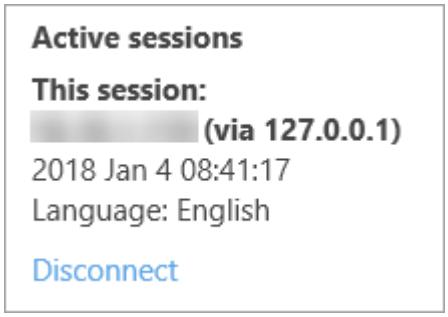
Uložený stav používateľského rozhrania môžete obnoviť kliknutím na možnosť **Obnoviť uložený stav používateľa**. Tento postup zahŕňa Sprievodcu spustením, veľkosť stĺpcov tabuľky, zapamätané filtre, pripnuté ponuky atď.



Aktívne relácie

Informácie o všetkých aktívnych reláciách aktuálneho používateľa obsahujú:

- IP adresu klientskeho počítača alebo zariadenia, z ktorého sa používateľ pripája do ESMC Web Console. V zátvorkách je ďalej uvedená IP adresa počítača, na ktorom je spustený webový server, prostredníctvom ktorého pracuje ESMC Web Console. V prípade, že nástroj ESMC Web Console je spustený na rovnakom počítači ako ESMC Server, v zátvorke bude uvedené **cez 127.0.0.1**.
- Dátum a čas prihlásenia používateľa.
- Jazyk zvolený pre ESMC Web Console.



Aktuálna relácia je označená ako **Táto relácia**. Ak chcete aktívnu reláciu ukončiť, kliknite na možnosť **Prerušiť**.

4.3 Riadiaci panel

Riadiaci panel je štandardná stránka zobrazená po prvom prihlásení používateľa do prostredia ESMC Web Console. Zobrazuje prednastavené správy o stave vašej siete. Pomocou kariet vo vrchnej časti môžete prepínať medzi jednotlivými riadiacimi panelmi. Každý panel obsahuje niekoľko oznamov.

Práca s riadiacim panelom

- **Pridať** – kliknite na ikonu + v záhlaví riadiaceho panela pre pridanie nového riadiaceho panela. Zadajte názov nového panela a potvrďte kliknutím na **Pridať riadiaci panel**. Vytvorí sa nový, prázdny riadiaci panel.
- **Presunúť** – kliknite na názov panela a podržaním tlačidla myši panel presuňte na nové miesto.
- **Prispôsobiť** – riadiace panely môžete upravovať podľa vlastných potrieb a preferencií, a to pridávaním nových správ alebo úpravou existujúcich (zmenou ich veľkosti, premiestňovaním alebo preskupovaním správ).

Kliknite na ikonu vedľa názvu **Riadiaceho panela** pre zobrazenie nasledujúcich možností v roletovom menu:

Obnoviť stránku	Obnovenie šablón správ v danom riadiacom paneli.
Zmazať	Odstránenie riadiaceho panela.
Premenovať	Premenovanie riadiaceho panela.
Duplikovať	Vytvorenie kópie riadiaceho panela s rovnakými parametrami v domácej skupine používateľa.
Zmeniť rozloženie	Výber nového rozloženia pre daný riadiaci panel. Vykonaním zmeny budú z riadiaceho panela odstránené aktuálne šablóny.

Poznámka:
Nie je možné prispôsobovať nasledujúce predvolené riadiace panely: **Prehľad** a **Prehľad incidentov**.

V ESET Security Management Center sú prednastavené nasledujúce riadiace panely:

Prehľad

Riadiaci panel **Prehľad** je štandardný riadiaci panel, ktorý sa zobrazí po každom prihlásení do ESET Security Management Center. Zobrazuje všeobecné informácie o stave vašej siete.

- **Filtre zariadení** – zobrazujú počet spravovaných zariadení na základe posledného hláseného stavu. Kliknutím na ktorúkoľvek zo štyroch dlaždíc môžete otvoriť filtrovaný zoznam zariadení.
- **Stav zariadenia** – na príslušných kartách zobrazuje počet spravovaných zariadení na základe typu nainštalovaného bezpečnostného produktu. Ak nie je nasadený žiadny bezpečnostný produkt z danej skupiny, na karte bude zobrazená možnosť nasadenia príslušného inštalačného balíka.
- **Stav pripojenia** – zobrazuje zoznam posledných pripojení spravovaných zariadení.
- **Stav verzie produktu** – zobrazuje pomer aktuálnych a zastaraných verzií bezpečnostných produktov podľa platformy.
- **Stav správy** – zobrazuje počet **spravovaných a chránených** zariadení (klientske zariadenia, na ktorých je nainštalovaný aj ESET Agent, aj bezpečnostný produkt), **spravovaných** zariadení (klientske zariadenia, kde je nainštalovaný len agent), **nespravovaných** zariadení (klientske zariadenia vo vašej sieti, ktoré síce ESMC pozná, avšak nie je na nich nainštalovaný agent) a **neautorizovaných** zariadení (klientske zariadenia, ktoré ESMC nepozná, avšak boli zachytené nástrojom Rogue Detection Sensor).
- **Informačný kanál RSS** – zobrazuje informačný kanál z **WeLiveSecurity** a z portálu **databázy znalostí spoločnosti ESET**. Ak kliknete na ikonu ozubeného kolesa v časti **Informačný kanál RSS**, môžete **vypnúť automatické prehrávania kanálov**, prípadne vypnúť konkrétny kanál.

Prehľad incidentov

Tento riadiaci panel poskytuje prehľad nevyriešených nájdených/nahlásených hrozieb za posledných 7 dní vrátane ich závažnosti, metódy detekcie a stavu riešenia, ako aj prehľad 10 počítačov/používateľov s najvyšším počtom incidentov.

Počítače

Tento riadiaci panel vám ponúka prehľad informácií o klientskych zariadeniach (ich stav ochrany, operačné systémy, stav aktualizácií a pod.).

Security Management Center Server

V tomto riadiacom paneli sú zobrazené informácie o samotnom ESET Security Management Center Serveri (zaťaženie servera, klientske zariadenia s problémami, vyťaženie procesora, pripojenia na databázu atď.).

Antivírusové hrozby

V tomto riadiacom paneli sú zobrazené informácie z antivírusových modulov pripojených bezpečnostných produktov ESET (aktívne hrozby, hrozby za posledných 7/30 dní atď.).

Hrozby firewallu

Udalosti firewallu z pripojených klientskych zariadení – zoradené podľa závažnosti, času atď.

ESET aplikácie

Tento riadiaci panel zobrazuje základné informácie o nainštalovaných produktoch od spoločnosti ESET.

Akcie v rámci správ riadiaceho panela

Zmena veľkosti panela	Kliknite na túto možnosť pre zobrazenie správy na celú šírku obrazovky.
Obnoviť	Obnovenie šablóny správy.
Zmeniť	Zmena šablóny správy na inú zo zoznamu šablón.
Upraviť šablónu správy	Úprava nastavení šablóny.
Nastaviť interval frekvencie obnovenia	Nastavenie vlastného intervalu obnovenia pre šablónu.

Naplánovať	Možnosť použitia tejto šablóny správy na naplánovanie správy.
Zmazať	Odstránenie šablóny správy z riadiaceho panela.
Premenovať	Premenovanie šablóny správy.
Táto bunka	Výber nového rozloženia pre daný riadiaci panel. Vykonaním zmeny budú z riadiaceho panela odstránené aktuálne šablóny.

Povolenia na prístup k riadiacemu panelu

Používateľ musí mať na prácu s riadiacimi panelmi pridelené príslušné povolenie. V jednotlivých paneloch môžu byť použité len šablóny správ zahrnuté v skupine, ku ktorej má používateľ pridelené prístupové práva. Pokiaľ používateľ nemá pridelené povolenia pre **Správy a riadiace panely**, nebudú sa mu v sekcii Riadiaci panel zobrazovať žiadne údaje. Správca môže predvolene vidieť všetky údaje.

Dôležité:
Povolenie na **Čítanie** – používateľ s týmto povolením si môže prezerať šablóny správ a ich kategórie. Daný používateľ tiež môže generovať správy na základe šablón správ. Môže si taktiež prezerať svoje riadiace panely.
Povolenie na **Použitie** – používateľ s týmto povolením môže upravovať vlastné riadiace panely s použitím dostupných šablón správ.
Povolenie na **Zápis** – používateľ s týmto povolením môže vytvárať, upravovať a vymazávať šablóny správ a ich kategórie.
Všetky prednastavené šablóny sú umiestnené v statickej skupine *Všetko*.

4.3.1 Zobrazenie podrobností

Pomocou riadiaceho panela môžete zobraziť podrobné informácie (agregované údaje) a vykonávať súvisiace akcie. Môžete interaktívne vyberať konkrétne položky zo súhrnu a zobraziť ich podrobnosti. Z celkového súhrnu dát v správe tak môžete prejsť na podrobnejšie informácie týkajúce sa konkrétnej položky. Detaily správy sú zväčša dostupné na viacerých úrovniach.

K dispozícii je niekoľko možností podrobného zobrazenia:

- Zobraziť **Podrobné informácie** – názov počítača a popis, názov statickej skupiny a pod. Zobrazí pôvodné (nie agregované) dáta pre vybraný riadok.
- Zobraziť **Iba „***hodnota***“** – zobrazia sa len údaje so zvolenou úrovňou závažnosti: Informácia, Kritické, Bezpečnostné riziko, Bezpečnostné oznámenie atď.
- **Rozšíriť stĺpec „***hodnota***“** – zobrazí agregované informácie (zvyčajne pre sumu, počet). Ak je napríklad v stĺpci zobrazené iba číslo a kliknete na Rozšíriť stĺpec Počítač, zobrazia sa podrobné informácie o počítačoch.
- Zobraziť **Na stránke počítačov (všetky)** – presmeruje vás do sekcie **Počítače** (vo výsledku sa zobrazí len 100 položiek).

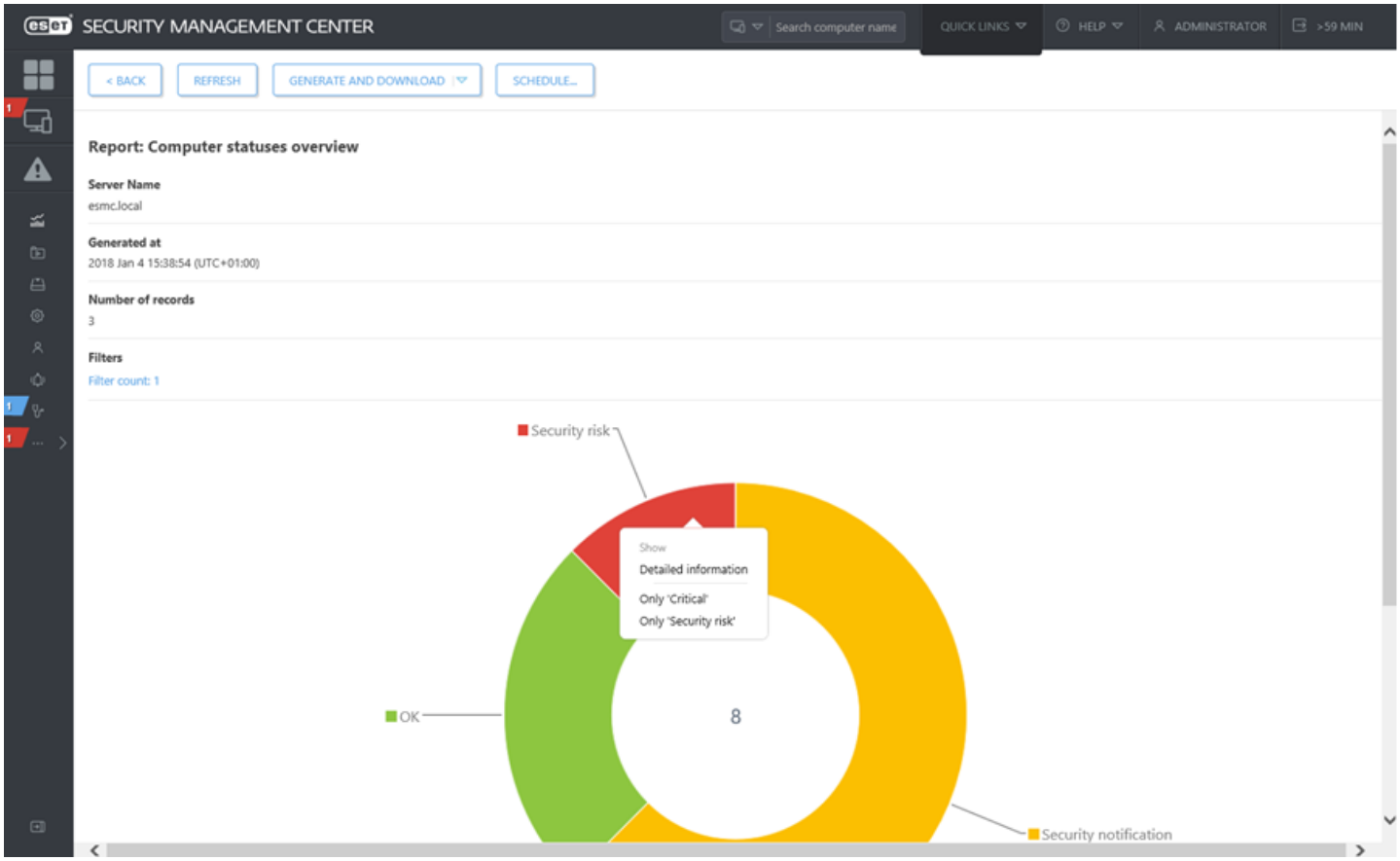
Akcie jediným kliknutím

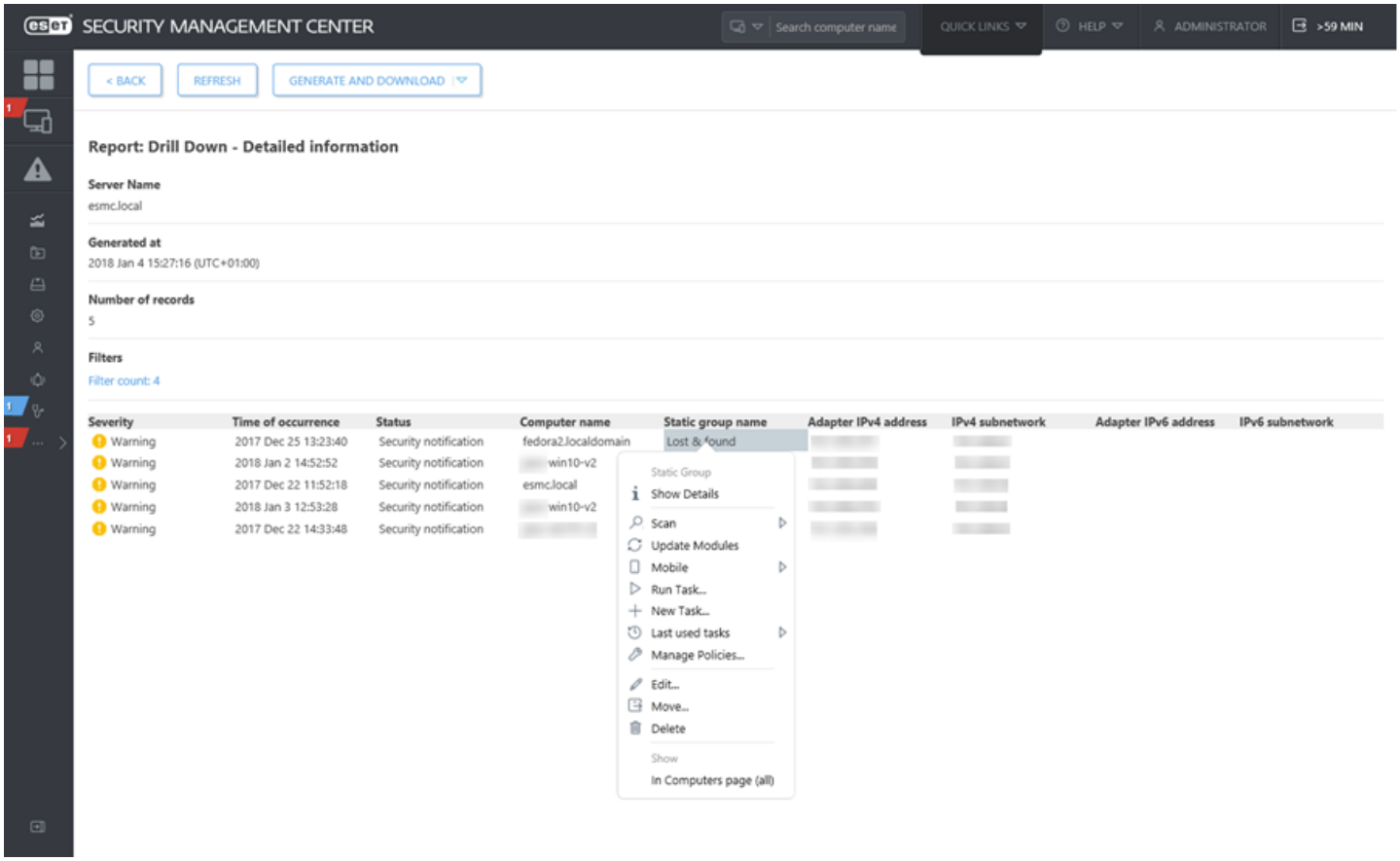
Správy s informáciami o objavených problémoch obsahujú dodatočné možnosti zobrazenia podrobností po kliknutí na položku v tabuľke/grafe:

- *„úloha pre vyriešenie označeného upozornenia“* – upozornenie môžete vyriešiť označením navrhnutej úlohy pre klienta, ktorá sa spustí hneď ako to bude možné.
  Ak upozornenie nie je možné vyriešiť úlohou pre klienta, avšak môže byť vyriešené nastavením politiky, zobrazia sa nasledujúce možnosti:
  - **Spravovať politiky**
  - **Nová politika**
- **Hľadať na webe** – pre označené upozornenie sa spustí vyhľadávanie pomocou vyhľadávača Google. Túto možnosť môžete použiť v prípade, ak nie je dostupná žiadna súvisiaca akcia pre vyriešenie označeného upozornenia (úloha pre klienta alebo nastavenie politiky).

Poznámka:
Vo výsledku zobrazených podrobností bude len prvých 1 000 položiek.

Ak chcete vygenerovať a stiahnuť správu, kliknite na tlačidlo **Vygenerovať a stiahnuť**. Dostupné sú formáty `.pdf`, `.ps` a `.csv` (len údaje tabuľky).





4.4 Počítače

Všetky klientske zariadenia, ktoré boli pridané do nástroja ESET Security Management Center, sú zobrazené tu a sú rozdelené do skupín. Každé zariadenie je zaradené do jednej statickej skupiny. Kliknutím na niektorú skupinu zo zoznamu (na ľavej strane) sa napravo zobrazia klientske počítače zaradené do danej skupiny.

Nespravované počítače (klienty v sieti, ktoré nemajú nainštalovaného ESET Management Agenta alebo bezpečnostný produkt spoločnosti ESET) sa zvyčajne zobrazujú v skupine **Stratené a nájdené**. Stav klienta, ktorý je zobrazený v ESMC Web Console, je nezávislý od nastavení bezpečnostných produktov ESET na danom kliente. To je dôvod, prečo aj v prípade, že určitý stav nie je zobrazený na kliente, je stále hlásený do ESMC Web Console. Klienty môžete presúvať medzi jednotlivými skupinami pomocou podržania tlačidla myši (drag and drop).

Počítače, zariadenia a akcie so skupinami

Prostredníctvom kontextového menu (ikona) vedľa už existujúcej skupiny môžete vytvoriť novú statickú alebo dynamickú skupinu, vytvoriť novú úlohu alebo vybrať niektorú inú z dostupných akcií.

Kliknite na tlačidlo **Pridať nové** a vyberte si z nasledujúcich možností:

- **Počítače** – počítače môžete pridať do zvolenej statickej skupiny.
- **Mobilné zariadenia** – mobilné zariadenia môžete pridať do zvolenej statickej skupiny.
- **Synchronizovať cez adresárový server** – môžete spustiť úlohu **Synchronizácia statickej skupiny**.

Kliknutím na konkrétne zariadenie otvoríte kontextové menu obsahujúce akcie, ktoré sú dostupné pre dané zariadenie. Môžete tiež označiť začiarkavacie políčko vedľa zariadenia a kliknúť na tlačidlo Akcie, ktoré sa nachádza v dolnom paneli. Menu Akcie zobrazí rôzne možnosti v závislosti od typu zariadenia. Pre bližšie informácie o rôznych typoch ikon a stavoch si pozrite Legendu ikon. Ak kliknete na číslo upozornení v stĺpci **Upozornenia**, v sekcii Podrobnosti o počítači sa zobrazí zoznam upozornení.

Filtrovanie zobrazenia

Existujú rôzne spôsoby filtrovania vášho zobrazenia:

- Štandardný filter: Ak chcete pridať viacero kritérií filtrovania, kliknite na **Pridať filter** a označte položku v zozname. Aktívne filtre sú zvýraznené modrou farbou.
- Ikony stavu vám umožňujú filtrovanie podľa závažnosti: červená – **Chyby**, žltá – **Varovania**, zelená – **OK** a sivá – **Nespravované** počítače. Tieto ikony zobrazujú aktuálny stav vašich produktov ESET na konkrétnych klientskych počítačoch. Môžete použiť aj kombináciu týchto ikon ich zapnutím alebo vypnutím. Ak si napríklad prajete zobraziť len počítače s varovaním, ponechajte označenú len žltú ikonu (ostatné ikony nesmú byť označené). Ak chcete, aby sa zobrazovali aj upozornenia, aj chyby, ponechajte zapnuté len tieto dve ikony.
- Pomocou možnosti **Pridať filter > Kategória produktov** a následným použitím roletového menu môžete zvoliť typy zariadení, ktoré budú zobrazené.
  - Možnosť **Všetky zariadenia** zobrazí všetky klientske počítače bez filtrovania. Následne môžete zoznam počítačov zúžiť použitím filtra, prípadne môžete použiť aj kombinácie filtrov.
  - **Chránené ESET produktom** – zariadenie s nainštalovaným bezpečnostným produktom od spoločnosti ESET.
  - **ESET Security Management Center** – jednotlivé ESMC komponenty, ako napríklad Agent, RD Sensor, Server atď.
  - **Iné** – zdieľaná lokálna vyrovnávacia pamäť, virtuálne zariadenie, Enterprise Inspector Agent a Enterprise Inspector Server.
- **Zobraziť podskupiny** – označte túto možnosť pre zobrazenie podskupín aktuálne zvolenej skupiny.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

Poznámka:
Ak v zozname nemôžete nájsť určitý počítač, ale s istotou viete, že vo vašej ESMC infraštruktúre sa nachádza, v prvom rade sa ubezpečte, že sú vypnuté všetky filtre.

4.4.1 Podrobnosti o počítači

Ak chcete zobraziť podrobnosti o konkrétnom počítači, vyberte klientsky počítač v statickej alebo dynamickej skupine a kliknite na **Zobraziť podrobnosti**. Z tohto okna (**Počítače**) môžete taktiež vykonať niektoré akcie kliknutím na možnosť **Počítač** v ľavom dolnom rohu.

Okno s informáciami sa skladá zo siedmich rôznych častí:

Prehľad

V tejto časti sa nachádzajú informácie, ktoré vám poskytnú ucelený prehľad aktuálneho stavu počítača.

Počítač

- Kliknutím na ikonu môžete zmeniť názov počítača, prípadne upraviť jeho popis. Ak už existuje spravovaný počítač s rovnakým názvom, môžete použiť možnosť **Povoliť duplicitné názvy**.
- **FQDN** – úplný názov domény počítača.

Poznámka:
Ak vaše klientske počítače a ESMC Server bežia pod Active Directory, môžete automaticky načítať **Názov** a **Popis** pomocou úlohy Synchronizácia statickej skupiny.

- **Nadradená skupina** – môžete zmeniť nadradenú statickú skupinu počítača.
- **IP** – IP adresa počítača.
- **Počet aplikovaných politík** – kliknite na číslo pre zobrazenie zoznamu aplikovaných politík.
- **Člen dynamických skupín** – zoznam dynamických skupín, v ktorých sa klientsky počítač nachádzal počas poslednej replikácie.

Hardvér

V tejto časti nájdete zoznam kľúčových parametrov hardvéru, informácie o operačnom systéme a unikátne identifikátory. Po kliknutí na túto dlaždicu sa zobrazí karta **Podrobnosti – Hardvér**.

Upozornenia

- **Upozornenia** – odkaz na zoznam problémov týkajúcich sa daného počítača.
- **Počet nevyriešených hrozieb** – táto položka zobrazuje počet nevyriešených hrozieb. Kliknutím na počet sa zobrazí zoznam nevyriešených hrozieb.
- **Čas posledného pripojenia** a **Čas poslednej kontroly** – informácia o čase posledného pripojenia alebo poslednej kontroly.
- **Detekčné jadro** – verzia detekčného jadra na cieľovom zariadení.
- **Aktualizovaný** – stav aktualizácie.

Produkty a licencie

V tejto časti nájdete zoznam komponentov ESET nainštalovaných na danom počítači. Po kliknutí na túto dlaždicu sa zobrazí karta **Podrobnosti – Produkty a licencie**.

Používatelia

- **Prihlásení používatelia** (iba počítače) – doména a používateľské meno prihlásených používateľov na zariadení.
- **Priradení používatelia**
  - Kliknite na možnosť **Pridať používateľa** alebo **Priradiť používateľa** pre priradenie používateľa zo sekcie Používatelia počítača k tomuto zariadeniu.
  - Ak chce zrušiť priradenie používateľa, kliknite na ikonu .
  - Ak chcete zobraziť podrobnosti účtu priradeného používateľa, kliknite na jeho používateľské meno.

Poloha (iba pre mobilné zariadenia)

Tlačidlo **Hardvér** je možné využiť v prípade, ak chcete pripraviť počítač na klonovanie. Vyžaduje sa to pri klonovaní počítačov alebo pri zmene ich hardvéru.

- **Označiť ako predloha pre klonovanie (porovnať s existujúcim počítačom)** – pre podrobnejšie informácie si pozrite možnosť **Vždy porovnať s existujúcim počítačom**. Túto možnosť odporúčame použiť pred vytvorením fondu VDI.
- **Označiť ako predloha pre klonovanie (vytvoriť nový počítač)** – pre podrobnejšie informácie si pozrite možnosť **Vždy vytvoriť nový počítač**. Túto možnosť odporúčame použiť pred vytvorením fondu VDI.
- **Vypnúť detekciu hardvéru** – trvalé vypnutie detekcie zmeny hardvéru. Túto akciu nie je možné vrátiť späť!
- **Zrušiť označenie ako predloha pre klonovanie** – pomocou tejto možnosti zrušíte označenie predlohy. Ak použijete túto možnosť, pri každom ďalšom klonovaní tohto počítača sa zobrazí otázka.

Dôležité:
Detekcia hardvérového odtlačku nie je podporovaná na:

- systémoch Linux, macOS, Android a iOS,
- systémoch spravovaných pomocou komponentov ESET Virtual Agent Host (ESET Virtualization Security),
- počítačoch, na ktorých nie je nainštalovaný ESET Management Agent verzie 7.

Konfigurácia

Konfigurácia – táto karta obsahuje zoznam konfigurácií nainštalovaných produktov ESET (ESET Management Agent, ESET Endpoint atď.). Sú dostupné tieto akcie:

- Kliknutím na tlačidlo **Požiadať o konfiguráciu** môžete vytvoriť úlohu pre ESET Management Agenta na zhromaždenie konfigurácií spravovaných produktov. Po doručení úlohy ESET Management Agentu je daná úloha okamžite vykonaná a výsledky sú doručené na ESMC Server pri ďalšom pripojení. Následne si budete môcť pozrieť zoznam konfigurácií spravovaných produktov.
- Otvorte konfiguráciu cez kontextové menu a prekonvertujte ju na politiku. Kliknite na konfiguráciu pre jej zobrazenie.
- Po otvorení konfigurácie ju môžete prekonvertovať na politiku. Kliknite na možnosť **Konvertovať na politiku** – aktuálna konfigurácia bude dostupná prostredníctvom Sprievodcu vytváraním novej politiky a vy ju budete môcť upraviť a uložiť ako novú politiku.
- Konfiguráciu si môžete stiahnuť na účely riešenia problémov. Kliknite na požadovanú konfiguráciu a následne v roletovom menu kliknite na možnosť **Stiahnuť pre diagnostiku**.

Aplikované politiky – táto karta obsahuje zoznam politík aplikovaných na daný počítač. Možnosť **Spravovať politiky** vám umožňuje spravovať, upravovať, priraďovať a odstraňovať politiky.

Protokoly (iba pre počítače)

- **SysInspector** – kliknite na možnosť **Požiadať o protokol** (iba pre systém Windows), čím spustíte na zvolených klientskych zariadeniach úlohu na Vyžiadanie SysInspector protokolu. Po dokončení úlohy pribudne v zozname konfigurácií nová konfigurácia. Kliknite na danú konfiguráciu, čím zobrazíte podrobnosti.
- **Log Collector** – kliknite na **Spustiť ESET Log Collector** pre spustenie diagnostickej úlohy. Po dokončení úlohy pribudne v zozname protokolov nový protokol. Kliknite na daný protokol, čím zobrazíte podrobnosti.
- **Diagnostické protokoly** – kliknite na možnosť **Diagnostika** > **Zapnúť** pre spustenie diagnostického režimu na aktuálnom zariadení. Pri aktívnom diagnostickom režime bude klientsky počítač odosielať všetky protokoly na ESMC Server. Všetky protokoly budú k dispozícii 24 hodín. Protokoly sú rozdelené do piatich kategórií: **protokol spamu**, **protokol firewallu**, **protokol HIPS**, **protokol správy zariadení** a **protokol webovej kontroly**.

Vykonávanie úloh

V tejto časti nájdete zoznam všetkých vykonaných úloh. Môžete použiť filter na zúženie výsledkov vyhľadávania, prejsť na detaily, upravovať, duplikovať, vymazať alebo spustiť úlohu.

Nainštalované aplikácie

V tejto časti nájdete zoznam nainštalovaných programov na klientskom zariadení vrátane informácií o verzii, veľkosti, bezpečnostnom stave atď. Pomocou nastavenia politiky môžete zapnúť nahlasovanie aplikácií, ktoré nie sú od spoločnosti ESET. Ak chcete odinštalovať niektorú aplikáciu, označte ju a kliknite na tlačidlo **Odinštalovať**. Budete vyzvaný na zadanie **Parametrov odinštalovania**. Ide o voliteľné parametre príkazového riadka pre inštalátor (inštalačný balík). Parametre odinštalovania sú unikátne pre každý inštalátor softvéru. Podrobnejšie informácie nájdete v dokumentácii pre príslušný produkt.

Ak je dostupná aktualizácia pre produkt ESET, môžete ju vykonať kliknutím na tlačidlo **Aktualizovať ESET produkty**.

Upozornenia

V tejto časti nájdete zoznam upozornení a ich podrobnosti: problém, stav, produkt, výskyt, závažnosť atď. Prístup k tomuto zoznamu je tiež možný priamo zo sekcie **Počítače**, a to kliknutím na počet upozornení v stĺpci **Upozornenia**. Upozornenia môžete vyriešiť jediným kliknutím.

Otázky (iba pre počítače)

Na karte **Otázky** nájdete zoznam otázok súvisiacich s klonovaním počítačov. Podrobnejšie informácie o riešení otázok súvisiacich s klonovanými alebo zmenenými počítačmi nájdete na nasledujúcom odkaze.

Hrozby a karanténa

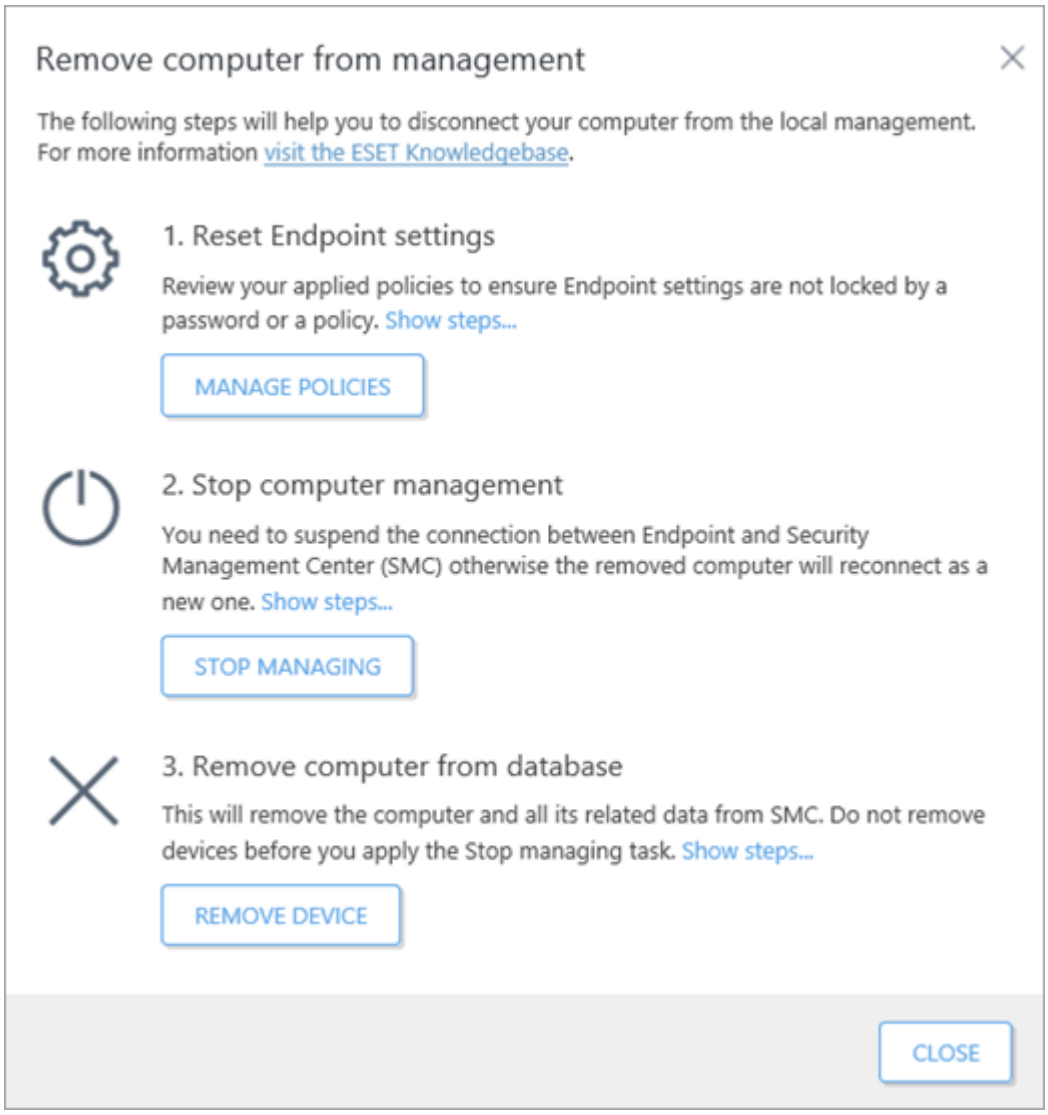
- **Hrozby** – štandardne sú zobrazené všetky typy hrozieb, ale môžete ich filtrovať podľa konkrétnych typov: **antivírus**, **firewall**, **blokované súbory**, **Enterprise Inspector** a **HIPS**.
- **Karanténa** – zoznam hrozieb umiestnených v karanténe s podrobnosťami, ako napr. názov hrozby, typ hrozby, názov objektu, veľkosť, prvý výskyt, počet, dôvod používateľa atď.

Podrobnosti

- **Základné** – informácie o spravovanom zariadení, ako napr. operačný systém, typ, verzia, sériové číslo, FQDN atď. Ďalej tu nájdete informácie o tom, či je počítač potlačený, či je spravovaný, čas poslednej aktualizácie a počet aplikovaných politík.
- **Hardvér** – informácie o hardvéri zariadenia, výrobcovi a modeli, ako aj informácie o konfigurácii siete (IPv4, IPv6, podsieť, sieťový adaptér atď.).
- **Produkty a licencie** – informácie o aktuálnej verzii detekčného jadra, verziách bezpečnostných produktov ESET nainštalovaných na zariadeniach, ako aj informácie o aktuálne používaných licenciách.

4.4.2 Odstránenie počítača zo správy

Ak chcete odstrániť zariadenie zo správy, kliknite na **Počítače**, vyberte zariadenie a kliknite na **Odstrániť**. V dialógovom okne sa zobrazia kroky potrebné na odstránenie vybraného počítača zo správy.



Dôležité:
Pred pokračovaním na ďalší krok sa uistite, že ste úspešne dokončili predchádzajúci krok. Je to dôležité pre správne odstránenie zariadenia.

1. **Vynulovať nastavenia Endpointu** – kliknite na **Spravovať politiky** a odstráňte všetky aplikované politiky, aby bolo možné spravovať lokálne zariadenie. Viac informácií nájdete v časti **Pravidlá odstraňovania politík** v kapitole **Politiky**. Ak je nastavené heslo na prístup ku konfigurácii produktu ESET určeného pre koncové zariadenia, vytvorte novú politiku na odstránenie hesla (vyberte možnosť nastavenia hesla, avšak žiadne heslo nezadávajte).
2. **Zastaviť správu počítača** – spustite úlohu **Ukončiť spravovanie** alebo odinštalujte ESMC Agenta/bezpečnostný produkt ESET lokálne na počítači. Týmto sa ukončí spojenie medzi počítačom a produktom ESMC.
3. **Odstrániť počítač z databázy** – keď ste si istý, že počítač sa už nepripája k ESMC, môžete ho odstrániť zo zoznamu spravovaných zariadení.

4.5 Hrozby

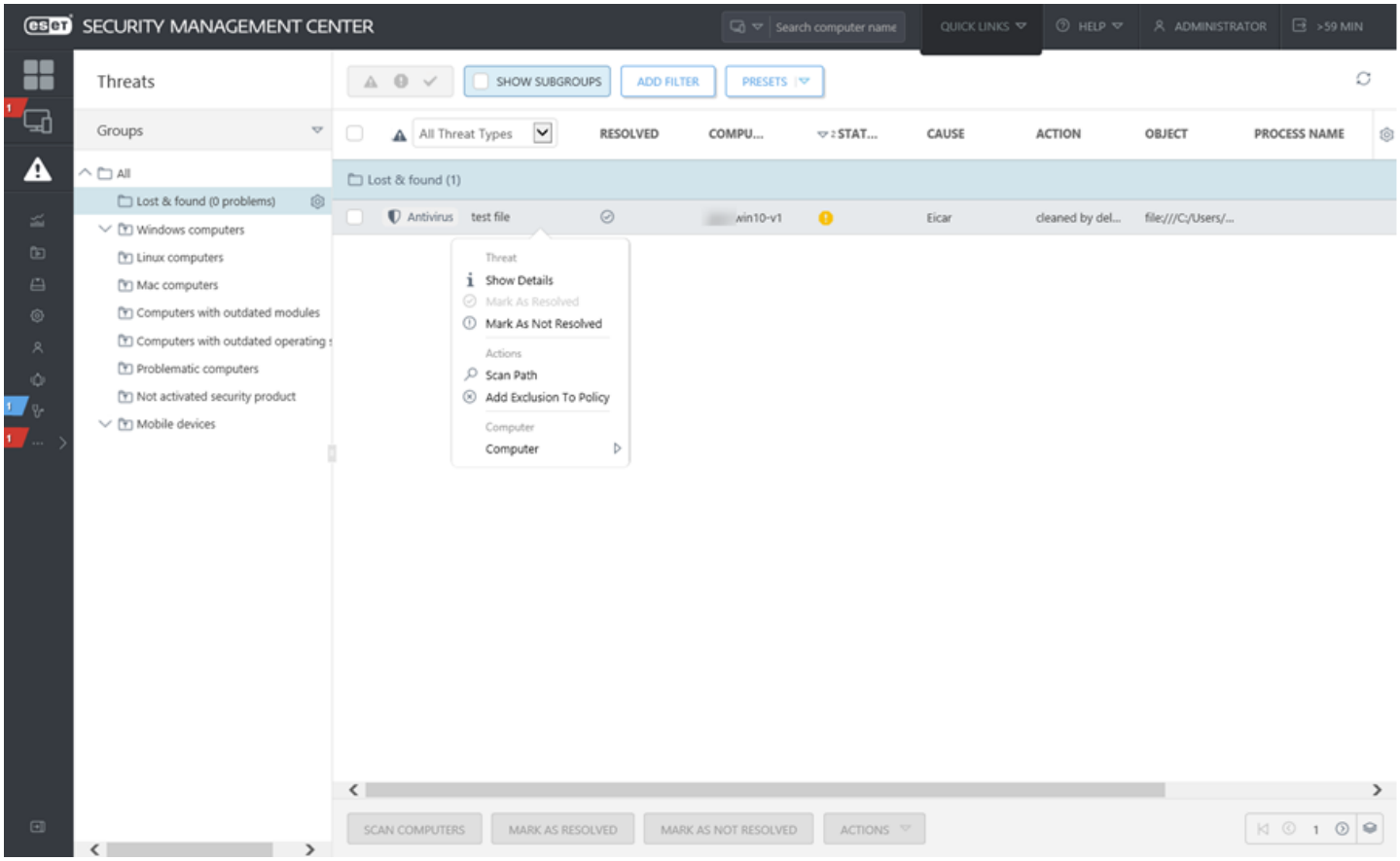
Sekcia **Hrozby** vám poskytuje prehľad hrozieb nájdených na zariadeniach spravovaných prostredníctvom vášho účtu. Na ľavej strane je zobrazená štruktúra skupín.

Môžete v nej prechádzať skupiny a zobraziť hrozby nájdené na počítačoch patriacich do danej skupiny. Pre zobrazenie všetkých hrozieb nájdených na klientoch priradených k skupinám v rámci vášho účtu kliknite na skupinu **Všetko** a použite filter **Všetky typy hrozieb**. Kliknite na konkrétnu hrozbu pre zobrazenie kontextového menu pre zariadenie, na ktorom sa našla daná hrozba.

Typy hrozieb

Aktívne hrozby – ide o hrozby, ktoré ešte neboli vyliečené. Môžu byť vyliečené spustením **Hĺbkovej kontroly** s povoleným liečením na cieľovom počítači.

Vyriešené hrozby – ide o hrozby, ktoré boli označené používateľom ako vyriešené, avšak zatiaľ neboli kontrolované pomocou **Hĺbkovej kontroly**. Zariadenia s hrozbami označenými ako vyriešené sa budú naďalej zobrazovať aj pri zapnutom filtrovaní až kým nebude vykonaná kontrola.



Filtrovanie hrozieb

Štandardne sa zobrazujú všetky typy hrozieb zachytených za posledných 7 dní vrátane hrozieb, ktoré boli úspešne vyliečené. Ak chcete pridať viacero kritérií filtrovania, kliknite na tlačidlo **Pridať filter** na hornom paneli a vyberte

jednu z položiek v zozname. Výsledky môžete filtrovať podľa položiek **Počítač potlačený**, **Hrozba vyriešená**, **Názov** (názov hrozby), **Príčina** (príčina hrozby), ďalej podľa **IP adresy** klientskeho počítača, z ktorého bola nahlásená hrozba, prípadne podľa názvu **Kontroly**. Štandardne sa zobrazujú všetky typy hrozieb, avšak pre podrobnejší náhľad môžete filtrovať podľa položiek **Antivírus**, **Blokované súbory**, **Enterprise Inspector**, **Firewall** a **HIPS**.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

Poznámka:
Niektoré filtre sú predvolene zapnuté. Ak sú na ľavom tlačidle ponuky uvedené hrozby, avšak nevidíte ich v zozname ohrození, skontrolujte, ktoré filtre sú zapnuté.

Ransomware Shield

Produkty ESET určené pre firmy (verzia 7 a novšie) obsahujú **Ransomware Shield**. Táto nová bezpečnostná funkcia je súčasťou systému HIPS a chráni počítače pred malvérom typu ransomware. Konfiguráciu **Ransomware Shield** môžete vzdialene meniť prostredníctvom ESMC Web Console cez nastavenia v **Politike** pre príslušný firemný produkt ESET. Ak na klientskom počítači dôjde k detekcii malvéru ransomware, podrobnosti o tejto detekcii si môžete zobraziť v ESMC Web Console v sekcii **Hrozby**. Viac informácií o funkcii Ransomware Shield nájdete v Online pomocníkovi pre produkt ESET Endpoint Security.

Skontrolovať počítače – táto funkcia spustí úlohu Manuálna kontrola na zariadení, ktoré nahlásilo zvolenú hrozbu.

Označiť za vyriešené/Označiť za nevyriešené – hrozby je možné označiť za vyriešené v sekcii Hrozby alebo v podrobnostiach zvoleného počítača.

Kliknutím na tlačidlo **Akcie** je možné vykonať nasledujúce akcie:

- **Spustiť úlohu** – spustenie existujúcej úlohy a vytvorenie spúšťača pre dokončenie úlohy.
- **Kontrolovať cestu** – táto akcia otvorí úlohu a prednastaví cesty a ciele. Táto možnosť je dostupná len pre hrozby, ktorých cesty sú známe.
- **Pridať vylúčenie do politiky** – vyberte existujúcu politiku pre koncové zariadenie, do ktorej chcete pridať vylúčenie pre hrozbu. Daná hrozba bude vylúčená z budúcej kontroly.

Poznámka:
Nie všetky hrozby nájdené na klientskych zariadeniach sú presunuté do karantény. Medzi hrozby, ktoré nie sú presunuté do karantény, patria:

- Hrozby, ktoré nie je možné odstrániť.
- Hrozby, ktoré sú vyhodnotené ako podozrivé na základe ich správania, ale nie sú detegované ako malvér, napríklad potenciálne nechcené aplikácie.

Podrobnosti hrozby

Ak sa chcete dozvedieť viac o konkrétnej hrozbe, kliknite na hrozbu v statickej alebo dynamickej skupine a potom kliknite na **Zobraziť podrobnosti**. Informácie budú zobrazené len pre hrozby nájdené počas kontroly. Ak chcete zobraziť filtrovaný zoznam hrozieb, ktoré boli nájdené počas rovnakej kontroly ako zvolená hrozba, kliknite na **Hrozby rovnakej kontroly**. Ak je hrozbou súbor, kliknite na **Odoslať súbor do EDTD** v časti **Podrobnosti hrozby** pre vytvorenie úlohy pre klienta, ktorá odošle súbor do ESET Dynamic Threat Defense na analýzu.

Počítače

Kliknite na hrozbu. V roletovom menu vám vedľajšie menu **Počítače** ponúka zoznam akcií, ktoré môžete vykonať na počítači, na ktorom bola nájdená hrozba. Tento zoznam je rovnaký ako zoznam v sekcii Počítače.

Stĺpce tabuľky

Kliknite na ikonu v pravom hornom rohu, zvoľte možnosť **Upraviť stĺpce** a vyberte stĺpce, ktoré chcete pridať do tabuľky. Na výber sú rôzne stĺpce, označte ich pomocou začiarkavacieho políčka.

4.5.1 Enterprise Inspector

ESET Enterprise Inspector (EEI)

ESET Enterprise Inspector (EEI) je komplexný systém detekcie a reakcie na hrozby v koncových bodoch (Endpoint Detection and Response – EDR), ktorý zahŕňa funkcie, ako napr. detekcia incidentov, manažment a reakcia na incidenty, zozbieravanie údajov, detekcia indikátorov ohrozenia, detekcia anomálií, detekcia správania, detekcia porušenia pravidiel atď. Bližšie informácie o nástroji ESET Enterprise Inspector, jeho inštalácii a funkciách nájdete v Online pomocníkovi (v anglickom jazyku).

Konfigurácia nástroja EEI

Nástroj EEI vyžaduje od ESMC nasledovné:

- Vytvorenie EEI používateľa s príslušnými povoleniami.
- Vytvorenie certifikátov, ktoré sú použité počas inštalácie EEI Servera.
- Aktivácia EEI na zariadení pripojenom k ESMC.

Poznámka:
Na aktiváciu EEI musíte mať platnú EEI licenciu.

Hlásenie hrozieb zistených nástrojom EEI v ESMC

Ak do ESMC pridáte zariadenie, na ktorom beží ESET Enterprise Inspector Agent (správne nastavený a pripojený k ESET Enterprise Inspector Serveru), EEI bude hlásiť zistené hrozby v nástroji ESMC v sekcii **Hrozby**. Takéto hrozby môžete filtrovať tak, že ako typ hrozby vyberiete **Enterprise Inspector**.

Ďalším typom hrozieb hlásených nástrojom Enterprise Inspector sú **Blokované súbory**. Ide o blokované pokusy o spustenie spustiteľných súborov, ktoré sú v rámci nástroja Enterprise Inspector označené ako nepovolené, čiže tie, ktoré sa nachádzajú v blackliste (blokované hashom súboru).

Správa hrozieb zistených nástrojom EEI v ESMC

Vďaka integrácii EEI s ESMC Web Console môžete spravovať hrozby hlásené nástrojom Enterprise Inspector priamo z ESMC Web Console bez potreby otvorenia EEI Web Console. Napríklad, ak označíte hrozbu ako vyriešenú v ESMC Web Console, bude zároveň označená rovnako aj v EEI Web Console.

Poznámka:
Ak vyriešite hrozby priamo v rozhraní EEI Web Console, budú označené ako vyriešené takisto v ESMC Web Console.

Pre umožnenie správy hrozieb zistených nástrojom Enterprise Inspector v rozhraní ESMC Web Console je nutné splniť nasledujúce systémové požiadavky:

- ESMC verzie 7 a novších verzií.
- Na spravovanom počítači musí byť nainštalovaný produkt ESET určený pre koncové zariadenia (ESET Endpoint Antivirus, ESET Endpoint Security) verzie 7 a novších verzií.

Poznámka:
ERA 6.5 zobrazuje hrozby hlásené nástrojom ESET Enterprise Inspector, avšak neposkytuje možnosť spravovať ich (označiť ich ako vyriešené).

4.6 Správy

Správy vám umožňujú pohodlný prístup k dátam z databázy a ich filtrovanie. Okno správ pozostáva z 2 kariet:

- **Kategórie a šablóny** – toto je predvolená karta pre sekciu **Správy**. Obsahuje prehľad kategórií správ a šablón. Môžete tu vytvoriť nové správy a kategórie alebo vykonať iné akcie týkajúce sa správ.
- **Naplánované správy** – táto karta poskytuje prehľad naplánovaných správ. Okrem toho tu môžete naplánovať novú správu.

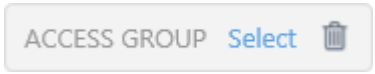
Správy sú generované zo šablón, ktoré sú kategorizované podľa typu správy. Správa môže byť vygenerovaná okamžite alebo môže byť naplánovaná na neskoršie vygenerovanie. Ak chcete vygenerovať a zobraziť správu okamžite, kliknite na **Generovať teraz** vedľa požadovanej šablóny správy. Môžete použiť vopred vytvorené šablóny správ zo zoznamu Kategórie a šablóny alebo môžete vytvoriť novú šablónu s vlastnými nastaveniami. Pre spustenie sprievodcu šablónami správ a špecifikovanie vlastných nastavení pre novú správu kliknite na možnosť Nová šablóna správy. Môžete tiež vytvoriť novú kategóriu správ (**Nová kategória**) alebo importovať šablóny správ exportované v minulosti (**Importovať šablóny správ**).

Vyhľadávanie správ

V hornej časti okna sa nachádza panel vyhľadávania. Môžete vyhľadávať názvy kategórií a šablón, nie však popisy. Kliknutím na šípky vedľa panelu vyhľadávania môžete komprimovať alebo rozbaliť všetky kategórie správ.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Používanie šablón správ

Vyberte šablónu správy a kliknite na šípku umiestnenú na dlaždici. Na výber sú tieto možnosti:

Generovať teraz	Následne bude vytvorená správa a vy si môžete prezrieť výstupné dáta.
Stiahnuť	Vyberte šablónu správy, kliknite na **Stiahnuť** a zvoľte želaný formát súboru – `.pdf`, `.ps` alebo `.csv` (formát `.csv` je vhodný len pre dáta tabuľky). Vygeneruje sa správa a následne bude stiahnutá.
Naplánovať	Naplánovať správu – otvorí sa okno, v ktorom môžete upravovať spúšťač plánovanej správy, kritéria pre potlačenie spúšťača a doručenie správy. Všetky naplánované správy sa zobrazia po kliknutí na kartu **Naplánované správy**.
Upraviť	Úprava už existujúcej šablóny správy. Na túto možnosť sa vzťahujú rovnaké nastavenia ako pri vytváraní novej šablóny správy.
Duplikovať	Duplikovanie umožňuje vytvoriť novú správu na základe označenej správy, pričom je nevyhnutné zadať pre duplikát nový (odlišný) názov.

Vymazať	Úplné odstránenie vybranej šablóny správy.
Exportovať	Šablóna správy bude exportovaná v podobe súboru `.dat`.

Používanie kategórií šablón

Zvoľte kategóriu správ a kliknite na ikonu v dolnom pravom rohu kategórie. Na výber sú tieto možnosti:

Nová kategória	Zadajte **Názov** pre novú kategóriu šablóny správy.
Nová šablóna správy	Vytvorenie novej, vlastnej šablóny správy.
Vymazať	Úplné odstránenie vybranej kategórie šablóny správy.
Upraviť	Premenovanie existujúcej kategórie šablóny správy.
Exportovať	Kategória šablóny správy a všetky obsiahnuté šablóny budú exportované v podobe súboru `.dat`. Neskôr môžete importovať kategóriu vrátane všetkých šablón pomocou možnosti **Importovať šablóny správ**. Toto je užitočné napríklad v prípade, keď chcete migrovať svoje vlastné šablóny správ na iný ESMC Server.
Prístupová skupina	Umožňuje presunúť kategóriu šablóny správy do inej statickej skupiny. Ku kategórii tak bude mať prístup lokálny správca danej cieľovej skupiny. Lokálny správca má vo svojej skupine plné prístupové práva.

Dôležité:
Funkcia **Import**/ **Export** je určená iba na importovanie a exportovanie šablón správ, nie na importovanie alebo exportovanie vygenerovanej správy obsahujúcej dáta.

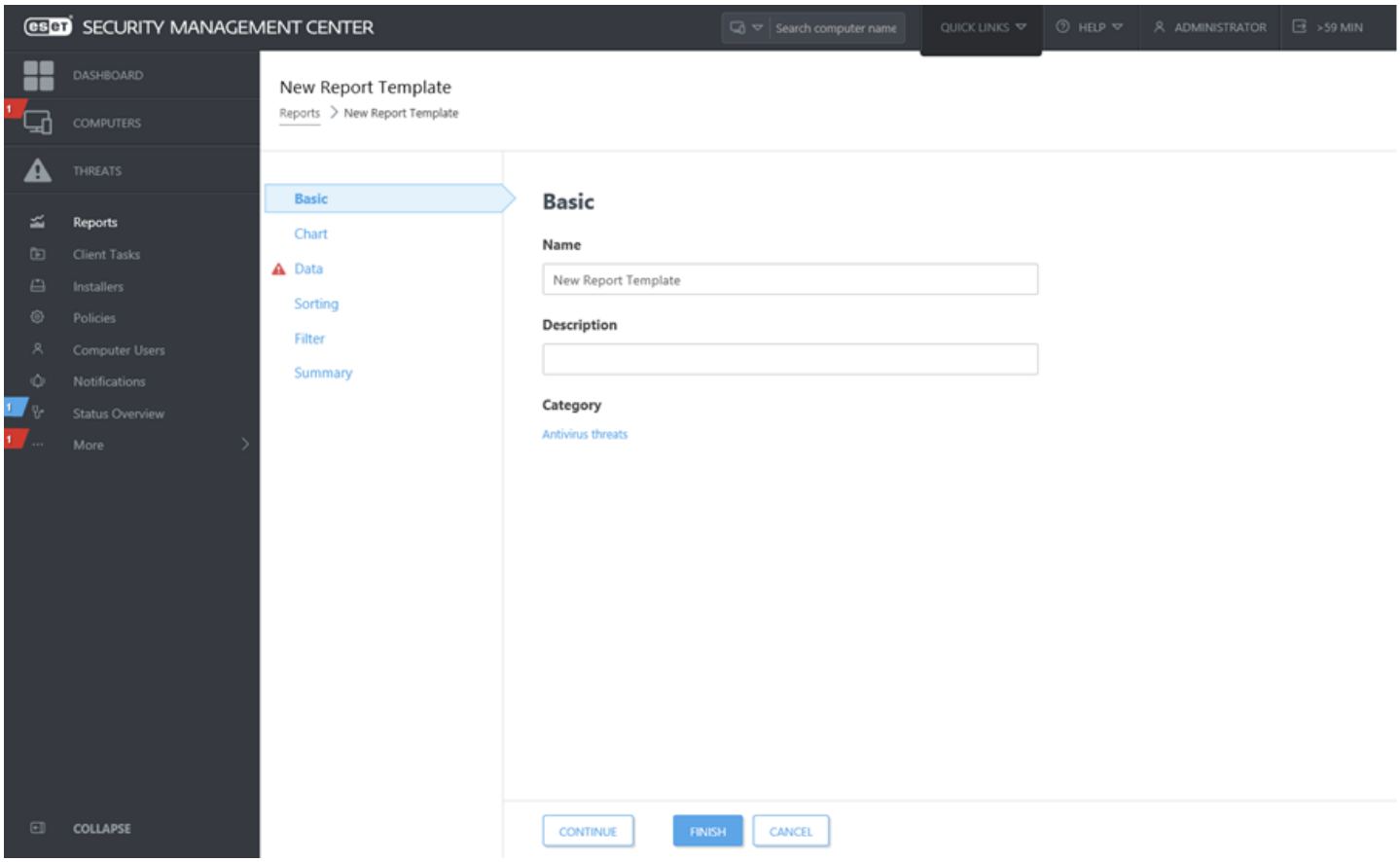
Povolenia na prístup k správam

Správy sú statické objekty, ktoré sa nachádzajú v štruktúre objektov v ESMC databáze. Každá nová šablóna správy bude uložená do domácej skupiny používateľa, ktorý ju vytvoril. Na prístup k správe sú potrebné povolenia. Taktiež sú potrebné povolenia na prístup k objektom, ktorých sa správa týka. Napríklad, ak generujete správu **Prehľad stavov počítačov**, budú sa v nej nachádzať len dáta z počítačov, kde máte povolenia na **Čítanie**.

Dôležité:
Povolenie na **Čítanie** – používateľ s týmto povolením si môže prezerať šablóny správ a ich kategórie. Daný používateľ tiež môže generovať správy na základe šablón správ. Môže si taktiež prezerať svoje riadiace panely.
Povolenie na **Použitie** – používateľ s týmto povolením môže upravovať vlastné riadiace panely s použitím dostupných šablón správ.
Povolenie na **Zápis** – používateľ s týmto povolením môže vytvárať, upravovať a vymazávať šablóny správ a ich kategórie.
Všetky prednastavené šablóny sú umiestnené v statickej skupine *Všetko*.

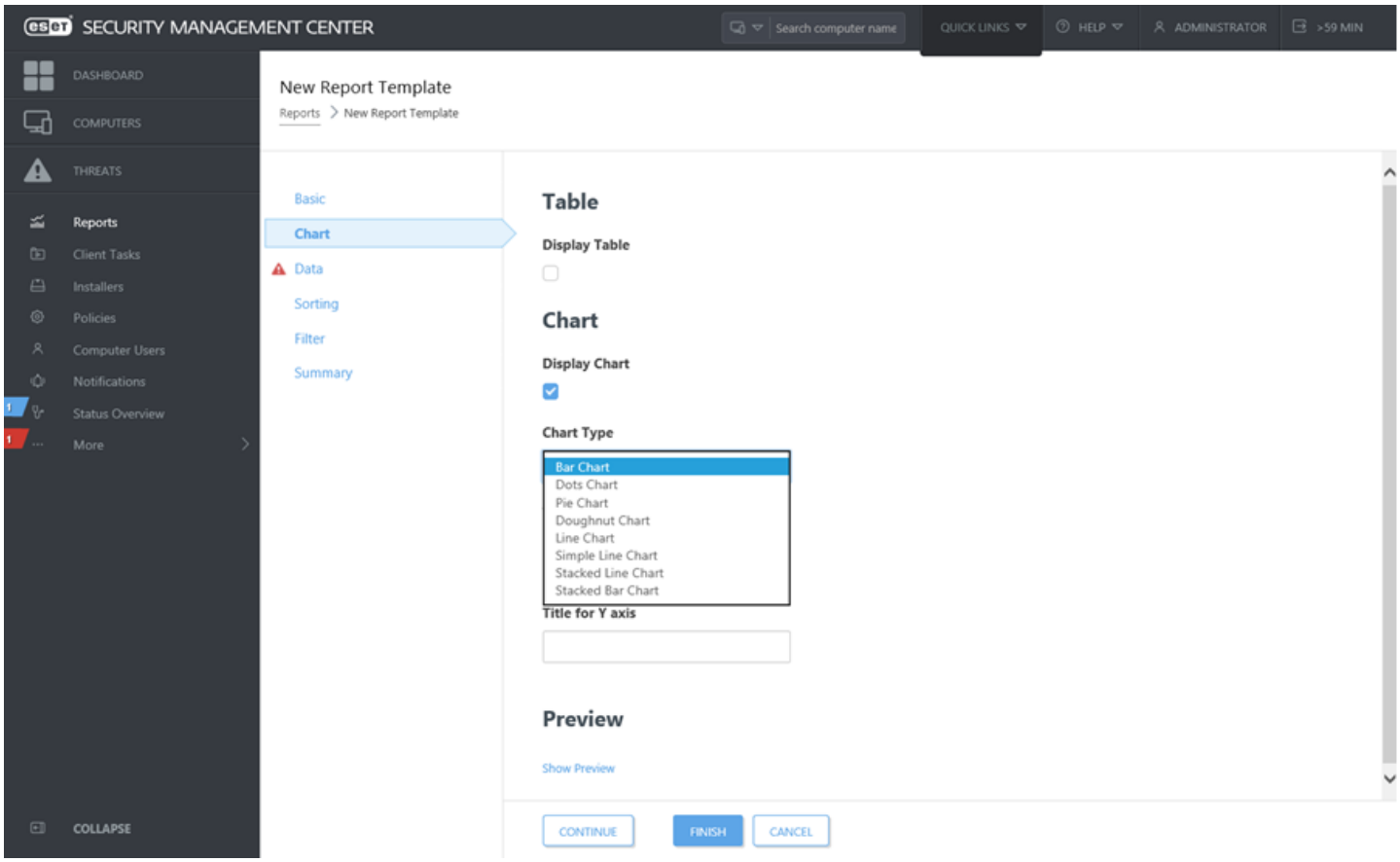
4.6.1 Vytvorenie novej šablóny správy

Prejdite do sekcie **Správy** a kliknite na tlačidlo **Nová šablóna správy**.



Základné

Upravte základné informácie o šablóne. Zadajte **Názov**, **Popis** a **Kategóriu**. Na výber sú len prednastavené kategórie. Vytvoriť novú kategóriu je možné pomocou možnosti **Nová kategória**, ktorá bola spomenutá v predchádzajúcej kapitole.



Graf

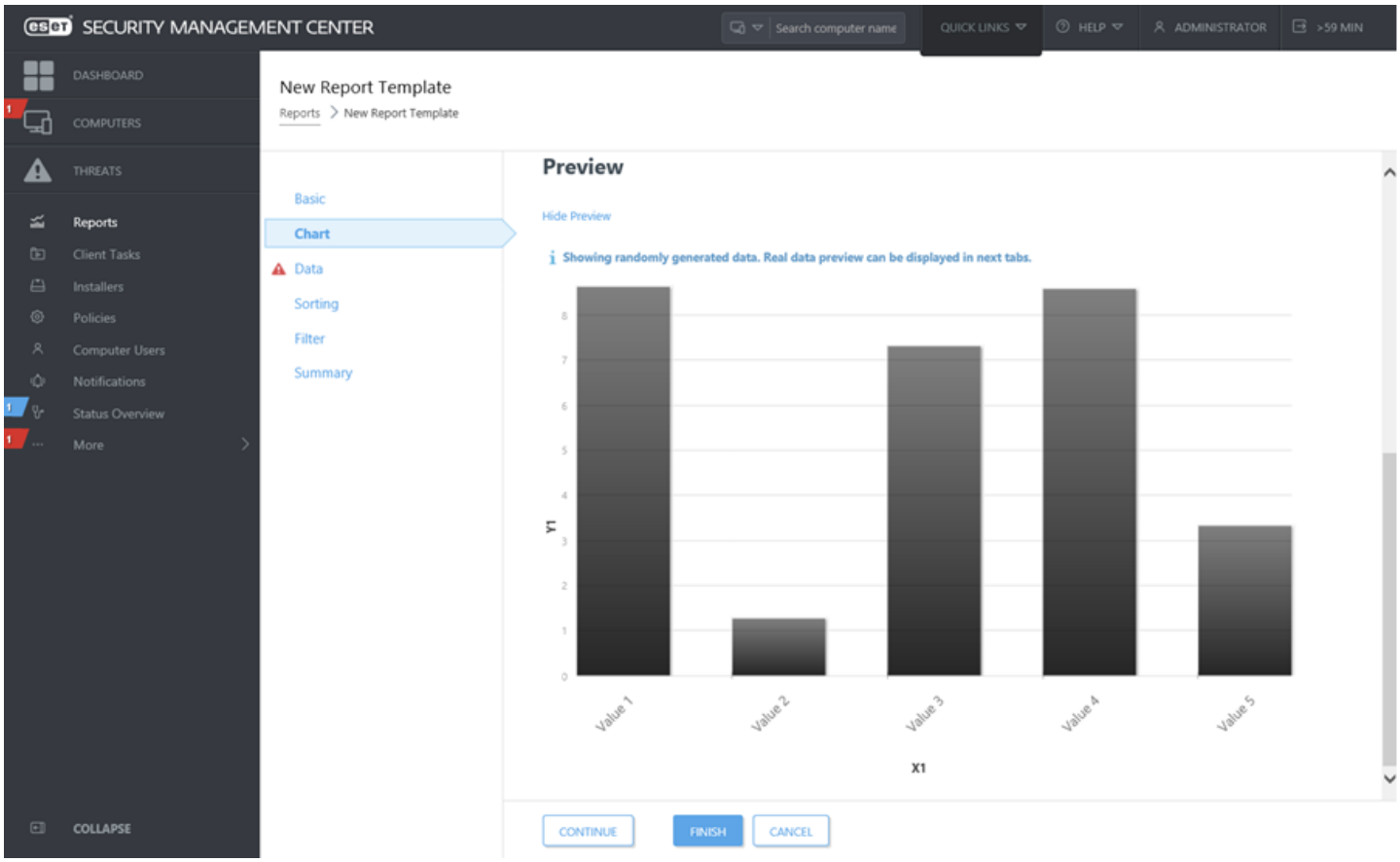
V sekcii **Graf** vyberte typ **Správy**. Môže to byť buď **Tabuľka**, v ktorej sú dáta rozdelené do riadkov a stĺpcov, alebo **Graf**, ktorý tvoria osi X a Y.

Poznámka:
Vybraný typ grafu bude zobrazený v sekcii **Ukážka**. Vďaka tomu môžete okamžite vidieť, ako bude správa vyzerať.

Možnosť **Graf** vám ponúka niekoľko nastavení:

- **Pruhový graf** – graf s obdĺžnikovými stĺpcami.
- **Bodový graf** – v tomto type grafu sú použité na zobrazenie hodnôt bodky (podobne ako pri stĺpcovom grafe).
- **Koláčový graf** – je to kruhový graf proporčne rozdelený na časti podľa príslušných hodnôt.
- **Prstencový graf** – podobný ako koláčový, môže však obsahovať rôzne typy dát.
- **Čiarový graf** – zobrazuje dáta v dátových bodoch spojených rovnými čiarami.
- **Jednoduchý čiarový graf** – zobrazuje dáta pomocou čiar, nezobrazuje dátové body.
- **Skladaný čiarový graf** – tento graf použite v prípade, ak potrebujete analyzovať dáta s rozdielnymi mernými jednotkami.
- **Skladaný pruhový graf** – podobný ako jednoduchý pruhový graf, môže však obsahovať rôzne typy dát s rozdielnymi mernými jednotkami.

Môžete prípadne zadať názvy pre osi **X** a **Y** pre zjednodušenie čítania grafov a celkovej orientácie v grafe.



Dáta

V sekcii **Dáta** si vyberte, ktoré údaje chcete zobraziť:

a. **Stĺpce tabuľky**: Dáta sú do tabuľky pridávané automaticky podľa zvoleného typu správy. Môžete upraviť **Názov**, **Označenie** a **Formát**.
b. **Osi grafu**: Zvoľte dáta pre osi **X** a **Y**. Po kliknutí na **Pridať os** sa otvorí okno s možnosťami. Možnosti dostupné pre os **Y** vždy závisia od možností vybraných pre os **X** a naopak, pretože graf zobrazuje ich vzájomný vzťah a dáta musia byť kompatibilné. Vyberte potrebné dáta a kliknite na **OK**.

Formát

Pre zobrazenie rozšírených možností formátovania kliknite na symbol ⤢ v sekcii **Dáta**.Môžete tiež zmeniť **Formát**, v ktorom sú dáta zobrazené, ako aj nastaviť formátovanie pre **Stĺpce tabuľky** a **Osi grafu**. Nie všetky možnosti sú dostupné pre každý typ dát.

Formátovať stĺpec	Vyberte stĺpec, podľa ktorého bude formátovaný aktuálny stĺpec. Napríklad pri formátovaní stĺpca **Názov** vyberte stĺpec **Závažnosť**, aby ste pridali ikony závažnosti vedľa názvov.
Minimálna hodnota	Nastavte minimálny limit pre zobrazované hodnoty.
Maximálna hodnota	Nastavte maximálny limit pre zobrazované hodnoty.
Farba	Vyberte farebnú schému pre stĺpec. Farba sa nastaví podľa hodnoty stĺpca vybraného v časti **Formátovať stĺpec**.
Ikony	Pridajte ikony do formátovaného stĺpca podľa hodnoty nastavenej v časti **Formátovať stĺpec**.

Kliknite na jednu zo šípok ↓ ↑ pre zmenu poradia stĺpcov.

Zoradenie

Ak dáta vybrané v sekcii **Dáta** obsahujú symbol zoradenia, je k dispozícii zoradenie. Na definovanie vzťahu medzi vybranými dátami použite možnosť **Pridať zoradenie**. Vyberte počiatočné dáta (hodnotu zoradenia) a metódu zoradenia, buď **Vzostupne**, alebo **Zostupne**. Určíte tak výsledok zobrazený v grafe. Pre zmenu poradia zoraďovacích prvkov kliknite na **Hore** alebo **Dole**. Pre odstránenie konkrétneho prvku z výberu kliknite na ikonu odpadkového koša .

Filter

Nastavte metódu filtrovania. Kliknite na **Pridať filter**, vyberte filtrovací prvok zo zoznamu a zadajte jeho hodnotu. Určíte tak, aké dáta budú zobrazené v grafe. Pre odstránenie konkrétneho prvku z výberu kliknite na ikonu odpadkového koša .

Súhrn

V sekcii **Súhrn** skontrolujte vybrané nastavenia a údaje. Kliknite na **Dokončiť** pre vytvorenie novej Šablóny správy.

4.6.2 Generovanie správy

Vygenerovať správu podľa šablóny správy je možné troma spôsobmi:

- Prejdite do ponuky **Rýchle odkazy** na hornom paneli a kliknite na možnosť **Generovať správu**. Vyberte si zo zoznamu šablónu správy a kliknite na **Generovať teraz**.
- Kliknite na **Správy** a prejdite na kartu **Kategórie a šablóny**. Vyberte šablónu správy, z ktorej chcete vygenerovať správu. Kliknite na ikonu ozubeného kolesa a následne kliknite na možnosť **Upraviť**, ak chcete vykonať zmeny v rámci šablóny.
  - Možnosť **Generovať teraz** vám umožňuje vygenerovať a zobraziť správu v ESMC Web Console. Po vygenerovaní správy môžete kliknúť na **Vygenerovať a stiahnuť** a následne uložiť správu v požadovanom formáte.
- Kliknite na **Viac** > **Úlohy pre server** > **Nová** pre vytvorenie novej úlohy generovania správy.
  - Úloha bola vytvorená a je zobrazená v zozname **Typy úloh**. Označte túto úlohu a kliknite na možnosť **Vykonať teraz** v dolnej časti obrazovky. Úloha bude okamžite vykonaná.
  - Upravte nastavenia (podľa návodu v sekcii Generovanie správy) a kliknite na **Dokončiť**.

Poznámka:
Ak kliknete na položku zobrazenú v správe nachádzajúcej sa v ESMC Web Console, zobrazí sa ďalšia ponuka s dodatočnými nastaveniami.

4.6.3 Naplánovanie generovania správy

Naplánovať generovanie správy je možné troma spôsobmi:

- Prejdite do sekcie **Viac** > **Úlohy pre server**. Kliknite na možnosť **Nová** pre vytvorenie novej úlohy **generovania správy**.
- Prejdite do sekcie **Správy**, vyberte šablónu správy, z ktorej chcete vygenerovať správu, kliknite na šípku umiestnenú na dlaždici šablóny a vyberte možnosť **Naplánovať**. Môžete použiť a upraviť predvolenú šablónu správy alebo vytvoriť novú šablónu správy.
- Kliknite na možnosť **Naplánovať** v kontextovom menu šablóny správy v riadiacom paneli.
- Prejdite do sekcie **Správy** > karta **Naplánované správy** a kliknite na možnosť **Naplánovať**.

V rámci plánovania správy máte k dispozícii viacero nastavení, ktoré sú bližšie špecifikované v úlohe Generovať správu:

- Pre jednu správu môžete zvoliť aj viacero šablón.
- Môžete nastaviť parametre spúšťača a obmedzovania.
- Doručenie správy je možné buď prostredníctvom e-mailu, alebo uložením do súboru.

Po naplánovaní správy kliknite na **Dokončiť**. Úloha bola vytvorená a bude spustená v intervale, ktorý je definovaný tu (raz alebo opakovane).

Karta Naplánované správy

Svoje naplánované správy si môžete skontrolovať v sekcii **Správy** > **Naplánované správy**. Ostatné akcie dostupné na tejto karte sú zobrazené nižšie:

Naplánovať	Vytvorenie nového naplánovania pre existujúcu správu.
Zobraziť podrobnosti	Zobrazia sa podrobné informácie o vybranom naplánovaní.
Vykonať teraz	Okamžité vykonanie naplánovanej správy.
Upraviť	Úprava naplánovania správy. Môžete pridať alebo odobrať šablóny správ, upraviť nastavenia naplánovania, alebo zmeniť nastavenia obmedzenia a doručenia správy.
Duplikovať	Vytvorenie duplicitného naplánovania vo vašej domácej skupine.
Vymazať	Odstránenie naplánovania. Šablóna správy nebude vymazaná.
Prístupová skupina	Premiestnenie naplánovania do inej prístupovej skupiny.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.6.4 Neaktuálne aplikácie

Ak chcete zistiť, ktoré komponenty ESMC nie sú aktuálne, použite správu **Neaktuálne aplikácie**.

Sú na to dva spôsoby:

- Pridajte nový riadiaci panel alebo upravte niektorý z existujúcich.
- Prejdite do sekcie **Správy** > **Počítače** > **Neaktuálne aplikácie** a kliknite na **Generovať teraz**.

V prípade, že ste našli neaktuálne aplikácie, môžete:

- použiť úlohu pre klienta Aktualizácia súčastí Security Management Center na aktualizáciu ESET Management Agenta, Servera a MDM,
- použiť úlohu pre klienta Inštalácia softvéru na aktualizáciu svojho bezpečnostného produktu.

4.6.5 Zobrazovač SysInspector protokolov

Pomocou zobrazovača SysInspector protokolov si môžete prezerať protokoly z nástroja SysInspector po tom, ako bol spustený na klientskom počítači. SysInspector protokoly môžete otvoriť aj priamo pomocou úlohy na vyžiadanie SysInspector protokolu. Protokoly môžu byť stiahnuté a zobrazené pomocou nástroja SysInspector na vašom lokálnom počítači.

Poznámka:
SysInspector protokoly môžu byť vyžiadané len na klientoch s operačným systémom Windows.

Ako zobraziť SysInspector protokol

Z riadiaceho panela

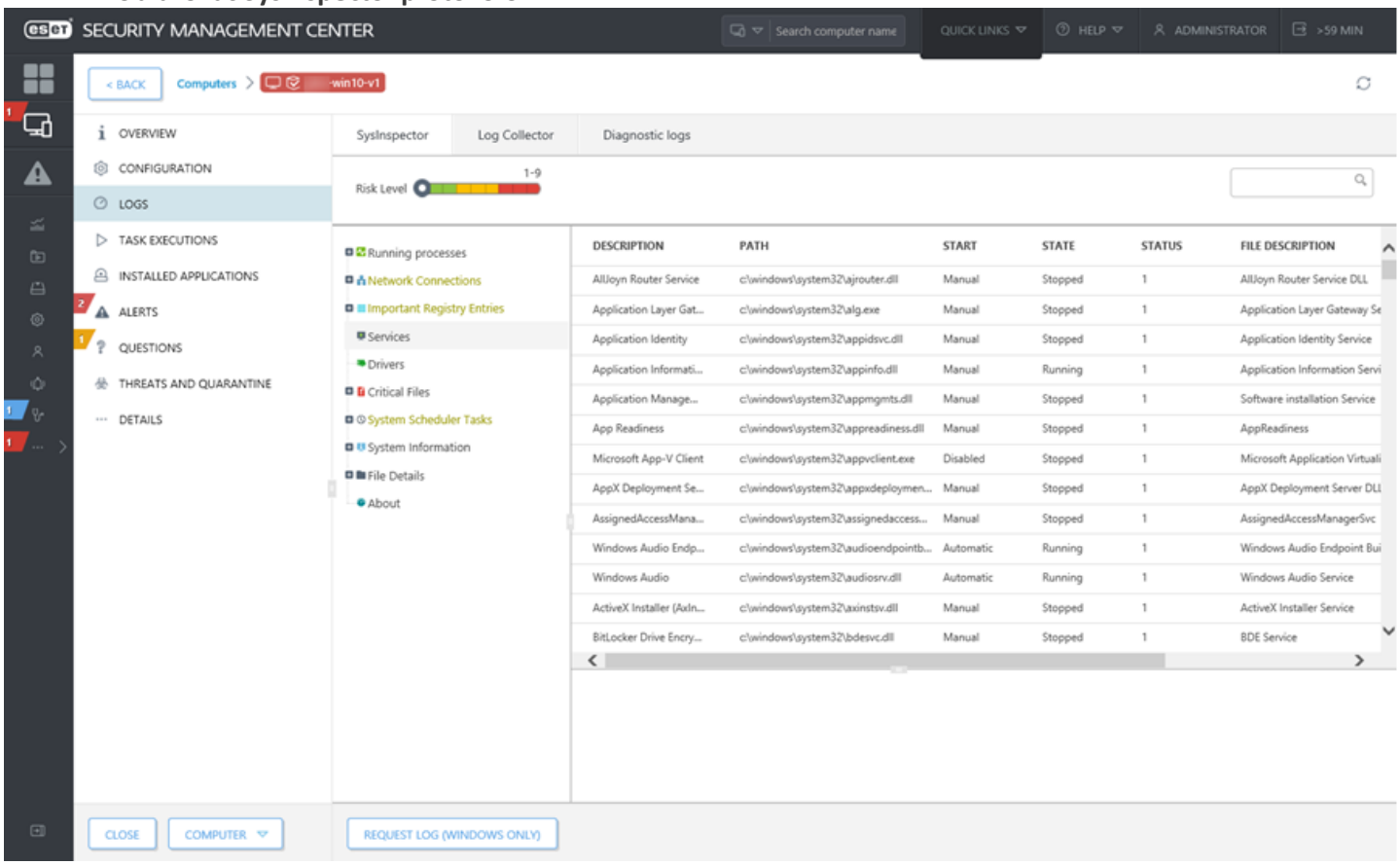
1. Pridajte nový riadiaci panel alebo upravte niektorú z existujúcich správ riadiaceho panela.
2. V rámci šablóny správy vyberte možnosť **Automatizácia** > **História SysInspector snímok za posledných 30 dní**.
3. Otvorte správu, vyberte počítač a následne vyberte z roletového menu možnosť **Otvoriť zobrazovač SysInspector protokolov**.

Zo správy

1. Prejdite do časti Správy > kategória **Automatizácia**.
2. Zo zoznamu vyberte šablónu **História SysInspector snímok za posledných 30 dní** a kliknite na **Generovať teraz**.
3. Otvorte správu, vyberte počítač a následne vyberte z roletového menu možnosť **Otvoriť zobrazovač SysInspector protokolov**.

Zo sekcie Počítače

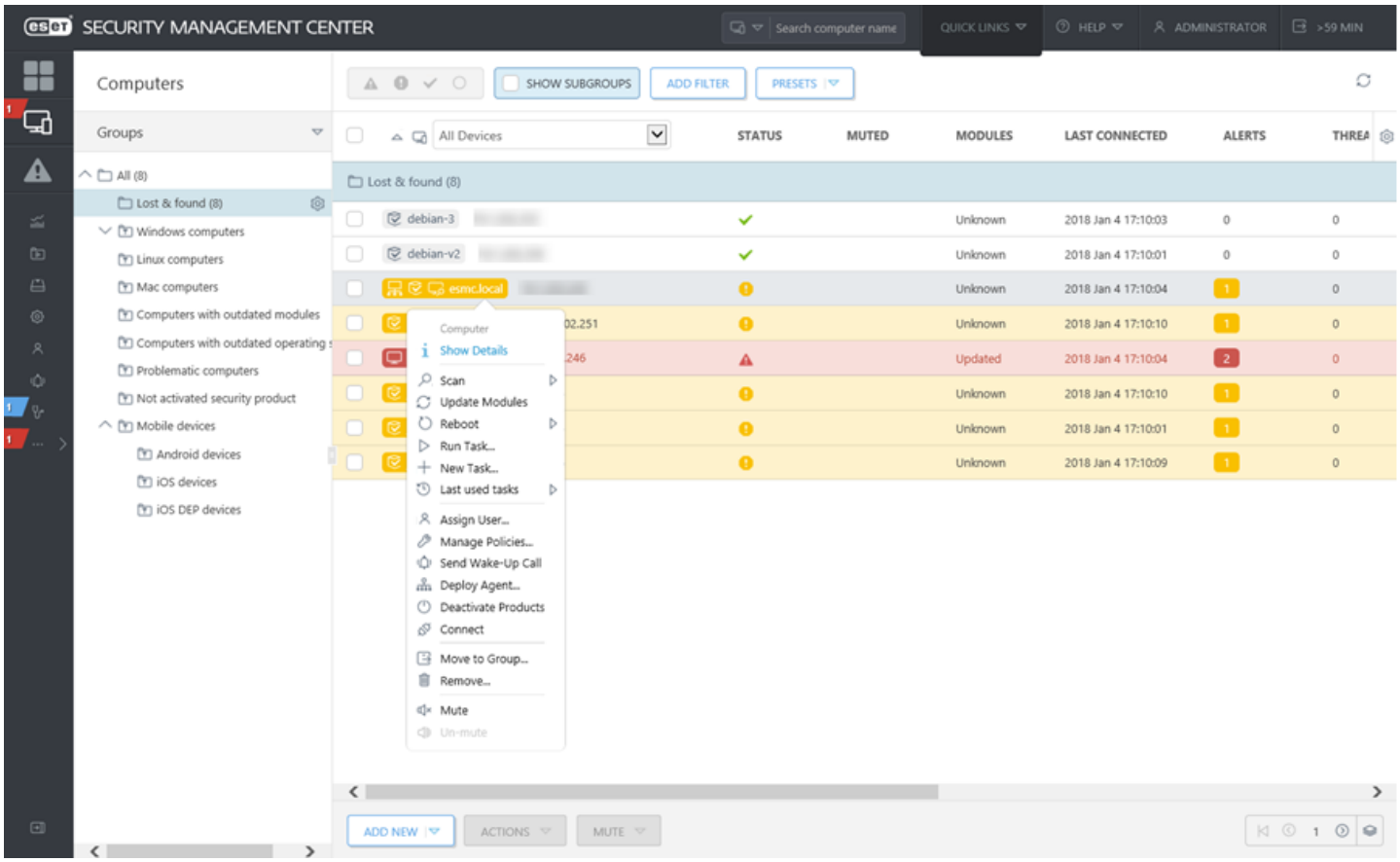
1. Prejdite do sekcie Počítače.
2. Vyberte počítač v statickej alebo dynamickej skupine a kliknite na **Zobraziť podrobnosti**.
3. Prejdite do časti **Protokoly** > karta **SysInspector**, kliknite na položku v zozname a vyberte možnosť **Otvoriť zobrazovač SysInspector protokolov**.



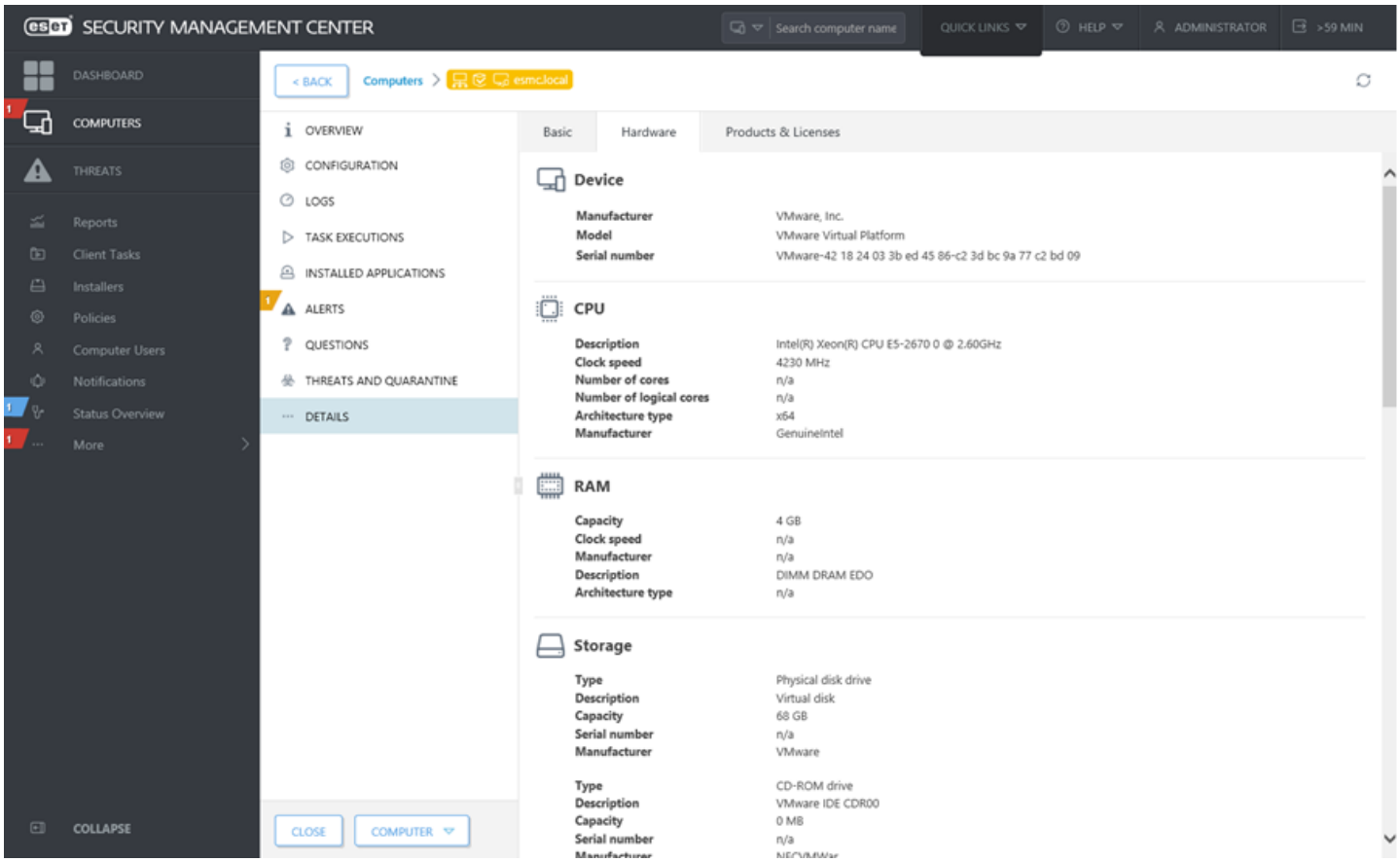
4.6.6 Hardvérový inventár

Najnovšia verzia produktu ESET Security Management Center má funkciu, ktorá mu umožňuje zhromažďovať podrobné informácie súvisiace s hardvérovým inventárom z pripojených zariadení, akými sú napr. podrobnosti o pamäti RAM, úložisku a procesore.

Kliknite na **Počítače**, ďalej kliknite na pripojené zariadenie a vyberte možnosť **Zobraziť podrobnosti**.



Kliknite na **Podrobnosti** a prejdite na kartu **Hardvér**.



Pripojené zariadenia môžete filtrovať podľa ich hardvérových parametrov. V rámci hardvérového inventára máte na výber z nasledujúcich kategórií: šasi, informácie o zariadení, displej, grafický adaptér, vstupné zariadenie, veľkokapacitné úložisko, sieťový adaptér, tlačiareň, procesor, RAM a zvukové zariadenie.

Súhrnné správy o hardvérovom inventári

Môžete si vytvoriť vlastné správy o hardvérovom inventári. Pri vytváraní novej šablóny správy vyberte v sekcii **Dáta** podkategóriu v rámci jedného z filtrov **Hardvérového inventára**. Po pridaní prvého stĺpca tabuľky alebo osi X budú na výber iba kompatibilné dáta.

Dynamické skupiny založené na hardvérovom inventári

Môžete si vytvoriť vlastné dynamické skupiny na základe podrobností hardvérového inventára pripojených zariadení. Pri vytváraní novej šablóny dynamickej skupiny vyberte pravidlo/pravidlá z kategórií **Hardvérového inventára**. Môžete napríklad vytvoriť dynamickú skupinu so zariadeniami filtrovanými podľa ich kapacity pamäte RAM a získať tak prehľad o zariadeniach, ktoré disponujú určitou veľkosťou pamäte RAM.

Hardvérový inventár na systéme Linux

Aby ESET Management Agent správne hlásil podrobnosti o hardvéri, musí byť na klientskom počítači so systémom Linux nainštalovaný nástroj `lshw`.

Na inštaláciu nástroja `lshw` použite nasledujúci príkaz (pod používateľom `root` alebo `sudo`):

Debian distribúcie (Ubuntu)	`apt-get install -y lshw`
Red Hat distribúcie (CentOS, Fedora, RHEL)	`apt-get install -y lshw`

Hardvérový inventár na systéme macOS

Funkcia hardvérového inventára je dostupná na systéme macOS verzie 10.9 a vyššej.

4.7 Úlohy pre klienta

Úlohy pre klienta môžete použiť na správu klientskych zariadení a na nich nainštalovaných bezpečnostných produktov spoločnosti ESET. Existuje mnoho preddefinovaných úloh, ktoré pokrývajú bežné a najčastejšie sa vyskytujúce situácie alebo scenáre, môžete však vytvoriť aj vlastné úlohy so špecifickými nastaveniami. Úlohy pre klienta použite na vynútenie určitej akcie na klientskych počítačoch. Pre úspešné spustenie úlohy na klientskom zariadení je potrebné mať dostatočné prístupové povolenia pre danú úlohu a pre objekty (zariadenia), pre ktoré je úloha určená. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

Úlohy pre klienta môžu byť priradené ku skupinám alebo individuálnym počítačom. Po jej vytvorení sa úloha spúšťa pomocou spúšťača. Úlohy pre klienta sú distribuované na klienty vtedy, keď sa ESET Management Agent klientskeho počítača pripojí na ESMC Server. Z tohto dôvodu môže nejaký čas trvať, kým je na ESMC Server doručená správa o spustení a výsledku vykonania úlohy. Pre urýchlenie vykonania úloh môžete upraviť interval pripojenia ESET Management Agenta. Ak chcete vytvoriť novú **úlohu pre klienta**, vyberte požadovaný **Typ úlohy** a kliknite na **Nová**. V ESMC máte k dispozícii nasledujúce prednastavené úlohy (každá **Kategória úloh** obsahuje **Typy úloh**):

- **Všetky úlohy**
  - **Bezpečnostný produkt ESET**
    - Diagnostika
    - Exportovať konfiguráciu spravovaných produktov
    - Aktualizácia modulov
    - Vrátenie zmien aktualizácie modulov
    - Manuálna kontrola
    - Aktivácia produktu
    - Správa karantény
    - Spustiť SysInspector skript
    - Odoslať súbor do EDTD
    - Kontrola servera
    - Inštalácia softvéru
    - Vyžiadať SysInspector protokol (iba Windows)
    - Odovzdať súbor v karanténe
  - **ESET Security Management Center**
    - Diagnostika
    - Obnoviť klonovaného agenta
    - Obnovenie Rogue Detection Sensor databázy
    - Aktualizácia súčastí Security Management Center
    - Ukončiť spravovanie (Odinštalovať ESET Management Agenta)
  - **Operačný systém**
    - Zobraziť správu
    - Aktualizácia operačného systému
    - Spustiť príkaz

Vypnúť počítač

Inštalácia softvéru

Odinštalovanie softvéru

Ukončiť spravovanie (Odinštalovať ESET Management Agenta)

- **Mobil**

  Anti-Theft akcie

  Zobraziť správu

  Exportovať konfiguráciu spravovaných produktov

  Aktualizácia modulov

  Manuálna kontrola

  Aktivácia produktu

  Inštalácia softvéru

  Ukončiť spravovanie (Odinštalovať ESET Management Agenta)

4.7.1 Vypnutie počítača

Pomocou úlohy **Vypnúť počítač** môžete vypnúť alebo reštartovať klientsky počítač. Kliknite na možnosť **Nová** a môžete začať nastavovať úlohu.

Základné

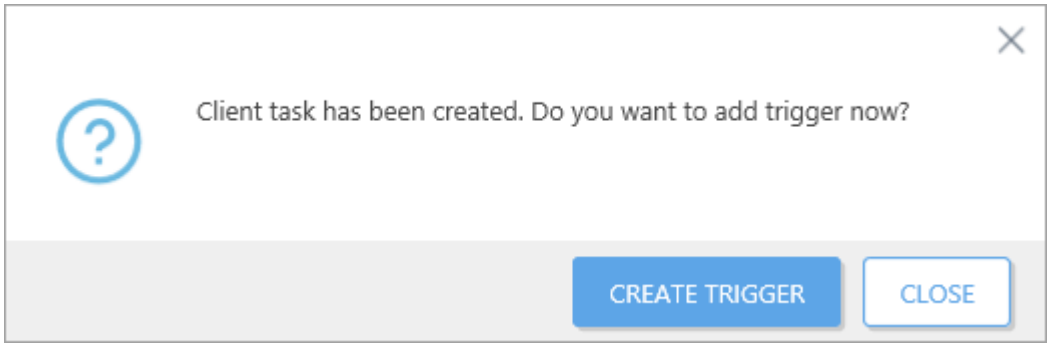
Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

- **Reštart počítača** – vyberte túto možnosť, ak chcete po dokončení úlohy reštartovať počítač. Ak chcete počítače vypnúť, ponechajte túto možnosť neoznačenú.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.2 Diagnostika

Postupujte podľa krokov uvedených nižšie, ak chcete vyžiadať diagnostickú akciu prostredníctvom bezpečnostného produktu ESET na klientskom počítači.

Vyberte úlohu **Diagnostika** a kliknite na **Nová**.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

Diagnostická akcia

- **Spustiť ESET Log Collector** – budú zozbierané konkrétne dáta (ako napr. konfigurácia a protokoly) z vybraného počítača s cieľom získať potrebné informácie o zákazníkovom počítači v prípade riešenia problémov s technickou podporou.
  - **Parametre ESET Log Collector** – pre zozbieranie všetkých dostupných dát ponechajte pole Parametre ESET Log Collector prázdne. Ak chcete špecifikovať parametre pre Log Collector, pozrite si zoznam jednotlivých parametrov podľa operačných systémov: Windows, macOS alebo Linux.
- **Nastaviť diagnostický režim –** diagnostický režim pozostáva z nasledujúcich kategórií: **protokol spamu**, **protokol firewallu**, **protokol HIPS**, **správa zariadení** a **protokol webovej kontroly**. Hlavným účelom diagnostického režimu je zhromažďovanie protokolov všetkých úrovní závažnosti pri riešení problémov.
  - **Zapnúť** – povolenie zapisovania do protokolov v rámci všetkých aplikácií ESET.
  - **Vypnúť** – zapisovanie do protokolov môžete vypnúť buď manuálne, alebo môžete počkať do najbližšieho reštartu počítača, po ktorom bude zapisovanie do protokolov vypnuté automaticky.

Pre úspešné vytvorenie diagnostických protokolov je potrebné splniť nasledujúce podmienky:

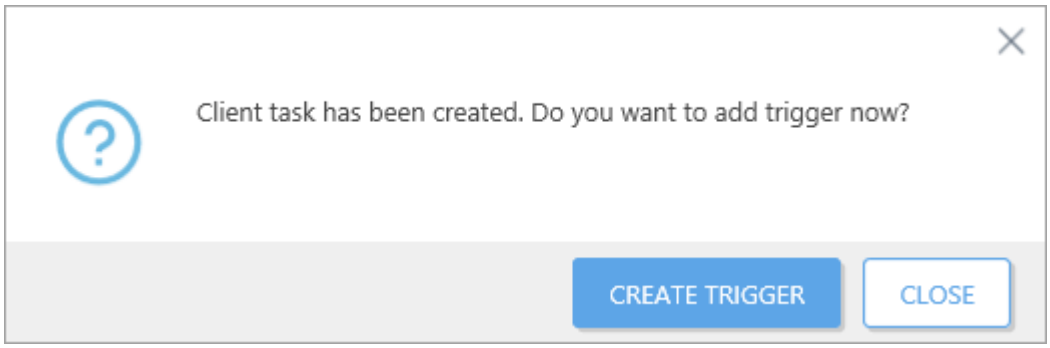
- Protokoly diagnostického režimu môžu byť zozbieravané z klientskych počítačov so systémom Windows a macOS.
- Na klientskom počítači musí byť nainštalovaný a aktivovaný bezpečnostný produkt ESET.

Poznámka:
ESET Management Agent odosiela iba protokoly zozbierané produktom ESET nainštalovaným na klientskom počítači. Kategória protokolu a úroveň podrobnosti protokolu závisí od typu produktu a konfigurácie. Nakonfigurujte každý produkt použitím Politík tak, aby zozbieraval konkrétne protokoly.

Diagnostické protokoly staršie ako 24 hodín sú každý deň o polnoci automaticky odstraňované. Vďaka tomu sa zamedzí preťaženiu ESMC databázy.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



Vytvorené protokoly si môžete prezrieť v sekcii Podrobnosti o počítači.

4.7.3 Manuálna kontrola

Úloha **Manuálna kontrola** vám umožňuje manuálne spustiť kontrolu klientskeho počítača.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

Po kontrole vypnúť počítač – po označení tejto možnosti bude počítač po skončení kontroly vypnutý.

Profil kontroly – vyberte profil kontroly z roletového menu:

- **Hĺbková kontrola** – toto prednastavený profil na klientskych počítačoch. Je nastavený na najpodrobnejšiu kontrolu systému, avšak vyžaduje najviac času a zdrojov.
- **Smart kontrola –** pomocou Smart kontroly je možné rýchlo skontrolovať počítač a vyliečiť infikované súbory bez potreby zásahu používateľa. Výhodou Smart kontroly je jednoduchá obsluha bez potreby nastavovania. Kontrolujú sa všetky súbory na lokálnych diskoch. Detegované infiltrácie budú automaticky vyliečené alebo zmazané. Úroveň liečenia je automaticky nastavená na štandardnú hodnotu.
- **Kontrola z kontextového menu** – tento typ kontroly kontroluje počítače pomocou predvoleného profilu. Môžete vybrať ciele kontroly.
- **Vlastný profil** – vlastná, resp. prispôsobená kontrola je užitočná v prípade, že chcete vybrať konkrétne ciele kontroly a metódy samotnej kontroly. Výhodou je možnosť podrobného nastavenia všetkých parametrov kontroly. Tieto nastavenia sa dajú uložiť do tzv. profilov, čo umožňuje vykonávať pravidelnú vlastnú kontrolu počítača s vašimi obľúbenými nastaveniami. Pred spustením úlohy s vlastným profilom musí byť vytvorený profil. Po zvolení vlastného profilu z roletového menu zadajte názov profilu do poľa **Vlastný profil**.

Liečenie

Predvolená je možnosť **Kontrolovať s liečením**. Toto nastavenie umožňuje automatické liečenie nájdených infikovaných objektov. Ak to nebude možné, budú presunuté do karantény.

Ciele kontroly

Možnosť **Kontrolovať všetky ciele** je takisto predvolene zapnutá. Pri použití týchto nastavení budú kontrolované všetky ciele špecifikované v profile kontroly. Po vypnutí tejto možnosti musíte manuálne zadať ciele kontroly do poľa **Pridať cieľ**. Zadajte názov cieľa do textového poľa a kliknite na možnosť **Pridať**. Cieľ bude zobrazený nižšie v poli **Ciele kontroly**. Cieľom kontroly môže byť napr. súbor alebo umiestnenie. Môžete prípadne spustiť aj vopred definovanú kontrolu použitím ktorýchkoľvek z nižšie uvedených reťazcov ako **Cieľ kontroly**:

Cieľ kontroly	Kontrolované lokality
`${DriveRemovable}`	Všetky vymeniteľné jednotky a zariadenia
`${DriveRemovableBoot}`	Boot sektory všetkých vymeniteľných jednotiek
`${DriveFixed}`	Pevné disky (HDD, SSD)
`${DriveFixedBoot}`	Boot sektory pevných diskov
`${DriveRemote}`	Sieťové disky
`${DriveAll}`	Všetky dostupné jednotky
`${DriveAllBoot}`	Boot sektory všetkých jednotiek

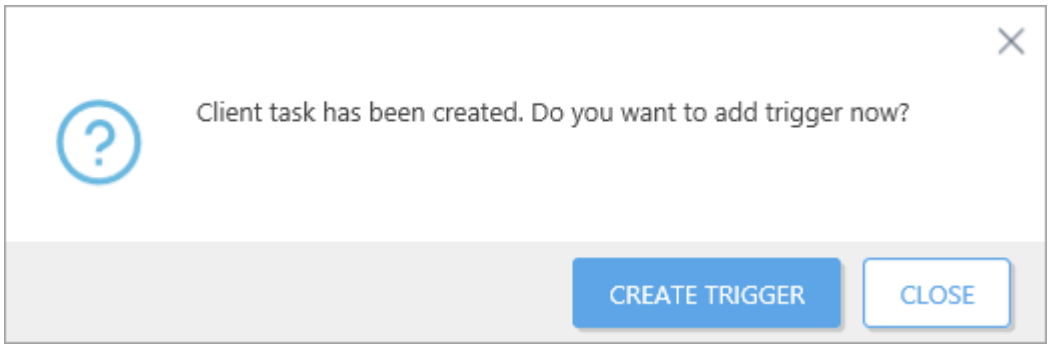
`${DriveSystem}`	Systémové jednotky
`${Share}`	Zdieľané disky
`${Boot}`	Hlavný boot sektor
`${Memory}`	Operačná pamäť

Príklad: Ciele kontroly
Nižšie sú uvedené príklady, ako používať parametre cieľov kontroly v rámci **Manuálnej kontroly**:

- Súbor: `C:\Users\Data.dat`
- Priečinok `C:\MyFolder`
- Unix cesta alebo súbor `/usr/data`
- Umiestnenie UNC (Windows) `\\server1\scan_folder`
- Vopred definovaný reťazec `${Memory}`

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.4 Aktualizácia operačného systému

Úloha **Aktualizácia operačného systému** je určená na aktualizovanie operačných systémov na klientskych počítačoch v sieti. Táto úloha spúšťa aktualizáciu operačného systému na operačných systémoch Windows, macOS a Linux.

macOS – úloha nainštaluje všetky aktualizácie pomocou nasledujúceho príkazu:

```
/usr/sbin/softwareupdate --install --all
```

Linux – úloha nainštaluje všetky aktualizácie. V rámci kontroly dostupnosti využíva viacero baliacich nástrojov, čím je zabezpečená podpora väčšiny distribúcií.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

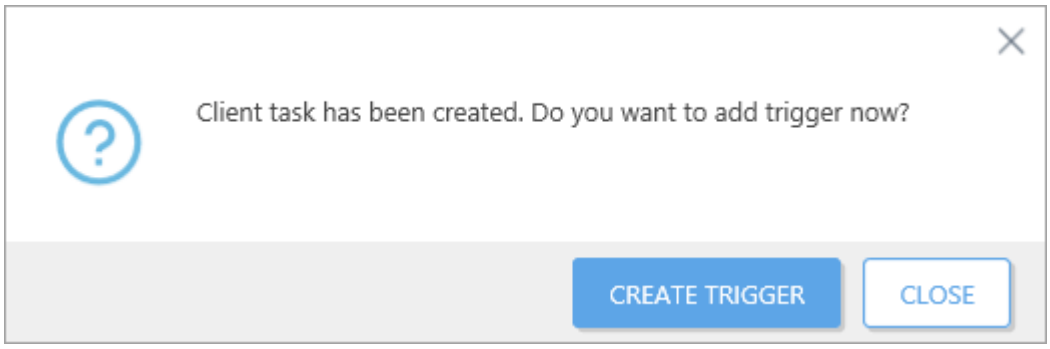
Nastavenia

Nižšie spomenuté nastavenia nemajú vplyv na úlohu, ak cieľové zariadenie používa systém Linux alebo macOS.

- **Automaticky prijať EULU** – označte túto možnosť, ak chcete, aby bola Licenčná dohoda s koncovým používateľom akceptovaná automaticky. Používateľovi sa nezobrazí žiadny text. Ak nepovolíte automatické akceptovanie Licenčnej dohody s koncovým používateľom, úloha vynechá tie aktualizácie, ktoré akceptovanie dohody vyžadujú.
- **Inštalovať voliteľné aktualizácie** – táto možnosť sa vzťahuje len na operačný systém Windows. Aktualizácie, ktoré sú označené ako voliteľné, budú takisto nainštalované.
- **Povoliť reštart** – táto možnosť je určená len pre operačné systémy Windows. Po jej povolení bude počítač po aktualizácii operačného systému reštartovaný. Ak táto možnosť nie je zvolená, aktualizácie vyžadujúce si reštart nebudú nainštalované.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.5 Obnovenie Rogue Detection Sensor databázy

Úloha **Obnovenie Rogue Detection Sensor databázy** je určená na zmazanie vyrovnávacej pamäte nástroja RD Sensor. Táto úloha vyčistí vyrovnávaciu pamäť a výsledky vyhľadávania budú opäť ukladané. Neodstráni však detegované počítače. Je vhodné ju použiť, ak sú detegované počítače stále len vo vyrovnávacej pamäti a neboli zatiaľ nahlásené na server.

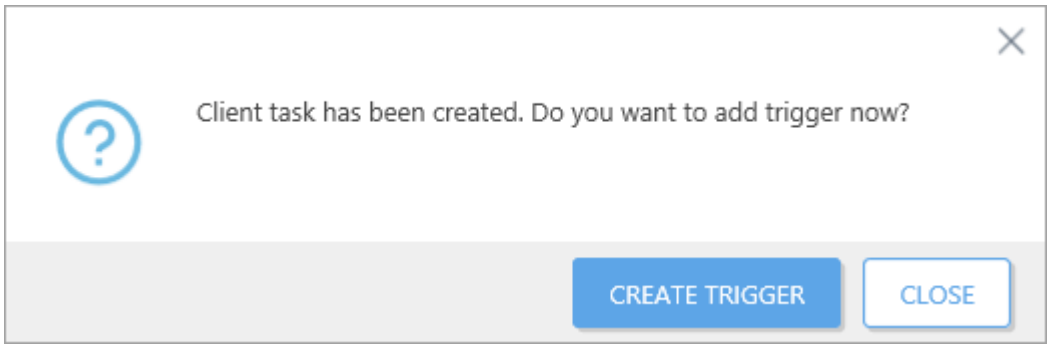
Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Poznámka:
Pre túto úlohu nie sú dostupné žiadne **nastavenia**.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.6 Správa karantény

Úloha **Správa karantény** sa používa na správu objektov umiestnených v karanténe ESMC Servera, ktoré sú infikované alebo podozrivé a boli objavené počas kontroly.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

Nastavenia správy karantény

Akcia – vyberte akciu, ktorá bude vykonaná s objektmi v karanténe.

- **Obnoviť objekt(y)** – obnovenie objektu do jeho pôvodného umiestnenia, po ďalšej kontrole sa však môže objekt dostať späť do karantény.
- **Obnoviť objekt(y) a vylúčiť v budúcnosti** – obnovenie objektu do jeho pôvodného umiestnenia, pričom po ďalšej kontrole sa objekt nemôže opäť dostať do karantény.
- **Odstrániť objekt(y)** – trvalé odstránenie objektu.

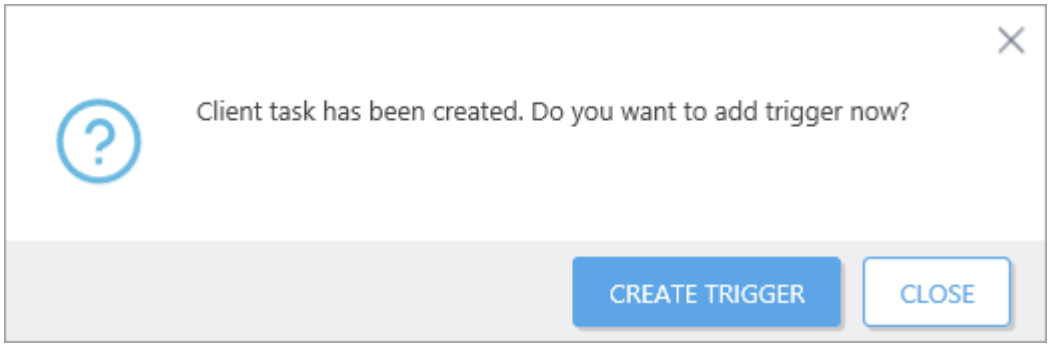
Typ filtra – filtrovanie objektov v karanténe na základe zadaných kritérií, a to buď podľa hash reťazca objektu, alebo podmienok.

Nastavenia podmieneného filtra:

- **Nastavenia hash filtra** – pridanie hash položky do poľa. Zadané môžu byť len známe objekty, napríklad objekty, ktoré už boli umiestnené do karantény.
- **Výskyt** – vyberte časový rozsah, v ktorom bol objekt pridaný do karantény.
- **Veľkosť** – vyberte rozsah veľkosti objektu pridaného do karantény (v bajtoch).
- **Názov hrozby** – vyberte hrozbu zo zoznamu položiek umiestnených v karanténe.
- **Názov objektu** – vyberte objekt zo zoznamu položiek umiestnených v karanténe.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.7 Aktualizácia súčastí Security Management Center

Úloha **Aktualizácia súčastí Security Management Center** sa používa na aktualizáciu súčastí ESMC (ESET Management Agent, ESMC Server, Web Console a MDM).

Dôležité:
Túto úlohu môžete použiť pre aktualizáciu na ESMC 7 len od ERA verzie 6.3 a novšej.

Aktualizačná úloha môže byť vykonaná len na počítači, kde je nainštalovaný ESET Management Agent. Agent musí byť nainštalovaný aj na ESMC Serveri.

Upozornenie:
Nevykonávajte aktualizáciu agentov skôr než je aktualizovaný ESMC Server. ESET Management Agenty 7.x používajú nový komunikačný protokol a nedokážu sa pripojiť na ERA Server 6.x.

Aby sa predišlo zlyhaniu inštalácie, ESMC vykoná pred inštaláciou alebo aktualizáciou produktov ESET nasledujúce kontroly:

- overí prístup k repozitáru,
- overí, či nie je na klientskom počítači čakajúci reštart (len na systémoch Windows),
- overí, či je na klientskom počítači dostatok voľného miesta (toto nie je dostupné na systéme Linux).

Poznámka:
Viac informácií nájdete v časti Aktualizácia súčastí. Pozrite si tiež kapitolu Aktualizácia ESMC. O ďalšom spôsobe, pomocou ktorého je možné aktualizovať nástroj ESET Security Management Center na najnovšiu verziu, sa dozviete v našom článku databázy znalostí.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

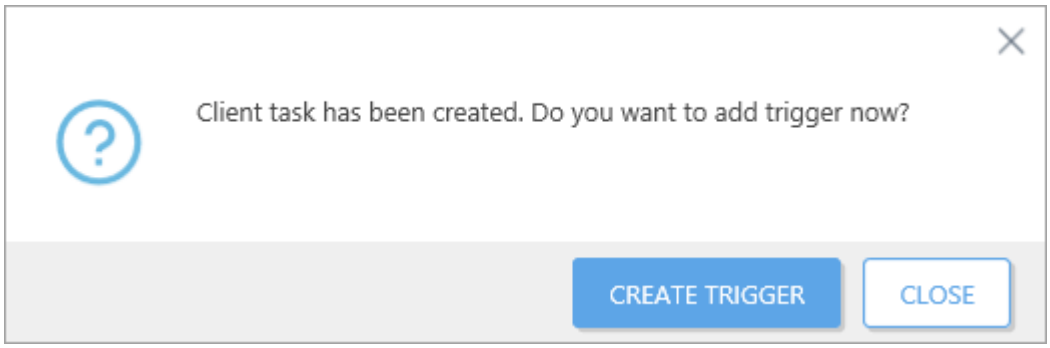
Nastavenia

Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.

- **Referenčný Security Management Center Server** – zo zoznamu vyberte verziu ESMC Servera. Všetky súčasti ESMC budú aktualizované na verzie kompatibilné s vybraným serverom.
- **Automaticky reštartovať, keď je to potrebné** – táto funkcia umožňuje vynútenie reštartu operačného systému klienta, ak to inštalácia vyžaduje.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.8 Obnovenie klonovaného agenta

ESET Management Agenta je možné distribuovať v rámci vašej siete pomocou vopred definovaných obrazov – podrobnejšie informácie nájdete v tomto článku databázy znalostí. Klonované agenty majú rovnaké SID, čo môže spôsobovať problémy. Riešením tohto problému je použitie úlohy **Obnoviť klonovaného agenta**, čím dôjde k vynulovaniu pridelených SID a prideleniu novej identity agentom.

Základné

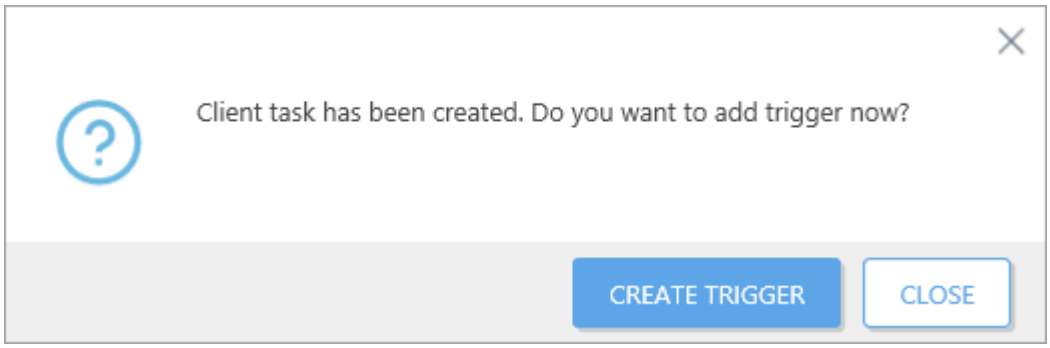
Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Upozornenie:
Túto úlohu používajte opatrne. Po obnovení aktuálneho ESET Management Agenta budú všetky úlohy prebiehajúce na danom agente zrušené.

POZNÁMKA:
Pre túto úlohu nie sú dostupné žiadne **nastavenia**.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.9 Spustenie príkazu

Pomocou úlohy **Spustiť príkaz** spustíte na klientskych počítačoch konkrétne príkazy. Správca môže určiť príkazy, ktoré budú spustené.

Dôležité:
Príkazy sú vykonávané bez prístupu k prostrediu pracovnej plochy. Z tohto dôvodu môže zlyhať spúšťanie príkazov, ktoré potrebujú prístup k grafickému používateľskému rozhraniu aplikácie.

V rámci úlohy Spustiť príkaz môžete použiť `ecmd` príkazy. Viac informácií nájdete v nasledujúcom článku databázy znalostí.

Operačný systém	Príkaz bude spustený pod používateľom/účtom	Predvolený pracovný adresár	Dostupné sieťové umiestnenia	Príkaz bude spustený v
Windows	*Local System*	*C:\Windows\Temp*	Iba umiestnenia v aktuálnej doméne, dostupné pre účet Local System	Príkazový riadok (`cmd.exe`)
Linux alebo macOS	*root*	*/tmp*	Iba ak je umiestnenie pripojené a dostupné pre root používateľa	Konzola

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

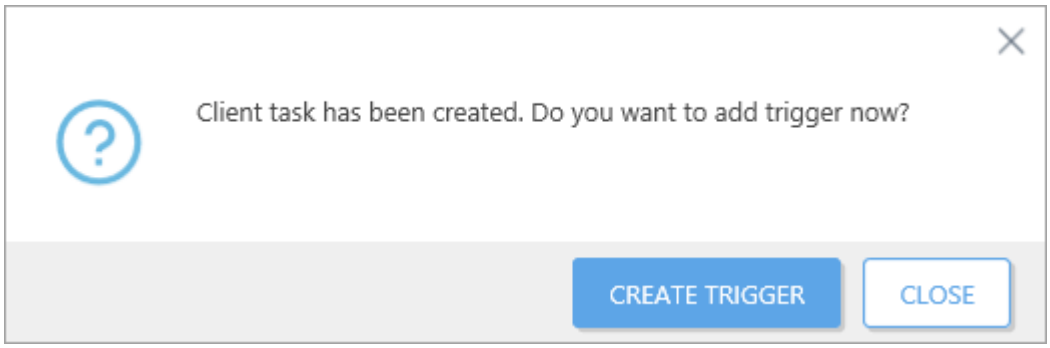
- **Príkazový riadok na spustenie** – zadajte príkaz, ktorý chcete spustiť na klientskom počítači.
- **Pracovný adresár** – zadajte adresár, v ktorom chcete daný príkaz spustiť.

Príklad: Ako spustiť lokálny skript
Pre spustenie lokálneho skriptu nachádzajúceho sa na kliente v umiestnení `C:\Users\user\script.bat` postupujte podľa nasledujúcich krokov:

1. Vytvorte novú úlohu pre klienta a vyberte možnosť **Spustiť príkaz**.
2. V sekcii **Nastavenia** zadajte:
Príkazový riadok na spustenie: `script.bat`
Pracovný adresár: `C:\Users\user`
3. Kliknite na **Dokončiť**, vytvorte spúšťač a vyberte cieľové klienty.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.10 Spustenie skriptu SysInspector

Úloha **Spustiť SysInspector skript** sa používa na odstránenie nechcených objektov zo systému. Pred spustením tejto úlohy musí byť najprv **SysInspector Skript** exportovaný z nástroja ESET SysInspector. Po exportovaní skriptu môžete označiť objekty, ktoré chcete odstrániť, a spustiť skript s upravenými dátami – označené objekty budú odstránené.

Poznámka:
Po vykonaní úlohy môžete skontrolovať výsledok vykonania danej úlohy v správe (zázname).

Základné

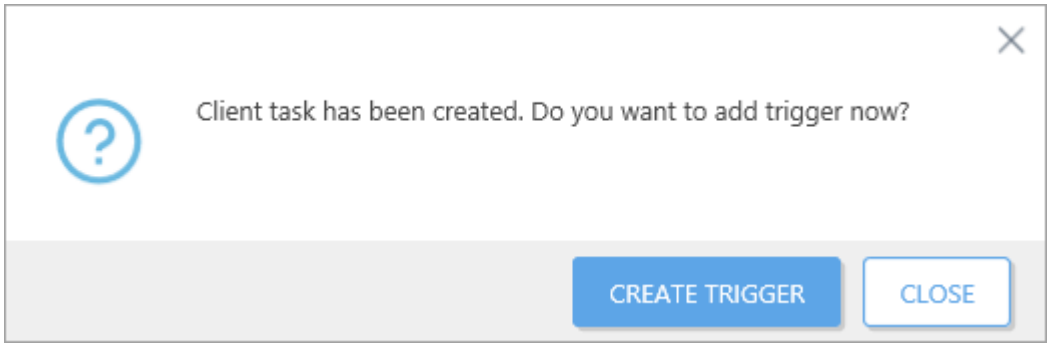
Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

- **SysInspector skript** – kliknite na **Prehľadávať** a vyberte servisný skript. Servisný skript musíte vytvoriť pred spustením úlohy.
- **Akcia** – môžete buď **Odovzdať**, alebo **Stiahnuť** skript z ESMC Web Console.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.11 Odoslanie súboru do EDTD

Používateľ môže odoslať súbor na analýzu malvéru (ESET Dynamic Threat Defense) z nástroja ESMC Web Console. Pre odoslanie súboru na analýzu prejdite do sekcie **Hrozby** a pre jednotlivé súbory zvoľte možnosť **Odoslať súbor do EDTD**.

4.7.12 Kontrola servera

Môžete použiť úlohu **Kontrola servera** na vykonanie kontroly klientskych počítačov pomocou nainštalovaného serverového riešenia od spoločnosti ESET. Typ spustenej kontroly závisí od nainštalovaného riešenia ESET:

Produkt	Kontrolovať	Popis
ESET File Security 6	**Kontrola Hyper-V**	Tento typ kontroly vám umožňuje kontrolovať disky Microsoft Hyper-V Servera, čo je virtuálny počítač (VM), a to bez potreby inštalácie ESET Management Agenta na daný virtuálny počítač.
ESET Security pre Microsoft SharePoint Server	**Kontrola databázy SharePoint, kontrola Hyper-V**	Táto funkcia umožňuje nástroju ESMC použiť vhodný cieľ kontroly pri spustení úlohy pre klienta **Kontrola servera**

Produkt	Kontrolovať	Popis
		na serveri, kde je nainštalované riešenie ESET Security pre Microsoft SharePoint.
ESET Mail Security 6	**Manuálna kontrola poštových databáz, kontrola Hyper-V**	Táto funkcia umožňuje nástroju ESMC použiť vhodný cieľ kontroly. Keď nástroj ESMC spustí úlohu pre klienta **Kontrola servera**, zozbiera zoznam cieľov a vyzve vás, aby ste zvolili ciele kontroly v rámci manuálnej kontroly poštových databáz na danom serveri.
ESET Mail Security pre IBM Domino	**Manuálna kontrola databáz, kontrola Hyper-V**	Táto funkcia umožňuje nástroju ESMC použiť vhodný cieľ kontroly pri spustení úlohy pre klienta **Kontrola servera** na serveri, kde je nainštalované riešenie ESET Mail Security pre IBM Domino.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

- Kliknite na **Vybrať** v časti **Kontrolovaný server** a vyberte počítač, kde je nainštalovaný bezpečnostný produkt určený pre server vo verzii 6 alebo novšej. Budete vyzvaný, aby ste na danom počítači zvolili konkrétne disky, priečinky alebo súbory, pre ktoré bude vykonaná kontrola.
- Následne pre túto úlohu vyberte **Spúšťač**, v prípade potreby môžete nastaviť aj obmedzovanie. Predvolene je táto úloha spustená ihneď.

Ciele kontroly

Nástroj ESMC vám ponúkne zoznam dostupných cieľov kontroly na zvolenom serveri. Aby bolo možné použiť tento zoznam, musí byť zapnutá možnosť **Generovať zoznam cieľov** v rámci politiky pre váš serverový produkt v sekcii **Nástroje** > **Ciele kontroly**:

- **Generovať zoznam cieľov** – povoľte toto nastavenie, aby mohol nástroj ESMC generovať zoznamy cieľov.
- **Doba aktualizácie [minúty]** – generovanie zoznamu cieľov po prvýkrát bude trvať polovicu tohto času.

Vyberte ciele kontroly zo zoznamu. Viac informácií nájdete v časti Ciele kontroly.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.7.13 Inštalácia softvéru

Úloha **Inštalácia softvéru** je určená na inštaláciu softvéru na klientske počítače v sieti alebo jeho aktualizáciu. Je určená primárne na inštaláciu produktov spoločnosti ESET, avšak môže slúžiť aj na inštaláciu iného softvéru.

Aby sa predišlo zlyhaniu inštalácie, ESMC vykoná pred inštaláciou alebo aktualizáciou produktov ESET nasledujúce kontroly:

- overí prístup k repozitáru,
- overí, či nie je na klientskom počítači čakajúci reštart (len na systémoch Windows),
- overí, či je na klientskom počítači dostatok voľného miesta (toto nie je dostupné na systéme Linux).

Poznámka:

- ESMC Server a ESET Management Agent musia mať prístup na internet, aby sa mohli pripojiť na repozitár a vykonať inštaláciu. Ak nemáte prístup na internet, musíte nainštalovať klientsky softvér lokálne. V opačnom

prípade vzdialená inštalácia zlyhá.

- Pri vykonávaní úlohy Inštalácia softvéru na počítačoch v doméne s bežiacim ESET Management Agentom musí mať používateľ pridelené povolenie na *čítanie* pre priečinok, v ktorom sú uložené inštalátory. V prípade, že je nutné prideliť tieto povolenia, postupujte podľa krokov uvedených nižšie:

1. Pridajte konto počítača pre službu Active Directory do počítača, na ktorom je daná úloha spustená (napr. *NewComputer$*).
2. Počítaču *NewComputer$* prideľte povolenie na **čítanie** pre priečinok s inštalátormi – kliknite pravým tlačidlom myši na priečinok, z kontextového menu zvoľte možnosť Vlastnosti, prejdite na kartu **Zdieľanie** a stlačte **Zdieľať**.Znak „$“ je na konci názvu počítača nutné uviesť.

Inštalácia zo zdieľaného umiestnenia je možná len v prípade, ak je klientsky počítač v doméne.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

- Kliknite na možnosť **<Vyberte ESET licenciu>** a zo zoznamu dostupných licencií vyberte licenciu pre inštalovaný produkt. Tento postup bude fungovať len pre produkty inštalované z repozitára, nebude fungovať pre produkty inštalované z vlastnej URL adresy.

Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.

- V sekcii **<Vyberte balík>** vyberte príslušný inštalačný balík z repozitára alebo zadajte URL adresu balíka. Zobrazí sa zoznam dostupných balíkov, kde si môžete vybrať produkt spoločnosti ESET, ktorý chcete nainštalovať (napr. ESET Endpoint Security). Vyberte požadovaný inštalačný balík a kliknite na **OK**. Ak chcete zadať URL adresu inštalačného balíka, napíšte ju alebo skopírujte do textového poľa (napr. *file://\\pc22\install\ees_nt64_ENU.msi*). Nepoužívajte URL adresu, ktorá vyžaduje autorizáciu.

  http://server_address/ees_nt64_ENU.msi – ak inštalujete z verejného webového servera alebo vášho vlastného HTTP servera.
  file://\\pc22\install\ees_nt64_ENU.msi – ak inštalujete z lokality vo vašej sieti.
  file://C:\installs\ees_nt64_ENU.msi – ak inštalujete z lokálneho disku.

V prípade potreby môžete zadať **parametre inštalácie**. Za iných okolností ponechajte toto pole prázdne.

Vyberte možnosť **Automaticky reštartovať, keď je to potrebné** pre vynútenie automatického reštartovania počítača po inštalácii. Túto možnosť však môžete vynechať, pretože klientsky počítač môže byť reštartovaný aj manuálne.

Poznámka:
Po inštalácii produktu ESET Endpoint Antivirus alebo ESET Endpoint Security verzie 6.5 alebo vyššej s využitím inštalačného parametra `CFG_LIVEGRID_ENABLED` bude správanie daného produktu nasledovné:

Funkcia	`CFG_LIVEGRID_ENABLED=0`	`CFG_LIVEGRID_ENABLED=1`
ESET LiveGrid® reputačný systém (odporúča sa)	Zapnutá	Zapnutá
Odoslať anonymné štatistiky	Vypnutá	Zapnutá
Odoslať vzorku	Vypnutá	Zapnutá

Inštalácia softvéru tretej strany

Úlohu **Inštalácia softvéru** môžete použiť aj na inštaláciu softvéru, ktorý nie je od spoločnosti ESET (softvér tretej strany).

Operačný systém	Podporované typy inštalačných súborov	Podpora inštalačných parametrov
Windows	.msi	Úloha Inštalácia softvéru vždy vykonáva tichú inštaláciu .msi balíkov. Nie je možné definovať msiexec parametre. Je možné definovať iba parametre samotného inštalačného balíka, ktoré sa líšia v závislosti od konkrétnej aplikácie.
Linux	.deb, .rpm, .sh	Parametre môžete použiť len pre .sh súbory (súbory .deb a .rpm nepodporujú parametre).
macOS	.pkg, .dmg (obsahujúce .pkg súbor)	Inštalačné parametre nie sú podporované.
Android	.apk	
iOS	.ipa	

PRÍKLAD:
Chcete nainštalovať softvér na systéme Linux pomocou súboru *install_script.sh*, ktorý má dva parametre: `-a` je prvý parameter a `-b` je druhý parameter.

Inštalácia v termináli (ako root používateľ v priečinku, kde sa *nachádza install_script.sh*):

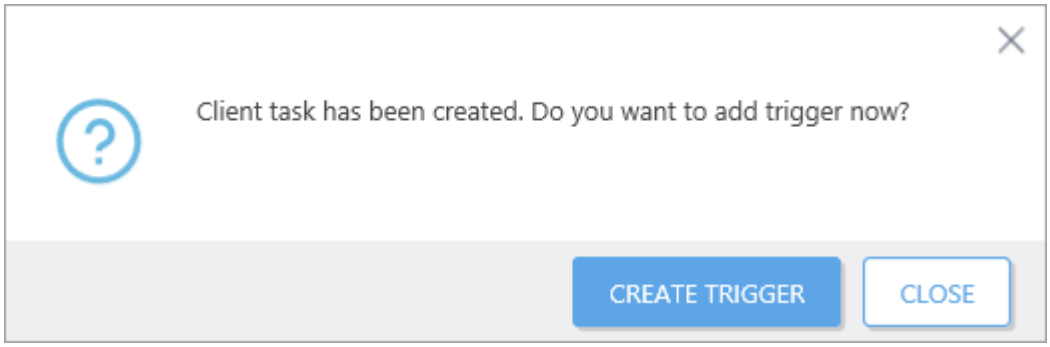
```
./install_script.sh -a parameter_1 -b parameter_2
```

Inštalácia pomocou úlohy Inštalácia softvéru:

- Do poľa **Inštalovať balík zadaním URL adresy** zadajte cestu k súboru, napr.: *file:///home/user/Desktop/install_script.sh*.
- Ako **Parametre inštalácie** zadajte: `-a parameter_1 -b parameter_2`.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.13.1 Aktualizácia softvéru ESET

Úloha pre klienta „Inštalácia softvéru“ môže byť použitá aj na aktualizáciu bezpečnostných produktov spoločnosti ESET. Spustite túto úlohu s použitím najnovšieho inštalátora, aby bola cez váš súčasný bezpečnostný produkt nainštalovaná najnovšia verzia programu.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

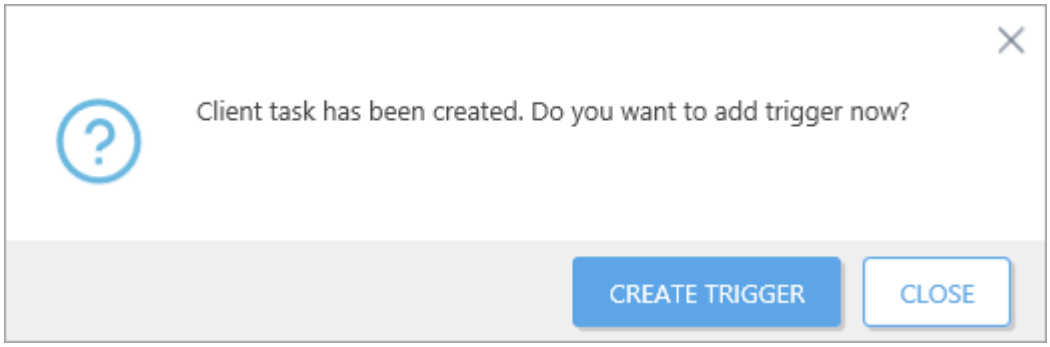
Označte možnosť **Súhlasím s podmienkami licenčnej dohody koncového používateľa a beriem na vedomie Ochranu súkromia**. Viac informácií nájdete v časti Správa licencií alebo v časti EULA.

ESET licencia – pri aktualizácii aktivovaného produktu nie je potrebné vybrať licenciu. Licenciu vyberte len v prípade, že inštalujete alebo aktualizujete produkty, ktoré zatiaľ aktivované neboli, prípadne chcete zmeniť aktuálne používanú licenciu na inú.

Balík na inštaláciu – z repozitára vyberte najnovšiu dostupnú verziu aktualizácie.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



Aktualizácia produktu ESET Security pre Microsoft SharePoint
Ak na aktualizáciu produktu ESET Security pre Microsoft SharePoint z verzie 4.x používate úlohu, úloha bude prerušená a zobrazí sa všeobecné chybové hlásenie inštalácie (0x643). Podrobné pokyny, ako úspešne dokončiť aktualizáciu produktu ESET Security pre Microsoft SharePoint, nájdete tu.

Nepoužívajte túto úlohu na aktualizáciu súčastí ESMC
Úlohu Inštalácia softvéru nepoužívajte na aktualizáciu súčastí ESMC, ako sú agent, server a MDM. Namiesto toho použite úlohu Aktualizácia súčastí.

4.7.14 Odinštalovanie softvéru

Úloha **Odinštalovanie softvéru** je určená na odinštalovanie produktov ESET z klientskych počítačov. Ak odinštalujete ESET Management Agenta z klientskeho počítača, bezpečnostný produkt ESET si môže ponechať niektoré nastavenia aj napriek tomu, že ESET Management Agent bol už odinštalovaný.

Dôležité:
Predtým, ako zrušíte spravovanie zariadenia, odporúčame pomocou politiky obnoviť niektoré nastavenia, ktoré si nechcete ponechať (napríklad ochranu heslom), naspäť na predvolené nastavenia. Všetky úlohy spustené na agente budú zrušené. Stavy vykonania úloh **Spustené**, **Dokončené** alebo **Zlyhalo** nemusia byť pre túto úlohu zobrazené v ESMC Web Console presne. Závisí to od replikácie. Po odinštalovaní agenta môžete spravovať svoj bezpečnostný produkt prostredníctvom integrovaného EGUI alebo eShell.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

Nastavenia odinštalovania softvéru

Odinštalovať – aplikáciu zo zoznamu:

- **Názov balíka** – vyberte komponent ESMC, bezpečnostný produkt alebo aplikáciu tretej strany. V zozname sú zobrazené všetky balíky, ktoré môžu byť odinštalované z označeného klienta.
- **Verzia balíka** – môžete odinštalovať buď konkrétnu verziu aplikácie (niekedy môže konkrétna verzia spôsobovať problémy), alebo použiť možnosť **Odinštalovať všetky verzie balíka**.
- **Parametre odinštalovania** – môžete zadať parametre odinštalovania.
- **Automaticky reštartovať, keď je to potrebné** – táto funkcia umožňuje vynútiť reštart operačného systému klienta, ak to odinštalovanie vyžaduje.

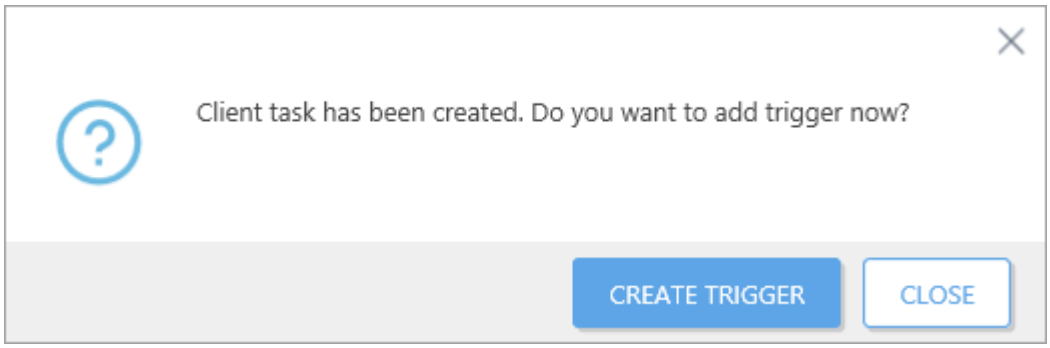
Odinštalovať – antivírusový softvér tretej strany (so vstavaným OPSWAT) – zoznam kompatibilného antivírusového softvéru nájdete v našom článku databázy znalostí. Tento spôsob odinštalovania softvéru je odlišný od funkcie **Pridať alebo odstrániť programy**. Ide tu o úplné odstránenie antivírusových programov tretích strán vrátane registrov.

Postupujte podľa podrobných inštrukcií nachádzajúcich sa v článku Ako odstránim antivírusový softvér tretej strany z klientskych počítačov použitím ERA? (6.x) pre odoslanie úlohy na odstránenie antivírusového softvéru tretej strany z klientskeho počítača.

Ak chcete povoliť odinštalovanie aplikácií chránených heslom, postupujte podľa nášho článku databázy znalostí.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



POZNÁMKA:
Odinštalovanie produktu ESET môže zlyhať kvôli chybovej správe súvisiacej s heslom, napr.: `Product: ESET Endpoint Security -- Error 5004. Enter a valid password to continue uninstallation`. Je to spôsobené tým, že v bezpečnostnom produkte ESET je zapnutá ochrana nastavení heslom. Pre odstránenie ochrany heslom je potrebné aplikovať politiku na klientske počítače. Potom už môžete odinštalovať bezpečnostný produkt ESET pomocou úlohy „Odinštalovanie softvéru“.

4.7.15 Aktivácia produktu

Postupujte podľa krokov uvedených nižšie, ak chcete aktivovať bezpečnostný produkt spoločnosti ESET na klientskom počítači alebo mobilnom zariadení.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

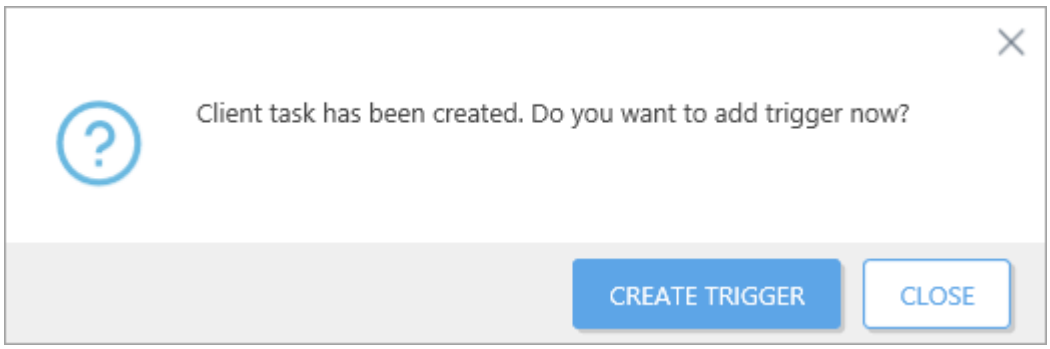
Nastavenia

Nastavenia aktivácie produktov – zo zoznamu vyberte príslušnú licenciu pre počítač. Následne bude táto licencia použitá pre už nainštalovaný produkt na počítači. Ak sa v zozname nenachádzajú žiadne licencie, prejdite do časti Licencie – pridanie novej licencie.

Dôležité:
Úloha **Aktivácia produktu** nemôže byť spustená na mobilných zariadeniach (**ESET Endpoint pre Android** a **MDM pre iOS**), ak sa používa offline licencia.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.16 Vyžiadanie SysInspector protokolu (iba Windows)

Úloha **Vyžiadať SysInspector protokol** je určená na vyžiadanie SysInspector protokolu z klientskych bezpečnostných produktov, ktoré majú túto funkciu.

Základné

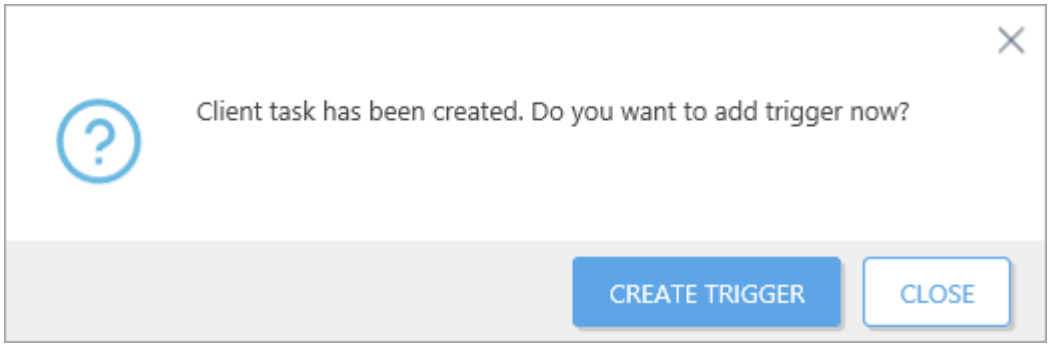
Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

- **Ukladať protokol na strane klienta** – túto možnosť vyberte vtedy, ak chcete ukladať protokol na strane klienta aj na ESMC Server. Napríklad, ak je na klientskom počítači nainštalovaný produkt ESET Endpoint Security, protokol je uložený v umiestnení *C:\Program Data\ESET\ESET Endpoint Antivirus\SysInspector*.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.17 Odovzdanie súboru v karanténe

Úloha **Odovzdať súbor v karanténe** je určená na správu súborov umiestnených v karanténe na klientskych počítačoch. Súbor nachádzajúci sa v karanténe môžete odovzdať do konkrétneho umiestnenia priamo z karantény na účely podrobnejšej analýzy.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

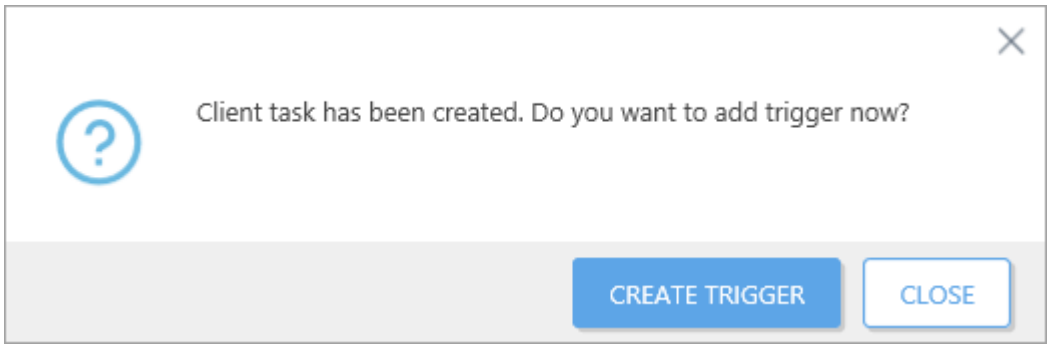
Nastavenia

- **Objekt v karanténe** – vyberte konkrétny objekt z karantény.
- **Heslo k objektu** – zadajte heslo na šifrovanie súboru z bezpečnostných dôvodov. Heslo bude zobrazené v príslušnej správe (zázname).
- **Cesta na odovzdanie** – cesta k adresáru, do ktorého chcete súbor odovzdať.
- **Odovzdať používateľské meno/Odovzdať heslo** – v prípade, že prístup k adresáru vyžaduje autorizáciu, zadajte prihlasovacie údaje na prístup k adresáru.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť

spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.18 Aktualizácia modulov

Úloha **Aktualizácia modulov** je určená na aktualizovanie všetkých modulov bezpečnostného produktu spoločnosti ESET nainštalovaného na klientskom zariadení. Táto úloha je dostupná pre všetky produkty a operačné systémy. Zoznam všetkých modulov produktu nájdete v sekcii **O programe** v danom bezpečnostnom produkte.

Základné

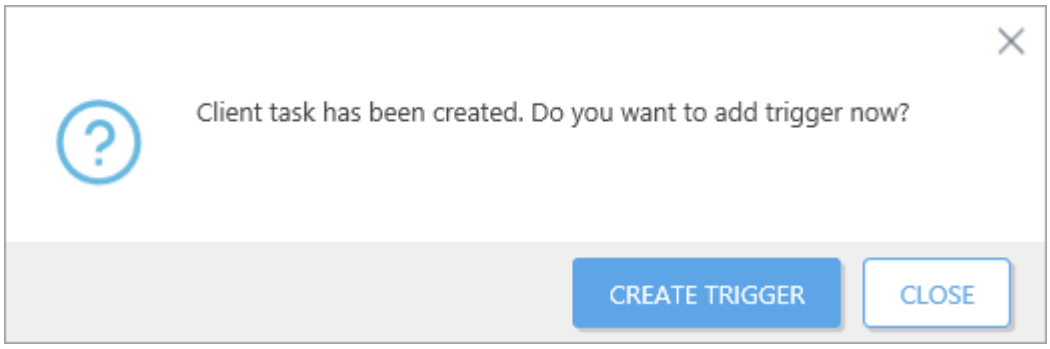
Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

- **Vyčistiť aktualizačnú vyrovnávaciu pamäť** – táto možnosť odstráni dočasné aktualizačné súbory z klientskeho počítača a často môže pomôcť vyriešiť problémy a chyby pri aktualizácii modulov.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.19 Vrátenie zmien aktualizácie modulov

V prípade, že aktualizácia modulov spôsobuje problémy, prípadne nechcete aktualizovať moduly na všetkých klientskych počítačoch (napríklad na účely testovania alebo pri používaní predbežných aktualizácií), môžete použiť úlohu **Vrátenie zmien aktualizácie modulov**. Po použití tejto úlohy sa moduly vrátia do svojej predchádzajúcej verzie.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

Rozbaľte túto sekciu a podľa vlastných potrieb upravte nastavenia pre vrátenie zmien aktualizácie modulov.

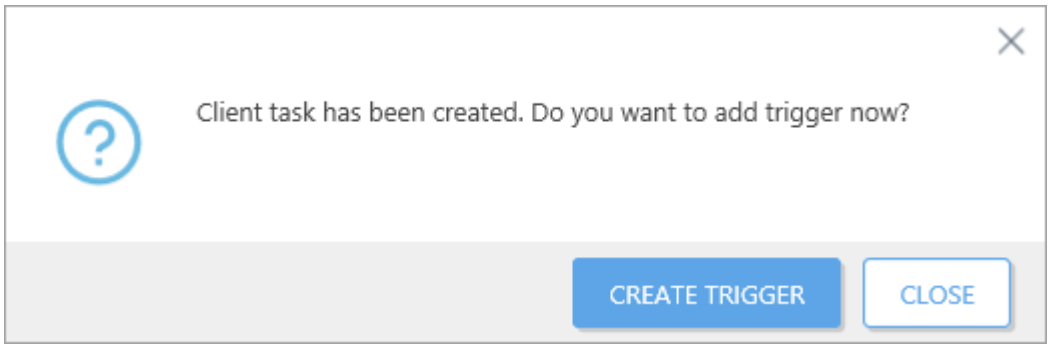
Akcia

- **Povoliť aktualizácie** – aktualizácie budú povolené a klient získa najbližšiu dostupnú aktualizáciu modulov.
- **Vrátiť zmeny a pozastaviť aktualizácie na** – aktualizácie budú pozastavené na čas nastavený v roletovom menu **Interval vypnutia** (24, 36, 48 hodín alebo do zrušenia).

Dôležité:
Povolením možnosti **Do zrušenia** vystavujete počítač možným bezpečnostným rizikám.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.20 Zobrazenie správy

Funkcia **Zobraziť správu** vám umožňuje odoslať správu na akékoľvek spravované zariadenie (počítač, tablet, mobil atď.). Táto správa sa používateľovi zobrazí na obrazovke zariadenia.

- Na systéme Windows sa správa zobrazí ako oznámenie.

Dôležité:
Na operačnom systéme Windows používa úloha pre klienta „Zobraziť správu“ príkaz msg.exe, ktorý je dostupný len v rámci edícií Windows Professional/Enterprise. Z tohto dôvodu nie je možné použiť túto úlohu na zobrazenie správy na klientskom počítači, na ktorom sa používa edícia Windows Home.

- Na systémoch macOS a Linux sa správa zobrazí iba v termináli.

Poznámka:
Pre zobrazenie správy na systéme macOS alebo Linux je potrebné najprv otvoriť terminál.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

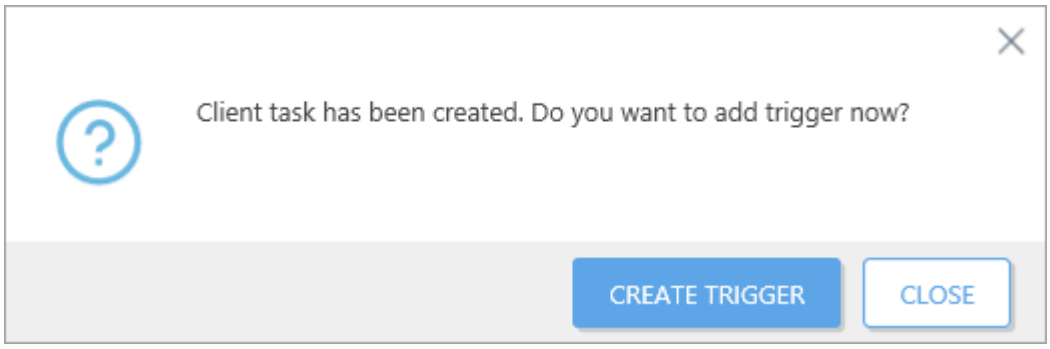
Nastavenia

Môžete zadať **Nadpis** a napísať **Správu**.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť

spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.21 Anti-Theft akcie

Funkcia **Anti-Theft** chráni vaše mobilné zariadenie pred neoprávneným prístupom.

Ak je mobilné zariadenie (registrované a spravované v ESMC) stratené alebo ukradnuté, niektoré akcie sú spustené automaticky, kým ostatné akcie môžu byť vykonané pomocou úlohy pre klienta.

Ak neoprávnený používateľ vymení dôveryhodnú SIM kartu za nedôveryhodnú, zariadenie bude automaticky **zamknuté** produktom ESET Endpoint Security pre Android a zároveň bude odoslaná SMS správa s upozornením na telefónne číslo, ktoré bolo zadané používateľom. Táto správa bude obsahovať nasledujúce informácie:

- telefónne číslo aktuálne vloženej SIM karty,
- číslo **IMSI** (International Mobile Subscriber Identity),
- číslo **IMEI** mobilného zariadenia (International Mobile Equipment Identity).

Neoprávnený používateľ nebude vedieť o odoslaní tejto správy, pretože správa bude po odoslaní vymazaná z telefónu. Môžete si tiež vyžiadať **GPS** súradnice strateného telefónu alebo vzdialene zmazať všetky dáta na zariadení pomocou úlohy pre klienta.

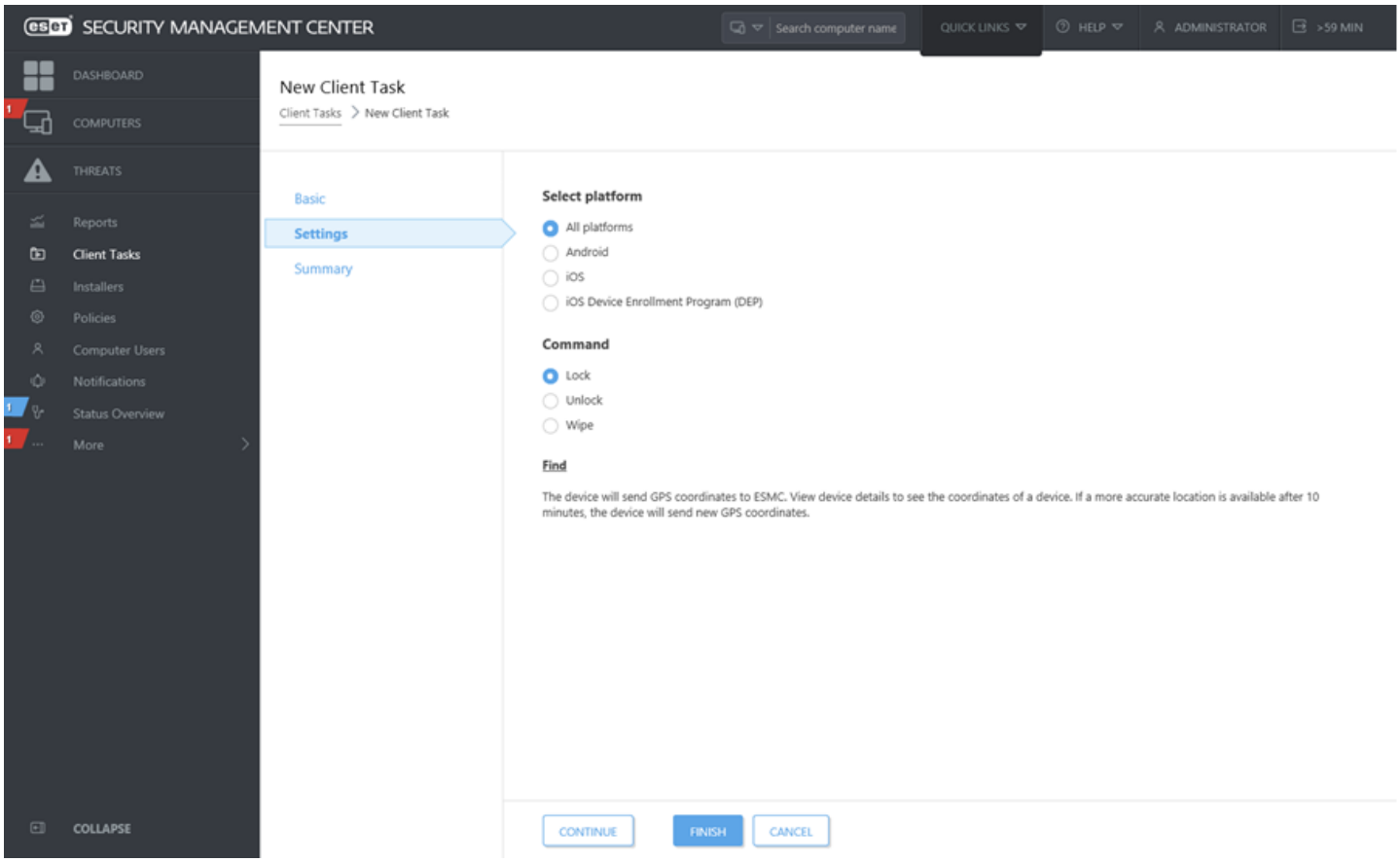
Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Nastavenia

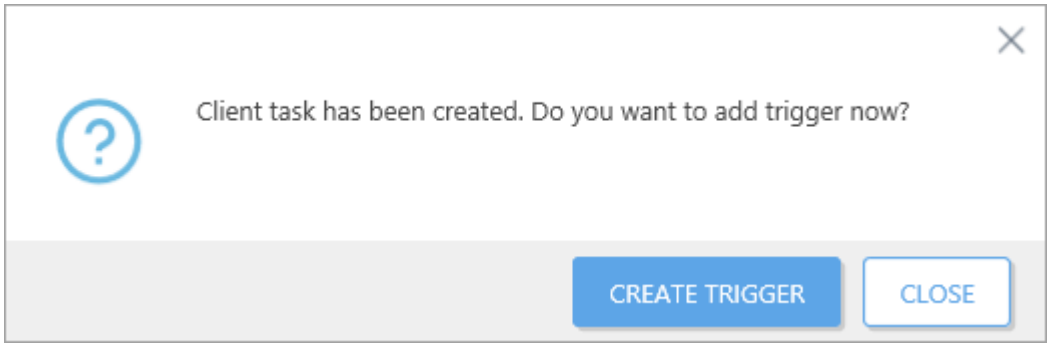
Akcia	Správanie na mobilných OS	Popis
Hľadať		Zariadenie odpovie SMS správou obsahujúcou GPS súradnice. Ak sú po 10 minútach dostupné presnejšie súradnice, bude odoslaná ďalšia správa. Získané informácie sa zobrazujú v časti Podrobnosti o počítači.
		Nepodporované.
Zamknúť		Zariadenie bude zamknuté. Môžete ho odomknúť pomocou hesla správcu alebo vzdialeným príkazom.
		Zariadenie bude zamknuté. Môžete ho odomknúť pomocou prístupového kódu iOS alebo vzdialeným príkazom.
Odomknúť		Zariadenie bude odomknuté a bude môcť byť znova používané. SIM karta v telefóne bude tým pádom uložená ako dôveryhodná SIM karta.

		Zariadenie bude odomknuté a bude môcť byť znova používané.
Siréna		Zariadenie bude zamknuté a na dobu 5 minút spustí veľmi hlasnú sirénu (pokiaľ nebude odomknuté).
		Nepodporované.
Vymazať		Všetky údaje uložené na zariadení budú zmazané bez možnosti obnovenia. Produkt ESET Endpoint Security pre Android zostáva po vymazaní údajov aj naďalej nainštalovaný na zariadení. Tento proces môže trvať niekoľko hodín.
		Všetky údaje uložené na zariadení budú zmazané bez možnosti obnovenia. Tento proces môže trvať niekoľko hodín.
Rozšírené obnovenie výrobných nastavení		Všetky údaje uložené na zariadení budú zmazané bez možnosti obnovenia a zariadenie bude obnovené na jeho výrobné nastavenia. Tento proces môže trvať niekoľko minút. Táto akcia nie je dostupná z kontextového menu **Počítače** > .
		Nepodporované.
Hľadať (Zapnúť režim strateného zariadenia)		Táto možnosť je dostupná len na zariadeniach, na ktoré sa vzťahuje program iOS DEP. Zariadenie sa prepne do režimu strateného zariadenia, uzamkne sa a následne bude môcť byť odomknuté iba spustením úlohy **Vypnúť režim strateného zariadenia** prostredníctvom nástroja ESMC. Môžete zároveň upraviť text správy, ktorá sa zobrazí na obrazovke strateného zariadenia.
Vypnúť režim strateného zariadenia		Táto možnosť je dostupná len na zariadeniach, na ktoré sa vzťahuje program iOS DEP.



Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.22 Ukončenie spravovania (odinštalovanie ESET Management Agenta)

Pomocou tejto úlohy je možné odinštalovať ESET Management Agenta z vybraných cieľových zariadení. Ak je zvolená pracovná stanica, úloha odstráni ESET Management Agenta. Ak je zvolené mobilné zariadenie, úloha zruší MDM registráciu daného zariadenia.

Po ukončení spravovania (odstránení agenta) daného zariadenia môžu byť niektoré nastavenia ponechané v konfigurácii spravovaných produktov.

Dôležité:
Predtým, ako zrušíte spravovanie zariadenia, odporúčame pomocou politiky obnoviť niektoré nastavenia, ktoré si nechcete ponechať (napríklad ochranu heslom), naspäť na predvolené nastavenia. Všetky úlohy spustené na agente budú zrušené. Stavy vykonania úloh **Spustené**, **Dokončené** alebo **Zlyhalo** nemusia byť pre túto úlohu zobrazené v ESMC Web Console presne. Závisí to od replikácie. Po odinštalovaní agenta môžete spravovať svoj bezpečnostný produkt prostredníctvom integrovaného EGUI alebo eShell.

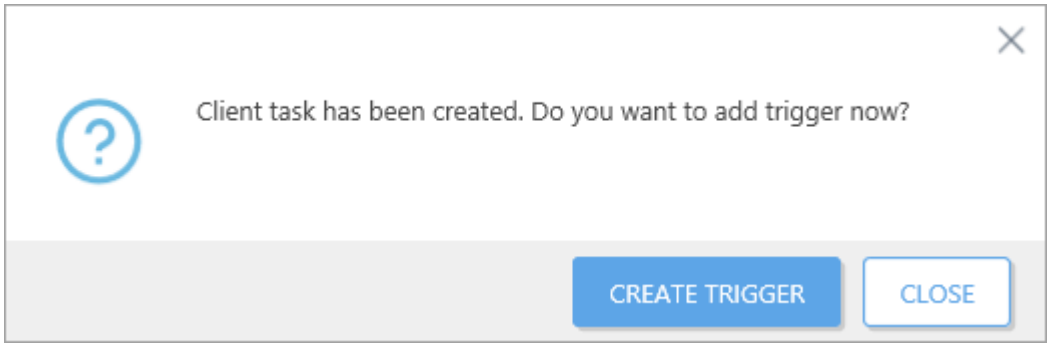
Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

Poznámka:
Pre túto úlohu nie sú dostupné žiadne **nastavenia**.

Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.23 Export konfigurácie spravovaných produktov

Úloha **Exportovať konfiguráciu spravovaných produktov** je určená na export nastavení jednotlivých komponentov ESMC alebo bezpečnostných produktov spoločnosti ESET nainštalovaných na klientskych počítačoch.

Základné

Sem môžete zadať základné informácie o úlohe, ako napr. **Názov**, prípadne môžete zadať **Popis**. **Kategória úlohy** a **Typ úlohy** sú zvolené automaticky podľa vášho predchádzajúceho výberu. **Typ úlohy** (pozrite si zoznam všetkých úloh pre klienta) definuje nastavenia a správanie danej úlohy.

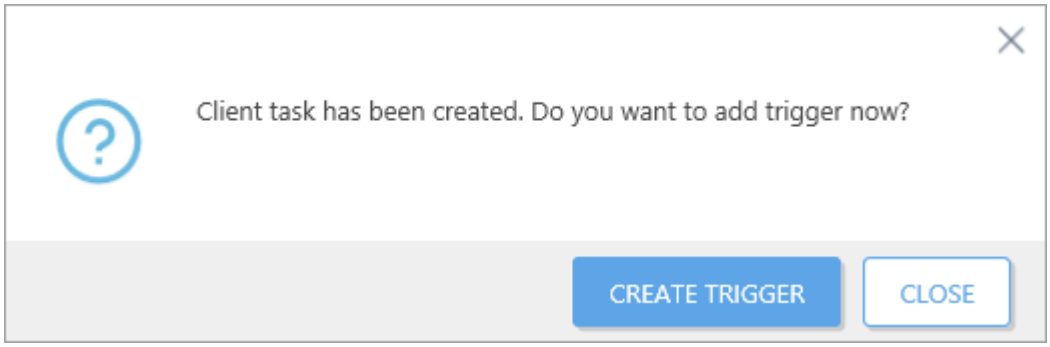
Nastavenia

Export konfigurácie spravovaných produktov

- **Produkt** – vyberte ESMC komponent alebo bezpečnostný produkt, pre ktorý chcete exportovať nastavenia.

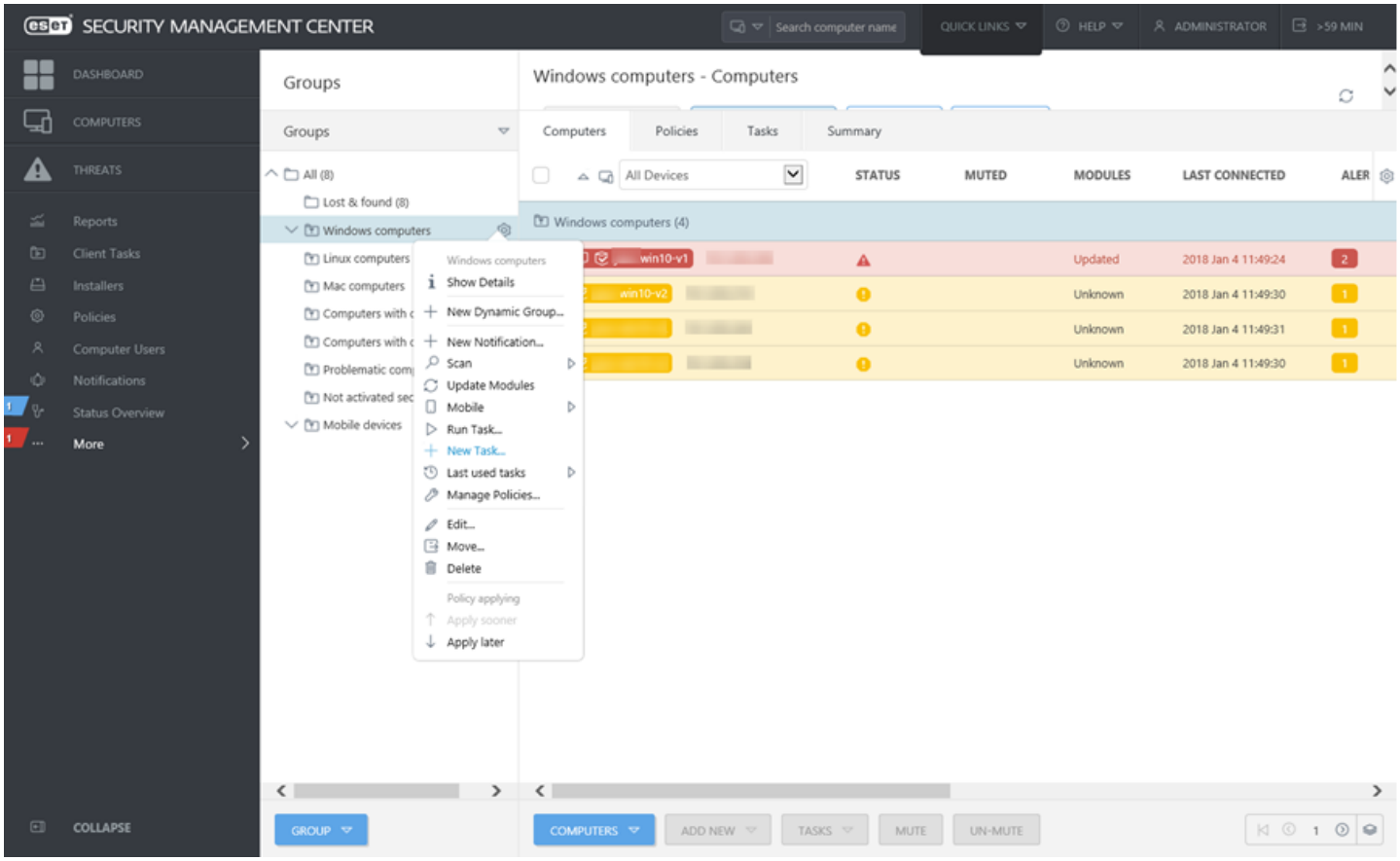
Súhrn

Skontrolujte súhrn nastavení a kliknite na **Dokončiť**. Úloha pre klienta bude následne vytvorená a zobrazí sa kontextové okno. Odporúčame vám kliknúť na možnosť Vytvoriť spúšťač pre upresnenie, kedy bude táto úloha pre klienta vykonaná a na akých cieľoch. Ak kliknete na **Zatvoriť**, spúšťač budete môcť vytvoriť neskôr. Ak chcete vytvoriť spúšťač neskôr, kliknite na danú úlohu pre klienta a v kontextovom menu vyberte možnosť **Spustiť na...**



4.7.24 Priradenie úlohy ku skupine

Kliknite na **Viac** > **Skupiny** > vyberte **Statickú** alebo **Dynamickú** skupinu > ⚙ vedľa označenej skupiny alebo kliknite na **Skupina** > + **Nová úloha**.

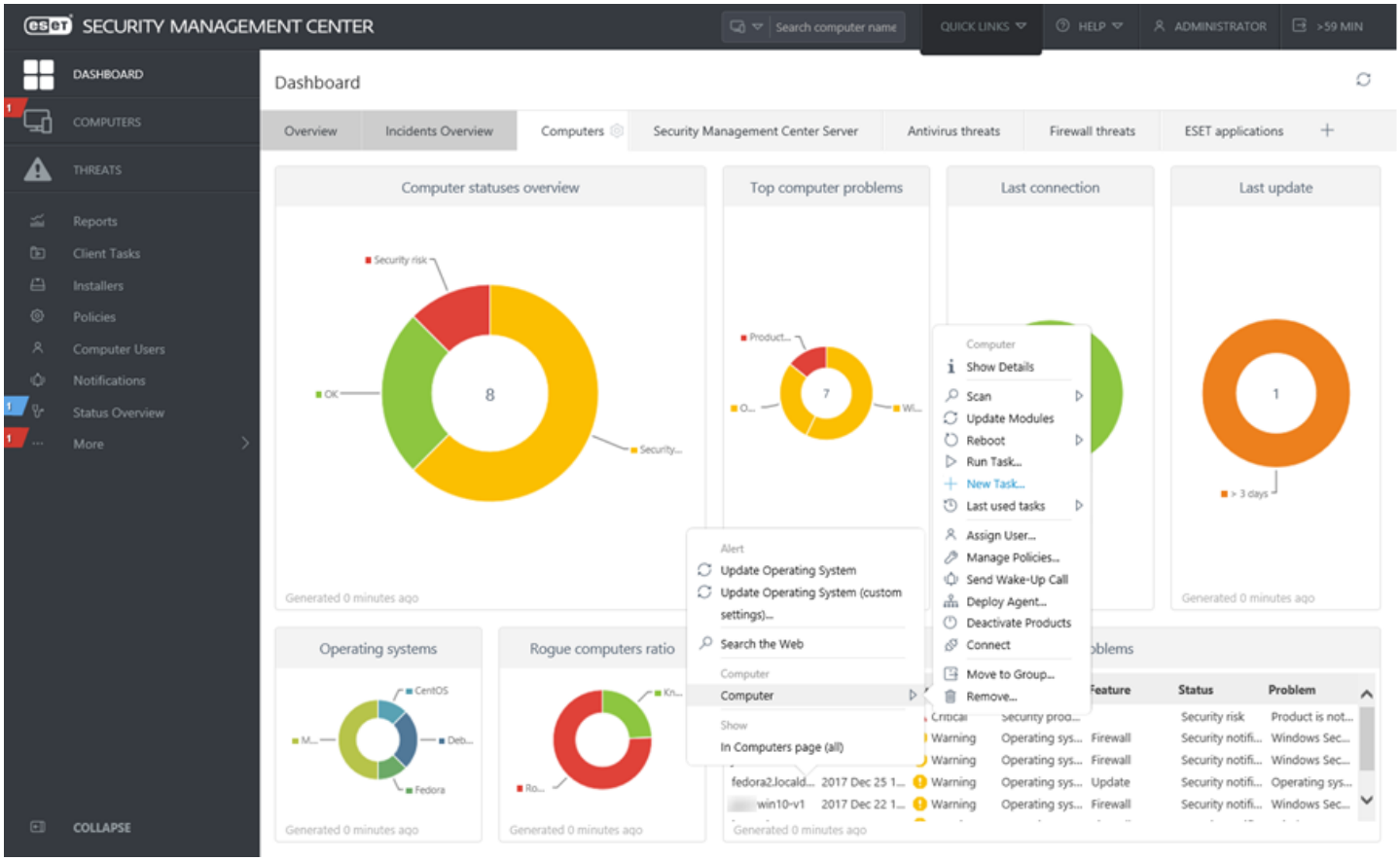


Rovnako môžete postupovať aj cez **Počítače** – vyberte **Statickú** alebo **Dynamickú skupinu** a kliknite na ⚙ > + **Nová úloha**. Následne sa zobrazí Sprievodca vytvorením novej úlohy pre klienta.

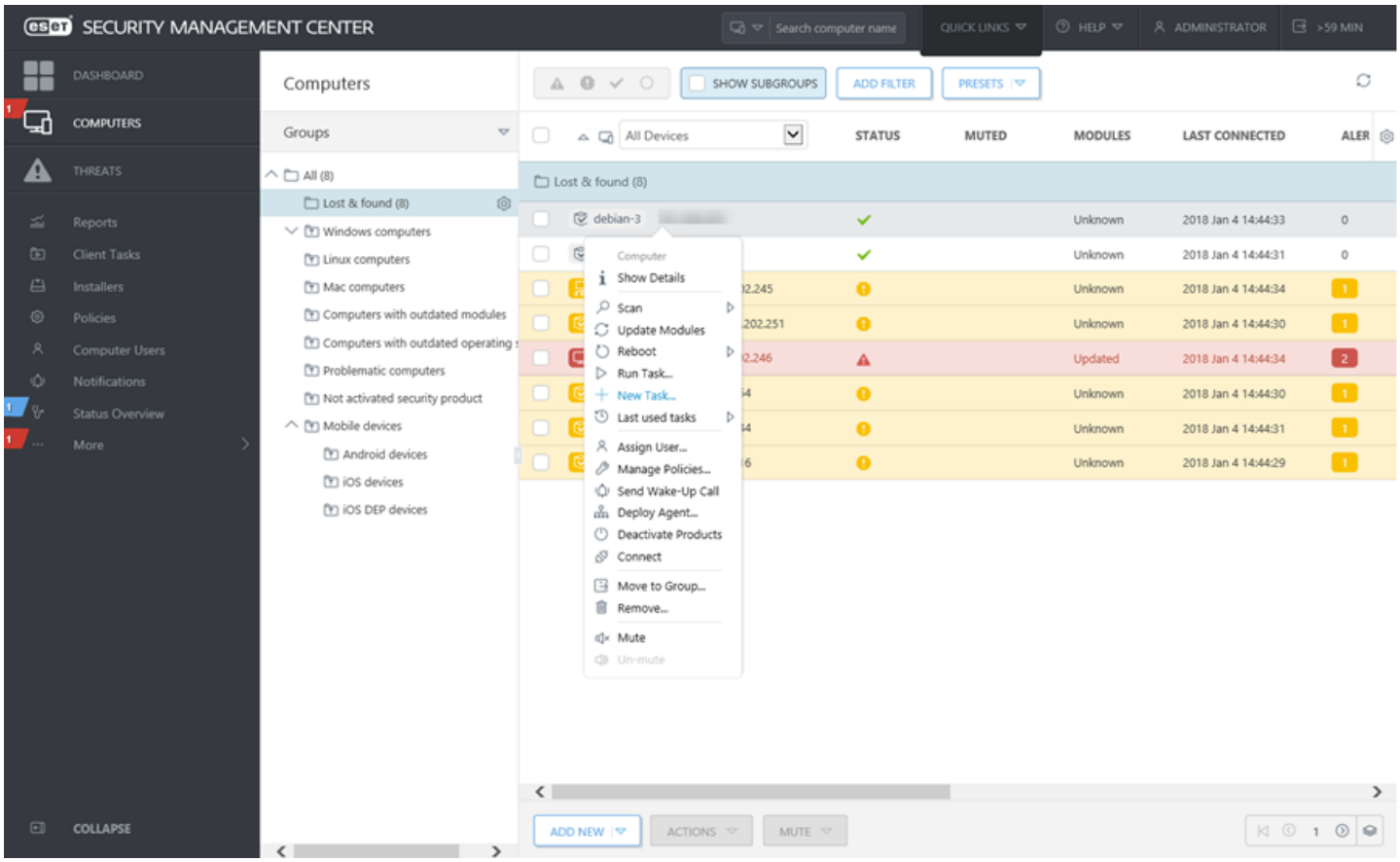
4.7.25 Priradenie úlohy k počítačom

Sú dostupné tri možnosti priradenia úlohy k počítaču:

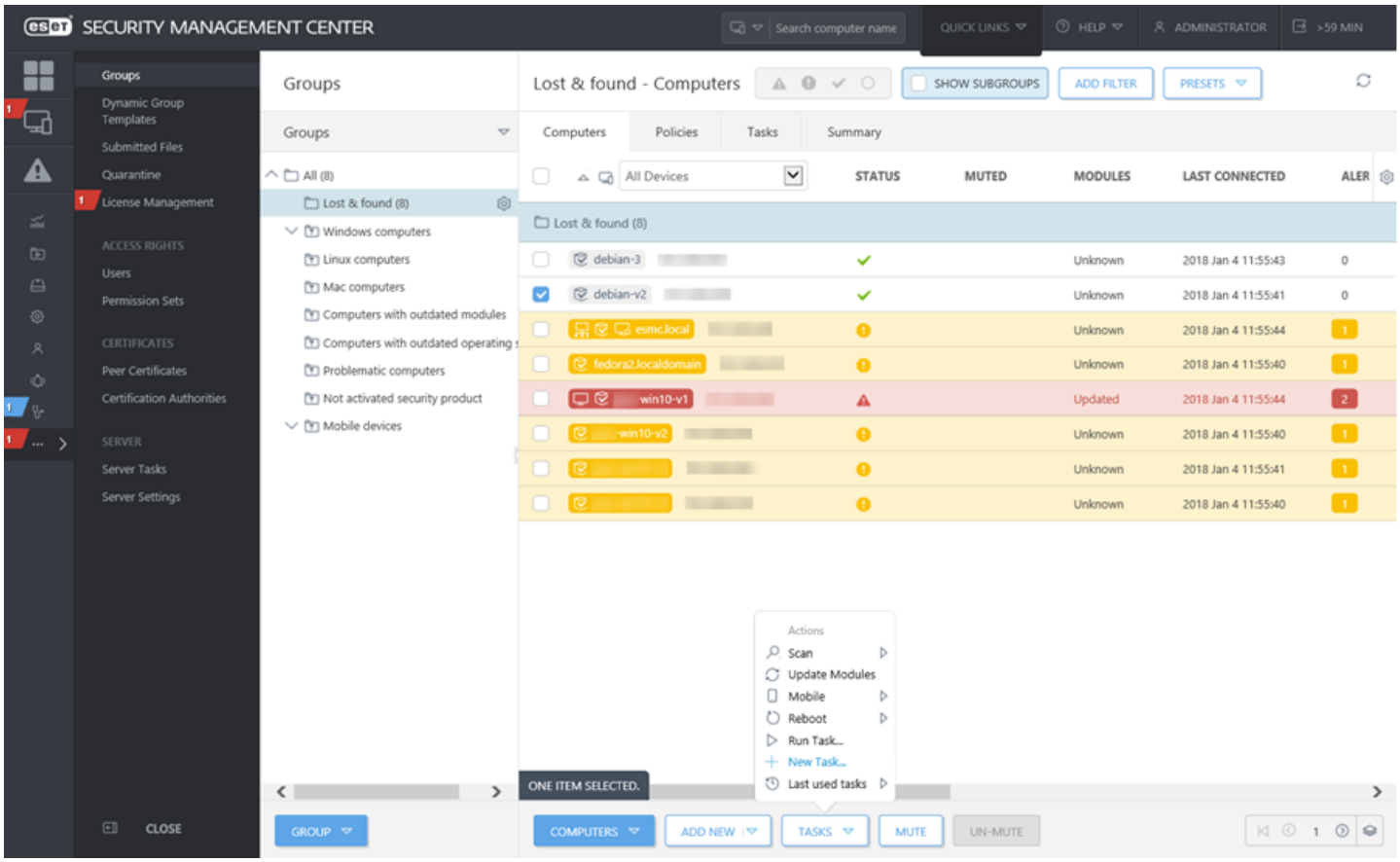
1. **Riadiaci panel** > **Počítače s problémami** > vyberte počítač, kliknite na **Počítač** a vyberte možnosť + **Nová úloha**.



2. **Počítač** > vyberte počítač/počítače pomocou začiarkavacích políčok a vyberte možnosť + **Nová úloha**.



3. **Viac** > **Skupiny** > vyberte počítač/počítače > kliknite na **Úlohy** a zvoľte možnosť + **Nová úloha**.



Následne sa zobrazí Sprievodca vytvorením novej úlohy pre klienta.

4.7.26 Spúšťače úloh pre klienta

Spúšťače sú senzory, ktoré reagujú na určité udalosti vopred definovaným spôsobom. Slúžia na spúšťanie úloh pre klienta, ku ktorým sú priradené. Môžu byť aktivované pomocou Plánovača (naplánovanej úlohy) alebo systémovou udalosťou.

Dôležité:
Jednotlivé spúšťače nie je možné opätovne priradiť k ďalším úlohám. Každá úloha pre klienta musí používať samostatný spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre klienta.

Spúšťač nespúšťa novopriradené úlohy okamžite (okrem spúšťača nastaveného na najskoršie možné spustenie), miesto toho sú úlohy spustené vtedy, keď spúšťač dostane impulz. Citlivosť spúšťača pre rôzne udalosti je možné redukovať pomocou obmedzovania.

Typy spúšťačov úloh pre klienta:

- **Hneď ako to bude možné** – tento spúšťač spustí úlohu hneď po tom, ako kliknete na tlačidlo **Dokončiť**. Hodnota uvedená v poli **Dátum skončenia platnosti** definuje dátum, po uplynutí ktorého úloha už nebude vykonaná.

Naplánované

- **Naplánovať raz** – tento spúšťač spustí úlohu raz v presne naplánovaný dátum a čas. Môžete tiež zadať maximálny čas, o ktorý sa spustenie úlohy môže oneskoriť.
- **Denne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch. Môžete zadať začiatok a koniec časového intervalu, počas ktorého sa bude úloha spúšťať. Môžete napríklad zvoliť, aby sa úloha spúšťala vždy cez víkendové dni po dobu desiatich za sebou idúcich týždňov.
- **Týždenne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch týždňa. Môžete napríklad zvoliť, aby sa úloha spúšťala každý pondelok a piatok v období od 1. júla do 31. augusta.
- **Mesačne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch a zvolenom týždni mesiaca počas vami stanoveného obdobia. Hodnota zadaná do poľa **Opakovať** definuje pracovný deň v mesiaci (napríklad druhý pondelok), počas ktorého bude úloha spustená.
- **Ročne** – tento spúšťač spustí úlohu každý rok (alebo každých niekoľko rokov, ak použijete toto nastavenie) v deň a čas, ktorý zadáte do poľa Štart.

Poznámka:
Náhodný interval oneskorenia je možné nastaviť pre všetky naplánované typy spúšťačov. Toto nastavenie určuje maximálny čas, o ktorý sa spustenie úlohy môže oneskoriť. Použitie náhodných oneskorení vykonania plánovaných úloh pomáha predchádzať vyťaženiu servera.

PRÍKLAD:
Ak používateľ *John* pre **Úlohu pre klienta** nastavil spúšťač na hodnotu **Týždenne**, zvolil deň opakovania na *pondelok*, do poľa **Štart** zadal *2017 feb 10 8:00:00*, **Náhodný interval oneskorenia** nastavil na *1 hodinu* a do poľa **Ukončiť do** zadal *2017 apr 6 00:00:00*, úloha bude spúšťaná s náhodným maximálne hodinovým oneskorením medzi 8:00 a 9:00 každý pondelok až do stanoveného dátumu a času ukončenia.

Poznámka:
Označením možnosti **Vyvolať súrne, ak dôjde k zmeškaniu udalosti** dôjde k okamžitému spusteniu úlohy, ak daná úloha nebola spustená v zadanom čase.

Označením možnosti **Použiť miestny čas** sa na vykonanie úlohy použije čas na cieľovom zariadení namiesto časového pásma, v ktorom je ESMC Web Console.

Iné

- **Spúšťač pri vstupe do dynamickej skupiny** – tento spúšťač sa aktivuje vždy v prípade, že klientske zariadenie sa stane súčasťou zvolenej dynamickej skupiny.
- **Spúšťač protokolu udalosti** – tento spúšťač sa aktivuje v prípade, že v protokole je zaznamenaná určitá udalosť. Napríklad, ak bola v protokole **Kontroly** počítača zaznamenaná hrozba. Pre tento typ spúšťača sa v sekcii Pokročilé nastavenia - Obmedzovanie nachádza niekoľko špeciálnych nastavení.
- **CRON výraz** – tento spúšťač sa aktivuje v deň a čas stanovený CRON výrazom.

Poznámka:
Spúšťač pri vstupe do dynamickej skupiny je v ponuke typov spúšťačov dostupný len v prípade, že v sekcii **Cieľ** je vybraná dynamická skupina. Spúšťač spustí úlohu len na zariadeniach, ktoré vstúpia do zvolenej dynamickej skupiny po vytvorení daného spúšťača. V prípade zariadení, ktoré boli súčasťou zvolenej dynamickej skupiny už pred vytvorením spúšťača, je úlohu nutné spustiť manuálne.

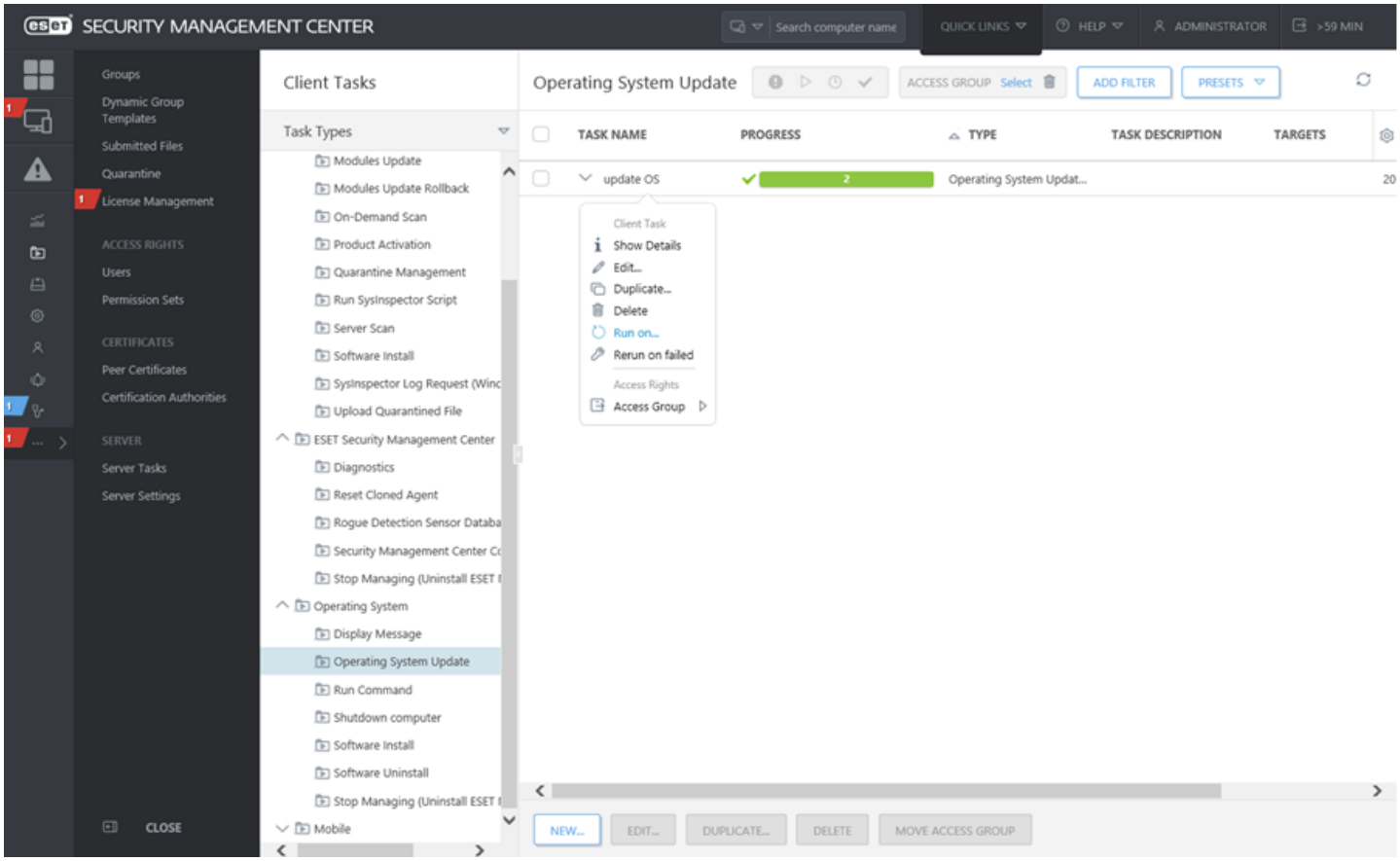
Naplánovaný spúšťač spúšťa úlohu v čase a dátume zadefinovanom v nastaveniach spúšťača. Úloha môže byť naplánovaná tak, aby bola spustená **raz**, opakovane alebo na základe CRON výrazu.

4.7.27 Spúšťanie úloh pre klienta

Aktuálny stav každej úlohy pre klienta môžete sledovať v časti **Úlohy pre klienta**. Pre každú úlohu je zobrazený priebeh úlohy a ikona stavu úlohy. Môžete použiť kontextové menu pre zobrazenie ďalších podrobností úlohy pre klienta a vykonať ďalšie akcie, ako napr. Spustiť na alebo Znovu spustiť pri zlyhaní.

Dôležité:
Na spustenie úloh pre klienta musíte vytvoriť spúšťač.

POZNÁMKA:
Počas tohto procesu je vyhodnocované veľké množstvo dát, čo môže v porovnaní s predošlými verziami vyžadovať viac času na vykonanie úlohy (v závislosti od úlohy pre klienta, spúšťača a celkového počtu počítačov).

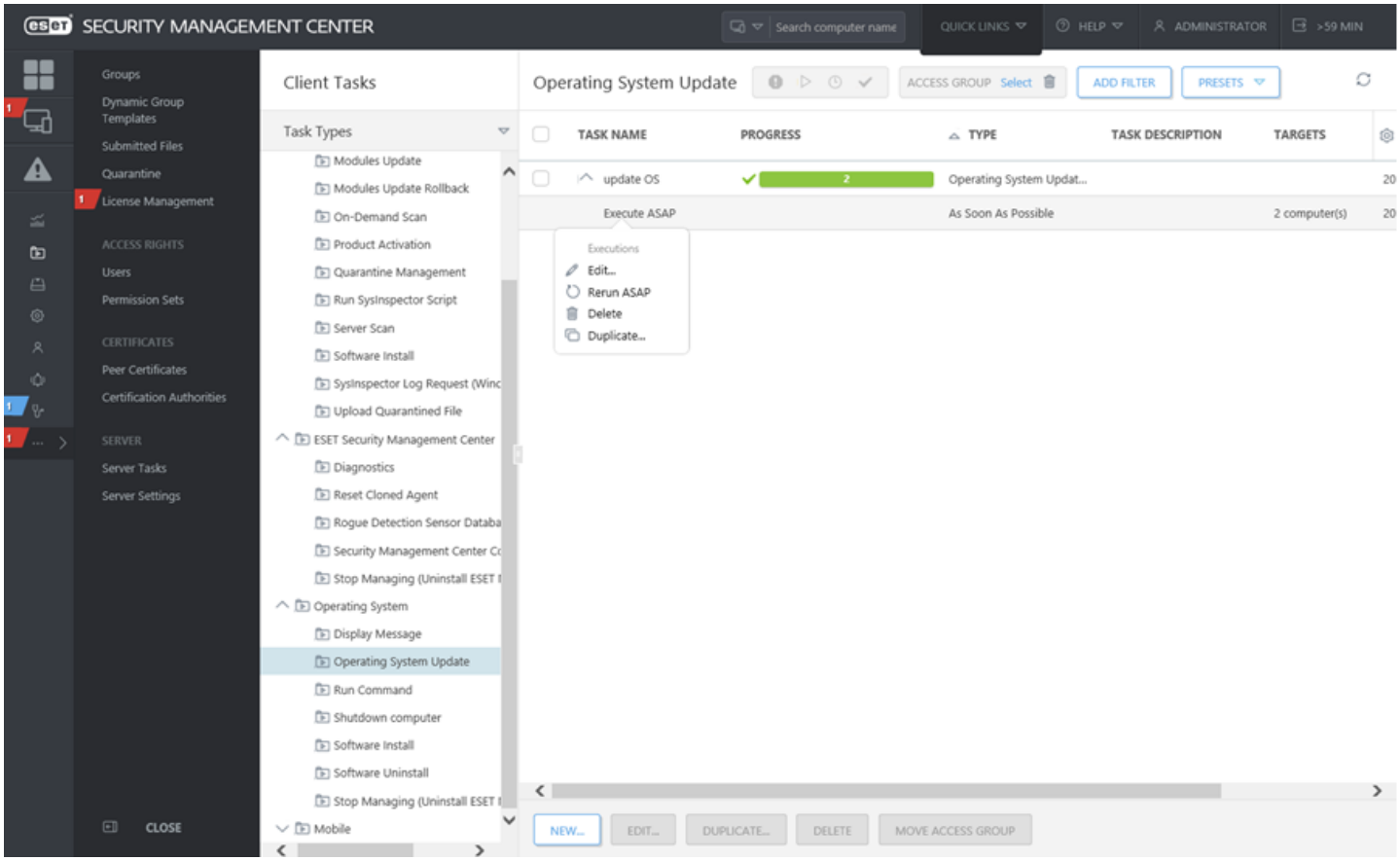


Pre bližšie informácie o rôznych typoch ikon a stavoch si pozrite ikonu stavu úlohy.

Možnosti dostupné pre **Úlohu pre klienta** (kliknite na úlohu pre klienta pre zobrazenie kontextového menu):

Zobraziť podrobnosti	Podrobnosti úlohy pre klienta obsahujú **Súhrn** informácií o úlohe. Kliknite na kartu **Vykonania** pre zobrazenie výsledku každého spustenia úlohy. Na zobrazenie podrobností konkrétnej úlohy pre klienta môžete použiť kontextové menu. Ak je počet vykonaní príliš veľký, môžete použiť filter pre jednoduchšie vyhľadávanie. **Poznámka:** Pri inštalácii starších produktov spoločnosti ESET zobrazí záznam o úlohe pre klienta nasledujúce informácie: **Úloha bola doručená spravovanému produktu**.
Upraviť	Táto funkcia vám umožňuje upravovať označenú úlohu pre klienta. Úprava existujúcej úlohy je užitočná vtedy, keď potrebujete vykonať iba menšie zmeny. V prípade úloh, ktoré sú odlišné od preddefinovaných úloh do väčšej miery, odporúčame vytvoriť si úplne novú, vlastnú úlohu.

Duplikovať	Táto funkcia vám umožňuje vytvoriť novú úlohu na základe označenej úlohy, pričom je nevyhnutné zadať pre duplikovanú úlohu nový (odlišný) názov.
Vymazať	Úplné odstránenie zvolenej úlohy. • Ak je úloha vymazaná po tom, ako bola vytvorená, avšak predtým, ako bolo naplánované jej spustenie, úloha bude vymazaná a nebude nikdy spustená. • Ak je úloha vymazaná po tom, ako bolo naplánované jej spustenie, dôjde k jej vykonaniu, avšak príslušné informácie sa vo Web Console nezobrazia.
Spustiť na	Pridajte nový spúšťač a vyberte cieľové počítače alebo skupiny pre túto úlohu.
Znovu spustiť pri zlyhaní	Vytvorí sa nový spúšťač, pričom všetky počítače, na ktorých bolo počas predošlého spustenia úlohy zaznamenané zlyhanie, budú nastavené ako ciele. Môžete upraviť nastavenia úlohy alebo kliknúť na **Dokončiť** a úloha bude spustená bez zmien.
Prístupová skupina	Umožňuje presunúť úlohu pre klienta do inej statickej skupiny.

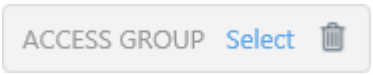


Vykonanie (kliknite na ikonu pre rozbalenie úlohy pre klienta a zobrazenie vykonaní/spúšťačov – pre zobrazenie kontextového menu kliknite na spúšťač):

Upraviť	Táto funkcia vám umožňuje upravovať zvolený spúšťač.
Znovu spustiť čo najskôr	Môžete spustiť úlohu pre klienta znova (čo najskôr) pomocou už existujúceho spúšťača bez potreby akýchkoľvek úprav.
Vymazať	Úplné odstránenie zvoleného spúšťača.
Duplikovať	Duplikovanie umožňuje vytvorenie nového spúšťača na základe označenej správy, pričom je nevyhnutné zadať pre duplikát nový (odlišný) názov.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.7.27.1 Indikátor priebehu

Indikátor priebehu je farebný panel, ktorý zobrazuje stav vykonania úloh pre klienta. Každá úloha pre klienta má vlastný indikátor priebehu (zobrazený v riadku **Priebeh**). Indikátor priebehu zobrazuje stav vykonania úlohy pre klienta v rôznych farbách, obsahuje tiež počet počítačov, na ktorých je úloha v danom stave:

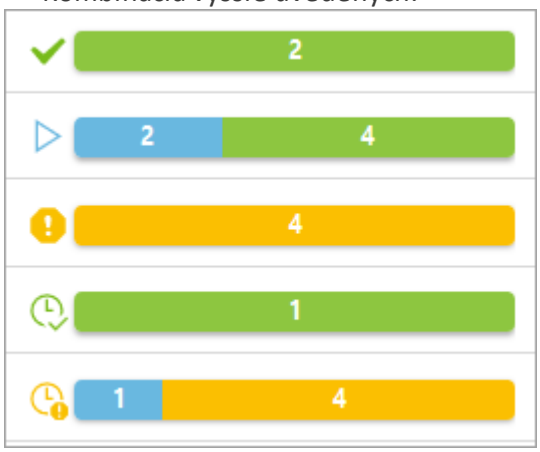
Spustené (modrá)

Úspešne dokončené (zelená)

Zlyhalo (oranžová)

Novovytvorená úloha pre klienta (biela) – zmena farby indikátora môže trvať nejaký čas, pretože ESMC Server musí najprv dostať odpoveď od ESET Management Agenta, aby sa zobrazil stav vykonania úlohy. Indikátor priebehu bude bielej farby aj v prípade, že nebol priradený žiadny spúšťač.

Kombinácia vyššie uvedených:



Po kliknutí na farebnú lištu indikátora si môžete vybrať jednotlivé výsledky vykonaní úloh a vykonať v prípade potreby ďalšie akcie. Bližšie informácie nájdete v časti Kontextové menu.

Pre bližšie informácie o rôznych typoch ikon a stavoch si pozrite ikonu stavu úlohy.

Dôležité:
Indikátor priebehu zobrazuje stav úlohy pre klienta z času, keď bola úloha naposledy vykonaná. Tieto informácie sú zhromažďované ESET Management Agentom. Indikátor priebehu zobrazuje presné informácie nahlásené ESET Management Agentom priamo z klientskeho počítača.

4.7.27.2 Ikona stavu úlohy

Ikona nachádzajúca sa vedľa ukazovateľa priebehu úlohy poskytuje dodatočné informácie. Zobrazuje, či existujú plánované spustenia pre danú úlohu klienta, ako aj výsledok dokončených úloh. Tieto informácie zhromažďuje ESMC Server. Pomocou ikony môžu byť znázornené tieto stavy:

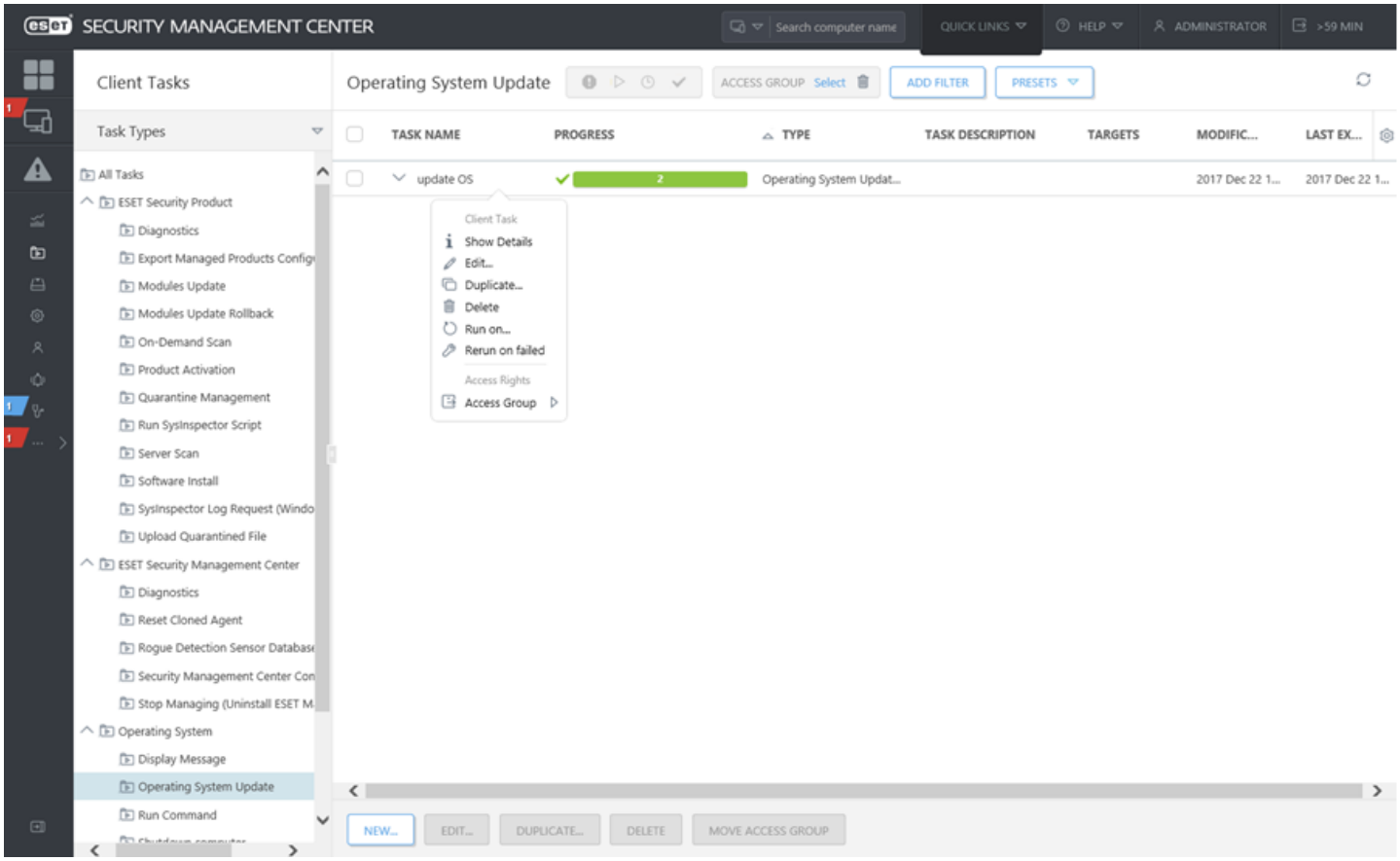
Spustené	Úloha pre klienta je spustená pre aspoň jeden cieľ, nie sú žiadne iné naplánované alebo neúspešne vykonané úlohy. Toto platí aj v prípade, že úlohy už boli na niektorých cieľoch vykonané.
Úspešné	Úloha pre klienta bola úspešne dokončená na všetkých cieľoch, nie sú žiadne iné naplánované alebo spustené úlohy.
Chyba	Vykonanie úlohy je ukončené pre všetky ciele, avšak aspoň na jednom počítači vykonanie úlohy zlyhalo. Nie sú naplánované žiadne ďalšie spustenia úloh.
Plánované	Úloha pre klienta je naplánovaná na spustenie, avšak zatiaľ nie sú spustené žiadne úlohy.
Plánované/spustené	Úloha pre klienta má naplánované spustenie (z minulosti alebo v budúcnosti). Žiadne spustenia nezlyhali a aspoň jedna úloha je práve spustená.
Plánované/úspešné	Úloha pre klienta má naplánované spustenia (z minulosti alebo naplánované v budúcnosti), nie sú žiadne prebiehajúce alebo neúspešne vykonané úlohy a aspoň jedna úloha bola úspešne ukončená.
Plánované/chyba	Úloha pre klienta má naplánované spustenie (z minulosti alebo naplánované v budúcnosti), nie sú žiadne prebiehajúce úlohy a aspoň jedna úloha zlyhala. Toto platí aj v prípade, že úlohy už boli na niektorých cieľoch úspešne vykonané.

4.7.27.3 Zobrazenie podrobností

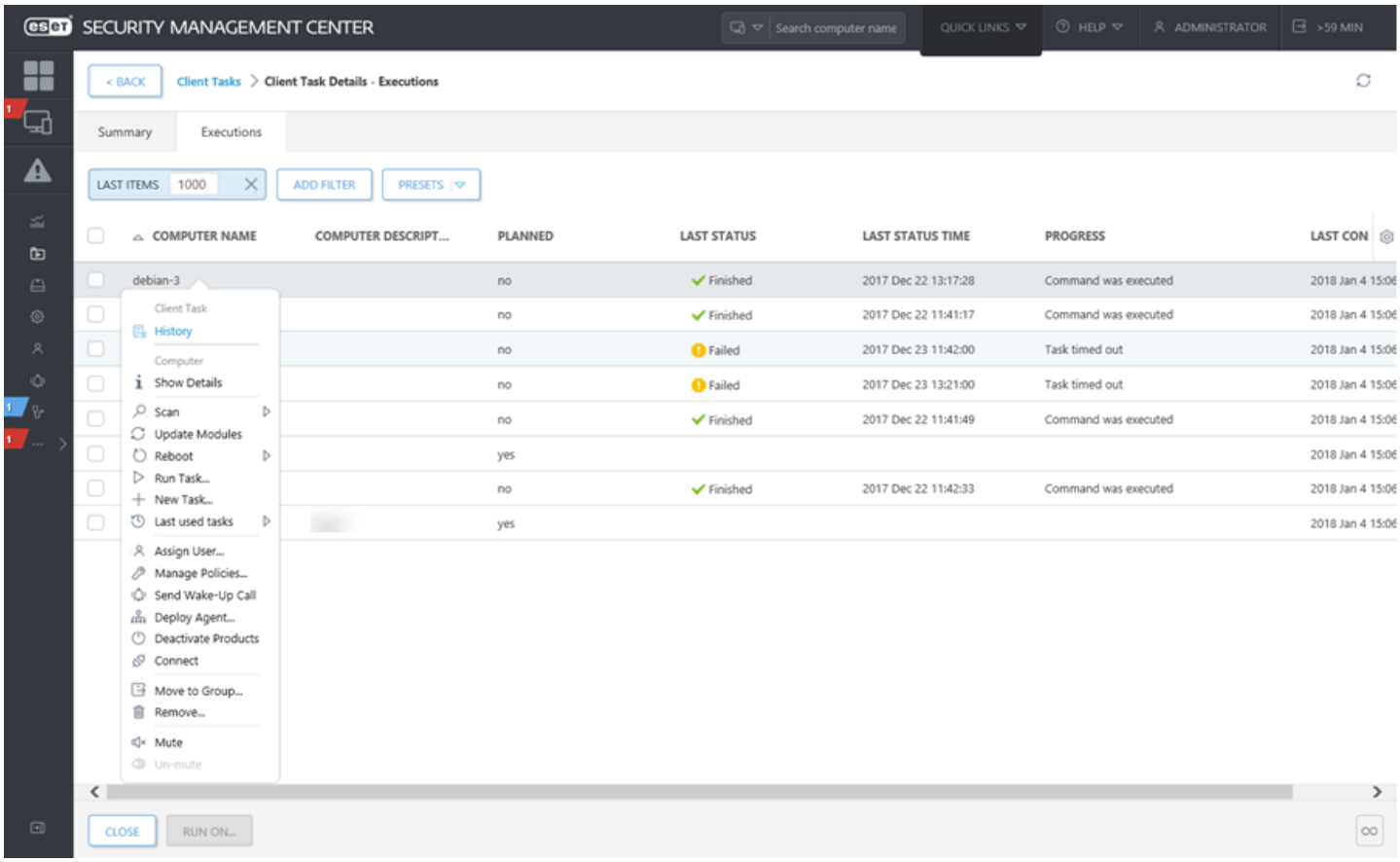
Keď kliknite na farebnú lištu indikátora priebehu, máte na výber nasledujúce možnosti:

- **Ukázať všetko**
- **Zobraziť plánované**
- **Zobraziť spustené**
- **Zobraziť úspešné**
- **Zobraziť zlyhané**

Po výbere ktorejkoľvek z vyššie uvedených možností sa zobrazí dialógové okno s históriou vykonaní úloh. Počítače, na ktorých bol zaznamenaný iný ako zvolený výsledok vykonania úlohy, nebudú zobrazené. Filter môžete zmeniť alebo vypnúť a zobraziť tak všetky počítače bez ohľadu na ich stav.



Môžete kliknúť na položku **História** a zobraziť tak podrobnosti o vykonaní úlohy pre klienta vrátane času **Výskytu**, **Stavu**, **Priebehu** a **Vyhľadania správy** (ak je daná možnosť dostupná). Môžete tiež kliknúť na **Názov počítača** alebo **Popis počítača** a vykonať v prípade potreby ďalšie akcie, prípadne zobraziť podrobnosti počítača konkrétneho klienta.



Poznámka:
Ak v tabuľke histórie spustení úloh nevidíte žiadne položky, skúste nastaviť filter **Výskyt** na dlhšie trvanie.

4.7.27.4 Spúšťač

Spúšťač musí byť priradený k úlohe pre klienta, aby bolo možné úlohu spustiť. Pri vytváraní spúšťača vyberte **cieľové** počítače alebo skupiny, na ktorých má byť daná úloha vykonaná. Po zvolení cieľov nastavte podmienky spúšťača pre spustenie úlohy v určitom čase alebo pri konkrétnej udalosti. Môžete tiež prípadne použiť **Pokročilé nastavenia – Obmedzovanie** pre podrobnejšie nastavenie spúšťača.

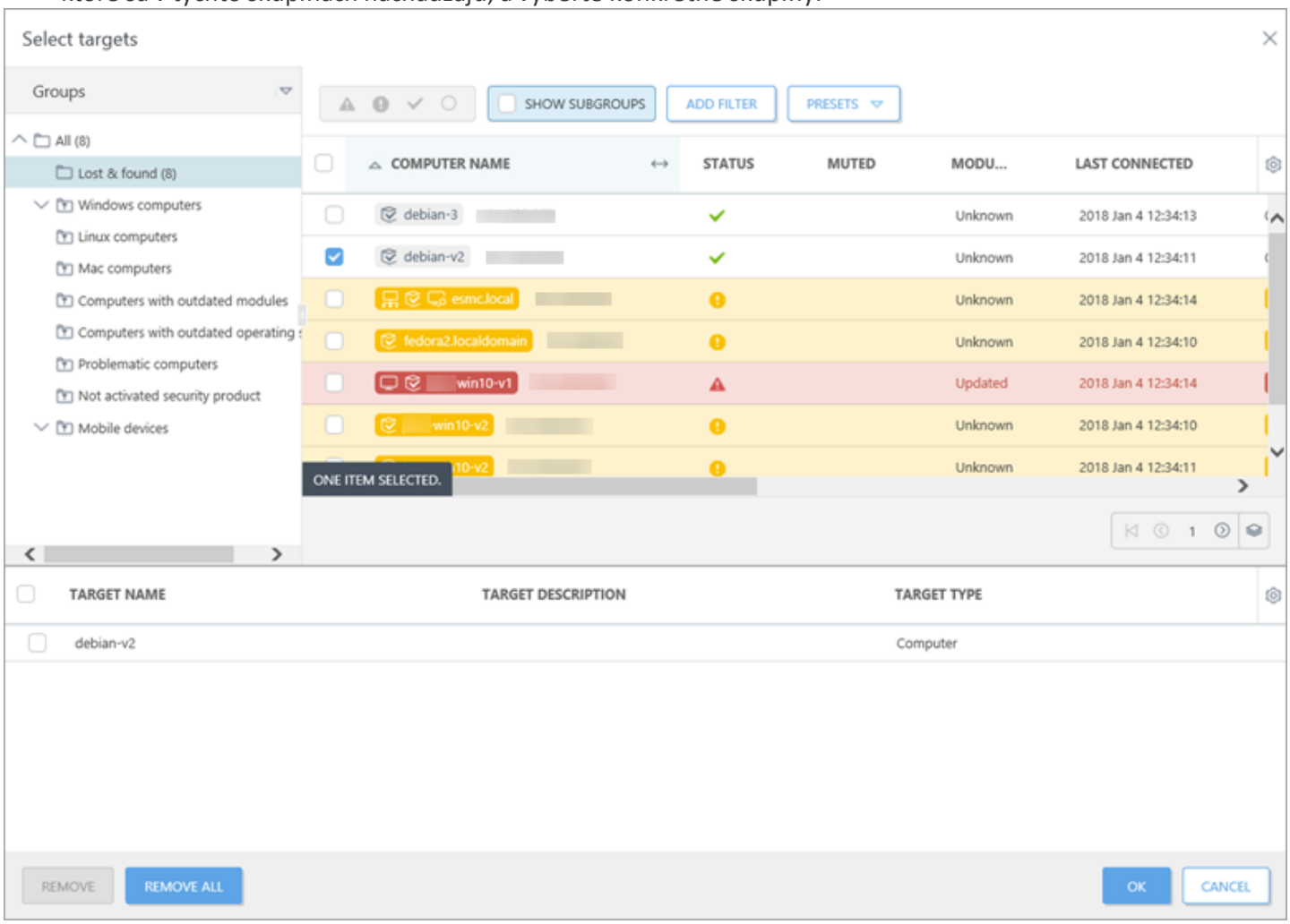
Základné

Zadajte základné informácie o **spúšťači** do poľa **Popis** a potom kliknite na **Cieľ**.

Cieľ

Sekcia **Cieľ** vám umožňuje vybrať klientske počítače (individuálne počítače alebo skupiny), na ktorých bude daná úloha vykonaná.

- Kliknite na možnosť **Pridať počítače** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré sa v týchto skupinách nachádzajú, a vyberte konkrétne zariadenia.
- Kliknite na možnosť **Pridať skupiny** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré sa v týchto skupinách nachádzajú, a vyberte konkrétne skupiny.



Následne kliknite na **OK** a prejdite do sekcie **Spúšťač**.

Spúšťač

Spúšťač určuje, aká udalosť spustí danú úlohu.

- **Hneď ako to bude možné** – úloha bude vykonaná okamžite po pripojení klienta na ESET Security Management Center Server a doručení úlohy na klienta. Ak úloha nemôže byť vykonaná do dátumu vypršania uvedeného v poli **Dátum skončenia platnosti**, úloha bude odstránená z poradia – nebude odstránená úplne, iba nebude vykonaná.
- **Naplánované** – spúšťa úlohu vo vybranom čase.
- **Spúšťač protokolu udalosti** – spúšťa úlohu na základe vybranej udalosti. Spúšťač sa aktivuje, ak je určitá udalosť zaznamenaná v protokoloch. Upresnite **typ protokolu**, **logický operátor** a kritériá **filtrovania**, ktoré spustia úlohu.
- **Spúšťač pri vstupe do dynamickej skupiny** – tento spúšťač spúšťa úlohu v prípade, že klientske zariadenie vstúpi do dynamickej skupiny zvolenej v sekcii Cieľ. Táto možnosť nebude dostupná, ak bola v sekcii Cieľ zvolená statická skupina alebo individuálne klientske zariadenia.
- CRON výraz – interval spúšťača môžete nastaviť aj pomocou CRON výrazu.

Poznámka:
Viac informácií o spúšťačoch nájdete v kapitole Spúšťače.

Pokročilé nastavenia – Obmedzovanie

Obmedzovanie sa používa na obmedzenie vykonania úlohy, ak je úloha spúšťaná pri veľmi často sa vyskytujúcej

udalosti (napríklad v prípade úloh spúšťaných **Spúšťačom protokolu udalosti** alebo **Spúšťačom pri vstupe do dynamickej skupiny**). Viac informácií nájdete v kapitole Obmedzovanie.

Po nastavení cieľov a spúšťačov kliknite na **Dokončiť** pre vykonanie úlohy.

4.8 Inštalátory

Táto sekcia vám umožňuje vytvárať inštalačné balíky pre nasadenie ESET Management Agenta na klientske počítače. Inštalačné balíky sú uložené v ESMC Web Console a je možné ich kedykoľvek upravovať a v prípade potreby ich opätovne stiahnuť.

1. Kliknite na **Inštalátory** > **Vytvoriť inštalátor**.
2. Zvoľte typ inštalátora, ktorý chcete vytvoriť. Sú dostupné tieto možnosti:

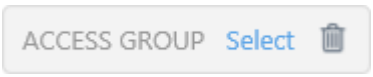
- **All-in-one inštalačný balík**
  Postupujte podľa krokov uvedených v kapitole Vytvorenie all-in-one inštalátora pre agenta, ktorá vás prevedie procesom vytvorenia a konfigurácie inštalačného balíka s pokročilými možnosťami nastavenia. Tieto možnosti zahŕňajú nastavenia **Politiky** pre ESET Management Agenta a bezpečnostné produkty ESET, **Názov hostiteľa** ESMC Servera a **Port**, ako aj možnosť zvoliť **Nadradenú skupinu**.

  Poznámka:
  Po vytvorení a stiahnutí all-in-one inštalátora máte dve možnosti, ako ESET Management Agenta nasadiť:
  - lokálne priamo na klientskom počítači,
  - použitím nástroja na nasadenie, ktorý umožňuje nasadiť ESET Management Agenty naraz na viacero klientskych počítačov.

- **Live inštalátor agenta**
  Postupujte podľa krokov uvedených v kapitole Vytvorenie Live inštalátora agenta, ktorá vás prevedie procesom vytvorenia a konfigurácie inštalátora. Tento typ nasadenia agenta je užitočný v prípade, že vám nevyhovuje vzdialené ani lokálne nasadenie. V takomto prípade môžete odoslať Live inštalátor agenta prostredníctvom e-mailu a nasadenie ponechať na používateľovi. Live inštalátor agenta môžete tiež spustiť z vymeniteľného média (napr. z USB kľúča).
- GPO alebo SCCM

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✓. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

+ Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

Inštalátory a povolenia

Používateľ môže vytvárať a upravovať inštalátory zahrnuté v skupinách, v rámci ktorých má pridelené povolenie na **zápis** pre **Uložené inštalátory**.

Poznámka:

- Pri vytváraní inštalátorov agenta bude používateľ pracovať s certifikátmi. Používateľ musí mať pridelené povolenie na **použitie Certifikátov** s prístupom k statickej skupine, kde sa nachádzajú certifikáty. Používateľ bude môcť nasadzovať ESET Management Agenta len v prípade, že mu bolo pridelené povolenie na **použitie** certifikačnej autority, ktorou je podpísaný samotný certifikát servera. Informácie o tom, ako udeliť prístupové práva k certifikátom bez možnosti prístupu k certifikačným autoritám, nájdete v tomto príklade.
- Používateľ potrebuje mať pridelené povolenie na **použitie** politík (kategória povolení **Politiky**) zvolených pri vytváraní all-in-one inštalátora, GPO inštalátora alebo SCCM skriptu v časti **Pokročilé** > **Počiatočná konfigurácia inštalátora** > **Typ konfigurácie** .
- Používateľ potrebuje mať pridelené povolenie na **použitie** licencií (kategória povolení **Licencie**), pokiaľ je v statickej skupine pridaná licencia.

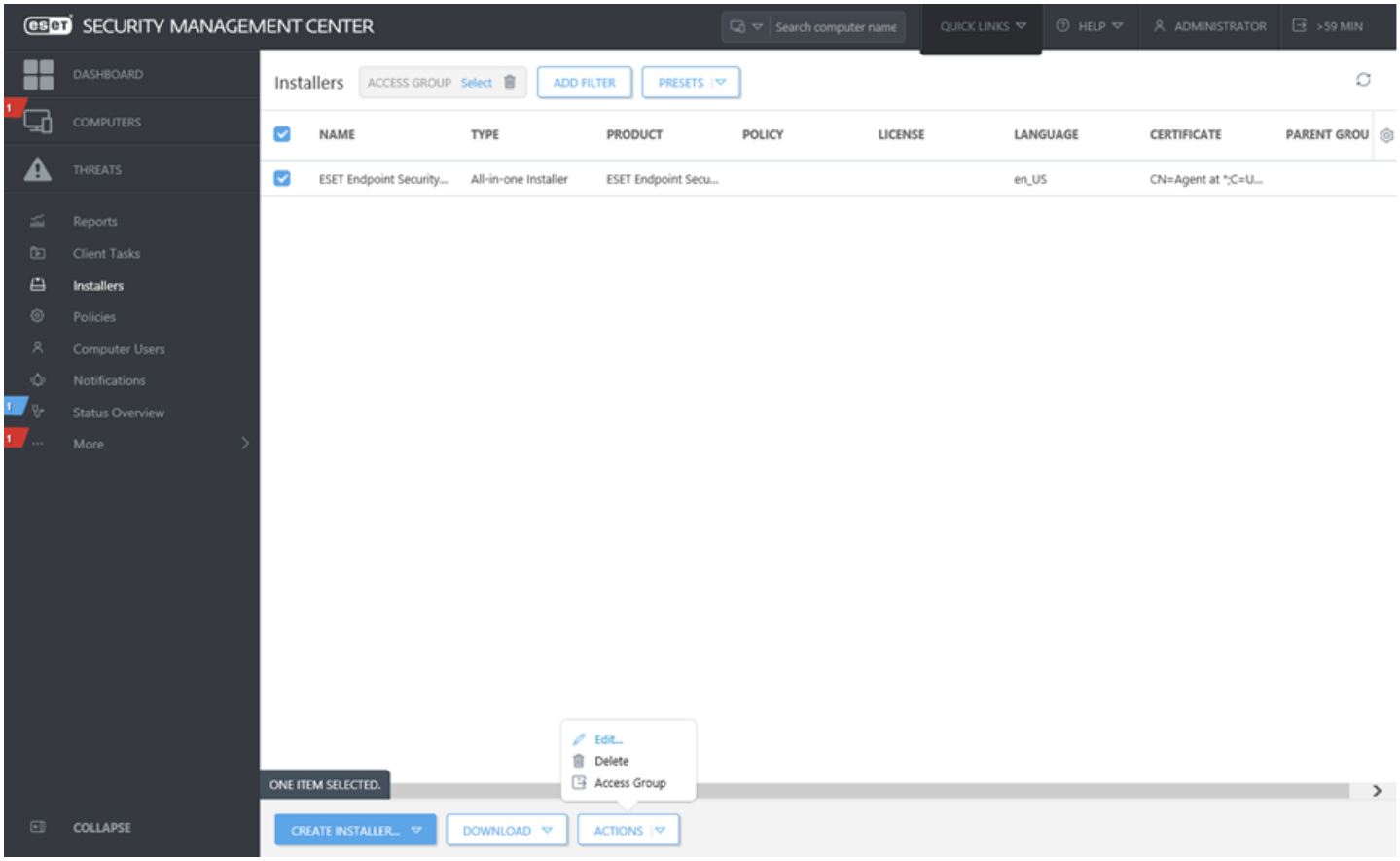
Príklad: Ako používateľovi povoliť vytváranie inštalátorov

Správca (Administrator) chce používateľovi s názvom *John* povoliť vytvárať a upravovať inštalátory v skupine *Johnova skupina*. *Správca* musí vykonať nasledujúce kroky:

1. Vytvoriť novú statickú skupinu nazvanú *Johnova skupina*.
2. Vytvoriť novú sadu povolení.
   a. nazvať ju *Povolenia pre Johna – vytváranie inštalátorov*
   b. pridať skupinu *Johnova skupina* do sekcie **Statické skupiny**
   c. v sekcii **Oprávnenia k funkciám** je potrebné zvoliť nasledujúce povolenia
      - **Zapísať** pre kategóriu **Uložené inštalátory**
      - **Použiť** pre kategóriu **Certifikáty**
      - **Zapísať** pre kategóriu **Skupiny a počítače**
   d. uložiť sadu povolení kliknutím na **Dokončiť**
3. Vytvoriť novú sadu povolení.
   a. nazvať ju *Povolenia pre Johna – certifikáty*
   b. pridať skupinu *Všetko* do sekcie **Statické skupiny**
   c. v sekcii **Oprávnenia k funkciám** je potrebné zvoliť povolenie na **Zápis** pre kategóriu **Certifikáty**
   d. uložiť sadu povolení kliknutím na **Dokončiť**

Tieto povolenia sú minimálnou požiadavkou pre umožnenie používania inštalátorov (vytváranie a úprava).

4. Vytvoriť nového používateľa.
   a. nazvať ho *John*
   b. v sekcii **Základné** zvoliť skupinu *Johnova skupina* ako domácu skupinu
   c. nastaviť pre tohto nového používateľa heslo
   d. v sekcii **Sady povolení** vybrať *Povolenia pre Johna – certifikáty* a *Povolenia pre Johna – vytváranie inštalátorov*
   e. uložiť používateľa kliknutím na **Dokončiť**



Ako stiahnuť inštalátory z ponuky inštalátorov vo Web Console

1. Kliknite na tlačidlo **Inštalátory**.
2. Označte začiarkavacie políčko vedľa inštalátora, ktorý chcete stiahnuť.
3. Kliknite na **Stiahnuť** a vyberte správnu verziu inštalačného balíka.

Ako upravovať inštalátory v ponuke inštalátorov vo Web Console

1. Kliknite na tlačidlo **Inštalátory**.
2. Označte začiarkavacie políčko vedľa inštalátora, ktorý chcete upraviť.
3. Po kliknutí na **Akcie** > **Upraviť** budete môcť robiť v inštalačnom balíku úpravy.

4.9 Politiky

Politiky predstavujú účinný nástroj na vzdialenú konfiguráciu bezpečnostných produktov spoločnosti ESET na klientskych počítačoch. Vďaka politikám sa môžete vyhnúť potrebe nastavovať bezpečnostný produkt ESET manuálne na každom počítači. Politika môže byť aplikovaná priamo na individuálne počítače, ako aj na skupiny (statické a dynamické). Môžete tiež priradiť viacero politík k počítaču alebo skupine, na rozdiel od ESET Security Management Center 5 a starších verzií, kde bolo možné priradiť politiku len k jednému produktu alebo komponentu.

Politiky a povolenia

Na vytvorenie a priraďovanie politík musí mať používateľ pridelené dostatočné povolenia. Povolenia potrebné na vykonávanie konkrétnych akcií týkajúcich sa politík:

- Na čítanie zoznamu politík a ich konfigurácie potrebuje používateľ povolenie na **čítanie**.
- Na priraďovanie politík k cieľovým zariadeniam potrebuje používateľ povolenie na **použitie**.
- Na vytváranie, zmenu a úpravu politík potrebuje používateľ povolenie na **zápis**.

Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

PRÍKLAD:

- Aby si používateľ *John* mohol prezerať politiky, ktoré sám vytvoril, potrebuje mať pridelené povolenie na **čítanie** politík (kategória povolení **Politiky**).

- Aby používateľ *John* mohol priraďovať určité politiky k počítačom, potrebuje mať pridelené povolenie na **použitie** politík (kategória povolení **Politiky**) a povolenie na **použitie** skupín a počítačov (kategória povolení **Skupiny a počítače**).
- Ak chce *správca* (Administrator) udeliť používateľovi *Johnovi* úplný prístup k politikám, musí mu prideliť povolenie na **zápis** v rámci politík (kategória povolení **Politiky**).

Aplikovanie politík

Politiky sú aplikované v poradí podľa hierarchickej štruktúry statických skupín. Toto však neplatí pre dynamické skupiny, v prípade ktorých sú najskôr prechádzané podradené skupiny. Vďaka tomuto princípu môžete vytvárať globálne politiky pre statické skupiny a politiky so špecifickým nastavením môžete priraďovať k podskupinám. Použitím príznakov môže používateľ nástroja ESMC, ktorý ma prístup do skupín nachádzajúcich sa vyššie v hierarchii, prepísať politiky nižších skupín. Algoritmus je podrobnejšie vysvetlený v časti Aplikovanie politík na klienty.

Pravidlá odstraňovania politík

Ak sa rozhodnete politiku vymazať, nastavenia klientskych počítačov budú po odstránení danej politiky závisieť od verzie nainštalovaného bezpečnostného produktu ESET na spravovaných počítačoch:

- Bezpečnostné produkty ESET verzie 6 a staršie: Nastavenia sa po odstránení politiky nevrátia na pôvodné nastavenia automaticky. Nastavenia budú zachované podľa poslednej politiky, ktorá bola priradená ku klientskemu počítaču. Rovnaké je to v prípade, ak sa klientsky počítač premiestni do dynamickej skupiny, na ktorú je aplikovaná určitá politika, ktorá upravuje nastavenia daného počítača. Tieto nastavenia budú zachované aj v prípade, že počítač opustí dynamickú skupinu. Odporúčame preto vytvoriť politiku s predvolenými nastaveniami a priradiť ju ku koreňovej skupine (**Všetko**) pre návrat k pôvodným nastaveniam. Ak v takomto prípade počítač opustí dynamickú skupinu, ktorej politika upravovala jeho nastavenia, budú nastavenia daného počítača vrátené na predvolené hodnoty.
- Bezpečnostné produkty ESET verzie 7: Nastavenia sa automaticky vrátia späť podľa poslednej politiky, ktorá bola priradená ku klientskemu počítaču. Ak dôjde k odobraniu počítača z dynamickej skupiny, kde bola aplikovaná príslušná politika, nastavenia budú z počítača odstránené.

Zlučovanie politík

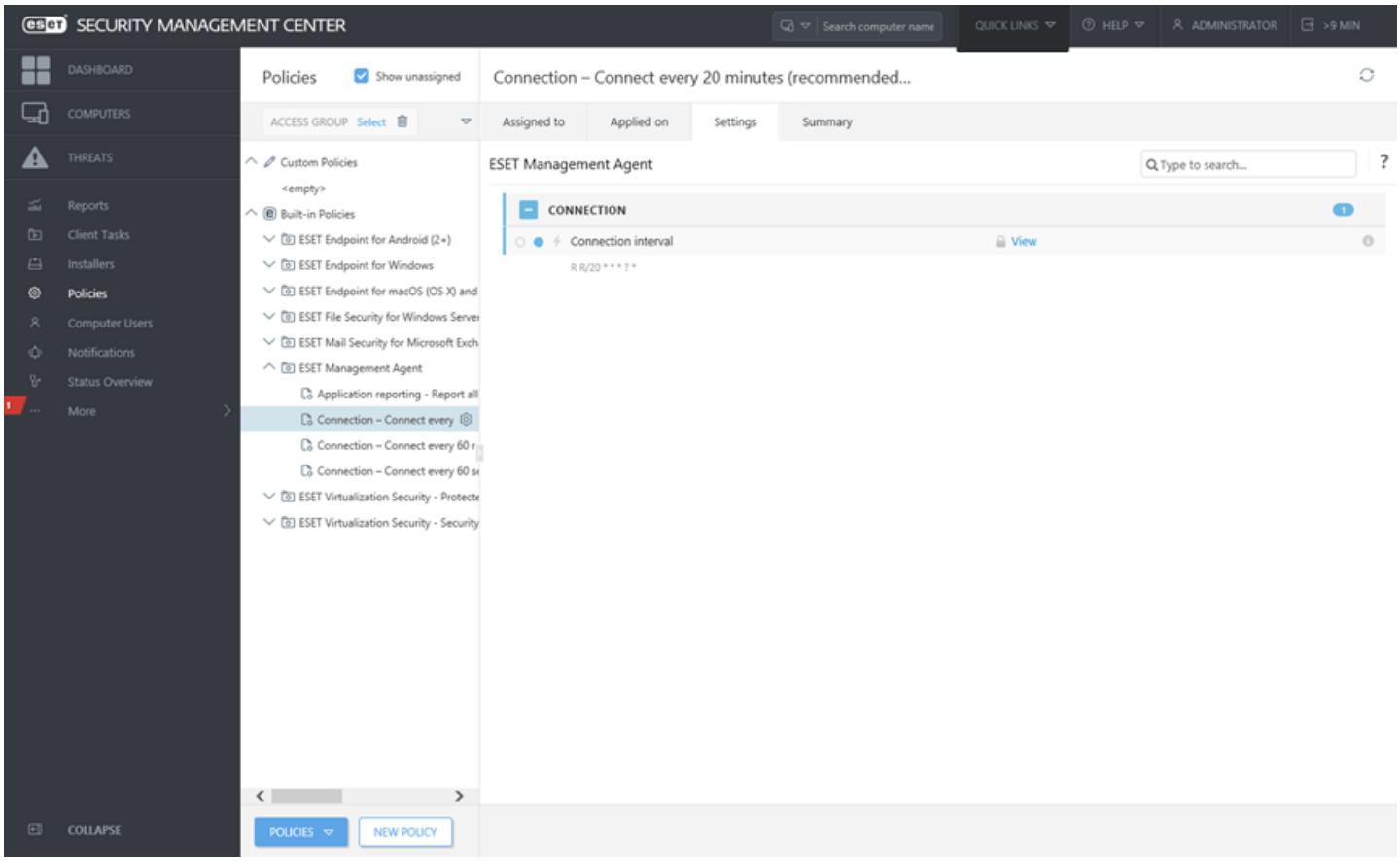
Politika aplikovaná na klienta je zvyčajne výsledkom zlúčenia viacerých politík do jednej finálnej politiky.

Poznámka:
Ku skupinám, ktoré sa nachádzajú vyššie v hierarchii, odporúčame priraďovať všeobecnejšie politiky (napr. nastavenia aktualizačného servera). Špecifickejšie politiky (napríklad nastavenia správy zariadenia) by mali byť priraďované hlbšie v stromovej štruktúre skupín. Politiky, ktoré sa nachádzajú v hierarchii nižšie, zvyčajne pri zlučovaní prepisujú nastavenia politík nachádzajúcich sa vyššie v hierarchii (ak nie je určené inak pomocou príznakov politík).

4.9.1 Sprievodca vytvorením novej politiky

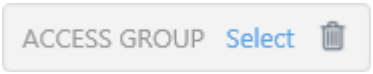
Politiky sú rozdelené do kategórií podľa bezpečnostných produktov spoločnosti ESET. Kliknite na ikonu ⌄, čím rozbalíte kategóriu a zobrazia sa dostupné politiky. Kategória Vstavané politiky obsahuje prednastavené politiky a kategória Vlastné politiky zobrazuje kategórie všetkých politík, ktoré ste vytvorili manuálne.

Pomocou politík môžete konfigurovať produkty spoločnosti ESET rovnako ako v okne rozšírených nastavení v samotnom produkte. Na rozdiel od politík v Active Directory politiky nástroja ESMC nemôžu prenášať skripty alebo príkazy. Začnite písať do vyhľadávacieho poľa pre vyhľadávanie v rámci pokročilých nastavení (napr. „HIPS“). Budú zobrazené všetky nastavenia HIPS. Ak kliknete na ikonu ⓘ v pravom hornom rohu, zobrazí sa stránka Online pomocníka týkajúca sa konkrétneho nastavenia.



Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Vytvorenie novej politiky

1. Kliknite na **Politiky** > **Nová politika**.
2. Zadajte základné informácie o politike, ako napríklad Názov a Popis (voliteľné).
3. V sekcii **Nastavenia** vyberte správny produkt.
4. Použite príznaky pre pridanie nastavení, ktoré budú politikou upravené.
5. Vyberte klientske zariadenia, pre ktoré má byť daná politika určená. Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte zariadenie, na ktoré chcete politiku aplikovať, a kliknite na **OK**.
6. Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

4.9.2 Príznaky

Proces zlučovania politík je možné ovplyvniť použitím príznakov. Príznaky určujú, ako je s nastavením v politike zaobchádzané.

Pre každé nastavenie môžete zvoliť jeden z nasledujúcich príznakov:

Neaplikovať – akékoľvek nastavenie s týmto príznakom nebude politikou aplikované. Keďže nastavenie nie je vynútené, môže byť neskôr zmenené inými politikami.

Aplikovať – nastavenie s týmto príznakom bude odoslané na klientske zariadenie. Pri zlučovaní politík však toto nastavenie môže byť prepísané neskoršou politikou. Ak je politika aplikovaná na klientsky počítač a určité nastavenie má tento príznak, dané nastavenie je zmenené bez ohľadu na to, čo bolo na klientskom počítači nakonfigurované lokálne. Keďže nastavenie nie je vynútené, môže byť neskôr zmenené inými politikami.

Vynútiť – nastavenie s týmto príznakom má vyššiu prioritu, čiže nemôže byť zmenené inou politikou (ani v prípade, že neskoršia politika má príznak „Vynútiť“). Týmto bude zaručené, že nastavenie nebude zmenené neskoršími politikami pri zlučovaní.

Pre jednoduchšiu orientáciu sú všetky pravidlá spočítané. Počet pravidiel, ktoré ste určili pre danú sekciu, sa zobrazuje automaticky. Počet sa zobrazuje aj pri názvoch kategórií v stromovej štruktúre po ľavej strane. Zobrazuje súčet pravidiel vo všetkých sekciách. Týmto spôsobom je možné rýchlo skontrolovať, koľko nastavení/pravidiel je definovaných.

V rámci zjednodušenia úpravy politiky môžete:

- Použiť , a tak nastaviť príznak „Aplikovať“ pre všetky nastavenia v aktuálne zobrazenej sekcii.
- Použiť pre odstránenie príznakov pri nastaveniach v aktuálne zobrazenej sekcii.

PRÍKLAD: AKO MÔŽE SPRÁVCA (ADMINISTRATOR) KONKRÉTNEMU POUŽÍVATEĽOVI POVOLIŤ ZOBRAZOVANIE VŠETKÝCH POLITÍK

Správca (Administrator) chce používateľovi s názvom *John* povoliť vytvárať a upravovať politiky v jeho domácej skupine a umožniť mu vidieť politiky vytvorené *správcom*. Politiky vytvorené *správcom* obsahujú príznaky **Vynútiť**. Používateľ *John* môže vidieť všetky politiky, avšak nemôže upravovať politiky vytvorené *správcom*, keďže mu boli pridelené povolenia na **čítanie** politík (kategória povolení **Politiky)** s prístupom k statickej skupine *Všetko*. Používateľ *John* môže vytvárať alebo upravovať politiky v jeho domácej skupine *San Diego*.
Správca musí vykonať nasledujúce kroky:

Vytvorenie prostredia

1. Vytvorte novú statickú skupinu nazvanú *San Diego*.
2. Vytvorte novú sadu povolení nazvanú *Politika – Všetko John* s prístupom k statickej skupine *Všetko* a s povolením na **čítanie** politík (kategória povolení **Politiky**).
3. Vytvorte novú sadu povolení nazvanú *Politika John* s prístupom k statickej skupine *San Diego*, s povolením na **zápis** v rámci kategórií **Skupiny a počítače** a **Politiky**. Táto sada povolení umožňuje *Johnovi* vytvárať a upravovať politiky v jeho domácej skupine *San Diego*.
4. Vytvorte nového používateľa nazvaného *John* a v sekcii **Sady povolení** vyberte vytvorené sady *Politika – Všetko John* a *Politika John*.

Vytvorenie politiky

5. Vytvorte novú politiku *Všetko – Zapnúť firewall*, rozbaľte sekciu **Nastavenia**, vyberte **ESET Endpoint pre Windows**, prejdite do sekcie **Personálny firewall** > **Základné** a pre všetky nastavenia nastavte príznak **Vynútiť**. Rozbaľte sekciu **Priradiť** a vyberte statickú skupinu *Všetko*.
6. Vytvorte novú politiku *Johnova skupina – Zapnúť firewall*, rozbaľte sekciu **Nastavenia**, vyberte **ESET Endpoint pre Windows**, prejdite do sekcie **Personálny firewall** > **Základné** a pre všetky nastavenia nastavte príznak **Aplikovať**. Rozbaľte sekciu **Priradiť** a vyberte statickú skupinu *San Diego*.

Výsledok

Politiky vytvorené *správcom* budú aplikované ako prvé z dôvodu použitia príznaku **Vynútiť**. Nastavenia s príznakom „Vynútiť“ majú vyššiu prioritu a nemôžu byť zmenené neskoršou politikou. Následne budú aplikované politiky vytvorené používateľom *John*.

Kliknite na **Viac** > **Skupiny** > **San Diego**, kliknite na počítač a vyberte možnosť **Zobraziť podrobnosti**. V sekcii **Konfigurácia** > **Aplikované politiky** nájdete konečné poradie uplatňovania politík.

POLICY ORDER	POLICY PRODUCT	POLICY NAME
1 (applied first)	ESET Management Agent	replicate every 10s
2	ESET Endpoint for Windows	Antivirus - Balanced

Politika vytvorená *správcom* je prvá a politika vytvorená používateľom *John* je druhá.

4.9.3 Správa politík

Politiky sú rozdelené do kategórií podľa bezpečnostných produktov spoločnosti ESET. Kliknite na ikonu , čím rozbalíte kategóriu a zobrazia sa dostupné politiky. Kategória Vstavané politiky obsahuje prednastavené politiky a kategória Vlastné politiky zobrazuje kategórie všetkých politík, ktoré ste manuálne vytvorili alebo upravili.

Pre politiky sú dostupné nasledujúce akcie:

Nová	Vytvorenie novej politiky.
Upraviť	Úprava existujúcej politiky.
Duplikovať	Vytvorenie novej politiky na základe vybranej existujúcej politiky. Pre takto vytvorenú novú politiku je potrebné zadať nový (odlišný) názov.
Priradiť	Priradenie politiky ku klientu alebo skupine.
Vymazať	Vymazanie politiky. Pozrite si tiež pravidlá odstraňovania politík.
Import	Kliknite na **Politiky** > **Import**, potom na **Vybrať súbor na odovzdanie** a vyhľadajte súbor, ktorý chcete odovzdať. Pre výber viacerých politík si pozrite **režimy výberu** uvedené nižšie. Importovať môžete len súbor .dat, ktorý obsahuje politiky exportované z ESMC Web Console. Nemôžete importovať súbor .xml, ktorý obsahuje politiky exportované z bezpečnostného produktu ESET.
Exportovať	Zo zoznamu vyberte politiku, ktorú chcete exportovať, a kliknite na **Politiky** > **Exportovať**. Politika bude exportovaná v podobe súboru *.dat*. Pre exportovanie viacerých politík zmeňte režim výberu (pozrite si dostupné **režimy výberu** nižšie).
Prístupová skupina	Presunutie politiky do inej skupiny.

Pre zmenu režimu výberu z jednej na viac položiek použite možnosť **Režimy**. Kliknite na šípku v pravom hornom rohu a vyberte si z kontextového menu:

- **Režim jedného výberu** – umožňuje označiť jednu položku zo zoznamu.
- **Režim viacerých výberov** – umožňuje pomocou začiarkavacích políčok označiť viac položiek.
- **Obnoviť** – umožňuje obnoviť/opätovné načítať zobrazené informácie.
- **Zobraz všetky položky** – umožňuje zobraziť všetky informácie.
- **Zobraz len hlavné sekcie** – umožňuje skryť všetky informácie.

4.9.4 Priraďovanie politík ku klientom

Skupiny a Počítače môžu mať priradené viaceré politiky. Počítač môže byť v hlboko vnorenej skupine, ktorej nadradené skupiny majú vlastné politiky.

Najdôležitejšie pri priraďovaní politík je ich správne poradie. Je odvodené od poradia skupín a poradia politík priradených ku skupine.

Pomocou nasledujúcich krokov zistíte aktívnu politiku pre každého klienta:

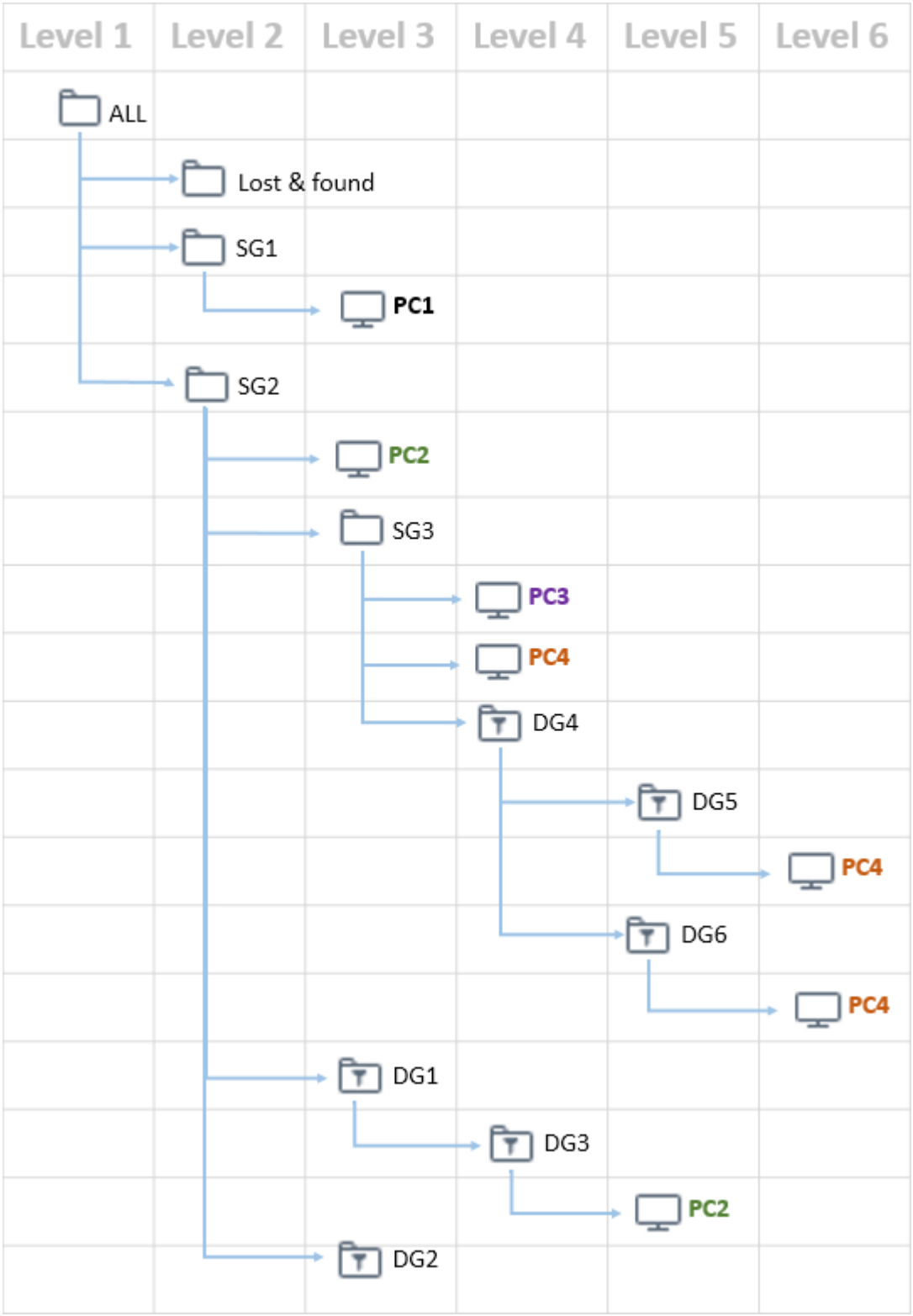
1. Zistenie poradia skupín, v ktorých sa počítač nachádza
2. Nahradenie skupín s ich priradenými politikami
3. Zlúčenie politík pre konečné nastavenia

4.9.4.1 Poradie skupín

Politiky môžu byť priradené ku skupinám a aplikované v určitom poradí. Pravidlá popísané nižšie určujú poradie, v akom budú politiky aplikované na klienty.

1. **Pravidlo 1**: Statické skupiny sú prechádzané od svojho koreňa, čiže od statickej skupiny **Všetko**.
2. **Pravidlo 2**: Na každej úrovni sú najprv prechádzané statické skupiny danej úrovne v poradí, v akom sú zobrazené v stromovej štruktúre. Toto prechádzanie sa nazýva aj prehľadávanie do šírky (Breadth-first search).
3. **Pravidlo 3**: Po prejdení všetkých statických skupín danej úrovne, začnú byť prechádzané aj dynamické skupiny.
4. **Pravidlo 4**: V dynamickej skupine je každá podskupina prechádzaná v poradí, v akom sa nachádza v zozname.
5. **Pravidlo 5**: Ak sa na akejkoľvek úrovni dynamickej skupiny nachádza podskupina, ktorá obsahuje ďalšie podskupiny, budú prechádzané aj tie. Až keď sa už v rámci danej dynamickej skupiny nevyskytujú žiadne ďalšie podskupiny, budú prechádzané ostatné dynamické skupiny. Toto prechádzanie sa nazýva aj prehľadávanie do hĺbky (Depth-first search).
6. **Pravidlo 6**: Prechádzanie skončí pri klientskom počítači.

Dôležité:
Politika je aplikovaná na počítač. To znamená, že prechádzanie stromovej štruktúry skupín sa skončí pri klientskom počítači, na ktorom má byť politika aplikovaná.



Poradie, v akom budú politiky aplikované na jednotlivých počítačoch z príkladu, bude na základe vyššie uvedených pravidiel nasledujúce (All = koreňová skupina Všetko; SG = statická skupina; DG = dynamická skupina):

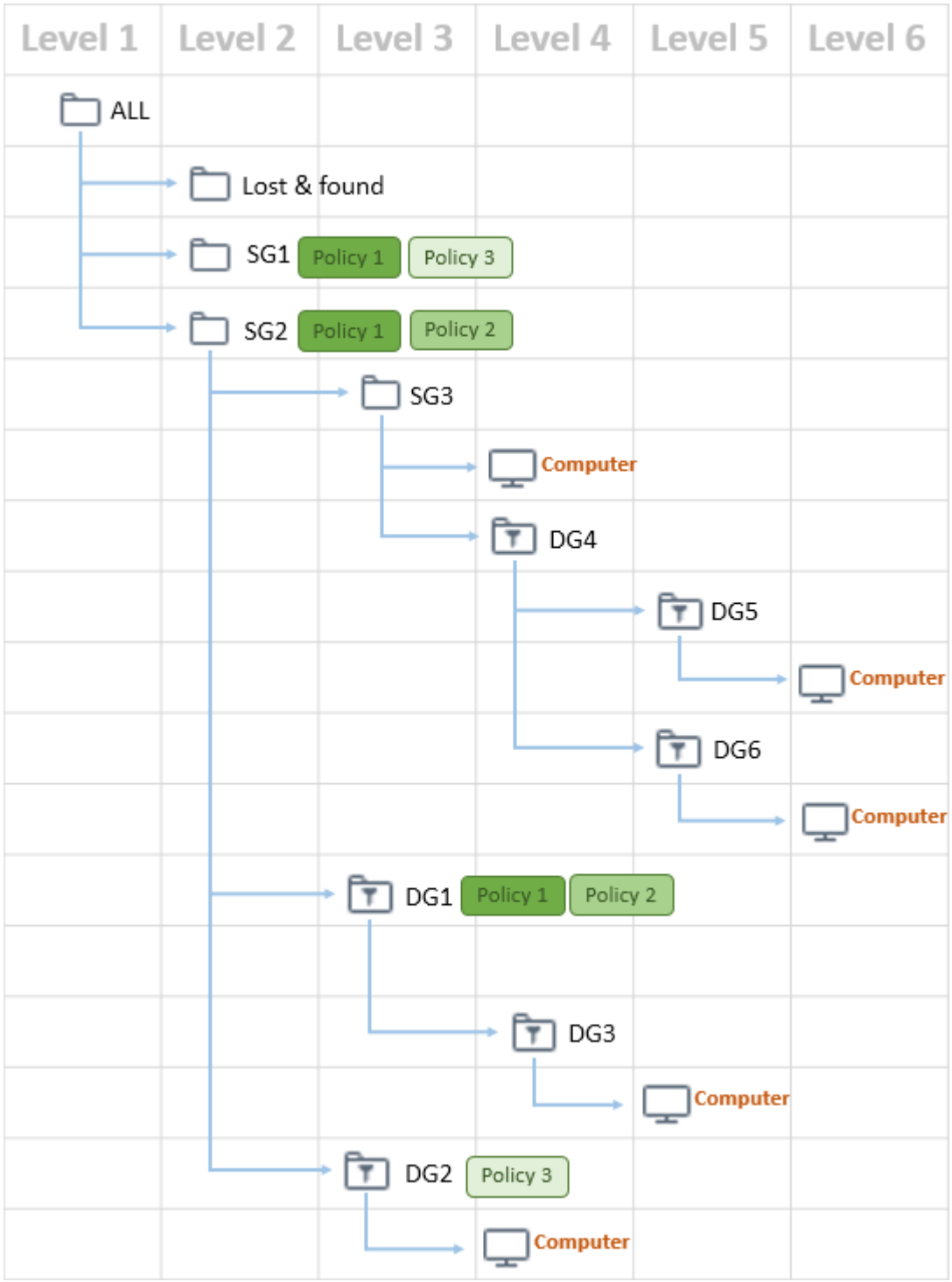
PC1:	**PC2:**	**PC3:**	**PC4:**
1. ALL 2. SG1 3. PC1	1. ALL 2. SG2 3. DG1 4. DG3 5. PC2	1. ALL 2. SG2 3. SG3 4. PC3	1. ALL 2. SG2 3. SG3 4. DG4 5. DG5 6. DG6 7. PC4

4.9.4.2 Získanie zoznamu politík

Keď je už poradie skupín známe, nasleduje nahradenie skupín politikami, ktoré sú k nim priradené. Politiky sú zobrazené v rovnakom poradí, v akom boli priradené ku skupine. Je možné upravovať prioritu politík pre skupinu, kde je viacero politík. Každá politika nastavuje len jeden produkt (ESET Management Agent, EES atď.).

Poznámka:
Skupina bez priradenej politiky je odstránená zo zoznamu.

K statickým a dynamickým skupinám sú pridelené 3 politiky (pozri obrázok):



Poradie, v akom budú politiky aplikované na klientsky počítač. V nasledujúcom zozname sú uvedené skupiny a k nim priradené politiky:

1. Statická skupina Všetko (All) -> odstránená – bez priradenej politiky
2. Statická skupina 2 (SG2) -> Politika 1, Politika 2
3. Statická skupina 3 (SG3) -> odstránená – bez priradenej politiky
4. Dynamická skupina 1 (DG1) -> Politika 1, Politika 2
5. Dynamická skupina 3 (DG3) -> odstránená – bez priradenej politiky
6. Dynamická skupina 2 (DG2) -> Politika 3
7. Dynamická skupina 4 (DG4) -> odstránená – bez priradenej politiky
8. Dynamická skupina 5 (DG5) -> odstránená – bez priradenej politiky
9. Dynamická skupina 6 (DG6) -> odstránená – bez priradenej politiky
10. Počítač -> odstránená – bez priradenej politiky

Konečný zoznam politík bude:

1. Politika 1
2. Politika 2
3. Politika 1
4. Politika 2
5. Politika 3

4.9.4.3 Zlučovanie politík

Politiky sú zlučované po jednom. Pri zlučovaní politík je hlavným pravidlom, že nastavenia definované v neskoršej politike vždy nahrádzajú príslušné nastavenia definované predchádzajúcou politikou. Na zmenu tohto správania môžete použiť príznaky politík (dostupné pre každé nastavenie). Pri niektorých nastaveniach je možné použiť ďalšie pravidlo (nahradiť/pripojiť na koniec/pripojiť na začiatok).

Berte, prosím, na vedomie, že štruktúra skupín (ich hierarchia) a postupnosť politík určuje, ako budú politiky zlúčené. Zlúčenie ľubovoľných dvoch politík môže mať rozdielny výsledok v závislosti od ich poradia.

Pri vytváraní politík si môžete všimnúť, že pri niektorých nastaveniach je možné konfigurovať dodatočné pravidlá. Tieto pravidlá vám umožňujú usporiadať rovnaké nastavenia definované viacerými politikami.

- **Nahradiť**: Predvolené pravidlo používané pri zlučovaní politík. Nastavenia definované v neskoršej politike nahrádzajú príslušné nastavenia definované predchádzajúcou politikou.
- **Pripojiť na koniec**: Pri aplikovaní rovnakého nastavenia viac ako jednou politikou môžete prostredníctvom tohto pravidla nastavenie pripojiť na koniec poradia. Nastavenie bude umiestnené na koniec zoznamu, ktorý bol vytvorený pri zlučovaní politík.
- **Pripojiť na začiatok**: Pri aplikovaní rovnakého nastavenia viac ako jednou politikou môžete prostredníctvom tohto pravidla nastavenie pripojiť na začiatok poradia. Nastavenie bude umiestnené na začiatok zoznamu, ktorý bol vytvorený pri zlučovaní politík.

Zlučovanie lokálnych a vzdialených zoznamov

Novšie bezpečnostné produkty ESET (zoznam podporovaných verzií nájdete nižšie) podporujú zlučovanie lokálnych nastavení so vzdialenými politikami novým spôsobom. Ak je nastavenie zoznamom (napr. zoznam webových stránok) a existuje konflikt medzi vzdialenou politikou a lokálnym nastavením, vzdialená politika dané nastavenie prepíše. Môžete si vybrať, ako kombinovať lokálne a vzdialené zoznamy. Rôzne pravidlá zlučovania môžete nastaviť pre:

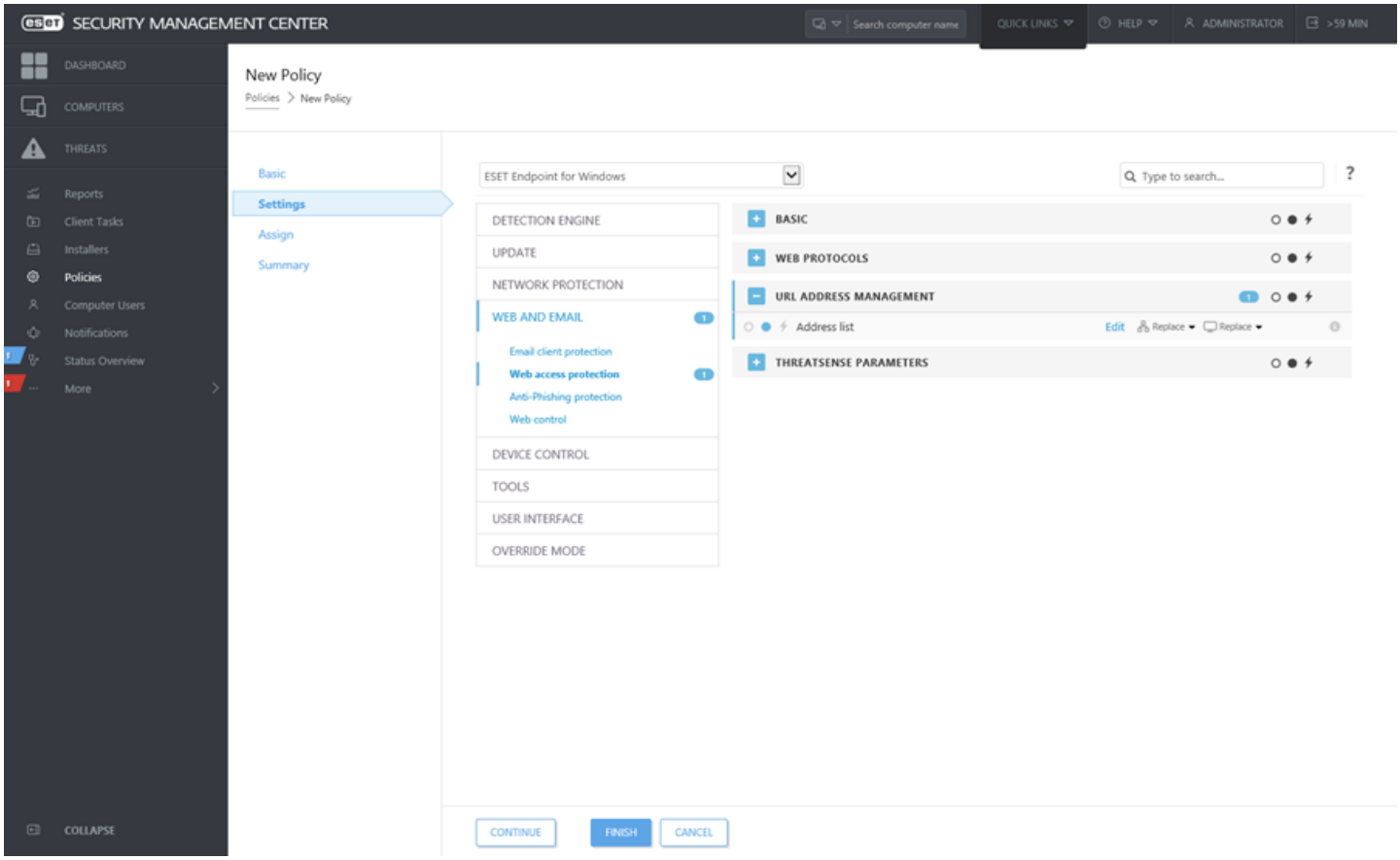
- Zlučovanie nastavení pre vzdialené politiky.
- Zlučovanie vzdialených a lokálnych politík – lokálne nastavenia s výslednou vzdialenou politikou.

Možnosti akcií sú rovnaké ako tie, ktoré sú spomenuté vyššie: **Nahradiť**, **Pripojiť na koniec**, **Pripojiť na začiatok**.

Zoznam produktov podporujúcich lokálne a vzdialené zoznamy:

Bezpečnostný produkt ESET	Verzia

ESET Endpoint pre Windows	7+
ESET Mail Security pre Microsoft Exchange	6+
ESET File Security pre Windows Server	6+
ESET Mail Security pre IBM Domino	6+
ESET Security pre Kerio	6+
ESET Security pre Microsoft SharePoint Server	6+



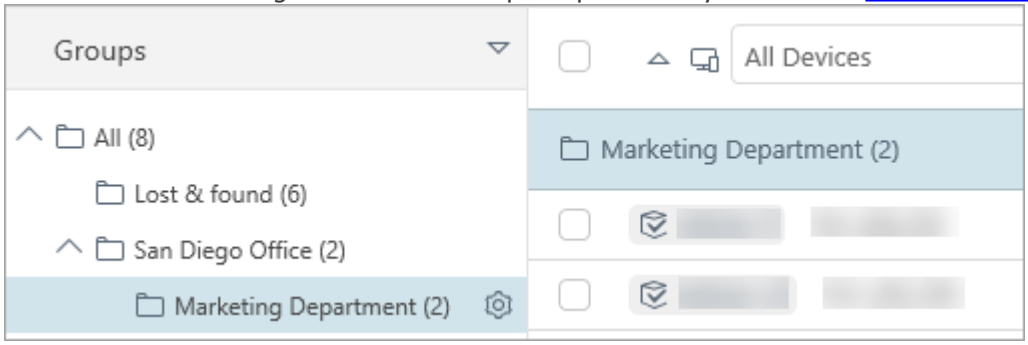
4.9.4.3.1 Príklad zlučovania politík

V tomto príklade nájdete:

- Inštrukcie, ako pomocou politiky upraviť nastavenia bezpečnostných produktov ESET určených pre koncové zariadenia.
- Postup zlučovania politík s použitím príznakov a pravidiel.

V prípade, že *správca* (Administrator) chce:

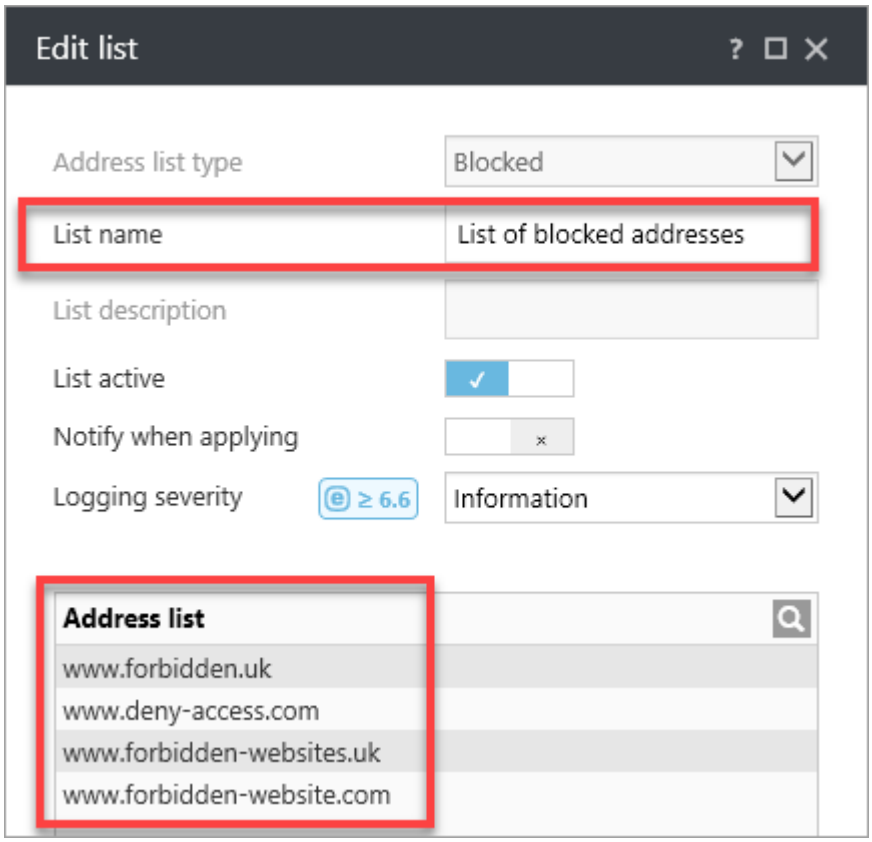
- Zakázať *Pobočke San Diego* prístup k webovým stránkam www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk a www.forbidden-website.com.
- Povoliť *Marketingovému oddeleniu* prístup k webovým stránkam www.forbidden.uk, www.deny-access.com.



Správca musí vykonať nasledujúce kroky:

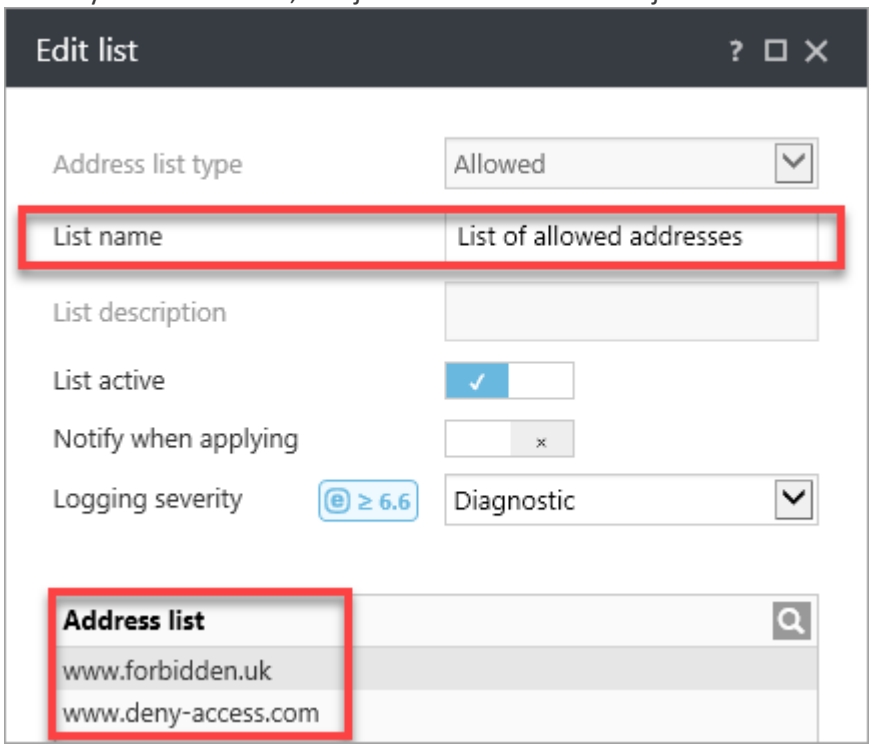
1. Vytvoriť novú statickú skupinu *Pobočka San Diego* a následne v tejto statickej skupine vytvoriť podskupinu *Marketingové oddelenie*.
2. Prejsť do sekcie **Politiky** a vytvoriť novú politiku podľa nasledujúceho postupu:
   i. Politiku nazvať *Pobočka San Diego*.
   ii. Rozbaliť sekciu **Nastavenia** a vybrať možnosť **ESET Endpoint pre Windows**.
   iii. Prejsť do sekcie **Web a mail** > **Ochrana prístupu na web** > **Manažment URL adries**.
   iv. Kliknúť na tlačidlo pre použitie príznaku **Aplikovať** a kliknúť na **Upraviť** pre úpravu **Zoznamu adries**.
   v. Kliknúť na **Zoznam blokovaných adries** a následne na **Upraviť**.
   vi. Pridať nasledujúce webové adresy: www.forbidden.uk, www.deny-access.com, www.forbidden-websites.uk a www.forbidden-website.com. Následne je potrebné uložiť zoznam blokovaných adries, ako aj zoznam adries.
   vii. Rozbaliť sekciu **Priradiť** a politiku priradiť ku skupine *Pobočka San Diego* a jej podskupine *Marketingové oddelenie*.
   viii. Politiku uložiť kliknutím na **Dokončiť**.

Politika bude aplikovaná na *Pobočku San Diego* a na *Marketingové oddelenie* a na základe tejto politiky budú blokované webové stránky tak, ako je zobrazené na nasledujúcom obrázku.

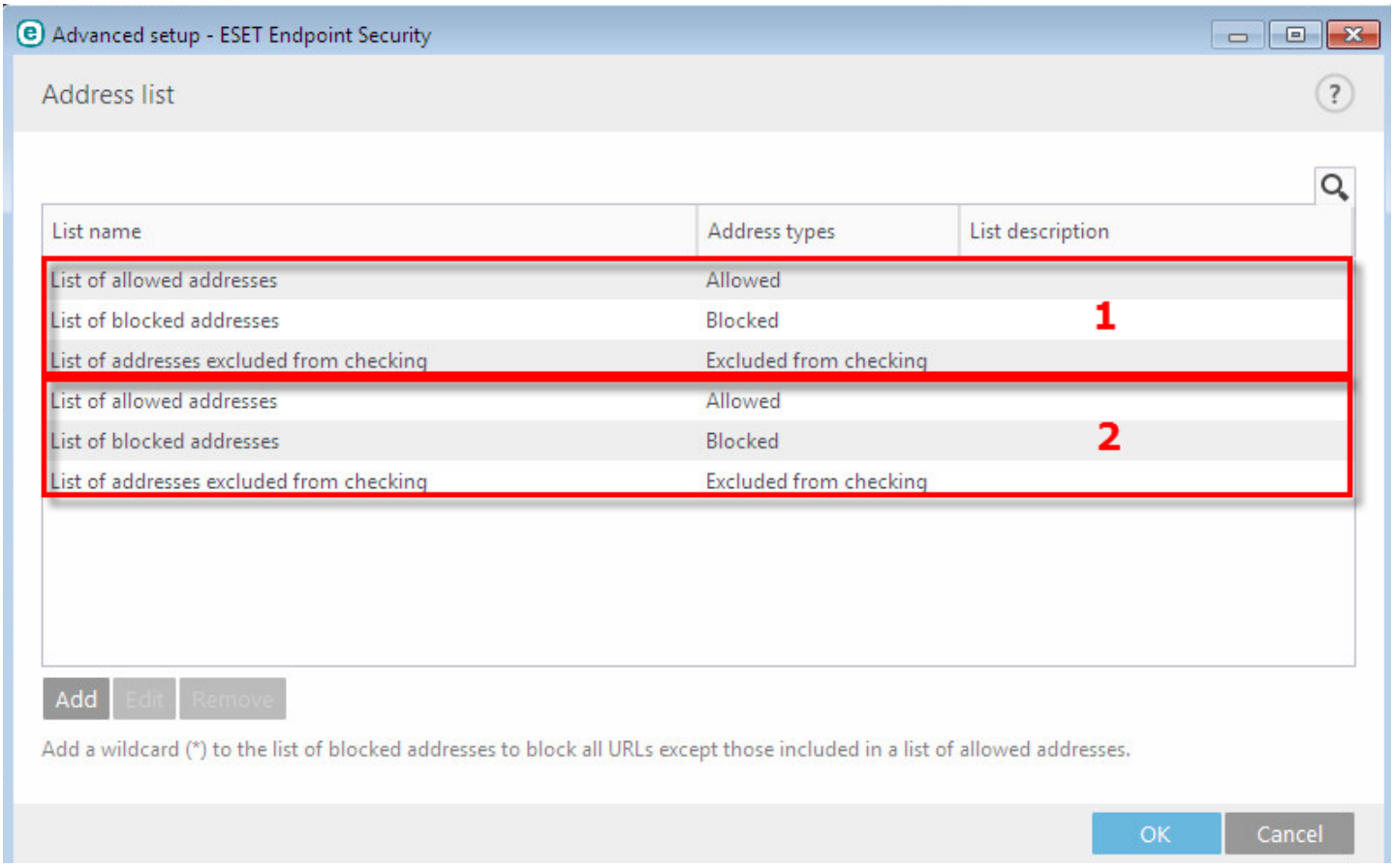


3. Prejsť do sekcie **Politiky** a vytvoriť novú politiku:
   i. Politiku nazvať *Marketingové oddelenie*.
   ii. Rozbaliť sekciu **Nastavenia** a vybrať možnosť **ESET Endpoint pre Windows**.
   iii. Prejsť do sekcie **Web a mail** > **Ochrana prístupu na web** > **Manažment URL adries**.
   iv. Kliknúť na tlačidlo pre použitie príznaku **Aplikovať**, vybrať pravidlo pripojenia a následne kliknúť na **Upraviť** pre úpravu **Zoznamu adries**. Pri zlučovaní politík pravidlo Pripojiť na koniec presunie toto nastavenie Zoznamu adries na koniec poradia.
   v. Kliknúť na **Zoznam blokovaných adries** > **Upraviť**.
   vi. Pridať nasledujúce webové adresy: www.forbidden.uk , www.deny-access.com. Následne je potrebné uložiť zoznam blokovaných adries, ako aj zoznam adries.
   vii. Rozbaliť sekciu **Priradiť** a politiku priradiť ku skupine *Marketingové oddelenie*.
   viii. Politiku uložiť kliknutím na **Dokončiť**.

Politika bude aplikovaná na *Marketingové oddelenie* a na základe tejto politiky bude povolený prístup k webovým stránkam tak, ako je zobrazené na nasledujúcom obrázku.



4. Konečná konfigurácia bude výsledkom zlúčenia oboch politík aplikovaných na skupiny *Pobočka San Diego* a *Marketingové oddelenie* . Otvorte **bezpečnostný produkt ESET určený pre koncové zariadenia**, prejdite do sekcie **Nastavenia** > **Web a mail** > **Rozšírené nastavenia**, kliknite na kartu **Web a mail** > **Ochrana prístupu na web** a rozbaľte sekciu **Manažment URL adries**. Zobrazí sa konečná konfigurácia produktu ESET určeného pre koncové zariadenia.



Konečná konfigurácia zahŕňa:

1. zoznam adries definovaný politikou *Pobočka San Diego*,
2. zoznam adries definovaný politikou *Marketingové oddelenie*.

4.9.5 Konfigurácia produktu z ESMC

Pomocou politík môžete konfigurovať produkty spoločnosti ESET rovnako ako v okne rozšírených nastavení v samotnom produkte. Na rozdiel od politík v Active Directory politiky nástroja ESMC nemôžu prenášať skripty alebo príkazy.

Pre bezpečnostné produkty ESET verzie 6 alebo novšej je možné nastaviť, aby boli určité stavy odosielané a hlásené na kliente alebo vo Web Console. Toto je možné nastaviť v rámci politiky pre produkt verzie 6 v sekcii **Používateľské rozhranie** > **Prvky používateľského rozhrania** > **Stavy**:

- **Zobraziť** – stav bude hlásený v grafickom používateľskom rozhraní na strane klienta.
- **Odoslať** – stav bude hlásený v ESMC.

Príklady použitia politík na konfiguráciu produktov ESET:

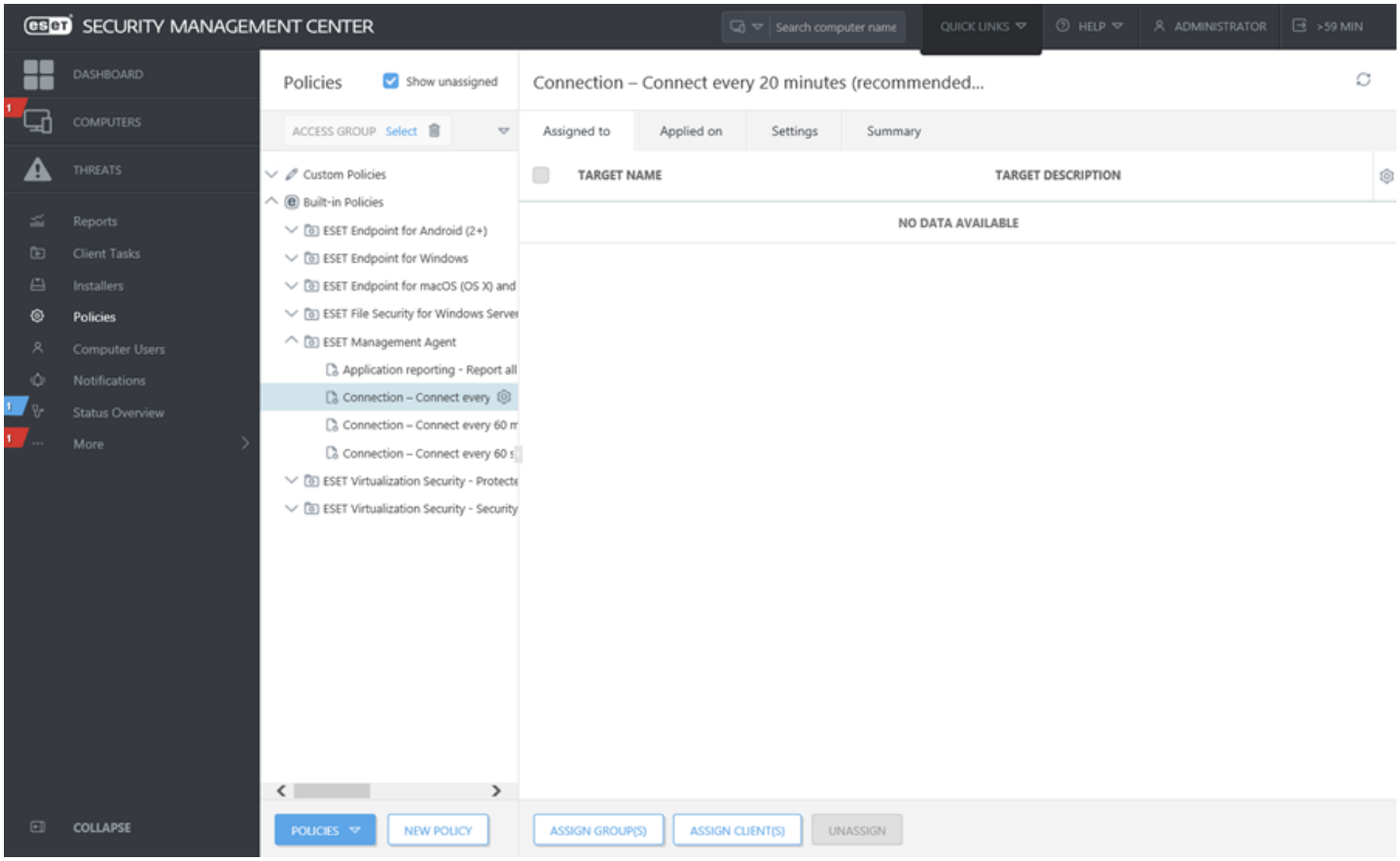
- Politika upravujúca nastavenia ESET Management Agenta
- Politika upravujúca nastavenia nástroja ESET RD Sensor
- Vytvorenie politiky pre iOS MDM – Exchange ActiveSync účet
- Vytvorenie politiky pre MDC na aktiváciu APNS a registráciu zariadení iOS

4.9.6 Priradenie politiky ku skupine

Po vytvorení politiky ju môžete priradiť k **statickej** alebo **dynamickej** skupine. Existujú dva spôsoby priraďovania politík:

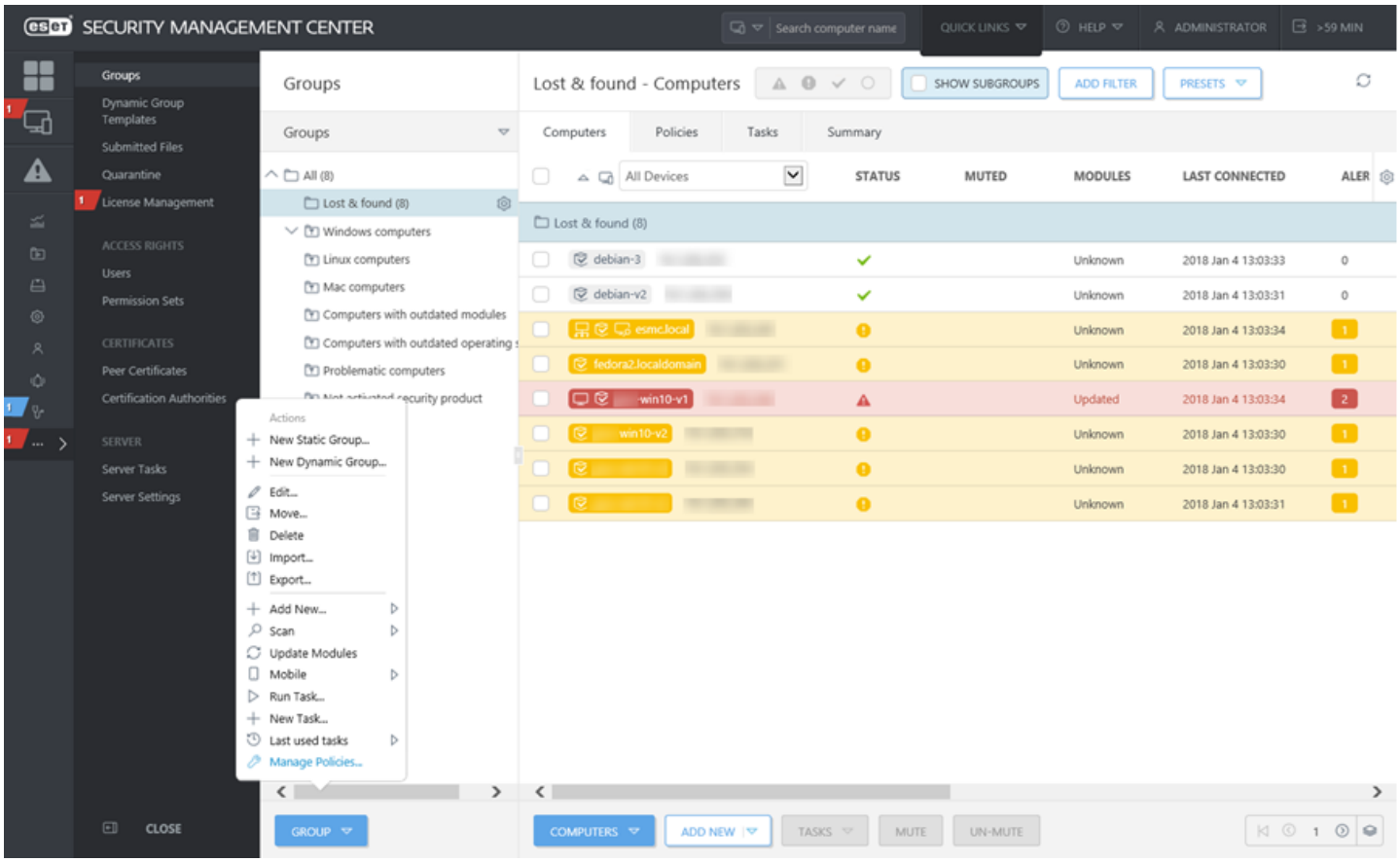
Metóda č. 1

V sekcii **Politiky** označte politiku a kliknite na **Priradiť skupinu(y)**. Vyberte statickú alebo dynamickú skupinu zo zoznamu (môžete vybrať viacero skupín) a kliknite na **OK**.



Metóda č. 2

1. Kliknite na **Viac** > **Skupiny** > **Skupina** alebo kliknite na ikonu vedľa názvu skupiny a vyberte možnosť **Spravovať politiky**.



2. V okne **Poradie uplatňovania politík** kliknite na **Pridať politiku**.
3. Označte politiku, ktorú chcete priradiť k tejto skupine a kliknite na **OK**.
4. Následne kliknite na **Zatvoriť**.

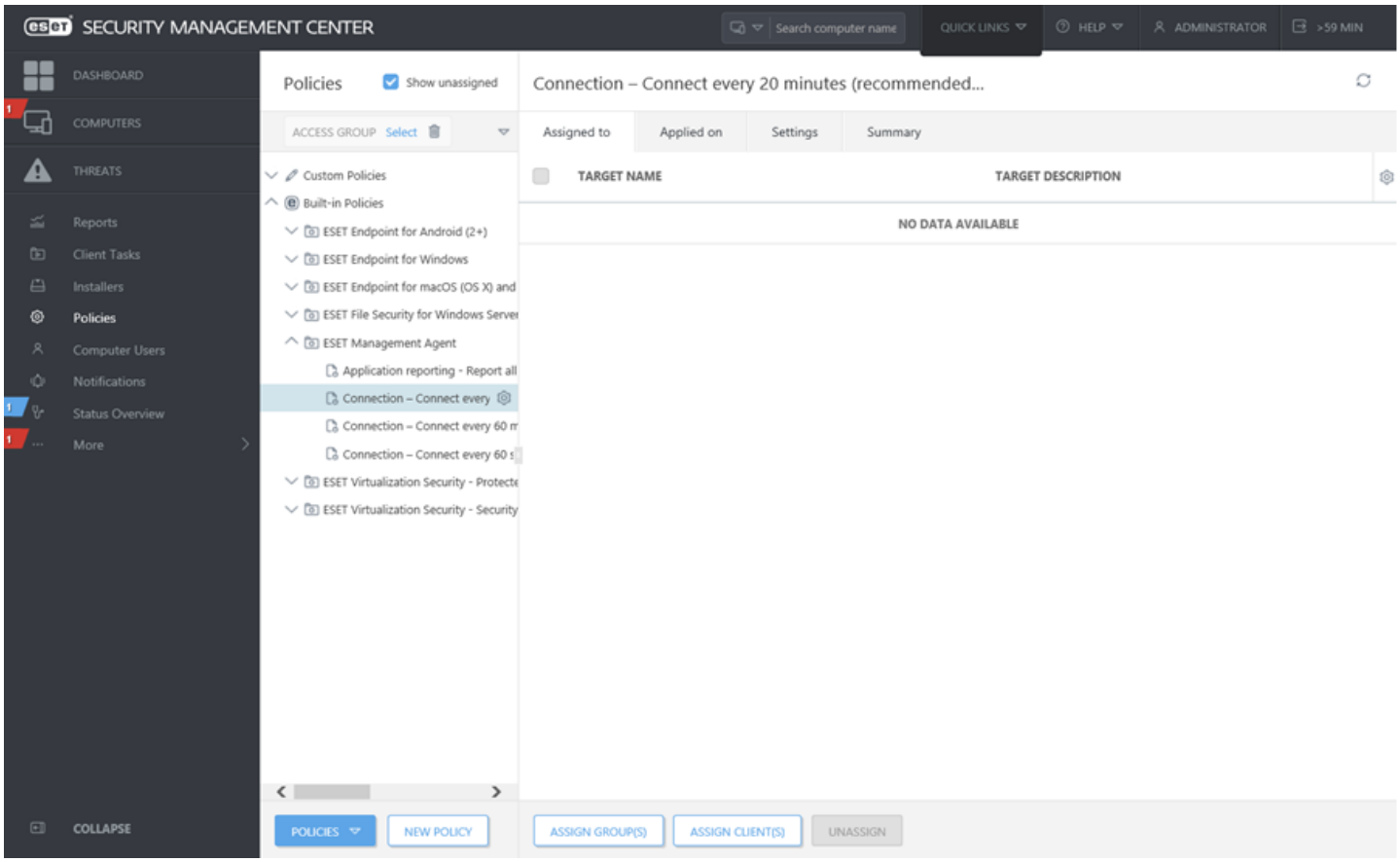
Ak chcete zobraziť, ktoré politiky sú priradené ku konkrétnej skupine, označte danú skupinu a kliknite na kartu **Politiky**.

Ak chcete zobraziť, ktoré skupiny sú priradené ku konkrétnej politike, označte danú politiku a kliknite na kartu **Aplikované na**.

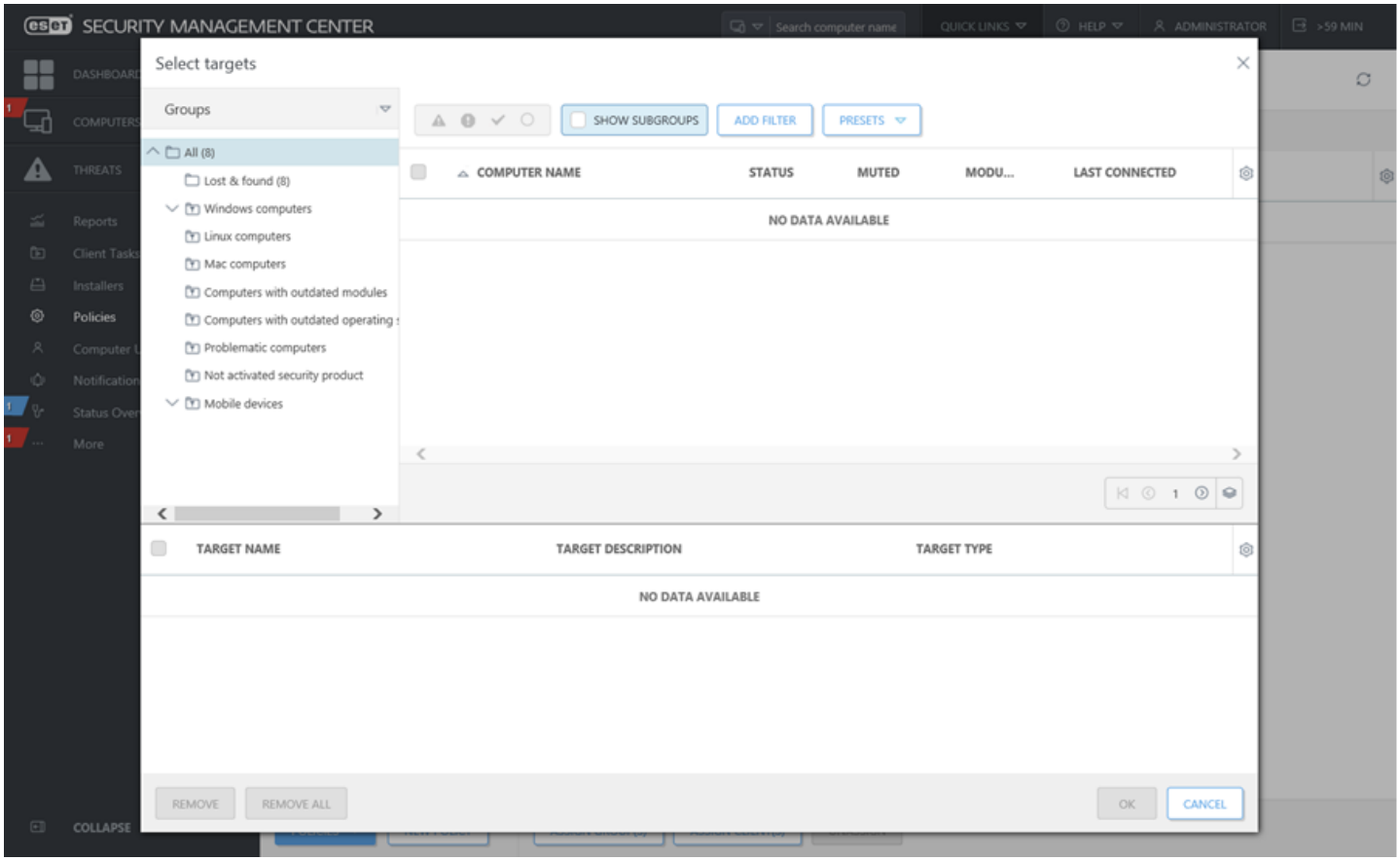
Poznámka:
Viac informácií o politikách nájdete v kapitole Politiky.

4.9.7 Priradenie politiky ku klientu

Ak chcete priradiť politiku ku klientskemu počítaču, kliknite na **Politiky**, vyberte politiku a kliknite na možnosť **Priradiť klienta(y)**.



Vyberte cieľové počítače a kliknite na **OK**. Politika bude použitá pre všetky počítače, ktoré ste vybrali.



Ak chcete zobraziť, ktoré klienty sú priradené ku konkrétnej politike, označte danú politiku a kliknite na kartu **Aplikované na**.

4.9.8 Politika upravujúca nastavenia nástroja ESET RD Sensor

Použitím politiky môžete meniť nastavenia a fungovanie nástroja ESET RD Sensor . Ide predovšetkým o úpravu nastavení, ako je napr. filtrovanie adries. Prostredníctvom politiky tak môžete napríklad zahrnúť určité adresy do zoznamu blokovaných adries, aby počítače s danými adresami neboli nástrojom RD Sensor vôbec zachytávané.

Prejdite do sekcie **Politiky** a rozbaľte kategóriu **Vlastné politiky**, kde môžete upravovať existujúce alebo vytvárať nové politiky.

Filtre

IPv4 Filter

Zapnúť filtrovanie IPv4 adries – po zapnutí filtrovania budú nástrojom RD Sensor zachytávané iba počítače, ktorých IP adresy sú v zozname povolených adries vo filtračnom zozname IPv4, alebo iba tie, ktoré nie sú v zozname blokovaných adries.

Filtre – špecifikujte, či má ísť o Zoznam povolených adries alebo o Zoznam blokovaných adries**.**

Zoznam IPv4 adries – pre pridanie alebo odstránenie adries zo zoznamu kliknite na možnosť **Upraviť zoznam IPv4**.

Filter prefixov MAC adries

Zapnúť filtrovanie prefixov MAC adries – po zapnutí filtrovania budú zachytávané iba počítače, ktorých MAC adresa obsahuje prefix (xx:xx:xx) zahrnutý v zozname povolených prefixov MAC adries, alebo iba tie počítače, ktorých prefix MAC adresy nie je v zozname blokovaných adries.

Režim filtrovania – špecifikujte, či má ísť o Zoznam povolených adries alebo o Zoznam blokovaných adries**.**

Zoznam prefixov MAC adries – pre pridanie alebo odstránenie prefixu zo zoznamu kliknite na možnosť **Upraviť zoznam prefixov MAC adries**.

Detekcia

Aktívna detekcia – Po zapnutí tejto možnosti bude ESET RD Sensor aktívne vyhľadávať počítače na lokálnej sieti. Detekcia tak bude efektívnejšia, avšak na niektorých počítačoch môže zapnutie tejto funkcie viesť k zobrazovaniu varovaní firewallu.

Porty detekcie OS – RD Sensor používa na vyhľadávanie počítačov na lokálnej sieti prednastavený zoznam portov. Zoznam portov je možné upravovať.

Pokročilé nastavenia

Diagnostika – môžete zapnúť alebo vypnúť odosielanie anonymných správ so štatistickými informáciami o zlyhaní programu do spoločnosti ESET. Povolením tejto možnosti nám pomáhate zlepšovať naše produkty.

Priradiť

Vyberte klientske zariadenia, pre ktoré má byť daná politika určená. Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte zariadenie, na ktoré chcete politiku aplikovať, a kliknite na **OK**.

Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

4.9.9 Politika upravujúca nastavenia ERA 6.x Proxy

Dôležité:
Nové ESET Management Agenty verzie 7 nie sú spätne kompatibilné s ERA (nedokážu sa pripojiť k serveru), pretože používajú nový replikačný protokol. Agenty verzie 6.x sa môžu pripojiť k serveru verzie 7 prostredníctvom ERA Proxy. Ak chcete vykonať migráciu, postupujte podľa príslušného návodu.

Použitím politiky môžete meniť nastavenia počítačov využívajúcich komponent ERA Proxy. Ide predovšetkým o úpravu nastavení, akými sú interval pripojenia a server, na ktorý sa proxy pripája. Prejdite do sekcie **Politiky** a rozbaľte kategóriu **Vlastné politiky**, kde môžete upravovať existujúce alebo vytvárať nové politiky.

Pripojenie

Remote Administrator port – tento port je používaný na spojenie ESET Security Management Center Servera s proxy. Aby sa zmena tohto nastavenia prejavila, vyžaduje sa reštart služby ERA Server.

Servery pre pripojenie – kliknite na **Upraviť zoznam serverov** pre upresnenie podrobností pripojenia k ERA Serveru (názov hostiteľa/IP a číslo portu). Je možné zadať viacero ERA Serverov. Politiku s týmto nastavením môžete využiť napríklad pri zmene IP adresy svojho ERA/ESMC Servera alebo v prípade, že vykonávate migráciu.

Dátový limit – zadajte maximálny počet bajtov pre odosielanie dát.

Interval pripojenia – zvoľte **Pravidelný interval** a upresnite časovú hodnotu intervalu pripojenia na server (prípadne použite CRON výraz).

Certifikát – môžete spravovať partnerské certifikáty pre ERA Proxy. Kliknite na **Zmeniť certifikát** a vyberte, ktorý ERA Proxy certifikát by mal byť používaný ERA Proxy serverom. Viac informácií nájdete v kapitole Partnerské certifikáty.

Pokročilé nastavenia

Diagnostika – môžete zapnúť alebo vypnúť odosielanie anonymných správ so štatistickými informáciami o zlyhaní programu do spoločnosti ESET. Povolením tejto možnosti nám pomáhate zlepšovať naše produkty.

Zapisovanie do protokolov – môžete nastaviť úroveň podrobnosti protokolov, čím určíte úroveň informácií, ktoré budú zhromažďované a zapisované do protokolov – od úrovne **Sledovanie** (informačné) až po **Závažné** (najdôležitejšie, kritické informácie).

Priradiť

Vyberte klientske zariadenia, pre ktoré má byť daná politika určená. Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte zariadenie, na ktoré chcete politiku aplikovať, a kliknite na **OK**.

Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

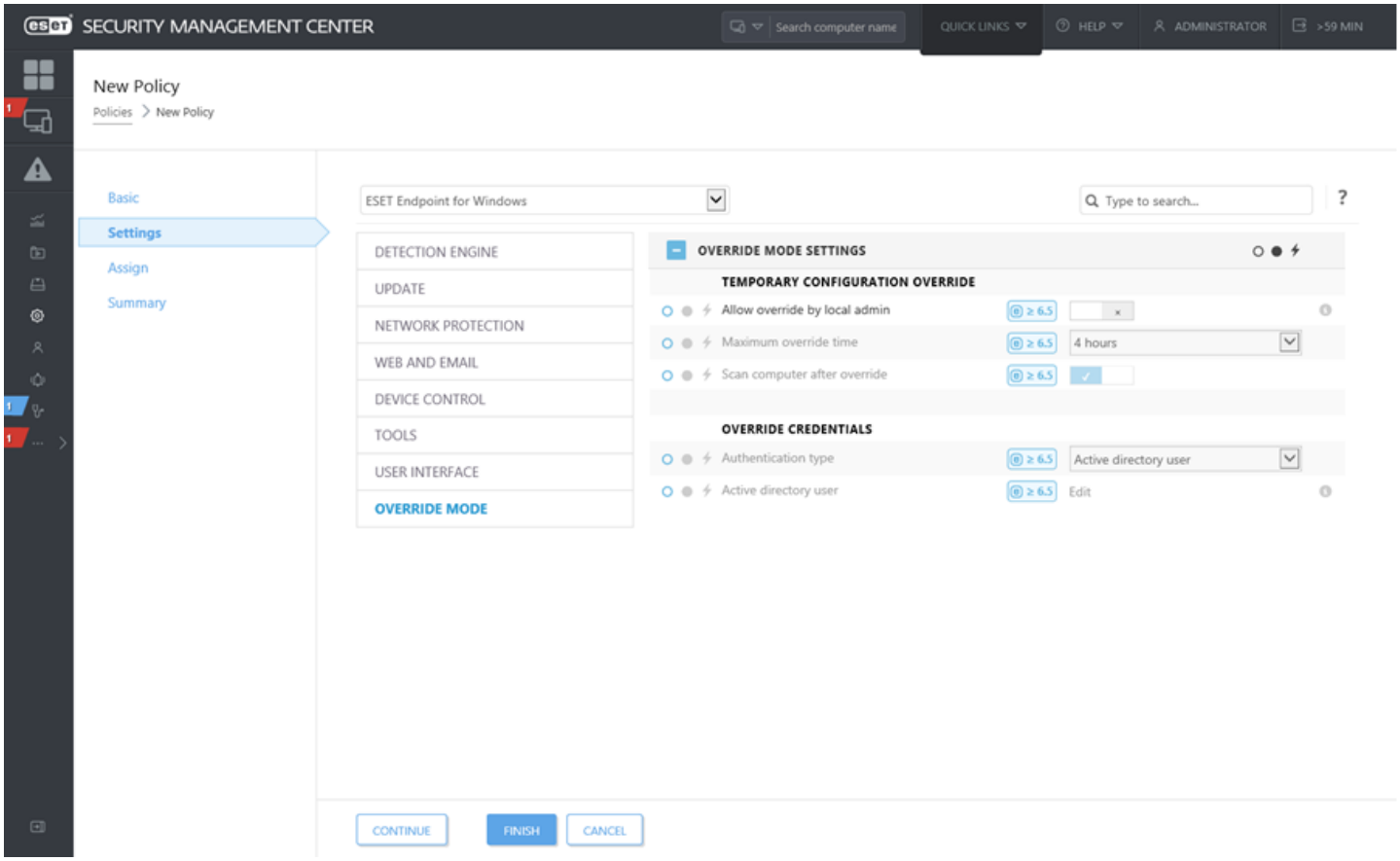
4.9.10 Ako používať Režim prepísania

Používatelia, ktorí majú na svojich zariadeniach nainštalované produkty ESET určené pre koncové zariadenia pre systém Windows (verzia 6.5 a vyššie), môžu využiť funkciu prepísania. Režim prepísania umožňuje používateľom na úrovni klienta meniť nastavenia v nainštalovaných produktoch ESET, a to aj v prípade, že nastavenia sú spravované politikou. Režim prepísania môže byť povolený pre používateľov AD alebo môže byť chránený heslom. Táto funkcia však nemôže byť povolená naraz dlhšie ako štyri hodiny.

Upozornenie:
- Režim prepísania nemôže byť po spustení zastavený pomocou nástroja ESMC Web Console. Režim prepísania sa vypne len po vypršaní stanoveného času alebo po vypnutí samotným klientom.
- Režim prepísania nemôže byť použitý pre Active Directory skupinu.

Nastavenie **Režimu prepísania**:

1. Prejdite do časti **Politiky** > **Nová politika**.
2. V sekcii **Základné** zadajte **Názov** a **Popis** pre danú politiku.
3. V sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows**.
4. Kliknite na **Režim prepísania** a nastavte pravidlá pre tento režim.
5. V sekcii **Priradiť** vyberte počítač alebo skupinu počítačov, na ktoré bude daná politika aplikovaná.
6. Skontrolujte nastavenia v sekcii **Súhrn** a kliknite na **Dokončiť** pre aplikovanie politiky.



PRÍKLAD:
Povedzme, že *John* má problém, kedy nastavenia jeho koncového bezpečnostného produktu blokujú na jeho počítači niektorú dôležitú funkcionalitu alebo prístup na internet. V takomto prípade môže správca *Johnovi* povoliť na jeho počítači prepísanie politiky aplikovanej na jeho koncovom bezpečnostnom produkte a umožniť manuálne doladenie nastavení. Tieto nové nastavenia môžu byť následne vyžiadané nástrojom ESMC, aby mohol na základne nich správca vytvoriť novú politiku.

Postupujte podľa nasledujúcich krokov:

1. Prejdite do časti **Politiky** > **Nová politika**.
2. Vyplňte polia **Názov** a **Popis**. V sekcii **Nastavenia** vyberte možnosť **ESET Endpoint pre Windows**.
3. Kliknite na **Režim prepísania**, povoľte tento režim na jednu hodinu a vyberte *Johna* ako používateľa AD.
4. Priraďte politiku na *Johnov počítač* a kliknite na **Dokončiť** pre uloženie politiky.
5. *John* musí povoliť **Režim prepísania** na svojom produkte ESET určenom pre koncové zariadenia a manuálne zmeniť nastavenia na svojom počítači.
6. V nástroji ESMC Web Console prejdite do časti **Počítače**, vyberte *Johnov počítač* a kliknite na možnosť **Zobraziť podrobnosti**.
7. V sekcii **Konfigurácia** kliknite na tlačidlo **Požiadať o konfiguráciu** pre naplánovanie úlohy pre klienta, aby ste z klienta čo najskôr získali konfiguráciu.
8. Po krátkom čase sa zobrazí nová konfigurácia. Kliknite na produkt, ktorého konfiguráciu chcete uložiť, a následne kliknite na **Otvoriť konfiguráciu**.
9. Môžete skontrolovať nastavenia a potom kliknúť na **Konvertovať na politiku**.
10. Vyplňte polia **Názov** a **Popis**.
11. V sekcii **Nastavenia** môžete v prípade potreby upraviť konfiguráciu.
12. V sekcii **Priradiť** môžete priradiť politiku k *Johnovmu počítaču* (alebo k iným počítačom).
13. Kliknite na **Dokončiť** pre uloženie nastavení.
14. Nezabudnite zrušiť prepisovanie politiky, ak už nie je potrebné.

4.10 Používatelia počítača

Táto časť vám umožňuje spravovať používateľov a skupiny používateľov na účely správy mobilných zariadení iOS. Správa mobilných zariadení je vykonávaná pomocou politík pridelených iOS zariadeniam. Odporúčame však najprv synchronizovať používateľov s Active Directory. Potom môžete upravovať používateľov alebo pridávať vlastné atribúty.

Dôležité:
Používatelia počítača sú odlišní od používateľov **ESMC Web Console**. Sekcia „Používatelia počítača“ vám umožňuje spárovať používateľa so zariadením, čím dôjde k synchronizácii určitých nastavení, ktoré sú špecifické pre daného používateľa. Pre správu používateľov ESMC Web Console a sád povolení prejdite do sekcie **Viac** > **Používatelia**.

- Používateľ zvýraznený oranžovou farbou nemá pridelené žiadne zariadenie. Kliknite na používateľa, vyberte možnosť Upraviť a kliknite na **Priradené počítače** pre zobrazenie podrobností o danom používateľovi. Kliknite na **Pridať počítače** pre priradenie počítačov alebo iných zariadení k používateľovi.

- Môžete tiež pridať alebo odstrániť **Priradených používateľov** zo sekcie Podrobnosti o počítači. Keď sa nachádzate v časti Počítače alebo v časti Skupiny, vyberte počítač alebo mobilné zariadenie a kliknite na **Zobraziť podrobnosti**. Používateľ môže byť priradený k viac ako jednému počítaču/mobilnému zariadeniu. Možnosť **Priradiť používateľa** vám umožňuje priradiť používateľa priamo k zvolenému zariadeniu. Ak je k používateľovi priradené zariadenie, môžete kliknúť na názov zariadenia a zobraziť jeho podrobnosti.
- Používateľov a skupiny používateľov môžete premiestňovať myšou (Drag & Drop). Označte používateľa alebo skupinu, podržte stlačené tlačidlo myši a presuňte položku do inej skupiny.
- Používateľov môžete filtrovať pomocou filtra v hornej časti obrazovky, a to kliknutím na tlačidlo **Pridať filter** a výberom položky zo zoznamu.

Akcie dostupné v rámci správy používateľov

Zobraziť podrobnosti

Časť podrobnosti o používateľovi zobrazuje informácie, ako napr. e-mailová adresa, pobočka alebo lokalita, vlastné atribúty a priradené počítače. K používateľovi môže byť priradený viac ako jeden počítač/mobilné zariadenie. Môžete zmeniť meno používateľa, popis alebo nadradenú skupinu. Vlastné atribúty, ktoré sú tu zobrazené, sú tie, ktoré môžu byť použité pri vytváraní politík.

Označte konkrétneho používateľa pre otvorenie roletového menu, odkiaľ môžete vykonávať akcie. Viac informácií o jednotlivých akciách nájdete v Legende ikon.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

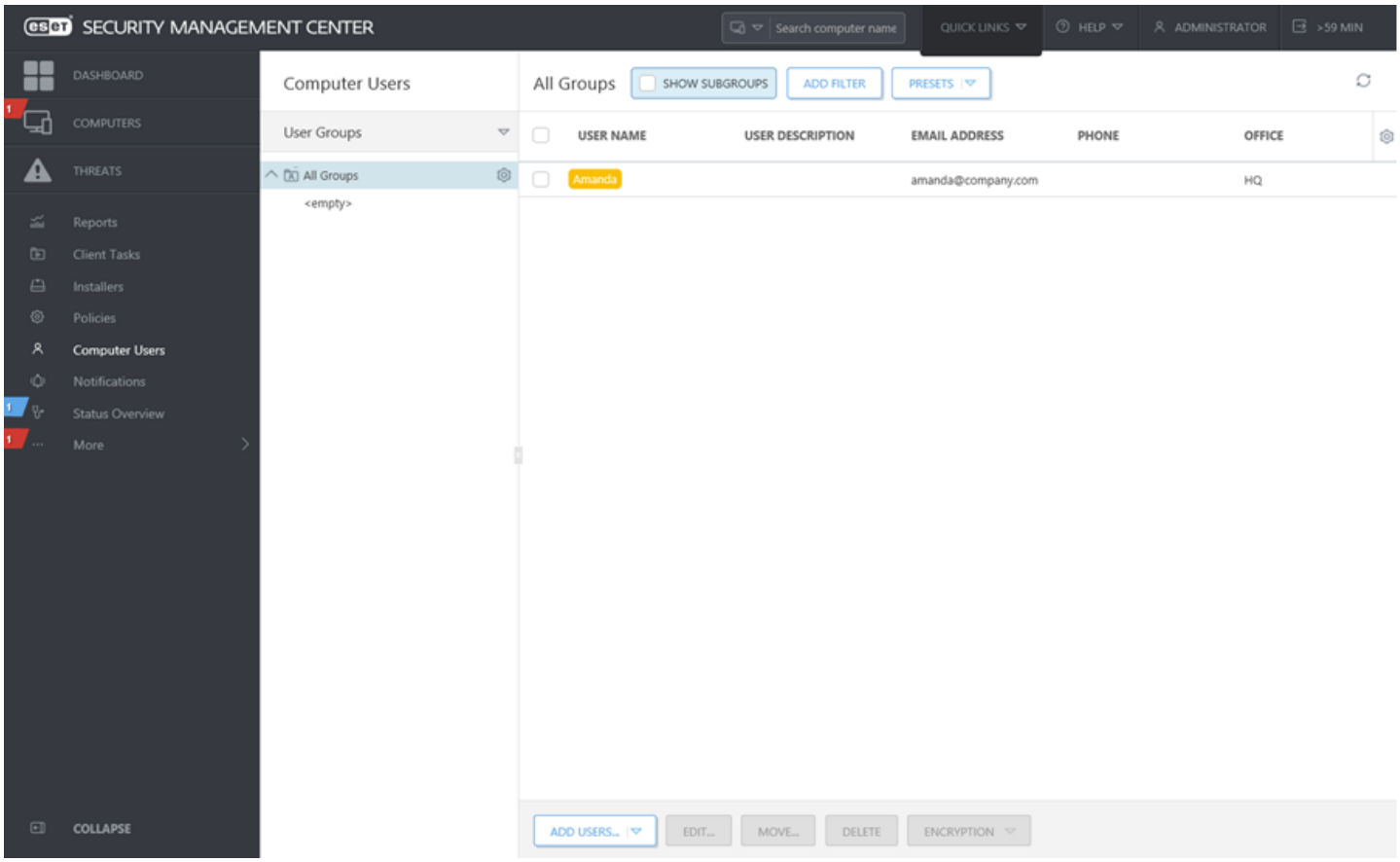
Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

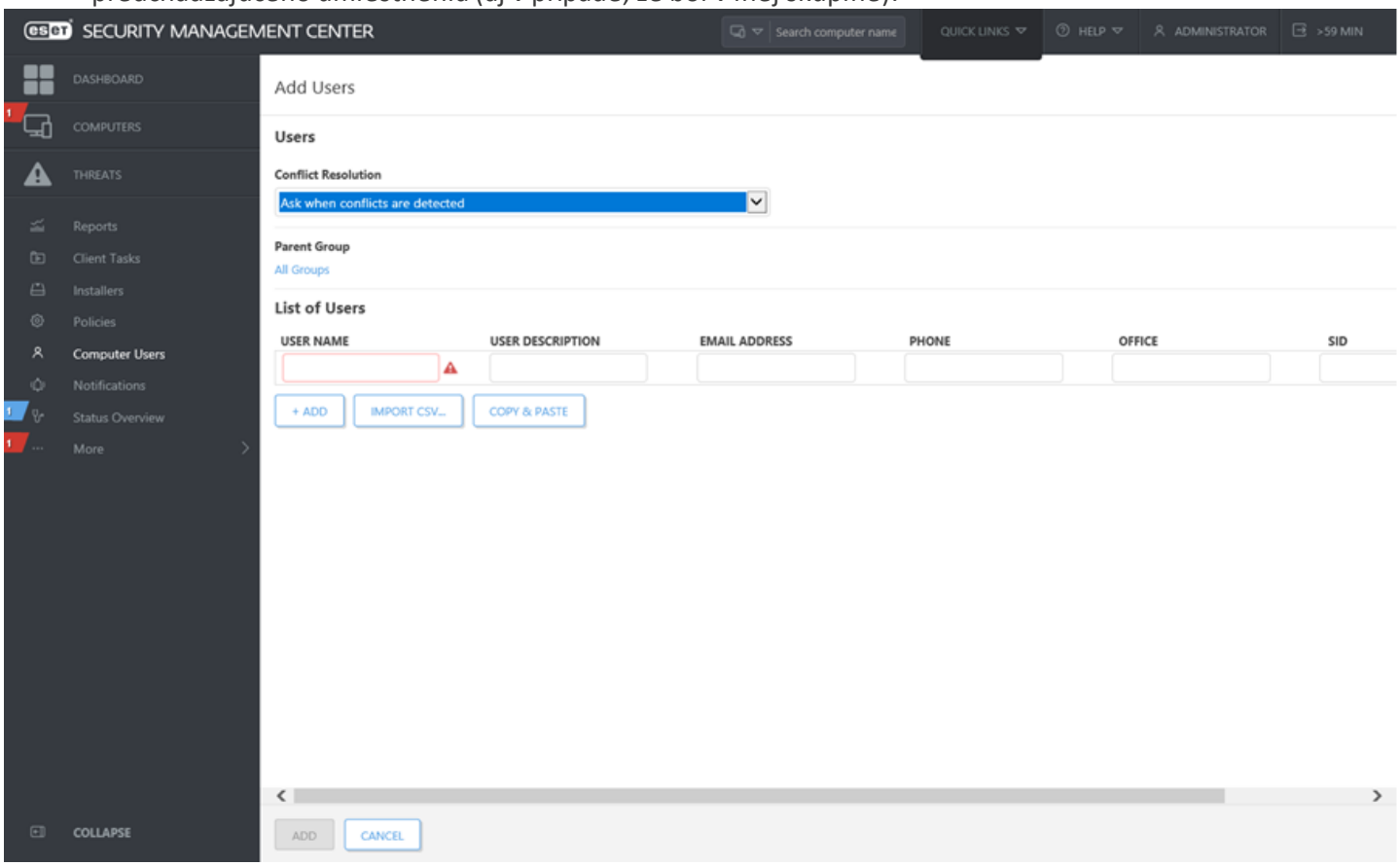
4.10.1 Pridanie nového používateľa

Kliknite na **Používatelia počítača** > **Pridať používateľov** pre pridanie používateľov, ktorí neboli nájdení alebo pridaní automaticky počas synchronizácie používateľov.



Zadajte meno používateľa, ktorého chcete pridať, do poľa **Meno používateľa**. Z roletového menu **Riešenie konfliktov** vyberte akciu, ktorá bude vykonaná, ak sa už používateľ, ktorého chcete pridať, nachádza v ESMC:

- **Spýtať sa, keď nastane konflikt**: Ak nastane konflikt, program sa spýta, akú akciu má vykonať (pozrite možnosti nižšie).
- **Preskočiť konfliktných používateľov:** Používatelia s rovnakým menom nebudú pridaní. Týmto sa tiež zaistí, že vlastné atribúty existujúceho používateľa v ESMC budú zachované (nie prepísané údajmi z Active Directory).
- **Prepísať konfliktných používateľov:** Existujúci používatelia v ESMC budú prepísaní používateľmi z Active Directory. Ak majú dvaja používatelia rovnaké SID, existujúci používateľ v ESMC bude odstránený zo svojho predchádzajúceho umiestnenia (aj v prípade, že bol v inej skupine).



Kliknite na + **Pridať** pre pridanie ďalších používateľov. Ak chcete naraz pridať viacero používateľov, kliknite na Import CSV pre odovzdanie *.csv* súboru obsahujúceho zoznam používateľov, ktorí majú byť pridaní. Kliknutím na **Skopírovať a vložiť** môžete importovať vlastný zoznam adries oddelených vlastnými oddeľovačmi (táto funkcia funguje podobne ako CSV import). V prípade potreby môžete zadať aj **Popis** pre používateľov, aby ich bolo možné jednoduchšie identifikovať.

Ak ste dokončili všetky zmeny, kliknite na **Pridať**. Používatelia sa zobrazia v nadradenej skupine, do ktorej ste ich zaradili.

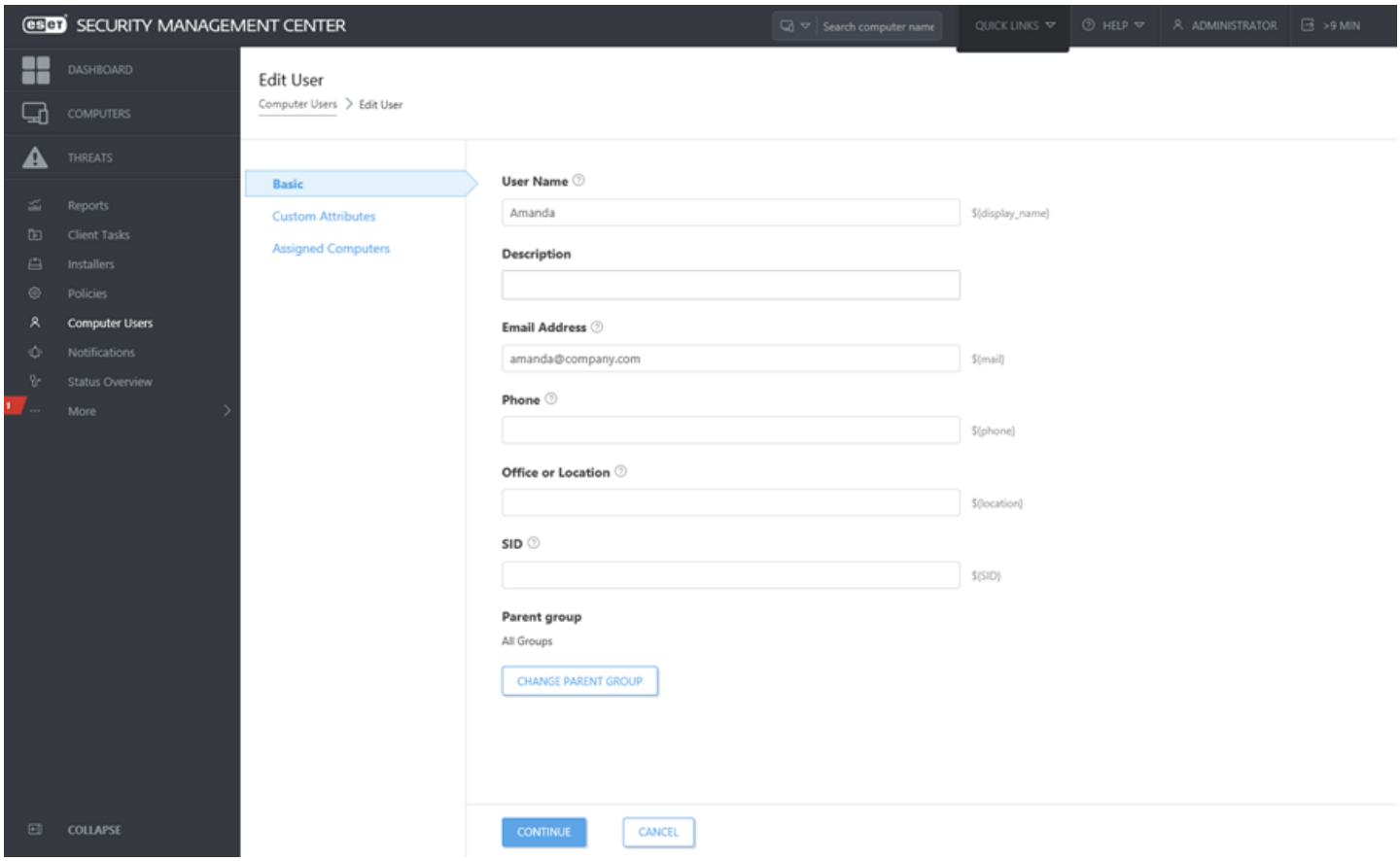
4.10.2 Úprava používateľov

Môžete upraviť podrobnosti o používateľovi, ako napr. **základné** informácie, **vlastné atribúty** a **priradené počítače**.

POZNÁMKA:
Pri vykonávaní úlohy Synchronizácia používateľa na používateľoch, ktorí majú špecifikované vlastné atribúty, nastavte pre funkciu **Riešenie kolízií pri vytváraní používateľov** možnosť **Preskočiť**. Ak tento krok nevykonáte, používateľské údaje budú prepísané údajmi z vášho Active Directory.

Základné

Ak ste na vytvorenie používateľa použili úlohu Synchronizácia používateľa a niektoré polia ostali nevyplnené, môžete ich vyplniť manuálne podľa požiadaviek.

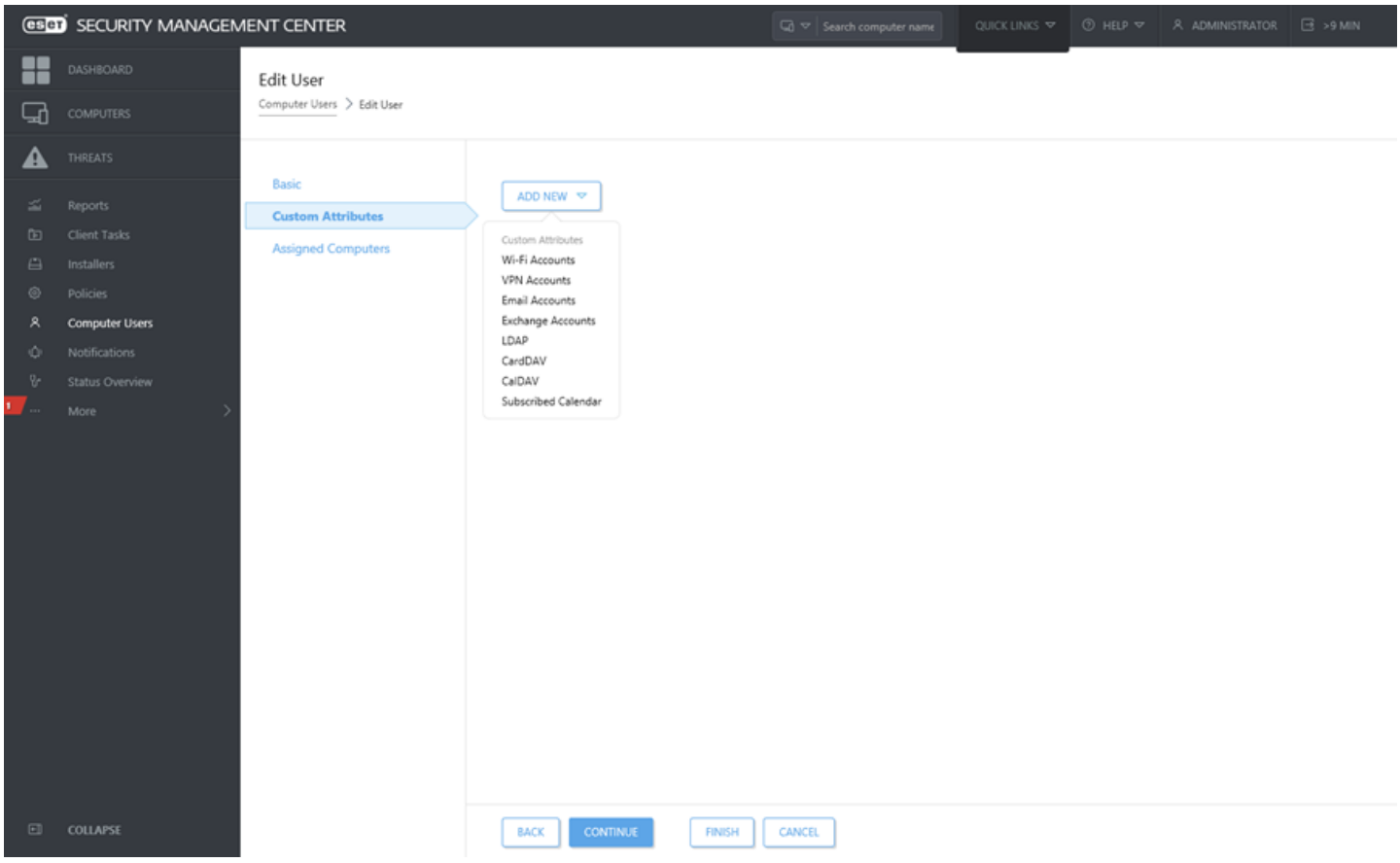


Vlastné atribúty

Môžete upraviť už existujúce vlastné atribúty alebo vytvoriť nové. Ak si želáte pridať nové atribúty, kliknite na možnosť **Pridať nový** a vyberte si z nasledujúcich kategórií:

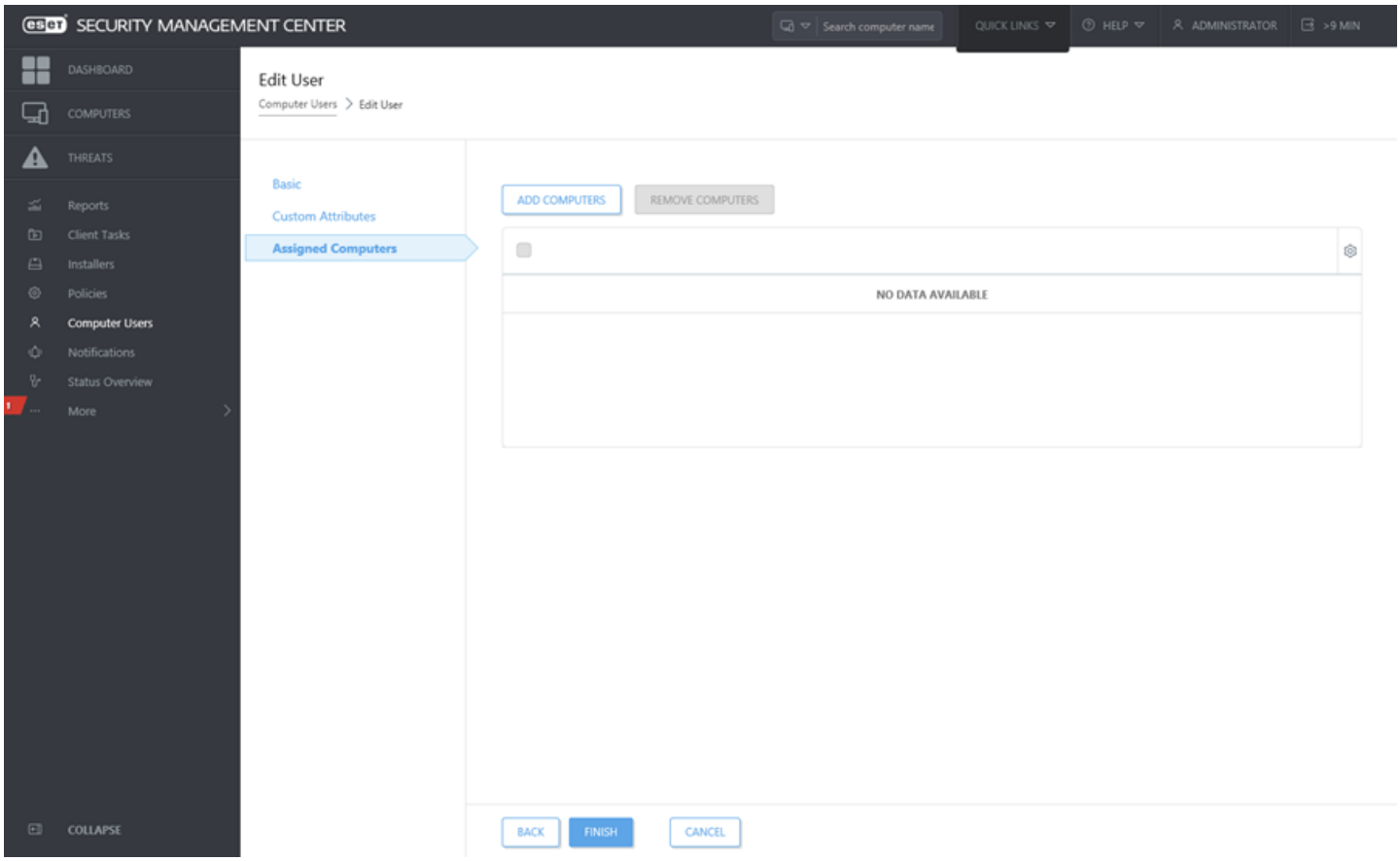
- **Wi-Fi účty:** Profily môžu byť použité na odosielanie podnikových Wi-Fi nastavení priamo na spravované zariadenia.
- **VPN účty:** Môžete nastaviť VPN spolu s povereniami, certifikátmi a ďalšími potrebnými informáciami na účely sprístupnenia VPN pre používateľov.
- **E-mailové účty**: Táto možnosť sa používa pre akýkoľvek e-mailový účet, ktorý používa IMAP alebo POP3 špecifikácie. Ak používate Exchange Server, použite Exchange ActiveSync nastavenia nižšie.
- **Exchange účty**: Ak vaša spoločnosť používa Microsoft Exchange, môžete vytvoriť všetky nastavenia priamo tu a tým pádom ušetriť čas potrebný pre nastavenie prístupu používateľom do pošty, kalendára a kontaktov.
- **LDAP (alias atribútu)**: Táto možnosť je obzvlášť užitočná v prípade, ak vaša spoločnosť využíva v rámci kontaktov LDAP. Môžete namapovať polia kontaktu k príslušným iOS poliam kontaktu.
- **CalDAV:** Táto sekcia obsahuje nastavenia pre akýkoľvek kalendár, ktorý využíva CalDAV špecifikácie.
- **CardDAV:** Táto možnosť je určená pre kontakty, ktoré sú synchronizované prostredníctvom CardDAV špecifikácie. Podrobnosti potrebné pre synchronizáciu môžu byť špecifikované tu.
- **Odoberaný kalendár**: Po nastavení CalDAV kalendárov tu môžete definovať prístup ku kalendárom ostatných, avšak tento prístup je len načítanie.

Z niektorých polí sa stane atribút, ktorý môže byť použitý pri vytváraní politiky pre mobilné zariadenie iOS ako premenná (zástupný symbol). Napríklad, prihlásenie `${exchange_login/exchange}` alebo e-mailová adresa `${exchange_email/exchange}`.



Priradené počítače

Tu môžete vybrať jednotlivé počítače/mobilné zariadenia. Toto je možné vykonať pomocou funkcie **Pridať počítače**. Budú zobrazené všetky statické a dynamické skupiny, ako aj členy týchto skupín. Pre výber použite začiarkavacie políčka a kliknite na **OK**.

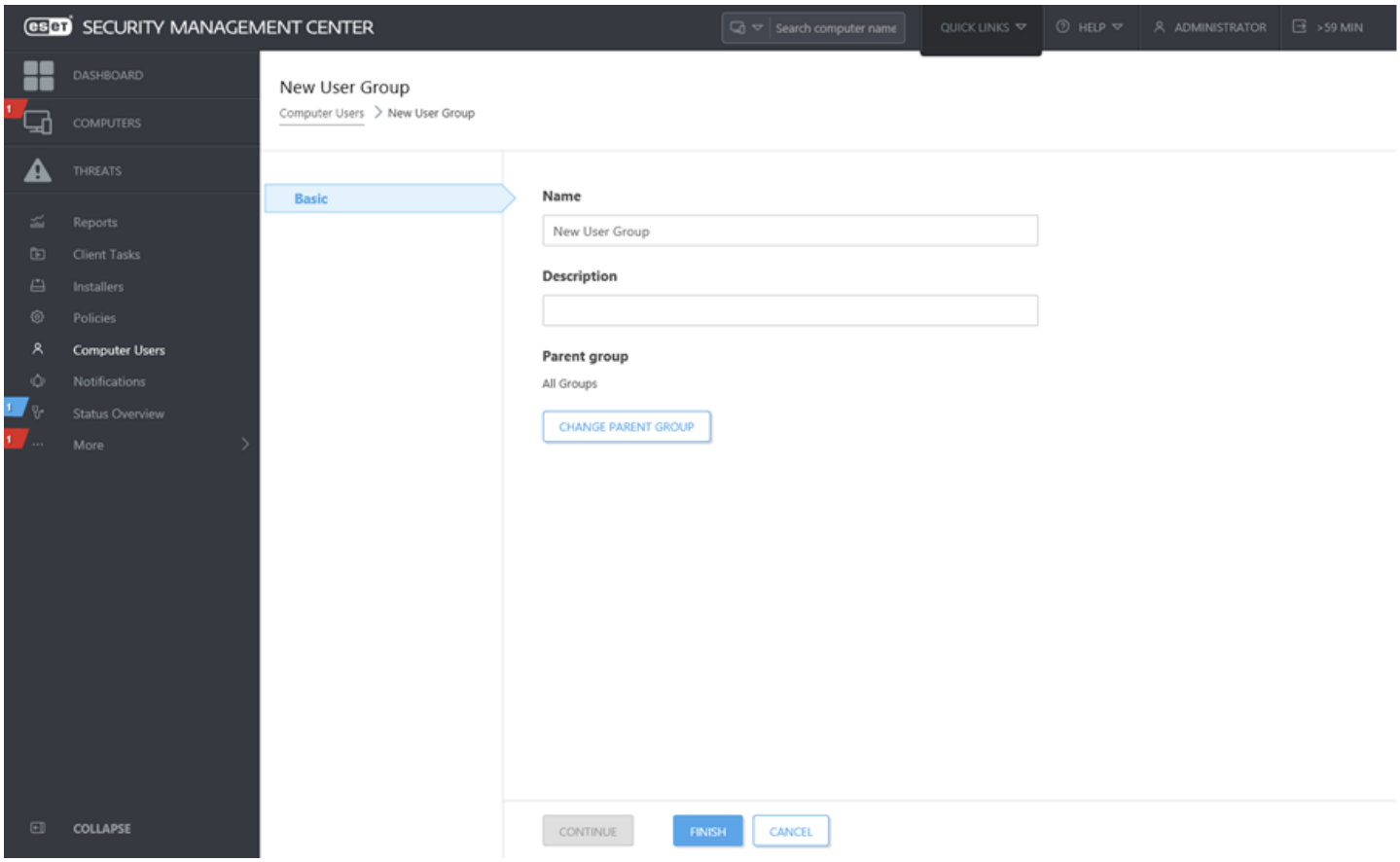

SECURITY MANAGEMENT CENTER
Search computer name
QUICK LINKS
HELP
ADMINISTRATOR
>9 MIN
DASHBOARD
COMPUTERS
THREATS
Reports
Client Tasks
Installers
Policies
Computer Users
Notifications
Status Overview
More
COLLAPSE
Edit User
Computer Users > Edit User
Basic
Custom Attributes
Assigned Computers
ADD COMPUTERS
REMOVE COMPUTERS
NO DATA AVAILABLE
BACK
FINISH
CANCEL

4.10.3 Vytvorenie novej skupiny používateľov

Kliknite na možnosť **Používatelia počítača** > ⚙ a vyberte možnosť + **Nová skupina používateľov**.

Základné

Zadajte **Názov** a **Popis** (voliteľné) pre novú skupinu používateľov. Štandardne je nadradenou skupinou skupina, ktorú ste označili pri vytváraní novej skupiny používateľov. Ak chcete zmeniť nadradenú skupinu, kliknite na možnosť **Zmeniť nadradenú skupinu** a označte príslušnú nadradenú skupinu zo stromovej štruktúry. Kliknite na **Dokončiť** pre vytvorenie novej skupiny používateľov.



–

Tejto skupine používateľov môžete prideliť špecifické povolenia v sekcii Prístupové práva pomocou Sád povolení (pozrite si sekciu **Skupiny používateľov**). Vďaka tomu môžete upresniť, ktorí konkrétni používatelia ESMC Web Console budú môcť spravovať ktoré konkrétne skupiny používateľov. V prípade potreby môžete používateľom dokonca pomocou politík zakázať prístup k určitým funkciám. Títo používatelia budú teda spravovať len skupiny používateľov.

4.11 Oznámenia

Oznámenia sú dôležité pre sledovanie celkového stavu vašej siete. Ak sa vyskytne nová udalosť (na základe vašej konfigurácie), budete upozornený pomocou vami nastavenej metódy (SNMP Trap, e-mail alebo syslog server). To vám umožní bezprostredne reagovať na danú situáciu.

- Všetky oznámenia môžu byť filtrované. Kliknite na **Pridať filter** v hornej časti obrazovky pre pridanie kritérií filtrovania a zadajte hľadaný výraz do poľa filtra:
  - **Názov** oznámenia.
  - **Popis** oznámenia.
  - **Používateľské meno** – používateľ, ktorý naposledy upravil oznámenie.
- Pre vytvorenie nového oznámenia kliknite na možnosť **Nové oznámenie** v dolnej časti obrazovky.
- Pre vykonanie akcií uvedených nižšie vyberte už existujúce oznámenie a kliknite na **Akcie**:
  - **Upraviť**: zmena nastavenia a odosielania oznámenia.
  - **Vymazať**: odstránenie oznámenia.
  - **Duplikovať**: vytvorenie duplicitného oznámenia s rovnakými parametrami vo vašej domácej skupine.
  - **Zapnúť/Vypnúť**: nastavenie **Stavu** oznámenia. Vypnuté oznámenie nie je vyhodnocované.

Oznámenia, používatelia a povolenia

Podobne ako pri úlohách pre server, aj v prípade oznámení ich používanie závisí od povolení, ktoré má pridelené aktuálne prihlásený používateľ. Pri každom vygenerovaní oznámenia sú brané do úvahy povolenia vykonávajúceho používateľa. Vykonávajúci používateľ je vždy ten používateľ, ktorý oznámenie upravoval ako posledný. Používateľ môže vidieť len tie oznámenia, ktoré sú zahrnuté v statickej skupine, pre ktorú má pridelené prístupové povolenia na **čítanie**.

Dôležité:
Pre správne fungovanie oznámenia je nevyhnutné, aby mal vykonávajúci používateľ pridelené dostatočné povolenia pre všetky objekty, na ktoré sa dané oznámenie viaže (zariadenia, skupiny, šablóny). Zvyčajne sú vyžadované povolenia na **čítanie** a **použitie**. Ak vykonávajúci používateľ tieto povolenia nemá, prípadne o ne časom príde, vygenerovanie oznámenia nebude úspešné. Oznámenia, ktorých vygenerovanie nebolo úspešné, sú označené oranžovou farbou a o ich zlyhaní bude používateľ informovaný prostredníctvom e-mailu.

Vytvorenie oznámenia – pre vytvorenie nového oznámenia musí mať používateľ pridelené povolenia na **zápis** pre oznámenia v jeho domácej skupine. Novovytvorené oznámenie bude zahrnuté do domácej skupiny používateľa.

Úprava oznámenia – pre upravovanie oznámenia musí mať používateľ pridelené povolenia na **zápis** pre oznámenia v rámci tej statickej skupiny, v ktorej je dané oznámenie umiestnené.

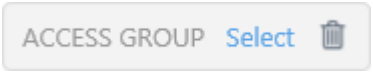
Odstránenie oznámenia – pre vymazanie oznámenia musí mať používateľ pridelené povolenia na **zápis** pre oznámenia v rámci tej statickej skupiny, v ktorej je dané oznámenie umiestnené.

Klonovanie a VDI

Existujú tri preddefinované oznámenia, ktoré môžu byť použité na upozornenie používateľa o udalostiach týkajúcich sa klonovania, prípadne si používateľ môže vytvoriť aj nové vlastné oznámenie.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

PRÍKLAD:
Používateľ *John*, ktorého **domáca skupina** je *Johnova skupina*, chce odstrániť (alebo upraviť) *Oznámenie 1*. Toto oznámenie bolo pôvodne vytvorené používateľom *Larry*, takže bolo automaticky zahrnuté do domácej skupiny Larryho, nazvanej *Larryho skupina*. Aby mohol *John* odstrániť (alebo upraviť) *Oznámenie 1*, musia byť splnené nasledujúce podmienky:

- *John* musí mať pridelenú sadu povolení, ktorá obsahuje povolenia na **zápis** v rámci kategórie Oznámenia.
- Sada povolení musí mať v časti **Statické skupiny** nastavenú skupinu *Larryho skupina*.

4.11.1 Správa oznámení

Oznámenia je možné spravovať v sekcii **Oznámenia**. S oznámeniami môžete vykonávať nasledujúce akcie:

- Kliknúť na **Nové oznámenie** pre vytvorenie nového oznámenia.
- Kliknúť na už existujúce oznámenie a z roletového menu vybrať konkrétnu akciu:

Zapnuté / **Vypnuté**	Zmena stavu oznámenia.
Upraviť	Zmena nastavení oznámenia.
Duplikovať	Vytvorenie duplicitného oznámenia vo vašej domácej skupine.
Vymazať	Odstránenie oznámenia.
Prístupová skupina > **Presunúť**	Premiestnenie oznámenia do inej prístupovej skupiny.

Nové oznámenie

Pre zasielanie oznámení e-mailom je potrebné najprv nakonfigurovať SMTP server.

Základné

Zadajte **Názov** a **Popis** oznámenia pre zjednodušenie filtrovania medzi rôznymi oznámeniami.

Každé nové oznámenie je predvolene **zapnuté**. Ak upravujete už existujúce oznámenie a chcete ho vypnúť, kliknite na tlačidlo prepínača a stav oznámenia sa zmení na **Vypnuté** .

Oznámenia môžu byť zapnuté alebo vypnuté kedykoľvek.

Konfigurácia

- **Udalosť**

  Existujú 3 základné typy udalostí, ktoré môžu vyvolať oznámenie. Každý typ udalosti ponúka rôzne možnosti v sekcii **Nastavenia**. Vyberte si jeden z nasledujúcich typov udalostí:

  - **Udalosti na spravovaných počítačoch**
  - **Aktualizácia stavu Security Management Center**
  - **Zmeny dynamických skupín**

Pokročilé nastavenia – Obmedzovanie

Obmedzovanie umožňuje nastaviť pokročilé pravidlá, ktoré určujú, kedy je vyvolané oznámenie. Viac informácií nájdete v časti Pokročilé nastavenia – Obmedzovanie.

Distribúcia

Nastavte spôsob distribúcie oznámení.

4.11.1.1 Udalosti na spravovaných počítačoch

Táto možnosť je použitá pre oznámenia, ktoré sa netýkajú dynamickej skupiny, ale systémových udalostí filtrovaných z protokolu udalostí. Vyberte kategóriu protokolov, na základe ktorej bude oznámenie vytvorené, a logický operátor pre filtre.

Kategória – vyberte si z nasledujúcich kategórií udalostí:

- **Hrozba firewallu**
- **Hrozba antivírusu**
- **Kontrolovať**
- **HIPS**
- **Upozornenia Enterprise Inspectora**
- **Blokované súbory**
- **Počítač pripojený prvýkrát**
- **Identita počítača obnovená**
- **Bola vytvorená otázka na klonovanie počítača**

V sekcii **Nastavenia** > **Filtrovať** sa nachádza zoznam dostupných udalostí, ktorý sa mení v závislosti od zvolenej kategórie. Hodnoty vo filtroch sú porovnávané priamo s udalosťami odoslanými od klientov. Neexistuje žiadny ohraničený zoznam dostupných hodnôt.

Monitorovaná statická skupina – vyberte statickú skupinu so zariadeniami, ktorá bude monitorovaná.

Nastavenia

V sekcii **Nastavenia** vyberte **Operátor** a hodnoty pre filter (**Filtrovať podľa**). Vybrať môžete len jeden operátor a všetky hodnoty budú vyhodnocované spolu pomocou daného operátora. Kliknite na **Pridať filter** pre pridanie novej hodnoty pre filter.

4.11.1.2 Aktualizácia stavu Security Management Center

Táto možnosť upozorní na zmeny stavu objektu vo vzťahu k nastaveným používateľským filtrom. Môžete použiť niektoré z existujúcich nastavení alebo si nastaviť vlastné parametre.

Načítať predvolené nastavenia – kliknutím na možnosť **Vybrať** môžete použiť niektoré z existujúcich nastavení. Kliknutím na **Vyčistiť** odstránite nastavenie zo sekcie **Nastavenia**.

Kategória – vyberte kategóriu objektov. V závislosti od vybranej kategórie sa budú zobrazovať objekty v sekcii **Nastavenia**.

Monitorovaná statická skupina – pre kategórie, kde sa oznámenie týka klienta (**Spravované klienty**, **Inštalovaný softvér**) môžete vybrať statickú skupinu, ktorá bude sledovaná. Ak nevyberiete žiadnu skupinu, budú sledované všetky objekty, ku ktorým máte prístup.

Nastavenia

Vyberte **Operátor** a hodnoty pre filter (**Filtrovať podľa**). Vybrať môžete len jeden operátor a všetky hodnoty budú vyhodnocované spolu pomocou daného operátora. Kliknutím na **Pridať filter** pridáte do filtra novú hodnotu. Ak použijete viacero filtrov, pri vyhodnocovaní sa použije operátor *AND* (oznámenie bude odoslané len v prípade, ak bude výsledok vyhodnotenia pre všetky hodnoty kladný – *true*).

Poznámka:
Niektoré filtre môžu spôsobiť, že oznámenia budú odosielané v nadmernom množstve. Preto sa odporúča použiť na agregáciu oznámení obmedzovanie.

Zoznam dostupných filtrov

Kategória	Hodnota	Poznámka
Certifikáty CA	Relatívny časový interval	Vyberte časový interval, v akom chcete sledovať udalosť.
Partnerské certifikáty		
Spravované klienty	Percento nepripájajúcich sa počítačov	Hodnota medzi 0 a 100. Toto je možné použiť len v kombinácii s filtrom **Relatívny časový interval**.
Licencie	Relatívny časový interval	Vyberte časový interval, v akom chcete sledovať vypršanie platnosti licencie.
	Percento využitia licencie	Hodnota medzi 0 a 100.
Úlohy pre klienta	Úloha	Vyberte úlohy pre filter platnosti. Ak nevyberiete žiadnu úlohu, budú vyhodnocované všetky úlohy.
	Úloha je neplatná	Vyberte možnosť **Áno** alebo **Nie**. Ak vyberiete možnosť **Nie**, oznámenie sa odošle v prípade, ak bude aspoň jedna z vybraných úloh (filter **Úloha**) neplatná.
Úlohy pre server	Počet (Zlyhalo)	Počet zlyhaní vybranej úlohy.
	Posledný stav	Posledný stav vybranej úlohy.
	Úloha	Vyberte úlohy pre tento filter. Ak nevyberiete žiadnu úlohu, budú vyhodnocované všetky úlohy.
	Úloha je neplatná	Vyberte možnosť **Áno** alebo **Nie**. Ak vyberiete možnosť **Nie**, oznámenie sa odošle v prípade, ak bude aspoň jedna z vybraných úloh (filter **Úloha**) neplatná.

Kategória	Hodnota	Poznámka
	Relatívny časový interval	Vyberte časový interval, v akom chcete sledovať udalosť.
Inštalovaný softvér	Názov aplikácie	Úplný názov aplikácie. Ak je sledovaných viacero aplikácií, použite operátor **je jedným z** pre pridanie ďalších záznamov.
	Dodávateľ aplikácie	Úplný názov výrobcu. Ak je sledovaných viacero výrobcov, použite operátor **je jedným z** pre pridanie ďalších záznamov.
	Stav kontroly verzie	Ak vyberiete možnosť **Neaktuálna verzia**, oznámenie sa odošle v prípade, ak je aspoň jedna aplikácia neaktuálna.
Sieťoví partneri	Partner	
	Stav servera	Ak je ESMC Server preťažený vytváraním protokolov, zmení sa jeho stav: • **Normálny** – okamžitá odpoveď zo servera. • **Obmedzený** – server odpovedá agentom raz za hodinu. • **Preťažený** – server agentom neodpovedá.
Oznámenia	Oznámenie	Vyberte oznámenie pre tento filter. Ak nevyberiete žiadnu úlohu, budú vyhodnocované všetky úlohy.
	Oznámenie je zapnuté	Vyberte možnosť **Áno** alebo **Nie**. Ak vyberiete možnosť **Nie**, oznámenie sa odošle v prípade, ak bude aspoň jedno z vybraných oznámení (filter **Oznámenie**) vypnuté.
	Oznámenie je platné	Vyberte možnosť **Áno** alebo **Nie**. Ak vyberiete možnosť **Nie**, oznámenie sa odošle v prípade, ak bude aspoň jedno z vybraných oznámení (filter **Oznámenie**) neplatné.

4.11.1.3 Zmeny dynamických skupín

Oznámenie bude odoslané po splnení podmienky. Môžete vybrať iba jednu podmienku, ktorá má byť monitorovaná pre konkrétnu dynamickú skupinu.

Dynamická skupina – vyberte dynamickú skupinu, ktorá bude vyhodnocovaná.

Nastavenia – **Podmienky**

Vyberte typ podmienky, ktorá vyvolá oznámenie.

- **Upozorniť pri každej zmene obsahu dynamickej skupiny**
  Povoľte túto možnosť, ak chcete byť upozornený pri pridaní, odstránení alebo zmene členov vybranej skupiny. ESMC kontroluje dynamickú skupinu každých 20 minút.

> **Dôležité:**
> ESMC kontroluje stav dynamickej skupiny jedenkrát každých 20 minút.
>
> Napríklad, ak prvá kontrola prebehne o 10.00, ostatné kontroly budú vykonané o 10.20, 10.40, 11.00 atď. Ak sa obsah dynamickej skupiny zmení o 10.05 a potom sa zmení späť o 10.13, ESMC počas najbližšej kontroly o 10.20 nerozpozná predošlú zmenu a nebude o nej informovať.

- Upozorniť, keď veľkosť skupiny prekročí zadaný počet
  Vyberte operátor **Veľkosť skupiny** a **Prah** pre oznámenie:
  - **Viac ako** – oznámenie bude odoslané, ak veľkosť skupiny dosiahne väčšiu hodnotu ako je stanovená prahová hodnota.
  - **Menej ako** – oznámenie bude odoslané, ak je veľkosť skupiny menšia ako je stanovená prahová hodnota.
- **Upozorniť, keď rest veľkosti skupiny prekročí zadanú mieru**
  Zadajte prahovú hodnotu a časové obdobie, ktoré vyvolajú oznámenie. Môžete zadať buď počet klientov, alebo

percento klientov (z celkového počtu klientov v dynamickej skupine). Zadajte časové obdobie (v minútach, hodinách alebo dňoch) pre porovnanie s novým stavom. Napríklad, pred 7 dňami bol počet klientov s neaktuálnymi bezpečnostnými produktmi na úrovni 10 a prahová hodnota (pozri nižšie) je nastavená na 20. Ak počet klientov s neaktuálnymi bezpečnostnými produktmi dosiahne hodnotu 30, budete upozornený.

- **Upozorniť, keď sa počet klientov v dynamickej skupine zmení v porovnaní s inou skupinou**
  Ak sa počet klientov v dynamickej skupine zmení podľa porovnávanej skupiny (statickej alebo dynamickej), bude odoslané oznámenie. **Prah** – udáva hraničnú hodnotu, ktorej presiahnutie spúšťa odoslanie oznámenia.

POZNÁMKA:
Oznámenie môžete priradiť len k dynamickej skupine, ku ktorej máte dostatočné prístupové práva. Ak chcete vidieť dynamickú skupinu, musíte mať **povolenie na čítanie** pre jej nadradenú statickú skupinu.

4.11.2 Distribúcia

Je potrebné zvoliť aspoň jeden z možných spôsobov distribúcie.

Odoslať SNMP Trap

Ak použijete túto možnosť, bude odoslaný SNMP Trap. SNMP Trap upozorní server pomocou SNMP správy. Viac informácií nájdete v kapitole Nastavenie služby SNMP Trap.

Odoslať e-mail

Ak použijete túto možnosť, bude odoslaná e-mailová správa vytvorená podľa vašich nastavení pre e-mailové správy. Podľa predvolených nastavení má notifikačný e-mail podobu HTML, pričom v päte e-mailu sa nachádza logo. V závislosti od vašich nastavení prispôsobenia (**Prispôsobenie** > **Logo so svetlým pozadím**) môžete použiť rôzne umiestnenia loga:

- **Žiadne prispôsobenie** – logo ESET Security Management Center bude umiestnené na ľavej strane päty.
- **Co-branding** – logo ESET Security Management Center bude umiestnené na ľavej strane päty, pričom vaše logo bude umiestnené na pravej strane päty.
- **White-labeling** – logo ESET Security Management Center sa nebude zobrazovať, zobrazené bude len vaše logo na ľavej strane päty.

Ak zvolíte možnosť **Odoslať e-mail**, zadajte aspoň jedného príjemcu správ.

- **E-mailová adresa** – zadajte e-mailové adresy príjemcov notifikačných správ.
- **Pridať e-mail** – umožňuje pridať nové pole s adresou.
- **Pridať používateľa** – pridanie adresy používateľa zo sekcie Používatelia počítača.
- **Import CSV** – import vlastného zoznamu adries z CSV súboru, kde sú použité oddeľovače.
- **Skopírovať a vložiť** – import vlastného zoznamu adries oddelených vlastnými oddeľovačmi. Táto funkcia funguje podobne ako CSV import.

Odoslať syslog

Je možné nastaviť, aby nástroj ESMC odosielal oznámenia a správy o udalostiach na váš Syslog server. Je tiež možné exportovať protokoly z bezpečnostného produktu spoločnosti ESET nainštalovaného na klientskom zariadení a odosielať ich na Syslog server. **Závažnosť syslogu** – z roletového menu vyberte úroveň závažnosti. Oznámenia so zvolenou úrovňou závažnosti sa potom zobrazia na Syslog serveri.

Základné polia v sekcii Distribúcia

- **Ukážka správy** – ukážka správy, ktorá sa zobrazí v oznámení. Ukážka obsahuje popis nastavení v textovej podobe. Môžete prispôsobiť obsah aj predmet správy a použiť premenné, ktoré sa pri generovaní oznámenia zmenia na skutočné hodnoty. Toto nastavenie je voliteľné, je však odporúčané pre lepšie filtrovanie oznámení a celkový prehľad. Na prispôsobenie predmetu a obsahu správy môžete použiť premenné.
  - **Predmet** – predmet notifikačnej správy. Pre úpravu obsahu kliknite na ikonu . Vhodný a presný predmet môže zlepšiť triedenie a filtrovanie správ.
  - **Obsah** – pre úpravu obsahu kliknite na ikonu .

- **Všeobecné**
  - **Jazyk** – jazyk predvolenej správy. Prispôsobená správa nie je preložená.
  - **Časové pásmo** – nastavte časové pásmo pre premennú **Čas výskytu** `${timestamp}`, ktorá sa môže použiť v rámci prispôsobenej správy.

PRÍKLAD:
Ak by udalosť nastala o 3.00 miestneho času, miestny čas by bol UTC+2, zvolená časová zóna UTC+4 a čas hlásený v oznámení 5.00.

Kliknite na **Dokončiť** pre vytvorenie novej šablóny na základe šablóny oznámenia, ktorej nastavenia ste práve upravili. Bude potrebné, aby ste pre takto vytvorenú šablónu zadali nový názov.

4.11.3 Nastavenie služby SNMP Trap

Pre prijímanie SNMP správ musíte nastaviť službu SNMP Trap. Postupujte podľa krokov uvedených nižšie v závislosti od vášho operačného systému:

WINDOWS

Prerekvizity

- Služba **Simple Network Management Protocol** musí byť nainštalovaná na počítači, na ktorom je nainštalovaný ESMC Server, a tiež na počítači, kde bude nainštalovaný softvér pre SNMP Trap.
- Oba počítače by sa mali nachádzať v rovnakej podsieti.
- Služba SNMP musí byť nastavená na počítači, na ktorom beží ESMC Server.

Konfigurácia služby SNMP (ESMC Server)

1. Stlačte kombináciu klávesov Windows + R pre otvorenie dialógového okna Spustenie, do poľa **Otvoriť** zadajte *Services.msc* a stlačte **Enter**. V okne služieb vyhľadajte službu SNMP Service.
2. Otvorte kartu **Traps**, zadajte **public** do poľa **Community name** (Názov komunity) a kliknite na **Add to list** (Pridať do zoznamu).
3. Kliknite na **Add** (Pridať), zadajte **Názov hostiteľa, IP adresu**, prípadne **IPX adresu** počítača, na ktorom je nainštalovaný softvér pre SNMP Trap, a kliknite na **Add** (Pridať).
4. Prejdite na kartu **Security** (Zabezpečenie). Kliknite na **Add** (Pridať) pre otvorenie okna **SNMP Service Configuration** (Konfigurácia služby SNMP). Zadajte **public** do poľa **Community name** (Názov komunity) a kliknite na **Add** (Pridať). Práva budú nastavené na **READ ONLY** (iba na čítanie), čo je v poriadku.
5. Uistite sa, že je označená možnosť **Accept SNMP packets from any hosts** (Pakety SNMP prijímať od všetkých hostiteľov) a kliknite na **OK** pre potvrdenie. Služba SNMP ešte nie je nakonfigurovaná.

Konfigurácia SNMP Trap aplikácie (klient)

1. Uistite sa, že služba SNMP je nainštalovaná na klientskom počítači.
2. Nainštalujte aplikáciu na prijímanie správ Trap (trap receiver).
3. Nakonfigurujte aplikáciu na prijímanie správ Trap tak, aby prijímala správy SNMP Trap z ESMC Servera (môže byť definovaná IP adresa ESMC Servera a nastavenia portu).
4. Uistite sa, že firewall na klientskych počítačoch povoľuje sieťovú komunikáciu v rámci SNMP komunikácie nastavenej v predchádzajúcom kroku.
5. Aplikácia na prijímanie správ Trap vám odteraz umožní prijímať správy z ESMC Servera.

Poznámka:
SNMP Trap nie je podporované virtuálnym zariadením ESMC.

LINUX

1. Nainštalujte balík snmpd pomocou niektorého z nasledujúcich príkazov:
   `apt-get install snmpd snmp` (pre distribúcie Debian, Ubuntu)
   `yum install net-snmp` (Red Hat a Fedora distribúcie)

2. Otvorte súbor */etc/default/snmpd* a vykonajte nasledujúce zmeny:

```
#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid'
```
Pridaním # na začiatok riadku tento riadok zakážete.

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid -c /etc/snmp/sn
```
Pridajte do súboru tento riadok.

```
TRAPDRUN=yes
```
Zmeňte parameter *trapdrun* na *yes*.

3. Vytvorte zálohu pôvodného súboru *snmpd.conf*. Súbor bude neskôr zmenený.

```
mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.original
```

4. Vytvorte nový súbor *snmpd.conf* a pridajte doň nasledujúce riadky:

```
rocommunity public
syslocation "Testing ESMC6"
syscontact admin@ERA6.com
```

5. Otvorte súbor */etc/snmp/snmptrapd.conf* a pridajte nasledujúci riadok na koniec súboru:

```
authCommunity log,execute,net public
```

6. Zadajte nasledujúci príkaz pre spustenie správcu služby SNMP a pre sledovanie prichádzajúcich správ:

```
/etc/init.d/snmpd restart
```
alebo
```
service snmpd restart
```

7. Pomocou nasledujúceho príkazu sa uistite, že služba je spustená a zachytávanie správ funguje:

```
tail -f /var/log/syslog | grep -i TRAP
```

4.12 Prehľad stavu

ESMC Server vykonáva pravidelné diagnostické kontroly. **Prehľad stavu** poskytuje informácie o štatistikách používania a všeobecnom stave vášho nástroja ESET Security Management Center. Môže vám tiež pomôcť s počiatočnou konfiguráciou nástroja ESET Security Management Center. Kliknite na **Prehľad stavu** pre zobrazenie podrobných informácií o celkovom stave nástroja ESET Security Management Center. Kliknutím na dlaždicu príslušnej sekcie zobrazíte panel úloh vpravo, ktorý obsahuje akcie. Každá dlaždica môže mať jednu z niekoľkých farieb v závislosti od stavu jednotlivých položiek, ktoré obsahuje (používa sa stav položky s najvyššou závažnosťou):

- Zelená (OK) – všetky položky v sekcii sú bez akýchkoľvek problémov.
- Žltá (Varovanie) – aspoň jedna položka v sekcii je označená varovaním.
- Červená (Chyba) – aspoň jedna položka v sekcii je označená chybou.
- Sivá (Nedostupný obsah) – obsah nie je dostupný kvôli nedostatočným prístupovým právam používateľa ESMC Web Console. V takomto prípade je potrebné, aby správca pridelil danému používateľovi dodatočné povolenia, prípadne je možné prihlásiť sa pod iným používateľom, ktorý má potrebné povolenia.
- Modrá (Informácie) – otázka súvisí s pripojenými počítačmi (podrobnejší popis nájdete nižšie v časti **Otázky**).

Prehľad stavu obsahuje nasledujúce sekcie:

Používatelia	V tejto časti môžete vytvoriť rôznych používateľov a nastaviť ich povolenia pre umožnenie správy v rámci nástroja ESET Security Management Center na rozdielnych úrovniach. Prednastavený účet správcu nástroja ESMC bol vytvorený počas inštalácie. Neodporúčame používať prednastavený účet správcu nástroja ESMC (účet Administrator) ako štandardný používateľský účet. Kliknite na možnosť **Pridať natívneho používateľa**, vytvorte nový natívny používateľský účet a používajte ho ako predvolený účet v ESET Security Management Center.

Certifikáty	Ak chcete použiť iné certifikáty ako tie, ktoré sú prednastavené a poskytnuté nástrojom ESMC, môžete pre umožnenie komunikácie s ESMC Serverom vytvoriť Certifikačné autority a Partnerské certifikáty pre individuálne súčasti nástroja ESET Security Management Center.
Licencie	ESET Security Management Center 7 využíva licenčný systém ESET. Vyberte metódu, ktorú chcete použiť na pridanie licencií pre aktiváciu súčastí ESMC a bezpečnostných produktov ESET na klientskych počítačoch.
Počítače	• **Pridať počítač** – pridanie klientskych počítačov, serverov a mobilných zariadení do vašej ESMC infraštruktúry. Pridať počítače a mobilné zariadenia môžete buď manuálne, alebo importovať zoznam zariadení. • **Pridať neautoriz. počítače** – automatický import počítačov detegovaných pomocou nástroja ESET RD Sensor. • **Nová synchronizačná úloha** – spustenie synchronizácie statickej skupiny s Active Directory, LDAP, VMware atď.
Agenty	• **Nová politika** – vytvorenie novej politiky pre ESET Management Agenta na zmenu intervalu pripojenia. • **Nasadiť agenta** – existuje viacero spôsobov, ako nasadiť ESET Management Agenta na klientske počítače vo vašej sieti.
Produkty	• **Konfigurovať repozitár** – zmena nastavení servera. • **Nainštalovať softvér** – ak je ESET Management Agent nasadený, môžete inštalovať softvér priamo z repozitára ESET alebo môžete upresniť umiestnenie inštalačného balíka (URL alebo zdieľaný priečinok). • **Nová politika** – vytvorenie novej politiky na zmenu konfigurácie bezpečnostného produktu spoločnosti ESET nainštalovaného na klientskych počítačoch.
Neplatné objekty	V tejto sekcii nájdete zoznam úloh pre klienta, úloh pre server, spúšťačov a oznámení, ktoré odkazujú na nedostupné alebo neplatné objekty. Po kliknutí na ktorékoľvek výsledkové pole sa zobrazí ponuka s vybraným zoznamom objektov.
Externé služby	Nástroj ESET Security Management Center môže byť nakonfigurovaný tak, aby sa pripájal k externým službám a poskytoval tak maximálnu funkcionalitu. • **Konfigurovať repozitár** – repozitár obsahuje inštalačné súbory pre ostatné bezpečnostné produkty ESET, ktoré môžete nainštalovať prostredníctvom úlohy určenej na inštaláciu softvéru. Repozitár sa konfiguruje v nastaveniach servera. V prípade potreby môžete vytvoriť offline repozitár. • **Konfigurovať aktualizácie** – aktualizácie sú dôležité pre udržiavanie nástroja ESET Security Management Center v aktuálnej verzii. Aktualizácie sú dostupné len ak ESET Security Management Center importoval licenciu pre produkt určený pre firmy, ktorej platnosť ešte nevypršala. Nastavenia aktualizácií môžete zmeniť v nastaveniach servera. • **Konfigurovať SMTP** – ESET Security Management Center môže byť nakonfigurovaný tak, aby sa pripájal na váš SMTP server, ktorý mu umožňuje odosielať e-mailové správy, napr. oznámenia, e-maily súvisiace s registráciou mobilných zariadení, správy atď.
Otázky	Otázka sa zobrazí v prípade, že je na klientskom zariadení zistené klonované zariadenie alebo zmena hardvéru. Podrobnejšie informácie o riešení otázok súvisiacich s klonovaním počítačov nájdete na nasledujúcom odkaze.

4.13 Viac

Sekcia **Viac** predstavuje pokročilý modul nastavení nástroja ESET Security Management Center. Táto sekcia obsahuje nástroje, ktoré správcovi umožňujú spravovať bezpečnostné riešenia spustené na klientskych počítačoch, ako aj nastavenia ESMC Servera. Tieto nástroje môžete použiť na nastavenie vášho sieťového prostredia tak, aby kládlo nízke požiadavky na údržbu.

V tejto sekcii sa nachádza:

- Skupiny
- Šablóny dynamickej skupiny
- Odoslané súbory
- Karanténa
- Správa licencií
- Prístupové práva
- Certifikáty
- Úlohy pre server
- Nastavenia servera

4.13.1 Skupiny

Skupiny je možné chápať ako priečinky, do ktorých sú triedené počítače a ostatné objekty. Nový bezpečnostný model prvýkrát uvedený v ERA 6.5 používa skupiny na zaraďovanie objektov a na priraďovanie povolení. Medzi objekty sa radia nielen počítače, ale aj oznámenia, politiky, certifikáty, inštalátory a sady povolení. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

Pre počítače a zariadenia môžete používať prednastavené skupiny a šablóny skupín alebo vytvárať svoje vlastné. Klientske počítače je možné do skupín pridávať. To vám umožňuje vytvoriť štruktúru počítačov podľa svojich predstáv a potrieb. Počítače môžete pridať do statickej skupiny.

Statické skupiny sú spravované manuálne. Dynamické sú usporiadané automaticky, na základe špecifických kritérií definovaných v šablóne. Ak sú počítače zaradené do skupín, môžete k týmto skupinám priradiť politiky, úlohy, nastavenia. Politika, úloha alebo nastavenia budú použité pre všetky vzdialené počítače z tejto skupiny. Sú dostupné dva typy skupín:

Statické skupiny

Statické skupiny sú skupiny s manuálne zvolenými počítačmi a objektmi. Členov tejto skupiny je možné pridať/odstrániť len manuálne, nie automaticky na základe dynamických kritérií. Každý objekt môže byť zahrnutý len v jednej statickej skupine. Statickú skupinu je možné vymazať len v prípade, že v nej nie sú zahrnuté žiadne objekty.

Dynamické skupiny

Dynamické skupiny sú skupiny zariadení, ktoré boli vytvorené na základe špecifických podmienok (do dynamických skupín sa iné objekty, ako napr. úlohy a politiky, nezaraďujú). Ak klientske zariadenie nespĺňa podmienku skupiny, bude zo skupiny odstránené. Počítače, ktoré spĺňajú podmienky, budú pridané do skupiny automaticky (preto tieto skupiny nesú názov „dynamické“).

Okno **Skupiny** je rozdelené na tri časti:

1. Na ľavej strane sa nachádza zoznam všetkých skupín a podskupín. Môžete tu vybrať skupinu a akciu pre túto skupinu z kontextového menu (vedľa názvu skupiny). Možnosti akcií sú rovnaké ako tie popísané nižšie (kontextové menu zobrazené po kliknutí na tlačidlo Akcie).
2. V pravej časti sa zobrazujú nasledujúce informácie o zvolenej skupine (môžete prepínať medzi kartami):
   - **Počítače**, ktoré patria do skupiny.
   - **Politiky** priradené ku skupine.
   - **Úlohy** priradené ku skupine.
   - **Súhrn** základných informácií o skupine.
3. Tlačidlá **Skupiny** a **Počítače** (v dolnej časti obrazovky) vám umožňujú vykonávať rôzne akcie so skupinami.

4.13.1.1 Akcie so skupinami

Kliknite na **Viac** > **Skupiny** a vyberte skupinu, ktorú chcete spravovať. Kliknite na tlačidlo **Skupina** alebo na ikonu vedľa názvu skupiny. Zobrazí sa ponuka s nasledujúcimi možnosťami:

Akcia so skupinou	Popis akcie so skupinou	Vzťahuje sa na	
		Statické skupiny	Dynamické skupiny
Zobraziť podrobnosti	Poskytuje prehľad vybranej skupiny.	✓	✓
Nová statická skupina	Vybraná skupina bude prednastavenou nadradenou skupinou. Ak je to potrebné, nadradenú skupinu môžete neskôr zmeniť pri vytváraní novej statickej skupiny.	✓	✗
Nova dynamická skupina	Vybraná skupina bude prednastavenou nadradenou skupinou. Ak je to potrebné, nadradenú skupinu môžete neskôr zmeniť pri vytváraní novej dynamickej skupiny.	✓	✓
Upraviť	Úprava vybranej skupiny. Zobrazia sa rovnaké nastavenia ako pri vytváraní novej skupiny (statickej alebo dynamickej).	✓	✓
Presunúť	Premiestnenie vybranej skupiny do inej skupiny alebo podskupiny.	✓	✓
Vymazať	Odstránenie vybranej skupiny.	✓	✓
Import	Umožňuje importovať zoznam (zvyčajne textový súbor) počítačov ako členov vybraných skupín a podskupín. Ak je už počítač členom danej skupiny, vyberte akciu, ktorá bude vykonaná v prípade konfliktu (duplikáty).	✓	✓
Exportovať	Pomocou tejto možnosti môžete exportovať členy vybranej skupiny (a podskupiny) ako zoznam (*.txt* súbor). Tento zoznam môžete neskôr importovať alebo ho použiť na kontrolu.	✓	✗
Pridať nové	Umožňuje pridať nové zariadenie.	✓	✗
Kontrolovať	Spustenie úlohy Manuálna kontrola na kliente, ktorý nahlásil hrozbu.	✓	✓
Aktualizovať moduly	Spustenie úlohy Aktualizácia modulov (aktualizácia bude spustená manuálne).	✓	✓

Mobil	Podrobnejšie informácie nájdete v časti Anti-Theft akcie. • **Znovu registrovať** – vytvorenie novej úlohy pre klienta. • **Hľadať** – vyžiadanie GPS súradníc vášho mobilného zariadenia. • **Zamknúť** – zariadenie bude uzamknuté po zachytení podozrivej aktivity alebo v prípade, že zariadenie je označené ako stratené. • **Odomknúť** – zariadenie bude odomknuté. • **Siréna** – vzdialené spustenie hlučnej sirény aj pokiaľ je na zariadení vypnutý zvuk. • **Vymazať** – všetky dáta uložené na zariadení budú natrvalo vymazané.	✓	✓
Spustiť úlohu	Táto funkcia vám umožňuje vybrať úlohy pre klienta, ktoré majú byť spustené na zariadeniach v tejto skupine.	✓	✓
Nová úloha	Vytvorenie novej úlohy pre klienta. Vyberte úlohu a nastavte pre danú úlohu obmedzenie (voliteľné). Úloha bude zaradená do poradia úloh čakajúcich na vykonanie podľa jej nastavení. Táto možnosť okamžite spustí úlohu, ktorú vyberiete zo zoznamu dostupných úloh. Pre túto úlohu nie je dostupný spúšťač, pretože bude vykonaná okamžite.	✓	✓
Naposledy použité úlohy	Zoznam naposledy použitých klientskych úloh pre všetky skupiny a počítače.	✓	✓
Správa politík	Umožňuje priradiť politiku k vybranej skupine.	✓	✓
Nové oznámenie	Vytvorenie nového oznámenia.	✗	✓
Aplikovať skôr **Aplikovať neskôr**	Zmena úrovne priority dynamickej skupiny.	✗	✓

4.13.1.2 Podrobnosti skupiny

Ak vyberiete v kontextovom menu skupiny možnosť **Zobraziť podrobnosti**, zobrazí sa prehľad vybranej skupiny:

Podrobnosti

V sekcii **Podrobnosti** môžete kliknutím na ikonu upraviť nastavenia skupiny, prípadne môžete **Pridať popis**. Nájdete tu informácie o umiestnení skupiny, jej **nadradenej skupine**, prípadne **podradených skupinách**. Ak je zvolená skupina dynamickou skupinou, môžete tu tiež vidieť dostupné operácie a pravidlá, podľa ktorých sú počítače vyhodnocované a priraďované k danej skupine.

Úlohy

V tejto časti môžete vidieť a upravovať úlohy pre klienta priradené k danej skupine.

Politiky

V tejto časti môžete vidieť a upravovať politiky priradené k danej skupine.

Poznámka:
V podrobnostiach skupiny sú zobrazené len tie úlohy a politiky, ktoré sú priradené k zvolenej skupine. Nie sú však zobrazené politiky a úlohy aplikované na jednotlivé počítače v danej skupine.

Upozornenia

V tejto časti nájdete zoznam upozornení prichádzajúcich z počítačov, ktoré patria do danej skupiny.

4.13.1.3 Presunutie statickej alebo dynamickej skupiny

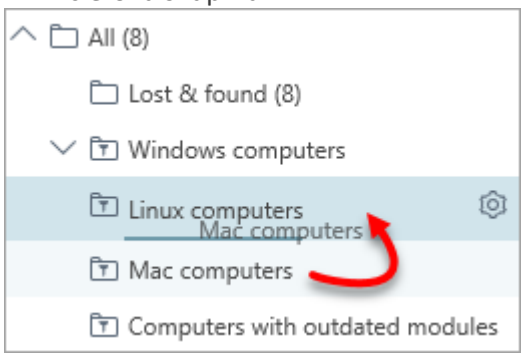
Dynamická skupina môže byť členom inej skupiny aj statickej. Statickú skupinu nie je možné presunúť do dynamickej skupiny. Taktiež nie je možné presunúť preddefinované statické skupiny (napr. statickú skupinu **Stratené a nájdené**) do žiadnej inej skupiny. Ostatné skupiny môžu byť presúvané.

Kliknite na ikonu vedľa názvu skupiny a potom kliknite na možnosť **Presunúť...** Otvorí sa okno zobrazujúce štruktúru skupín. Označte v ňom cieľovú skupinu (statickú alebo dynamickú), do ktorej chcete vybranú skupinu premiestiť. Cieľová skupina sa stane nadradenou skupinou. Skupiny môžete presúvať aj pomocou kurzora myši.

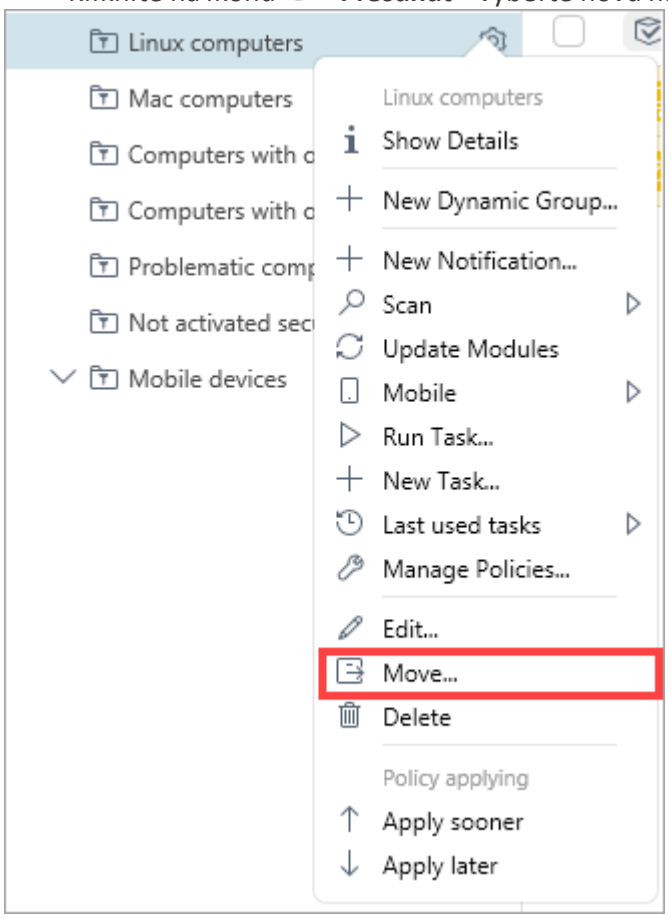
Poznámka:
Dynamická skupina nachádzajúca sa v novom umiestnení filtruje počítače (na základe šablóny) bez ohľadu na svoje predchádzajúce umiestnenie.

Skupinu je možné presunúť 3 spôsobmi:

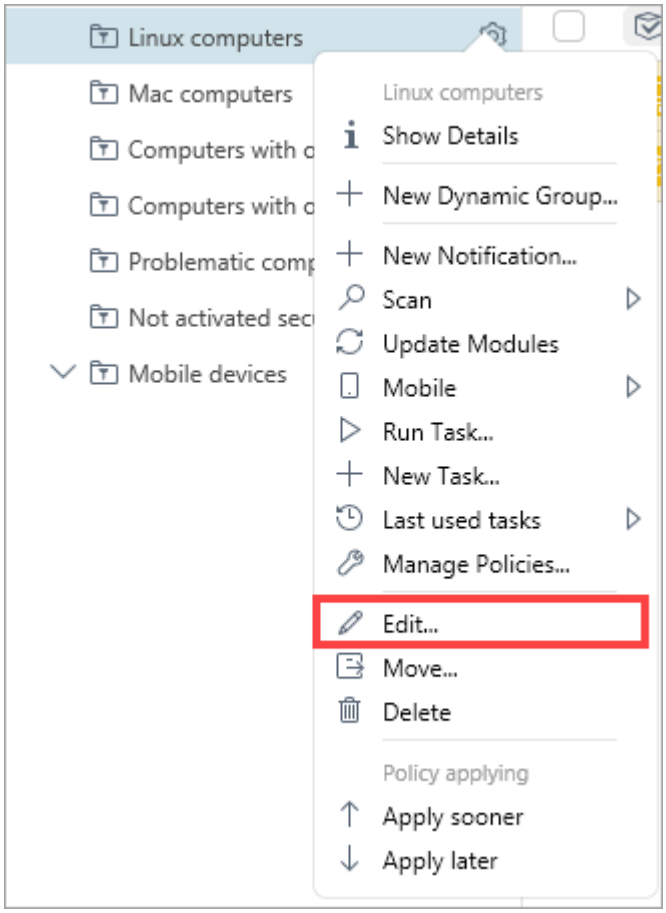
- **Drag and drop** – kliknite na skupinu a držte stlačené tlačidlo myši, až kým nepresuniete danú skupinu na cieľovú skupinu.



- Kliknite na ikonu > **Presunúť** > vyberte novú nadradenú skupinu zo zoznamu a kliknite na **OK**.

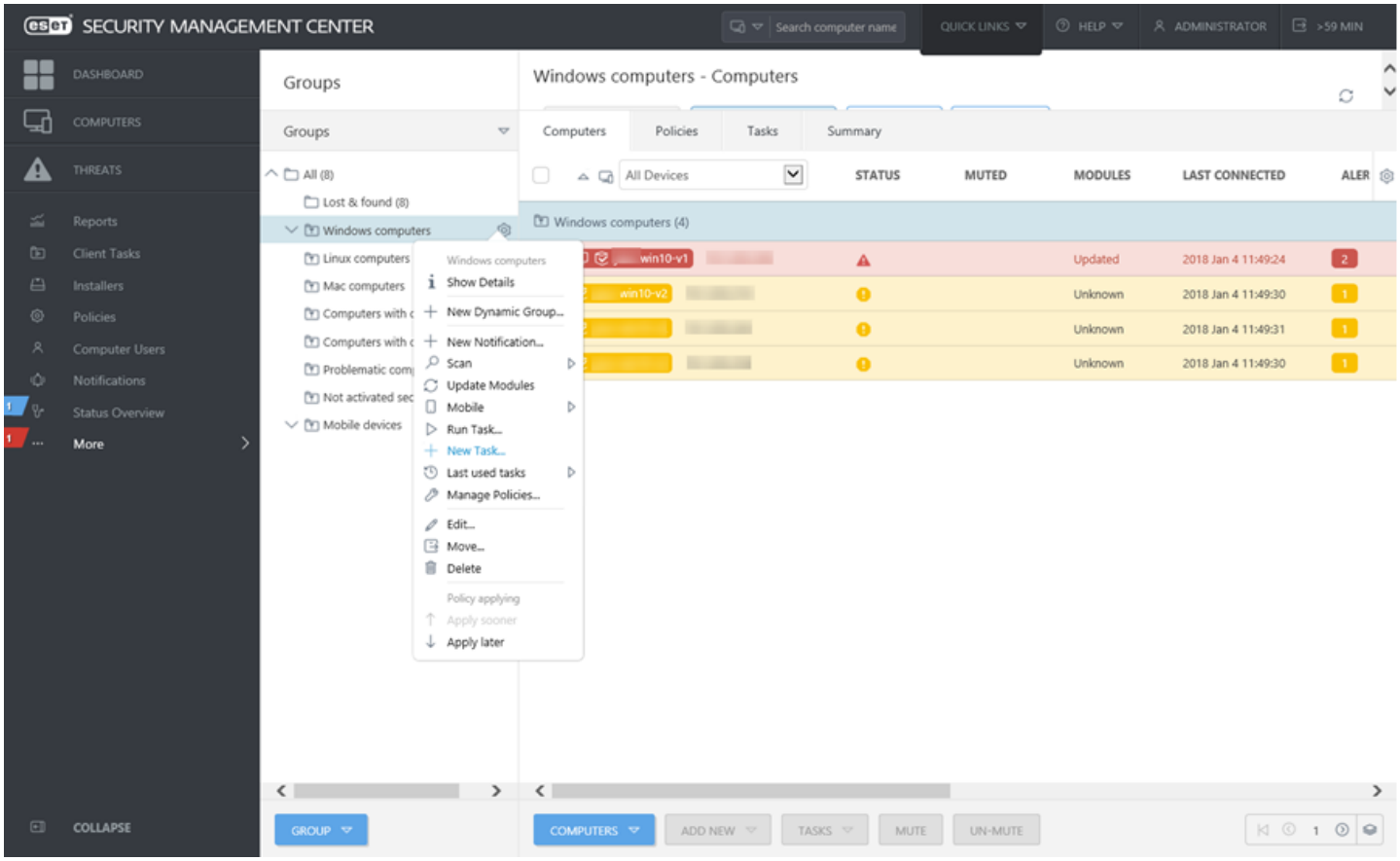


- Kliknite na ikonu > **Upraviť** > vyberte možnosť **Zmeniť nadradenú skupinu**. Vyberte novú nadradenú skupinu zo zoznamu a kliknite na **OK**.



4.13.1.4 Priradenie úlohy ku skupine

Kliknite na **Viac** > **Skupiny** > vyberte **Statickú** alebo **Dynamickú** skupinu > ⚙ vedľa označenej skupiny alebo kliknite na **Skupina** > + **Nová úloha**.



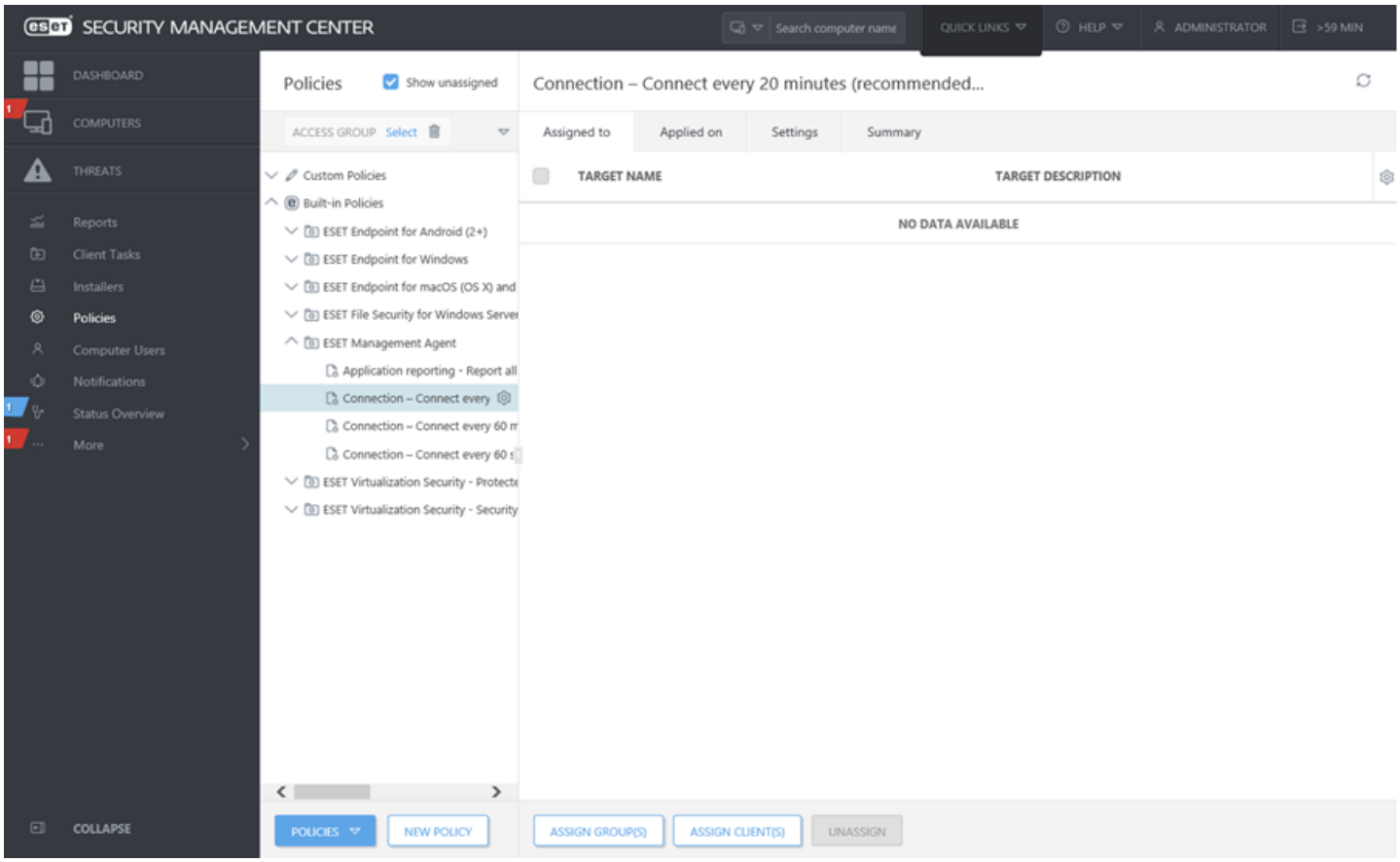
Rovnako môžete postupovať aj cez **Počítače** – vyberte **Statickú** alebo **Dynamickú skupinu** a kliknite na ⚙ > + **Nová úloha**. Následne sa zobrazí Sprievodca vytvorením novej úlohy pre klienta.

4.13.1.5 Priradenie politiky ku skupine

Po vytvorení politiky ju môžete priradiť k **statickej** alebo **dynamickej** skupine. Existujú dva spôsoby priraďovania politík:

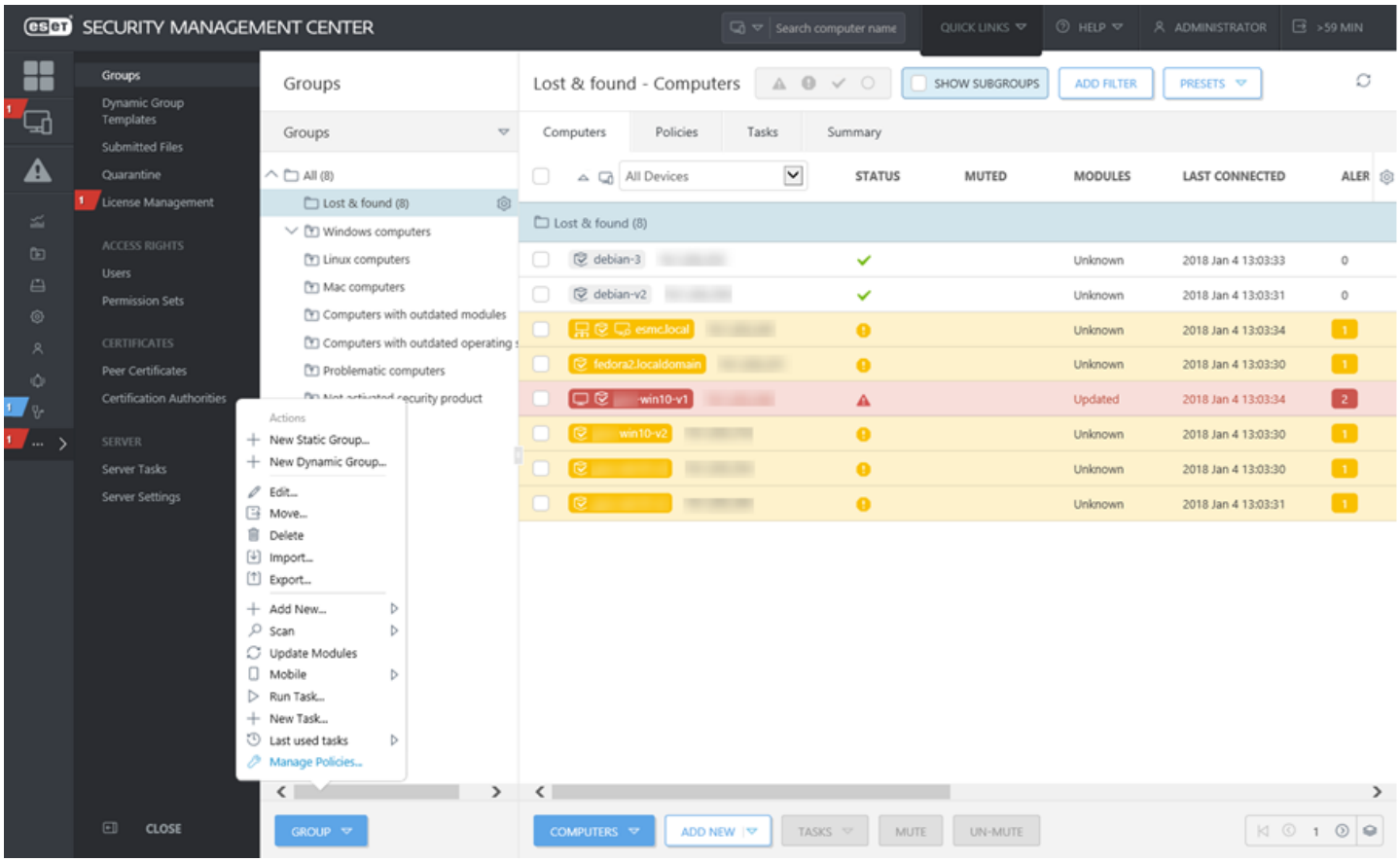
Metóda č. 1

V sekcii **Politiky** označte politiku a kliknite na **Priradiť skupinu(y)**. Vyberte statickú alebo dynamickú skupinu zo zoznamu (môžete vybrať viacero skupín) a kliknite na **OK**.



Metóda č. 2

1. Kliknite na **Viac** > **Skupiny** > **Skupina** alebo kliknite na ikonu vedľa názvu skupiny a vyberte možnosť **Spravovať politiky**.



2. V okne **Poradie uplatňovania politík** kliknite na **Pridať politiku**.
3. Označte politiku, ktorú chcete priradiť k tejto skupine a kliknite na **OK**.
4. Následne kliknite na **Zatvoriť**.

Ak chcete zobraziť, ktoré politiky sú priradené ku konkrétnej skupine, označte danú skupinu a kliknite na kartu **Politiky**.

Ak chcete zobraziť, ktoré skupiny sú priradené ku konkrétnej politike, označte danú politiku a kliknite na kartu **Aplikované na**.

Poznámka:
Viac informácií o politikách nájdete v kapitole Politiky.

4.13.1.6 Statické skupiny

Statické skupiny sa používajú:

- na triedenie zariadení a vytváranie hierarchického usporiadania skupín a podskupín,
- na triedenie objektov,
- ako domáce skupiny pre používateľov.

Statické skupiny je možné vytvárať iba manuálne. Zariadenia môžu byť manuálne presúvané do skupín. Každý počítač alebo mobilné zariadenie môže byť súčasťou len jednej statickej skupiny. Správa statických skupín je dostupná prostredníctvom akcií so skupinami.

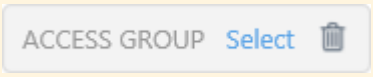
Existujú dve predvolené statické skupiny:

- **Všetko** – hlavná skupina pre všetky zariadenia v sieti ESMC Servera. Všetky objekty vytvorené správcom sú štandardne zahrnuté v tejto skupine. Táto skupina je vždy zobrazená a nie je možné ju premenovať. Prístup do tejto skupiny dáva používateľom automaticky prístup aj od všetkých jej podskupín; prideľovanie prístupových práv do tejto skupiny je preto potrebné vždy dobre zvážiť.
- **Stratené a nájdené** – podskupina skupiny **Všetko**. Každý nový počítač, ktorý sa po prvýkrát pripojí na ESMC Server, je automaticky zobrazený v tejto skupine. Túto skupinu je možné premenovať alebo kopírovať, ale nie je možné ju odstrániť alebo presunúť.

Dôležité:
Statickú skupinu je možné odstrániť len ak sú splnené tieto podmienky:

- Používateľ má pre túto skupinu pridelené povolenie na zápis,
- Skupina je prázdna.

Pokaľ daná statická skupina obsahuje nejaké objekty, odstránenie skupiny nebude možné. Tlačidlo filtra s názvom **Prístupová skupina** je umiestnené v každej sekcii s objektmi (napr. **Inštalátory**).



Kliknite na **Vybrať** pre zvolenie statickej skupiny – v príslušnej sekcii sa následne zobrazia iba objekty, ktoré sú súčasťou zvolenej skupiny. Tento filter umožňuje používateľovi jednoducho pracovať s objektmi patriacimi do jednej zvolenej skupiny.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

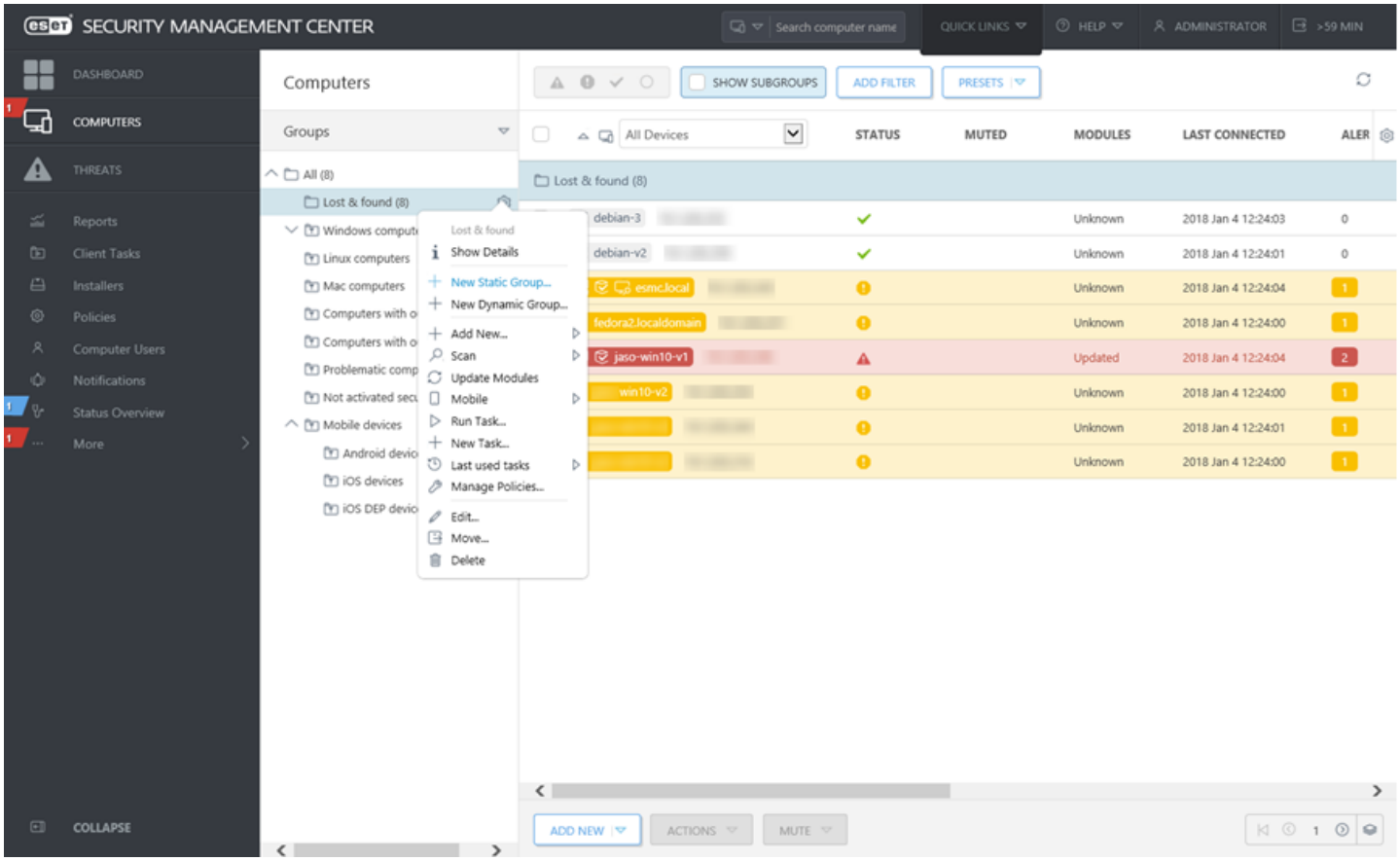
Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

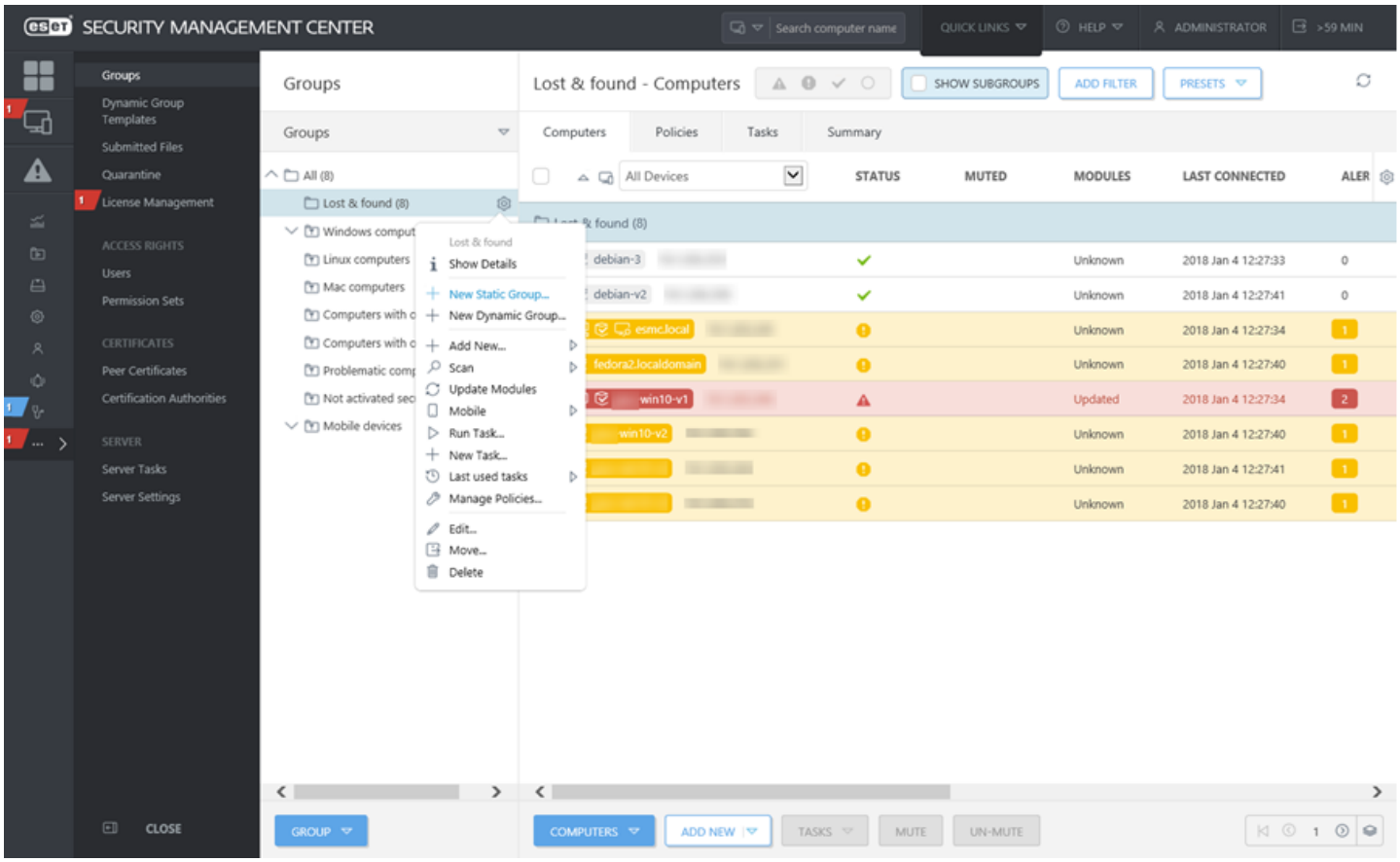
4.13.1.6.1 Vytvorenie novej statickej skupiny

Sú dostupné tri možnosti vytvorenia statickej skupiny:

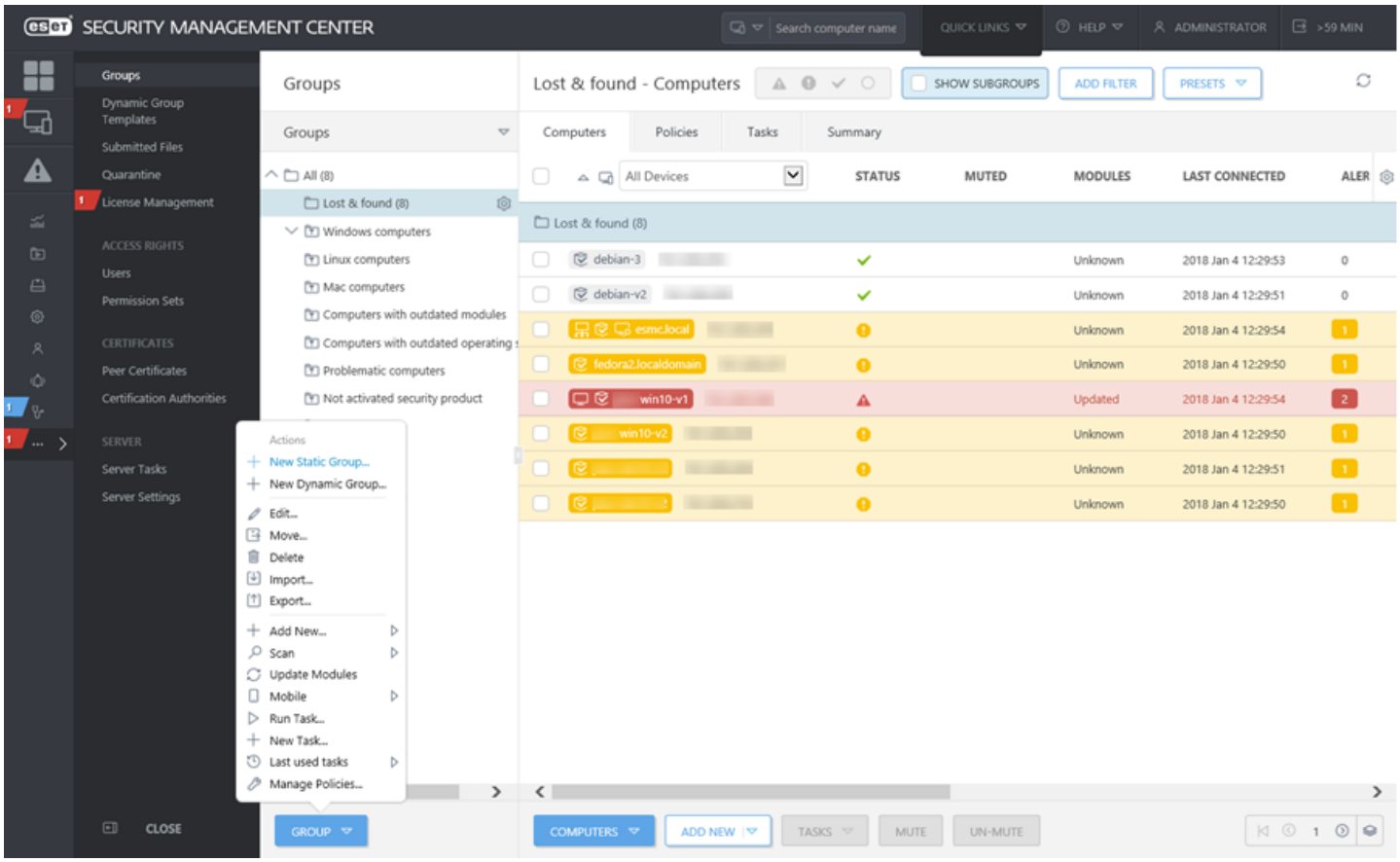
1. Kliknite na **Počítače** > **Skupiny** > ikonu ⚙ vedľa statickej skupiny a vyberte možnosť **Nová statická skupina**.



2. Kliknite na **Viac** > **Skupiny** > ikonu ⚙ vedľa statickej skupiny a vyberte možnosť **Nová statická skupina**.



3. Kliknite na **Viac** > **Skupiny** > vyberte statickú skupinu a kliknite na tlačidlo **Skupina**.



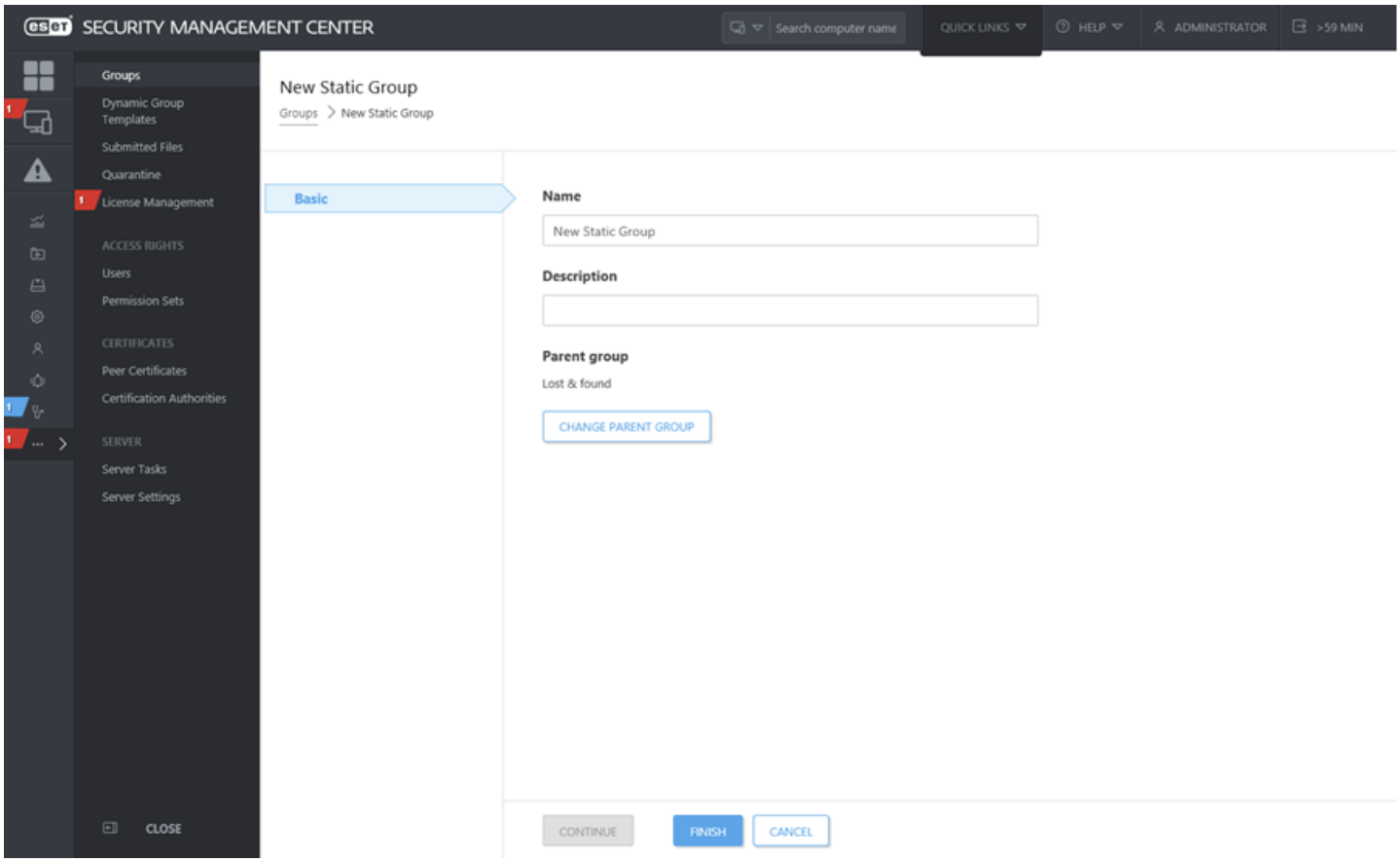
Pokračujte vo vytváraní novej statickej skupiny pomocou sprievodcu.

4.13.1.6.2 Sprievodca vytvorením novej statickej skupiny

Po zvolení možnosti Nová statická skupina postupujte podľa nasledujúcich krokov:

Základné

Zadajte **Názov** a **Popis** pre novú skupinu. V prípade potreby môžete zmeniť **Nadradenú skupinu**. Štandardne je nadradenou skupinou skupina, ktorú ste vybrali pri vytváraní novej statickej skupiny. Ak chcete zmeniť nadradenú skupinu, kliknite na možnosť **Zmeniť nadradenú skupinu** a označte príslušnú nadradenú skupinu zo stromovej štruktúry. Nadradená skupina novej statickej skupiny musí byť tiež statická skupina. Statická skupina nemôže byť súčasťou dynamickej skupiny. Pre vytvorenie novej statickej skupiny kliknite na **Dokončiť**.



4.13.1.6.3 Import počítačov z Active Directory

Pre import počítačov z AD vytvorte novú úlohu pre server: Synchronizácia statickej skupiny.

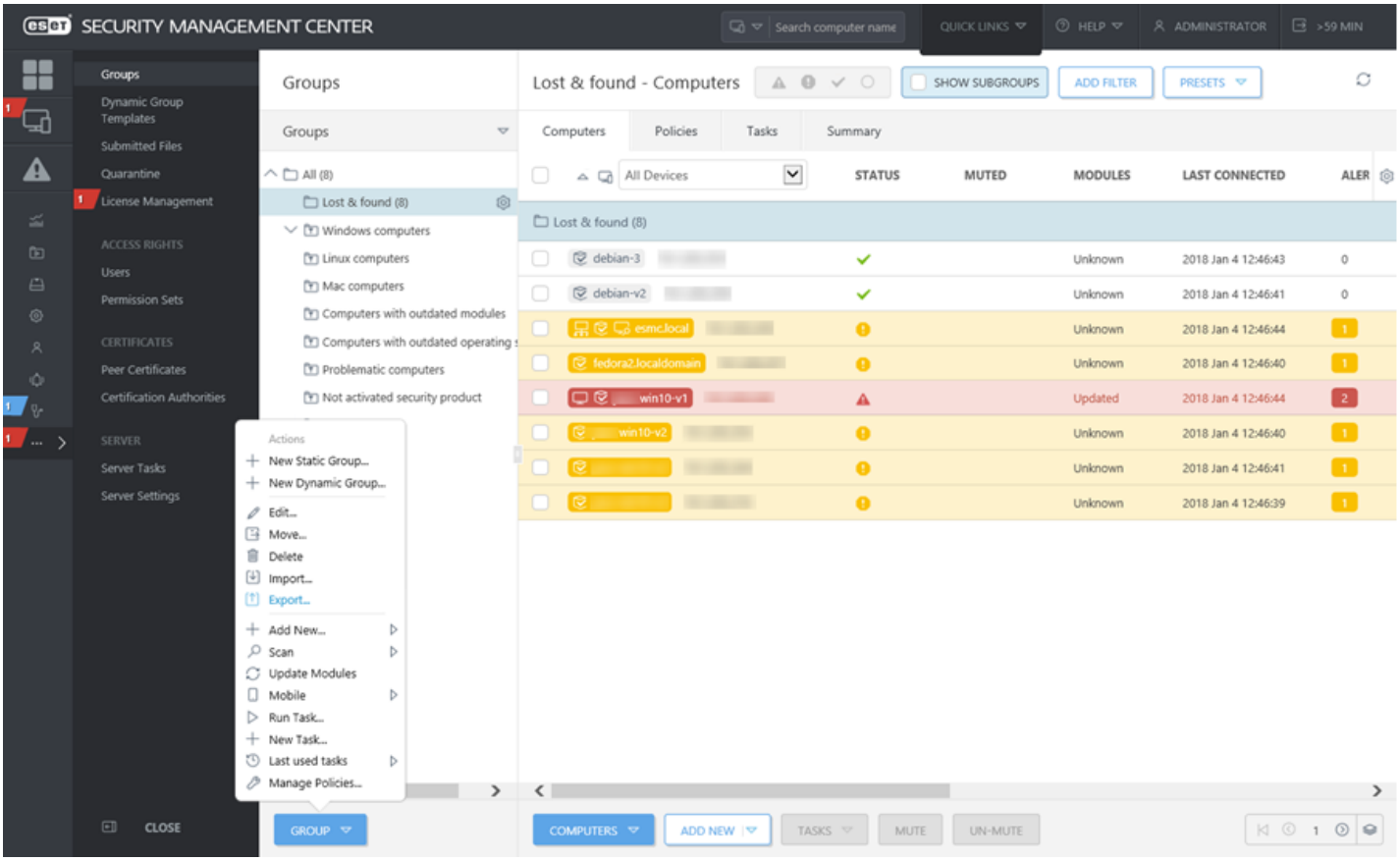
Vyberte skupinu, do ktorej chcete pridať nové počítače zo služby Active Directory. Taktiež vyberte objekty v AD, ktoré chcete synchronizovať a nastavte, čo sa má stať v prípade výskytu duplikátov. Nastavte parametre pripojenia k Active Directory a režim synchronizácie nastavte na **Active Directory/Open Directory/LDAP**.

4.13.1.6.4 Export statických skupín

Exportovanie zoznamu počítačov nachádzajúcich sa v ESMC štruktúre je jednoduché. Môžete exportovať zoznam a zálohovať ho tak, aby ste mohli daný zoznam kedykoľvek importovať späť, napríklad, ak chcete obnoviť štruktúru skupiny.

Poznámka:
Statické skupiny musia obsahovať aspoň jeden počítač. Exportovanie prázdnej skupiny nie je možné.

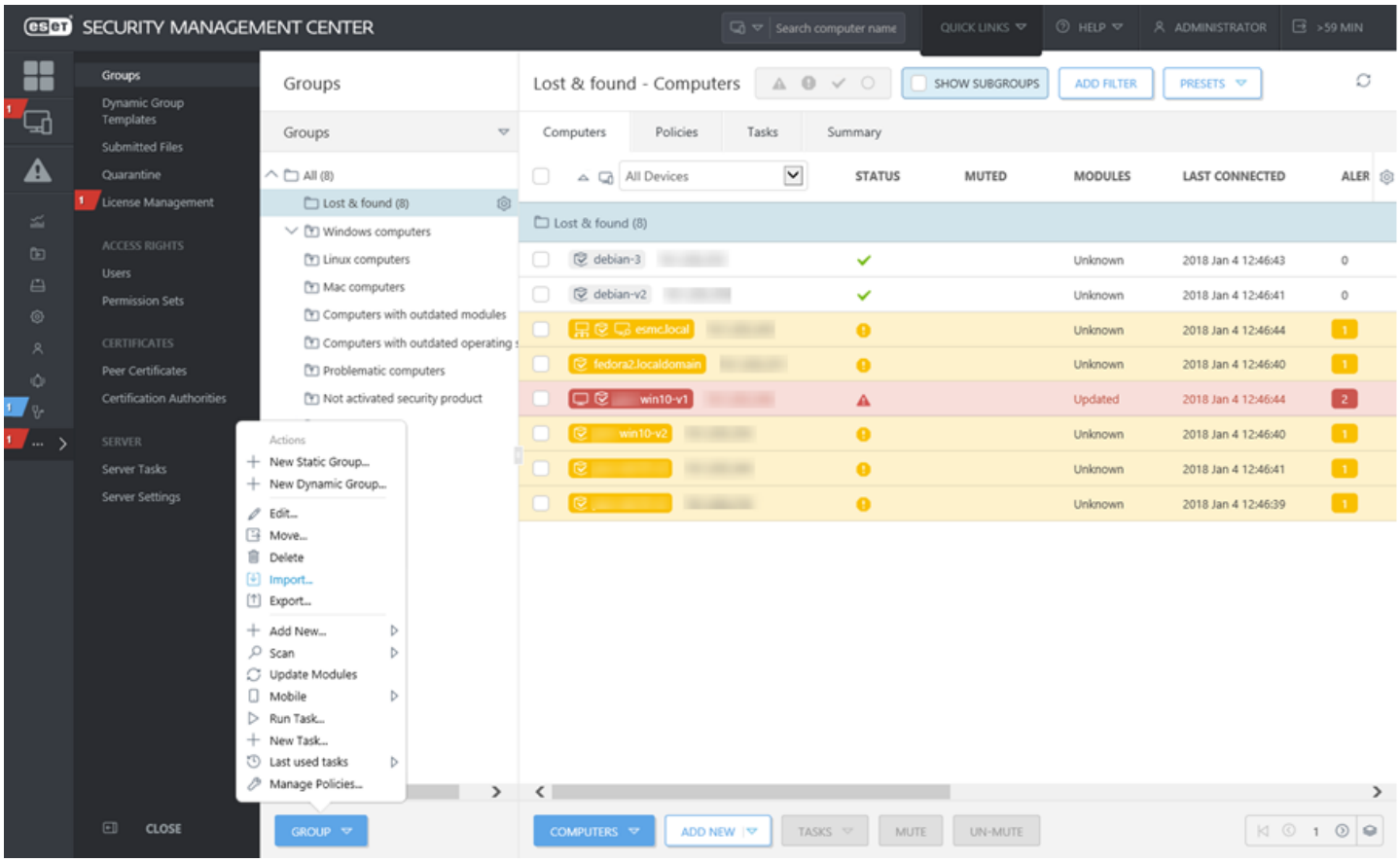
1. Kliknite na **Viac** > **Skupiny** > označte statickú skupinu, ktorú chcete exportovať.
2. Kliknite na tlačidlo **Skupiny** v spodnej časti okna.
3. Vyberte možnosť **Exportovať**.
4. Exportovaný súbor bude uložený vo formáte *.txt*.



Poznámka:
Dynamické skupiny nemôžu byť exportované, pretože dynamická skupina len odkazuje na počítače, ktoré spĺňajú kritériá definované v jej šablóne.

4.13.1.6.5 Import statickej skupiny

Exportované súbory zo statických skupín môžu byť importované späť do ESMC Web Console a zahrnuté do vašej existujúcej skupinovej štruktúry.



1. Kliknite na možnosť **Skupina**.
2. Vyberte možnosť **Importovať**.
3. Kliknite na **Prehľadávať** a prejdite na požadovaný *.txt* súbor.
4. Označte súbor a kliknite na **Otvoriť.** Názov súboru je zobrazený v textovom poli.
5. Vyberte si jednu z nasledujúcich možností riešenia konfliktov:
   - **Preskočiť konfliktné zariadenia**
     Ak už statická skupina existuje a počítače zo súboru *.txt* sa už v danej skupine nachádzajú, nebudú tieto počítače importované. Používateľ bude o tejto skutočnosti informovaný.
   - **Presunúť konfliktné zariadenia z iných skupín**
     Ak už statická skupina existuje a počítače zo súboru *.txt* sa už v danej skupine nachádzajú, je potrebné premiestniť počítače do inej statickej skupiny pred tým, ako bude vykonaný import. Po importovaní budú tieto počítače presunuté späť do pôvodných skupín, z ktorých boli presunuté.
   - **Duplikovať konfliktné zariadenia**
     Ak už statická skupina existuje a počítače zo súboru *.txt* sa už v danej skupine nachádzajú, duplikáty týchto počítačov budú vytvorené v rovnakej statickej skupine. Pôvodný počítač bude zobrazený s úplnými informáciami a jeho duplikát bude zobrazený len s názvom počítača.
6. Po kliknutí na možnosť **Importovať** budú importované statické skupiny a počítače zo súboru.

4.13.1.7 Dynamické skupiny

Dynamické skupiny sú v podstate filtre, ktoré sú založené na stave počítačov. Na jeden počítač môžu byť aplikované rôzne filtre, preto môže byť zaradený do viacerých dynamických skupín. To je rozdiel oproti statickým skupinám, kde môže byť počítač len v jedinej skupine.

Dynamické skupiny majú pravidlá definované v šablónach dynamickej skupiny. Na to, aby sa počítač stal členom dynamickej skupiny, musí splniť určité podmienky. Tieto podmienky sú definované v šablóne dynamickej skupiny. Každá šablóna sa skladá z niekoľkých pravidiel. Tieto pravidlá môžete definovať pri vytváraní novej šablóny.

Spôsobilosť zariadení na zaradenie do dynamických skupín je vyhodnocovaná vždy, keď sa prihlásia do nástroja ESET Security Management Center. Akonáhle stav zariadenia zodpovedá hodnotám definovaným v šablóne dynamickej skupiny, počítač bude automaticky pridaný do danej skupiny. Počítače sú filtrované na strane agenta, takže na server nie sú odosielané žiadne dodatočné informácie. Agent rozhoduje o tom, do ktorej dynamickej skupiny klient patrí a na server odosiela len svoje rozhodnutie.

Poznámka:
Pokiaľ klientske zariadenie nie je pripojené (napr. je vypnuté), jeho členstvo v dynamických skupinách nie je aktualizované. Keď sa zariadenie opäť pripojí, dôjde k aktualizácii jeho členstva v dynamických skupinách.

Po inštalácii nástroja ESET Security Management Center sú k dispozícii prednastavené dynamické skupiny. V prípade potreby môžete vytvoriť vlastné dynamické skupiny. Sú na to 2 spôsoby:

- Vytvoriť šablónu a až potom vytvoriť dynamickú skupinu.
- Vytvoriť novú šablónu pri vytváraní novej dynamickej skupiny.

Používateľ môže využívať dynamické skupiny v rôznych častiach ESMC. Je možné k nim priradiť priradiť politiku (politiky sú aplikované tak, ako je uvedené tu) alebo pripraviť úlohy pre všetky počítače v skupine.

Dynamická skupina môže byť podskupinou statickej skupiny alebo ďalších dynamických skupín. Statickú skupinu však nie je možné presunúť do dynamickej skupiny. Všetky dynamické skupiny pod určitou statickou skupinou môžu filtrovať len zariadenia zaradené v nadradenej statickej skupine. Ak sa dynamická skupina nachádza v inej dynamickej skupine, filtruje výsledky nadradenej dynamickej skupiny. Po vytvorení môžete dynamickú skupinu v rámci stromovej štruktúry presúvať.

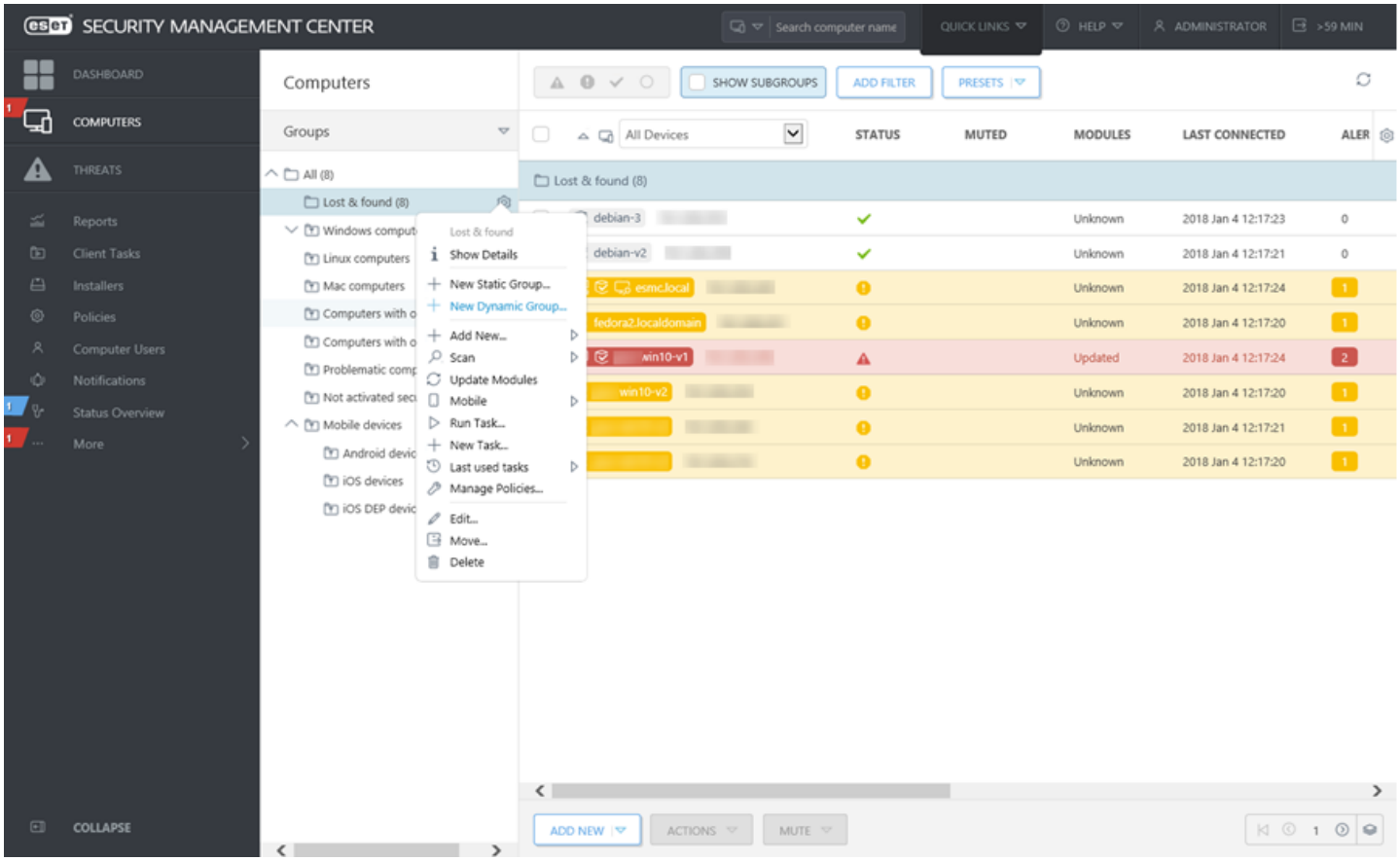
Správa dynamických skupín je dostupná prostredníctvom akcií so skupinami.

4.13.1.7.1 Vytvorenie novej dynamickej skupiny

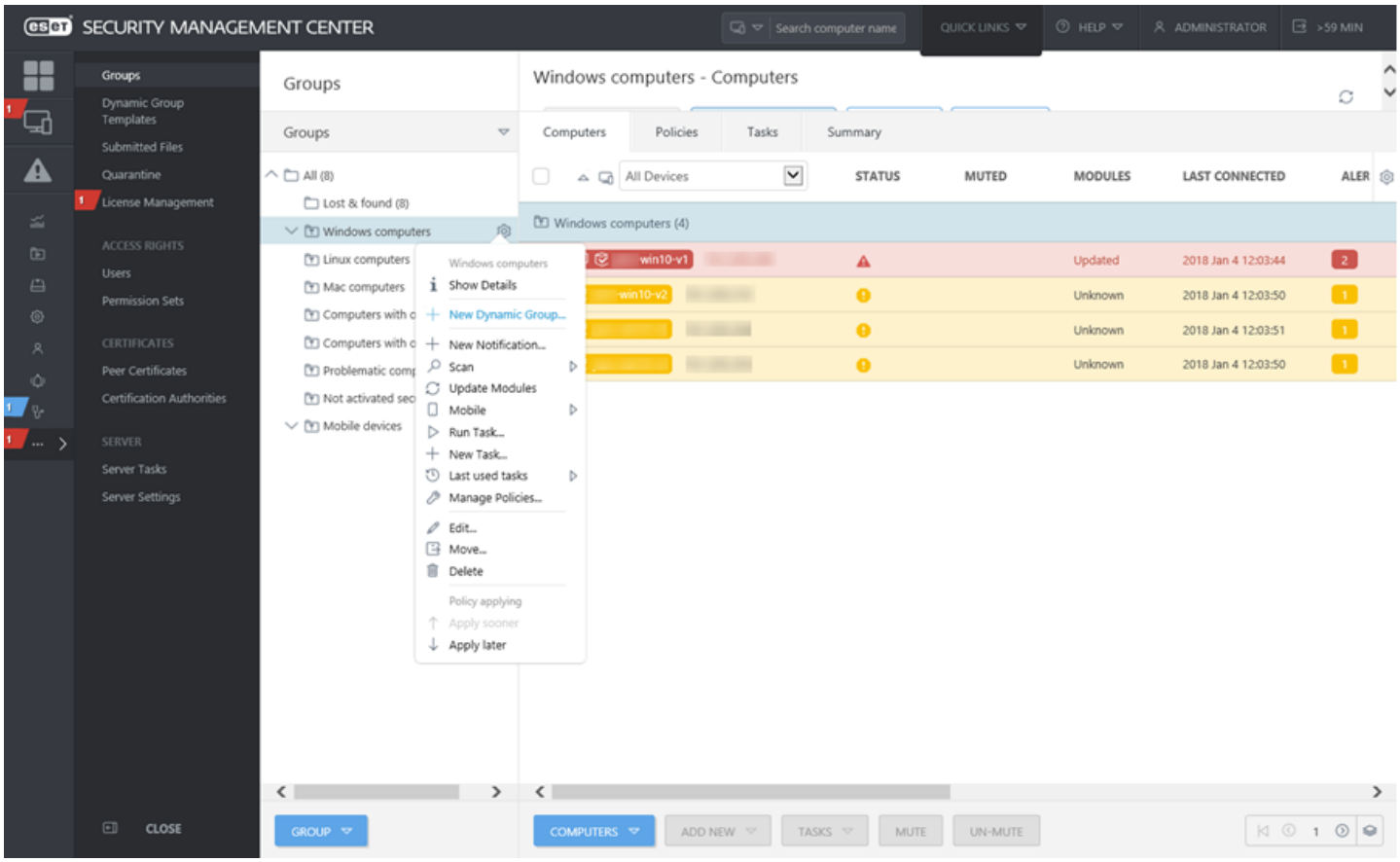
Dynamické skupiny sú usporiadané automaticky, na základe špecifických kritérií šablóny. Ak počítač nespĺňa podmienku skupiny, bude zo skupiny odstránený. Ak počítač spĺňa podmienku skupiny, bude pridaný do skupiny. Výber skupiny je automatický, na základe nastavení, výnimkou sú statické skupiny.

Sú dostupné tri možnosti vytvorenia dynamickej skupiny:

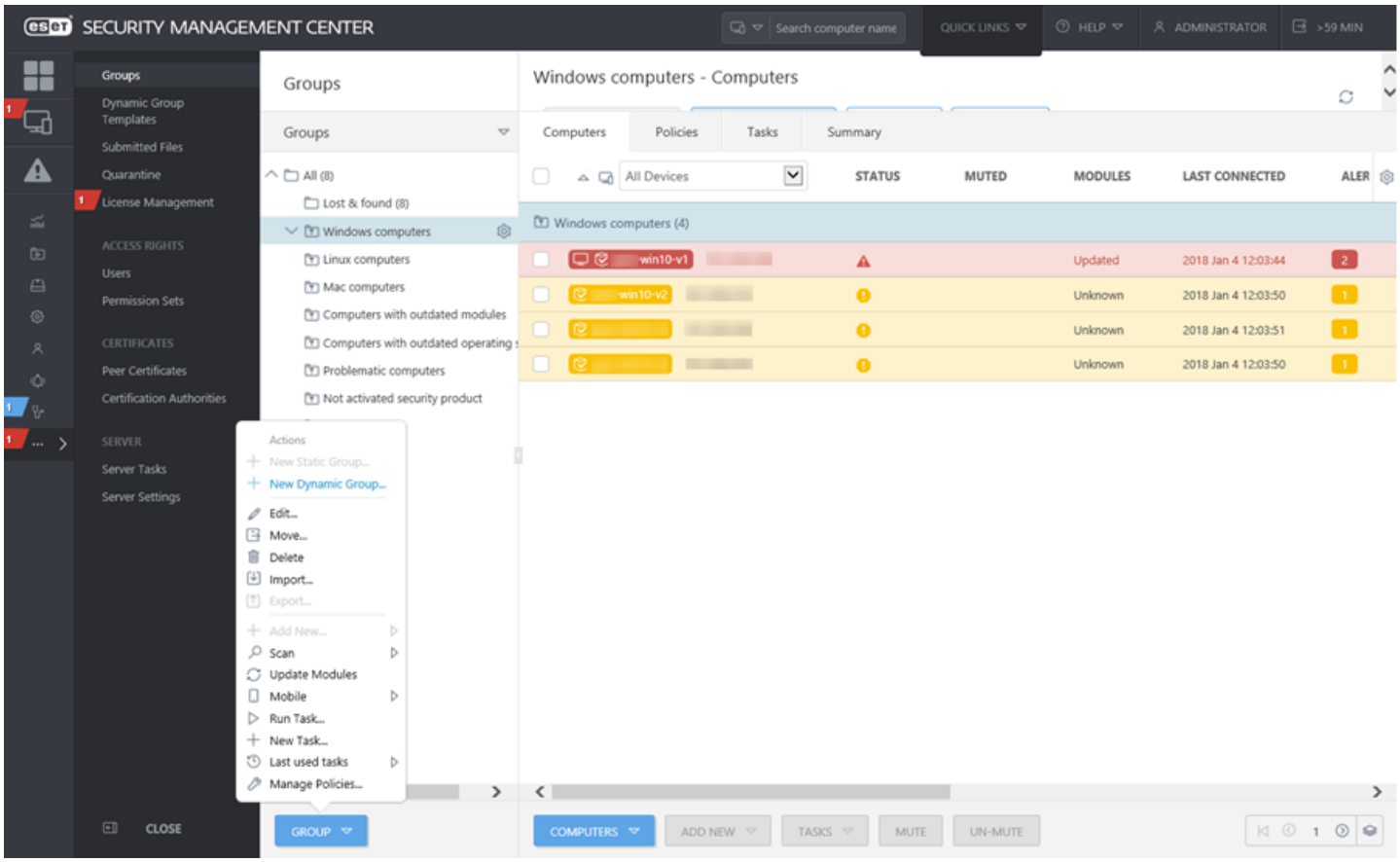
1. Kliknite na **Počítače** > **Skupiny** > ⚙ a vyberte možnosť **Nová dynamická skupina**.



2. Kliknite na **Viac** > **Skupiny** > ⚙ a vyberte možnosť **Nová dynamická skupina**.



3. Kliknite na **Viac** > **Skupiny** > následne na tlačidlo **Skupina** a vyberte možnosť **Nová dynamická skupina**.

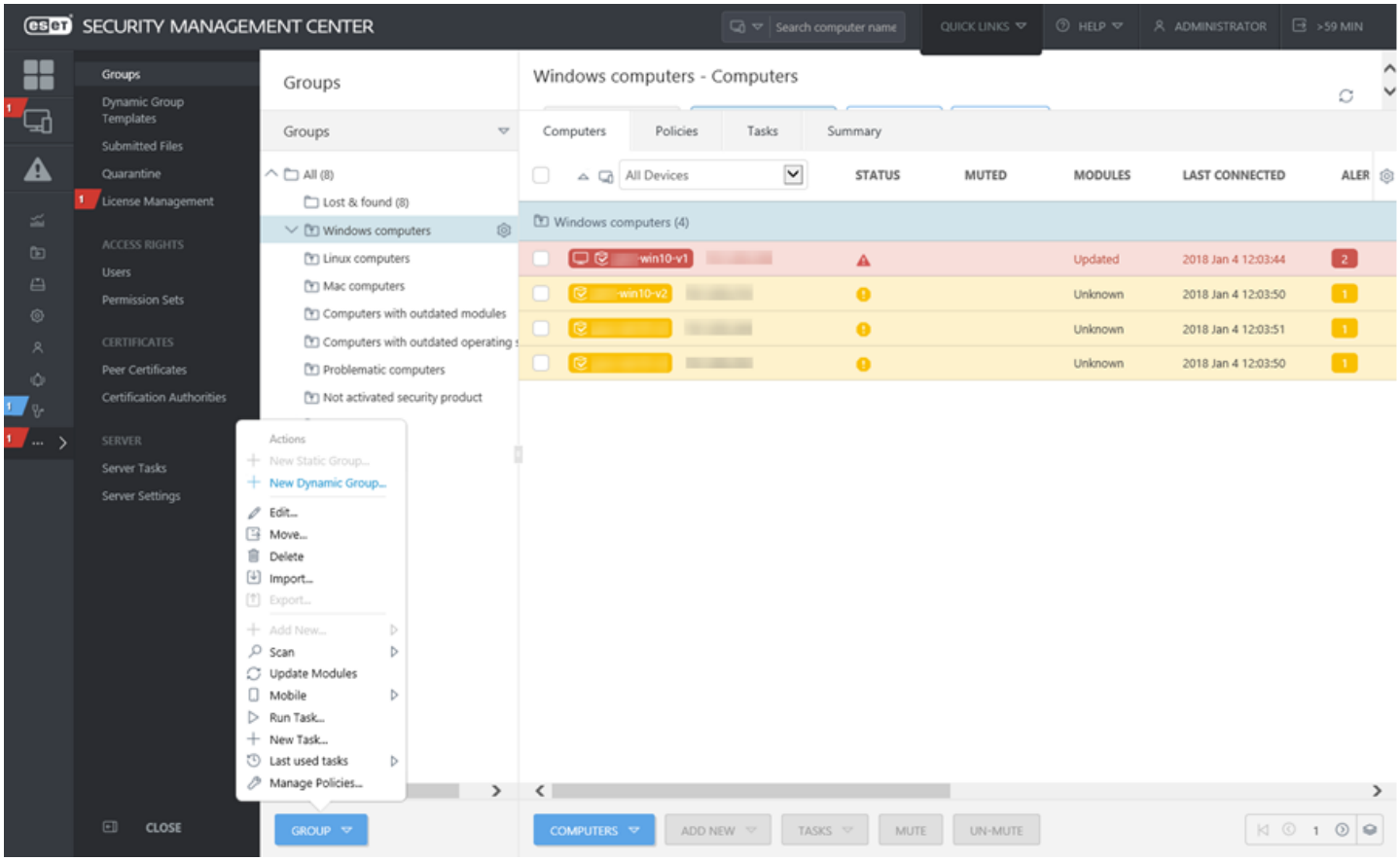


Zobrazí sa okno Sprievodca vytvorením dynamickej skupiny. Príklady vytvárania nových dynamických skupín na základe šablón s pravidlami nájdete v tejto kapitole.

Sekcia Šablóny dynamickej skupiny obsahuje prednastavené šablóny aj vlastné používateľské šablóny založené na rôznych kritériách. Všetky šablóny sú zobrazené v zozname. Po kliknutí na existujúcu šablónu ju môžete upravovať. Pre vytvorenie novej šablóny dynamickej skupiny kliknite na možnosť **Nová šablóna**.

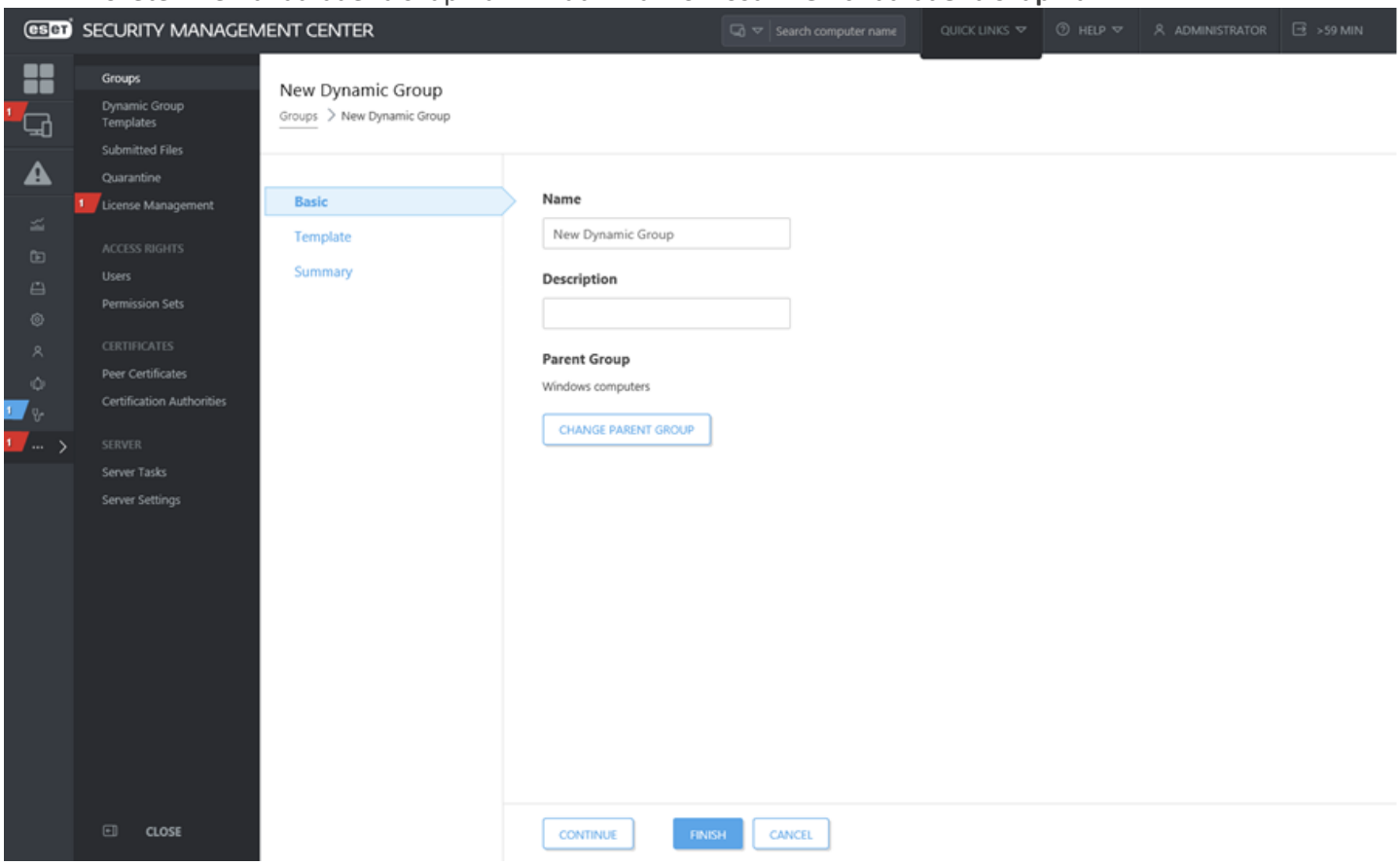
4.13.1.7.2 Sprievodca vytvorením novej dynamickej skupiny

Pre vytvorenie novej dynamickej skupiny kliknite na ikonu vedľa názvu dynamickej skupiny a následne kliknite na možnosť **Nová dynamická skupina**. Možnosť **Nová dynamická skupina** sa nachádza aj v časti **Viac** > **Skupiny**. Označte skupinu zo zoznamu skupín a kliknite na tlačidlo **Skupina** v dolnej časti okna. Následne pokračujte pomocou sprievodcu vytvorením dynamickej skupiny.



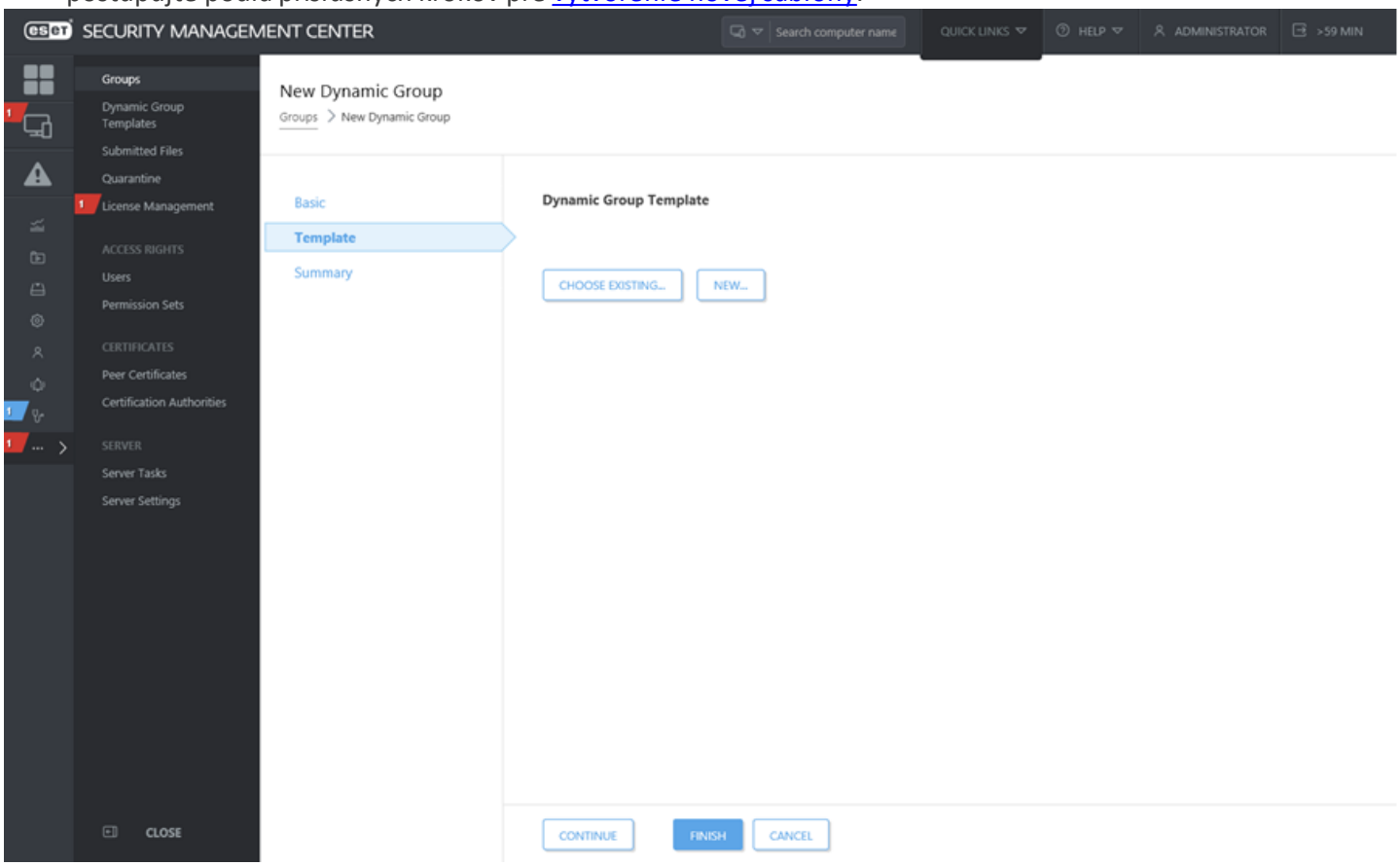
Sprievodca vytvorením novej dynamickej skupiny

1. Zadajte názov a popis pre novú šablónu.
2. Môžete zmeniť nadradenú skupinu kliknutím na možnosť **Zmeniť nadradenú skupinu**.



3. Kliknite na kartu **Šablóna**.

- Ak chcete vytvoriť dynamickú skupinu na základe predvolenej šablóny alebo šablóny, ktorú ste už vytvorili, kliknite na možnosť **Vybrať existujúcu** a zo zoznamu vyberte požadovanú šablónu.
- Ak ste ešte nevytvorili žiadnu šablónu a predvolené šablóny vám nevyhovujú, kliknite na možnosť **Nová** a postupujte podľa príslušných krokov pre vytvorenie novej šablóny.



Každá dynamická skupina je vytvorená zo šablóny, ktorá definuje, ako skupina filtruje klientske počítače. Z jednej šablóny môže byť vytvorený neobmedzený počet dynamických skupín.

Poznámka:
Šablóna je statický objekt uložený v statickej skupine. Na to, aby mali používatelia prístup k šablónam, musia mať pridelené príslušné povolenia. Na prácu so šablónami dynamických skupín potrebuje používateľ príslušné prístupové práva. Všetky prednastavené šablóny sú umiestnené v statickej skupine **Všetko** a sú štandardne dostupné len pre správcu. Ostatným používateľom musia byť pridelené dodatočné povolenia. V dôsledku toho sa môže stať, že používatelia nebudú vidieť predvolené šablóny. Šablóny je možné presunúť do skupiny, ku ktorej má konkrétny používateľ pridelené prístupové práva.

Duplikovanie šablóny je možné len v prípade, že používateľovi boli pridelené povolenia na zápis (v rámci kategórie povolení s názvom Šablóny dynamickej skupiny) pre skupinu, v ktorej je umiestnená pôvodná šablóna, a taktiež pre domácu skupinu daného používateľa (do ktorej bude umiestnená kópia pôvodnej šablóny). V nasledujúcom príklade nájdete návrh na zlepšenie.

4. Kliknite na kartu **Súhrn**. Nová skupina sa zobrazí pod nadradenou skupinou.

4.13.1.8 Šablóny dynamickej skupiny

Šablóny dynamickej skupiny stanovujú kritériá, ktoré musia počítače splniť, aby boli zaradené do konkrétnej dynamickej skupiny. Ak počítač tieto kritériá splní, bude automaticky presunutý do príslušnej dynamickej skupiny.

Poznámka:
Šablóna je statický objekt uložený v statickej skupine. Na to, aby mali používatelia prístup k šablónam, musia mať pridelené príslušné povolenia. Na prácu so šablónami dynamických skupín potrebuje používateľ príslušné prístupové práva. Všetky prednastavené šablóny sú umiestnené v statickej skupine **Všetko** a sú štandardne dostupné len pre správcu. Ostatným používateľom musia byť pridelené dodatočné povolenia. V dôsledku toho sa môže stať, že používatelia nebudú vidieť predvolené šablóny. Šablóny je možné presunúť do skupiny, ku ktorej má konkrétny používateľ pridelené prístupové práva.

Duplikovanie šablóny je možné len v prípade, že používateľovi boli pridelené povolenia na zápis (v rámci kategórie povolení s názvom Šablóny dynamickej skupiny) pre skupinu, v ktorej je umiestnená pôvodná šablóna, a taktiež pre domácu skupinu daného používateľa (do ktorej bude umiestnená kópia pôvodnej šablóny). V nasledujúcom príklade nájdete návrh na zlepšenie.

- Vytvorenie novej šablóny dynamickej skupiny
- Pravidlá pre šablónu dynamickej skupiny
- Šablóna dynamickej skupiny – príklady

Správa šablón dynamických skupín

Šablóny môžete spravovať v sekcii **Viac** > **Šablóny dynamických skupín**.

Nová šablóna	Kliknite na túto možnosť pre vytvorenie novej šablóny vo svojej domácej skupine.
Zobraziť podrobnosti	Zobrazenie súhrnu informácií o zvolenej šablóne.
Upraviť/Upraviť šablónu správy	Úprava zvolenej šablóny. Kliknite na **Uložiť ako**, ak chcete ponechať pôvodnú šablónu a vytvoriť novú podľa šablóny, ktorú práve upravujete. Pre vašu novú šablónu zadajte názov.
Duplikovať	Vytvorenie novej šablóny dynamickej skupiny na základe zvolenej šablóny. Pre takto vytvorenú novú šablónu je potrebné zadať nový (odlišný) názov. Duplicitná šablóna bude umiestnená vo vašej domácej skupine.
Vymazať	Trvalé odstránenie šablóny.
Prístupová skupina	Presunutie zvolenej šablóny do inej statickej skupiny. Toto je užitočné v prípade riešenia problémov týkajúcich sa prístupu ostatných používateľov.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené

predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.13.1.8.1 Nová šablóna dynamickej skupiny

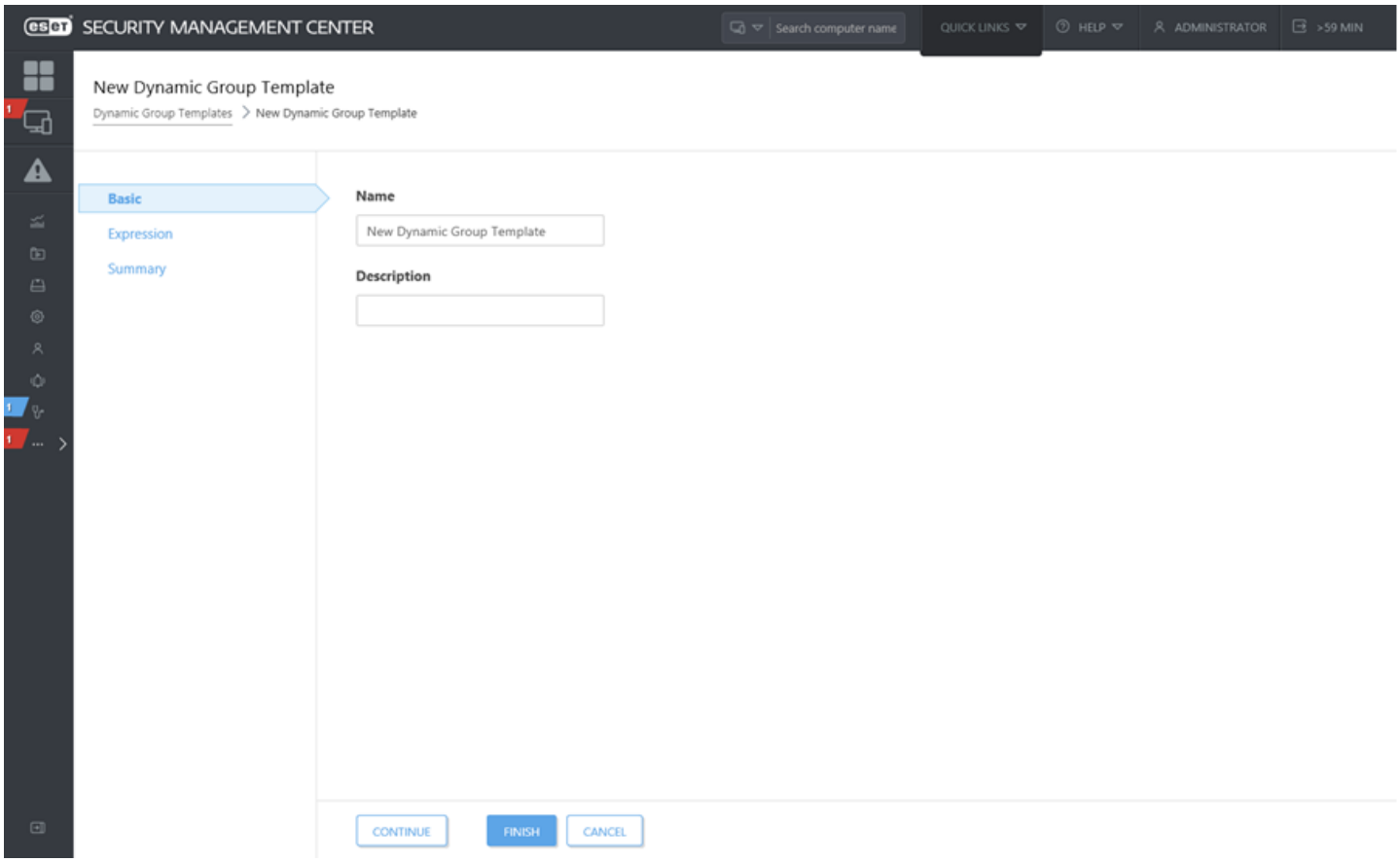
Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

Podrobnejšie inštrukcie o používaní dynamických skupín vo vašej sieti nájdete aj v našich príkladoch.



Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.9 Pravidlá pre šablónu dynamickej skupiny

Pri nastavovaní pravidiel pre šablónu dynamickej skupiny môžete použiť rôzne operátory pre rôzne podmienky, aby ste dosiahli želaný scenár.

Nasledujúce kapitoly popisujú pravidlá a logické operátory používané v šablónach dynamických skupín:

- Operácie
- Pravidlá a logické operátory
- Vyhodnocovanie pravidiel šablóny
- Automatizácia procesov v nástroji ESET Security Management Center
- Šablóny dynamickej skupiny
- Vytvorenie špecifickej šablóny dynamickej skupiny

4.13.1.9.1 Operácie

Ak nastavíte viaceré pravidlá (podmienky), musíte označiť, ktorý operátor bude kombinovať dané pravidlá. V závislosti od výsledku klientsky počítač bude alebo nebude pridaný do dynamickej skupiny, ktorá používa túto šablónu.

Poznámka:
Zvolená **Operácia** funguje nielen pri kombinovaní viacerých pravidiel, ale aj pri jedinom pravidle.

AND (Všetky podmienky musia byť splnené)	Splnené, ak sú všetky podmienky hodnotené pozitívne – počítač musí splniť všetky požadované parametre.
OR (Aspoň jedna podmienka musí byť splnená)	Splnené, ak je aspoň jedna z podmienok hodnotená pozitívne – počítač musí splniť aspoň jeden z požadovaných parametrov.
NAND (Aspoň jedna podmienka nesmie byť splnená)	Splnené, ak aspoň jedna z podmienok nie je hodnotená pozitívne – počítač nespĺňa aspoň jeden požadovaný parameter.
NOR (Žiadna podmienka nesmie byť splnená)	Splnené, ak žiadne podmienky nie sú hodnotené pozitívne – počítač nespĺňa žiadny z požadovaných parametrov.

Poznámka:
Operátory nie je možné kombinovať. Pre šablónu dynamickej skupiny možno použiť iba jeden operátor, ktorý sa vzťahuje na všetky jej podmienky.

4.13.1.9.2 Pravidlá a logické operátory

Pravidlo pozostáva z položky, logického operátora a hodnoty.

Po kliknutí na **+ Pridať pravidlo** sa zobrazí nové okno so zoznamom položiek rozdelených do kategórií. Napríklad:

Inštalovaný softvér > **Názov aplikácie**
Sieťové adaptéry > **MAC adresa**
Edícia OS > **Názov OS**

Ak chcete vytvoriť pravidlo, vyberte položku, logický operátor a zadajte hodnotu. Pravidlo sa vyhodnotí podľa zadanej hodnoty a použitého operátora.

Hodnoty zadávané do šablóny môžu mať podobu čísiel, reťazcov, enumerácií, IP adries, masiek produktov a ID počítačov. Ku každému typu hodnoty sú priradené rôzne logické operátory a ESMC Web Console automaticky zobrazí len tie, ktoré sú podporované.

- **„= (rovná sa)“** – hodnota zvolenej položky sa musí zhodovať s hodnotou zadanou v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„> (väčšie ako)“** – hodnota zvolenej položky musí byť väčšia ako hodnota zadaná v šablóne. Tento operátor môžete použiť aj pri definovaní rozsahu IP adries.
- **„≥ (rovné alebo väčšie ako)“** – hodnota zvolenej položky musí byť väčšia alebo rovná hodnote zadanej v šablóne. Tento operátor môžete použiť aj pri definovaní rozsahu IP adries.
- **„< (menšie ako)“** – hodnota zvolenej položky musí byť menšia ako hodnota zadaná v šablóne. Tento operátor môžete použiť aj pri definovaní rozsahu IP adries.
- **„≤ (rovné alebo menšie ako)“** – hodnota zvolenej položky musí byť menšia alebo rovná hodnote zadanej v šablóne. Tento operátor môžete použiť aj pri definovaní rozsahu IP adries.
- **„obsahuje“** – hodnota zvolenej položky obsahuje hodnotu zadanú v šablóne. V prípade reťazcov sa bude vyhľadávať podreťazec. Pri vyhľadávaní sa nerozlišujú malé a veľké písmená.
- **„má predponu“** – hodnota zvolenej položky má rovnakú textovú predponu ako uvádzaná hodnota v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená. Zadajte prvé znaky vyhľadávaného reťazca. Napríklad pre reťazec „Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319“ bude predpona „Micros“, „Micr“, prípadne „Microsof“ atď.
- **„má príponu“** – hodnota zvolenej položky má rovnakú textovú príponu ako uvádzaná hodnota v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená. Zadajte prvé znaky vyhľadávaného reťazca, napríklad pre reťazec „Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319“ bude prípona „M´319“ alebo „0.30319“ atď.
- **„má masku“** – hodnota zvolenej položky sa musí zhodovať s maskou zadanou v šablóne. Formátovanie masky umožňuje použiť všetky znaky a špeciálne symboly, napríklad „*“ pre nahradenie žiadneho, jedného alebo viacerých znakov a „?“ pre nahradenie presne jedného znaku, napr.: „6.2.*“ alebo „6.2.2033.?“.
- **„regex“** – hodnota zvolenej položky sa musí zhodovať s regulárnym výrazom (regex) zadaným v šablóne. Regulárny výraz musí byť zadaný vo formáte **Perl**.

Poznámka:
Regulárny výraz, *regex* alebo *regexp*, je postupnosť znakov, ktoré definujú určitý vyhľadávací vzor. Napríklad, *gray|grey* a *gr(a|e)y* sú ekvivalentné vyhľadávacie vzory, ktoré vyhľadajú tieto 2 slová: „*gray*“ a „*grey*“.

- **„je jedným z“** – hodnota zvolenej položky sa musí zhodovať s akoukoľvek hodnotou zo zoznamu v šablóne. Pre pridanie ďalších položiek kliknite na **+ Pridať**. Každý riadok v novej položke v zozname. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„je jedným z (maska reťazca)“** – hodnota zvolenej položky sa musí zhodovať s akoukoľvek maskou zo zoznamu v šablóne.
- **„má hodnotu“**

Negatívne operátory:

Dôležité:
Negatívne operátory používajte opatrne, pretože v prípade protokolov, ktoré obsahujú viacero riadkov, ako napríklad „Nainštalované aplikácie“, sú voči podmienkam pravidla testované všetky riadky. Pre pochopenie princípu negatívnych operátorov alebo negatívnych operácií si pozrite vzorové príklady (Vyhodnocovanie pravidiel šablóny a Šablóna dynamickej skupiny – príklady).

- **„≠ (nerovná sa)“** – hodnota zvolenej položky sa nesmie zhodovať s hodnotou zadanou v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„neobsahuje“** – hodnota zvolenej položky neobsahuje hodnotu zadanú v šablóne. Pri vyhľadávaní sa nerozlišujú malé a veľké písmená.
- **„nemá predponu“** – hodnota zvolenej položky nemá rovnakú textovú predponu ako uvádzaná hodnota v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„nemá príponu“** – hodnota zvolenej položky nemá rovnakú textovú príponu ako uvádzaná hodnota v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„nemá masku“** – hodnota zvolenej položky sa nesmie zhodovať s maskou zadanou v šablóne.
- **„nie je regex“** – hodnota zvolenej položky sa nesmie zhodovať s regulárnym výrazom zadaným v šablóne. Regulárny výraz musí byť zadaný vo formáte **Perl**. Negatívna operácia je poskytnutá ako pomocník pri negovaní zhodných regulárnych výrazov bez prepísania.
- **„nie je jedným z“** – hodnota zvolenej položky sa nesmie rovnať ani jednej hodnote zo zoznamu v šablóne. Pri porovnávaní reťazcov sa nerozlišujú malé a veľké písmená.
- **„nie je jedným z (maska reťazca)“** – hodnota zvolenej položky sa nemôže zhodovať s akoukoľvek maskou zo zoznamu v šablóne.
- **„nemá žiadnu hodnotu“**

PRÍKLAD:
Je potrebné rozlišovať medzi testom existencie (niečo s určitou hodnotou neexistuje vôbec) a testom rozdielu (niečo existuje, ale má inú hodnotu). Nižšie sú uvedené niektoré základné pravidlá, ktoré slúžia vytvorenie tohto rozdielu:

- Pre overenie existencie: Operácia bez negácie (**AND**, **OR**) a operátor bez negácie (**=**, **>**, **<**, **obsahuje**...).
- Pre overenie existencie odlišnej hodnoty: Operácia **AND** a operátory obsahujúce aspoň 1 negáciu (**=**, **>**, **<**, **obsahuje**, **neobsahuje**...).
- Pre overenie neexistencie hodnoty: Operácie s negáciou (**NAND**, **NOR**) a operátory bez negácie (**=**, **>**, **<**, **obsahuje**...).

4.13.1.9.3 Vyhodnocovanie pravidiel šablóny

Vyhodnocovanie pravidiel šablóny je riadené ESET Management Agentom, nie ESMC Serverom (na ESMC Server je odoslaný len výsledok). Proces vyhodnocovania je podmienený pravidlami, ktoré sú nakonfigurované v šablóne. Nižšie je uvedených niekoľko príkladov procesu vyhodnocovania pravidiel šablóny.

Stav počítača je klaster rôznych informácií. Niektoré zdroje poskytujú len jednorozmerný stav (napríklad operačný systém, veľkosť RAM atď.), iné zdroje aj viacrozmerné informácie o stave (napríklad IP adresu, inštalované aplikácie atď.).

Nižšie nájdete vizuálne znázornenie dát získaných z klienta:

Sieťové adaptéry – IP adresa	Sieťové adaptéry – MAC adresa	Názov OS	Verzia OS	HW – veľkosť RAM v MB	Inštalované aplikácie
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Stav počítača sa skladá z niekoľkých skupín. Skupina dát vždy ponúka súvislé informácie usporiadané do riadkov. Počet riadkov v skupine sa môže líšiť.

Podmienky sú vyhodnocované podľa skupiny a podľa riadka – ak je zadaných viac podmienok pre skupinu, sú posudzované len hodnoty v rovnakom riadku.

Príklad č. 1:

V tomto príklade berieme do úvahy nasledujúce podmienky:

```
Sieťové adaptéry.IP adresa = 10.1.1.11 AND Sieťové adaptéry.MAC adresa = 4A-64-3F
```

Toto pravidlo nevyhovuje pre žiadny počítač, pretože neexistuje riadok, v ktorom by boli obe hodnoty pravdivé.

Sieťové adaptéry – IP adresa	Sieťové adaptéry – MAC adresa	Názov OS	Verzia OS	HW – veľkosť RAM v MB	Inštalované aplikácie
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Príklad č. 2:

V tomto príklade berieme do úvahy nasledujúce podmienky:

```
Sieťové adaptéry.IP adresa = 192.168.1.2 AND Sieťové adaptéry.MAC adresa = 4A-64-
```

Tentokrát pravidlo vyhovuje pre obe podmienky v rovnakom riadku, a preto je pravidlo ako celok vyhodnotené ako pravdivé. Počítač je označený.

Sieťové adaptéry – IP adresa	Sieťové adaptéry – MAC adresa	Názov OS	Verzia OS	HW – veľkosť RAM v MB	Inštalované aplikácie
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

Príklad č. 3:

Pre podmienky s operátorom OR platí (aspoň jedna podmienka musí byť pravdivá) napríklad:

```
Sieťové adaptéry.IP adresa = 10.1.1.11 OR Sieťové adaptéry.MAC adresa = 4A-64-3F-
```

Pravidlo je pravdivé pre oba riadky, keďže je potrebné splniť len jednu z podmienok. Počítač je označený.

Sieťové adaptéry – IP adresa	Sieťové adaptéry – MAC adresa	Názov OS	Verzia OS	HW – veľkosť RAM v MB	Inštalované aplikácie
192.168.1.2	4A-64-3F-10-FC-75	Windows 7 Enterprise	6.1.7601	2048	ESET Endpoint Security
10.1.1.11	2B-E8-73-BE-81-C7				PDF Reader
124.256.25.25	52-FB-E5-74-35-73				Office Suite
					Weather Forecast

4.13.1.10 Šablóna dynamickej skupiny – príklady

V tejto kapitole nájdete príklady šablón dynamických skupín, ktoré môžete použiť na správu vašej siete.

- Dynamická skupina detegujúca, či je nainštalovaný bezpečnostný produkt
- Dynamická skupina detegujúca, či je nainštalovaná konkrétna verzia softvéru
- Dynamická skupina detegujúca chýbajúcu inštaláciu konkrétnej verzie softvéru
- Dynamická skupina detegujúca chýbajúcu inštaláciu konkrétnej verzie softvéru a zároveň prítomnosť inej verzie daného softvéru
- Dynamická skupina detegujúca, či sa počítač nachádza v konkrétnej podsieti
- Dynamická skupina detegujúca nainštalovaný, ale neaktivovaný bezpečnostný produkt určený pre server
- Dynamická skupina detegujúca počítače, na ktorých je nainštalovaný ESET Management Agent bez bezpečnostného produktu ESET (článok databázy znalostí)

Pomocou šablón dynamických skupín môžete kombinovať mnoho pravidiel na rôzne účely. Možnosti sú prakticky nekonečné. Napríklad, môžete použiť podrobnosti hardvérového inventára na vytvorenie pravidiel pre dynamickú skupinu, ktorá bude obsahovať zariadenia spĺňajúce zadané hardvérové kritéria.

4.13.1.10.1 Dynamická skupina – bezpečnostný produkt je nainštalovaný

Táto dynamická skupina sa používa na spustenie úlohy okamžite po inštalácii bezpečnostného produktu spoločnosti ESET na počítač (napr. na spustenie aktivácie, manuálnej kontroly atď.).

Môžete vytvoriť **Novú šablónu** v sekcii **Viac** > **Šablóny dynamickej skupiny** a vytvoriť novú dynamickú skupinu so šablónou alebo vytvoriť novú dynamickú skupinu pomocou už existujúcej alebo novej šablóny.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **AND** (všetky podmienky musia byť splnené).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku. Vyberte možnosť **Počítač** > **Maska spravovaných produktov** > **je jedným z** > **Chránené ESET produktom: Pracovná plocha**. Môžete si vybrať z rôznych produktov spoločnosti ESET.

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.10.2 Dynamická skupina – je nainštalovaná špecifická verzia softvéru

Táto dynamická skupina môže byť použitá na detegovanie nainštalovaného bezpečnostného produktu spoločnosti ESET na počítači. Po detekcii môžete na danom počítači spustiť napríklad aktualizáciu alebo vlastný príkaz. Môžete použiť rôzne operátory, napríklad **„obsahuje“** alebo **„má predponu“**.

Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **AND** (všetky podmienky musia byť splnené).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku:
   - **Nainštalovaný softvér** > **Názov aplikácie** > **= (rovná sa)** > *ESET Endpoint Security*
   - **Nainštalovaný softvér** > **Verzia aplikácie** > **= (rovná sa)** > *6.2.2033.0*

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.10.3 Dynamická skupina – špecifická verzia softvéru nie je nainštalovaná

Táto dynamická skupina môže byť použitá na detegovanie chýbajúcej inštalácie bezpečnostného produktu spoločnosti ESET na počítači. Nastavenia v tomto príklade budú zahŕňať počítače, na ktorých daný softvér nie je nainštalovaný vôbec alebo je nainštalovaná iná verzia softvéru ako tá, ktorá je špecifikovaná.

Táto skupina je užitočná napríklad v tom, že po detekcii môžete na danom počítači spustiť napríklad aktualizáciu alebo inštaláciu softvéru. Môžete použiť rôzne operátory, napríklad **„obsahuje“** alebo **„má predponu“**.

Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **NAND** (aspoň jedna podmienka nesmie byť splnená).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku:
   - **Nainštalovaný softvér** > **Názov aplikácie** > **= (rovná sa)** > *ESET Endpoint Security*
   - **Nainštalovaný softvér** > **Verzia aplikácie** > **= (rovná sa)** > *6.2.2033.0*

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.10.4 Dynamická skupina – špecifická verzia softvéru nie je nainštalovaná, ale je nainštalovaná iná verzia

Táto dynamická skupina môže byť použitá na detegovanie inštalácie softvéru v inej verzii, akú požadujete. Táto skupina je užitočná, pretože budete môcť vykonať aktualizáciu na tých počítačoch, na ktorých sa požadovaná verzia softvéru nenachádza. Môžete použiť rôzne operátory, uistite sa však, že pri testovaní verzie softvéru je použitý negatívny operátor.

Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **AND** (všetky podmienky musia byť splnené).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku:
   - **Nainštalovaný softvér** > **Názov aplikácie** > **= (rovná sa)** > *ESET Endpoint Security*
   - **Nainštalovaný softvér** > **Verzia aplikácie** > **≠ (nerovná sa)** > *„6.2.2033.0“*

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.10.5 Dynamická skupina – počítač sa nachádza v špecifickej podsieti

Táto dynamická skupina môže byť použitá na detegovanie konkrétnej podsiete. Následne môže byť použitá na aplikovanie vlastnej politiky na kontrolu webu alebo aktualizácie. Môžete zadať rôzne rozsahy.

Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **AND** (všetky podmienky musia byť splnené).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku:
   - **IP adresy siete** > **IP adresa adaptéra** > **≥ (väčšie alebo rovné)** > *„10.1.100.1“*
   - **IP adresy siete** > **IP adresa adaptéra** > **≤ (menšie alebo rovné)** > *„10.1.100.254“*
   - **IP adresy siete** > **IP adresa adaptéra** > **= (rovná sa)** > *„255.255.255.0“*

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.10.6 Dynamická skupina – nainštalovaný ale neaktivovaný bezpečnostný produkt určený pre server

Táto dynamická skupina môže byť použitá na detegovanie neaktivovaného bezpečnostného produktu určeného pre server. Po detegovaní takýchto produktov môžete priradiť k tejto skupine úlohu pre klienta na aktiváciu klientskych počítačov pomocou platnej licencie. V tomto príklade je špecifikovaný len produkt ESET Mail Security pre Microsoft Exchange Server, avšak môžete špecifikovať aj viacero produktov.

Kliknite na možnosť **Nová šablóna** v sekcii **Viac** > **Šablóny dynamických skupín**.

Základné

Zadajte **Názov** a **Popis** pre novú šablónu dynamickej skupiny.

Výraz

1. Vyberte logický operátor z menu Operácia: **AND** (všetky podmienky musia byť splnené).
2. Kliknite na **+ Pridať pravidlo** a vyberte podmienku:
   - **Počítač** > **Maska spravovaných produktov** > **je jedným z** > **Chránené ESET produktom: Poštový server**
   - **Problémy s funkciou/ochranou** > **Zdroj** > **= (rovná sa)** > **Bezpečnostný produkt**
   - **Problémy s funkciou/ochranou** > **Problém** > **= (rovná sa)** > **Produkt nie je aktivovaný**

Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie novej šablóny. Vytvorená šablóna teraz bude pridaná do zoznamu všetkých šablón a neskôr môže byť použitá pri vytváraní novej dynamickej skupiny.

4.13.1.11 Automatizácia procesov v nástroji ESET Security Management Center

Podobne ako v príklade uvedenom nižšie môžete automatizovať rôzne procesy v ESMC, napr. aktualizáciu operačného systému a produktu, spúšťanie kontroly, aktiváciu nových produktov s vopred vybranou licenciou či dokonca riešenie komplexných bezpečnostných incidentov.

Upozornenie:
Kroky uvedené v tomto príklade by sa mali vykonávať len na klientskych zariadeniach, ktoré nemajú nainštalovaný bezpečnostný softvér od iného výrobcu a ani bezpečnostný produkt od spoločnosti ESET určený pre domácnosti (napr. ESET Smart Security). Neodporúčame inštalovať produkty ESET na klientske zariadenia s nainštalovaným bezpečnostným softvérom tretej strany. Na odstránenie iných antivírusových programov nainštalovaných na vašom počítači môžete použiť nástroj ESET AV Remover.

PRÍKLAD: AKO AUTOMATICKY NAINŠTALOVAŤ PRODUKTY SPOLOČNOSTI ESET NA NOVOPRIPOJENÉ POČÍTAČE S OPERAČNÝM SYSTÉMOM WINDOWS

1. Vytvorte dynamickú skupinu nazvanú *Bez bezpečnostného produktu*.
   a. Priraďte ju ako podradenú skupinu prednastavenej skupiny **Windows počítače > Windows (počítače)**.
   b. Kliknite na **Nová šablóna**.
   c. Pridajte nasledujúce pravidlo: **Počítač** > **Maska spravovaných produktov**.
   d. Ako logický operátor zvoľte **nerovná sa**.
   e. Vyberte masku **Chránené ESET produktom: Počítač**
   f. Novovytvorenú skupinu uložte kliknutím na **Dokončiť**.
2. Prejdite do sekcie **Úlohy pre klienta** > **ESET bezpečnostný produkt** > **Inštalácia softvéru**.
   a. Kliknite na možnosť **Nová** a zadajte pre úlohu **Názov**.
   b. V sekcii **Nastavenia** vyberte balík inštalátora a v prípade potreby nastavte ďalšie parametre.
   c. Kliknite na **Dokončiť** > **Vytvoriť spúšťač**.
   d. V sekcii **Cieľ** kliknite na **Pridať skupiny** a zvoľte dynamickú skupinu *Bez bezpečnostného produktu*.
   e. V sekcii **Spúšťač** vyberte **Spúšťač pri vstupe do dynamickej skupiny**.
   f. Kliknutím na **Dokončiť** uložte vytvorenú úlohu a spúšťač.

Táto úloha bude spúšťaná na klientskych počítačoch, ktoré sa od momentu vytvorenia úlohy pridajú do zvolenej dynamickej skupiny. Na klientoch, ktorí boli súčasťou zvolenej dynamickej skupiny už pred vytvorením tejto úlohy, bude potrebné úlohu spustiť manuálne.

PRÍKLAD: AKO VYNÚTIŤ POLITIKU LEN NA URČITÚ ČASŤ SIETE (PODSIEŤ)

1. Vytvorte dynamickú skupinu nazvanú *Podsieť 120*.

a. Priraďte ju ako podradenú skupinu prednastavenej skupiny **Všetko**.
b. Kliknite na **Nová šablóna**.
c. Pridajte pravidlo: **IP adresy siete** > **IP podsieť**.
d. Ako logický operátor zvoľte **rovná sa**.
e. Zadajte podsieť, ktorú chcete filtrovať, napr. 10.1.120.0 (posledná číslica musí byť 0, aby boli vyfiltrované všetky IP adresy z podsiete 10.1.120.).
f. Novovytvorenú skupinu uložte kliknutím na **Dokončiť**.

2. Prejdite do sekcie **Politiky**.

a. Kliknite na **Nová politika** a zadajte pre politiku **Názov**.
b. V sekcii **Nastavenia** vyberte možnosť **ESET Management Agent**.
c. Zmeňte nastavenia, ktoré chcete politikou upraviť. Môžete napríklad zmeniť **Interval pripojenia** na 5 minút.
d. V sekcii **Priradiť** kliknite na tlačidlo **Priradiť** a označte začiarkavacie políčko vedľa skupiny *Podsieť 120*. Následne výber potvrďte kliknutím na tlačidlo **OK**.
e. Politiku uložte kliknutím na **Dokončiť**.

Táto politika bude aplikovaná na klientske počítače, ktoré sa od momentu vytvorenia tejto politiky pridajú do zvolenej dynamickej skupiny.

Upozornenie:
Keď klientske zariadenie opustí dynamickú skupinu (t. j. zariadenie už viac nespĺňa podmienky, na základe ktorých bolo zaradené do danej dynamickej skupiny), nastavenia zostanú upravené podľa poslednej použitej politiky, až pokým nebudú tieto konkrétne nastavenia zmenené inou politikou aplikovanou na klientske zariadenie.

4.13.2 Odoslané súbory

ESET Dynamic Threat Defense je služba, ktorá poskytuje pokročilú ochranu pred doposiaľ neobjavenými hrozbami. Používateľ môže odoslať súbory na analýzu malvéru v cloudovom prostredí a následne získať správu o aktivite odoslanej vzorky. Podrobné inštrukcie nájdete v používateľskej príručke pre ESET Dynamic Threat Defense. Súbor môžete odoslať vzdialene priamo z nástroja ESMC Web Console v sekcii **Hrozby** > **Zobraziť podrobnosti** > **Odoslať súbor do EDTD**.

V okne **Odoslané súbory** si môžete tiež prezrieť zoznam všetkých súborov odoslaných na servery spoločnosti ESET.

Okno Odoslané súbory

V tomto okne si môžete prezrieť zoznam odoslaných súborov a ich podrobnosti, napr. môžete nájsť používateľa, ktorý odoslal súbor, ako aj dátum odoslania súboru. Kliknite na odoslaný súbor a z roletového menu vyberte konkrétnu akciu.

Zobraziť podrobnosti	Kliknutím na túto možnosť zobrazíte kartu **naposledy odoslaných** vzoriek.
Zobraziť aktivitu	Kliknutím na túto možnosť zobrazíte správu o analýze aktivity pre danú vzorku.
Pridať vylúčenie do politiky	Označte jeden alebo viacero súborov a kliknite na **Pridať vylúčenie do politiky** pre pridanie vylúčenia z detekcie pre označené súbory do existujúcej politiky. V kontextovom okne vyberte jednu politiku a kliknite na **Pridať**.

Okno Detaily súborov

V tomto okne nájdete podrobnosti o vybranom súbore. Ak bol súbor odoslaný viackrát, budú zobrazené podrobnosti z posledného odoslania.

Stav	Výsledky analýzy malvéru. **Neznámy** – súbor zatiaľ nebol analyzovaný. **Neškodný** – žiadne z detekčných jadier nevyhodnotilo analyzovaný súbor ako škodlivý. **Podozrivý**, **Veľmi podozrivý** – analyzovaný súbor bol na základe zachytenej aktivity vyhodnotený ako podozrivý, avšak nemusí ísť nevyhnutne o malvér. **Škodlivý** – analyzovaný súbor bol na základe zachytenej aktivity vyhodnotený ako škodlivý.
Stav	Stav analýzy. Stav **Prebieha opätovná analýza** znamená, že výsledok prvotnej analýzy je už k dispozícii, avšak môže sa ešte zmeniť po vykonaní dodatočnej analýzy.
Naposledy spracované v	Súbor môže byť odoslaný na analýzu viackrát z viacerých počítačov. Toto je čas poslednej vykonanej analýzy.
Odoslané v	Čas odoslania súboru.
Aktivita	Pre zobrazenie analýzy vykonanej systémom ESET Dynamic Threat Defense kliknite na **Zobraziť aktivitu**. Táto funkcia je dostupná len v prípade, ak má počítač, ktorý odoslal súbor, platnú licenciu pre ESET Dynamic Threat Defense.
Počítač	Názov počítača, z ktorého bol súbor odoslaný.
Používateľ	Používateľ počítača, ktorý súbor odoslal.
Dôvod	Dôvod odoslania súboru.
Odoslané do	Časť ESET cloudu, ktorá prijala súbor. Nie každý odoslaný súbor je analyzovaný na prítomnosť malvéru.
Hash	SHA1 hash odoslaného súboru.
Veľkosť	Veľkosť odoslaného súboru.
Kategória	Kategória súboru.

Bližšie informácie súvisiace s ESET Dynamic Threat Defense správami o aktivite súborov nájdete v príslušnej dokumentácii.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

+ Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené

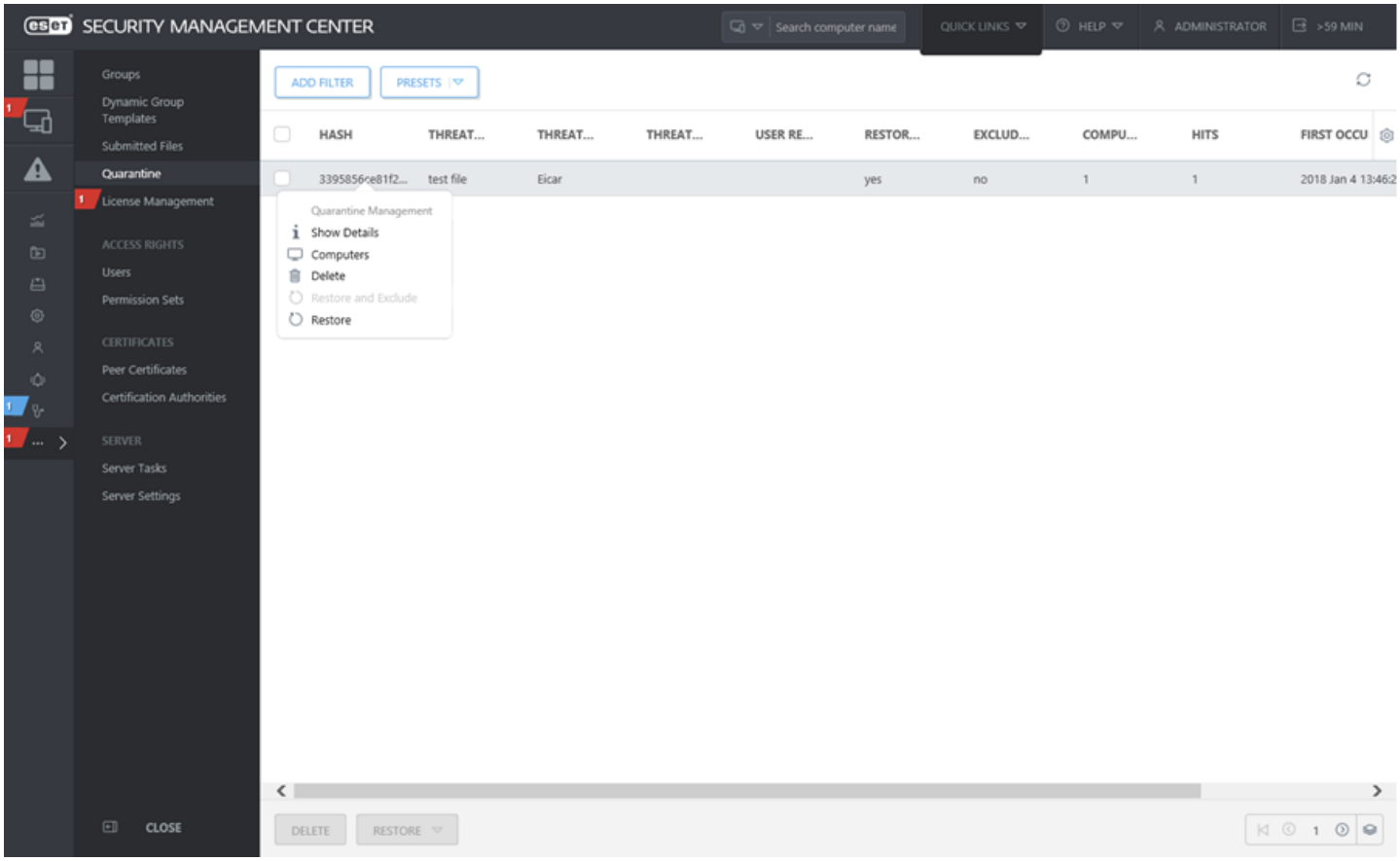
predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.13.3 Karanténa

V tejto sekcii sa zobrazujú všetky súbory, ktoré boli presunuté do karantény na klientskych zariadeniach. Vo väčšine prípadov ide o súbory, pre ktoré neexistuje liečenie, ktorých zmazanie nie je odporúčané alebo nie je bezpečné, prípadne pri ktorých došlo k nesprávnej detekcii antivírusovej ochrany produktu ESET.



Súbor presunutý do karantény môžete **Vymazať** alebo ho **Obnoviť** do pôvodného umiestnenia. Akciu **Obnoviť a vylúčiť** môžete použiť na to, aby ste daný súbor vylúčili z kontroly, a zabránili tak jeho opätovnému umiestneniu do karantény.

Na filtrovanie zoznamu súborov umiestnených v karanténe môžete použiť rôzne filtre.

Do sekcie **Karanténa** môžete prejsť dvoma spôsobmi:

1. **Viac** > **Karanténa**.
2. **Podrobnosti o počítači** > **Hrozby a karanténa** > karta **Karanténa**.

Keď kliknete na niektorú z položiek zobrazených v sekcii **Karanténa**, otvorí sa ponuka s názvom **Správa karantény**.

Zobraziť podrobnosti – zobrazí sa zdroj hrozby (zariadenie), názov a typ hrozby, názov objektu s úplnou cestou k súboru, hash, veľkosť atď.

Počítače – otvorí sa sekcia **Počítače** s vyfiltrovaným zoznamom zariadení, ktoré sa týkajú daného súboru v karanténe.

Vymazať – súbor bude odstránený z karantény a taktiež zo zariadenia.

Obnoviť – súbor bude obnovený späť do jeho pôvodného umiestnenia.

Obnoviť a vylúčiť – súbor bude obnovený späť do jeho pôvodného umiestnenia a bude vylúčený z kontroly.

Odovzdať – otvorí sa úloha pre klienta Odovzdať súbor v karanténe.

Dôležité:

Funkciu **Odovzdať** odporúčame používať len skúseným používateľom. Ak chcete súbor presunutý do karantény podrobnejšie preskúmať, môžete ho **Odovzdať** do zdieľaného adresára.

Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

+ Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.13.4 Správa licencií

Svoje licencie môžete jednoducho spravovať prostredníctvom nástroja ESET Security Management Center. Zakúpením licencie pre akýkoľvek produkt spoločnosti ESET určený pre firmy automaticky získate prístup k nástroju ESET Security Management Center.

Poznámka:
Bezpečnostný produkt ESET určený pre firmy môžete aktivovať pomocou nástroja ESET Security Management Center. Toto sa vzťahuje aj na staršie verzie.

Ak už máte prihlasovacie meno a heslo, ktoré vám boli vydané spoločnosťou ESET, môžete ich konvertovať na licenčný kľúč. Viac informácií nájdete v časti Konvertovanie licenčných prihlasovacích údajov na licenčný kľúč. Prihlasovacie meno a heslo boli nahradené **Licenčným kľúčom/Verejným ID licencie**.

- **Licenčný kľúč** je jedinečný reťazec znakov, ktorý je používaný na identifikáciu vlastníka licencie a samotnú aktiváciu produktu.
- **Verejné ID** je krátky reťazec znakov, ktorým sa identifikuje tretia strana využívajúca licenciu (napr. **bezpečnostný správca** zodpovedný za správu jednotiek).
- **Bezpečnostný správca** je osoba, ktorá spravuje licencie a nemusí to byť samotný **vlastník licencie**. Vlastník licencie môže poveriť bezpečnostného správcu správou licencií. Ak bezpečnostný správca toto poverenie prijme, obdrží oprávnenia na správu licencií. Vlastníkom licencie odporúčame vytvoriť si vlastný účet bezpečnostného správcu.

Licencie môžu byť spravované online v tejto časti kliknutím na **Otvoriť > Business Account** (ESET Business Account), prípadne použitím webového rozhrania nástroja ESET Business Account.

Povolenia na prístup k správe licencií

Každému používateľovi je možné prideliť povolenie na prístup k licenciám. Povolenia sú platné len pre licencie, ktoré sú zahrnuté v statickej skupine, ku ktorej je daná sada povolení priradená. Každý typ povolení umožňuje používateľovi vykonávať iné akcie.

Dôležité:
Pridávať a odstraňovať licencie môžu len správcovia, ktorých domácou skupinou je skupina **Všetko** a ktorí majú pridelené povolenia na **zápis** pre licencie (umiestnené v skupine Všetko). Každá licencia je identifikovaná **Verejným ID** a môže obsahovať jednu alebo viacero jednotiek. Licencie môže ostatným používateľom (tým, ktorí majú dostatočné povolenia) distribuovať len správca. Licenciu nie je možné rozdeliť.

Práca vo Web Console

Sekcia **Správa Licencií** je v nástroji ESET Security Management Center dostupná z hlavného menu v časti **Viac** > **Správa licencií**.

Licencie sú identifikovateľné podľa **verejného identifikačného čísla**. V portáli ESET Business Account a nástroji ESMC je každá licencia identifikovaná podľa **Verejného ID licencie**, **Typu licencie** a **Označení**:

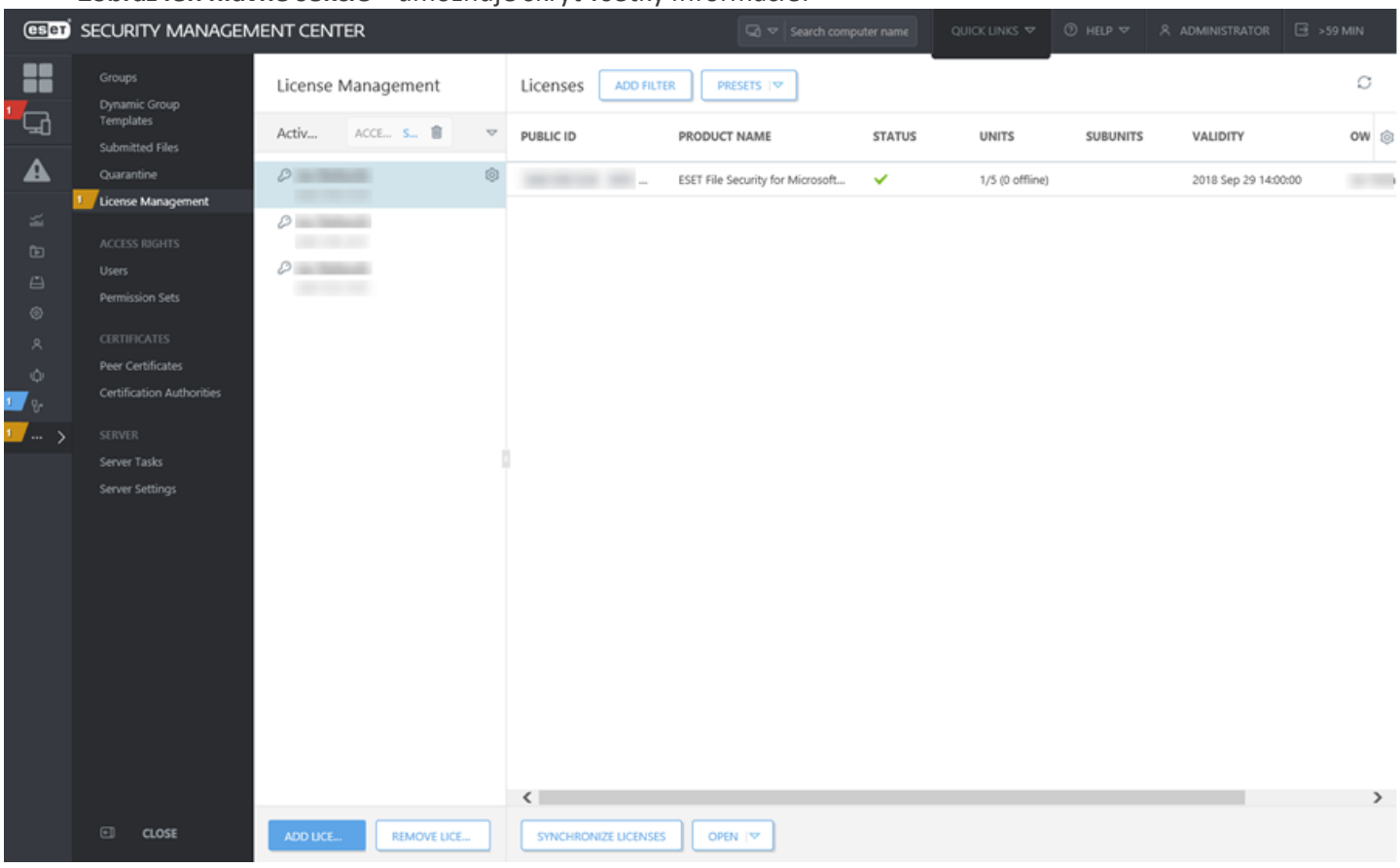
- **Typ licencie** môže byť: **Platená** (platená licencia), **Skúšobná** (skúšobná licencia) a **NFR** (nepredajná licencia).
- **Označenia** môžu byť **MSP**, **Biznis** a **Spotrebiteľ**.

Podľa ikon ľahko rozpoznáte, akým spôsobom ste danú licenciu do ESMC odovzdali: **offline licenčný súbor**, **licenčný kľúč** alebo pomocou portálu **Business Account**.

Vyberte licenciu v hlavnom okne napravo a kliknite na možnosť **Použite licenciu pre aktiváciu**, čím dôjde k spusteniu úlohy na aktiváciu produktu.

Pre zmenu režimu výberu z jednej na viac položiek použite možnosť **Režimy**. Kliknite na šípku v pravom hornom rohu a vyberte si z kontextového menu:

- **Režim jedného výberu** – umožňuje označiť jednu položku zo zoznamu.
- **Režim viacerých výberov** – umožňuje pomocou začiarkavacích políčok označiť viac položiek.
- **Obnoviť** – umožňuje obnoviť/opätovné načítať zobrazené informácie.
- **Zobraz všetky položky** – umožňuje zobraziť všetky informácie.
- **Zobraz len hlavné sekcie** – umožňuje skryť všetky informácie.



- **Názov produktu**, pre ktorý je licencia určená.
- Celkový **Stav** licencie (zobrazí sa upozornenie, ak licencia vypršala, došlo k prekročeniu počtu povolených licencií atď.).
- Počet **Jednotiek**, ktoré môžu byť aktivované pomocou tejto licencie a počet offline jednotiek.
- Počet **Podjednotiek** serverových produktov spoločnosti ESET (poštové schránky, ochrana brán, pripojenia).
- Dátum **vypršania platnosti** licencie.
  - Pre licencie vo forme predplatného nemusí byť zobrazený dátum vypršania platnosti.
- **Meno vlastníka** licencie a **Kontakt**.

Stav licencie sa zobrazuje pre aktívnu položku menu.

Zelená – vaša licencia je úspešne aktivovaná.
Červená – licencia nie je registrovaná pomocou nástroja ESET License Administrator alebo jej platnosť vypršala.
Oranžová – vaša licencia je vyčerpaná alebo sa blíži dátum uplynutia jej platnosti (ostáva 30 dní).

Synchronizácia licencií

Vaše licencie sa synchronizujú s portálom ESET Business Account automaticky jedenkrát denne. V prípade potreby môžete synchronizáciu vykonať manuálne kliknutím na možnosť **Synchronizovať licencie**.

Otvoriť

Kliknutím na možnosť **Otvoriť** zobrazíte odkazy slúžiace na prístup k portálu ESET Business Account a SET MSP Administrator.

Pridanie licencie alebo licenčného kľúča

Kliknite na **Pridať licencie** a vyberte metódu, ktorú chcete použiť na pridanie novej licencie:

1. ESET Business Account – pripojenie účtu EBA a všetkých jeho licencií do časti **Správa licencií**.
2. Licenčný kľúč – zadajte platný licenčný kľúč a kliknite na **Pridať licencie**. Licenčný kľúč bude overený pomocou aktivačného servera a pridaný do zoznamu.
3. Offline licenčný súbor – vyberte licenčný súbor (*.lf*) a kliknite na **Pridať licenciu**. Licenčný súbor bude overený a licencia pridaná do zoznamu.

Licencie vo forme predplatného

ESMC 7 podporuje správu licencií vo forme predplatného. Takúto licenciu môžete pridať cez EBA alebo pomocou licenčného kľúča. Platnosť svojho predplatného si môžete skontrolovať v sekcii **Správa licencií** v stĺpci **Platnosť**, prípadne tiež cez sekciu **Počítače** > Podrobnosti o počítači. Z licencie formou predplatného nie je možné vytvoriť offline licenčný súbor.

ESET Business Account – účty lokalít

Účty lokalít z portálu EBA nie sú v rámci ESMC podporované. Ak má používateľ portálu EBA práva na **čítanie** a **zápis** na úrovni **prístupu do spoločnosti**, všetky licencie budú importované pri synchronizácii účtu. Ak používateľ portálu EBA nemá práva na **prístup do spoločnosti** (nastavená je možnosť **Bez prístupu**), nebudú importované žiadne licencie.

Odstránenie licencií

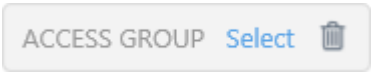
Označte licenciu v zozname a kliknutím na „Odstrániť licencie“ ju odstráňte. Budete vyzvaný na potvrdenie tejto akcie. Odstránenie licencie však nedeaktivuje produkt. Vaše bezpečnostné produkty ESET zostanú aktivované aj po odstránení licencie pomocou Správy licencií ESMC.

Licencie môžu byť distribuované na klientske stanice s nainštalovanými produktmi ESET prostredníctvom ESMC dvoma spôsobmi:

- Inštalácia softvéru
- Aktivácia produktu

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

+ Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

PRÍKLAD: AKO ZDIEĽAŤ LICENCIE SO SPRÁVCAMI V JEDNOTLIVÝCH POBOČKÁCH FIRMY

Okrem samotného Správcu (účet Administrator) sú v ESMC vytvorení traja používatelia, pričom každý má svoju vlastnú domácu skupinu:

- *John*, *San Diego*
- *Larry*, *Sydney*
- *Makio*, *Tokyo*

Správca naimportuje 2 licencie. Tieto licencie budú zahrnuté v statickej skupine *Všetko* a ostatní používatelia ich nebudú môcť použiť.

Ak chce správca priradiť licenciu k inému používateľovi, môže kliknúť na ikonu umiestnenú vedľa licencie, ktorú chce priradiť, a následne môže kliknúť na **Prístupová skupina** > **Presunúť** a vybrať skupinu, do ktorej má daný používateľ prístup. V prípade používateľa *John* je potrebné kliknúť na skupinu *San Diego*. Používateľ *John* musí mať pridelené povolenie na **použitie Licencií** v skupine *San Diego*.

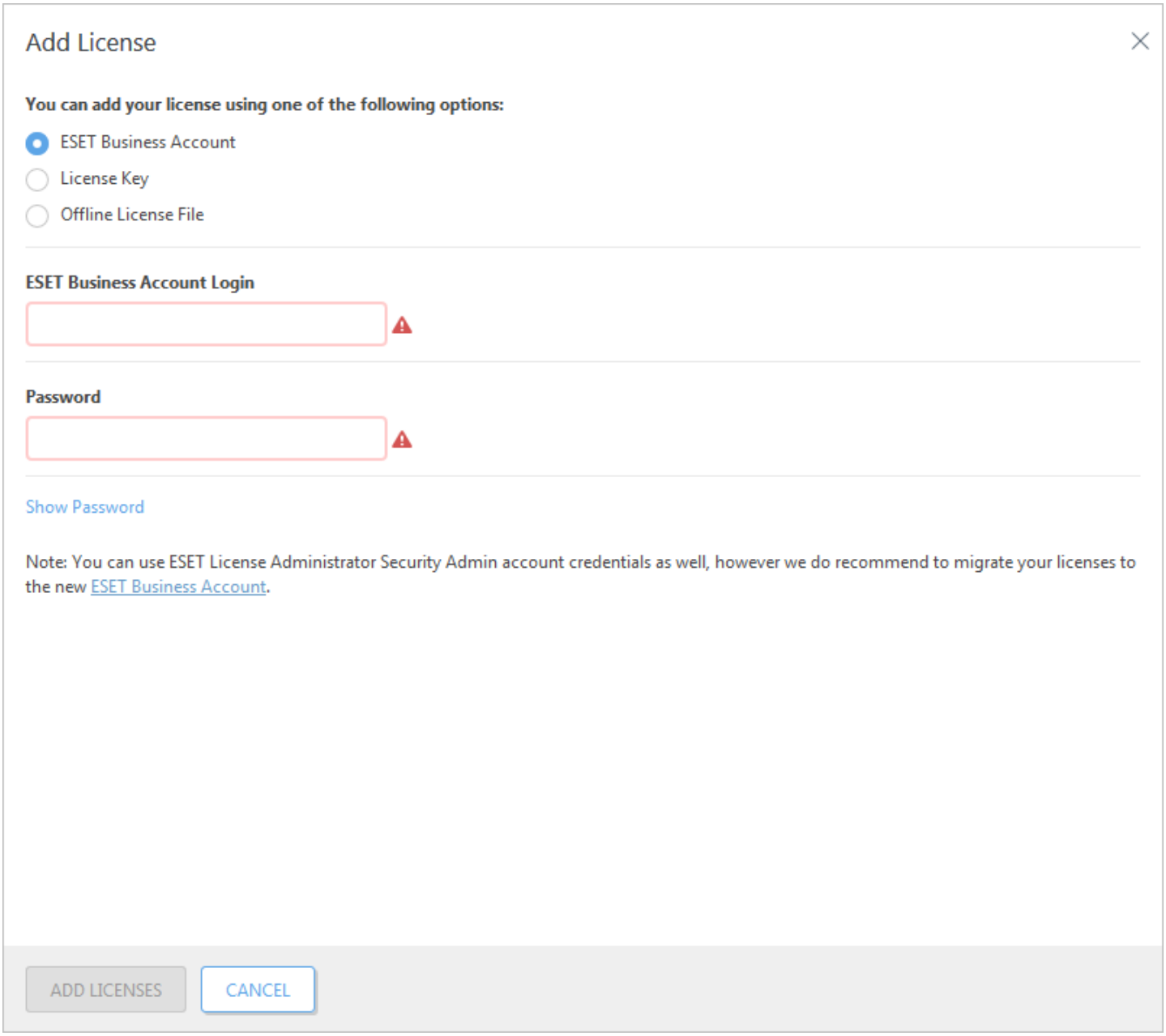
Akonáhle sa používateľ *John* prihlási do ESMC Web Console, bude môcť vidieť a použiť len tú licenciu, ktorá bola presunutá do jeho skupiny. Správca by mal tento postup následne zopakovať aj pre ostatných používateľov (*Larry* a *Makio*); používatelia vidia len svoje licencie, kým správca vidí všetky licencie.

4.13.4.1 ESET Business Account

Dôležité:
Pridávať a odstraňovať licencie môžu len správcovia, ktorých domácou skupinou je skupina **Všetko** a ktorí majú pridelené povolenia na **zápis** pre licencie (umiestnené v skupine Všetko). Každá licencia je identifikovaná **Verejným ID** a môže obsahovať jednu alebo viacero jednotiek. Licencie môže ostatným používateľom (tým, ktorí majú dostatočné povolenia) distribuovať len správca. Licenciu nie je možné rozdeliť.

ESET Business Account **prihlasovacie údaje**

Zadajte prihlasovacie údaje pre portál ESET Business Account (ESMC zobrazí všetky delegované licencie v Správe licencií ESMC) a kliknite na **Pridať licencie**.



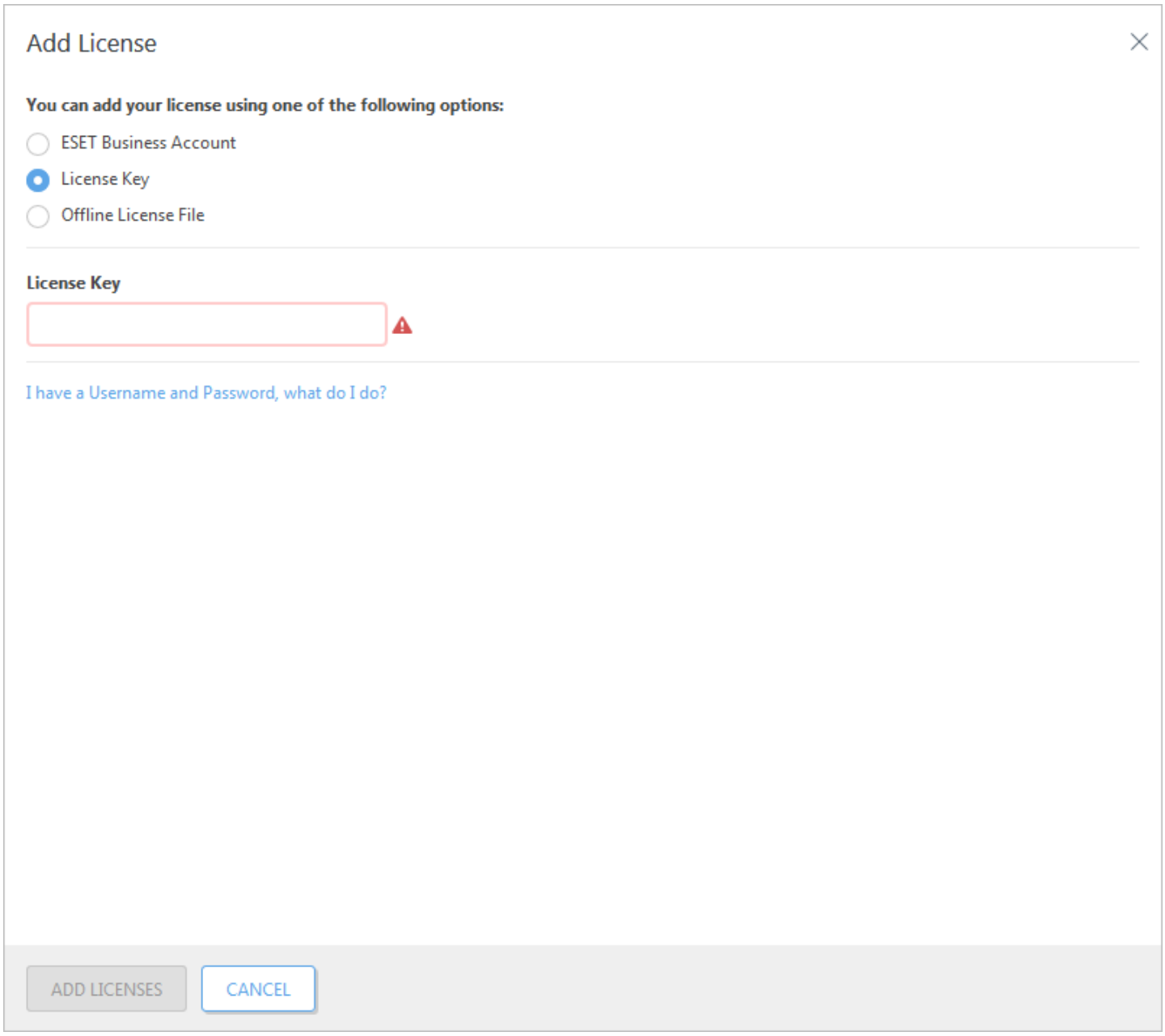
4.13.4.2 Pridanie licencie – licenčný kľúč

Dôležité:
Pridávať a odstraňovať licencie môžu len správcovia, ktorých domácou skupinou je skupina **Všetko** a ktorí majú pridelené povolenia na **zápis** pre licencie (umiestnené v skupine Všetko). Každá licencia je identifikovaná **Verejným ID** a môže obsahovať jednu alebo viacero jednotiek. Licencie môže ostatným používateľom (tým, ktorí majú dostatočné povolenia) distribuovať len správca. Licenciu nie je možné rozdeliť.

Licenčný kľúč

Do poľa **Licenčný kľúč** napíšte alebo skopírujte licenčný kľúč, ktorý ste dostali pri kúpe vášho bezpečnostného produktu od spoločnosti ESET a kliknite na **Pridať licencie**.

Ak používate staršie licenčné údaje (používateľské meno a heslo), prekonvertujte tieto údaje na licenčný kľúč. Ak licencia nie je registrovaná, spustí sa proces registrácie, ktorý prebieha v portáli EBA (ESMC poskytne platnú URL adresu na registráciu podľa pôvodu licencie).



4.13.4.3 Offline aktivácia

Na aktiváciu ESMC a iných bezpečnostných produktov ESET môžete použiť licenčný súbor z portálu ESET Business Account. Každý offline licenčný súbor je generovaný len pre jeden produkt, napr. ESET Endpoint Security. Offline licencia sa používa len u klientov, ktorí nemajú a nebudú mať prístup k licenčným serverom ESET (offline licenciu nie je vhodné použiť ani v prípade, ak je klient pripojený k internetu prostredníctvom proxy servera s prístupom obmedzeným iba na služby ESET). Z licencie formou predplatného nie je možné vytvoriť offline licenčný súbor.

Ak chcete nahradiť existujúcu offline licenciu, je potrebné vykonať nasledujúce kroky:

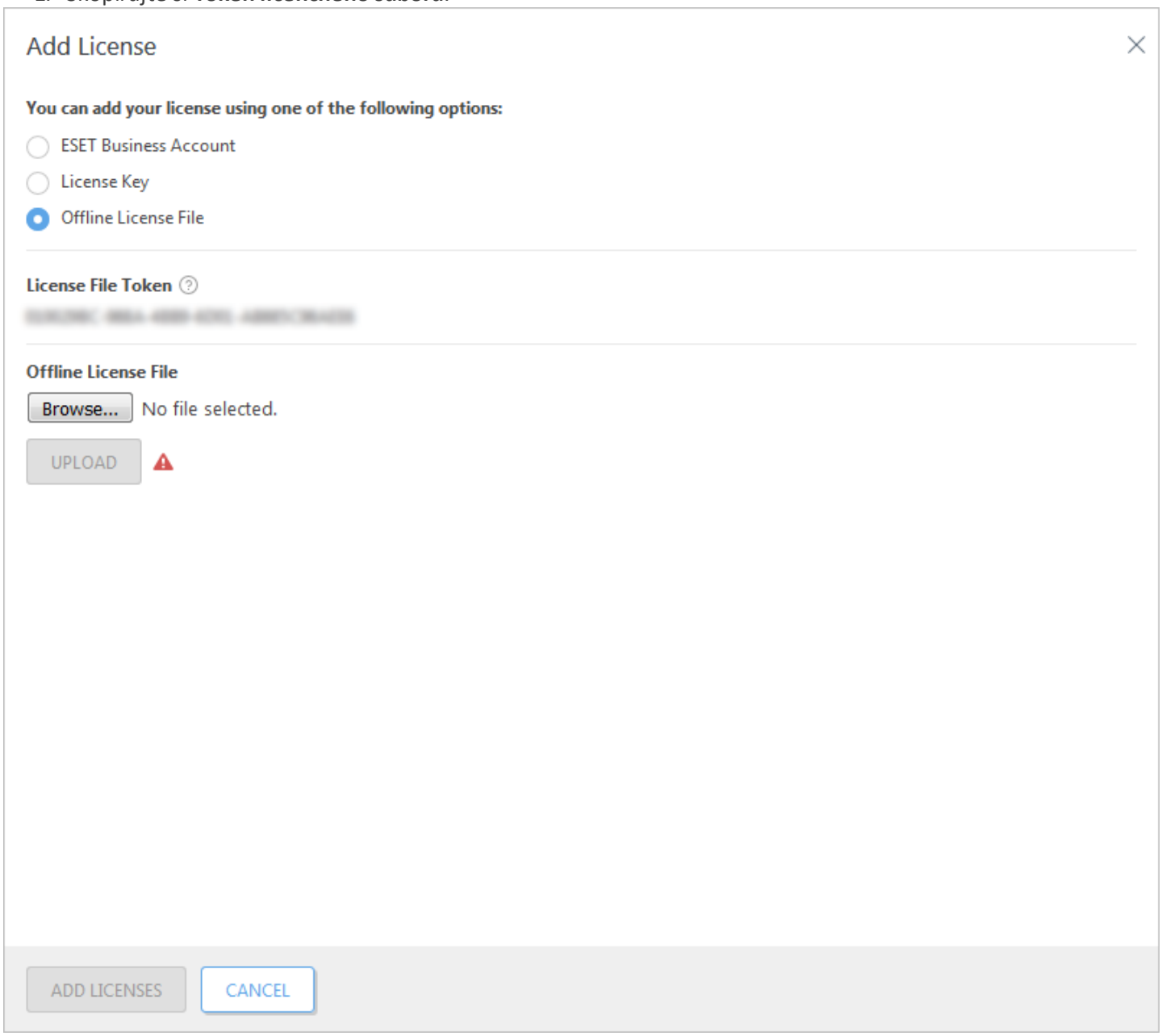
1. Odstrániť starú licenciu v ESMC a licenčný súbor v portáli ESET Business Account.
2. Vytvoriť novú offline licenciu v portáli ESET Business Account.
3. Importovať novú licenciu do ESMC.
4. Opätovne aktivovať produkty použitím novej licencie.

Dôležité:
Pridávať a odstraňovať licencie môžu len správcovia, ktorých domácou skupinou je skupina **Všetko** a ktorí majú pridelené povolenia na **zápis** pre licencie (umiestnené v skupine Všetko). Každá licencia je identifikovaná **Verejným ID** a môže obsahovať jednu alebo viacero jednotiek. Licencie môže ostatným používateľom (tým, ktorí majú dostatočné povolenia) distribuovať len správca. Licenciu nie je možné rozdeliť.

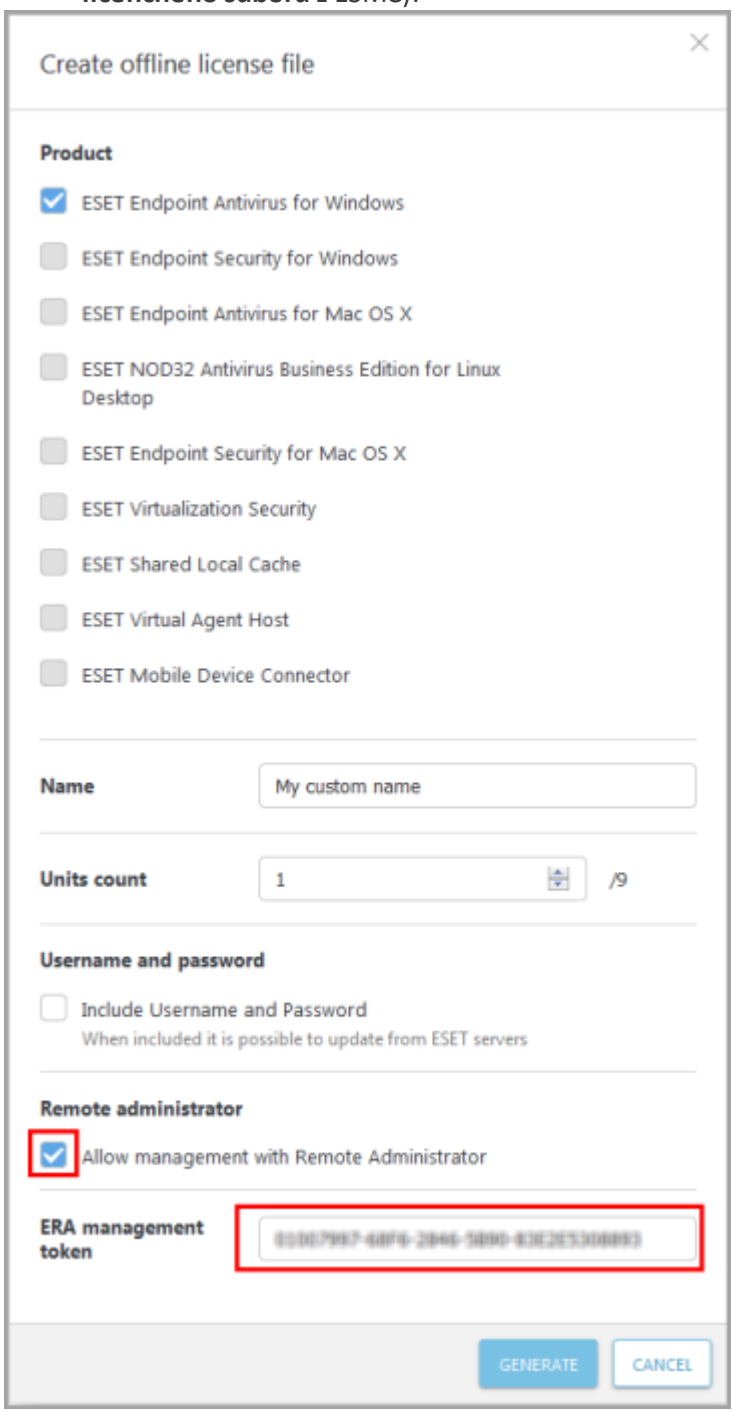
Offline licenčný súbor

Pre vytvorenie a následný import offline licenčného súboru postupujte podľa nasledujúcich pokynov:

1. Skopírujte si **Token licenčného súboru**.



2. Prihláste sa do svojho účtu ESET Business Account, kde ste importovali svoju licenciu.
3. Vyberte licenciu, ktorú chcete exportovať a zvoľte možnosť **Vytvoriť offline súbory**.
4. Vyberte produkt, pre ktorý chcete vytvoriť licenčný súbor a zadajte jeho **Názov** a **Počet jednotiek** (jednotky licencie, ktoré budú exportované do licenčného súboru).
5. Označte možnosť **Povoliť správu pomocou Remote Administratora** a zadajte **ERA management token** (**Token licenčného súboru** z ESMC).

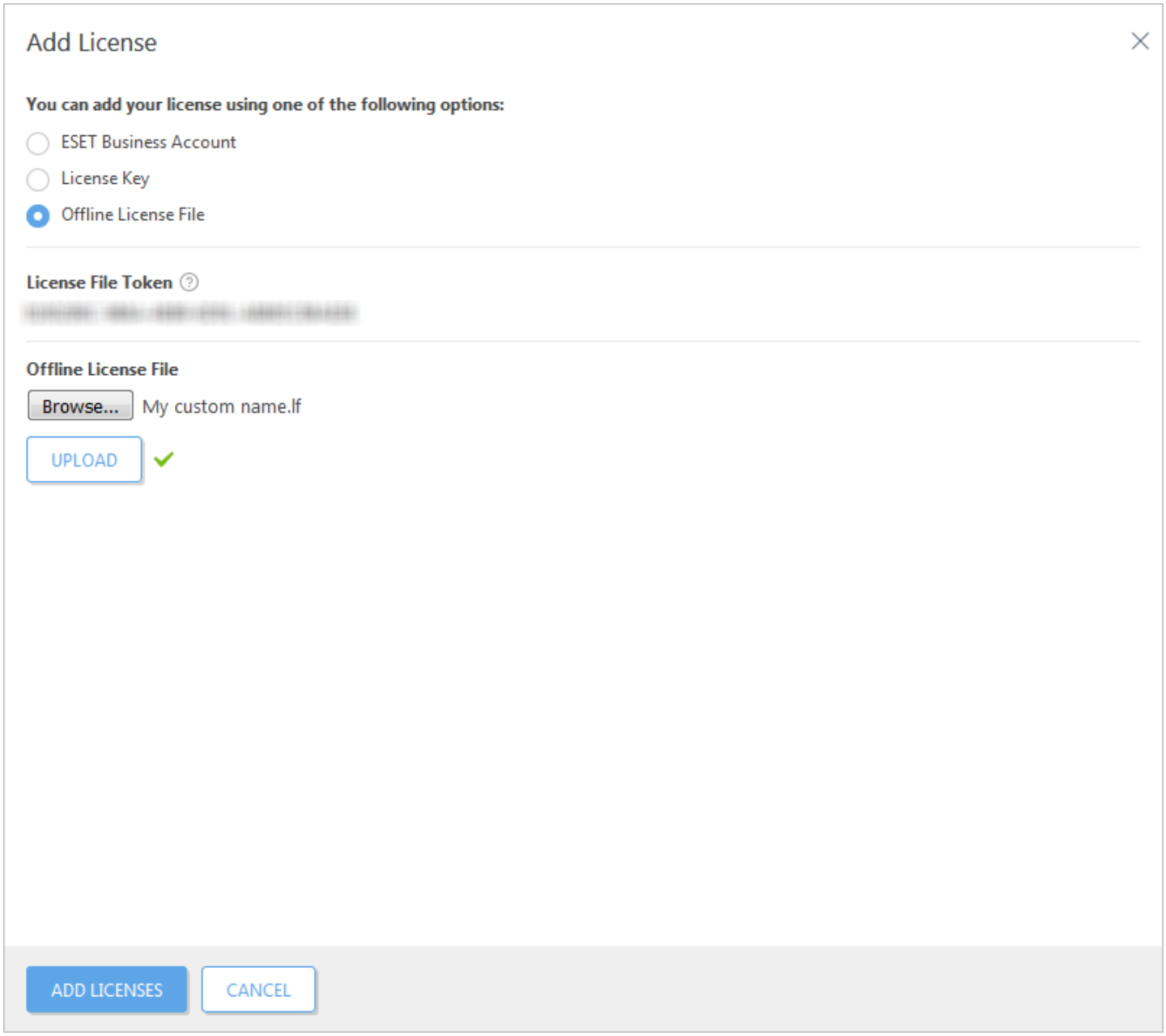


6. Kliknite na **Vygenerovať**.

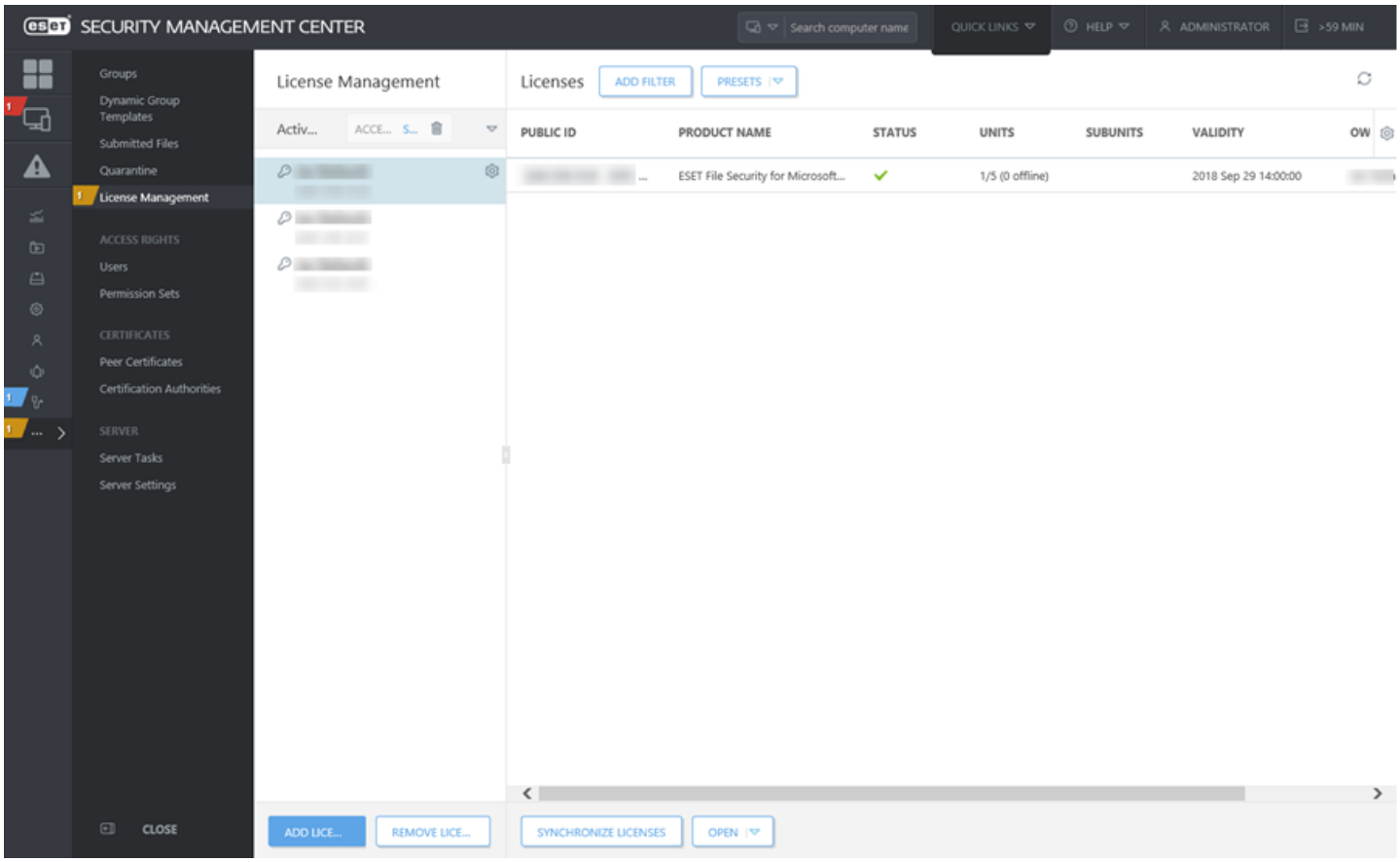
Pre stiahnutie súboru postupujte podľa nasledujúcich krokov:

1. Vyberte licenciu a kliknite na možnosť **Zobraziť detailné informácie**.
2. Prejdite na kartu **Offline súbory**.
3. Kliknite na licenčný súbor, ktorý ste vytvorili a zvoľte možnosť **Stiahnuť**.

Vráťte sa späť do ESMC do časti Správa licencií, vyberte možnosť **Prehľadávať**, nájdite offline licenčný súbor, ktorý ste exportovali z portálu EBA, kliknite na **Odovzdať** a napokon kliknite na **Pridať licencie**.



Podľa ikon ľahko rozpoznáte, akým spôsobom ste danú licenciu pridali: – pomocou **licenčného kľúča**, – pomocou **offline licencie** alebo – pomocou **účtu bezpečnostného správcu**.



Licencie môžu byť distribuované na klientske stanice s nainštalovanými bezpečnostnými produktmi spoločnosti ESET prostredníctvom ESMC dvoma spôsobmi:

- pomocou úlohy Inštalácia softvéru,
- pomocou úlohy Aktivácia produktu.

4.13.5 Prístupové práva

Prístupové práva vám umožňujú spravovať používateľov ESMC Web Console a ich oprávnenia. Prístupové práva môžete prideľovať:

- Natívnym používateľom – používateľské účty vytvorené a spravované pomocou ESMC Web Console.
- Namapovaným bezpečnostným skupinám domény – používateľské účty spravované a overované prostredníctvom Active Directory.

Pre natívnych používateľov a namapované bezpečnostné skupiny domény môžete prípadne použiť aj dvojúrovňovú autentifikáciu. Bude tak zaistená vyššia úroveň zabezpečenia pri prihlasovaní do ESMC Web Console.

Povolenie na prístup k položkám patriacim do určitej kategórie musí byť jednotlivým používateľom ESMC Web Console pridelené pomocou sady povolení.

Dôležité:
Natívny používateľ Administrator (správca), ktorého domáca skupina je *Všetko*, má prístup ku všetkým skupinám a objektom. Tento účet preto neodporúčame používať na bežné účely. Odporúčame vytvoriť si ďalší „správcovský“ účet alebo použiť správcov z namapovanej bezpečnostnej skupiny domény, ktorí majú pridelené potrebné povolenia. To zabezpečí možnú obnovu pri zlyhaní alebo chybe účtu správcu. Taktiež odporúčame vytvoriť ďalšie používateľské účty, ktoré budú mať pridelené požadované povolenia umožňujúce vykonávanie len určitých činností. Predvolený účet správcu (Administrator) používajte iba ako záložnú možnosť, nie ako štandardný používateľský účet.

Používatelia sú spravovaní v sekcii **Viac** v časti Používatelia. Sady povolení určujú, aká úroveň prístupu k rôznym položkám bude umožnená pre určitých používateľov. Podrobnejšie informácie nájdete v zozname všetkých prístupových práv a ich funkcií.

Zoznam príkladov zaoberajúcich sa prístupovými právami

V tejto príručke správcu je uvedených viacero príkladov, ktoré sa sa priamo týkajú prístupových práv. Toto je ich zoznam:

- Ako duplikovať politiky
- Rozdiel medzi povoleniami na použitie a zápis
- Prístupové práva pre správcov v jednotlivých pobočkách firmy
- Ako zdieľať objekty použitím duplikovania
- Ako udeliť prístupové práva k certifikátom bez možnosti prístupu k certifikačným autoritám
- Ako používateľovi povoliť vytváranie inštalátorov
- Ako odstrániť oznámenia
- Ako vytvoriť politiky
- Ako používateľovi povoliť zobrazovanie všetkých politík
- Ako zdieľať licencie so správcami v jednotlivých pobočkách firmy

4.13.5.1 Používatelia

Správa používateľov je súčasťou sekcie **Viac** v ESMC Web Console.

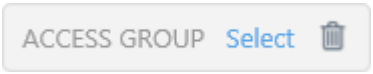
Bezpečnostný model

Nižšie sú uvedené kľúčové termíny nového modelu:

Termín	Vysvetlenie
Domáca skupina	Domáca skupina je skupina, kde sa automaticky uložia všetky objekty vytvorené používateľom (zariadenia, úlohy, šablóny atď.). Každý používateľ musí mať iba jednu domácu skupinu.
Objekt	Objekty sa nachádzajú v **Statických skupinách**. Prístup k objektom funguje podľa skupín, nie používateľov (poskytovanie prístupu podľa skupín uľahčuje prispôsobenie viacerým používateľom, napríklad ak je jeden používateľ na dovolenke). Úlohy pre server a oznámenia patria medzi výnimky, pre ktoré je vyžadovaný takzvaný „vykonávajúci používateľ“.
Prístupová skupina	Prístupová skupina funguje ako statická skupina, ktorá umožňuje používateľom filtrovať umiestnenie objektu podľa prístupových práv.
Správca	Správca je používateľ s domácou skupinou **Všetko** a kompletnou sadou povolení viazaných k tejto skupine.
Prístupové práva	Práva na prístup k objektu alebo práva na vykonanie úlohy sú prideľované pomocou sady povolení.
Sada povolení	Sady povolení predstavujú oprávnenia používateľov, ktorí majú prístup do ESMC Web Console. Určujú, čo môže používateľ v ESMC Web Console vidieť a robiť. K používateľovi je možné priradiť viacero sád povolení. Sady povolení sa uplatňujú len v rámci objektov zahrnutých v zadefinovaných statických skupinách. Tieto **statické skupiny** sa nastavujú v sekcii **Statické skupiny** pri vytváraní alebo upravovaní sady povolení.
Funkcia	Funkcia je jeden typ objektu alebo akcie. Funkcie majú zvyčajne nasledujúce hodnoty: **Čítanie**, **Zapísať**, **Použiť**. Kombinácia funkcií, ktoré sa vzťahujú na prístupovú skupinu, sa nazýva sada povolení.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

+ Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

PRÍKLAD: PRÍSTUPOVÉ PRÁVA PRE SPRÁVCOV V JEDNOTLIVÝCH POBOČKÁCH FIRMY
Ak má firma dve vzdialené pobočky a každá má svojho lokálneho správcu, je potrebné týmto správcom prideliť sady povolení viazané na rozdielne statické skupiny.

Povedzme, že pre pobočku v *San Diegu* je lokálnym správcom *John* a pre pobočku v *Sydney* je lokálnym správcom *Larry*. Obaja potrebujú spravovať len tie zariadenia, ktoré spadajú do lokálnej siete ich pobočky, a používať príslušné **Politiky**, **Riadiace panely**, **Správy** a **Šablóny dynamických skupín**. Z účtu hlavného správcu *(Administrator)* je potrebné vykonať nasledujúce kroky:

1. Vytvorte nové statické skupiny: *Pobočka San Diego*, *Pobočka Sydney*.
2. Vytvorte nové sady povolení:
   a. **Sada povolení** s názvom *Sada povolení – Sydney* , s priradenou statickou skupinou *Pobočka Sydney* a s kompletnou sadou prístupových povolení (okrem kategórie povolení **Nastavenia servera**).
   b. **Sada povolení** s názvom *Sada povolení – San Diego* , s priradenou statickou skupinou *Pobočka San Diego* a s kompletnou sadou prístupových povolení (okrem kategórie povolení **Nastavenia servera**).
   c. **Sada povolení** s názvom *Skupina Všetko/Riadiaci panel,* s priradenou statickou skupinou *Všetko* a s nasledujúcimi pridelenými povoleniami:
      - povolenie na **čítanie** v rámci kategórie **Úlohy pre klienta**,
      - povolenie na **použitie** v rámci kategórie **Šablóny dynamických skupín**,
      - povolenie na **použitie** v rámci kategórie **Správy a riadiace panely**,
      - povolenie na **použitie** v rámci kategórie **Politiky**,
      - povolenie na **použitie** v rámci kategórie **Odoslať e-mail**,
      - povolenie na **použitie** v rámci kategórie **Odoslať SNMP Trap**,
      - povolenie na **použitie** v rámci kategórie **Exportovať správu do súboru**,
      - povolenie na **použitie** v rámci kategórie **Licencie**,
      - povolenie na **zápis** v rámci kategórie **Oznámenia**.
3. Vytvorte nového používateľa nazvaného *John* s domácou skupinou *Pobočka San Diego* a s priradenými sadami povolení *Sada povolení – San Diego* a *Skupina Všetko / Riadiaci panel*.
4. Vytvorte nového používateľa nazvaného *Larry* s domácou skupinou *Pobočka Sydney* a s priradenými sadami povolení *Sada povolení – Sydney* a *Skupina Všetko / Riadiaci panel*.

S takto nastavenými povoleniami môžu *John* a *Larry* používať rovnaké úlohy, politiky, správy a riadiace panely a môžu používať šablóny dynamických skupín bez obmedzení (každý z nich však môže používať iba šablóny pre zariadenia zahrnuté vo vlastnej domácej skupine).

Bezpečnostné skupiny domény

Pre zjednodušenie používania služby Active Directory je možné používateľom patriacim do **bezpečnostných skupín domény** povoliť prihlasovanie do ESMC. Takíto používatelia môžu existovať súčasne s **Natívnymi používateľmi** nástroja ESMC. Sady povolení sú však nastavované pre celú bezpečnostnú skupinu Active Directory (nie pre jednotlivých používateľov, ako je to v prípade **Natívneho používateľa**).

Zdieľanie objektov

Ak chce správca (Administrator) zdieľať objekty, napr. šablóny dynamických skupín, šablóny správ alebo politiky, s inými používateľmi, môže využiť jednu z nasledujúcich možností:

- Požadované objekty presunúť do zdieľaných skupín
- Požadované objekty duplikovať a vytvorené duplikáty objektov premiestniť do statických skupín, ku ktorým majú ostatní používatelia prístup (pozrite si príklad uvedený nižšie)

PRÍKLAD: AKO ZDIEĽAŤ OBJEKTY POUŽITÍM DUPLIKOVANIA

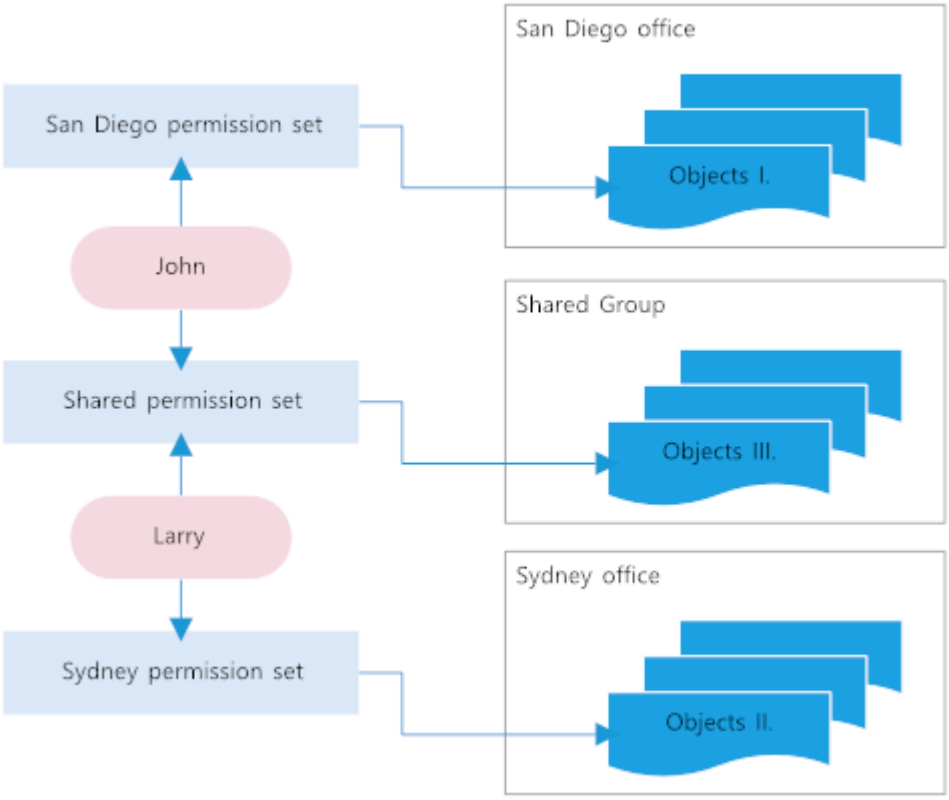
Na duplikovanie určitého objektu musí mať používateľ pridelené povolenie na **čítanie** pre pôvodný objekt a mať povolenie na **zápis** v rámci svojej **Domácej skupiny** pre tento typ akcie.

Správca (Administrator), ktorého domáca skupina je *Všetko*, chce zdieľať *Špeciálnu šablónu* s používateľom *John*. Šablóna bola pôvodne vytvorená hlavným správcom *(Administrator)*, a preto je automaticky zahrnutá v skupine *Všetko*. *Správca* musí vykonať nasledujúce kroky:

1. Prejsť do sekcie **Viac** > **Šablóny dynamickej skupiny**.
2. Zo zoznamu vybrať *Špeciálnu šablónu* a kliknúť na **Duplikovať**. V prípade potreby sa môže zadať pre duplikovanú šablónu nový názov a popis. Nakoniec je potrebné kliknúť na tlačidlo **Dokončiť**.
3. Duplikát šablóny bude umiestnený do domácej skupiny *Správcu*, t. j. do skupiny *Všetko*.
4. Prejsť do sekcie **Viac** > **Šablóny dynamickej skupiny**, vybrať duplikovanú šablónu, kliknúť na **Prístupová skupina** > **Presunúť** a vybrať statickú skupinu, do ktorej má byť šablóna presunutá (je potrebné vybrať skupinu, do ktorej má *John* prístup). Kliknite na **OK**.

Ako zdieľať objekty medzi viacerými používateľmi pomocou zdieľanej skupiny

Pre lepšie pochopenie toho, ako nový bezpečnostný model funguje, si pozrite schému uvedenú nižšie. V tomto príklade figurujú dvaja používatelia vytvorení Správcom, konkrétne John a Larry. Každý z týchto používateľov má svoju vlastnú domácu skupinu, ktorá obsahuje všetky objekty vytvorené daným používateľom. *Sada povolení – San Diego* udeľuje *Johnovi* oprávnenie narábať s *Objektmi* umiestnenými v jeho domácej skupine *Pobočka San Diego*. Situácia je podobná aj v prípade *Larryho*. Ak títo používatelia potrebujú medzi sebou zdieľať nejaké objekty (napríklad počítače), tieto objekty treba presunúť do statickej skupiny *Zdieľaná skupina*. K obom používateľom je následne potrebné priradiť *Zdieľanú sadu povolení*, ktorá má v sekcii **Statické skupiny** uvedenú *Zdieľanú skupinu*.



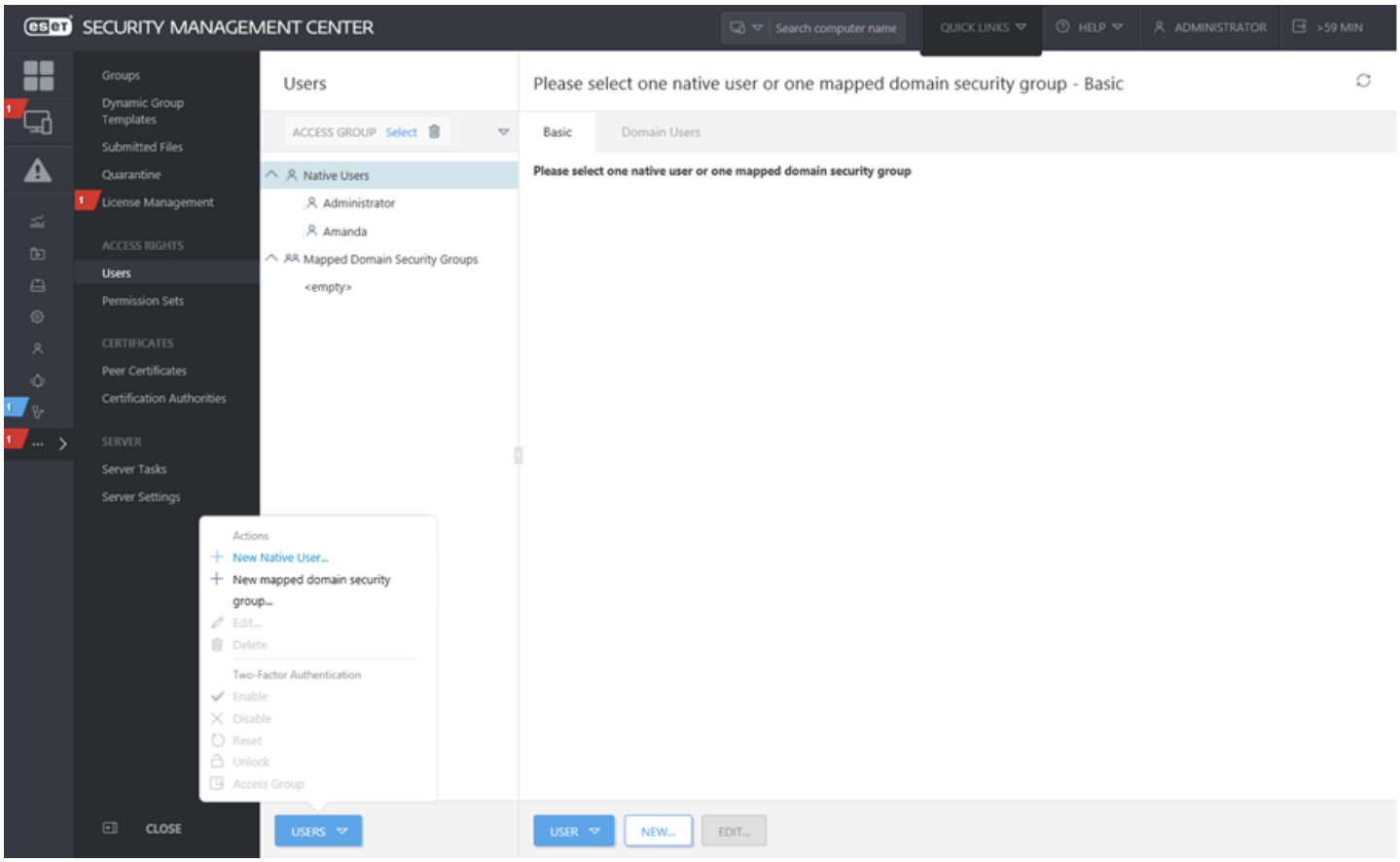
Poznámka:
Po dokončení inštalácie nástroja ESMC existuje iba jediný používateľský účet – **Správca** (natívny používateľ s domácou skupinou **Všetko**).

4.13.5.1.1 Vytvorenie natívneho používateľa

Ak chcete vytvoriť nového natívneho používateľa, prejdite na kartu **Viac**, kliknite na **Používatelia** a následne kliknite na tlačidlo **Nový...** v dolnej časti obrazovky.

Poznámka:
Pre správne vytvorenie používateľa sa riaďte týmto postupom:

1. Rozhodnite sa, ktorá statická skupina sa má stať domácou skupinou daného používateľa. V prípade potreby vytvorte novú skupinu.
2. Rozhodnite sa, ktorú sadu povolení chcete danému používateľovi prideliť. V prípade potreby vytvorte novú sadu povolení.
3. Postupujte podľa krokov uvedených v tejto kapitole pre nastavenie a vytvorenie účtu používateľa.



Základné

Zadajte **Používateľské meno** a prípadne aj **Popis**. Zvoľte **Domácu skupinu**. Ide o statickú skupinu, v ktorej budú automaticky zahrnuté všetky objekty vytvorené daným používateľom.

Nastaviť heslo

Heslo používateľa by malo mať minimálne 8 znakov. Zároveň by nemalo obsahovať používateľské meno.

Účet

Zapnuté – označte túto možnosť, ak chcete, aby bol účet aktívny (ak chcete účet aktivovať neskôr, zrušte výber danej možnosti).

Je potrebné zmeniť heslo – ak označíte túto možnosť, daný používateľ bude musieť po prvom prihlásení do ESMC Web Console zmeniť svoje heslo.

Platnosť hesla – táto možnosť udáva platnosť hesla v dňoch, pričom po uplynutí stanoveného počtu dní musí byť heslo zmenené.

Automaticky odhlásiť (min) – táto možnosť udáva časový interval nečinnosti (v minútach), po uplynutí ktorého je používateľ automaticky odhlásený z Web Console.

Celé meno, **E-mailový kontakt** a **Telefónny kontakt** slúžia na lepšiu identifikáciu používateľa.

Sady povolení

K používateľovi je možné priradiť viacero sád povolení. Môžete vybrať prednastavenú sadu povolení: **Sada povolení iba na čítanie** (práva len na čítanie pre skupinu Všetko), **Sada povolení správcu** (úplné prístupové práva pre skupinu Všetko) alebo **Sada povolení serverom asistovanej inštalácie** (minimálne prístupové práva vyžadované pre serverom asistovanú inštaláciu). Môžete tiež použiť vlastnú sadu povolení. Každá sada povolení poskytuje povolenia len pre tie objekty, ktoré sú obsiahnuté v **Statických skupinách** zvolených v danej sade povolení. Používatelia, ktorí nemajú priradenú žiadnu sadu povolení, sa nebudú môcť prihlásiť do Web Console.

Upozornenie:
Všetky predvolené sady povolení majú v sekcii **Statické skupiny** nastavenú skupinu **Všetko**. Používateľom preto tieto sady povolení prideľujte veľmi obozretne. Používatelia s týmito sadami povolení by disponovali oprávneniami vzťahujúcimi sa na všetky objekty v ESMC.

Súhrn

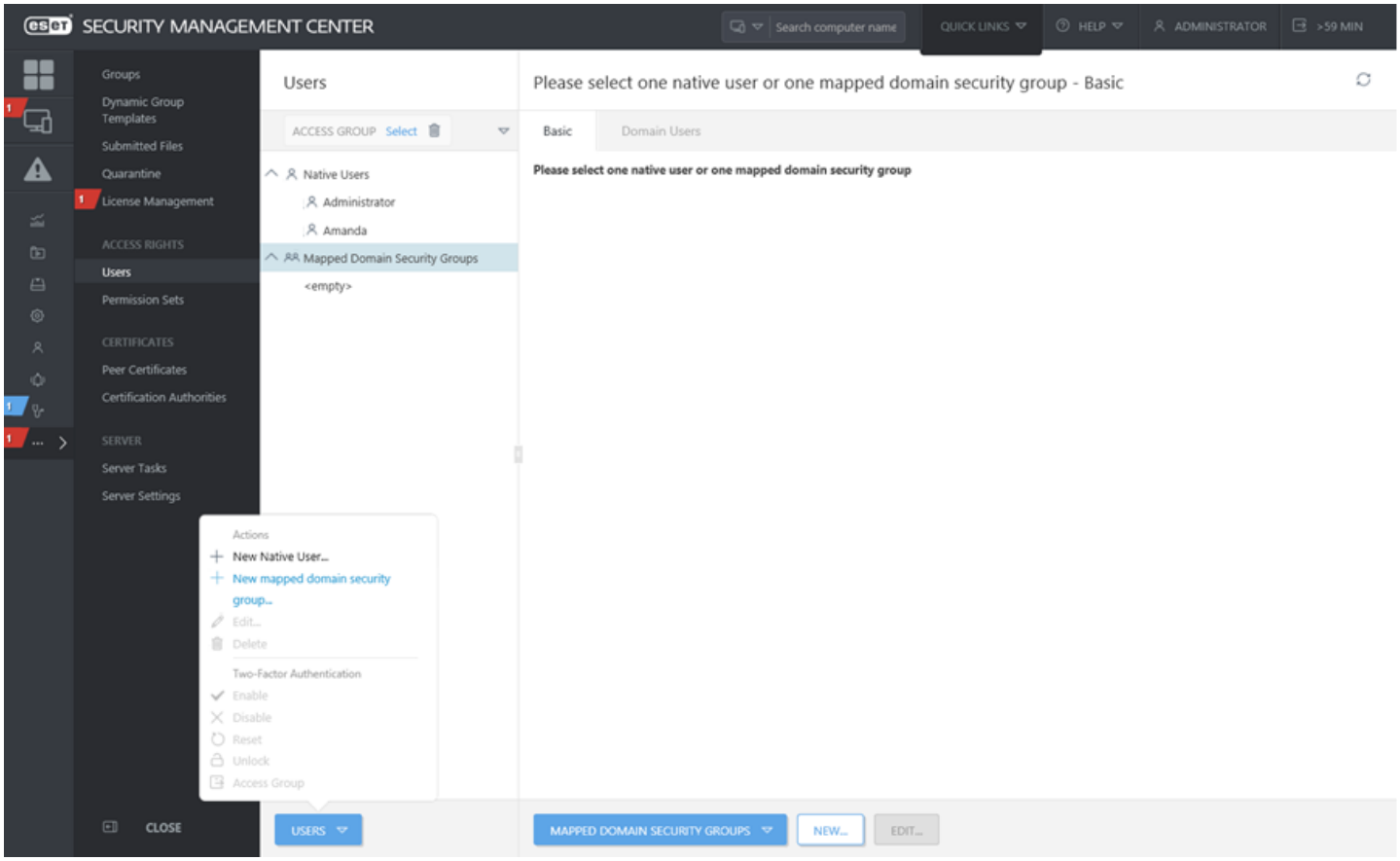
Skontrolujte nastavenia a kliknite na **Dokončiť** pre vytvorenie používateľa.

4.13.5.1.2 Namapovanie bezpečnostnej skupiny domény

Bezpečnostnú skupinu domény môžete namapovať na ESMC Server a umožniť existujúcim používateľom (členom doménových bezpečnostných skupín), aby sa stali používateľmi ESMC Web Console.

Poznámka:
Táto funkcia je dostupná len pre systémy s Active Directory. Nemôže byť použitá s LDAP.

Ak chcete vytvoriť novú **Namapovanú bezpečnostnú skupinu domény**, prejdite v hlavnom menu na kartu **Viac** > **Používatelia** > **Namapované bezpečnostné skupiny domény** > **Nová** alebo jednoducho kliknite na možnosť **Nová...**, ak je v zozname označená možnosť Namapované bezpečnostné skupiny domény.



Základné

Skupina domény

Zadajte pre skupinu **Názov**. V prípade potreby môžete zadať aj **Popis**. Zvoľte **Domácu skupinu**. Ide o statickú skupinu, v ktorej budú automaticky zahrnuté všetky objekty vytvorené používateľmi z danej doménovej skupiny.

Táto doménová skupina bude identifikovaná pomocou bezpečnostného identifikátora **SID**. Kliknite na možnosť **Vybrať**, vyberte skupinu zo zoznamu a kliknite na tlačidlo **OK**. Váš ESMC Server musí byť pripojený k doméne, v opačnom prípade v zozname nebudú žiadne skupiny (v prípade, že používate virtuálne zariadenie, si prečítajte túto kapitolu).

Účet

Zapnuté – označte túto možnosť, ak chcete, aby bol účet aktívny (ak chcete účet aktivovať neskôr, zrušte výber danej možnosti).

Automaticky odhlásiť (min) – táto možnosť udáva časový interval nečinnosti (v minútach), po uplynutí ktorého je používateľ automaticky odhlásený z Web Console.

E-mailový kontakt a **Telefónny kontakt** slúžia na lepšiu identifikáciu skupiny.

Sady povolení

Prideľte oprávnenia používateľom patriacim do tejto doménovej skupiny. Ku skupine môžete priradiť aj viacero sád povolení. Môžete použiť prednastavené sady povolení:

- **Sada povolení iba na čítanie** (práva len na čítanie pre skupinu Všetko)
- **Sada povolení správcu** (úplné prístupové práva pre skupinu Všetko)
- **Sada povolení serverom asistovanej inštalácie** (minimálne prístupové práva vyžadované pre serverom asistovanú inštaláciu)
- Vlastná sada povolení

Každá sada povolení poskytuje povolenia len pre tie objekty, ktoré sú obsiahnuté v **Statických skupinách** zvolených v danej sade povolení. Používateľ, ktorý nemá priradenú žiadnu sadu povolení, sa nebude môcť prihlásiť do Web Console.

> **Upozornenie:**
> Všetky predvolené sady povolení majú v sekcii **Statické skupiny** nastavenú skupinu **Všetko**. Používateľom preto tieto sady povolení prideľujte veľmi obozretne. Používatelia s týmito sadami povolení by disponovali oprávneniami vzťahujúcimi sa na všetky objekty v ESMC.

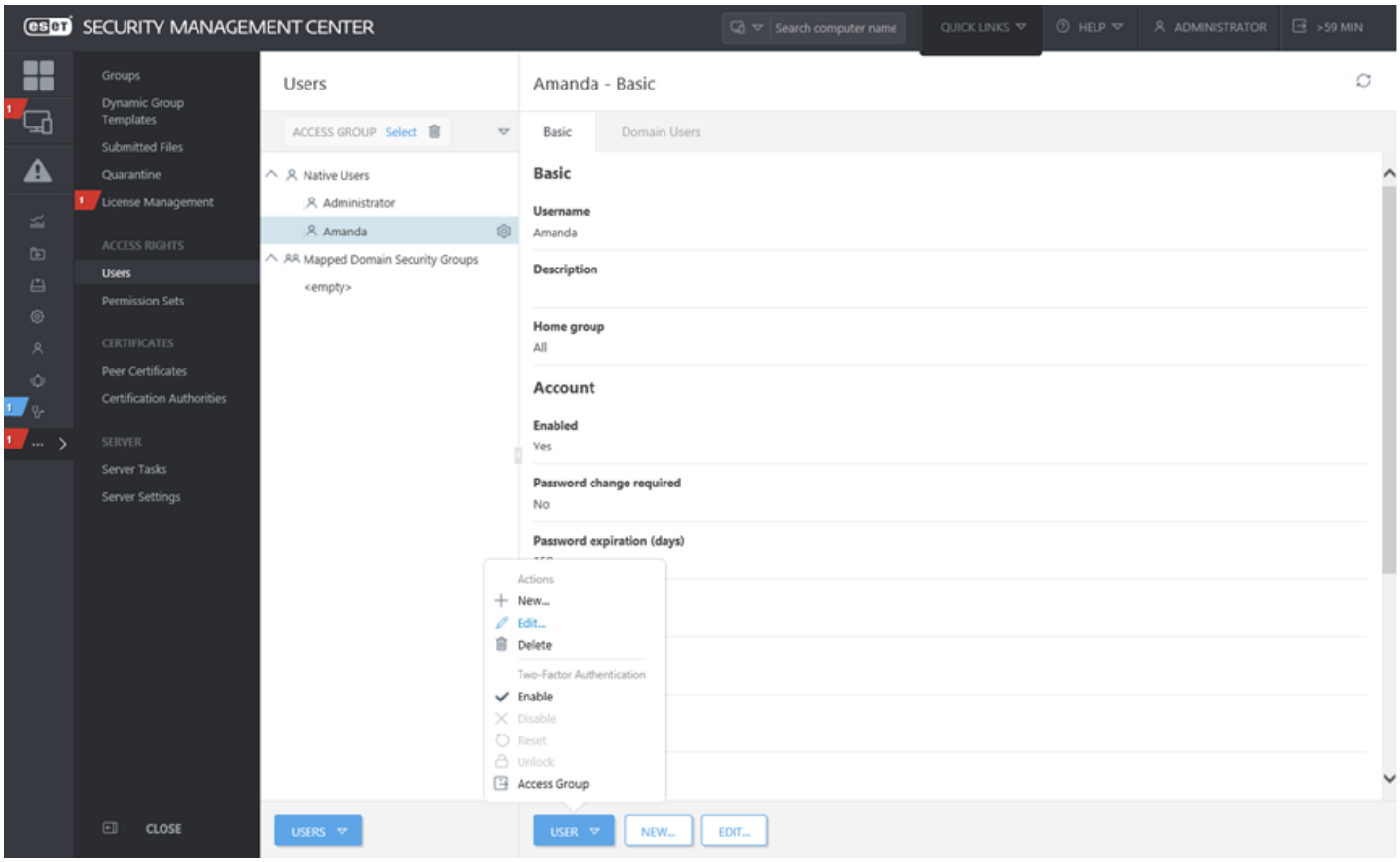
Súhrn

Skontrolujte nastavenia a kliknite na **Dokončiť**.

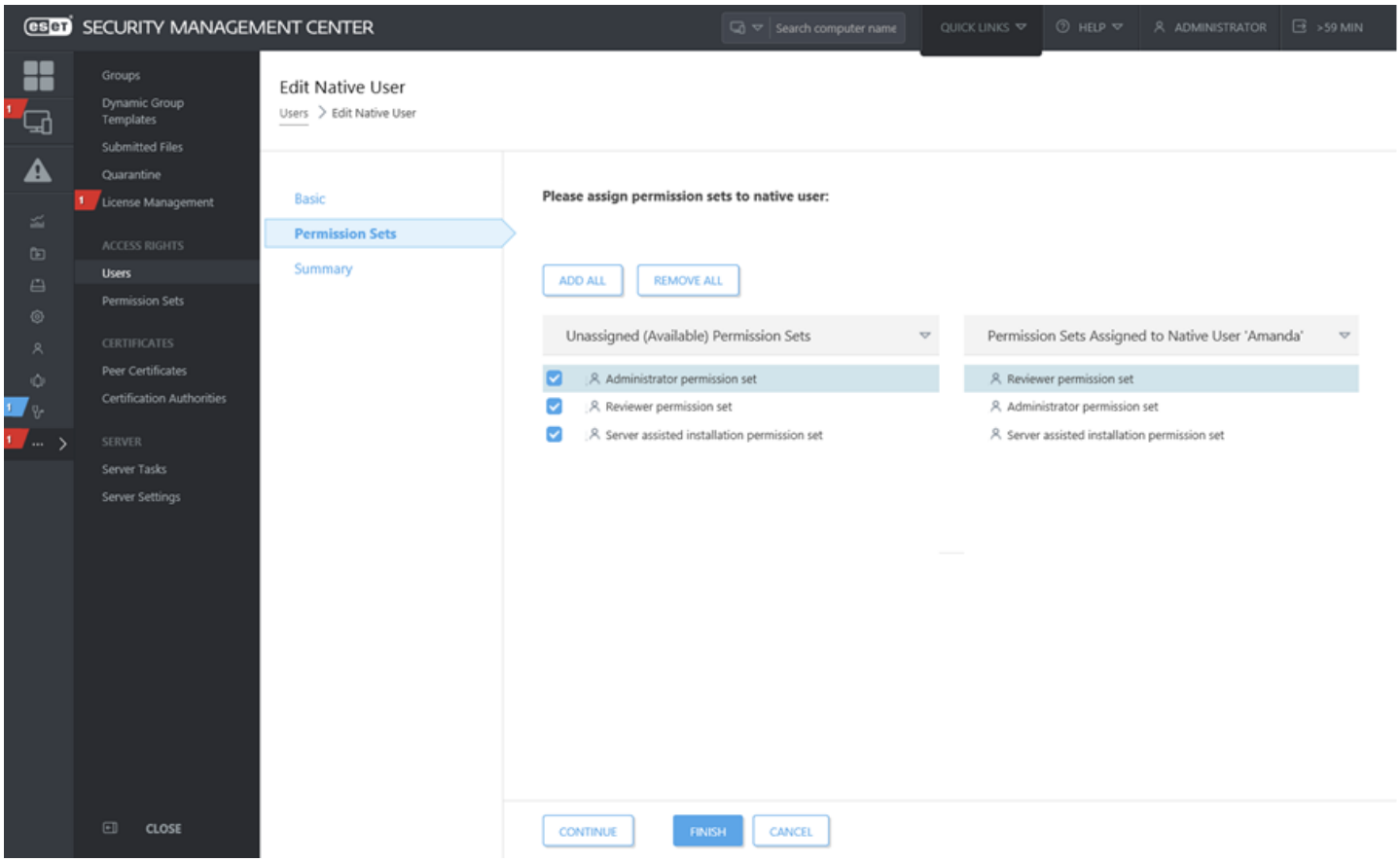
Po prvom prihlásení budú používatelia zobrazení na karte **Používatelia domény**.

4.13.5.1.3 Pridelenie sady povolení používateľovi

Pre pridelenie sady povolení konkrétnemu používateľovi prejdite do sekcie **Viac** > **Sady povolení** a kliknite na **Upraviť**. Viac informácií nájdete v časti Správa povolení.



V sekcii **Používatelia** môžete upraviť konkrétneho používateľa kliknutím na **Upraviť**, v časti **Nepriradené (dostupné) sady povolení** následne označte začiarkavacie políčko vedľa sady povolení, ktorú chcete k danému používateľovi priradiť.


SECURITY MANAGEMENT CENTER
Search computer name
QUICK LINKS
HELP
ADMINISTRATOR
>59 MIN
Groups
Dynamic Group Templates
Submitted Files
Quarantine
License Management
ACCESS RIGHTS
Users
Permission Sets
CERTIFICATES
Peer Certificates
Certification Authorities
SERVER
Server Tasks
Server Settings
CLOSE
Edit Native User
Users > Edit Native User
Basic
Permission Sets
Summary
Please assign permission sets to native user:
ADD ALL
REMOVE ALL
Unassigned (Available) Permission Sets
Administrator permission set
Reviewer permission set
Server assisted installation permission set
Permission Sets Assigned to Native User 'Amanda'
Reviewer permission set
Administrator permission set
Server assisted installation permission set
CONTINUE
FINISH
CANCEL

4.13.5.1.4 Dvojúrovňová autentifikácia

- Dvojúrovňová autentifikácia (2FA) poskytuje najbezpečnejšiu formu prihlásenia do ESMC Web Console.
- Dvojúrovňová autentifikácia je zabezpečená technológiou ESET Secure Authentication od spoločnosti ESET. ESET Secure Authentication nie je potrebné inštalovať, ESMC sa automaticky prihlási na servery spoločnosti ESET pre overenie používateľov, ktorí sa pokúšajú prihlásiť do ESMC Web Console.
- Používatelia, pre ktorých je povolená dvojúrovňová autentifikácia, sa musia prihlásiť do nástroja ESET Security Management Center pomocou ESET Secure Authentication.
- Bližšie informácie o funkciách a výhodách produktu ESET Secure Authentication nájdete na jeho stránke.
- Počet používateľov, ktorí sa môžu prihlásiť do ESMC pomocou dvojúrovňovej autentifikácie ESA, nie je obmedzený.

Prerekvizity

- Dvojúrovňovú autentifikáciu pre iného používateľa je možné zapnúť len v prípade, že máte pridelené povolenie na **zápis**, ktoré vám umožňuje robiť zmeny v nastaveniach daného používateľa. Akonáhle je táto funkcia zapnutá, daný používateľ si musí pred prihlásením do Web Console nastaviť dvojúrovňovú autentifikáciu. Cez SMS správu mu bude doručený odkaz, pomocou ktorého si zobrazí postup na nastavenie dvojúrovňovej autentifikácie.
- Dvojúrovňová autentifikácia nefunguje bez priameho prístupu k serverom dvojúrovňovej autentifikácie ESET. Je nevyhnutné povoliť vo firewalle aspoň určité servery dvojúrovňovej autentifikácie. Ak je nastavené proxy v sekcii **Viac** > **Nastavenia servera** > **Pokročilé nastavenia** > **HTTP proxy**, nevzťahuje sa na dvojúrovňovú autentifikáciu.

Poznámka:
Serverom asistovaná inštalácia nie je povolená pre používateľov s dvojúrovňovou autentifikáciou.

Ako zapnúť dvojúrovňovú autentifikáciu pre používateľa Web Console?

1. Vytvorte nového používateľa alebo použite existujúceho.
2. V ESMC Web Console prejdite do časti **Viac** > **Používatelia**.
3. Kliknite na ikonu vedľa používateľa.
4. Kliknite na **Dvojúrovňové overovanie** – **Zapnúť**.
5. Pri ďalšom prihlásení bude používateľ vyzvaný, aby zadal svoje telefónne číslo.
6. Nainštalujte mobilnú aplikáciu ESET Secure Authentication na mobilný telefón používateľa pomocou odkazu v SMS správe alebo QR kódu.
7. Ak sa aplikácia nainštaluje pomocou tokenu, vaša inštancia ESMC bude pridaná do aplikácie.
8. Pokračujte prihlásením a po výzve zadajte do Web Console jednorazové heslo vygenerované mobilnou aplikáciou. Nové heslo bude vygenerované mobilnou aplikáciou pri každom prihlásení.

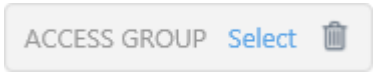
4.13.5.2 Sady povolení

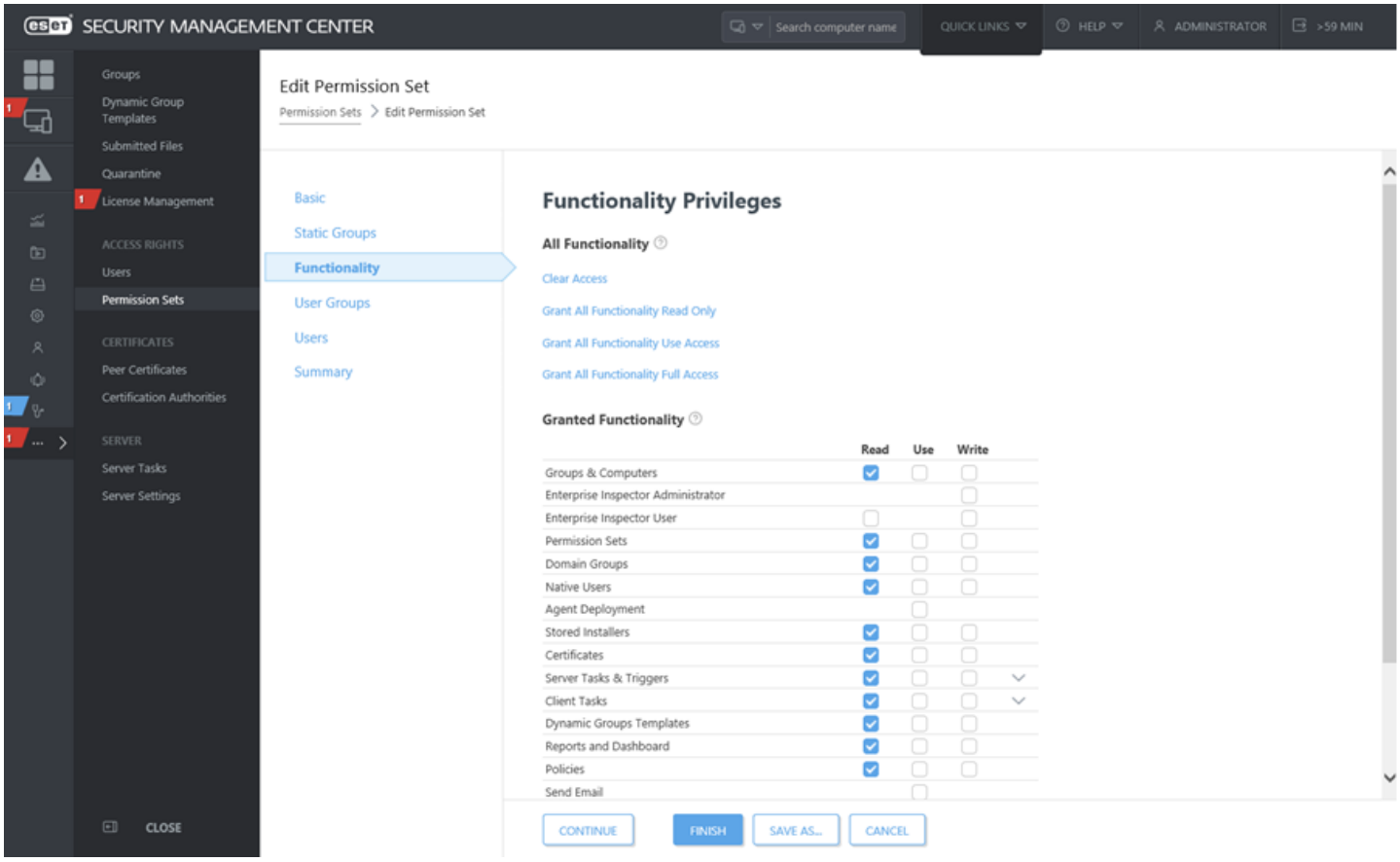
Sady povolení predstavujú oprávnenia používateľov, ktorí majú prístup do ESMC Web Console. Určujú, čo môže používateľ vo Web Console vidieť a robiť. Natívni používatelia majú svoje vlastné oprávnenia, kým doménoví používatelia majú oprávnenia, ktoré má pridelená ich namapovaná bezpečnostná skupina domény. Každá sada povolení sa uplatňuje na konkrétne statické skupiny. Povolenia zvolené v sekcii **Oprávnenia k funkciám** sa budú viazať len na tie objekty, ktoré sú obsiahnuté v statických skupinách zvolených v sekcii **Statické skupiny**. Všetci používatelia, ku ktorým bude táto sada povolení priradená, budú mať pridelené príslušné povolenia v rámci zvolených statických skupín. Mať prístup do statickej skupiny automaticky znamená mať prístup aj do každej jej podskupiny. Pre vzdialene pobočky firmy je možné vytvoriť samostatné statické skupiny, ku ktorým budú mať prístupové povolenia lokálni správcovia daných pobočiek (pozrite si príslušný príklad).

Používateľ môže mať pridelenú určitú sadu povolení aj bez toho, že by ju mohol vidieť. Sada povolení je v štruktúre ESMC tiež chápaná ako objekt a je vždy automaticky zahrnutá do domácej skupiny používateľa, ktorý ju vytvoril. To isté platí aj pri vytváraní nového používateľského účtu, používateľ (chápaný ako objekt) je automaticky umiestnený do domácej skupiny používateľa, ktorý tento nový účet vytvára. Používateľov zvyčajne vytvára hlavný správca (Administrator), takže sú zahrnutí v skupine *Všetko*.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.





Dôležité:
Pri práci s povoleniami je dobré dodržiavať nasledujúce zásady:

- Neskúseným používateľom nikdy neprideľujte prístupové práva k Nastaveniam servera – prístup k nim by mal mať iba hlavný správca.
- Zvážte obmedzenie prístupu k úlohe Spustiť príkaz v kategórii povolení **Úlohy pre klienta** – ide o úlohu so širokým využitím a veľkým dosahom, ktorá môže byť potenciálne zneužitá.
- Bežní používatelia, ktorí nie sú správcami, by nemali mať pridelené povolenia v rámci kategórií **Natívni používatelia**, **Sady povolení**, **Nastavenia servera**.
- Ak je vo vašom prípade potrebná komplexnejšia štruktúra povolení, je dobré vytvoriť väčší počet sád povolení a tie následne prideliť podľa potreby.

Okrem oprávnení týkajúcich sa funkcií ESMC je možné prideliť oprávnenia aj na prístup ku Skupinám používateľov (je možné zvoliť povolenie na **čítanie**, **použite** a **zápis**).

PRÍKLAD: DUPLIKOVANIE
Na duplikovanie určitého objektu musí mať používateľ pridelené povolenie na **čítanie** pre pôvodný objekt a mať povolenie na **zápis** v rámci svojej **Domácej skupiny** pre tento typ akcie.

John, ktorého domáca skupina je *Johnova skupina*, chce duplikovať objekt *Politika 1,* ktorý bol pôvodne vytvorený používateľom *Larry*, a je preto automaticky zahrnutý v Larryho domácej skupine nazvanej *Larryho skupina*.

1. Vytvorte novú statickú skupinu. Nazvite ju napr. *Zdieľané politiky*.
2. Obom používateľom, *Johnovi* aj *Larrymu*, prideľte sadu povolení, ktorá bude obsahovať povolenie na **čítanie** pre **Politiky** zahrnuté v statickej skupine *Zdieľané politiky*.
3. *Larry* presunie *Politiku 1* do skupiny *Zdieľané politiky*.
4. *Johnovi* prideľte povolenie na **zápis** pre **Politiky** zahrnuté v jeho domácej skupine.
5. *John* teraz môže **duplikovať** *Politiku 1* – duplikát tejto politiky sa objaví v jeho domácej skupine.

PRÍKLAD: ROZDIEL MEDZI POVOLENIAMI NA POUŽITIE A ZÁPIS
Ak *Správca* (Administrator) používateľovi s názvom *John* nechce povoliť upravovanie politík umiestnených v skupine *Zdieľané politiky*, musí vytvoriť sadu povolení s nasledujúcimi nastaveniami:

- Sekcia **Oprávnenia k funkciám**: povolenia na **čítanie** a **použitie** pre **Politiky**
- **Statické skupiny**: Zdieľané politiky

Ak má *John* pridelenú takúto sadu povolení, môže príslušné politiky používať, avšak nemôže ich upravovať, vymazávať a taktiež nemôže vytvárať nové politiky. Ak by správca používateľovi pridelil aj povolenie na **zápis**, John by v rámci zvolenej statickej skupiny *Zdieľané politiky* mohol vytvárať nové politiky a existujúce politiky duplikovať, upravovať a vymazávať.

4.13.5.2.1 Správa povolení

Ak chcete zmeniť nastavenia pre konkrétnu sadu povolení, kliknite na danú sadu povolení a potom kliknite na **Upraviť**. Kliknite na **Duplikovať** pre vytvorenie duplicitnej sady povolení, ktorú môžete následne upraviť a priradiť ku konkrétnemu používateľovi. Duplikát bude umiestnený do domácej skupiny používateľa, ktorý ho vytvoril.

Upozornenie:
Všetky predvolené sady povolení majú v sekcii **Statické skupiny** nastavenú skupinu **Všetko**. Používateľom preto tieto sady povolení prideľujte veľmi obozretne. Používatelia s týmito sadami povolení by disponovali oprávneniami vzťahujúcimi sa na všetky objekty v ESMC.

Základné

Zadajte **Názov** pre sadu povolení (povinné) a môžete prípadne zadať aj **Popis**.

Statické skupiny

Môžete pridať **Statickú skupinu** (alebo viacero statických skupín), na ktorú sa bude táto sada povolení aplikovať. Povolenia zvolené v sekcii **Oprávnenia k funkciám** sa budú viazať len na tie objekty, ktoré sú obsiahnuté v statických skupinách zvolených v tejto sekcii.

Funkcia

Vyberte jednotlivé funkcie Web Console, ku ktorým chcete povoliť prístup. Používateľ s prístupom k danej funkcii bude mať prístup aj ku všetkým súvisiacim úlohám. V rámci kategórií povolení Úlohy pre server a Úlohy pre klienta môžete pre jednotlivé typy úloh nastaviť rozličné povolenia. K dispozícii sú štyri preddefinované sady oprávnení k funkciám. Vyberte si jednu zo štyroch sád alebo zvoľte oprávnenia k funkciám manuálne pomocou začiarkavacích políčok.

Pridelenie práv na **zápis** automaticky udeľuje práva na **použitie** a **čítanie**; pridelenie práv na **použitie** automaticky udeľuje práva na **čítanie**.

Skupiny používateľov

Môžete pridať Skupinu používateľov (alebo viacero skupín používateľov), kde parametre používateľov patriacich do danej skupiny môžu byť použité v rámci politiky (napríklad ESET Mobile Device Management pre iOS alebo Režim prepísania).

Používatelia

Vyberte používateľa, ktorému má byť táto sada povolení pridelená. Všetci dostupní používatelia sú zobrazení naľavo. Označte konkrétnych používateľov alebo vyberte všetkých dostupných používateľov kliknutím na tlačidlo **Pridať všetko**. Priradení používatelia budú zobrazení napravo. Pri vytváraní sady povolení nemusíte zvoliť žiadneho používateľa, sadu povolení môžete ku konkrétnemu používateľovi priradiť aj neskôr.

Súhrn

Skontrolujte nastavenia povolení a kliknite na **Dokončiť**. Sada povolení bude uložená do domácej skupiny používateľa, ktorý ju vytvoril.

Kliknite na **Uložiť ako** pre vytvorenie novej šablóny na základe tej šablóny, ktorú práve upravujete. Bude potrebné, aby ste pre takto vytvorenú šablónu zadali nový názov.

4.13.5.2.2 Zoznam povolení

Typy povolení

Keď vytvárate alebo upravujete sadu povolení v sekcii **Viac** > **Sady povolení** > **Nová**/**Upraviť** > **Oprávnenia k funkciám**, k dispozícii máte kompletný zoznam všetkých dostupných povolení. Povolenia pre prístup k funkciám ESMC Web Console sú rozdelené do kategórií, napríklad: **Skupiny a Počítače**, **Natívni používatelia**, **Certifikáty**, **Politiky** atď. V rámci jednotlivých kategórií povolení môžete nastaviť, či má ísť o prístupové práva na **čítanie**, **použitie** alebo **zápis**. Vo všeobecnosti platí:

Čítanie – povolenia na čítanie sú vhodné pre používateľov vykonávajúcich kontrolu. Môžu vidieť údaje alebo nastavenia, ale nemôžu ich meniť.
Použitie – povolenia na použitie umožňujú používateľom používať objekty a spúšťať úlohy, avšak bez možnosti ich upravovať alebo mazať.
Zápis – povolenia na zápis umožňujú používateľom objekty upravovať, prípadne ich duplikovať.

Určité typy povolení (vymenované nižšie) sa vzťahujú na proces, nie objekt. To je dôvod, prečo povolenia fungujú na globálnej úrovni bez ohľadu na to, na ktorú statickú skupinu sa konkrétne povolenie vzťahuje. Ak je používateľovi umožnené využívať určitý proces, môže ho využívať len pre tie objekty, pre ktoré má dostatočné povolenia. Napríklad, povolenie na **Export správy do súboru** umožňuje využívať funkciu exportovania, avšak údaje obsiahnuté v správe sú podmienené ostatnými povoleniami.

Používateľom môžu byť pridelené povolenia pre nasledujúce procesy:

- **Enterprise Inspector Administrator**
- **Používateľ Enterprise Inspector**
- **Nasadenie agentov**
- **Správy a riadiace panely** (k dispozícii budú len funkcie riadiaceho panelu, použiteľné šablóny správ sú však stále závislé od dostupných statických skupín)
- **Odoslať e-mail**
- **Odoslať SNMP Trap**
- **Exportovať správu do súboru**
- **Nastavenia servera**

Kategórie prístupových povolení:

Skupiny a Počítače

Čítanie – zobrazovanie počítačov, skupín a počítačov vo vnútri skupiny.
Použitie – používanie počítača/skupiny ako cieľa určitej politiky alebo úlohy.
Zápis – pridávanie, úprava a odstraňovanie počítačov. Zaraďuje sa sem aj povolenie premenovať počítač alebo skupinu.

Enterprise Inspector Administrator

Zápis – vykonávanie správcovských funkcií v produkte Enterprise Inspector.

Používateľ Enterprise Inspector

Čítanie – prístup do produktu Enterprise Inspector len na čítanie.
Zápis – povolenie na čítanie a zápis v produkte Enterprise Inspector.

Sady povolení

Čítanie – prezeranie zoznamu sád povolení a zoznamu prístupových práv.
Použitie – priraďovanie existujúcich sád povolení konkrétnym používateľom a rušenie takéhoto priradenia.
Zápis – vytváranie, úprava a odstraňovanie sád povolení.

Dôležité:
Pre priradenie (alebo zrušenie priradenia) sady povolení k používateľovi je potrebné mať pridelené oprávnenia na **použitie** v rámci kategórií **Sady povolení** a **Natívni používatelia**.

Skupiny domény

Čítanie – zobrazovanie doménových skupín.
Použitie – priradenie/zrušenie priradenia sady povolení.
Zápis – vytváranie, úprava a odstraňovanie skupín domény.

Natívni používatelia

Čítanie – zobrazovanie natívnych používateľov.
Použitie – priradenie/zrušenie priradenia sady povolení.
Zápis – vytváranie, úprava a odstraňovanie natívnych používateľov.

Nasadenie agentov

Použitie – umožnenie prístupu k funkcii Nasadiť agenta prostredníctvom **Rýchlych odkazov** alebo umožnenie pridania klientskych počítačov manuálne v prostredí ESMC Web Console.

Uložené inštalátory

Čítanie – zobrazovanie uložených inštalátorov.
Použitie – exportovanie uložených inštalátorov.
Zápis – vytváranie, úprava a odstraňovanie uložených inštalátorov.

Certifikáty

Čítanie – prezeranie zoznamu partnerských certifikátov a certifikačných autorít.
Použitie – exportovanie certifikačných autorít a partnerských certifikátov a ich použitie pri práci s inštalátormi a príslušnými úlohami.
Zápis – vytváranie/rušenie partnerských certifikátov alebo certifikačných autorít.

Úlohy a spúšťače servera

Čítanie – prezeranie zoznamu úloh a ich nastavení (okrem citlivých položiek, ako sú napr. heslá).
Použitie – spustenie existujúcej úlohy pre server pomocou možnosti Vykonať teraz (ako používateľ aktuálne prihlásený do Web Console).
Zápis – vytváranie, úprava a odstraňovanie úloh pre server.
Túto kategóriu povolení je možné rozbaliť kliknutím na ⌄ a z ponuky môžete následne vybrať jeden alebo viacero typov úloh pre server.

Úlohy pre klienta

Čítanie – prezeranie zoznamu úloh a ich nastavení (okrem citlivých položiek, ako sú napr. heslá).
Použitie – naplánovanie vykonania úloh pre klienta alebo zrušenie ich vykonania. Pre priradenie úlohy (alebo pre zrušenie priradenia) na konkrétne ciele (počítače alebo skupiny) sa vyžaduje aj povolenie na použitie pre príslušné cieľové zariadenia alebo skupiny.
Zápis – vytváranie, úprava a vymazávanie úloh pre klienta. Pre priradenie úlohy (alebo pre zrušenie priradenia) na konkrétne ciele (počítače alebo skupiny) sa vyžaduje aj povolenie na **použitie** pre príslušné cieľové zariadenia alebo skupiny.
Túto kategóriu povolení je možné rozbaliť kliknutím na a z ponuky môžete následne vybrať jeden alebo viacero typov úloh pre klienta.

Šablóny dynamických skupín

Čítanie – prezeranie zoznamu šablón dynamických skupín.
Použitie – používanie existujúcich šablón pre dynamické skupiny.
Zápis – vytváranie, úprava a vymazávanie šablón dynamických skupín.

Správy a riadiace panely

Čítanie – zobrazovanie šablón správ a ich kategórií. Generovanie správ na základe šablón správ. Prezeranie vlastných riadiacich panelov založených na predvolených riadiacich paneloch.
Použitie – úprava vlastných riadiacich panelov s použitím dostupných šablón správ.
Zápis – vytváranie, úprava a vymazávanie šablón správ a ich kategórií. Upravovanie predvolených riadiacich panelov.

Politiky

Čítanie – prezeranie zoznamu politík a nastavení, ktoré obsahujú.
Použitie – priraďovanie existujúcich politík k cieľom (prípadne zrušenie tohto priradenia). Pre priradenie politiky k cieľom sa vyžaduje aj povolenie na **použitie** pre príslušné cieľové zariadenia alebo skupiny.
Zápis – vytváranie, úprava a vymazávanie politík.

Odoslať e-mail

Použitie – odosielanie e-mailov (využívané pri Oznámeniach a úlohe Generovať správu).

Odoslať SNMP Trap

Použitie – umožňuje odosielanie správy SNMP Trap (užitočné v rámci oznámení).

Exportovať správu do súboru

Použitie – umožňuje vám ukladať správy v súborovom systéme na serveri, na ktorom beží ESMC Server (využívané pri úlohe Generovať správu).

Licencie

Čítanie – prezeranie zoznamu licencií a štatistík ich používania.
Použitie – používanie licencií na aktiváciu.
Zápis – pridávanie a odstraňovanie licencií (ako domáca skupina používateľa musí byť nastavená skupina Všetko; podľa predvolených nastavení môže licencie pridávať a odstraňovať iba hlavný správca).

Oznámenia

Čítanie – prezeranie zoznamu oznámení a ich nastavení.
Zápis – vytváranie, úprava a vymazávanie oznámení. Pre prácu s oznámeniami sa môžu v závislosti od konfigurácie oznámení vyžadovať aj povolenia na **používanie** pre kategórie **Odoslať SNMP Trap** a **Odoslať e-mail**.

Nastavenia servera

Čítanie – prezeranie nastavení servera.
Zápis – upravovanie nastavení servera.

4.13.6 Certifikáty

Certifikáty sú dôležitou súčasťou produktu ESET Security Management Center. Sú potrebné na komunikáciu medzi ESMC komponentmi a ESMC Serverom. Aby mohli všetky komponenty komunikovať správne, všetky partnerské certifikáty musia byť platné a podpísané rovnakou certifikačnou autoritou.

V ESMC Web Console môžete vytvoriť novú **Certifikačnú autoritu** a **Partnerské certifikáty**. Ďalej postupujte podľa nasledujúcich inštrukcií:

- Vytvorenie novej certifikačnej autority
  - Import verejného kľúča
  - Export verejného kľúča
  - Export verejného kľúča vo formáte BASE64
- Vytvorenie partnerských certifikátov
  - Vytvorenie certifikátu
  - Export certifikátu
  - Vytvorenie APN certifikátu
  - Zneplatnenie certifikátu
  - Využitie certifikátu
  - Nastavenie nového certifikátu pre ESMC Server
  - Vlastné certifikáty pre ESET Security Management Center
  - Certifikát s končiacou platnosťou – hlásenie a nahradenie

Dôležité:
Operačný systém macOS/OS X nepodporuje certifikáty, ktorých platnosť skončí 19. januára 2038 a neskôr. ESET Management Agent bežiaci na operačnom systéme macOS/OS X nebude schopný pripojiť sa k ESMC Serveru.

Poznámka:
Pre všetky certifikáty a certifikačné autority vytvorené počas inštalácie súčastí nástroja ESMC musí byť hodnota „Platné od“ nastavená na 2 dni pred vytvorením certifikátu.

Pre všetky certifikáty a certifikačné autority vytvorené v ESMC Web Console musí byť hodnota „Platné od“ nastavená na 1 deň pred vytvorením certifikátu. Dôvodom je pokryť všetky možné časové odchýlky medzi všetkými dotknutými systémami.

Napríklad, certifikačná autorita a certifikát vytvorený 12. januára 2017 počas inštalácie bude mať prednastavenú hodnotu „Platné od“ na 10. január 2017 00:00:00 a certifikačná autorita a certifikát vytvorený 12. januára 2017 v ESMC Web Console bude mať prednastavenú hodnotu „Platné od“ na 11. január 2017 00:00:00.

4.13.6.1 Partnerské certifikáty

Ak sa vo vašom systéme nachádza Certifikačná autorita, mali by ste vytvoriť partnerský certifikát pre jednotlivé komponenty nástroja ESET Security Management Center. Každý z komponentov (ESET Management Agent a ESMC Server) vyžaduje špecifický certifikát.

+ Nová
Táto možnosť sa používa na vytvorenie nového certifikátu. Tieto certifikáty sa používajú pre ESET Management Agenta a ESMC Server.

+ APN/DEP certifikát
Táto možnosť sa používa na vytvorenie nového APN/DEP certifikátu. Tento certifikát je používaný nástrojom MDM. Použitie tejto možnosti vyžaduje platnú licenciu.

Využitie certifikátu
Môžete si pozrieť, ktoré klienty používajú tento ESMC certifikát.

Upraviť
Upravte certifikát zo zoznamu. Tieto nastavenia môžete definovať pri vytváraní nových certifikátov.

Exportovať
Táto možnosť sa používa na export certifikátu v podobe súboru. Tento súbor je potrebný pri inštalácii ESET Management Agenta lokálne na počítač alebo pri inštalácii MDM.

Exportovať ako Base64...
Táto možnosť sa používa na export certifikátu v podobe súboru `.txt`.

Zneplatniť
Ak už nechcete používať konkrétny certifikát, kliknite na **Zneplatniť**. Po použití tejto možnosti bude certifikát permanentne zneplatnený a zároveň vylúčený. Táto informácia bude odoslaná ESET Management Agentom pri ďalšom pripojení. Neplatné certifikáty nebudú akceptované nástrojom ESET Security Management Center.

Dôležité:
Pred zneplatnením certifikátu sa uistite, že ho už nepoužívajú žiadne ESET Management Agenty. Po zneplatnení certifikátu sa komponenty nebudú môcť pripojiť k ESMC Serveru. Pre obnovenie funkčnosti preinštalujte komponenty za použitia platného certifikátu.

Prístupová skupina
Certifikáty alebo certifikačné autority môžu byť presunuté do inej statickej skupiny. Stanú sa tak dostupnými pre používateľov, ktorí majú pre danú statickú skupinu pridelené dostatočné prístupové práva. Zistiť, v ktorej domácej skupine sa konkrétny certifikát nachádza, je veľmi jednoduché – stačí kliknúť na daný certifikát a zo zobrazeného roletového menu vybrať možnosť **Prístupová skupina**. Domáca skupina certifikátu je zobrazená v prvom riadku kontextovej ponuky (napríklad /All/San Diego. Prezrite si náš ukážkový scenár o zdieľaní prístupu k certifikátom).

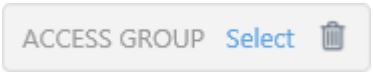
Dôležité:
Budú sa vám zobrazovať len tie certifikáty, ktoré sú umiestnené vo vašej domácej skupine (za predpokladu, že máte pridelené povolenia na **čítanie** certifikátov). Certifikáty vytvorené počas inštalácie ESMC sú zahrnuté v skupine **Všetko** a prístup k nim tak majú iba správcovia.

Zobraziť zrušené – zobrazí všetky vaše zrušené certifikáty.

Certifikát agenta pre serverom asistovanú inštaláciu – tento certifikát sa generuje počas inštalácie servera za predpokladu, že ste zvolili možnosť **Generovať certifikáty**.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom . Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

4.13.6.1.1 Vytvorenie nového certifikátu

Súčasťou inštalačného procesu je aj vytvorenie partnerského certifikátu pre ESET Security Management Center Agenty. Tieto certifikáty sa používajú na overovanie produktov distribuovaných pod vašou licenciou.

POZNÁMKA:
Jedinou výnimkou je, že **Certifikát agenta pre serverom asistovanú inštaláciu** nemôže byť vytvorený manuálne. Tento certifikát je generovaný počas inštalácie servera za predpokladu, že je zvolená možnosť **Generovať certifikáty**.

Pre vytvorenie nového certifikátu v ESMC **Web Console** prejdite do sekcie **Viac** > **Partnerské certifikáty** a kliknite na **Akcie** > **Nový**.

Základné

Popis – zadajte popis certifikátu.

Produkt – z roletového menu vyberte typ certifikátu, ktorý chcete vytvoriť.

Hostiteľ – v tomto poli ponechajte **predvolenú možnosť (hviezdičku)** pre umožnenie distribúcie certifikátu bez naviazania na konkrétny DNS názov alebo IP adresu.

Dôležité:
Pri vytváraní MDM certifikátu vyplňte IP adresu alebo hostiteľský názov MDM hostiteľského zariadenia. Predvolená hodnota (hviezdička) nie je platná pre tento typ certifikátu.

Prístupová fráza – odporúčame ponechať toto pole prázdne, môžete však zadať frázu (heslo), ktorá bude vyžadovaná pri aktivácii na klientskych zariadeniach.

Atribúty (predmet)

Vyplnenie týchto polí nie je povinné, môžete ich však použiť na zadanie podrobných informácií o certifikáte.

Spoločný názov – tento názov by mal obsahovať slová „agent“ alebo „server“, v závislosti od položky zvolenej v poli **Produkt**. V prípade potreby môžete zadať podrobnosti o certifikáte. Vyplňte polia **Platné od** a **Platné do** pre nastavenie doby platnosti certifikátu.

Poznámka:
Pre všetky certifikáty a certifikačné autority vytvorené počas inštalácie súčastí nástroja ESMC musí byť hodnota „Platné od“ nastavená na 2 dni pred vytvorením certifikátu.

Pre všetky certifikáty a certifikačné autority vytvorené v ESMC Web Console musí byť hodnota „Platné od“ nastavená na 1 deň pred vytvorením certifikátu. Dôvodom je pokryť všetky možné časové odchýlky medzi všetkými dotknutými systémami.

Napríklad, certifikačná autorita a certifikát vytvorený 12. januára 2017 počas inštalácie bude mať prednastavenú hodnotu „Platné od“ na 10. január 2017 00:00:00 a certifikačná autorita a certifikát vytvorený 12. januára 2017 v ESMC Web Console bude mať prednastavenú hodnotu „Platné od“ na 11. január 2017 00:00:00.

Podpísať

Vyberte si jednu z dvoch metód podpisovania certifikátov:

- **Certifikačná autorita** – v prípade, že si želáte vykonať podpísanie pomocou **ESMC Certifikačnej autority** (vytvorenej počas inštalácie ESMC).
  - Vyberte **ESMC Certifikačnú autoritu** zo zoznamu certifikačných autorít.
  - Vytvorenie novej certifikačnej autority
- **Vlastný pfx súbor** – pre použitie vlastného `.pfx` súboru kliknite na **Prechádzať**, vyhľadajte svoj `.pfx` súbor a kliknite na **OK**. Vyberte možnosť **Odovzdať**, čím odošlete tento certifikát na server. Nie je možné použiť vlastný certifikát.

POZNÁMKA:
Ak chcete podpísať nový certifikát ESMC Certifikačnou autoritou (vytvorenou počas inštalácie ESMC) vo Virtuálnom zariadení ESMC, je potrebné zadať **Prístupovú frázu certifikačnej autority**. Ide o heslo, ktoré ste zadali počas konfigurácie Virtuálneho zariadenia ESMC.

Súhrn

Skontrolujte súhrn informácií o certifikáte a kliknite na **Dokončiť**. Po úspešnom vytvorení bude certifikát dostupný v zozname **Certifikátov**, ktoré je možné použiť pri inštalácii agenta. Novovytvorený certifikát bude umiestnený vo vašej domácej skupine.

POZNÁMKA:
Alternatívou vytvorenia nového certifikátu je import verejného kľúča, export verejného kľúča alebo export partnerského certifikátu.

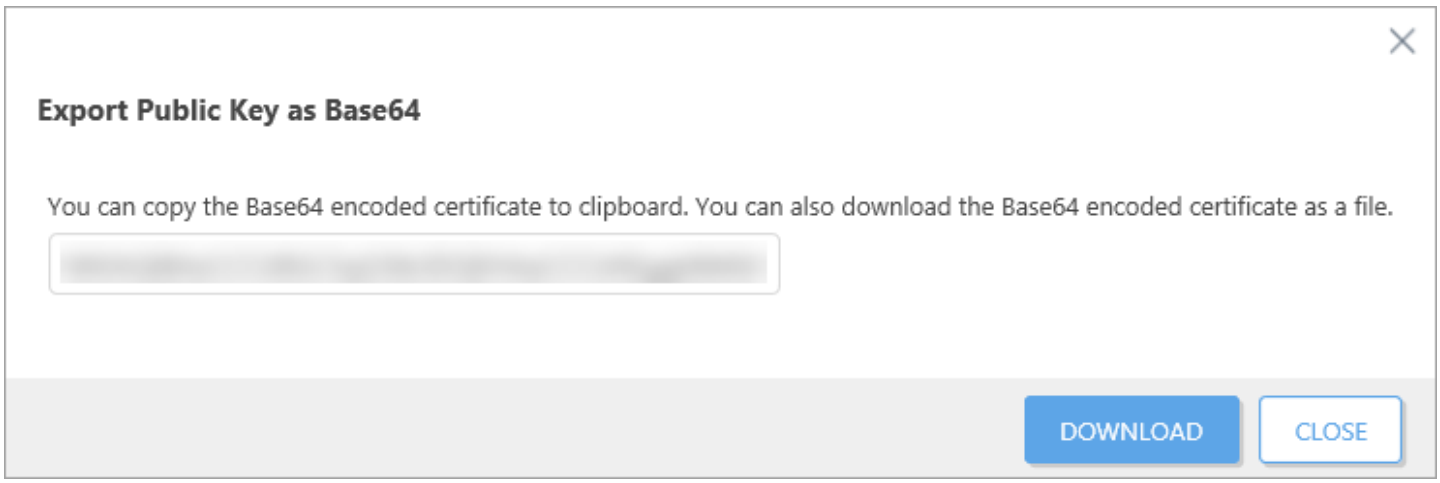
4.13.6.1.2 Export partnerského certifikátu

Export partnerských certifikátov

1. Vyberte **partnerský certifikát** zo zoznamu a kliknite na začiarkavacie políčko vedľa jeho názvu.
2. Z kontextového menu vyberte možnosť **Exportovať**. Certifikát bude exportovaný (vrátane privátneho kľúča) ako `.pfx` súbor. Zadajte názov pre váš verejný kľúč a kliknite na **Uložiť**.

Export partnerských certifikátov vo formáte Base64

Certifikáty pre komponenty ESMC sú dostupné v nástroji Web Console. Pre skopírovanie obsahu certifikátu vo formáte Base64 kliknite na **Viac** > **Partnerské certifikáty**, vyberte certifikát a zvoľte možnosť **Exportovať ako Base64**. Certifikát môžete stiahnuť aj ako súbor. Tento postup zopakujte pre všetky certifikáty komponentov, ako aj pre certifikačnú autoritu.



Poznámka:
Ak používate vlastné certifikáty, ktoré nie sú vo formáte **Base64**, bude potrebné ich **skonvertovať** na formát **Base64** (prípadne môžete tieto certifikáty exportovať podľa popisu vyššie). Toto je jediný akceptovaný formát v rámci pripojenia komponentov ESMC k ESMC Serveru. Podrobnejšie informácie o konvertovaní certifikátov nájdete v príslušných príručkách pre Linux a OS X. Napríklad:

```
'cat ca.der | base64 > ca.base64.txt'
'cat agent.pfx | base64 > agent.base64.txt'
```

4.13.6.1.3 APN/DEP certifikát

ESMC MDM používa na registráciu iOS zariadení certifikát APN (Apple Push Notification), prípadne certifikát DEP (Device Enrollment Program). Pred samotnou registráciou iOS zariadení do ESMC je potrebné vytvoriť a podpísať **APN certifikát** na príslušnom portáli spoločnosti Apple. Pre vytvorenie certifikátu sa vyžaduje platná licencia pre ESMC.

Kliknite na **Viac** > **Partnerské certifikáty**, ďalej kliknite na **Nový** a potom vyberte možnosť **APN/DEP certifikát**.

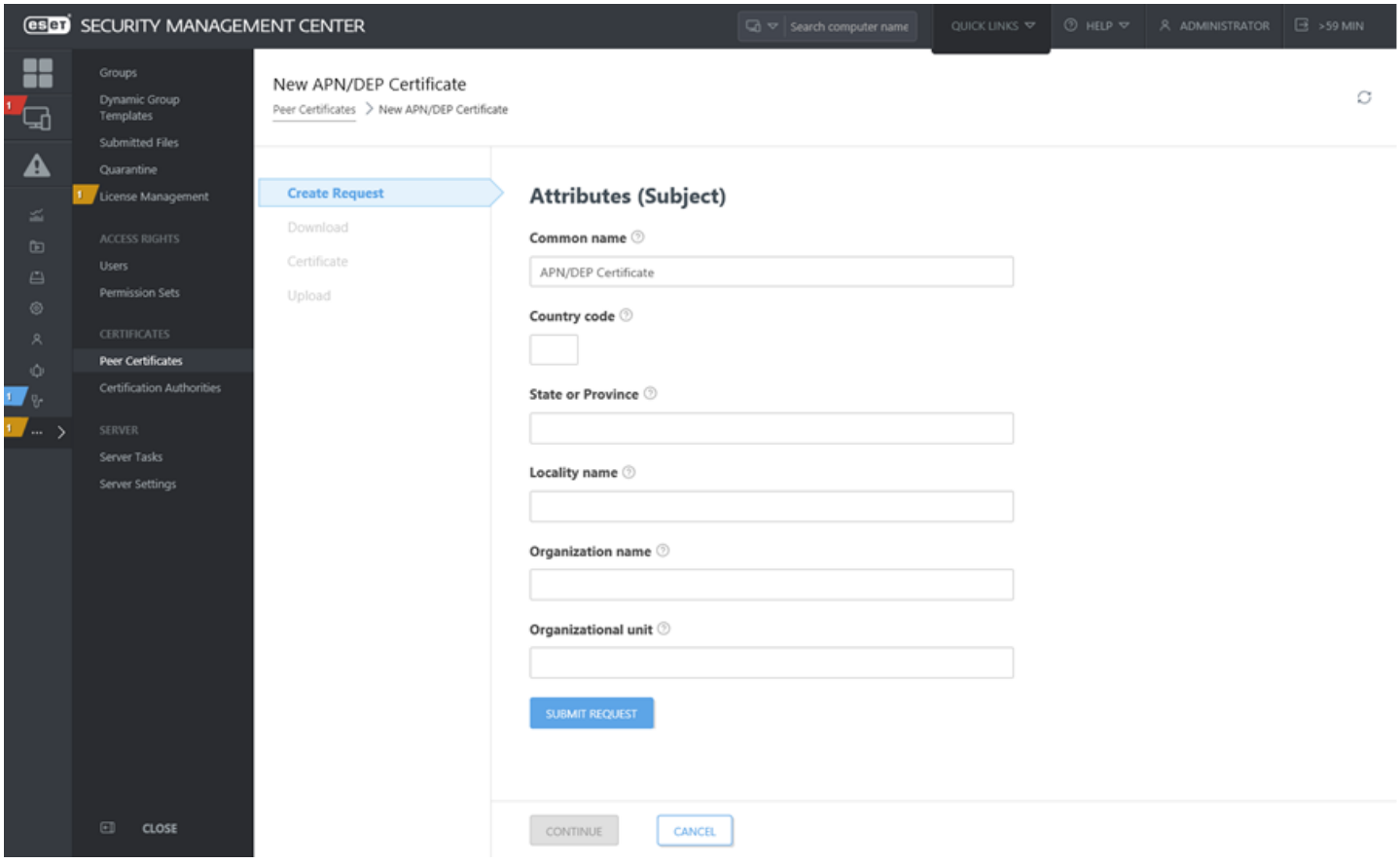
Poznámka:
Pre získanie APN certifikátu budete potrebovať Apple ID. Apple ID je potrebné pre prihlásenie do portálu Apple Push Certificates Portal, na ktorom je APN certifikát podpísaný spoločnosťou Apple.

APN certifikát má platnosť 1 rok. Ak sa blíži dátum vypršania platnosti vášho certifikátu, postupujte podľa krokov nižšie a v kroku č. 2 sekcie „Certifikát“ vyberte možnosť **Renew** (Obnoviť).

Pre získanie registračného Apple DEP tokenu musíte mať vytvorený Apple DEP účet.

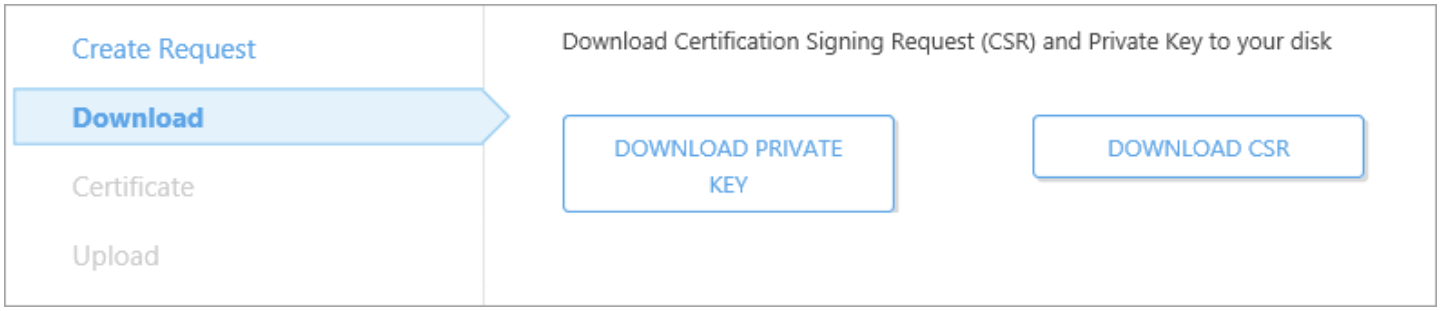
Vytvoriť požiadavku

Zadajte atribúty certifikátu (kód krajiny, názov organizácie atď.) a kliknite na **Odoslať požiadavku**.



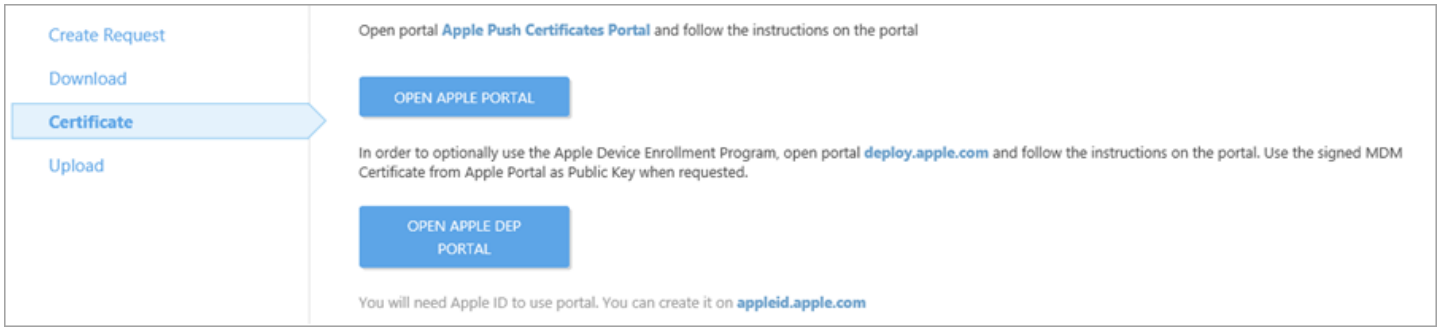
Stiahnuť

Stiahnite si váš **CSR** súbor (Certification Signing Request – Požiadavka na podpísanie certifikátu) súbor a **Privátny kľúč**.



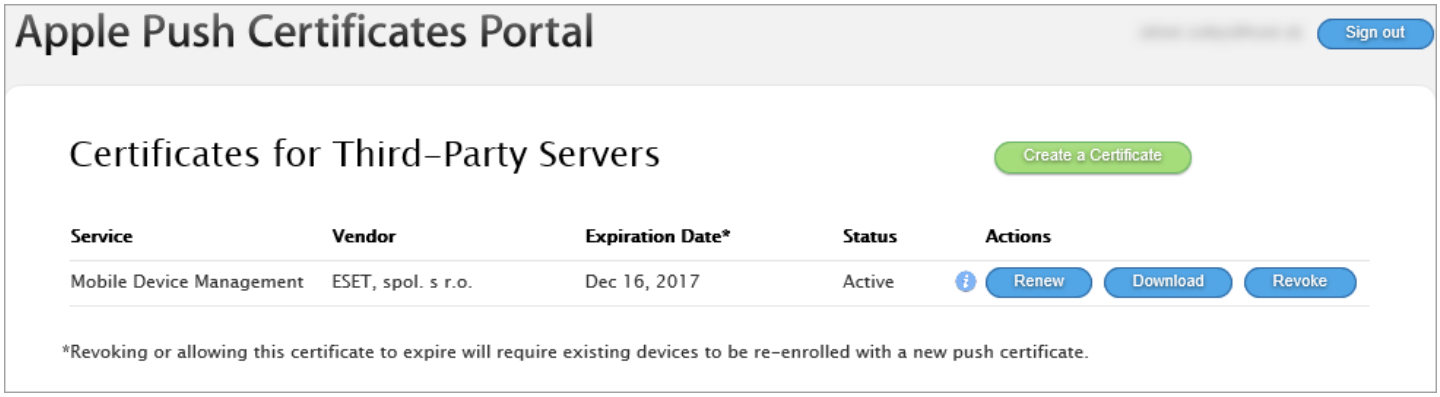
Certifikát

1. Otvorte Apple Push Certificates Portal a prihláste sa pomocou vášho Apple ID.
2. Pre vytvorenie certifikátu kliknite na možnosť **Create a Certificate**.
3. Voliteľne je možné zadať poznámku. Kliknite na možnosť **Choose File** (Vybrať súbor), vyhľadajte CSR súbor, ktorý ste stiahli v predchádzajúcom kroku, a kliknite na **Upload** (Odovzdať).
4. Po chvíli sa na obrazovke zobrazí potvrdenie o úspešnom vytvorení APNS certifikátu pre ESET Mobile Device Management Server.
5. Kliknite na **Download** (Stiahnuť) a APNS certifikát v podobe `.pem` súboru uložte do svojho počítača.
6. Zatvorte Apple Push Certificate Portal a prejdite nižšie do sekcie Upload (Odovzdať).



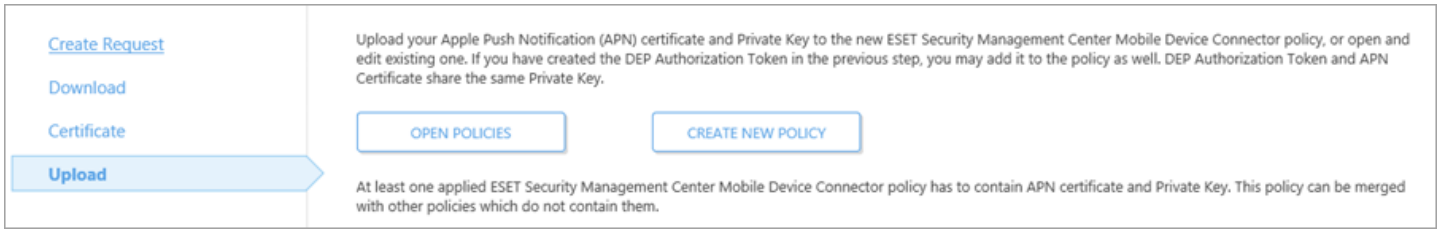
Dôležité:
APNS certifikát bude potrebné zadať pri vytváraní politiky pre nástroj ESET Mobile Device Connector pre umožnenie registrácie zariadení iOS prostredníctvom programu Apple DEP, ako aj registrácie klasickým spôsobom.

Ak vytvárate registračný certifikát DEP (Apple DEP Token), pokračujte podľa inštrukcií v tejto kapitole.



Odovzdať

Po vykonaní krokov uvedených vyššie môžete vytvoriť politiku pre MDC na aktiváciu APNS pre umožnenie registrácie zariadení iOS. Následne môžete registrovať akékoľvek iOS zariadenie tak, že navštívite adresu *https://<mdmcore>:<enrollmentport>/unique_enrollment_token* z prehliadača zariadenia.

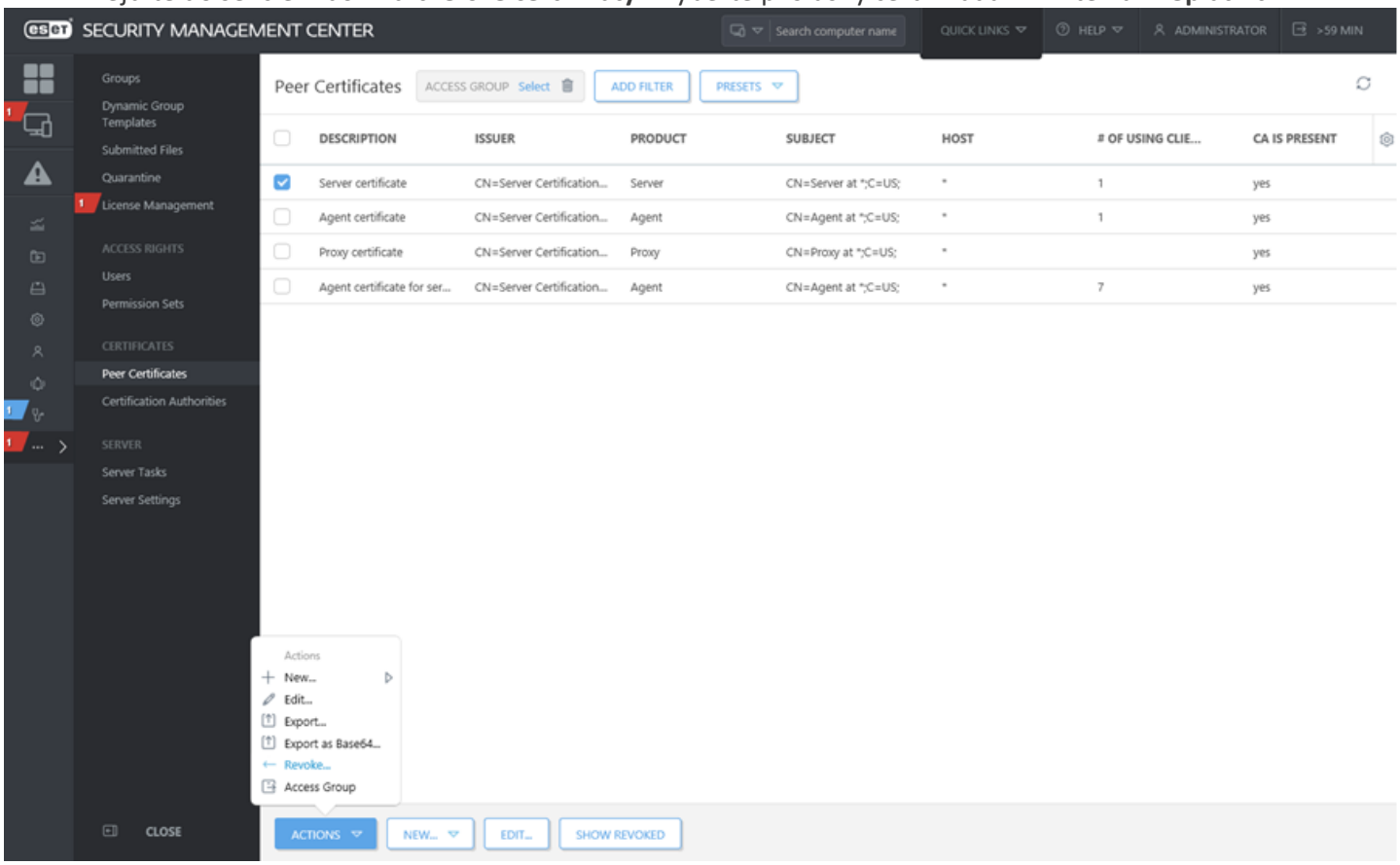


4.13.6.1.4 Zneplatnenie certifikátu

Zoznam „Zobraziť zrušené“ obsahuje všetky certifikáty, ktoré boli vytvorené a následne zneplatnené/zrušené ESMC Serverom. Zrušené certifikáty budú automaticky odstránené z hlavnej obrazovky **Partnerské certifikáty**. Kliknutím na tlačidlo **Zobraziť zrušené** zobrazíte certifikáty, ktoré boli zrušené v hlavnom okne.

Pre zrušenie/zneplatnenie certifikátu postupujte podľa nasledujúcich krokov:

1. Prejdite do sekcie **Viac** > **Partnerské certifikáty** > vyberte príslušný certifikát a kliknite na **Zneplatniť**.

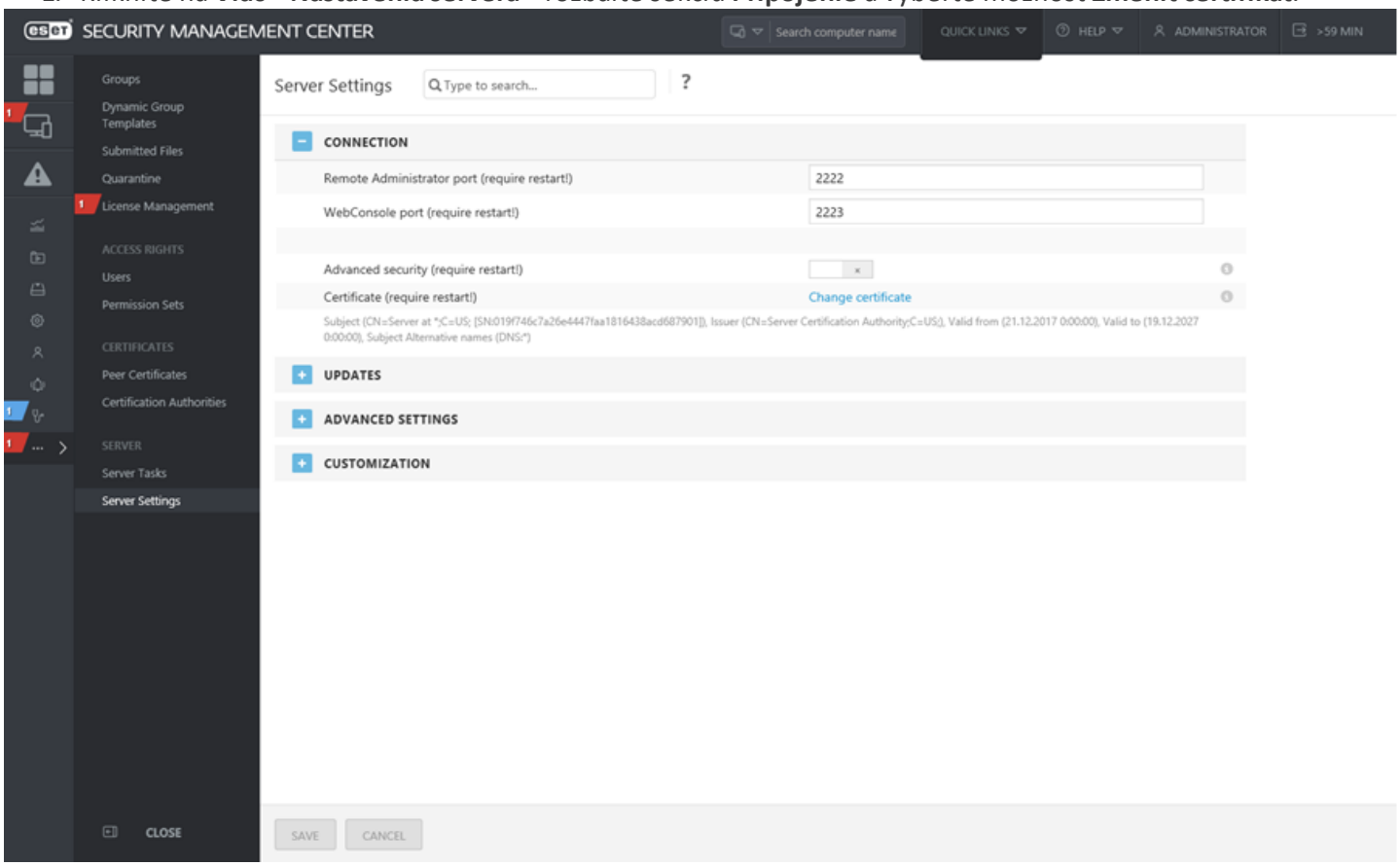


2. Zadajte **Dôvod** zneplatnenia a kliknite na **Zneplatniť**.
3. Kliknite na **OK**. Certifikát sa vymaže zo zoznamu partnerských certifikátov. Pre zobrazenie zneplatnených/zrušených certifikátov kliknite na tlačidlo **Zobraziť zrušené**.

4.13.6.1.5 Nastavenie nového certifikátu pre ESMC Server

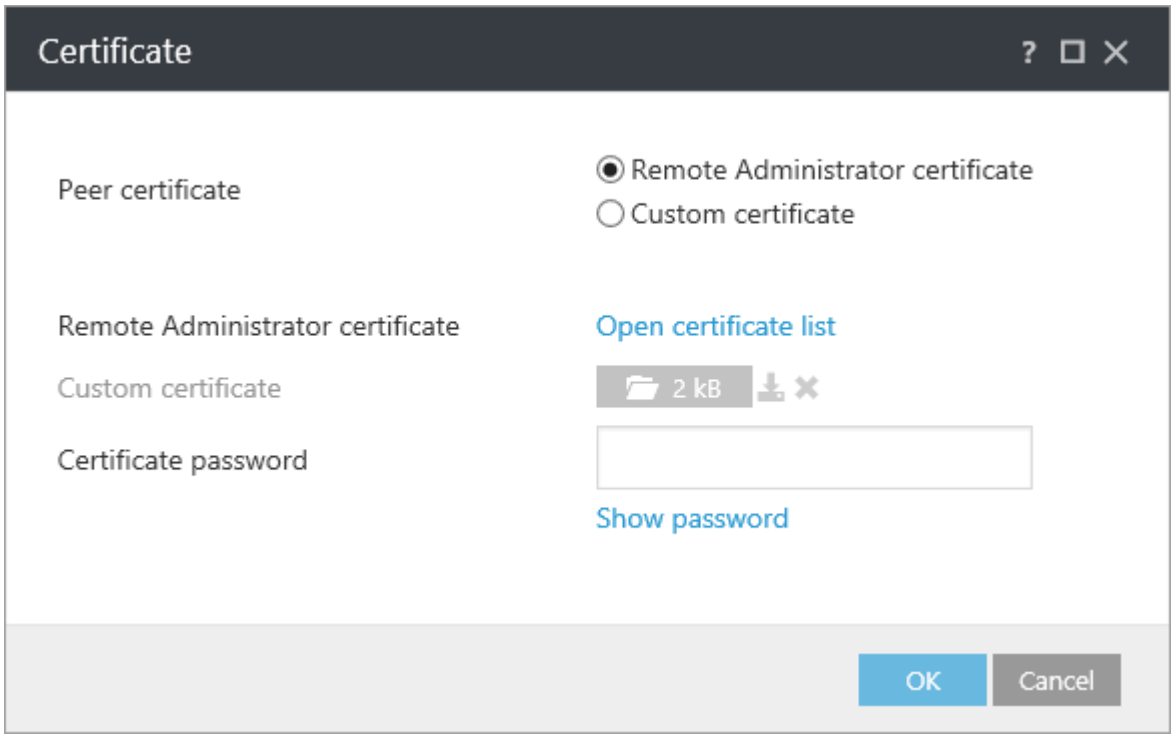
Váš certifikát ESMC Servera je vytvorený pri inštalácii a je distribuovaný na ESET Management Agenty a ostatné komponenty, aby mohli s ESMC Serverom komunikovať. V prípade potreby môžete nastaviť ESMC Server tak, aby používal odlišný partnerský certifikát. Okrem certifikátu ESMC Servera (vytvoreného automaticky pri inštalácii) teda môžete použiť aj **Vlastný certifikát.** Certifikát ESMC Servera je potrebný na zabezpečené TLS pripojenie a overovanie. Certifikát servera zabezpečí, že ESET Management Agenty a ESMC Proxy sa nepripoja na žiadny iný (nedôveryhodný) server. Pre zmenu nastavení certifikátu kliknite na **Nástroje** > **Nastavenia servera**.

1. Kliknite na **Viac** > **Nastavenia servera** > rozbaľte sekciu **Pripojenie** a vyberte možnosť **Zmeniť certifikát**.



2. Vyberte si z dvoch typov partnerského certifikátu:

- **Remote Administrator certifikát** – kliknite na **Otvoriť certifikát** a vyberte certifikát, ktorý bude použitý.
- **Vlastný certifikát** – prejdite do umiestnenia vášho vlastného certifikátu. Pri vykonávaní migrácie vyberte certifikát exportovaný z vášho starého ESMC Servera.



3. Vyberte **Vlastný certifikát**, ďalej vyberte certifikát ESMC Servera exportovaný zo starého servera v podobe súboru `.pfx` a kliknite na **OK**.
4. **Reštartujte** službu ESMC Server. Bližšie informácie nájdete v nasledujúcom článku databázy znalostí.

4.13.6.1.6 Vlastné certifikáty pre ESET Security Management Center

Ak máte svoju vlastnú PKI (infraštruktúru verejných kľúčov) a chcete, aby ESET Security Management Center používal vaše vlastné certifikáty na komunikáciu medzi jednotlivými komponentmi, pozrite si príklad nižšie. Tento príklad bol vykonaný na systéme Windows Server 2012 R2. Niektoré obrazovky sa môžu do malej miery líšiť v závislosti od konkrétnej verzie operačného systému Windows, avšak cieľ tohto postupu ostáva rovnaký.

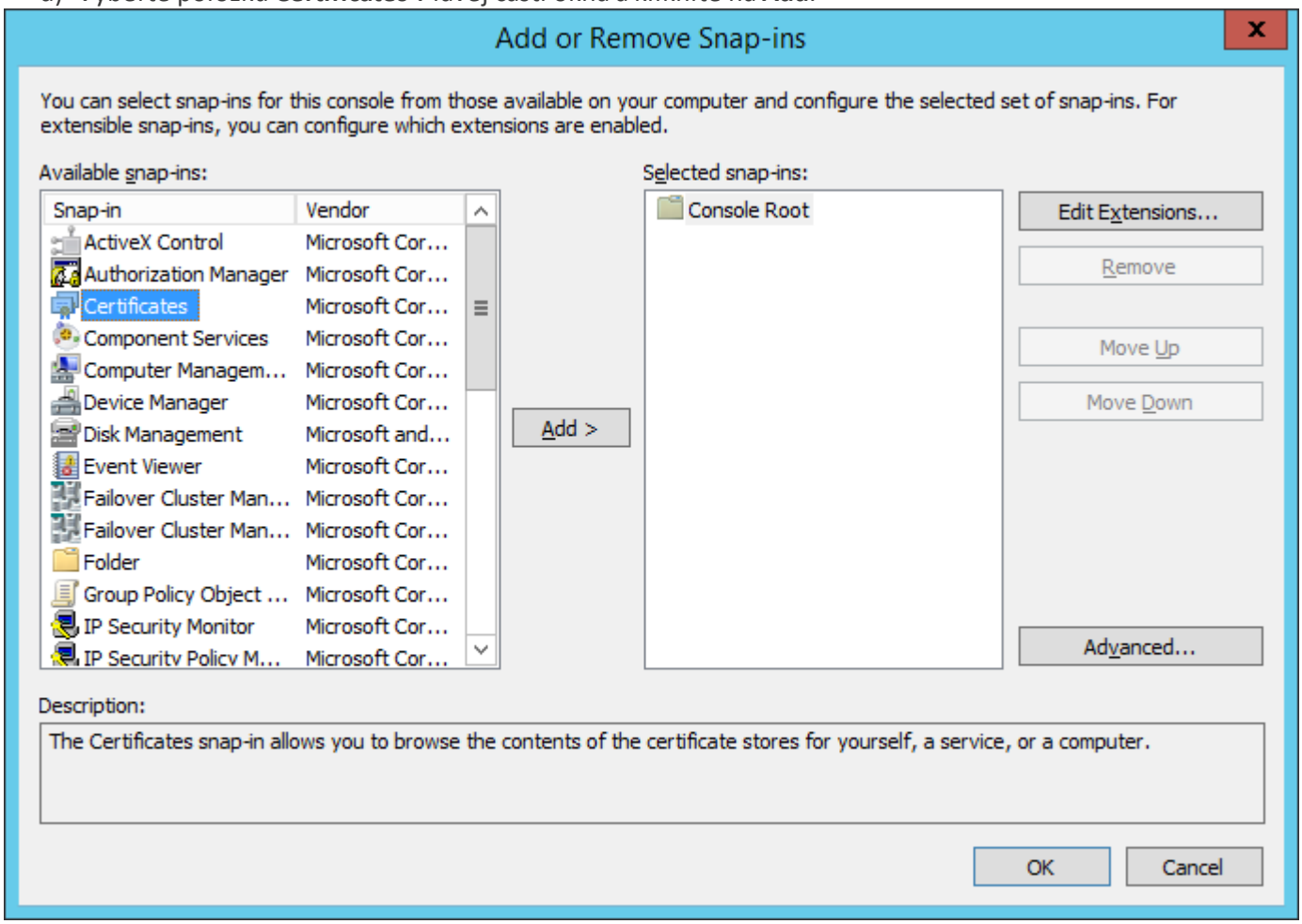
Poznámka:
Pre rýchle a jednoduché vytvorenie nových certifikátov použite nástroj keytool, ktorý je súčasťou Javy. Viac informácií nájdete v nasledujúcom článku databázy znalostí spoločnosti ESET.

Požadované serverové roly:

- Active Directory Domain Services.
- Active Directory Certificate Services s nainštalovanou samostatnou koreňovou certifikačnou autoritou.

1. Otvorte **Management Console** a pridajte snap-in **Certificates**:

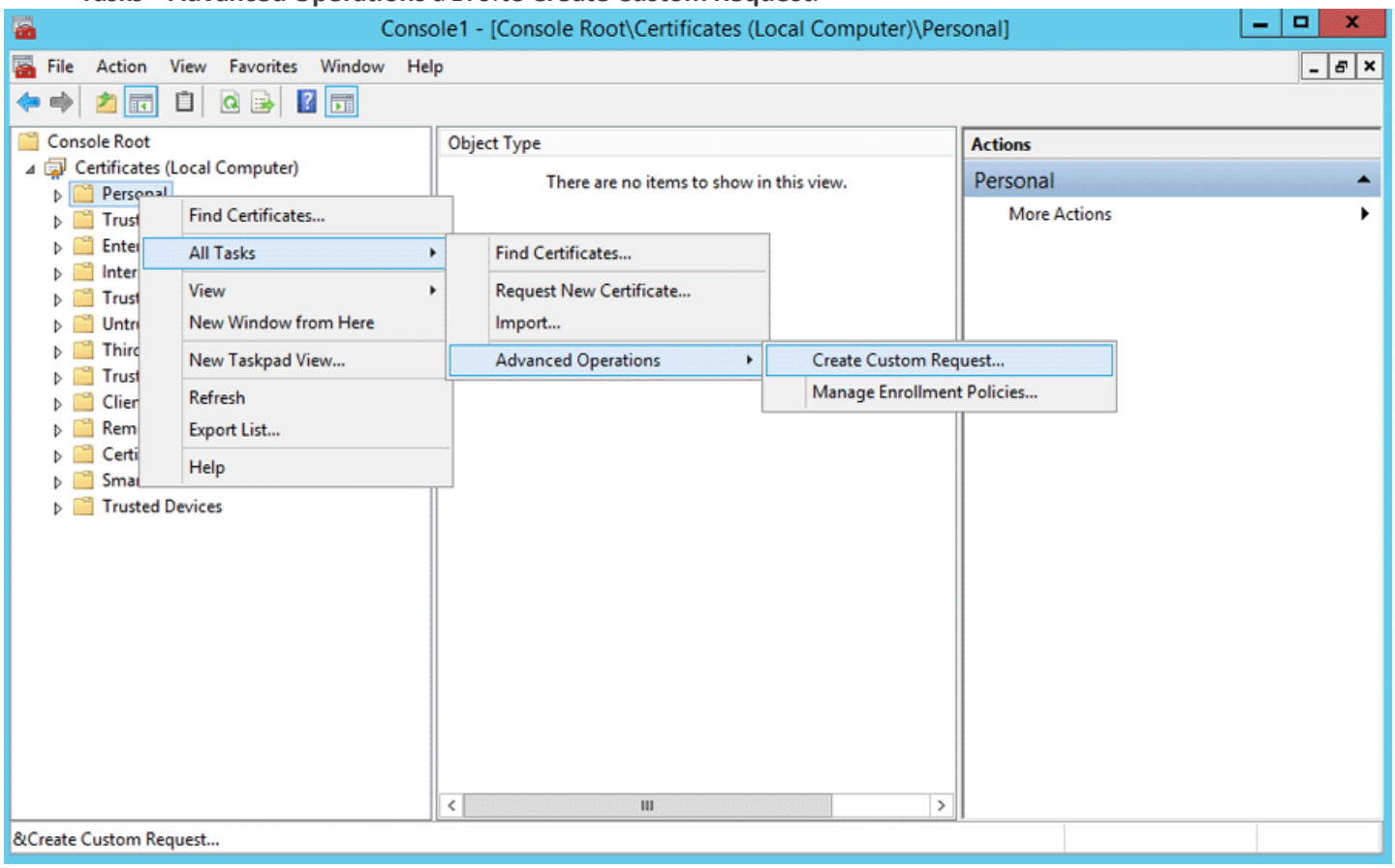
a) Prihláste sa na server ako člen lokálnej skupiny správcov.
b) **Spustite** Management Console pomocou príkazu mmc.exe.
c) Kliknite na **File** a vyberte možnosť **Add/Remove Snap-in…** (prípadne použite klávesovú skratku CTRL + M).
d) Vyberte položku **Certificates** v ľavej časti okna a kliknite na **Add**.



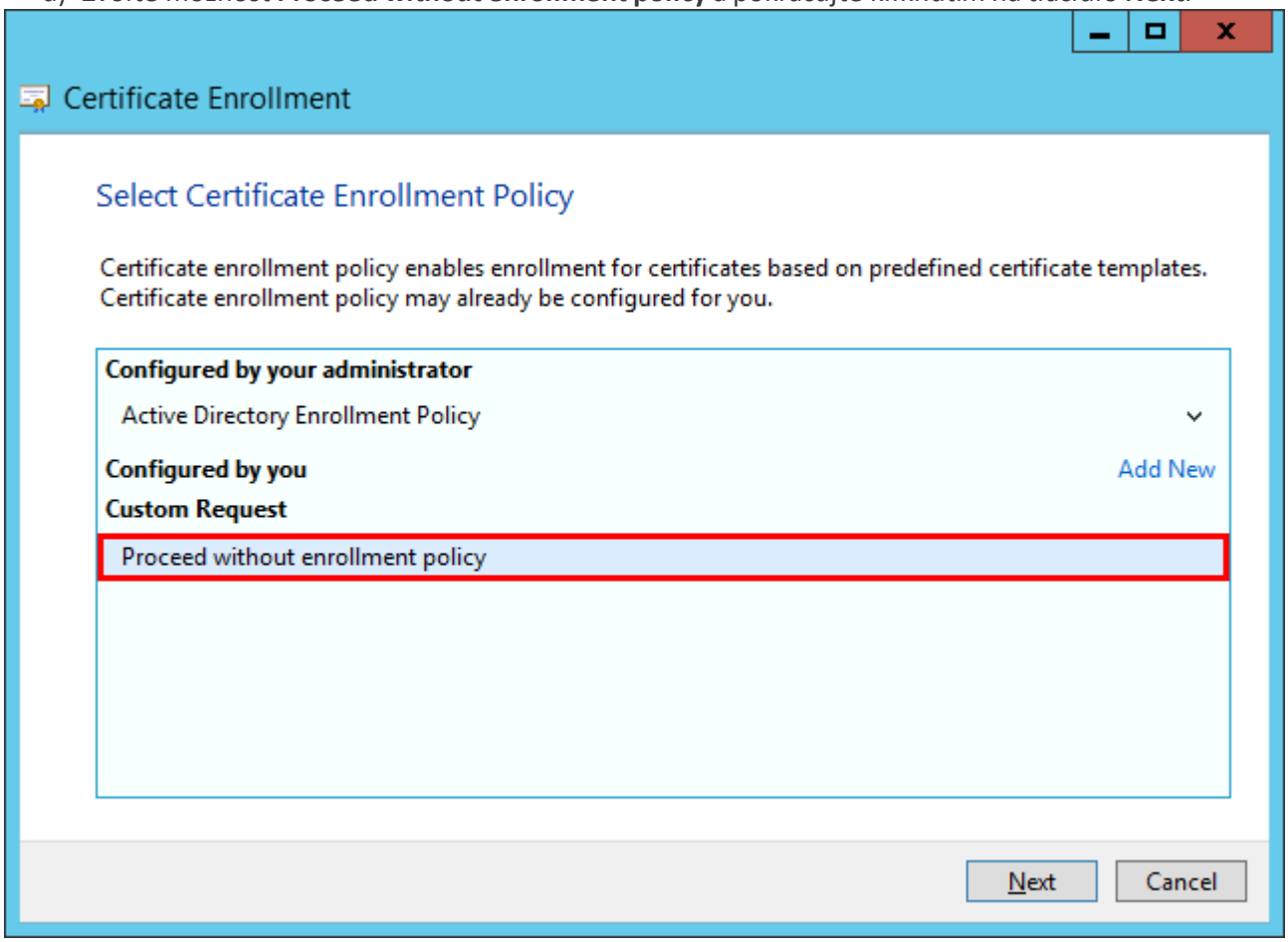
e) Zvoľte možnosť **Computer Account** a kliknite na **Next**.
f) Uistite sa, že ste zvolili možnosť **Local Computer** a kliknite na tlačidlo **Finish**.
g) Kliknite na **OK**.

2. Vytvorte **Custom Certificate Request**:

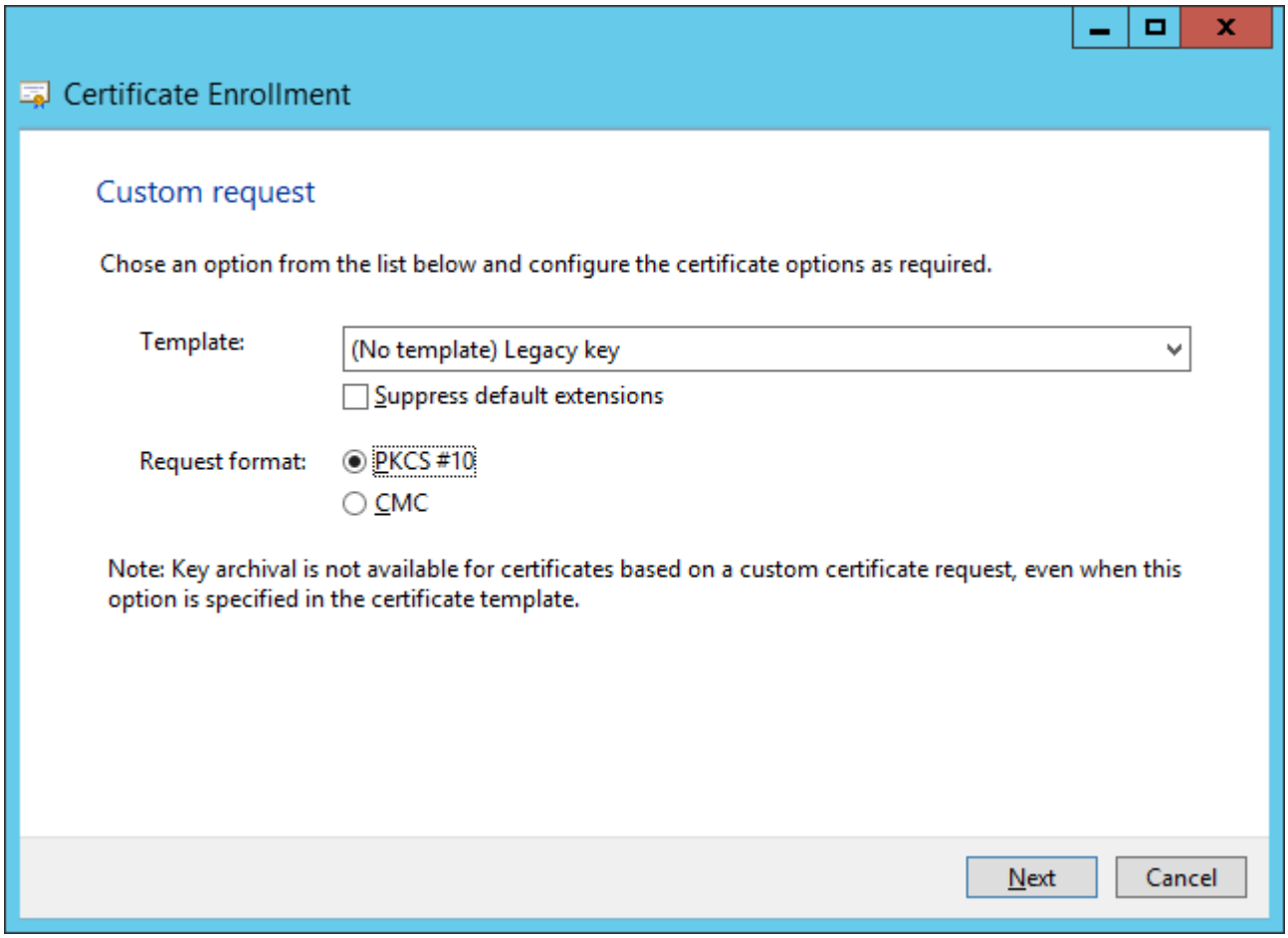
a) Dvojitým kliknutím rozbaľte ponuku **Certificates (Local Computer)**.
b) Dvojitým kliknutím rozbaľte ponuku **Personal**. Pravým tlačidlom kliknite na **Certificates**, vyberte možnosť **All Tasks** > **Advanced Operations** a zvoľte **Create Custom Request**.



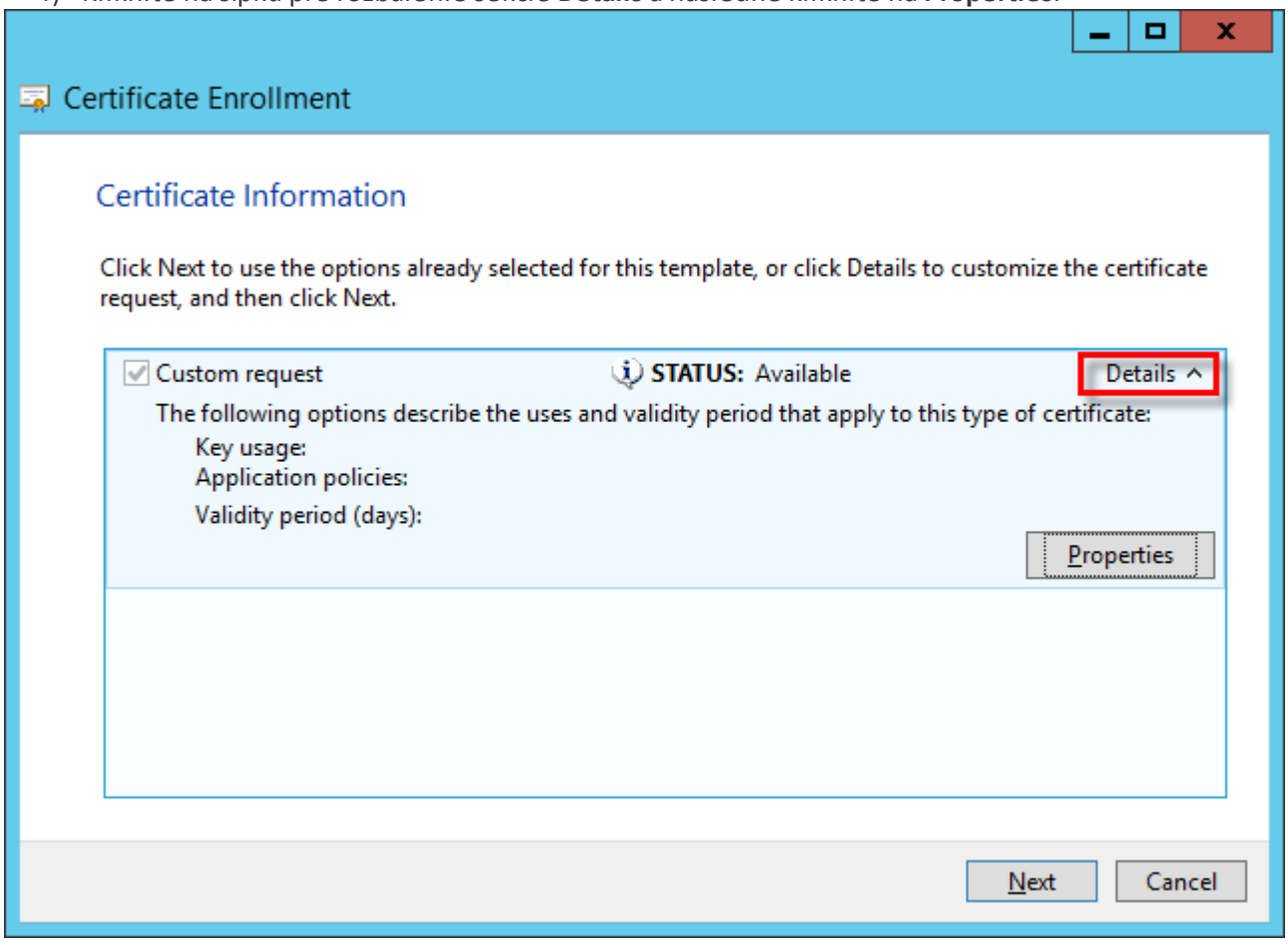
c) V okne sprievodcu pre registráciu certifikátu kliknite na **Next**.
d) Zvoľte možnosť **Proceed without enrollment policy** a pokračujte kliknutím na tlačidlo **Next**.



e) Z roletového menu vyberte možnosť **(No Template) Legacy Key** a uistite sa, že máte vybratý formát **PKCS #10**. Kliknite na **Next**.



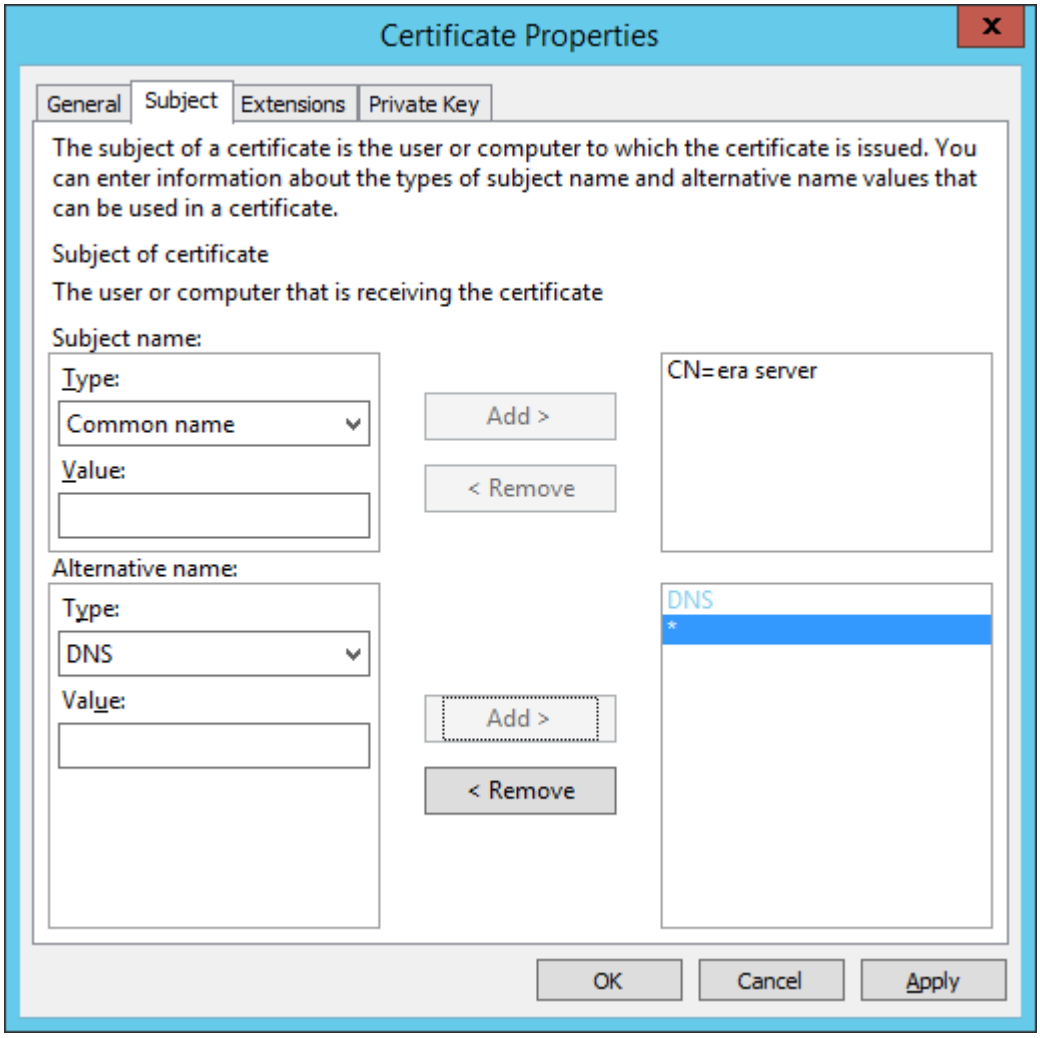
f) Kliknite na šípku pre rozbalenie sekcie **Details** a následne kliknite na **Properties**.



g) Na karte **General** zadajte **Friendly name** pre váš certifikát, pričom môžete zadať aj popis.
h) Na karte **Subject** vykonajte nasledovné:

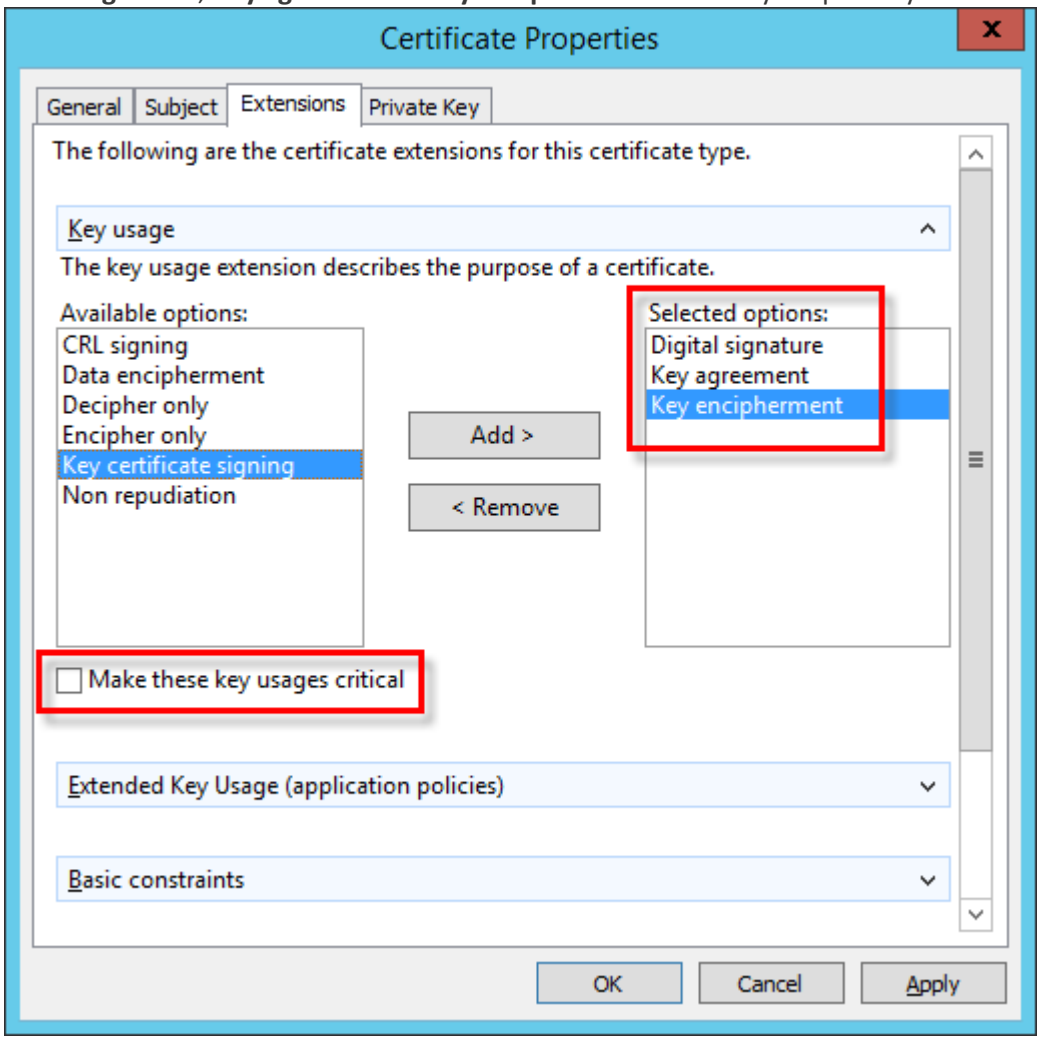
V sekcii **Subject name** vyberte z roletového menu **Type** položku **Common Name**. Zadajte `era server` ako hodnotu do poľa **Value** a kliknite na **Add**. **CN=era server** sa následne zobrazí ako informácia v poli napravo. Ak vytvárate žiadosť o vydanie certifikátu pre ESET Management Agenta, do poľa hodnoty pre Common name zadajte `era agent`.

Poznámka:
Common Name musí obsahovať jeden z nasledujúcich reťazcov v závislosti od toho, aký Certificate Request chcete vytvoriť: „**server**“ alebo „**agent**“.



i) V sekcii **Alternative name** vyberte z roletového menu **Type** položku **DNS**. Zadajte * (hviezdičku) ako hodnotu do poľa **Value** a kliknite na tlačidlo **Add**.

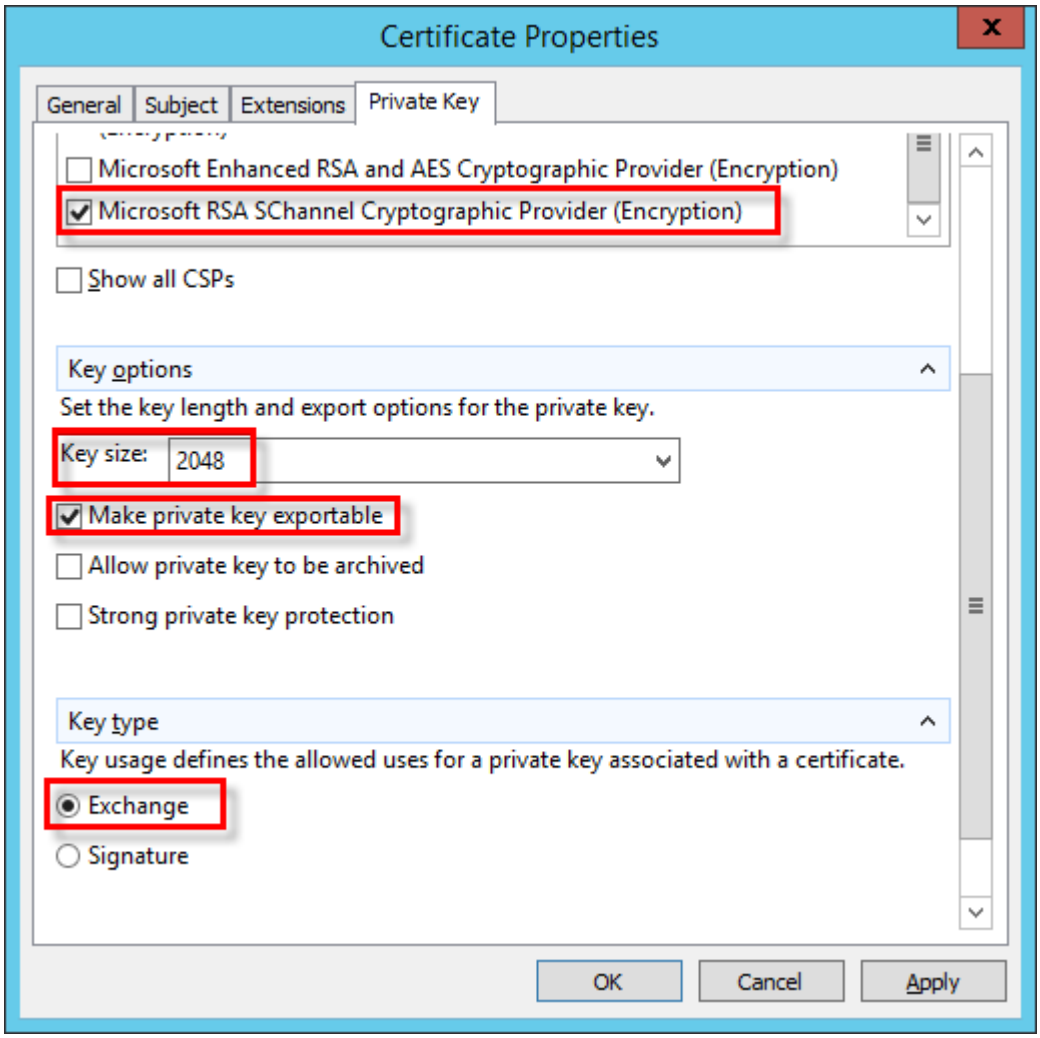
j) Na karte **Extensions** rozbaľte sekciu **Key usage** kliknutím na šípku**.**Vyberte nasledujúce položky: **Digital signature**, **Key agreement** a **Key encipherment**.Zrušte výber položky **Make these key usages critical**.



k) Na karte **Private Key** vykonajte nasledovné:

Rozbaľte sekciu **Cryptographic Service Provider**. Následne sa zobrazí zoznam všetkých poskytovateľov kryptografických služieb (CSP). Uistite sa, že je zvolená iba položka **Microsoft RSA SChannel Cryptographic Provider (Encryption)**.

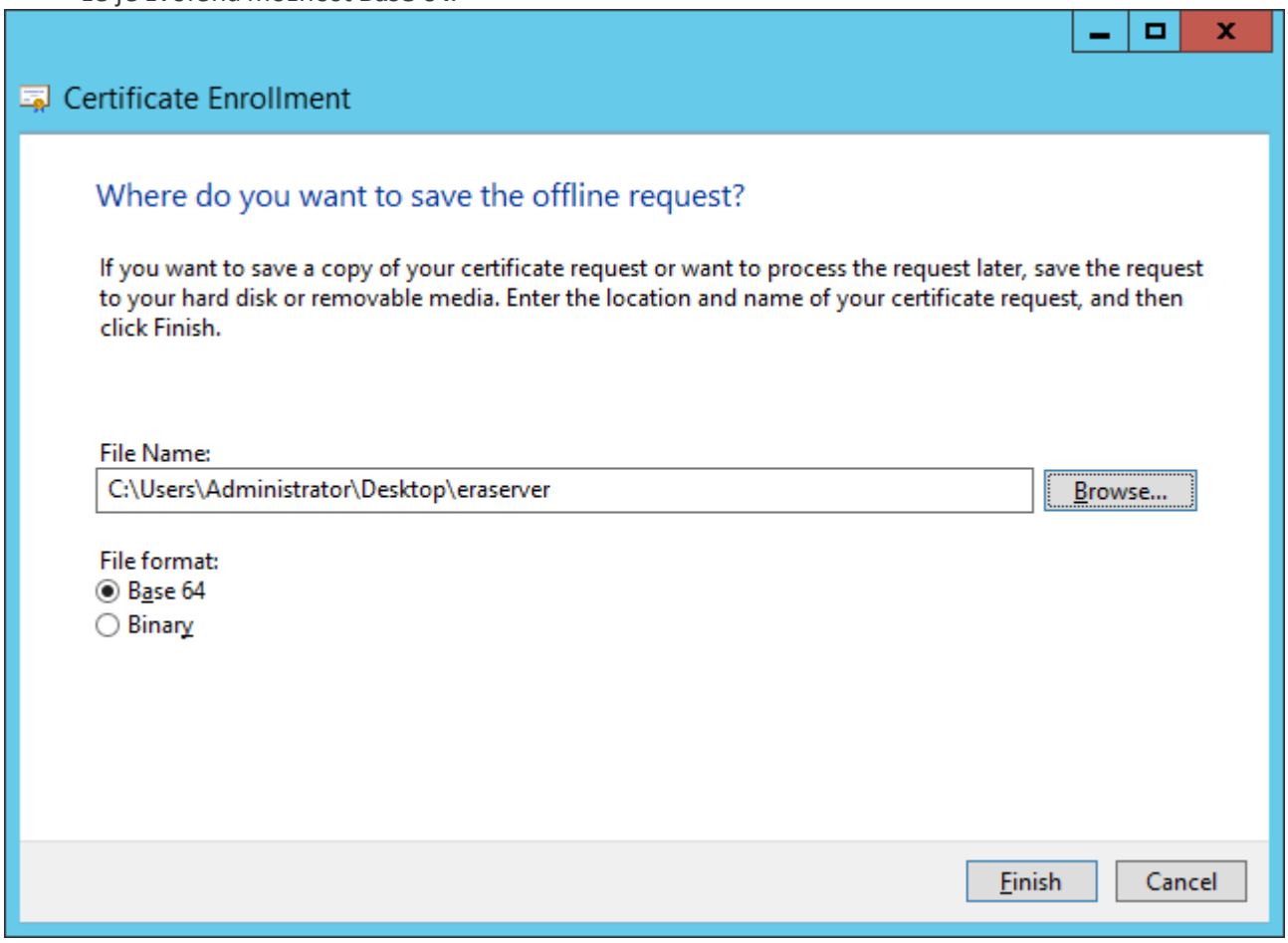
Poznámka:
Zrušte výber všetkých ostatných CSP okrem **Microsoft RSA SChannel Cryptographic Provider (Encryption)**.



l) Rozbaľte sekciu **Key Options**. V menu **Key size** nastavte hodnotu aspoň **2048**. Označte možnosť **Make private key exportable**.

m) Rozbaľte sekciu **Key Type** a vyberte možnosť **Exchange**. Kliknite na **Apply** a skontrolujte si svoje nastavenia.

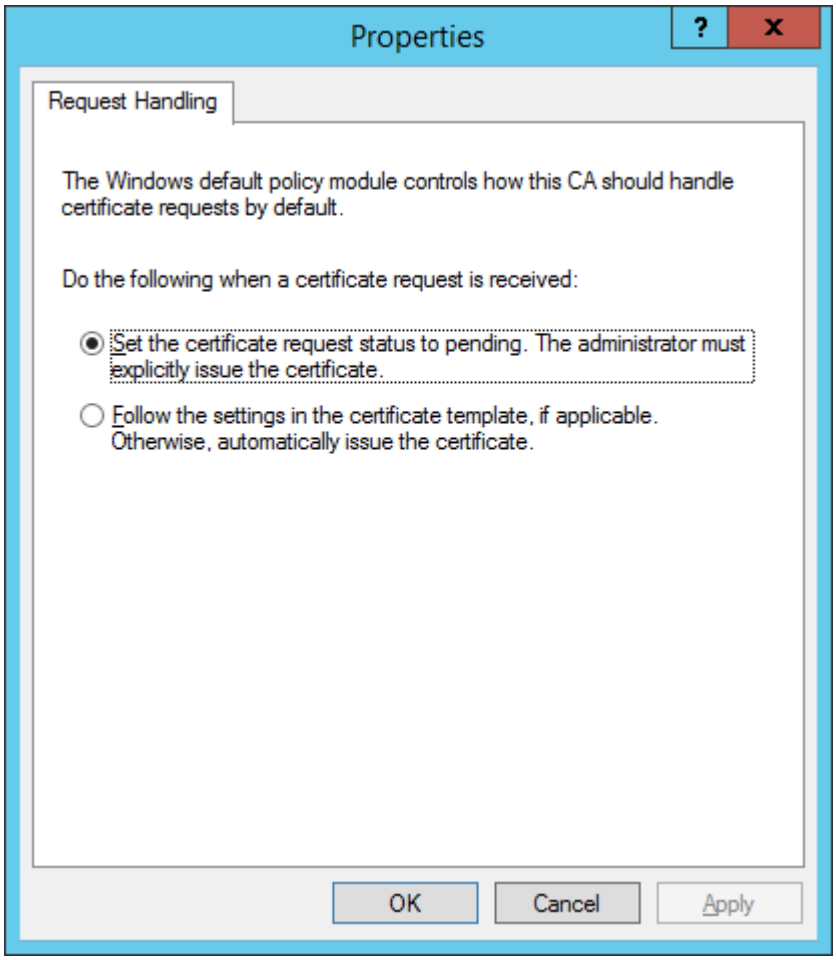
n) Kliknite na **OK**. Zobrazia sa informácie o certifikáte. Pokračujte kliknutím na tlačidlo **Next**. Kliknite na **Browse** a vyberte umiestnenie, kde chcete uložiť žiadosť o vydanie certifikátu (CSR). Zadajte názov súboru a uistite sa, že je zvolená možnosť **Base 64**.



o) Vašu žiadosť CSR vygenerujete kliknutím na tlačidlo Finish.

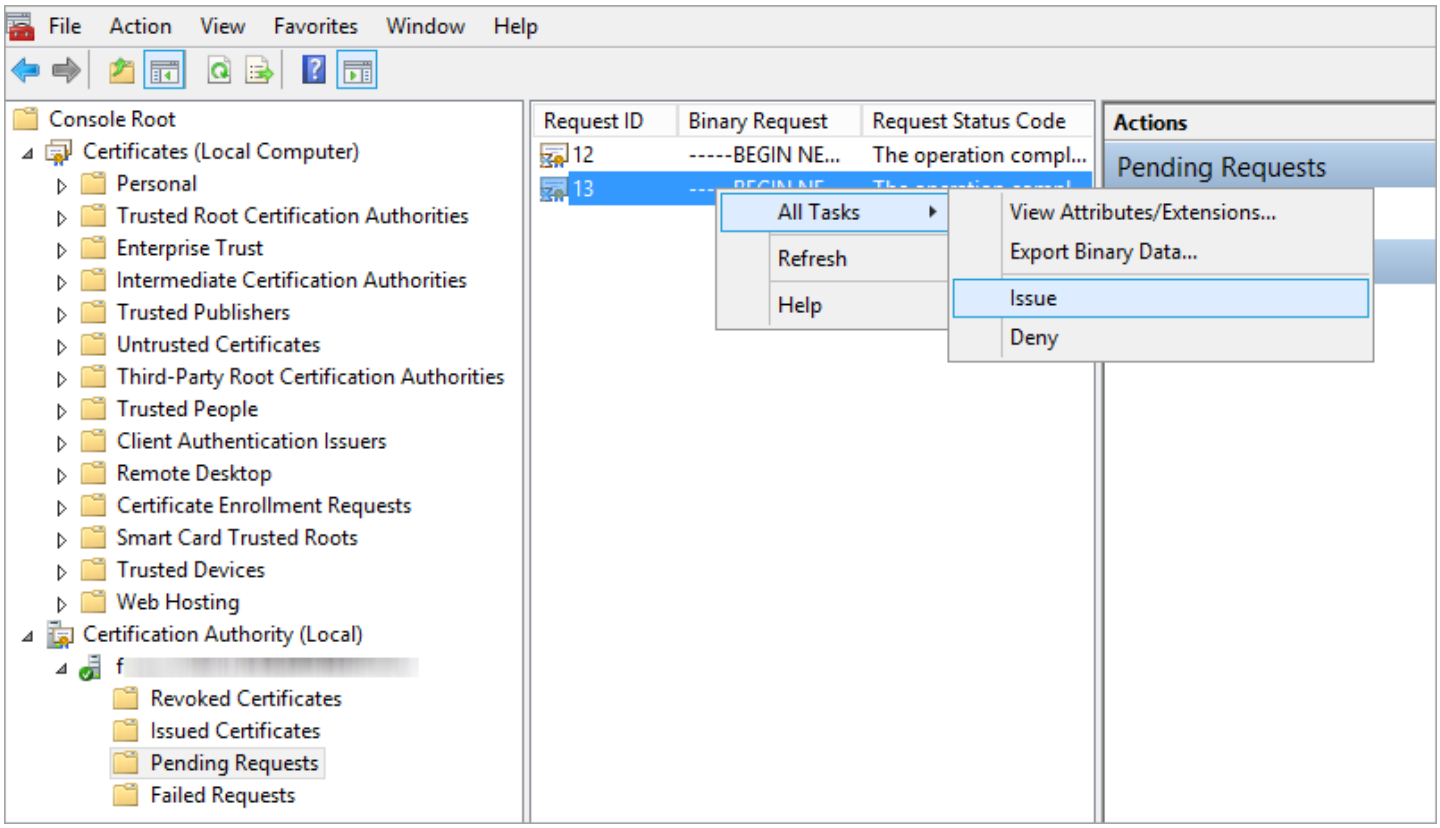
3. Ak chcete importovať svoj vlastný Custom Certificate Request, postupujte podľa krokov uvedených nižšie:

a) Otvorte Server Manager a kliknite na **Tools** > **Certification Authority**.
b) V stromovej štruktúre **Certification Authority (Local)** vyberte možnosť **Your Server (usually FQDN)** > **Properties** a následne prejdite na kartu **Policy Module**. Kliknite na **Properties** a vyberte možnosť **Set the certificate request status to pending. The administrator must explicitly issue the certificate**. V opačnom prípade táto operácia nebude fungovať správne. Ak potrebujete toto nastavenie zmeniť, musíte reštartovať certifikačné služby Active Directory.



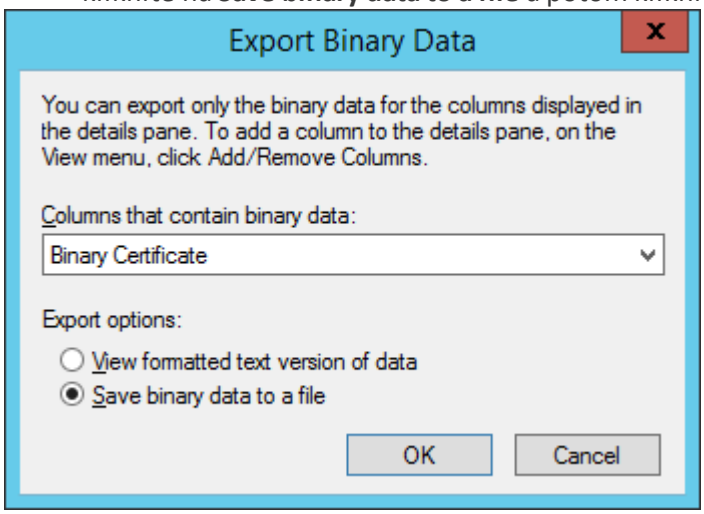
c) V stromovej štruktúre **Certification Authority (Local)** vyberte **Your Server (usually FQDN)** > **All Tasks** > **Submit new request...** a vyberte súbor žiadosti **CSR**, vygenerovaný v kroku 2.

d) Certifikát bude pridaný do zoznamu **Pending Requests**. V pravom navigačnom okne vyberte konkrétne **CSR**. V menu **Action** vyberte **All Tasks** > **Issue**.



4. Exportujte **Issued Custom Certificate** do `.tmp` súboru.

a) Kliknite na **Issued Certificates** v ľavom okne. Kliknite pravým tlačidlom na certifikát, ktorý chcete exportovať, a následne kliknite na **All Tasks** > **Export Binary Data**.
b) V dialógovom okne **Export Binary Data** vyberte z roletového menu **Binary Certificate**. V časti **Export options** kliknite na **Save binary data to a file** a potom kliknite na **OK**.



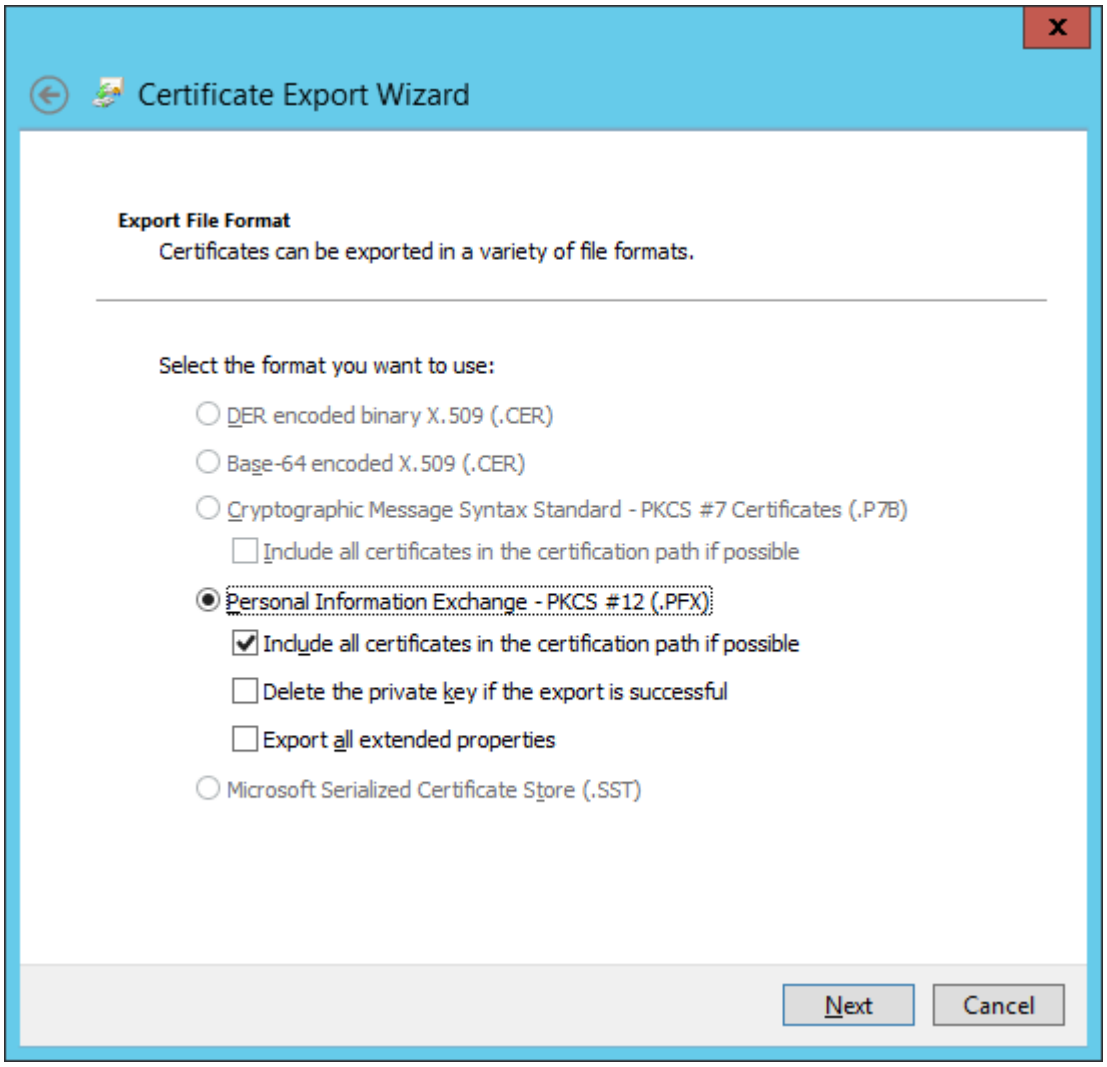
c) V dialógovom okne Save Binary Data vyberte lokalitu, kde chcete uložiť certifikát a kliknite na **Save**.

5. Importujte vytvorený `.tmp` súbor.

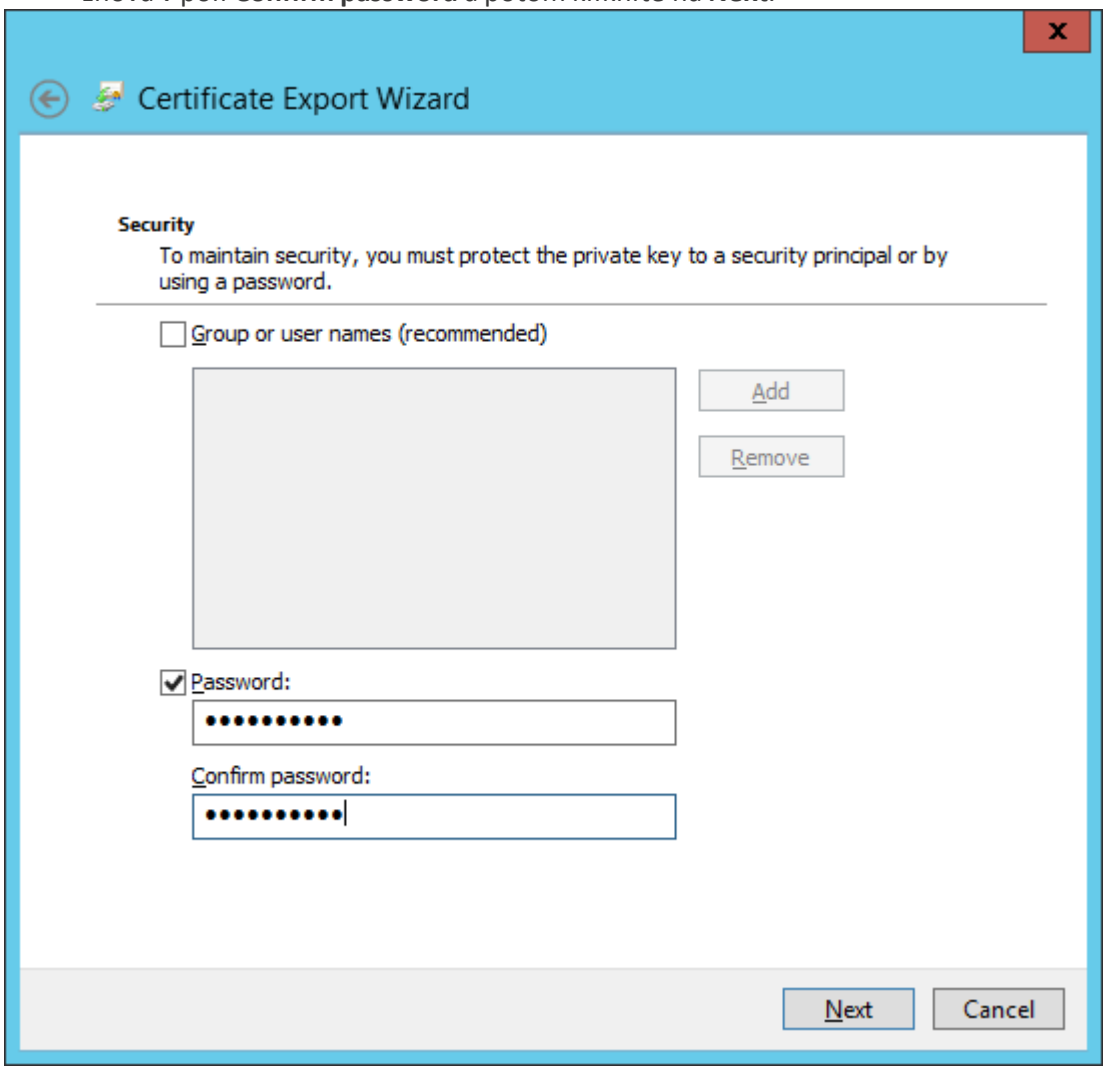
a) Prejdite na Certificate (Local Computer) > kliknite pravým tlačidlom na Personal a vyberte All Tasks > Import.
b) Kliknite na **Next**.
c) Pomocou tlačidla Browse nájdite vytvorený .tmp binárny súbor a kliknite na **Open**. Ďalej vyberte možnosť Place all certificates in the following store > **Personal**. Kliknite na **Next**.
d) Certifikát sa importuje po kliknutí na tlačidlo **Finish**.

6. Exportujte certifikát vrátane súkromného kľúča do `.pfx` súboru.

a) V časti **Certificates (Local Computer)** rozbaľte možnosť **Personal** a kliknite na **Certificates**. Vytvorený certifikát, ktorý chcete exportovať, vyberte v menu **Action** a prejdite na **All Tasks** > **Export**.
b) V sprievodcovi **Certificate Export Wizard** kliknite na **Yes, export the private key**. (Táto možnosť sa zobrazí iba v prípade, že je súkromný kľúč označený ako exportovateľný a máte k nemu prístup.)
c) V sekcii Export File Format vyberte možnosť **Personal Information Exchange -PKCS #12 (`.PFX`)**, následne označte možnosť **Include all certificates in the certification path if possible** pomocou začiarkavacieho políčka a kliknite na **Next**.


Certificate Export Wizard
Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Microsoft Serialized Certificate Store (.SST)
Next
Cancel

d) **Password**, type a password to encrypt the private key you are exporting. Pre potvrdenie hesla ho zadajte znova v poli **Confirm password** a potom kliknite na **Next**.



e) **File name**, type a file name and path for the `.pfx` file that will store the exported certificate and private key. Kliknite na **Next** a potom na **Finish**.

Poznámka:
Príklad vyššie znázorňuje, ako vytvoriť certifikát pre ESET Management Agenta. Rovnaký postup platí aj pre vytvorenie certifikátov pre ESMC Server.

Tento certifikát nie je možné použiť na podpísanie ďalšieho nového certifikátu vo Web Console.

7. Exportujte certifikačnú autoritu:

a) Otvorte Server Manager a kliknite na **Tools** > **Certification Authority**.

b) V stromovej štruktúre **Certification Authority (Local)** vyberte možnosť **Your Server (usually FQDN)** > **Properties** > karta **General** a kliknite na **View Certificate**.

c) Na karte **Details** kliknite na **Copy to File**. Otvorí sa sprievodca **Certificate Export Wizard**.

d) V okne **Export File Format** vyberte **DER encoded binary X.509 (.CER)** a kliknite na **Next**.

e) Kliknite na **Browse**, vyberte umiestnenie, kde chcete uložiť `.cer` súbor, a následne kliknite na **Next**.

f) Certifikačná autorita bude vyexportovaná po kliknutí na **Finish**.

Podrobné inštrukcie týkajúce sa používania vlastných certifikátov v ESMC nájdete v nasledujúcej kapitole.

4.13.6.1.7 Ako použiť vlastné certifikáty v rámci nástroja ESMC?

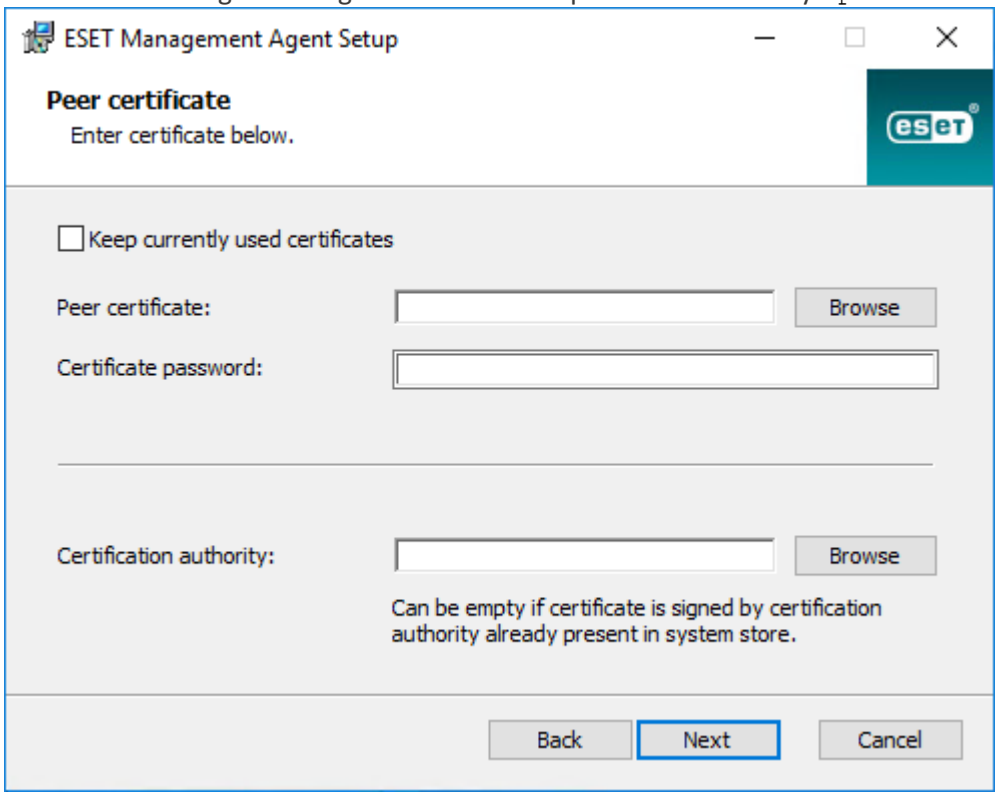
Pokračujte od prechádzajúcej kapitoly:

1. Importujte svoju certifikačnú autoritu tretej strany do ESMC Web Console.
2. V ESMC Web Console nastavte nový, vlastný certifikát servera.

Dôležité:
Ak už máte ESET Management Agenty, ktoré sa pripájajú na ESMC Server, vytvorte novú politiku a použite ju na zmenu certifikátu:

1. Spustite ESMC Web Console.
2. Kliknite na **Politiky** > **Nová**. Zadajte názov úlohy.
3. Rozbaľte sekciu **Nastavenia** a z roletového menu vyberte možnosť **ESET Management Agent**.
4. Rozbaľte sekciu **Pripojenie** a kliknite na **Zmeniť certifikát** vedľa položky **Certifikát**.
5. Kliknite na **Vlastný certifikát** a vyberte certifikát pre ESET Management Agenta.
6. Zadajte heslo certifikátu a kliknite na **OK**.
7. Priraďte túto politiku k všetkým klientom.

3. Prejdite na **Štart** > **Programy a súčasti**, kliknite pravým tlačidlom na **ESET Management Agenta** a vyberte možnosť **Zmeniť**.
4. Kliknite na tlačidlo **Ďalej** a použite možnosť **Opraviť**.
5. Nastavenia pre hostiteľa servera a port servera ponechajte nezmenené a pokračujte kliknutím na **Ďalej**.
6. Kliknite na tlačidlo **Prehľadávať** vedľa položky **Partnerský certifikát** a nájdite váš certifikačný súbor `.pfx`.
7. Zadajte heslo certifikátu, ktoré ste vytvorili v kroku 6.
8. Kliknite na **Prehľadávať** vedľa položky **Certifikačná autorita** a vyberte súbor .der (verejný kľúč) exportovaný z Web Console. Musí ísť o verejný kľúč, ktorým je podpísaný vlastný certifikát.
9. Kliknite na **Ďalej** pre dokončenie opravy.
10. ESET Management Agent bude odteraz používať váš vlastný `.pfx` certifikát.



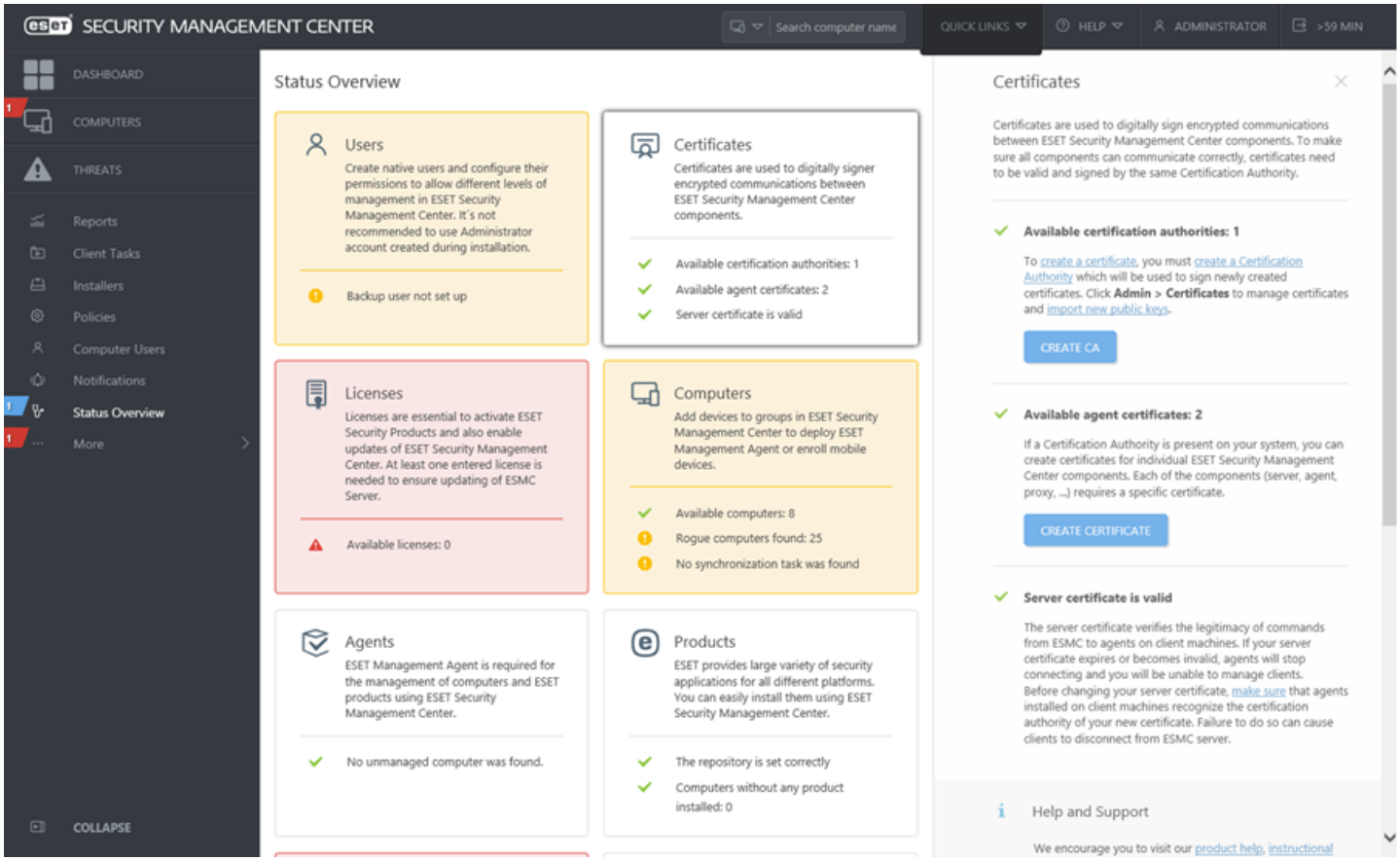
4.13.6.1.8 Certifikát s končiacou platnosťou – hlásenie a nahradenie

Ak sa blíži dátum vypršania platnosti niektorého certifikátu, prípadne certifikačnej autority, ESMC vás o tejto udalosti dokáže včas informovať. Na karte **Oznámenia** sú k dispozícii prednastavené oznámenia pre ESMC certifikát aj pre ESMC certifikačnú autoritu.

Pre aktivovanie tejto funkcie zvoľte príslušné prednastavené oznámenie, kliknite na **Upraviť oznámenie** a upresnite podrobnosti uvedené v časti Distribúcia, napr. e-mailovú adresu alebo SNMP trap. Používateľovi sa zobrazujú len oznámenia týkajúce sa certifikátov, ktoré sú zahrnuté v jeho domácej skupine (za predpokladu, že má daný používateľ pridelené povolenia na **čítanie** v rámci kategórie **Certifikáty**).

Poznámka:
Je potrebné mať nakonfigurované pripojenie k SMTP Serveru v sekcii Nastavenia servera. Až následne môžete upraviť oznámenie a pridať e-mailovú adresu, na ktorú bude oznámenie odosielané.

Ak počítač používa certifikát, ktorého platnosť čoskoro vyprší, informácia o jeho stave sa automaticky zmení. Stav bude hlásený a zobrazený v Riadiacom paneli, Zozname počítačov, v časti Prehľad stavu a na karte Certifikáty:



Postupujte podľa nasledujúcich krokov pre vytvorenie náhrady za certifikačnú autoritu alebo certifikát s končiacou platnosťou:

1. Vytvorte novú certifikačnú autoritu s novou dobou platnosti (v prípade, že stará čoskoro vyprší). Certifikačná autorita by ideálne mala byť platná ihneď.
2. Vytvorte nové partnerské certifikáty pre ESMC Server a ostatné komponenty (Agent/MDM), ktorých platnosť bude pokrytá v rámci doby platnosti certifikačnej autority.
3. Vytvorte politiky, prostredníctvom ktorých nastavíte nové partnerské certifikáty. Aplikujte tieto politiky na komponenty ESMC, MDM a na ESET Management Agenty na všetkých klientskych počítačoch vo svojej sieti.
4. Počkajte, kým všetky súčasti ESMC začnú používať nové certifikáty a prebehne replikácia.

Poznámka:
Odporúča sa počkať 24 hodín, prípadne dovtedy, kým sa všetky komponenty ESMC (agenty) replikujú aspoň dvakrát.

5. Nahraďte certifikát servera v nastaveniach ESMC Servera, aby sa klienty pri pripájaní mohli overovať použitím svojich nových certifikátov.
6. Po úspešnom vykonaní krokov uvedených vyššie (t. j. ak sa klienty úspešne pripájajú k ESMC a všetko funguje tak, ako má) zrušte svoje staré certifikáty a vymažte starú certifikačnú autoritu.

4.13.6.2 Certifikačné autority

Certifikačné autority sú zobrazené a spravované v sekcii **Certifikačné autority**. Ak používate viaceré certifikačné autority, môžete na ich triedenie a zoradenie použiť filtre.

Poznámka:
Na prístup k certifikačným autoritám a certifikátom sa vyžadujú povolenia, ktoré sa prideľujú v rámci rovnakej kategórie povolení nazvanej **Certifikáty**. Certifikáty a certifikačné autority vytvorené počas inštalácie, ako aj tie vytvorené neskôr správcom sú zahrnuté v statickej skupine **Všetko**. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

Akcie > **Nová** – Vytvorenie novej certifikačnej autority

Akcie > **Vymazať** – Vymazanie zvolenej certifikačnej autority

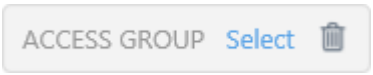
Akcie > Importovať verejný kľúč

Akcie > Exportovať verejný kľúč

Akcie > **Prístupová skupina** – Certifikačnú autoritu je možné presunúť do inej statickej skupiny, aby sa tak stala dostupnou pre používateľov, ktorí majú pre danú statickú skupinu pridelené dostatočné prístupové práva.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

PRÍKLAD: AKO UDELIŤ PRÍSTUPOVÉ PRÁVA K CERTIFIKÁTOM BEZ MOŽNOSTI PRÍSTUPU K CERTIFIKAČNÝM AUTORITÁM

Ak *Správca* používateľovi s menom *John* nechce udeliť prístup k certifikačným autoritám ESMC, no zároveň mu potrebuje prideliť povolenie na používanie certifikátov, je potrebné (cez účet správcu) vykonať nasledujúce kroky:

1. Vytvorte novú statickú skupinu nazvanú *Certifikáty*.
2. Vytvorte novú sadu povolení.
   a. Túto sadu povolení pomenujte *Povolenia pre certifikáty*.
   b. V sekcii **Statické skupiny** pridajte novovytvorenú skupinu *Certifikáty*.
   c. V sekcii **Oprávnenia k funkciám** je potrebné zvoliť povolenie na **zápis** pre kategóriu **Certifikáty**.
   d. V sekcii **Používatelia** kliknite na **Natívni používatelia** a zvoľte používateľa *John*.
   e. Sadu povolení uložte kliknutím na **Dokončiť**.
3. Presuňte certifikáty zo statickej skupiny **Všetko** do novovytvorenej skupiny **Certifikáty**:
   a. Prejdite do časti **Viac** > **Partnerské certifikáty**.
   b. Označte začiarkavacie políčka vedľa tých certifikátov, ktoré chcete presunúť.
   c. Kliknite na **Akcie** > **Prístupová skupina**, zvoľte statickú skupinu nazvanú **Certifikáty** a následne kliknite na **OK**.

Používateľ *John* môže odteraz upravovať a používať presunuté certifikáty. Na druhej strane certifikačné autority sú bezpečne uložené mimo dosah daného používateľa. *John* nebude môcť používať existujúce certifikačné autority (umiestnené v skupine **Všetko**) dokonca ani na podpisovanie certifikátov.

4.13.6.2.1 Vytvorenie novej certifikačnej autority

Pre vytvorenie novej certifikačnej autority prejdite do sekcie **Viac** > **Certifikačné autority** a kliknite na tlačidlo **Akcia** > **Nová** v dolnej časti okna.

Certifikačná autorita

Zadajte **Popis** certifikačnej autority a taktiež **Prístupovú frázu**. **Prístupová fráza** musí obsahovať aspoň 12 znakov.

Atribúty (Predmet)

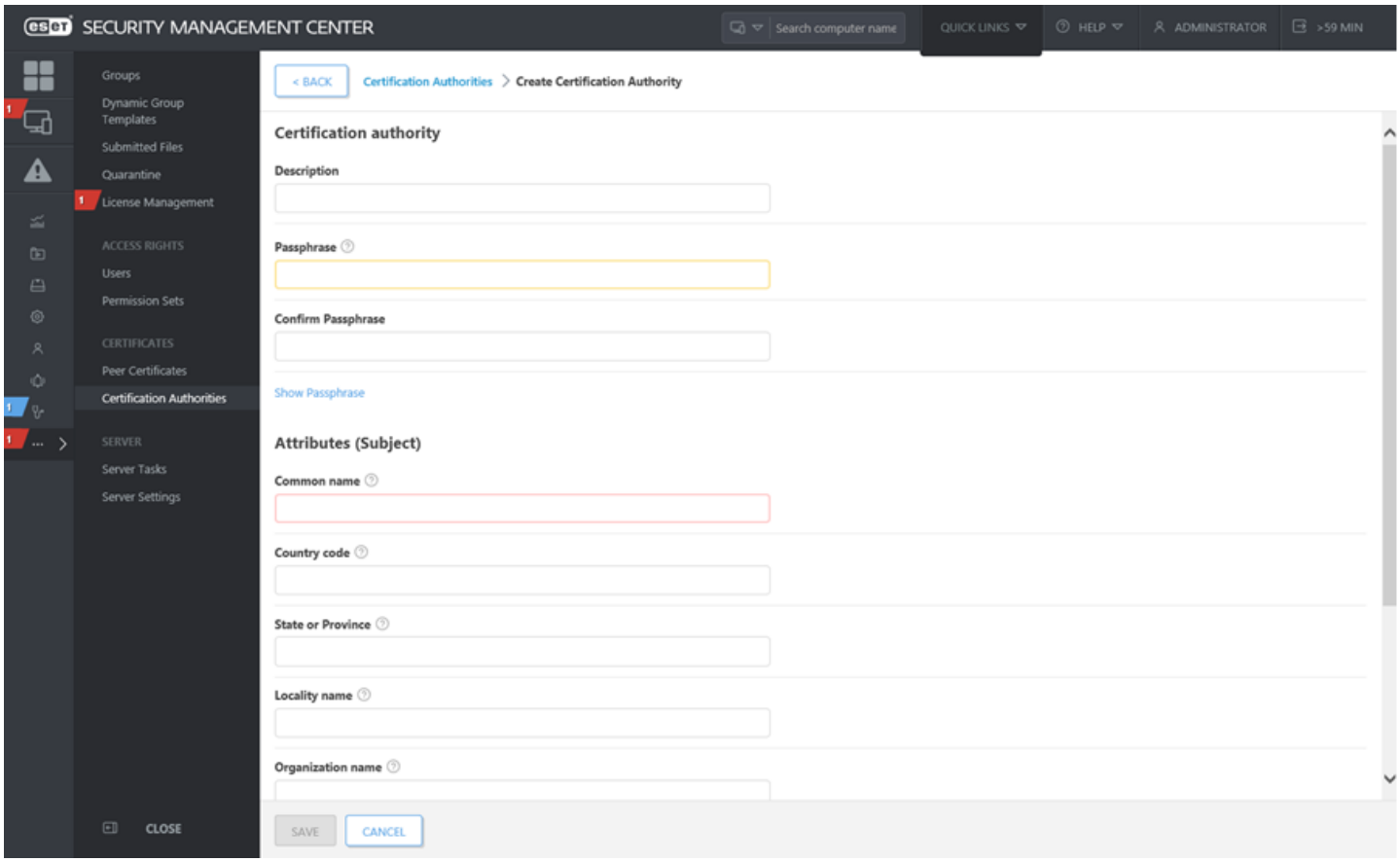
1. Zadajte **Spoločný názov** (názov) certifikačnej autority. Zadajte jedinečný názov, aby bolo možné odlíšiť viaceré certifikačné autority. Môžete prípadne zadať aj dodatočné informácie o danej certifikačnej autorite.
2. Zadajte hodnoty **Platné od** a **Platné do** pre uistenie sa, že je certifikát platný.

Poznámka:
Pre všetky certifikáty a certifikačné autority vytvorené počas inštalácie súčastí nástroja ESMC musí byť hodnota „Platné od“ nastavená na 2 dni pred vytvorením certifikátu.

Pre všetky certifikáty a certifikačné autority vytvorené v ESMC Web Console musí byť hodnota „Platné od“ nastavená na 1 deň pred vytvorením certifikátu. Dôvodom je pokryť všetky možné časové odchýlky medzi všetkými dotknutými systémami.

Napríklad, certifikačná autorita a certifikát vytvorený 12. januára 2017 počas inštalácie bude mať prednastavenú hodnotu „Platné od“ na 10. január 2017 00:00:00 a certifikačná autorita a certifikát vytvorený 12. januára 2017 v ESMC Web Console bude mať prednastavenú hodnotu „Platné od“ na 11. január 2017 00:00:00.

3. Kliknite na **Uložiť** pre uloženie novej certifikačnej autority. Vytvorená certifikačná autorita bude teraz zobrazená v zozname certifikačných autorít v časti **Viac** > **Certifikačné autority** a je pripravená na použitie. Certifikačná autorita je umiestnená do domácej skupiny používateľa, ktorý túto certifikačnú autoritu vytvoril.



Pre správu certifikačnej autority kliknite na **začiarkavacie políčko** vedľa jej názvu v zozname a použite kontextové menu (kliknite ľavým tlačidlom myši na certifikačnú autoritu) alebo tlačidlo **Akcia** v dolnej časti okna. Dostupné možnosti sú Importovať verejný kľúč a Exportovať verejný kľúč alebo **Upraviť** certifikačnú autoritu.

4.13.6.2.2 Export verejného kľúča

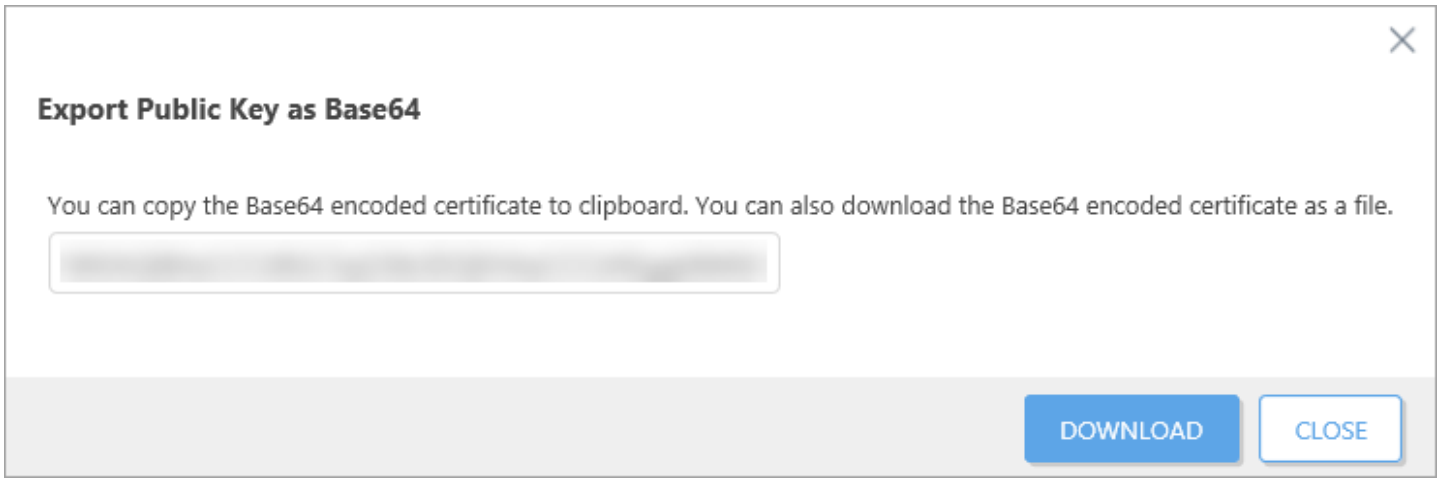
Export verejného kľúča z certifikačnej autority:

1. Vyberte certifikačnú autoritu zo zoznamu a kliknite na začiarkavacie políčko vedľa jej názvu.
2. Kliknite na **Akcie** > **Exportovať verejný kľúč**. Verejný kľúč bude exportovaný ako `.der` súbor. Zadajte názov pre verejný kľúč a kliknite na **Uložiť**.

Poznámka:
Ak vymažete pôvodnú ESMC certifikačnú autoritu a vytvoríte novú, nebude funkčná. Taktiež je potrebné zmeniť certifikát servera v nastaveniach servera a následne reštartovať službu ESMC Server.

Export verejného kľúča z certifikačnej autority ako Base64:

1. Vyberte certifikačnú autoritu zo zoznamu a kliknite na začiarkavacie políčko vedľa jej názvu.
2. Kliknite na **Akcie** > **Exportovať verejný kľúč ako Base64**. Certifikát s kódovaním Base64 môžete tiež stiahnuť do súboru. Tento postup zopakujte pre všetky certifikáty komponentov, ako aj pre certifikačnú autoritu.



Poznámka:

- Ak používate vlastné certifikáty, ktoré nie sú vo formáte **Base64**, bude potrebné ich skonvertovať na formát **Base64** (prípadne môžete tieto certifikáty exportovať podľa popisu vyššie). Toto je jediný akceptovaný formát v rámci pripojenia ESMC komponentov k ESMC Serveru. Podrobnejšie informácie o konvertovaní certifikátov nájdete na odkazoch http://linux.die.net/man/1/base64 a https://developer.apple.com/library/mac/documentation/Darwin/Reference/ManPages/man1/base64.1.html . Napríklad:

  ```
  'cat ca.der | base64 > ca.base64.txt'
  'cat agent.pfx | base64 > agent.base64.txt'
  ```

- Na export certifikátu musí mať používateľ pridelené povolenie na **použitie** certifikátov (v rámci kategórie povolení **Certifikáty**). Podrobnejšie informácie nájdete v tejto kapitole obsahujúcej kompletný zoznam povolení.

4.13.6.2.3 Import verejného kľúča

Ak chcete importovať certifikačnú autoritu tretej strany, kliknite na **Viac** > **Certifikačné autority**.

1. Ďalej kliknite na tlačidlo **Akcie** a následne vyberte možnosť **Importovať verejný kľúč**.
2. **Vybrať súbor na odovzdanie**: kliknite na **Prechádzať...** a vyberte súbor, ktorý chcete importovať.
3. Zadajte **Popis** certifikátu a kliknite na **Importovať**. Certifikačná autorita bude importovaná.

4.13.7 Server

V sekcii Server môžete nastaviť:

- Úlohy pre server – úlohy vykonávané ESMC Serverom nad samotným serverom alebo inými zariadeniami.
- Nastavenia servera – nastavenia ESMC Servera. Tieto nastavenia sú podobné politikám, avšak sú aplikované priamo na ESMC Server.

4.13.7.1 Úlohy pre server

Úlohy pre server predstavujú účinný nástroj na automatizáciu pravidelných úloh. Pre každú úlohu pre server je možné nastaviť spúšťač. Ak chcete, aby bola niektorá úloha pre server spúšťaná pri viacerých udalostiach, musíte každú túto udalosť špecifikovať v samostatnej úlohe pre server v rámci nastavení spúšťača. ESMC obsahuje 6 preddefinovaných typov úloh pre server.

Poznámka:
Úlohy pre server nemôžu byť priradené ku konkrétnym klientom alebo skupinám klientov.

Úlohy pre server a povolenia

Úloha aj spúšťač vyžadujú svojho vykonávajúceho používateľa. Ide o používateľa, ktorý úlohu (a spúšťač) upravuje a mení. Na konkrétne akcie musí mať tento používateľ pridelené dostatočné povolenia. Pri vykonávaní úlohy sa vždy

použije vykonávajúci používateľ zo spúšťača. Ak je úloha spustená na základe nastavenia **Spustiť úlohu okamžite po dokončení**, vykonávajúci používateľ je ten používateľ, ktorý je aktuálne prihlásený do ESMC Web Console. Používateľ bude mať povolenia (na čítanie, použitie, zápis) pre zvolenú úlohu pre server, ak sú tieto povolenia zadefinované v jemu pridelenej sade povolení (**Viac** > **Sady povolení**) a zároveň je pre tieto povolenia nastavená tá statická skupina, v ktorej je umiestnená daná úloha pre server. Prezrite si zoznam povolení, kde sa dozviete viac o prístupových právach.

PRÍKLAD:
Používateľ *John*, ktorého domáca skupina je *Johnova skupina*, chce odstrániť *Úlohu pre server 1*: **Generovať správu**. Táto úloha bola pôvodne vytvorená používateľom *Larry*, takže bola automaticky zahrnutá do domácej skupiny Larryho, nazvanej *Larryho skupina*. Aby mohol *John* úlohu odstrániť, musia byť splnené nasledujúce podmienky:

- *John* musí mať pridelenú sadu povolení, ktorá obsahuje povolenia na zápis v rámci kategórie **Úlohy a spúšťače servera** – **Generovať správu**.
- Sada povolení musí mať v časti **Statické skupiny** nastavenú skupinu *Larryho skupina*.

Povolenia potrebné na vykonávanie konkrétnych akcií týkajúcich sa úloh pre server

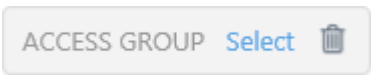
- Na vytvorenie novej úlohy pre server musí mať používateľ pridelené povolenie na zápis pre zvolený typ úlohy a taktiež príslušné prístupové práva ku všetkým objektom, na ktoré sa daná úloha viaže (počítače, licencie, skupiny).
- Na upravovanie úlohy pre server musí mať používateľ pridelené povolenie na zápis pre zvolený typ úlohy a taktiež príslušné prístupové práva ku všetkým objektom, na ktoré sa daná úloha viaže (počítače, licencie, skupiny).
- Na odstránenie úlohy pre server musí mať používateľ pridelené povolenie na zápis pre zvolený typ úlohy.
- Na spustenie úlohy pre server musí mať používateľ pridelené povolenie na použitie pre zvolený typ úlohy.

Vytvorenie novej úlohy pre server

1. Kliknite na **Viac** > **Úlohy pre server** > **Nová**.
2. Zadajte základné informácie o úlohe, ako napr. názov úlohy, popis (voliteľné) a typ úlohy. Typ úlohy definuje nastavenia a správanie úlohy.
3. Môžete sa rozhodnúť, či chcete:
   - **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo **Dokončiť**.
   - **Konfigurovať spúšťač** – po označení tejto možnosti môžete v sekcii **Spúšťač** upraviť nastavenia spúšťača.
   - Nastaviť spúšťač neskôr (v tomto prípade neoznačte žiadnu z uvedených dvoch možností).
4. V sekcii **Nastavenia** upravte nastavenia úlohy.
5. Ak je sekcia **Spúšťač** dostupná, upravte nastavenia spúšťača.
6. V sekcii **Súhrn** skontrolujte všetky nastavenia pre danú úlohu a následne kliknite na **Dokončiť**.

Filter prístupovej skupiny

Tlačidlo filtra s názvom **Prístupová skupina** umožňuje používateľom zvoliť statickú skupinu a vyfiltrovať zobrazené objekty podľa statickej skupiny, v ktorej sú zahrnuté.



Predvolené nastavenia filtra

Filtre môžu byť uložené do vášho používateľského profilu, vďaka čomu ich môžete v budúcnosti jednoduchšie znova použiť. Kliknite na **Pridať filter** a nastavte filter podľa svojich požiadaviek. V časti **Predvoľby** sú na výber tieto možnosti:

Sady filtrov – vaše uložené filtre, ktoré môžete aplikovať kliknutím. Aplikovaný filter je označený potvrdzovacím znakom ✔. Označte možnosť **Zahrnúť viditeľné stĺpce, triedenie a stránkovanie** pre uloženie týchto parametrov do predvoľby.

Uložiť sadu filtrov – pomocou tejto možnosti môžete uložiť svoju súčasnú konfiguráciu filtra ako novú predvoľbu. Po uložení predvoľby už však v rámci nej nemôžete meniť konfiguráciu filtra.

Spravovať sady filtrov – odstránenie alebo premenovanie existujúcich predvolieb. Kliknite na **Uložiť** pre aplikovanie zmien v predvoľbách.

Vymazať hodnoty filtrov – kliknutím na túto možnosť odstránite len súčasné hodnoty z označených filtrov. Uložené predvoľby ostanú nezmenené.

Odstrániť filtre – kliknutím na túto možnosť odstránite označené filtre. Uložené predvoľby ostanú nezmenené.

Odstrániť nepoužité filtre – odstránenie polí filtrov, pre ktoré nie je definovaná hodnota.

Poznámka:
Používateľom, ktorí často používajú úlohy pre server, odporúčame, aby si namiesto používania úloh zdieľaných s inými používateľmi vytvorili vlastné úlohy. Pri každom spustení úlohy pre server sú totiž použité povolenia vykonávajúceho používateľa. Toto môže byť v prípade niektorých používateľov mätúce.

4.13.7.2 Typy úloh pre server

Nasledujúce úlohy pre server sú prednastavené:

- Nasadenie agentov – nasadenie agentov na klientske počítače.
- Odstrániť nepripájajúce sa počítače – odstránenie všetkých klientskych počítačov, ktoré sa už nepripájajú do nástroja ESET Security Management Center, z rozhrania Web Console.
- Generovať správu – táto úloha sa používa na generovanie správ podľa potreby.
- Premenovať počítače – táto úloha bude pravidelne premenovávať počítače v skupinách pomocou formátu FQDN.
- Synchronizácia statickej skupiny – táto úloha aktualizuje informácie o danej skupine, aby boli zobrazované aktuálne údaje.
- Synchronizácia používateľa – aktualizuje používateľa alebo skupinu používateľov.

4.13.7.2.1 Nasadenie agenta

Vzdialené nasadenie ESET Management Agenta môžete vykonať zo sekcie **Viac**. Pre vytvorenie novej úlohy kliknite na **Úlohy pre server** > **Nasadenie agentov** > **Nová**.

Poznámka:
Odporúčame vám hromadné nasadenie agenta vo vašom prostredí najskôr otestovať. Ak prebehne úspešne, môžete začať so skutočným nasadením agenta na klientske počítače. Pred otestovaním hromadného nasadenia vám tiež odporúčame zmeniť interval pripojenia agenta.

Upozornenie:
Nasadenie založené na SSH nie je podporované v prostredí Windows Server 2003. Ak na danom systéme nie je nainštalovaný ESMC Server, úloha nebude vykonaná úspešne.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia nasadenia agenta

Automatické zvolenie vhodného agenta – ak používate vo svojej sieti rôzne operačné systémy (Windows, Linux, macOS), vyberte túto možnosť a program automaticky nájde vhodný typ agenta pri nasadzovaní.
Ciele – pomocou tejto možnosti vyberte klienty, na ktorých bude daná úloha vykonaná.

Poznámka:
Ak boli počítače pridané do ESMC pomocou úlohy Synchronizácia statickej skupiny, uistite sa, že sú názvy týchto počítačov zadané ako úplné názvy domén. Tieto názvy sú počas nasadenia použité ako klientske adresy a ak nie sú správne, nasadenie nebude úspešné. Počas synchronizácie použite atribút `dNSHostName` ako **Atribút názvu hostiteľa počítača** na účely nasadenia agenta.

Názov hostiteľa servera (voliteľný) – môžete zadať názov hostiteľa servera, ak je tento názov odlišný na strane klienta a na strane servera.

Prihlasovacie údaje cieľových počítačov

Používateľské meno/heslo – prihlasovacie meno a heslo používateľa s dostatočnými právami na vykonanie vzdialenej inštalácie agenta.

Nastavenia certifikátu

Peer certifikát:

- **ESMC certifikát** – bezpečnostný certifikát a certifikačná autorita pre inštaláciu agenta. Môžete vybrať prednastavený certifikát a certifikačnú autoritu alebo použiť vlastné certifikáty.
- **Vlastný certifikát** – ak použijete na overenie vlastný certifikát, prejdite do sekcie certifikát a vyberte daný certifikát pri inštalácii agenta. Viac informácií nájdete v kapitole Certifikáty.

Prístupová fráza certifikátu – heslo pre certifikát; buď heslo zadané pri inštalácii ESMC Servera (krok, v ktorom ste vytvorili certifikačnú autoritu), alebo heslo vášho vlastného certifikátu.

Poznámka:

- ESMC Server dokáže automaticky vybrať vhodný inštalačný balík agenta pre konkrétny operačný systém. Ak chcete inštalačný balík vybrať manuálne, zrušte výber možnosti **Automatické zvolenie vhodného agenta** a vyberte požadovaný inštalačný balík z ESMC repozitára.
- Pri inštalácii agenta na počítačoch Linux alebo Mac sa uistite, že na daných cieľových počítačoch je SSH daemon povolený a spustený na porte 22 a že toto spojenie nie je blokované firewallom. Pre pridanie výnimky v rámci Linux firewallu použite nasledujúci príkaz (nahraďte IP adresu IP adresou svojho ESMC Servera):
  `iptables -A INPUT -s 10.0.0.1 -p tcp --dport 22 -m state --state NEW -j ACCEPT`
- Pre inštaláciu na Linux vyberte používateľa s povolením používať príkaz `sudo` alebo `root` používateľa. Ak sa použije `root`, služba `ssh` vám musí povoliť prihlásiť sa ako `root`.
- Ak chcete opätovne nasadiť agenta, nikdy neodstraňujte aktuálneho agenta. Miesto toho spustite úlohu nasadenia nad aktuálnym agentom. Je možné, že ak odstránite agenta, budú po vykonaní nového nasadenia spúšťané staré úlohy.

Ostatné nastavenia

Ak nesúhlasíte so zasielaním správ o zlyhaní programu a telemetrických údajov spoločnosti ESET, zrušte označenie možnosti **Zúčastnite sa programu zlepšovania produktov**. Ak ponecháte túto možnosť označenú, telemetrické údaje a správy o zlyhaní programu budú odosielané spoločnosti ESET.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.2 Odstránenie nepripájajúcich sa počítačov

Úloha **Odstrániť nepripájajúce sa počítače** vám umožňuje odstrániť počítače podľa zadaných kritérií. Napríklad, ak sa ESET Management Agent na klientskom počítači nepripojí počas 30 dní, počítač bude odstránený z ESMC Web Console.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Názov skupiny – vyberte existujúcu statickú skupinu alebo vytvorte novú statickú skupinu, ktorej počítače budú premenované.

Počet dní, počas ktorých sa počítač nepripojil – zadajte počet dní, po uplynutí ktorých budú nepripojené počítače odstránené.

Deaktivovať licenciu – túto možnosť použite v prípade, ak si želáte tiež deaktivovať licencie odstránených počítačov.

Odstrániť nespravované počítače – po označení tejto možnosti budú odstránené počítače, ktoré nie sú spravované.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača.

Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.3 Generovať správu

Úloha **Generovať správu** umožňuje generovanie správ na základe prednastavených alebo vytvorených šablón správ.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Šablóny správ – kliknite na **Pridať šablónu správy** a zo zoznamu vyberte požadovanú šablónu správy. Používateľ, ktorý túto úlohu vytvára, bude môcť vidieť a zvoliť len tie šablóny správ, ktoré sú dostupné v jeho skupine. Pre jednu správu môžete zvoliť aj viacero šablón.

Vyberte možnosť Odoslať e-mail alebo Uložiť do súboru pre získanie vygenerovanej správy.

Doručenie správy

Odoslať e-mail

Aby bolo možné odosielanie/prijímanie e-mailových správ, musíte v sekcii Nastavenia servera > **Pokročilé nastavenia** povoliť používanie SMTP servera.

Odoslať – zadajte e-mailové adresy prijímateľov, ktorým budú odosielané e-maily obsahujúce správu. Môžete zadať viac adries a oddeliť ich čiarkou. Je tiež možné zadať CC a BCC, ktorých funkcia je rovnaká ako v prípade e-mailových klientov.
Predmet – predmet správy. Zadajte charakteristický predmet, aby bolo možné prichádzajúce správy triediť. Predmet je voliteľný, ale odporúčame ho zadať.
Obsah správy – zadajte obsah správy.
Odoslať e-mail, ak je správa prázdna – použite túto možnosť, ak chcete, aby bola správa odoslaná aj v prípade, že neobsahuje žiadne údaje.

Možnosti tlače

Kliknite na **Zobraziť možnosti tlače** pre zobrazenie nasledujúcich nastavení:

- **Výstupný formát** – vyberte jeden z formátov tlače.
- **Výstupný jazyk** – vyberte jazyk správy. Prednastavený jazyk je jazyk nastavený v rozhraní ESMC Web Console.
- **Veľkosť stránky/Rozlíšenie (DPI)/Orientácia papiera/Formát farby/Jednotky okraja/Okraje** – tieto nastavenia využijete pri tlači správy. Vyberte vhodné nastavenia na základe vašich požiadaviek na tlač. Tieto nastavenia sú aplikovateľné len na formáty PDF a PS, formát CSV nie je podporovaný.

Poznámka:
Úloha **Generovať správu** vám umožňuje vybrať niekoľko formátov výstupu. Pri použití formátu CSV bude dátum a čas správy uložený v časovom štandarde UTC. Pri použití formátov PDF alebo PS bude dátum a čas správy uložený v lokálnom čase servera.

Uložiť do súboru

Možnosti súboru

Relatívna cesta k súboru – správa bude vygenerovaná do konkrétneho adresára, napríklad:
Na systéme Windows sú správy väčšinou umiestnené v *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports*.
Na starších systémoch Windows môže byť použité umiestnenie *C:\Users\All Users\ESET\RemoteAdministrator\Server\EraServerApplicationData\Data\GeneratedReports*.
Na systéme Linux sú správy väčšinou umiestnené v */var/opt/eset/RemoteAdministrator/Server/GeneratedReports/*.

Uložiť súbor, ak je správa prázdna – použite túto možnosť, ak chcete, aby bola správa uložená aj v prípade, že neobsahuje žiadne údaje.

Možnosti tlače

Kliknite na **Zobraziť možnosti tlače** pre zobrazenie nasledujúcich nastavení:

- **Výstupný formát** – vyberte jeden z formátov tlače.
- **Výstupný jazyk** – vyberte jazyk správy. Prednastavený jazyk je jazyk nastavený v rozhraní ESMC Web Console.
- **Veľkosť stránky/Rozlíšenie (DPI)/Orientácia papiera/Formát farby/Jednotky okraja/Okraje** – tieto nastavenia využijete pri tlači správy. Vyberte vhodné nastavenia na základe vašich požiadaviek na tlač. Tieto nastavenia sú aplikovateľné len na formáty PDF a PS, formát CSV nie je podporovaný.

Poznámka:
Úloha **Generovať správu** vám umožňuje vybrať niekoľko formátov výstupu. Pri použití formátu CSV bude dátum a čas správy uložený v časovom štandarde UTC. Pri použití formátov PDF alebo PS bude dátum a čas správy uložený v lokálnom čase servera.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

Poznámka:
Operačný systém Ubuntu Server Edition vyžaduje služby **X server** a **xinit** pre správnu funkciu aplikácie Report Printer (PDF správy).

```
sudo apt-get install server-xorg
sudo apt-get install xinit
startx
```

4.13.7.2.4 Premenovanie počítačov

Pomocou úlohy **Premenovať počítače** môžete v rámci ESMC premenovať klientske počítače a nastaviť ich názvy do FQDN formátu. Môžete použiť prednastavenú úlohu pre server, ktorá je štandardnou súčasťou ESMC inštalácie. Ak je názov klientskeho zariadenia iný ako ten, ktorý je uvedený v podrobnostiach o danom zariadení, spustením tejto úlohy je možné obnoviť správny názov zariadenia.

Táto úloha automaticky každú hodinu premenuje synchronizované počítače nachádzajúce sa v skupine **Stratené a nájdené**. Pre vytvorenie novej úlohy kliknite na **Úlohy pre server** > **Premenovať počítače** > **Nová**.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Názov skupiny – vyberte existujúcu statickú alebo dynamickú skupinu, prípadne vytvorte **novú statickú** alebo **dynamickú skupinu**, v ktorej sa majú premenovať počítače.

Premenovať na základe:

- **Názov počítača** – každý počítač je na lokálnej sieti identifikovaný na základe jedinečného názvu počítača.
- **Úplný názov domény počítača (FQDN)** – začína sa názvom hostiteľa a pokračuje názvami domén až po doménu na najvyššej úrovni v stromovej hierarchii DNS.

Toto nastavenie prináša riešenie konfliktu názvov počítačov, ktoré sa už nachádzajú v ESMC (názvy počítačov musia byť jedinečné), a počítačov pridaných pomocou synchronizácie. Kontrola je potrebná iba pre názvy počítačov, ktoré sa nachádzajú mimo synchronizovaný podstrom.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.5 Synchronizácia statickej skupiny

Úloha **Synchronizácia statickej skupiny** vyhľadáva vo vašej sieti (Active Directory, Open Directory, LDAP, lokálna sieť alebo VMware) počítače a zaraďuje ich do statickej skupiny. Ak počas inštalácie ESMC Servera vyberiete možnosť **Synchronizovať s Active Directory**, nájdené počítače budú zaradené do skupiny **Všetko**. Pre synchronizáciu počítačov s operačným systémom Linux pripojených k Windows doméne postupujte podľa týchto podrobných inštrukcií.

Sú dostupné tri **Režimy synchronizácie**:

- **Active Directory/Open Directory/LDAP** – zadajte základné informácie pre pripojenie na server. Podrobnejšie inštrukcie nájdete v tejto kapitole.
- **Sieť MS Windows** – zadajte **Pracovnú skupinu (Workgroup)**, ktorá bude použitá, a taktiež príslušné prihlasovacie údaje. Podrobnejšie inštrukcie nájdete v tejto kapitole.
- **VMware** – zadajte základné informácie pre pripojenie na VMware vCenter Server. Podrobnejšie inštrukcie nájdete v tejto kapitole.

4.13.7.2.5.1 Režim synchronizácie – Active Directory

Kliknite na **Viac** > **Úlohy pre server** > **Synchronizácia statickej skupiny** > **Nová**.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Spoločné nastavenia

Kliknite na možnosť **Vybrať** vedľa položky **Názov statickej skupiny** – štandardne bude pre synchronizované počítače použitá domáca skupina vykonávajúceho používateľa. Môžete tiež zvoliť možnosť **Nová statická skupina** a vytvoriť novú skupinu.

- **Objekty k synchronizácii** – sú to buď **Počítače a skupiny**, alebo **Iba počítače**.
- **Akcia pri výskyte kolízie počas vytvárania počítačov** – ak synchronizácia pridáva počítače, ktoré sú už členmi danej statickej skupiny, môžete vybrať metódu riešenia konfliktu:
  - **Vynechať** (nové počítače nebudú pridané).
  - **Presunúť** (nové počítače budú presunuté do podskupiny)
  - **Duplikovať** (nové počítače budú pridané so zmeneným názvom)
- **Akcia pri odstránení počítača** – ak počítač už neexistuje, môžete ho buď **Zmazať**, alebo **Vynechať**.
- **Akcia pri odstránení skupiny** – ak skupina už neexistuje, môžete ju **Zmazať** alebo **Vynechať**.
- **Režim synchronizácie** – Active Directory/Open Directory/LDAP

Nastavenia pripojenia servera

- **Server** – zadajte názov servera alebo IP adresu vášho doménového radiča.
- **Prihlásenie** – zadajte prihlasovacie údaje pre váš doménový radič vo formáte **DOMAIN\username**.
- **Heslo** – zadajte heslo, pomocou ktorého sa prihlasujete na váš doménový radič.
- Použitie LDAP parametrov – ak chcete použiť LDAP, označte možnosť **Použiť LDAP namiesto Active Directory** a zadajte atribúty zodpovedajúce vášmu serveru. Môžete tiež použiť predvolené atribúty kliknutím na položku Vlastné v časti Predvoľby. Automaticky budú načítané a vyplnené nasledujúce atribúty:
  - **Active Directory** – kliknite na možnosť **Prechádzať...** vedľa položky **Rozlišujúci názov**. Zobrazí sa stromová štruktúra vášho Active Directory. Vyberte hornú položku pre synchronizáciu všetkých skupín s ESMC alebo vyberte len konkrétne skupiny, ktoré chcete pridať. Po dokončení úprav kliknite na **OK**.
  - **Open directory Mac OS X Servera (názvy hostiteľských počítačov)**
  - **Open directory Mac OS X Servera (IP adresy počítačov)**
  - **OpenLDAP so Samba záznamami** – pre nastavenie parametrov DNS názov v Active Directory.
  - Pri použití predvolených nastavení pre **LDAP** a **Active Directory** môžete do sekcie Podrobnosti o počítači načítať atribúty zo svojej Active Directory štruktúry. Môžu byť použité len atribúty typu `DirectoryString`. Pre kontrolu atribútov na vašom doménovom radiči môžete použiť nástroj, akým je napríklad *ADExplorer*. Pozrite si príslušné polia v tabuľke nižšie:

Polia podrobností o počítači	Polia synchronizačnej úlohy
Názov	**Atribút názvu hostiteľa počítača**
Popis	**Atribút popisu počítača**

Nastavenia synchronizácie

- **Rozlišujúci názov** – cesta k uzlu v stromovej štruktúre Active Directory. Ak ponecháte toto pole prázdne, bude synchronizovaná celá stromová štruktúra AD.
- **Vylúčené rozlišujúce názvy** – v prípade potreby môžete vylúčiť (ignorovať) určité uzly v stromovej štruktúre Active Directory.
- **Ignorovať deaktivované počítače (iba v Active Directory)** – počítače, ktoré sú deaktivované v AD, budú pri synchronizácii ignorované (pri vykonaní úlohy budú tieto počítače preskočené).

Dôležité:
Ak sa zobrazí chyba `Server not found in Kerberos database` po kliknutí na **Browse**, použite AD FQDN servera miesto IP adresy.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.5.2 Režim synchronizácie – MS Windows Network

Kliknite na **Viac** > **Úlohy pre server** > **Synchronizácia statickej skupiny** > **Nová**.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Spoločné nastavenia

Kliknite na možnosť **Vybrať** vedľa položky **Názov statickej skupiny** – štandardne bude pre synchronizované počítače použitá domáca skupina vykonávajúceho používateľa. Môžete tiež zvoliť možnosť **Nová statická skupina** a vytvoriť novú skupinu.

- **Objekty k synchronizácii** – sú to buď **Počítače a skupiny**, alebo **Iba počítače**.
- **Akcia pri výskyte kolízie počas vytvárania počítačov** – ak synchronizácia pridáva počítače, ktoré sú už členmi danej statickej skupiny, môžete vybrať metódu riešenia konfliktu:
  - **Vynechať** (nové počítače nebudú pridané).
  - **Presunúť** (nové počítače budú presunuté do podskupiny)
  - **Duplikovať** (nové počítače budú pridané so zmeneným názvom)
- **Akcia pri odstránení počítača** – ak počítač už neexistuje, môžete ho buď **Zmazať**, alebo **Vynechať**.
- **Akcia pri odstránení skupiny** – ak skupina už neexistuje, môžete ju **Zmazať** alebo **Vynechať**.
- **Režim synchronizácie** – sieť MS Windows

V sekcii **Nastavenia synchronizácie siete Microsoft Windows** uveďte nasledujúce informácie:

- **Pracovná skupina** – zadajte doménu alebo pracovnú skupinu, ktorá obsahuje počítače, ktoré budú synchronizované. Ak nezadáte žiadnu pracovnú skupinu, budú synchronizované všetky viditeľné počítače.
- **Prihlásenie** – zadajte prihlasovacie údaje pre synchronizáciu počítačov vo vašej sieti Windows.
- **Heslo** – zadajte heslo potrebné pre prihlásenie sa do vašej siete Windows.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

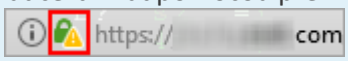
Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.5.3 Režim synchronizácie – VMware

Virtuálne počítače bežiace na VMware vCenter Serveri je možné synchronizovať.

Poznámka:
Pre úspešné spustenie tejto úlohy je potrebné importovať certifikačnú autoritu nástroja vCenter do svojho ESMC Servera. Exportovať ju môžete prostredníctvom webového prehliadača.

Napríklad, ak chcete exportovať certifikát pomocou prehliadača Firefox, kliknite na ikonu zabezpečeného pripojenia v paneli s adresou 

a následne kliknite na možnosť **Zobraziť podrobnosti pripojenia** > **Ďalšie informácie** > **Zobraziť certifikát** > **Podrobnosti** > **Exportovať** > **Uložiť**.

Kliknite na **Viac** > **Úlohy pre server** > **Synchronizácia statickej skupiny** > **Nová**.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Spoločné nastavenia

Kliknite na možnosť **Vybrať** vedľa položky **Názov statickej skupiny** – štandardne bude pre synchronizované počítače použitá domáca skupina vykonávajúceho používateľa. Môžete tiež zvoliť možnosť **Nová statická skupina** a vytvoriť novú skupinu.

- **Objekty k synchronizácii** – sú to buď **Počítače a skupiny**, alebo **Iba počítače**.
- **Akcia pri výskyte kolízie počas vytvárania počítačov** – ak synchronizácia pridáva počítače, ktoré sú už členmi danej statickej skupiny, môžete vybrať metódu riešenia konfliktu:
  - **Vynechať** (nové počítače nebudú pridané).
  - **Presunúť** (nové počítače budú presunuté do podskupiny)
  - **Duplikovať** (nové počítače budú pridané so zmeneným názvom)
- **Akcia pri odstránení počítača** – ak počítač už neexistuje, môžete ho buď **Zmazať**, alebo **Vynechať**.
- **Akcia pri odstránení skupiny** – ak skupina už neexistuje, môžete ju **Zmazať** alebo **Vynechať**.
- **Režim synchronizácie** – VMware

Nastavenia pripojenia servera

- **Server** – zadajte DNS alebo IP adresu pre VMware vCenter Server. Adresa musí byť rovnaká ako hodnota **CN** importovanej certifikačnej autority nástroja vCenter. Túto hodnotu nájdete v stĺpci **Predmet** v sekcii **Viac** > okno **Certifikačné autority**.
- **Prihlásenie** – zadajte prihlasovacie údaje pre VMware vCenter Server.
- **Heslo** – zadajte heslo pre prihlásenie sa do svojho VMware vCenter Servera.

Nastavenia synchronizácie

- **Zobrazenie štruktúry** – zvoľte typ zobrazenia štruktúry, teda **Adresáre** alebo **Fondy prostriedkov**.
- **Cesta k štruktúre** – kliknite na **Prechádzať** a vyberte priečinok, ktorý chcete synchronizovať. Ak pole ponecháte prázdne, bude synchronizovaná celá štruktúra.
- **Zobrazenie počítača** – vyberte, či chcete po synchronizácii zobrazovať počítače podľa Názvu, Názvu hostiteľa alebo **IP adresy**.

Dôležité:
Ak sa zobrazí chyba `Server not found in Kerberos database` po kliknutí na **Browse**, použite AD FQDN servera miesto IP adresy.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.2.5.4 Synchronizácia statickej skupiny – Linuxové počítače

Počítače s operačným systémom Linux vo Windows doméne nezobrazujú žiadny text vo vlastnostiach počítača v Active Directory Users and Computers (ADUC), je preto nutné zadať informácie manuálne.

Skontrolujte požiadavky servera a nasledujúce prerekvizity:

- Počítače s operačným systémom Linux sa nachádzajú v Active Directory.
- Doménový radič má nainštalovaný DNS server.
- **ADSI Edit** je nainštalovaný.

1. Otvorte príkazový riadok a spustite príkaz `adsiedit.msc`.
2. Prejdite do sekcie **Action** > **Connect to**. Zobrazí sa okno s nastaveniami pripojenia.
3. Kliknite na tlačidlo **Select a well known Naming context**.
4. Otvorte rozbaľovacie pole so zoznamom a vyberte možnosť **Default naming context** (predvolený názvový kontext).
5. Kliknite na **OK**. ADSI hodnota na ľavej strane by mala byť názvom vášho doménového radiča – Default naming context (váš doménový radič).
6. Kliknite na hodnotu **ADSI** a otvore jej podskupinu.
7. Kliknite na **podskupinu** a prejdite do časti CN (Common Name) alebo OU (Organizational Unit), kde sa zobrazujú počítače s operačným systémom Linux.
8. Kliknite na položku **hostname** pre konkrétne Linuxové počítače a v kontextovom menu vyberte možnosť **Properties**. Prejdite k parametru **dNSHostName** a kliknite na tlačidlo **Edit**.
9. Zmeňte hodnotu **<not set>** na platný text (napr. `ubuntu.TEST`).
10. Kliknite na **OK** > **OK**. Otvorte **ADUC** a zobrazte **vlastnosti** konkrétneho Linuxového počítača – mal by tu byť zobrazený nový zadaný text.

4.13.7.2.6 Synchronizácia používateľov

Táto úloha pre server slúži na synchronizáciu informácií o používateľoch a skupinách používateľov zo zdroja, ako napr. Active Directory, LDAP parametre atď. Pre spustenie tejto úlohy kliknite na **Viac** > **Úlohy pre server** > **Synchronizácia používateľa** > **Nová**.

Základné

V tejto sekcii môžete zadať základné informácie o úlohe, ako napr. Názov a Popis (voliteľné). Máte tiež na výber z nasledujúcich nastavení spúšťača úlohy:

- **Spustiť úlohu okamžite po dokončení** – označte túto možnosť, ak chcete úlohu spustiť automaticky hneď po kliknutí na tlačidlo Dokončiť.
- **Konfigurovať spúšťač** – označte túto možnosť, ak chcete povoliť zobrazenie sekcie Spúšťač, ktorá vám umožňuje upraviť nastavenia spúšťača úlohy.
- Túto možnosť ponechajte neoznačenú, ak chcete spúšťač nastaviť neskôr.

Nastavenia

Spoločné nastavenia

Názov skupiny používateľov – predvolene bude použitá koreňová skupina synchronizovaných používateľov (štandardne je to skupina **Všetko**). Môžete tiež vytvoriť novú skupinu používateľov.

Riešenie kolízií pri vytváraní používateľov – môžu sa vyskytnúť dva typy konfliktov:

- Používatelia s rovnakým menom v tej istej skupine.
- Používateľ s rovnakým SID (kdekoľvek v systéme).

Riešenie kolízii môže byť nastavené na:

- **Vynechať** – používateľ nie je pridaný do ESMC počas synchronizácie s Active Directory.
- **Prepísať** – existujúci používateľ v ESMC je prepísaný používateľom z Active Directory. V prípade SID konfliktu je existujúci používateľ v ESMC odstránený z jeho predchádzajúceho umiestnenia (aj v prípade, že používateľ sa nachádzal v inej skupine).

Riešenie zániku používateľov – ak už používateľ neexistuje, môžete ho buď **Zmazať**, alebo **Vynechať**.

Riešenie zániku skupín používateľov – ak už skupina používateľov neexistuje, môžete ju buď **Zmazať**, alebo **Vynechať**.

POZNÁMKA:
Ak pre používateľa použijete vlastné atribúty, nastavte možnosť **Riešenie kolízií pri vytváraní používateľov** na **Vynechať**. V opačnom prípade bude používateľ a všetky jeho údaje prepísané údajmi z Active Directory a vlastné atribúty budú stratené. Ak chcete používateľa prepísať, zmeňte možnosť **Riešenie zániku používateľov** na **Vynechať**.

Nastavenia pripojenia servera

Server – zadajte názov servera alebo IP adresu vášho doménového radiča.

Prihlásenie – zadajte prihlasovacie údaje pre váš doménový radič vo formáte **DOMAIN\username**.

Používateľské heslo – zadajte heslo používané na prihlásenie sa do vášho doménového radiča.

Použitie LDAP parametrov – ak chcete použiť LDAP, zaškrtnite začiarkavacie políčko vedľa možnosti **Použiť LDAP namiesto Active Directory** a zadajte informácie o vašom serveri. Môžete si tiež prípadne vybrať možnosť **Predvoľby** kliknutím na položku **Vlastné...** a parametre budú vyplnené automaticky:

- **Active Directory**
- **Open directory Mac OS X Servera (názvy hostiteľských počítačov)**
- **Open directory Mac OS X Servera (IP adresy počítačov)**
- **OpenLDAP so Samba záznamami** – nastavenie parametrov – DNS názov v Active Directory.

Nastavenia synchronizácie

Rozlišujúci názov – cesta k uzlu v stromovej štruktúre Active Directory. Ak ponecháte toto pole prázdne, bude synchronizovaná celá stromová štruktúra AD.

Atribúty používateľa a skupiny používateľov – predvolené atribúty používateľa sú špecifické pre adresár, do ktorého používateľ patrí. Ak chcete synchronizovať atribúty Active Directory, vyberte AD parameter z roletového menu v príslušných poliach alebo zadajte vlastný názov pre atribút. Vedľa každého synchronizovaného poľa sa nachádza zástupný symbol (napr.: `${display_name}`), ktorý bude vyjadrovať daný atribút v určitých nastaveniach týkajúcich sa ESMC politík.

Pokročilé atribúty používateľa – ak chcete použiť pokročilé atribúty, kliknite na možnosť **Pridať nový**. Pre tieto polia budú použité údaje o používateľovi, ktoré môžu byť v editore politík pre iOS MDM uvedené v podobe zástupného symbolu.

Dôležité:
Ak sa zobrazí chyba `Server not found in Kerberos database` po kliknutí na **Browse**, použite AD FQDN servera miesto IP adresy.

Spúšťač

Sekcia **Spúšťač** obsahuje informácie o spúšťačoch, ktoré spúšťajú vykonanie danej úlohy. Každá úloha pre server môže mať nastavený len jeden spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server. Pokiaľ v sekcii **Základné** nie je označená možnosť **Konfigurovať spúšťač**, zobrazenie sekcie **Spúšťač** nebude povolené. Úlohu je možné vytvoriť aj bez spúšťača. Takúto úlohu je následne možné spustiť manuálne, prípadne je možné spúšťač pre túto úlohu nastaviť neskôr.

Pokročilé nastavenia – Obmedzovanie

V sekcii Obmedzovanie môžete pre vytvorený spúšťač nastaviť pokročilé pravidlá pre potlačenie aktivácie spúšťača. Nastavenie obmedzovania je voliteľné.

Súhrn

Všetky použité nastavenia sú zobrazené v tejto sekcii. Skontrolujte dané nastavenia a následne kliknite na **Dokončiť**. Úloha bude vytvorená a pripravená na použitie.

4.13.7.3 Nastavenia servera

V tejto časti môžete upraviť nastavenia pre ESET Security Management Center Server.

Pripojenie

Remote Administrator port (vyžaduje reštart!) – tento port je používaný na prepojenie ESET Security Management Center Servera s agentmi. Aby sa prejavila zmena tohto nastavenia, je potrebné reštartovať službu ESMC.

WebConsole port (vyžaduje reštart!) – tento port je používaný na spojenie ESMC Servera s ESMC Web Console.

Pokročilá bezpečnosť (vyžaduje sa reštart!) – toto nastavenie povoľuje pokročilé zabezpečenie sieťovej komunikácie komponentov ESMC.

Certifikát (vyžaduje reštart!) – v tejto časti môžete spravovať certifikáty ESMC Servera. Kliknite na Zmeniť certifikát a vyberte certifikát, ktorý bude používaný vaším ESMC Serverom. Viac informácií nájdete v kapitole Partnerské certifikáty.

Dôležité:
Tieto zmeny vyžadujú reštart služby `ESET Security Management Center Server`. Inštrukcie nájdete v našom článku databázy znalostí.

Aktualizácie

Interval aktualizácie – časový interval, v ktorom budú prijímané aktualizácie. Môžete zvoliť pravidelný interval a upresniť nastavenia, prípadne môžete použiť CRON výraz.

Aktualizačný server – aktualizačný server, z ktorého bude ESMC Server sťahovať aktualizácie pre bezpečnostné produkty a komponenty ESMC.

Typ aktualizácie – vyberte typ aktualizácií modulov, ktoré má ESMC Server sťahovať. Aktuálne nainštalovanú verziu modulov ESMC Servera nájdete v sekcii **Pomocník** > **O programe**.

Priebežné aktualizácie	Aktualizácie modulov ESMC Servera budú automaticky sťahované zo servera spoločnosti ESET s najnižšou sieťovou prevádzkou. Ide o predvolené nastavenia.
Predbežné aktualizácie	Tieto aktualizácie prešli dôkladným interným testovaním a budú čoskoro dostupné pre verejnosť. Výhodou povolenia predbežných aktualizácií je, že budete mať prístup k najnovším aktualizáciám modulov ESMC Servera. Predbežné aktualizácie vám môžu v niektorých prípadoch pomôcť vyriešiť problémy s ESMC Serverom. Avšak, treba brať na vedomie, že predbežné aktualizácie nemusia byť vždy dostatočne stabilné a

	nemali by byť používané na produkčných serveroch, kde sa vyžaduje maximálna dostupnosť a stabilita. Predbežné aktualizácie sú dostupné len v prípade, že pre **Aktualizačný server** je nastavený parameter AUTOSELECT.
Oneskorené aktualizácie	Toto nastavenie umožňuje sťahovať aktualizácie zo špeciálnych aktualizačných serverov poskytujúcich aktualizácie s niekoľkohodinovým oneskorením (t. j. databázy testované v reálnom prostredí, tým pádom vyhodnotené ako stabilné). Tieto servery predstavujú presný opak serverov poskytujúcich predbežné aktualizácie. Oneskorené aktualizácie minimalizujú riziko výskytu problémov spôsobených aktualizáciami. Avšak, oneskorené aktualizácie môžu mať negatívny dopad v prípade, že kritické aktualizácie komponentov ESMC Servera musia byť rýchlo poskytnuté prostredníctvom aktualizačného mechanizmu. Oneskorené aktualizácie modulov ESMC Servera sú dostupné len v prípade, že pre **Aktualizačný server** je nastavený parameter AUTOSELECT.

Pokročilé nastavenia

HTTP Proxy – môžete použiť proxy server pre riadenie komunikácie medzi serverom a klientmi. Ak nainštalujete ESMC pomocou all-in-one inštalátora, HTTP proxy bude predvolene povolené. **HTTP Proxy** nastavenia nie sú aplikované v rámci komunikácie so zabezpečenými autentifikačnými servermi (dvojfaktorová autentifikácia – 2FA).

Volanie na prebudenie – ESMC Server dokáže spustiť okamžitú replikáciu ESET Management Agenta na klientskom počítači prostredníctvom služby EPNS. Toto je užitočné, ak nechcete čakať na pravidelný interval pripojenia ESET Management Agenta na ESMC Server. Ak napríklad chcete, aby bola úloha pre klienta spustená na klientoch okamžite alebo chcete, aby bola politika aplikovaná ihneď.

Wake-on-LAN – ak chcete odosielať pokyn Wake-on-LAN na jednu alebo viacero IP adries, je potrebné nastaviť **rozosielacie adresy**.

SMTP server – povoľte používanie SMTP servera pre umožnenie odosielania e-mailových správ z ESMC Servera (napríklad e-mailových oznámení alebo správ). Upresnite podrobnosti vášho SMTP servera.

Active Directory – môžete definovať, aby vaše AD nastavenia (hostiteľ, prihlasovacie meno, heslo a koreňový kontajner) boli predvolene používané v rámci úloh súvisiacich so synchronizáciou s Active Directory.

Syslog server – v rámci tejto funkcie môžete nastaviť, aby na váš Syslog server boli z ESMC odosielané oznámenia a správy o udalostiach. Je tiež možné exportovať protokoly z bezpečnostného produktu spoločnosti ESET nainštalovaného na klientskom počítači a odosielať ich na Syslog server.

Statické skupiny – táto funkcia umožňuje automatické párovanie nájdených počítačov s počítačmi, ktoré sa už v statických skupinách nachádzajú. Párovanie funguje na základe hláseného názvu hostiteľa ESET Management Agentom a ak tomu nie je možné dôverovať, odporúčame túto funkciu vypnúť. Ak párovanie zlyhá, počítač bude umiestnený do skupiny Stratené a nájdené.

Repozitár – umiestnenie repozitára, kde sú uložené všetky inštalačné súbory.

Poznámka:
Predvolený repozitár je nastavený na **AUTOSELECT**. Je možné vytvoriť a používať offline repozitár.

Diagnostika – môžete zapnúť alebo vypnúť odosielanie anonymných správ so štatistickými informáciami o zlyhaní programu do spoločnosti ESET. Povolením tejto možnosti nám pomáhate zlepšovať naše produkty.

Zapisovanie do protokolov – môžete nastaviť úroveň podrobnosti protokolov, čím určíte úroveň informácií, ktoré budú zhromažďované a zapisované do protokolov – od úrovne **Sledovanie** (informačné) až po **Závažné** (najdôležitejšie, kritické informácie).

Aktuálne súbory protokolu ESMC Servera sa nachádzajú v nasledujúcom umiestnení:

- Windows: *C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
- Linux: */var/log/eset/RemoteAdministrator/Server/*

V tejto časti je možné povoliť a nastaviť exportovanie protokolov do Syslogu.

Vyčistiť databázu – môžete nastaviť pravidelné čistenie protokolov, aby sa predišlo preťaženiu databázy. Čistenie databázy vymaže nasledujúce typy protokolov: SysInspector protokoly a protokoly, ktoré už nie sú zozbieravané (protokoly z odstránených zariadení a protokoly z odstránených šablón správ). Proces čistenia databázy sa podľa predvolených nastavení spúšťa každú polnoc. Zmeny v týchto nastaveniach sa prejavia po nasledujúcom čistení. Interval čistenia môžete nastaviť pre každý z nasledujúcich typov protokolov:

Typ protokolu	Príklad typu protokolu
Protokoly incidentov	Protokoly o hrozbách s vysokou závažnosťou.
Protokoly správy	Údaje o kvalite služby.
Protokoly auditov	Správy o audite.
Protokoly monitorovania	Protokoly Web Console, protokoly správy zariadení a protokoly HIPS s nízkou závažnosťou.

Prispôsobenie

Prispôsobiť používateľské rozhranie – môžete pridať vlastné logo, ktoré bude zobrazované v ESMC Web Console a v správach vygenerovaných na základe úlohy pre server.

- **Žiadne** – základný dizajn bez použitia vlastného loga.
- **Co-branding** – povoľuje použitie vlastného loga vo Web Console a v päte správ.
- **White-labeling** – povoľuje použitie vlastného loga vo Web Console a v päte alebo hlavičke správ.

Logo spoločnosti

- **Logo s tmavým pozadím** (hlavička Web Console) – logo bude zobrazené v ľavom hornom rohu rozhrania Web Console.
- **Logo so svetlým pozadím** – logo bude zobrazené v hlavičke správ (v prípade vlastníkov MSP licencie) alebo v päte správ (pri použití nastavenia Co-branding) vygenerovaných na základe úlohy pre server.

Kliknutím na  vyberte logo. Kliknutím na môžete aktuálne logo stiahnuť. Kliknutím na môžete aktuálne logo vymazať.

Správy – ak je toto nastavenie povolené, môžete do poľa Text päty správy zadať ľubovoľný text, ktorý bude umiestnený v pravom dolnom rohu správ vygenerovaných vo formáte PDF.

Dôležité:
Vlastné logo nie je možné použiť spoločne s vlastným textom päty správy. Logo je totiž umiestnené na rovnakom mieste ako text päty správy. Ak sa súčasne použije logo aj text päty správy, viditeľné bude iba logo. Pri použití nastavenia **White-labeling** bude vlastné logo zobrazené v ľavom hornom rohu správy; menšie logo ESET bude umiestnené v pravom dolnom rohu namiesto textu päty správy.

4.13.7.3.1 Pokročilá bezpečnosť

Zapnutím Pokročilej bezpečnosti aktivujete toto nastavenie pre sieťovú komunikáciu komponentov ESMC.

Pokročilá bezpečnosť zahŕňa tieto funkcie:

- Novovytvorené certifikáty a certifikačné autority používajú SHA-256 (miesto SHA-1).
- ESMC Server používa na komunikáciu s agentmi najnovší protokol TLS (TLS 1.2).
- Zapnutá Pokročilá bezpečnosť si vynucuje používanie TLS 1.2 pre Syslog a SMTP komunikáciu.

Dôležité:
Ak zapnete Pokročilú bezpečnosť, budete musieť pred začatím používania tejto funkcie reštartovať ESMC Server.

Minimálne požiadavky týkajúce sa kompatibility zahŕňajú nasledovné:

- Windows: Windows Vista alebo novší.
- Linux: OpenSSL 1.0.1 a novšie na podporovanej verzii operačného systému (Ubuntu 12.04 a novší, RHEL/CentOS 6 a novší, Debian 7.0 a novší).
- OS X 10.9 a novší.

Dôležité:
Pokročilá bezpečnosť neovplyvňuje už existujúce certifikačné autority a certifikáty, ovplyvnené sú iba nové certifikačné autority a certifikáty vytvorené po aktivovaní Pokročilej bezpečnosti.

Ak chcete aplikovať Pokročilú bezpečnosť na existujúcu ESMC infraštruktúru, je potrebné nahradiť existujúce certifikáty.

Poznámka:
ESET Management Agent 7 obsahuje vlastný SSL modul, ktorý umožňuje použitie TLS 1.2 aj so staršími operačnými systémami (Windows XP a Windows Server 2003).

Kompatibilitu svojho klientskeho zariadenia so systémom Linux môžete skontrolovať pomocou nasledujúceho príkazu:

```
openssl s_client -connect google.com:443 -tls1_2
```

Ako zapnúť a aplikovať Pokročilú bezpečnosť vo vašej sieti

Pred zapnutím tejto funkcie sa uistite, že všetky vaše klientske počítače môžu komunikovať cez protokol TLS 1.2 (pozrite si poznámku vyššie). Tieto zmeny si vyžadujú dvakrát reštartovať službu ESMC Server.

Pre zapnutie a aplikovanie Pokročilej bezpečnosti postupujte podľa nasledujúcich krokov:

1. Prejdite do sekcie **Viac** > **Nastavenia servera** a kliknite na tlačidlo vedľa možnosti **Pokročilá bezpečnosť (vyžaduje sa reštart!)**.
2. Kliknite na **Uložiť** pre aplikovanie nastavenia.
3. Zatvorte Web Console a reštartujte službu ESMC Server.
4. Počkajte niekoľko minút, kým sa služba znova spustí, a prihláste sa do Web Console.
5. Skontrolujte, či sú aj naďalej pripojené všetky počítače a či sa nevyskytli žiadne iné problémy.
6. Prejdite do sekcie **Viac** > **Certifikačné autority** > **Nová** a vytvorte novú certifikačnú autoritu. Nová certifikačná autorita bude automaticky odoslaná na všetky klientske počítače počas ďalšieho pripojenia agentov k serveru.
7. Vytvorte nové partnerské certifikáty podpísané novou certifikačnou autoritou. Vytvorte certifikát pre agenta a pre server (v sprievodcovi použite roletové menu **Produkt**).
8. Zmeňte svoj súčasný certifikát ESMC Servera na nový.
9. Vytvorte novú politiku pre ESET Management Agenta, pomocou čoho nastavíte svoje agenty tak, aby používali nový certifikát.
    a. V sekcii **Pripojenie** kliknite na **Certifikát** > **Otvoriť zoznam certifikátov** a vyberte nový partnerský certifikát.
    b. Priraďte politiku k počítačom, na ktorých chcete používať Pokročilú bezpečnosť.
    c. Kliknite na **Dokončiť**.
10. Keď sa už všetky zariadenia pripájajú pomocou nového certifikátu, môžete odstrániť svoju starú certifikačnú autoritu a zneplatniť staré certifikáty.

Dôležité:
Neodstraňujte svoju starú certifikačnú autoritu a nezneplatňujte staré certifikáty v prípade, že ste aplikovali **Pokročilú bezpečnosť** iba na niektoré (nie všetky) pripojené klientske počítače.

Pokročilá bezpečnosť na systémoch s nainštalovaným komponentom MDM

Toto nastavenie ovplyvní iba komunikáciu medzi ESMC Serverom a MDM Serverom. Komunikácia medzi MDM Serverom a mobilnými zariadeniami nebude ovplyvnená. Ak chcete aplikovať Pokročilú bezpečnosť na komponent

MDM, vytvorte nové MDM a Proxy certifikáty podpísané novou certifikačnou autoritou a priraďte ich pomocou politiky k MDM Serveru nasledovne:

- Politika pre ESET Mobile Device Connector > Všeobecné > HTTPS certifikát. Importujte nový MDM certifikát.
- Politika pre ESET Mobile Device Connector > Propojenie > Certifikát = Proxy certifikát.

4.13.7.3.2 SMTP server

ESET Security Management Center dokáže automaticky odosielať správy a oznámenia prostredníctvom e-mailu. Povoľte možnosť **Používať SMTP server**, prejdite do časti **Viac** > **Nastavenia servera** > **Pokročilé nastavenia** > **SMTP Server** a upresnite nasledujúce údaje:

- **Hostiteľ** – názov hostiteľa alebo IP adresa vášho SMTP servera.
- **Port** – SMTP využíva štandardne port 25, ale môžete ho zmeniť v prípade, že váš SMTP server využíva iný port.
- **Prihlasovacie meno** – ak váš SMTP server vyžaduje overenie, zadajte prihlasovacie meno SMTP účtu (neuvádzajte doménu, pretože to nebude fungovať).
- **Heslo** – heslo pre používateľský SMTP účet.
- **Typ zabezpečenia pripojenia** – upresnite typ pripojenia, predvolená je možnosť **Nezabezpečený**, ale ak váš SMTP server umožňuje zabezpečené pripojenia, vyberte TLS alebo STARTTLS. Ak chcete, aby bolo vaše pripojenie bezpečnejšie, je dobré použiť STARTTLS alebo SSL/TLS rozšírenie, ktoré využíva na šifrovanú komunikáciu osobitný port.
- **Typ autentifikácie** – prednastavená je možnosť **Bez autentifikácie**, avšak môžete vybrať vhodný typ overovania z roletového menu (napr. prihlásenie, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM alebo automatický).
- **E-mailová adresa odosielateľa** – upresnite adresu odosielateľa, ktorá bude zobrazená v hlavičke e-mailovej správy obsahujúcej oznámenie (Od:).
- **Test SMTP servera** – pomocou tejto funkcie môžete overiť, či sú nastavenia SMTP správne. Stlačte tlačidlo **Odoslať testovací e-mail** a otvorí sa kontextové okno. Zadajte e-mailovú adresu prijímateľa a testovací e-mail bude odoslaný prostredníctvom SMTP servera na jeho adresu. Skontrolujte poštovú schránku prijímateľa a overte, či bol testovací e-mail úspešne doručený.

4.13.7.3.3 Automatické párovanie nájdených počítačov

V situácii, keď existuje viacero inštancií rovnakého počítača v ESMC (napr. pri preinštalovaní ESET Management Agenta na klientskom počítači, ktorý je už spravovaný), funkcia **Automaticky párovať nájdené počítače** tieto inštancie spáruje do jednej. Tým pádom by nemalo byť potrebné manuálne overovanie a triedenie nájdených počítačov.

Párovanie funguje na základe názvu hostiteľa hláseného ESET Management Agentom. Ak takýto princíp z nejakého dôvodu nemôže byť považovaný za spoľahlivý, odporúčame funkciu **Automaticky párovať nájdené počítače** vypnúť. Ak párovanie zlyhá, počítač bude umiestnený do skupiny **Stratené a nájdené**. Podstatou párovania je, že pri každom preinštalovaní ESET Management Agenta na už spravovanom počítači by bol takýto počítač automaticky spárovaný, a tým pádom správne umiestnený do ESMC bez vášho zásahu. Nový ESET Management Agent tiež okamžite dostane svoje politiky a úlohy.

- Pri **vypnutí** tejto funkcie budú počítače, ktoré by mali byť umiestnené do skupiny **Stratené a nájdené**, spárované s prvým nájdeným nespravovaným počítačom (zástupný symbol, ikona kruhu) nachádzajúcim sa kdekoľvek v stromovej štruktúre ESMC. Ak sa nevyskytuje žiadny zástupný symbol s rovnakým názvom, počítač bude umiestnený do skupiny Stratené a nájdené.
- Ak je táto funkcia **zapnutá (predvolené)**, počítače, ktoré by mali byť umiestnené do skupiny **Stratené a nájdené**, budú spárované s prvým nájdeným nespravovaným počítačom (zástupný symbol, ikona kruhu) nachádzajúcim sa kdekoľvek v stromovej štruktúre ESMC. Ak sa nevyskytuje žiadny zástupný symbol s rovnakým názvom, počítač bude spárovaný s prvým nájdeným spravovaným počítačom (ikona upozornenia alebo začiarknutia) nachádzajúcim sa kdekoľvek v stromovej štruktúre ESMC. Ak toto párovanie takisto zlyhá, počítač bude umiestnený do skupiny Stratené a nájdené.

Poznámka:
Ak si neželáte používať automatické párovanie, vypnite túto funkciu. Vždy môžete počítače overovať a triediť manuálne.

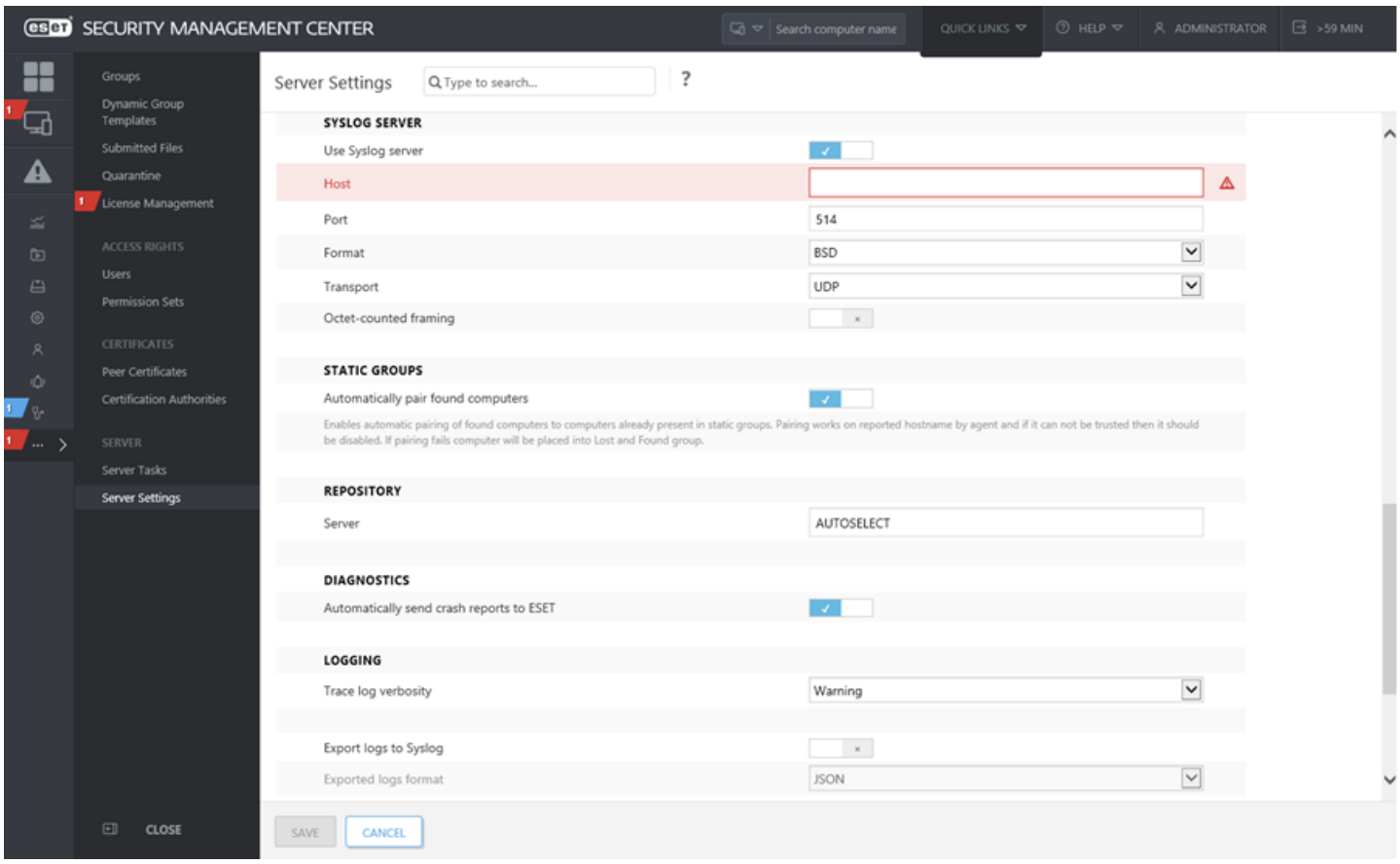
4.13.7.3.4 Syslog server

Ak máte vo svojej sieti bežiaci Syslog server, môžete nakonfigurovať ESMC Server tak, aby na Syslog server odosielal oznámenia. Môžete tiež povoliť exportovanie protokolov do Syslogu, aby ste dostávali informácie o určitých udalostiach (napr. o udalostiach týkajúcich sa hrozieb, o udalostiach firewallu, modulu HIPS atď.) z klientskych počítačov, na ktorých je spustený bezpečnostný produkt spoločnosti ESET (napr. ESET Endpoint Security).

Pre aktivovanie Syslog servera postupujte podľa nasledujúcich krokov:

1. Prejdite do sekcie **Viac** > **Nastavenia servera** > **Pokročilé nastavenia**. > **Syslog server** a použite tlačidlo prepínača vedľa položky **Použiť Syslog server**.
2. Upravte nasledujúce povinné nastavenia:
   a. **Hostiteľ** (IP adresa alebo názov hostiteľa servera, na ktorý majú byť zasielané Syslog správy)
   b. **Port** (predvolené číslo portu je 514)
   c. **Formát** protokolu: **BSD** (špecifikácia), **Syslog** (špecifikácia)
   d. **Prenos** – prenosový protokol pre odosielanie správ na Syslog server (**UDP**, **TCP**, **TLS**)

Vykonané zmeny uložte kliknutím na tlačidlo **Uložiť**.



Poznámka:
Do pravidelného protokolu aplikácie sú dáta zapisované nepretržite. Syslog slúži len ako nástroj na exportovanie niektorých nepravidelných udalostí, akými sú napríklad oznámenia alebo udalosti klientskych počítačov.

4.13.7.3.5 Exportovanie protokolov do Syslogu

ESET Security Management Center dokáže exportovať určité protokoly/udalosti a odosielať ich na váš Syslog server. Na Syslog server sú exportované udalosti z nasledujúcich kategórií protokolov: Hrozba, Firewall, HIPS, Audit a Enterprise Inspector. Udalosti sú generované na spravovaných klientskych počítačoch, na ktorých je spustený bezpečnostný produkt spoločnosti ESET (napr. ESET Endpoint Security). Tieto udalosti môžu byť spracované akýmkoľvek nástrojom SIEM (Security Information and Event Management) určeným na správu bezpečnostných informácií a udalostí, ktorý je schopný importovať udalosti zo Syslog servera. Udalosti sú zapisované na Syslog server nástrojom ESET Security Management Center.

1. Pre aktiváciu Syslog servera kliknite na **Viac** > **Nastavenia servera** > **Pokročilé nastavenia** > **Syslog server** > **Použiť Syslog server**.
2. Pre aktiváciu exportu protokolov kliknite na **Viac** > **Nastavenia servera** > **Pokročilé nastavenia** > **Protokoly** > **Exportovať protokoly do Syslogu**.
3. Vyberte jeden z nasledujúcich formátov pre exportované protokoly (t. j. pre správy o udalostiach), ktoré budú zasielané na Syslog server:
   a. JSON (JavaScript Object Notation)
   b. LEEF (Log Event Extended Format) – formát používaný aplikáciou QRadar spoločnosti IBM

4.13.7.3.6 Udalosti exportované vo formáte LEEF

Formát LEEF je prispôsobený formát udalostí používaný SIEM nástrojom IBM® Security QRadar®. Udalosti majú predvolené a vlastné atribúty. V rámci ESMC sa používajú niektoré predvolené atribúty popísané v oficiálnej dokumentácii spoločnosti IBM. Vlastné atribúty sú rovnaké ako v prípade formátu JSON. Rozlišuje sa päť kategórií udalostí:

- Hrozba
- Firewall
- HIPS
- Audit
- Upozornenia Enterprise Inspectora

Poznámka:
Viac informácií o formáte Log Event Extended Format (LEEF) nájdete na oficiálnej webovej stránke spoločnosti IBM.

4.13.7.3.7 Udalosti exportované vo formáte JSON

JSON je jednoduchý formát pre výmenu dát. Je založený na dvoch dátových štruktúrach: kolekcia párov názov-hodnota a zoradený zoznam hodnôt.

Exportované udalosti

Táto sekcia obsahuje podrobnosti o formáte a význame atribútov všetkých exportovaných udalostí. Správa o udalosti má podobu objektu JSON vrátane niektorých povinných a voliteľných kľúčov (atribútov). Každá exportovaná udalosť bude obsahovať nasledujúci kľúč:

event_type	reťazec		Typ exportovanej udalosti: Threat_Event, FirewallAggregated_Event, HipsAggregated_Event.
ipv4	reťazec	voliteľné	IPv4 adresa počítača, ktorý generoval udalosť.
ipv6	reťazec	voliteľné	IPv6 adresa počítača, ktorý generoval udalosť.

event_type	reťazec		Typ exportovanej udalosti: Threat_Event, FirewallAggregated_Event, HipsAggregated_Event.
source_uuid	reťazec		UUID počítača, ktorý generoval udalosť.
occurred	reťazec		Čas vo formáte UTC, kedy udalosť vznikla. Formát: %d-%b-%Y %H:%M:%S.
severity	reťazec		Závažnosť udalosti. Možné hodnoty (od najmenej závažnej po najviac závažnú) sú: Informácie, Upozornenie, Varovanie, Chyba, Kritický, Závažný.

Vlastné kľúče (atribúty) podľa **event_type**:

1. ThreatEvent

Všetky záznamy o zachytených hrozbách sú spravované koncovými bezpečnostnými produktmi a odosielané na Syslog. Záznam vyzerá nasledovne:

threat_type	reťazec	voliteľné	Typ hrozby
threat_name	reťazec	voliteľné	Názov hrozby
threat_flags	reťazec	voliteľné	Príznaky súvisiace s hrozbou
scanner_id	reťazec	voliteľné	ID skenera
scan_id	reťazec	voliteľné	ID kontroly
engine_version	reťazec	voliteľné	Verzia skenovacieho jadra
object_type	reťazec	voliteľné	Typ objektu týkajúci sa tejto udalosti
object_uri	reťazec	voliteľné	URL objektu
action_taken	reťazec	voliteľné	Akcia vykonaná koncovým produktom
action_error	reťazec	voliteľné	Chybové hlásenie v prípade, že „akcia“ nebola úspešná.
threat_handled	bool	voliteľné	Udáva, či hrozba bola alebo nebola vyriešená.
need_restart	bool	voliteľné	Informácia o tom, či je potrebný reštart.
username	reťazec	voliteľné	Názov používateľského účtu spojeného s touto udalosťou
processname	reťazec	voliteľné	Názov procesu spojeného s touto udalosťou
circumstances	reťazec	voliteľné	Krátka informácia o tom, čo spôsobilo danú udalosť.
hash	reťazec	voliteľné	SHA1 hash (hrozby) dátového toku.
firstseen	reťazec	voliteľné	Čas a dátum, kedy bola hrozba po prvýkrát zistená na zariadení. ESMC používa rozdielne formáty času a dátumu pre atribút `firstseen` (a každý iný atribút času a dátumu) v závislosti od výstupného formátu (JSON alebo LEEF): • JSON formát: "%d-%b-%Y %H:%M:%S" • LEEF formát: "%b %d %Y %H:%M:%S"

2. FirewallAggregated_Event

Protokoly udalostí generované firewallom ESET agreguje riadiaci ESET Management Agent na účely zníženia množstva dát prenášaných počas replikácie ESET Management Agenta/ESMC Servera. Záznam o udalostiach firewallu vyzerá nasledovne:

event	reťazec	voliteľné	Názov udalosti
source_address	reťazec	voliteľné	Adresa zdroja udalosti
source_address_type	reťazec	voliteľné	Typ adresy zdroja udalosti
source_port	číslo	voliteľné	Port zdroja udalosti
target_address	reťazec	voliteľné	Adresa cieľa udalosti
target_address_type	reťazec	voliteľné	Typ adresy cieľa udalosti
target_port	číslo	voliteľné	Port cieľa udalosti
protocol	reťazec	voliteľné	Protokol
account	reťazec	voliteľné	Názov používateľského účtu spojeného s touto udalosťou
process_name	reťazec	voliteľné	Názov procesu spojeného s touto udalosťou
rule_name	reťazec	voliteľné	Názov pravidla
rule_id	reťazec	voliteľné	ID pravidla
inbound	bool	voliteľné	Informácia, či išlo o prichádzajúce pripojenie.
threat_name	reťazec	voliteľné	Názov hrozby
aggregate_count	číslo	voliteľné	Počet rovnakých správ vygenerovaných koncovým produktom medzi dvoma replikáciami ESMC Agenta na ESET Management Server.

3. HIPSAggregated_Event

Udalosti z modulu HIPS (Host-based Intrusion Prevention System) sú filtrované na základe **závažnosti** pred tým, ako sú ďalej odosielané v podobe Syslog správ. Na Syslog sú odosielané len udalosti s úrovňou **závažnosti** *Chyba*, *Kritický* a *Závažný*. Záznam o udalostiach modulu HIPS vyzerá nasledovne:

application	reťazec	voliteľné	Názov aplikácie
operation	reťazec	voliteľné	Operácia
target	reťazec	voliteľné	Cieľ
action	reťazec	voliteľné	Akcia
rule_name	reťazec	voliteľné	Názov pravidla
rule_id	reťazec	voliteľné	ID pravidla
aggregate_count	číslo	voliteľné	Počet rovnakých správ vygenerovaných koncovým produktom medzi dvoma replikáciami ESMC Agenta na ESET Management Server.

4. Audit

ESMC preposiela do Syslogu správy z interného protokolu auditu servera. Záznam o udalostiach vyzerá nasledovne:

domain	reťazec	voliteľné	Doména protokolu auditu
action	reťazec	voliteľné	Vykonávaná akcia
target	reťazec	voliteľné	Cieľ, na ktorom je akcia vykonávaná.
detail	reťazec	voliteľné	Podrobný popis akcie
user	reťazec	voliteľné	Užívateľ vykonávajúci akciu
result	reťazec	voliteľné	Výsledok akcie

5. Enterprise Inspector Alert Event

ESMC preposiela do Syslogu upozornenia ESET Enterprise Inspector. Záznam o udalostiach vyzerá nasledovne:

processname	reťazec	voliteľné	Názov procesu, ktorý spôsobil upozornenie.
username	reťazec	voliteľné	Vlastník procesu
rulename	reťazec	voliteľné	Názov Enterprise Inspector pravidla, ktoré aktivovalo toto upozornenie.
count	číslo	voliteľné	Počet upozornení tohto typu vygenerovaných od posledného upozornenia

4.14 Spúšťače a obmedzovanie

Spúšťače sú senzory, ktoré reagujú na určité udalosti vopred definovaným spôsobom. Slúžia na spúšťanie úloh pre server, ku ktorým sú priradené. Môžu byť aktivované pomocou Plánovača (naplánovanej úlohy) alebo systémovou udalosťou.

Dôležité:
Jednotlivé spúšťače nie je možné opätovne priradiť k ďalším úlohám. Každá úloha pre server musí používať samostatný spúšťač. Každý spúšťač môže spúšťať len jednu úlohu pre server.

Spúšťač nespúšťa novopriradené úlohy okamžite, miesto toho sú úlohy spustené vtedy, keď spúšťač dostane impulz. Citlivosť spúšťača pre rôzne udalosti je možné redukovať pomocou obmedzovania.

Typy spúšťačov úloh pre server:

Naplánované

- **Naplánovať raz** – tento spúšťač spustí úlohu raz v presne naplánovaný čas. Môžete tiež zadať maximálny čas, o ktorý sa spustenie úlohy môže oneskoriť.
- **Denne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch. Môžete zadať začiatok a koniec časového intervalu, počas ktorého sa bude úloha spúšťať. Môžete napríklad zvoliť, aby sa úloha spúšťala vždy cez víkendové dni po dobu desiatich za sebou idúcich týždňov.
- **Týždenne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch týždňa. Môžete napríklad zvoliť, aby sa úloha spúšťala každý pondelok a piatok v období od 1. júla do 31. augusta.
- **Mesačne** – tento spúšťač spustí úlohu vždy vo zvolených dňoch a zvolenom týždni mesiaca počas vami stanoveného obdobia. Hodnota zadaná do poľa **Opakovať** určuje pracovný deň v mesiaci (napríklad druhý pondelok), počas ktorého bude úloha spustená.
- **Ročne** – tento spúšťač spustí úlohu každý rok (alebo každých niekoľko rokov, ak použijete toto nastavenie) v deň a čas, ktorý zadáte do poľa Štart.

Poznámka:

Náhodný interval oneskorenia je možné nastaviť pre všetky naplánované typy spúšťačov. Toto nastavenie určuje maximálny čas, o ktorý sa spustenie úlohy môže oneskoriť. Použitie náhodných oneskorení vykonania plánovaných úloh pomáha predchádzať vyťaženiu servera.

PRÍKLAD:
Ak používateľ *John* pre **Úlohu pre server** nastavil spúšťač na hodnotu **Týždenne**, zvolil deň opakovania na *pondelok*, do poľa **Štart** zadal *2017 feb 10 8:00:00*, **Náhodný interval oneskorenia** nastavil na *1 hodinu* a do poľa **Ukončiť do** zadal *2017 apr 6 00:00:00*, úloha bude spúšťaná s náhodným maximálne hodinovým oneskorením medzi 8:00 a 9:00 každý pondelok až do stanoveného dátumu a času ukončenia.

Dynamická skupina

- **Členy dynamickej skupiny sa zmenili** – tento spúšťač sa aktivuje vtedy, keď sa zmení obsah dynamickej skupiny. Napríklad, ak klient vstúpi alebo odíde z konkrétnej dynamickej skupiny.
- **Veľkosť dynamickej skupiny sa zmenila podľa hraničnej hodnoty** – tento spúšťač sa aktivuje v prípade, ak je počet klientov nachádzajúcich sa v dynamickej skupine väčší alebo menší ako zadaná hraničná hodnota. Napríklad, ak sa v konkrétnej skupine nachádza viac ako 100 počítačov.
- **Veľkosť dynamickej skupiny sa zmenila počas časového obdobia** – tento spúšťač sa aktivuje v prípade, ak sa počet klientov nachádzajúcich sa v dynamickej skupine zmení počas zadaného časového obdobia. Napríklad, ak sa počet počítačov v konkrétnej skupine zvýši v priebehu hodiny o 10 %.
- **Veľkosť dynamickej skupiny sa zmenila podľa porovnanej skupiny** – tento spúšťač sa aktivuje v prípade, ak sa počet klientov nachádzajúcich sa v pozorovanej dynamickej skupine zmení podľa porovnávanej skupiny (statickej alebo dynamickej). Napríklad, ak je viac ako 10 % všetkých počítačov infikovaných (porovnávajú sa skupiny **Všetko** a **Infikované**).

Iné

- **Spustenie servera** – tento spúšťač sa aktivuje vtedy, keď sa spustí server. Tento spúšťač sa používa napr. pri úlohe Synchronizácia statickej skupiny.
- **Spúšťač protokolu udalosti** – tento spúšťač sa aktivuje v prípade, že v protokole je zaznamenaná určitá udalosť. Napríklad, ak bola v protokole **Kontroly** počítača zaznamenaná hrozba. Pre tento typ spúšťača sa v sekcii Pokročilé nastavenia – Obmedzovanie nachádza niekoľko špeciálnych nastavení.
- **CRON výraz** – tento spúšťač sa aktivuje v deň a čas stanovený CRON výrazom.

Naplánovaný spúšťač spúšťa úlohu v čase a dátume zadefinovanom v nastaveniach spúšťača. Úloha môže byť naplánovaná tak, aby bola spustená **raz**, opakovane alebo na základe CRON výrazu.

4.14.1 CRON výraz

CRON výraz sa používa na nastavovanie podmienky spúšťania. Hlavne sa však používa na plánované opätovné spúšťanie. Je to textový reťazec pozostávajúci zo šiestich alebo siedmich polí, ktoré predstavujú individuálne hodnoty plánu. Tieto polia sú oddelené medzerou a obsahujú niektorú z povolených hodnôt v rôznych kombináciách.

CRON výraz môže byť jednoduchý, napr.: `* * * * ? *` alebo zložitejší, napr.: `0/5 14,18,3-39,52 * ? JAN,MAR,SEP MON-FRI 2012-2020`

Zoznam hodnôt, ktoré môžete použiť v CRON výraze:

Názov	Vyžaduje sa	Hodnota	Povolené špeciálne znaky
Sekundy	Áno	0-59	, - * / R
Minúty	Áno	0-59	, - * / R
Hodiny	Áno	0-23	, - * / R
Deň v mesiaci	Áno	1-31	, - * / ? L W

Názov	Vyžaduje sa	Hodnota	Povolené špeciálne znaky
Mesiac	Áno	1-12 alebo JAN-DEC	, - */
Deň v týždni	Áno	0-6 alebo SUN-SAT	, - / ? L #
Rok	Áno	1970-2099	, - * /

Syntax CRON výrazu je nasledujúca:

```
┌──────────── Sekundy (0 – 59)
│ ┌────────── Minúty (0 – 59)
│ │ ┌──────── Hodiny (0 – 23)
│ │ │ ┌────── Deň v mesiaci (1 – 31)
│ │ │ │ ┌──── Mesiac (1 – 12 alebo JAN-DEC)
│ │ │ │ │ ┌── Deň v týždni (0 – 6 alebo SUN-SAT)(napr., 0 je to isté
ako SUN)
│ │ │ │ │ │ ┌── Rok
│ │ │ │ │ │ │
* * * * * ? *
```

- 0 0 0 znamená polnoc (sekundy, minúty, hodiny).
- Použite znak ? v prípade, že hodnota nemôže byť definovaná, pretože bola definovaná v inom poli (deň v mesiaci alebo deň v týždni).
- Znak * predstavuje každý výskyt (sekundy, minúty, hodiny, deň v mesiaci, mesiac, deň v týždni, rok).
- SUN znamená nedeľa.

Poznámka:
V názvoch mesiacov a dní v týždni sa nerozlišujú malé a veľké písmená. Napríklad, MON je akceptovateľné aj v podobe mon a JAN je akceptovateľné aj v podobe jan.

Špeciálne znaky:

Čiarka (,)
Čiarky sa používajú na oddeľovanie položiek v zozname. Napríklad, ak použijete „MON,WED,FRI“ v 6. poli (deň v týždni), bude to znamenať pondelky, stredy a piatky.

Spojovník (-)
Spojovník sa používa na určenie rozsahu. Napríklad, 2012-2020 znamená každý rok medzi 2012 a 2020 (vrátane).

Hviezdička (*)
Tento znak sa používa ako zástupný symbol pre všetky možné hodnoty v danom poli. Napríklad, * v poli minúty bude predstavovať každú minútu. Hviezdička nemôže byť použitá v poli deň v týždni.

Otáznik (?)
Pri výbere konkrétneho dňa môžete zadať buď deň v mesiaci, alebo deň v týždni. Nemôžete zadať oba. Ak zadáte deň v mesiaci, musíte použiť ? pre deň v týždni a naopak. Napríklad, ak chcete, aby sa spúšťač aktivoval v určitý deň v mesiaci (napr. 10.), ale nezáleží na tom, ktorý deň by to mal presne byť, zadajte hodnotu 10 do poľa deň v mesiaci a otáznik ? zadajte do poľa deň v týždni.

Hash (#)
Tento znak sa používa na definovanie „n-tého“ dňa v mesiaci. Napríklad, hodnota 4#3 v poli deň v týždni predstavuje tretí štvrtok v mesiaci (deň 4 = štvrtok a #3 = 3. štvrtok v mesiaci). Ak zadáte #5 a mesiac nemá toľko dní, podmienka nebude uplatnená a spúšťač sa neaktivuje.

Lomka (/)
Lomka popisuje inkrementy rozsahu. Napríklad, 3-59/15 v 2. poli (minúty) predstavuje tretiu minútu v hodine a každých ďalších 15 minút.

Posledný (L)
Ak sa použije v poli deň v týždni, umožní vám vytvoriť špecifickú konštrukciu, ako napr. posledný piatok (5L) v mesiaci. V poli deň v mesiaci predstavuje posledný deň mesiaca. Napríklad, 31. deň v januári a 28. deň vo februári.

Pracovný deň v týždni (W)
Znak W je povolený pre pole deň v mesiaci. Používa sa len pre pracovné dni (pondelok – piatok) a v prípade, že deň v mesiaci pripadne na víkend, použije sa najbližší pracovný deň. Napríklad, ak zadáte 15W ako hodnotu do poľa deň v mesiaci, bude to znamenať najbližší pracovný deň k 15. dňu v mesiaci. To znamená, že ak 15. vychádza na sobotu, spúšťač sa aktivuje v piatok 14. Ak 15. vychádza napr. na nedeľu, spúšťač sa aktivuje v pondelok 16. Ak však zadáte 1W ako hodnotu pre deň v mesiaci, pričom 1. je sobota, spúšťač sa aktivuje v pondelok 3.

Poznámka:
Znaky L a W sa môžu v poli deň v mesiaci aj kombinovať, výsledkom čoho bude LW, čo znamená posledný pracovný deň v mesiaci.

Náhodný (R)
R predstavuje špeciálny znak pre ERA CRON výraz, ktorý umožňuje definovať náhodné časové momenty. Napríklad, R 0 0 * * ? * aktivuje spúšťač každý deň o 00.00 v náhodnú sekundu (0-59).

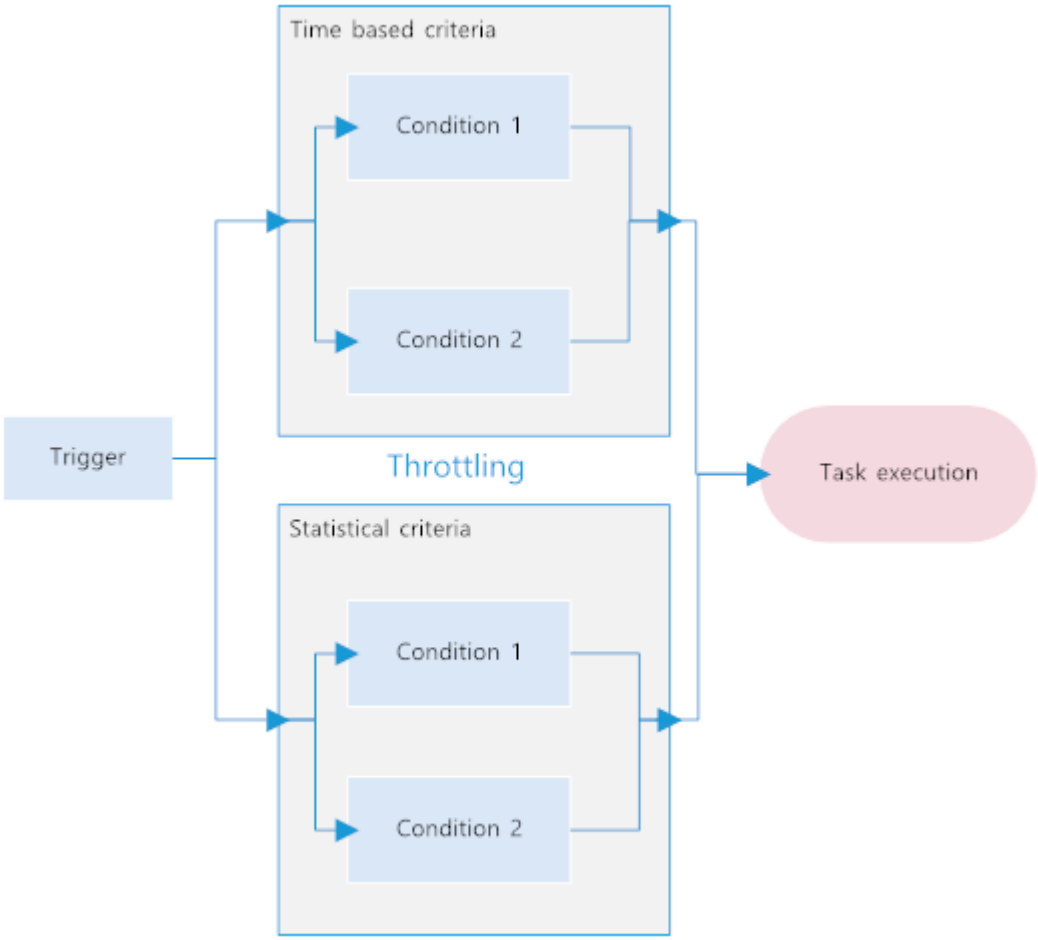
Dôležité:
Odporúčame vám používať náhodné časové momenty, aby sa zabránilo prípadu, kedy sa všetky ESET Management Agenty pripoja na váš ESMC Server súčasne.

Nižšie nájdete skutočné príklady, ktoré znázorňujú niektoré variácie CRON výrazu:

CRON výraz	Význam
0 0 12 * * ? *	Spustí sa každý deň o 12.00 (poludnie).
R 0 0 * * ? *	Spustí sa každý deň o 00.00 v náhodnú sekundu (0-59).
R R R 15W * ? *	Spustí sa v 15. dni každý mesiac v náhodnom čase (sekundy, minúty, hodiny). To znamená, že ak 15. vychádza na sobotu, spúšťač sa aktivuje v piatok 14. Ak 15. vychádza napr. na nedeľu, spúšťač sa aktivuje v pondelok 16.
0 15 10 * * ? 2016	Spustí sa každý deň o 10.15 v priebehu roka 2016.
0 * 14 * * ? *	Spustí sa každú minútu medzi 14.00 a 14.59, každý deň.
0 0/5 14 * * ? *	Spustí sa každých minút medzi 14.00 a 14.55, každý deň.
0 0/5 14,18 * * ? *	Spustí sa každých 5 minút medzi 14.00 a 14.55 a každých 5 minút medzi 18.00 a 18.55, každý deň.
0 0-5 14 * * ? *	Spustí sa každú minútu medzi 14.00 a 14.05, každý deň.
0 10,44 14 ? 3 WED *	Spustí sa o 14.10 a 14.44 každú stredu v mesiaci marec.
0 15 10 ? * MON-FRI *	Spustí sa o 10.15 každý pracovný deň (pondelok, utorok, streda, štvrtok a piatok).
0 15 10 15 * ? *	Spustí sa o 10.15 v 15. dni každého mesiaca.
0 15 10 ? * 5L *	Spustí sa o 10.15 posledný piatok každého mesiaca.
0 15 10 ? * 5L 2016-2020	Spustí sa o 10.15 každý posledný piatok každého mesiaca od roku 2016 do roku 2020 (vrátane).
0 15 10 ? * 5#3 *	Spustí sa o 10.15 tretí piatok každého mesiaca.
0 0 * * * ? *	Spustí sa každú hodinu, každý deň.

4.14.2 Pokročilé nastavenia – Obmedzovanie

Obmedzovanie sa používa na obmedzenie vykonania úlohy. Obmedzovanie môžete nastaviť napríklad pre tie úlohy, ktoré sú spúšťané pri veľmi často sa vyskytujúcej udalosti. Za určitých podmienok môže obmedzovanie úplne potlačiť aktiváciu spúšťača, a tým zabrániť spusteniu úlohy, pre ktorú je spúšťač vytvorený. Pri každom prijatí impulzu na aktivovanie spúšťača prebehne vyhodnocovanie podmienok spúšťača podľa schémy uvedenej nižšie. Len tie spúšťače, ktoré splnia zadefinované podmienky, vyvolajú spustenie a vykonanie k nim priradenej úlohy. Ak nie sú nastavené žiadne podmienky obmedzovania, daná úloha bude spúšťaná pri každej udalosti aktivujúcej spúšťač.



Podmienky pre potlačenie aktivácie spúšťača sú rozdelené do troch kategórií:

1. **Kritériá na základe času**
2. **Štatistické kritériá**
3. **Kritériá protokolu udalostí**

Úloha je vykonaná v prípade, že platí nasledovné:

- Boli splnené všetky druhy podmienok.
- Podmienky musia byť nastavené; pokiaľ je podmienka prázdna, bude vynechaná.
- Všetky časové podmienky musia byť splnené, keďže ich pri vyhodnocovaní spája logický operátor AND.
- Všetky štatistické podmienky, ktoré pri vyhodnocovaní spája logický operátor AND, musia byť splnené; pri použitom logickom operátore OR musí byť splnená aspoň jedna zo štatistických podmienok.
- Ak sú pre jednu úlohu nastavené časové aj štatistické podmienky, musí byť splnená každá z týchto podmienok, keďže ich pri vyhodnocovaní spája logický operátor AND – len v tom prípade bude úloha spustená.

Ak sú podmienky splnené, všetky zaznamenané informácie o stave spúšťača budú vynulované (počítanie výskytov začína znova od nuly). Toto platí pre časové aj štatistické podmienky. Zaznamenané informácie sú vynulované aj pri reštartovaní agenta alebo ESMC Servera. Každá zmena spúšťača vedie k vynulovaniu jeho stavu. Odporúčame používať len jednu štatistickú podmienku a viacero časových podmienok. Nastavenie viacerých štatistických podmienok môže spôsobovať zbytočné komplikácie a pozmenené výsledky.

Predvolené nastavenia

K dispozícii sú 3 predvolené nastavenia. Po zvolení konkrétneho predvoleného nastavenia budú vaše súčasné nastavenia obmedzovania prepísané hodnotami daného predvoleného nastavenia. Tieto hodnoty môžu byť dodatočne upravené, avšak nie je možné vytvoriť nové predvolené nastavenie.

Kritériá na základe času

Časové obdobie (T2) – táto možnosť vám umožňuje nastaviť, aby počas stanoveného časového obdobia bol spúšťač aktivovaný len raz. Ak napríklad túto možnosť nastavíte na 10 sekúnd a počas tohto časového obdobia sa vyskytne 10 impulzov na aktivovanie spúšťača, len prvý z nich skutočne vyvolá spustenie úlohy.

Časový plán (T1) – táto možnosť vám umožňuje nastaviť, aby bol spúšťač aktivovaný len počas stanoveného časového rozsahu. Kliknite na **Pridať obdobie** a otvorí sa nové okno. Nastavte **Trvanie rozsahu** v zvolených časových jednotkách. Vyberte jednu možnosť zo zoznamu **Opakovanie** a vyplňte polia, ktoré sa menia v závislosti od zvoleného opakovania. Opakovanie môžete definovať aj v podobe CRON výrazu. Kliknite na **OK** pre uloženie rozsahu. Môžete pridávať viaceré časové obdobia, ktoré budú zoradené chronologicky.

Úloha je spustená len v tom prípade, že sú splnené všetky nastavené časové podmienky.

Štatistické kritériá

Podmienka – štatistické podmienky je možné kombinovať nasledovne:

- **Odoslať oznámenie po splnení všetkých štatistických kritérií** – LOGICKÝ OPERÁTOR AND je použitý v rámci vyhodnotenia.
- **Odoslať oznámenie po splnení aspoň jedného štatistického kritéria** – logický operátor OR je použitý v rámci vyhodnotenia.

Počet výskytov (S1) – táto možnosť vám umožňuje nastaviť, aby bol spúšťač aktivovaný len pri každom X-tom impulze (výskyte). Ak napríklad zadáte hodnotu 10, bude započítaný len každý desiaty impulz na aktivovanie spúšťača.

Počet výskytov vo zvolenom časovom období

Počet výskytov (S2) – táto možnosť vám umožňuje nastaviť, aby bol spúšťač aktivovaný na základe frekvencie impulzov (výskytov). Prostredníctvom tohto nastavenia môžete určiť, pri dosiahnutí akej minimálnej frekvencie impulzov (výskytov) bude úloha spustená. Napríklad môžete nastaviť, aby bola úloha spustená vždy vtedy, keď sa v priebehu jednej hodiny vyskytne 10 impulzov na aktivovanie spúšťača. Aktivácia spúšťača vynuluje zaznamenané informácie a počítanie výskytov sa začne odznova (od nuly).

Časové obdobie – vyberte frekvenciu pre možnosť uvedenú vyššie.

Tretiu štatistickú podmienku je možné nastaviť len pre niektoré typy spúšťačov. Prejdite do sekcie: **Spúšťač** > **Typ spúšťača** > **Spúšťač protokolu udalosti**.

Kritériá protokolu udalostí

Tieto kritériá sú vyhodnocované nástrojom ESMC ako tretie štatistické kritériá (S3). Logický operátor (AND/OR) zvolený v sekcii **Aplikácia pre štatistické kritériá** je použitý pri vyhodnocovaní všetkých troch štatistických podmienok spoločne. Kritériá protokolu udalostí odporúčame používať v prípade úlohy pre server **Generovať správu**. Aby fungovali kritériá protokolu udalostí, je nutné vyplniť všetky tri polia v príslušnej sekcii. Medzipamäť symbolov sa vynuluje, ak je spúšťač aktivovaný a symbol je už v pamäti.

Podmienka – toto určuje, ktoré udalosti alebo množiny udalostí spustia podmienku. Sú dostupné tieto možnosti:

- **Prijatých v rade dosiahne limit** – udalosti musia nastať po sebe v stanovenom počte. Musí zároveň ísť o rozdielne udalosti.
- **Prijatých od posledného výskytu** – podmienka sa spustí po dosiahnutí stanoveného počtu jedinečných udalostí, ktoré nastali od posledného spustenia úlohy.

Počet výskytov – pre spustenie úlohy zadajte počet jedinečných udalostí s vybranými symbolmi.

Symbol – z ponuky môžete vybrať symbol, ktorý sa bude vyhľadávať vo zvolenom type protokolu. Položky dostupné v tejto ponuke závisia od Typu protokolu, ktorý ste vybrali v sekcii **Spúšťač**. Ponuka sa zobrazí po kliknutí na tlačidlo **Vybrať**. Zvolený symbol môžete odstrániť kliknutím na tlačidlo **Zmazať**.

Poznámka:
Keď sú tieto kritériá použité pre serverovú úlohu (Úloha pre server), posudzované sú všetky klientske počítače. Zaznamenanie väčšieho počtu po sebe nasledujúcich (nerovnakých) udalostí je teda málo pravdepodobné. Nastavenie **Aplikuje sa, keď počet udalostí – Prijatých v rade dosiahne limit** preto používajte len v opodstatnených prípadoch. Chýbajúca hodnota (N/A) nie je posudzovaná ako unikátna hodnota symbolu, a preto je medzipamäť vynulovaná od posledného spustenia.

Dodatočné nastavenia

Ako už bolo spomínané, spúšťač sa nemusí aktivovať pri každom výskyte udalosti. Pre takéto udalosti (ktoré neaktivujú spúšťač) je možné vykonať nasledujúce akcie:

- Ak je vynechaná viac ako jedna udalosť, posledných **N** udalostí zoskupiť do jednej (uložiť dáta potlačených impulzov) [**N** <= 100]
- Pre **N** == 0 je spracovaná len posledná udalosť (**N** predstavuje dĺžku histórie, pričom je vždy spracovaná posledná udalosť)
- Zlúčiť všetky udalosti, ktoré neaktivovali spúšťač (zlúčenie posledného impulzu s **N** predchádzajúcimi impulzmi)

V prípade, že sa spúšťač aktivuje príliš často, môžete použiť nasledujúce postupy:

- Ak chcete, aby sa spúšťač aktivoval len v prípade, že sa vyskytnú viaceré udalosti (nie iba jedna), použite štatistickú podmienku S1.
- Ak chcete aktivovať spúšťač len v prípade, že sa vyskytne klaster udalostí, použite štatistickú podmienku S2.
- Ak chcete ignorovať udalosti s nechcenými hodnotami, použite štatistickú podmienku S3.
- Ak chcete ignorovať udalosti, ktoré sa vyskytujú v čase, ktorý pre vás nie je relevantný (napr. mimo pracovných hodín), použite časovú podmienku T1.
- Ak chcete nastaviť minimálny časový interval medzi dvoma aktiváciami spúšťača, použite časovú podmienku T2.

Poznámka:
Podmienky je možné kombinovať pre vytvorenie komplexnejších scenárov obmedzovania aktivácie spúšťača. Podrobnejšie informácie nájdete v časti Príklady obmedzovania.

4.14.2.1 Príklady obmedzovania

Nasledujúce príklady znázorňujú, ako sú podmienky pre potlačenie aktivácie spúšťača (T1, T2, S1, S2, S3) kombinované a vyhodnocované.

Poznámka:
„Impulz“ na aktiváciu spúšťača (zvaný aj „tik“) predstavuje výskyt určitej udalosti, ktorá môže vyvolať aktivovanie spúšťača. „T“ označuje časové podmienky a „S“ štatistické podmienky. „S3“ predstavuje kritériá protokolu udalostí.

S1: Kritérium pre počet výskytov (povoliť každý tretí impulz)

Čas	00	01	02	03	04	05	06	Spúšťač je zmenený	07	08	09	10	11	12	13	14	15
Impulzy	x	x	x	x	x	x	x		x	x		x	x		x		x
S1			1			1						1					1

S2: Kritérium pre počet výskytov počas stanoveného časového intervalu (povoliť, ak sa vyskytnú 3 impulzy v priebehu 4 sekúnd)

Čas	00	01	02	03	04	05	06	Spúšťač je zmenený	07	08	09	10	11	12	13
Impulzy	x		x	x	x	x			x		x		x	x	x
S2				1										1	

S3: Kritérium pre unikátne hodnoty symbolov (povoliť, ak sa vyskytnú po sebe tri rozdielne hodnoty)

Čas	00	01	02	03	04	05	06	Spúšťač je zmenený	07	08	09	10	11	12	13
Hodnota	A	B	B	C	D	G	H		J	K	n/a	L	M	N	N
S3					1									1	

S3: Kritérium pre unikátne hodnoty symbolov (povoliť, ak sa od posledného impulzu vyskytnú tri rozdielne hodnoty)

Čas	00	01	02	03	04	05	06	07	Spúšťač je zmenený	08	09	10	11	12	13	14
Hodnota	A	B	B	C	D	G	H	I		J	K	n/a	L	M	N	N
S3				1			1						1			

T1: Povoliť impulzy na aktiváciu spúšťača počas stanoveného časového obdobia (každý deň od 8:10 počas 60 sekúnd)

Čas	8:09:50	8:09:59	8:10:00	8:10:01	Spúšťač je zmenený	8:10:59	8:11:00	8:11:01
Impulzy	x	x	x	x		x	x	x
T1			1	1		1		

Toto kritérium nemá žiadny stav, preto zmeny spúšťača nemajú vplyv na výsledok.

T2: Povoliť jeden impulz počas stanoveného časového obdobia (povoliť maximálne raz počas každých 5 sekúnd)

Čas	00	01	02	03	04	05	06	Spúšťač je zmenený	07	08	09	10	11	12	13
Impulzy	x		x	x	x	x			x		x		x	x	x
T2	1					1			1					1	

Kombinácia S1 + S2

- S1: každý piaty impulz
- S2: 3 impulzy počas 4 sekúnd

Čas	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Impulzy	x	x	x	x	x		x	x	x			x		x	x		
S1															1		
S2			1				1								1		
Výsledok			1				1								1		

Výsledok je vyhodnotený ako: S1 (logický operátor OR) S2

Kombinácia S1 + T1

- S1: povoliť každý tretí impulz
- T1: povoliť každý deň od 8:08 počas 60 sekúnd

Čas:	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Impulzy	x	x	x	x	x	x	x	x	x	x
S1			1			1			1	
T1					1	1	1	1	1	
Výsledok						1			1	

Výsledok je vyhodnotený ako: S1 (logický operátor AND) T1

Kombinácia S2 + T1

- S2: 3 impulzy počas 10 sekúnd
- T1: povoliť každý deň od 8:08 počas 60 sekúnd

Čas:	8:07:50	8:07:51	8:07:52	8:07:53	8:08:10	8:08:11	8:08:19	8:08:54	8:08:55	8:09:01
Impulzy	x	x	x	x	x	x	x	x	x	x
S2			1	1			1			1
T1					1	1	1	1	1	
Výsledok							1			

Výsledok je vyhodnotený ako: S2 (logický operátor AND) T1
Stav podmienky S2 je vynulovaný iba v prípade, že je celkový výsledok rovný 1.

Kombinácia S2 + T2

- S2: 3 impulzy počas 10 sekúnd
- T2: povoliť maximálne raz počas každých 20 sekúnd

Čas:	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
Impulzy	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x
S2			1			1	1	1				1	1	1	1	1		

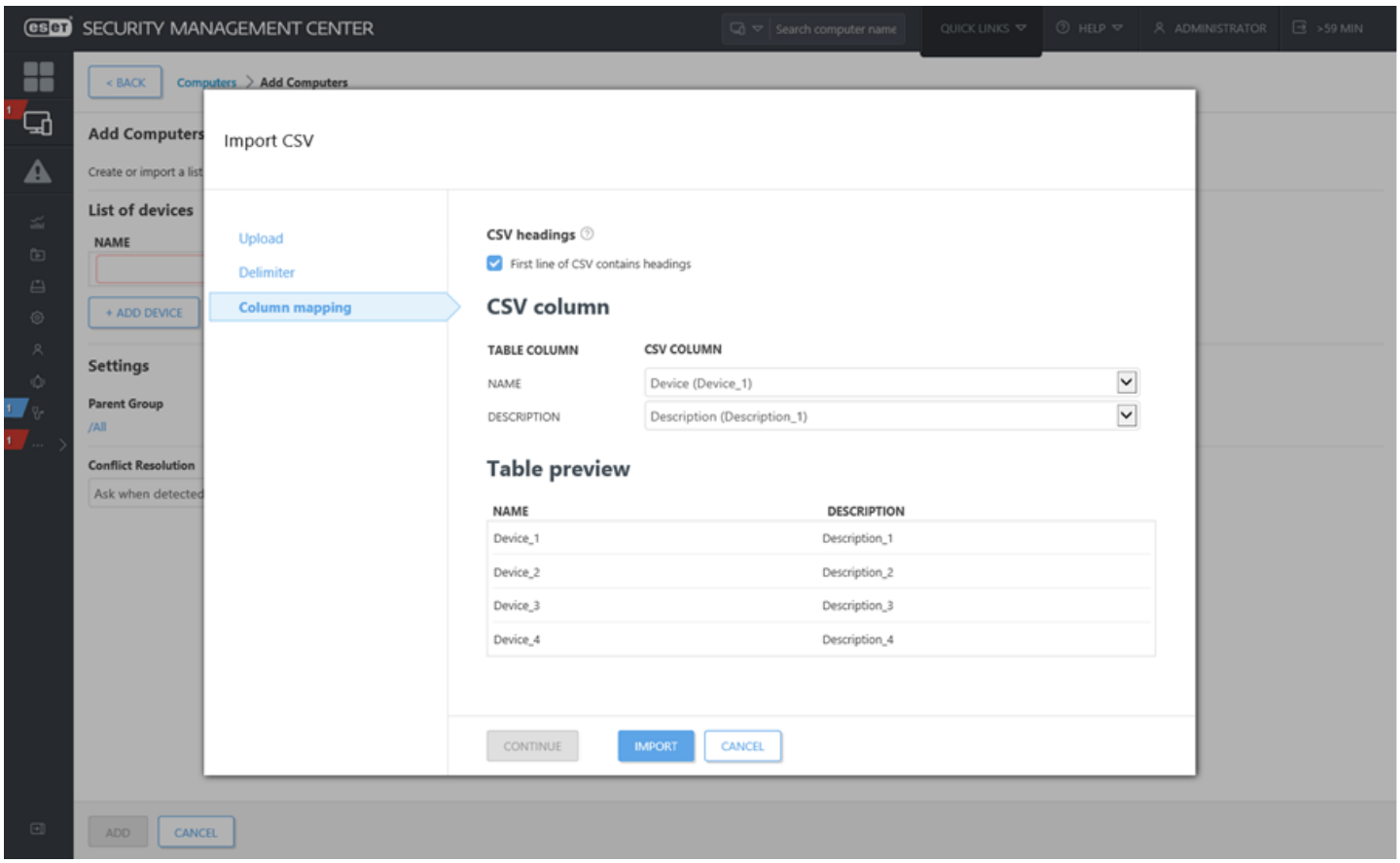
Čas:	00	01	02	03	04	05	06	07	...	16	17	18	19	20	21	22	23	24
T2	1	1	1													1		
Výsledok			1													1		

Výsledok je vyhodnotený ako: S2 (logický operátor AND) T2
Stav podmienky S2 je vynulovaný iba v prípade, že je celkový výsledok rovný 1.

4.15 Import CSV

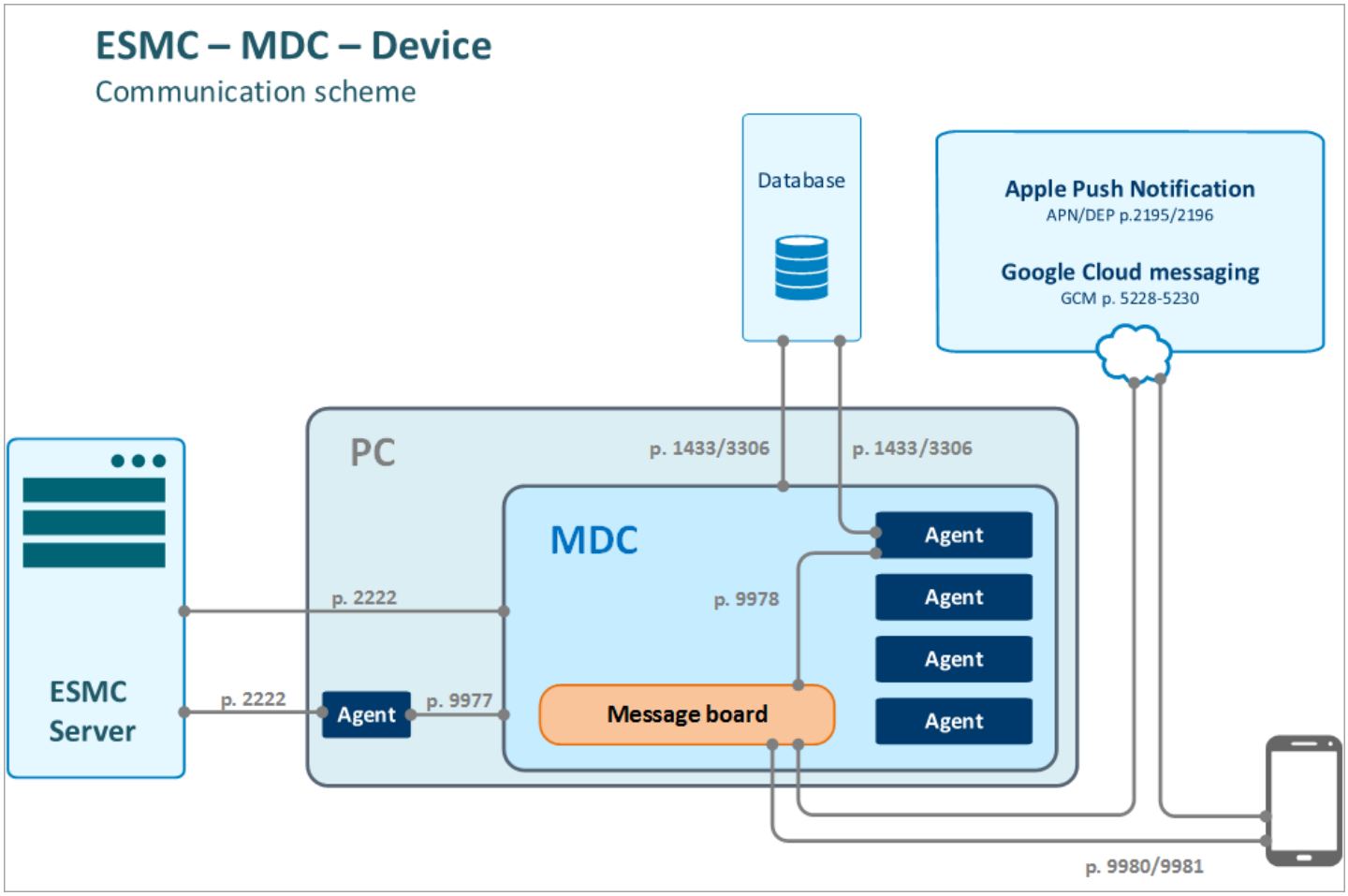
Importovať zoznam je možné pomocou vlastného `.csv` súboru, ktorý má správnu štruktúru. Táto funkcia je dostupná v rôznych častiach a ponukách v rámci používateľského rozhrania produktu ESET Security Management Center. Stĺpce sa menia v závislosti od toho, čo sa importuje.

1. Kliknite na možnosť **Import CSV**.
2. **Odovzdať** – kliknite na **Vybrať súbor**, vyhľadajte `.csv` súbor, ktorý chcete odovzdať, a následne kliknite na **Odovzdať**.
3. **Oddeľovač** – oddeľovač je znak, ktorý slúži na oddeľovanie textových reťazcov. Vyberte vhodný oddeľovač (**Bodkočiarka**, **Čiarka**, **Medzera**, **Tabulátor**, **Bodka** alebo **Zvislá čiara**), ktorý sa zhoduje s tým, čo používa váš `.csv` súbor. Ak váš `.csv` súbor používa ako oddeľovač iný znak, označte možnosť **Iné** a zadajte príslušný znak. **Ukážka dát** zobrazuje obsah vášho `.csv` súboru, čo vám môže pomôcť identifikovať, ktorý oddeľovač je používaný na oddelenie reťazcov.
4. **Mapovanie stĺpcov** – keď je už `.csv` súbor odovzdaný a spracovaný, môžete namapovať jednotlivé stĺpce v naimportovanom `.csv` súbore k príslušným ESMC stĺpcom. Na priradenie **CSV stĺpca** ku konkrétnemu ESMC stĺpcu použite roletové menu. Ak váš `.csv` súbor neobsahuje riadok hlavičky, zrušte označenie možnosti **Prvý riadok CSV obsahuje nadpisy**.
5. Pozrite si **Ukážku tabuľky** a uistite sa, že mapovanie stĺpcov je nastavené správne.
6. Ak ste úspešne namapovali všetky stĺpce a ukážka tabuľky je správna, kliknite na tlačidlo **Spustiť import**, čím spustíte operáciu.



5. Správa mobilných zariadení (MDM)

Nasledujúci diagram znázorňuje princíp komunikácie medzi komponentmi nástroja ESET Security Management Center a mobilným zariadením:



Poznámka:
Bezpečnostné odporúčanie pre MDM: MDM hostiteľské zariadenie vyžaduje pripojenie na internet. Odporúčame, aby bolo toto zariadenie chránené bránou firewall a zároveň aby boli pre MDM otvorené len potrebné porty. Môžete tiež nasadiť IDS/IPS pre monitorovanie siete.

Mobile Device Connector (MDC) je komponent ESMC, ktorý umožňuje správu mobilných zariadení pomocou nástroja ESET Security Management Center. Umožňuje vám spravovať mobilné zariadenia s operačným systémom Android alebo iOS a takisto ich bezpečnosť.

MDC poskytuje riešenie, kde agenty nebežia priamo na mobilných zariadeniach, vďaka čomu dochádza k šetreniu batérie a výkonu mobilného zariadenia. MDC slúži ako hostiteľ pre tieto virtuálne agenty. Dáta mobilných zariadení ukladá do svojej vlastnej SQL databázy.

Na overovanie komunikácie medzi mobilným zariadením a komponentom MDC je potrebný HTTPS certifikát. Na overovanie komunikácie medzi ESMC Serverom a komponentom MDC sa používa Proxy certifikát.

Správa zariadení Apple zahŕňa niektoré ďalšie požiadavky. Používanie komponentu ESMC MDC na správu zariadení s operačným systémom iOS vyžaduje certifikát služby Apple Push Notification Service (APNS). Služba APN umožňuje komponentu ESET MDC bezpečne komunikovať s mobilnými zariadeniami Apple. Tento certifikát musí byť podpísaný priamo spoločnosťou Apple (pomocou portálu Apple Push Certificates Portal) a odoslaný do MDC pomocou politiky. Následne môžu byť zariadenia s operačným systémom iOS registrované do ESMC MDC.

V niektorých krajinách je dostupný program Apple Device Enrollment Program (DEP). Program DEP predstavuje nový efektívny spôsob registrácie firemných zariadení iOS. Prostredníctvom programu DEP môžete zariadenia registrovať

do MDC automaticky bez potreby priameho kontaktu so zariadením a taktiež pri minimálnej interakcii používateľa. Program DEP značne rozširuje možnosti správy mobilných zariadení iOS a umožňuje ich úplné prispôsobenie.

Po úspešnej inštalácii a nastavení komponentu Mobile Device Connector môžete mobilné zariadenia registrovať. Po úspešnej registrácii môžete mobilné zariadenie spravovať pomocou nástroja ESMC Web Console.

5.1 Nastavenie MDM

Ak chcete využívať komponent slúžiaci na správu mobilných zariadení v nástroji ESET Security Management Center, postupujte podľa nasledujúcich krokov po vykonaní inštalácie MDM pre umožnenie registrácie a správy mobilných zariadení.

1. Nainštalujte **Mobile Device Connector** (MDC) pomocou all-in-one inštalátora alebo vykonajte inštaláciu jednotlivých komponentov na systéme Windows alebo Linux. Pred inštaláciou sa uistite, že sú splnené všetky prerekvizity.

Poznámka:
Ak inštalujete MDC pomocou all-in-one inštalátora, HTTPS certifikáty podpísané certifikačnou autoritou ESMC sú vytvorené automaticky počas samotnej inštalácie (tento certifikát nie je zobrazený v časti **Viac** > **Partnerské certifikáty**).

Ak chcete nainštalovať ESMC pomocou all-in-one inštalátora a použiť HTTPS certifikát tretej strany, nainštalujte najprv ESET Security Management Center a potom zmeňte svoj HTTPS certifikát pomocou politiky (vytvorte novú politiku pre **ESET Mobile Device Connector**, prejdite do sekcie **Všeobecné** a kliknite na **Zmeniť certifikát** > **Vlastný certifikát**).

Ak inštalujete komponent MDC samostatne, môžete použiť:

a) certifikát podpísaný certifikačnou autoritou ESMC (**Základné** > **Produkt**: Mobile Device Connector; **Hostiteľ**: Názov hostiteľa/IP adresa MDC; **Podpísať** > **Metóda podpisovania**: Certifikačná autorita; **Certifikačná autorita**: Certifikačná autorita ESMC).
b) HTTPS certifikačný reťazec tretej strany podpísaný dôveryhodnou certifikačnou autoritou spoločnosti Apple (zoznam dôveryhodných certifikačných autorít spoločnosti Apple).

2. Aktivujte ESMC MDC pomocou úlohy pre klienta Aktivácia produktu. Postup je rovnaký ako pri aktivácii bezpečnostných produktov spoločnosti ESET na klientskom počítači (nebude použitá licenčná jednotka).
3. Odporúčame spustiť úlohu pre server Synchronizácia používateľa. Táto úloha vám umožní automaticky synchronizovať používateľov s Active Directory alebo LDAP na účely sekcie Používatelia počítača.

Poznámka:
Ak plánujete spravovať iba zariadenia so systémom **Android** (t. .j nebudú spravované žiadne iOS zariadenia), prejdite na krok č. 7.

4. Vytvorte APN/DEP certifikát. Tento certifikát používa ESMC MDM na registráciu iOS zariadení. Certifikáty, ktoré budú pridané do vášho registračného profilu, musia byť pridané aj do DEP profilu.
5. Na aktiváciu APNS vytvorte novú politiku pre ESET Mobile Device Connector.

Poznámka:
Ak registrujete iOS zariadenia prostredníctvom programu Apple Device Enrollment Program (DEP), prejdite na túto kapitolu.

6. Zaregistrujte mobilné zariadenia pomocou úlohy Registrácia zariadenia. Úlohu nakonfigurujte podľa toho, či chcete registrovať zariadenie s operačným systémom Android alebo iOS. Toto sa dá vykonať aj v sekcii **Počítače** alebo **Skupiny** kliknutím na **Pridať nový** > **Mobilné zariadenia** za predpokladu, že ste vybrali **Statickú skupinu** (možnosť **Pridať nový** nemôže byť použitá pri dynamických skupinách).

7. Ak ste počas registrácie zariadení neposkytli licenciu, aktivujte mobilné zariadenia pomocou klientskej úlohy Aktivácia Produktu – zvoľte licenciu ESET Endpoint Security. Pre každé mobilné zariadenie bude použitá licenčná jednotka.

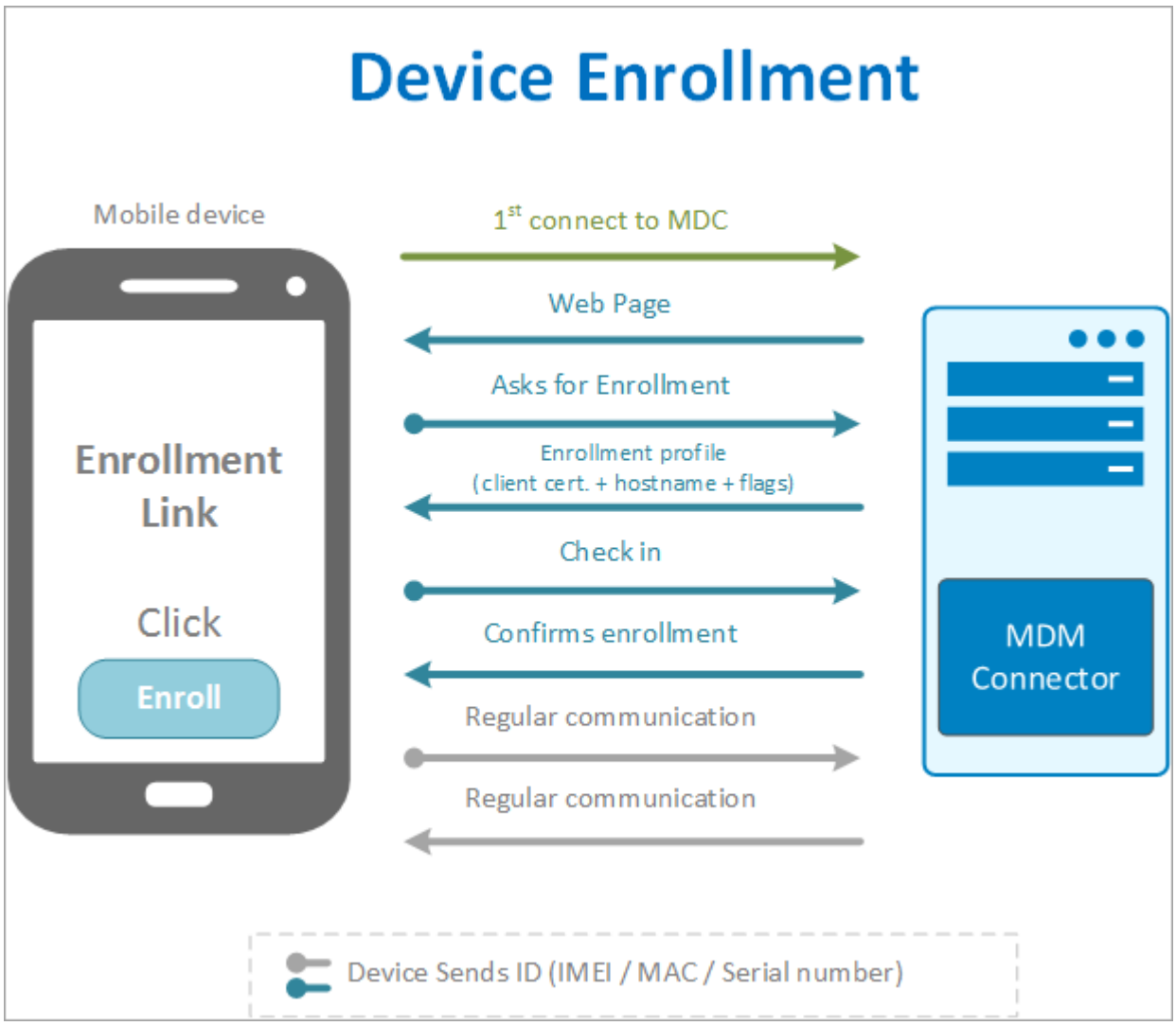
Dôležité:
Úloha **Aktivácia produktu** nemôže byť spustená na mobilných zariadeniach (**ESET Endpoint pre Android** a **MDM pre iOS**), ak sa používa offline licencia.

8. Môžete upraviť používateľov pre nastavenie vlastných atribútov a priradenie mobilných zariadení, ak ste nepriradili používateľov počas registrácie zariadení.
9. Teraz môžete začať aplikovať politiky a spravovať mobilné zariadenia. Napríklad môžete vytvoriť politiku pre iOS MDM – Exchange ActiveSync účet, ktorá na iOS zariadeniach automaticky nastaví poštový účet, kontakty a kalendár. Môžete tiež aplikovať obmedzenia na iOS zariadenie a/alebo pridať Wi-Fi pripojenie.
10. Ďalej môžete použiť možnosť **Znovu registrovať** na mobilnom zariadení, ktoré je poškodené alebo z neho boli vymazané všetky údaje. Odkaz na opätovnú registráciu bude odoslaný prostredníctvom e-mailu.
11. Úloha Ukončiť spravovanie (Odinštalovať ESET Management Agenta) zruší MDM registráciu mobilného zariadenia a úplne ho odstráni z ESMC.

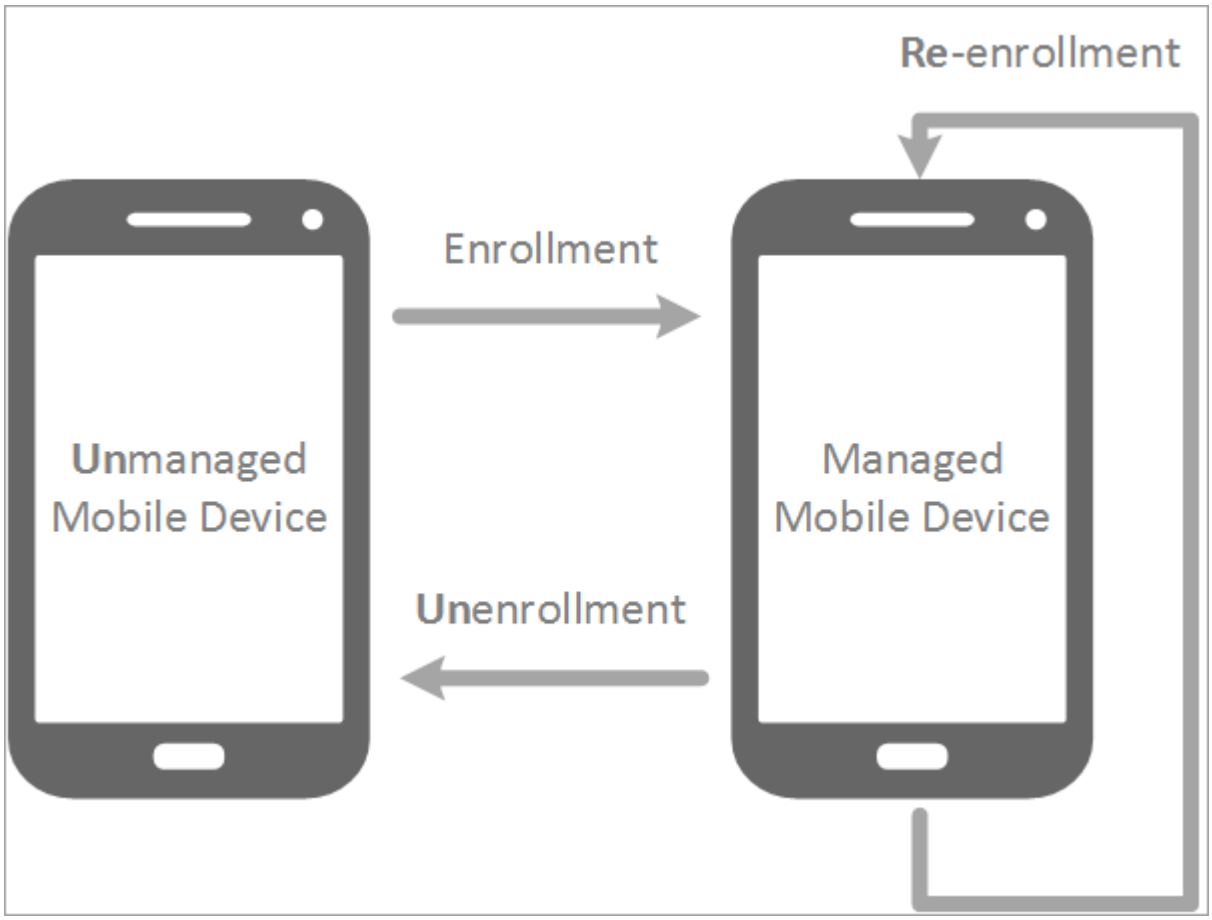
5.2 Registrácia zariadení

Mobilné zariadenia môžu byť spravované pomocou ESMC a bezpečnostného produktu spoločnosti ESET spusteného na mobilnom zariadení. Nato, aby ste mohli začať spravovať mobilné zariadenia, je potrebné ich zaregistrovať do ESMC (už nie je potrebné zadávať IMEI alebo iné identifikačné čísla mobilného zariadenia).

Nižšie uvedený diagram znázorňuje princíp komunikácie medzi mobilným zariadením a nástrojom Mobile Device Connector počas procesu registrácie zariadenia:



Nasledujúci diagram znázorňuje možnosti použitia registrácie, opätovnej registrácie a zrušenia registrácie, ako aj rozdiel medzi spravovanými a nespravovanými zariadeniami.



- **Registrácia**: Registráciu je možné vykonať len v prípade, že zariadenie ešte nie je spravované cez MDM. To znamená, že dané zariadenie nie je zahrnuté v sekcii **Počítače**. Pokiaľ zariadenie vymažete z tejto sekcie vo Web Console, zariadenie bude aj naďalej spravované a po úspešnej replikácii sa znova zobrazí vo Web Console. Spravovanie zariadenia je možné zrušiť iba prostredníctvom zrušenia registrácie. Každý registračný token je jedinečný a je možné ho použiť len raz. Ak ste token už raz použili, druhýkrát sa použiť nedá.
- **Opätovná registrácia**: Opätovnú registráciu je možné vykonať len v prípade, že je zariadenie spravované. Token pre opätovnú registráciu sa vždy líši od registračného tokenu a je možné ho použiť len raz.
  Pre opätovné zaregistrovanie zariadenia prejdite do sekcie **Počítače** a vyberte mobilné zariadenie, ktoré chcete opätovne zaregistrovať. Kliknite na **Akcie** a z ponuky vyberte položku **Mobil > Znovu registrovať**.
- **Zrušenie registrácie**: Zrušenie registrácie slúži na zastavenie spravovania určitého zariadenia. Zrušenie registrácie sa vykonáva prostredníctvom úlohy pre klienta Ukončiť spravovanie. Pokiaľ zariadenie neodpovedá, odstránenie zariadenia môže trvať aj 3 dni. Ak chcete zariadenie odstrániť zo zoznamu spravovaných zariadení len kvôli tomu, aby ste mohli zariadenie znova zaregistrovať, použite opätovnú registráciu.

Poznámka:
Ak registrujete iOS zariadenia prostredníctvom programu Apple Device Enrollment Program (DEP), prejdite na túto kapitolu.

Registrovať nové mobilné zariadenia môžete v časti **Počítače** alebo v časti **Viac** > **Skupiny**. Vyberte **Statickú skupinu**, do ktorej chcete pridať mobilné zariadenia a kliknite na **Pridať nový** > **Mobilné zariadenia** a vyberte jednu z nasledujúcich metód registrácie:

- Registrácia prostredníctvom e-mailu – hromadná registrácia mobilných zariadení prostredníctvom e-mailu. Táto možnosť je najvhodnejšia v prípade, že potrebujete zaregistrovať väčšie množstvo mobilných zariadení alebo v prípade, že chcete zaregistrovať mobilné zariadenia, ku ktorým nemáte fyzicky prístup. Táto možnosť si zároveň vyžaduje interakciu používateľa/majiteľa mobilného zariadenia.
- Individuálna registrácia prostredníctvom odkazu alebo QR kódu – registrácia jedného mobilného zariadenia. Naraz budete môcť zaregistrovať len jedno zariadenie, čo znamená, že tento postup bude potrebné zopakovať pre každé zariadenie zvlášť. Odporúčame vám použiť túto možnosť len v prípade, že potrebujete zaregistrovať menšie

množstvo mobilných zariadení. Táto možnosť je naopak vhodná v prípade, že si neželáte, aby používatelia/majitelia mobilného zariadenia museli čokoľvek robiť a chcete celú registráciu vykonať sami. Túto možnosť môžete použiť aj v prípade, že máte nové mobilné zariadenia, ktoré budú po nakonfigurovaní všetkých potrebných nastavení odovzdané používateľom.

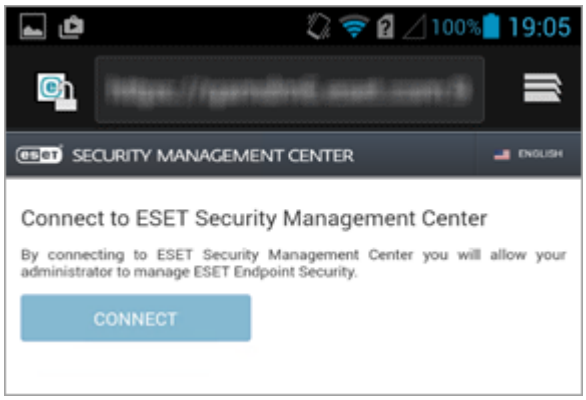
- Individuálna registrácia ako vlastník zariadenia (iba Android 7 a vyššie) – registrácia jedného mobilného zariadenia so systémom Android. Naraz budete môcť zaregistrovať len jedno zariadenie, čo znamená, že tento postup bude potrebné zopakovať pre každé mobilné zariadenie zvlášť. Túto registráciu je možné vykonať iba na zariadeniach, ktoré sú nové alebo vymazané, prípadne boli na nich obnovené výrobné nastavenia. Vykonaním daného procesu registrácie získa správca v porovnaní s používateľom zariadenia vyššie práva, čo mu umožní lepšiu kontrolu nad zariadením.

5.2.1 Registrácia zariadení Android

V tejto kapitole sú popísané dva scenáre registrácie zariadení Android, pričom odlišujúcim faktorom je, či aplikácia ESET Endpoint Security pre Android (EESA) už na mobilnom zariadení aktivovaná je alebo ešte nie. Ak aplikácia EESA na mobilnom zariadení ešte nie je aktivovaná, je možné použiť úlohu pre klienta Aktivácia produktu (odporúča sa). Druhý scenár sa týka mobilných zariadení s už aktivovanou aplikáciou ESET Endpoint Security pre Android.

Aplikácia EESA je už aktivovaná – pre registráciu mobilného zariadenia postupujte podľa nasledujúcich krokov:

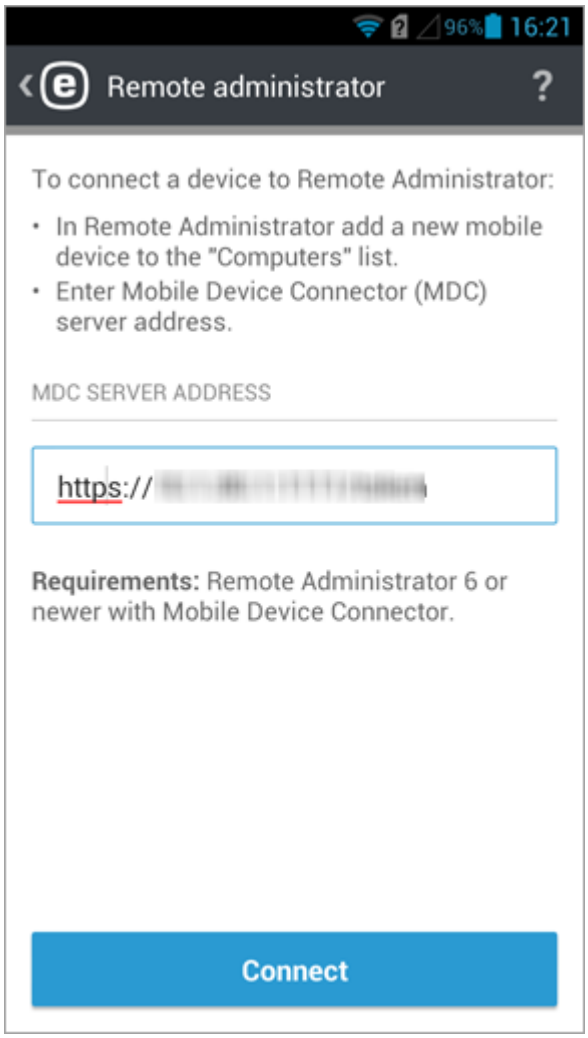
1. Na zariadení ťuknite na registračný URL odkaz (vrátane čísla portu), ktorý ste obdržali prostredníctvom e-mailu, alebo ho manuálne zadajte do prehliadača (napr. *https://eramdm:9980/<token>*). Pokiaľ budete vyzvaný na prijatie SSL certifikátu, prijatie odsúhlaste a následne ťuknite na **Pripojiť**.



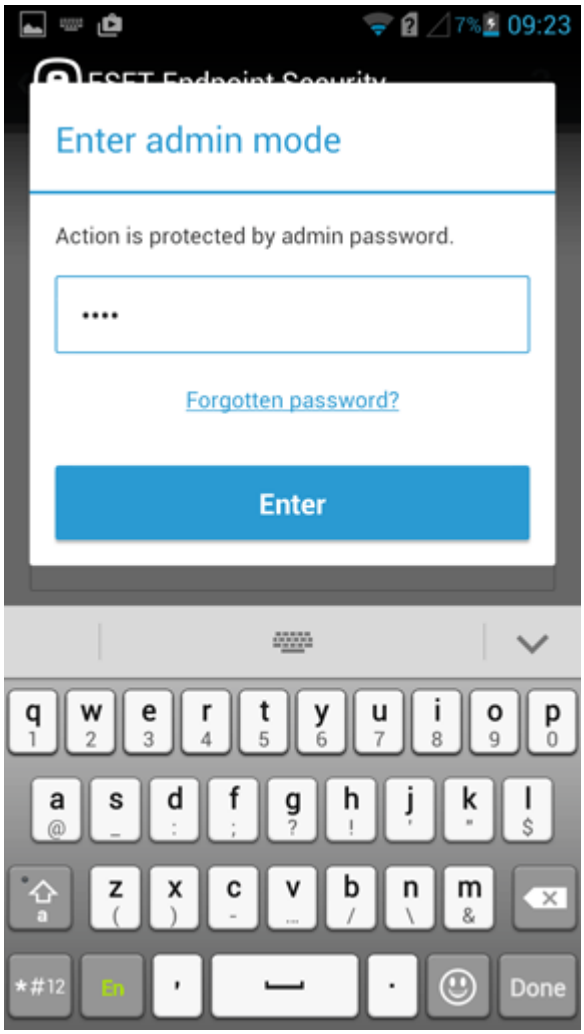
Dôležité:
Ak nie je na mobilnom zariadení nainštalovaný produkt ESET Endpoint Security, budete automaticky presmerovaný do obchodu Google Play, odkiaľ môžete stiahnuť aplikáciu.

POZNÁMKA:
Ak sa zobrazí oznámenie **Nepodarilo sa nájsť aplikáciu na otvorenie tohto odkazu**, skúste registračný odkaz otvoriť v predvolenom webovom prehliadači systému Android.

2. Skontrolujte podrobnosti pripojenia (adresu servera pre Mobile Device Connector a číslo portu) a zvoľte **Pripojiť**.



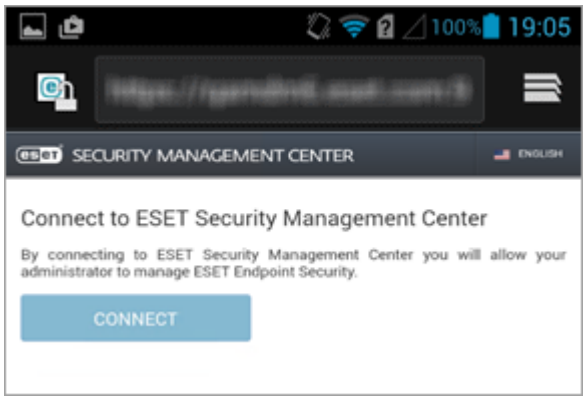
3. Do prázdneho poľa zadajte heslo pre vstup do administrátorského režimu aplikácie ESET Endpoint Security a ťuknite na **Vstúpiť**.



4. Mobilné zariadenie je teraz spravované prostredníctvom ESMC. Môžete ťuknúť na **Dokončiť**.

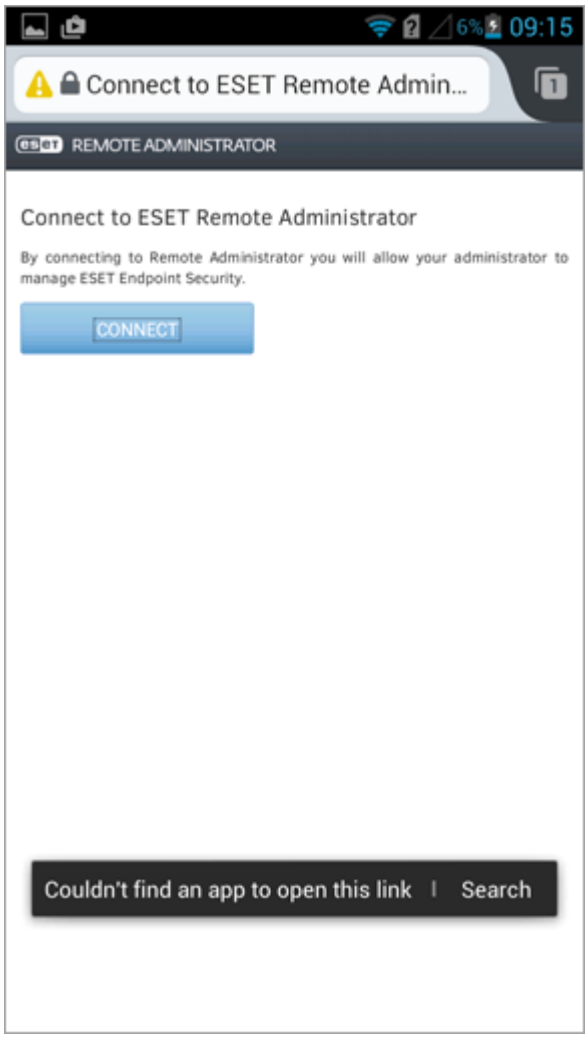
Aplikácia EESA nie je aktivovaná – pre aktiváciu produktu a registráciu mobilného zariadenia postupujte podľa nasledujúcich krokov:

1. Na zariadení ťuknite na registračný URL odkaz (vrátane čísla portu) alebo ho manuálne zadajte do prehliadača (napr. *https://esmcmdm:9980/<token>*). Môžete tiež použiť uvedený **QR kód**. Pokiaľ budete vyzvaný na prijatie SSL certifikátu, prijatie odsúhlaste a následne ťuknite na **Pripojiť**.

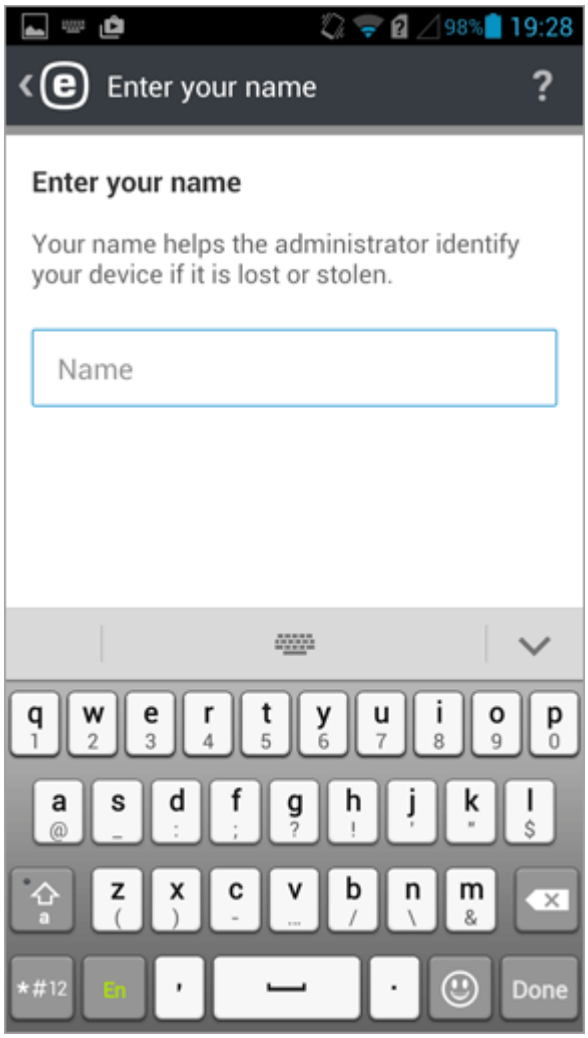


Dôležité:
Ak nie je na mobilnom zariadení nainštalovaný produkt ESET Endpoint Security, budete automaticky presmerovaný do obchodu Google Play, odkiaľ môžete stiahnuť aplikáciu.

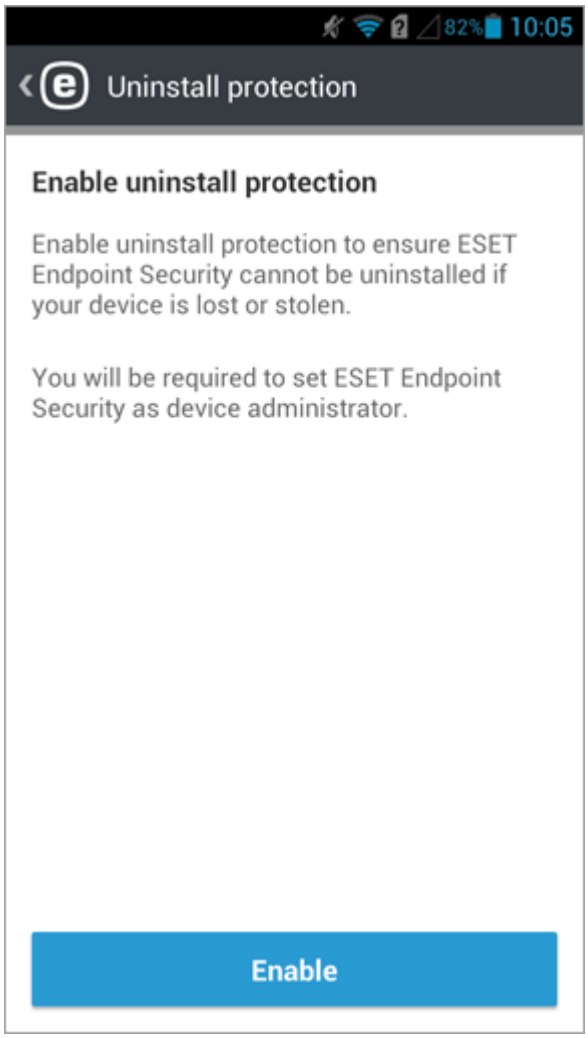
Poznámka:
Ak sa zobrazí oznámenie **Nepodarilo sa nájsť aplikáciu na otvorenie tohto odkazu**, skúste registračný odkaz otvoriť v predvolenom webovom prehliadači systému Android.



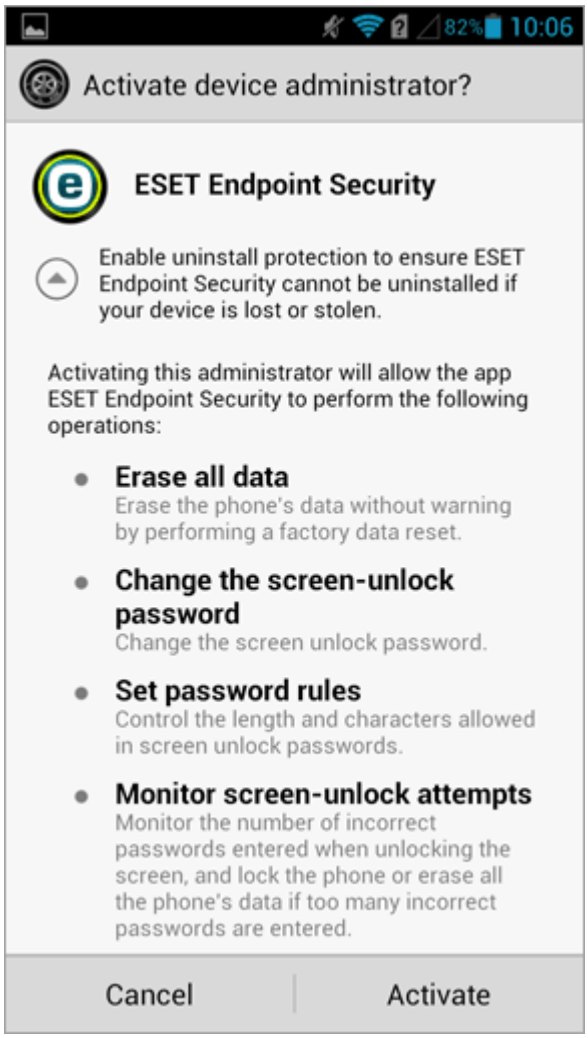
2. Zadajte názov mobilného zariadenia (tento názov nie je viditeľný v ESMC, je užitočný len pre nástroj Anti-Theft a na účely diagnostických protokolov).



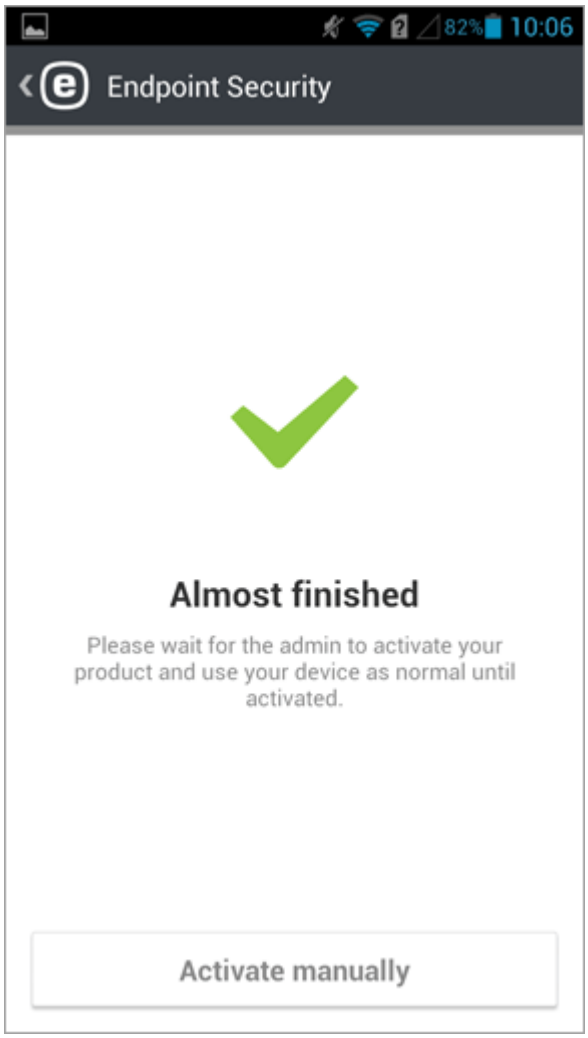
3. Ťuknite na **Zapnúť**, čím zapnete ochranu pred odinštalovaním aplikácie.



4. Ťuknite na **Aktivovať** pre aktivovanie aplikácie ako správcu daného zariadenia.

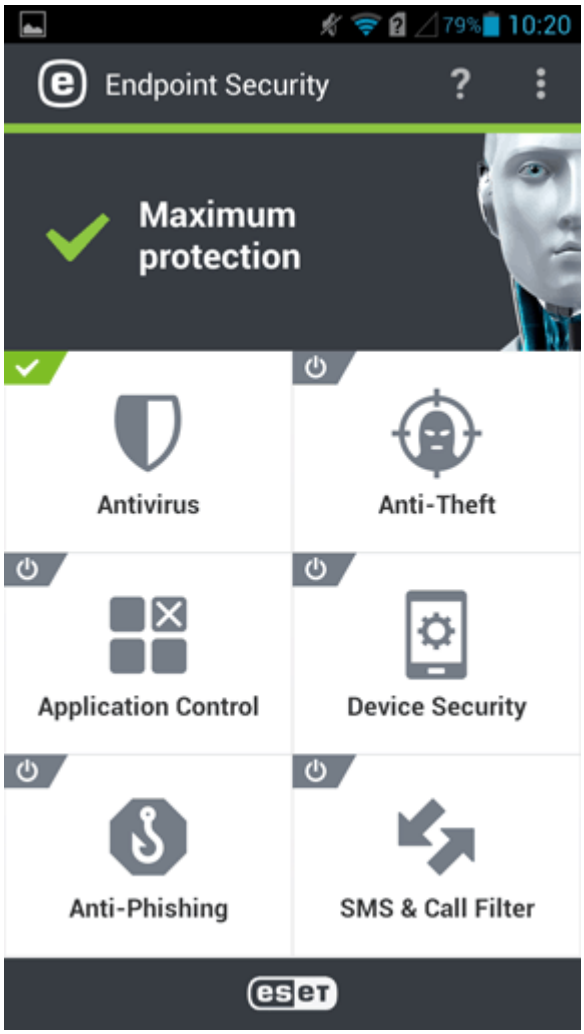


5. Teraz môžete zatvoriť aplikáciu EESA na mobilnom zariadení a otvoriť ESMC Web Console.



6. V ESMC Web Console prejdite do sekcie **Úlohy pre klienta** > **Mobil** > Aktivácia produktu a kliknite na **Nová**.

Spustenie tejto úlohy na mobilnom zariadení môže trvať dlhší čas. Po úspešnom spustení úlohy bude aplikácia EESA na mobilnom zariadení aktivovaná a mobilné zariadenie budete môcť spravovať pomocou nástroja ESMC. Od tejto chvíle bude môcť používateľ mobilného zariadenia používať aplikáciu EESA. Po otvorení aplikácie ESET Endpoint Security pre Android sa zobrazí hlavná ponuka:

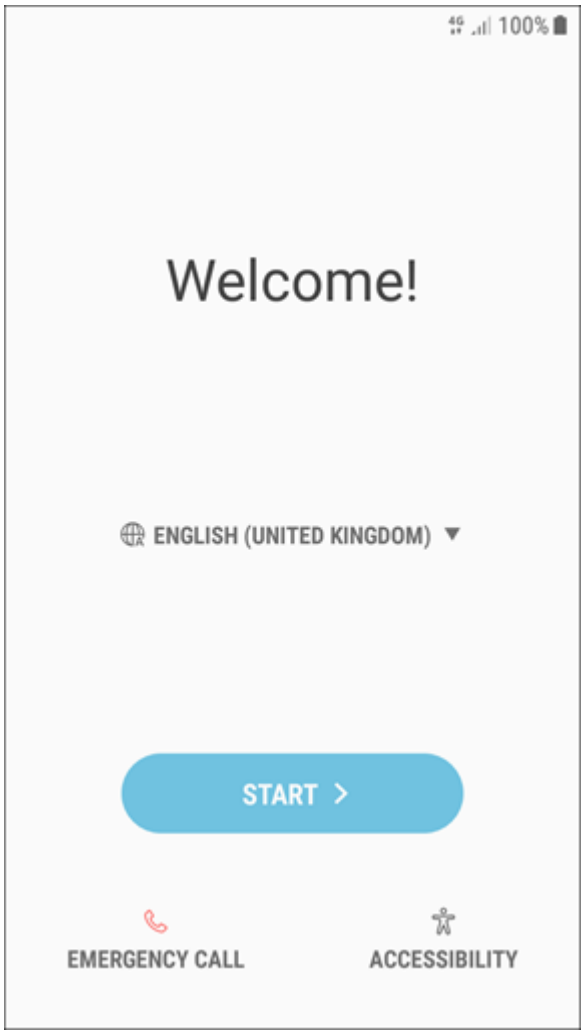


5.2.1.1 Registrácia zariadení Android v rámci režimu Vlastník zariadenia

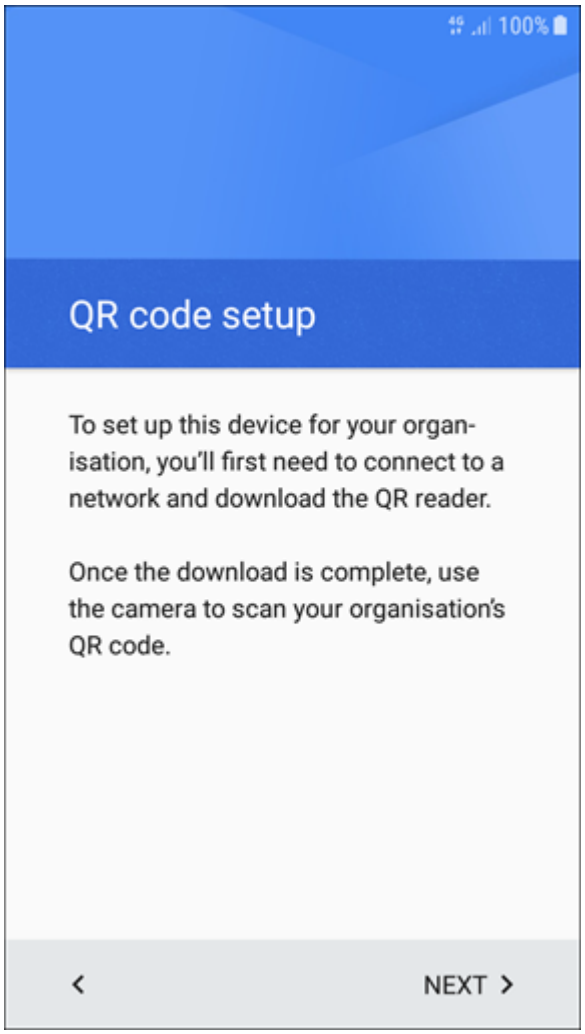
Poznámka:
Tento typ registrácie je dostupný len pre zariadenia Android s operačným systémom Android 7 a vyšším.

Nato, aby bolo možné vykonať nasledujúce kroky registrácie, musí byť zariadenie Android po vymazaní/obnove výrobných nastavení alebo v pôvodnom stave.

1. Zapnite mobilné zariadenie.
2. Zadajte PIN kód SIM karty.
3. Na úvodnej obrazovke si zvoľte preferovaný jazyk a potom ťuknite na obrazovku 6-krát v okolí textu „Welcome“ pre spustenie nastavenia QR kódu.

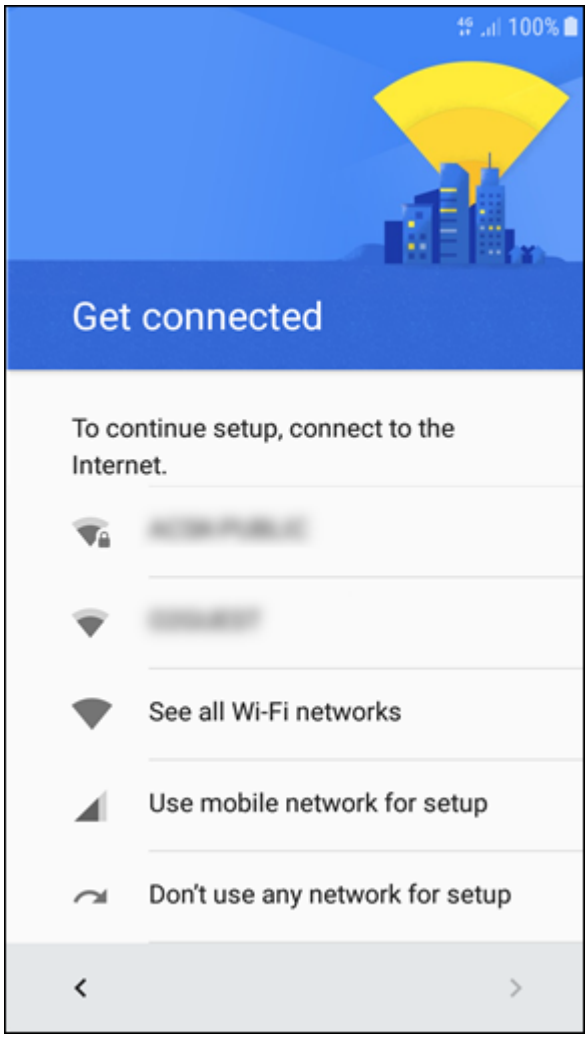


4. Ak ste predchádzajúci krok vykonali správne, zobrazí sa **nastavenie QR kódu**. Ťuknite na **NEXT** pre pokračovanie.

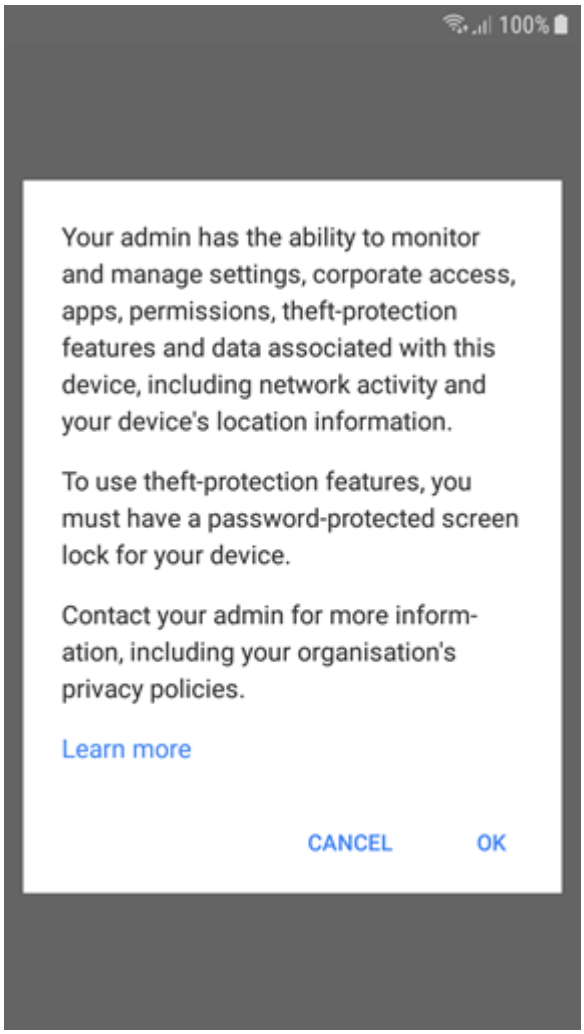


Poznámka:
Niektoré zariadenia od vás môžu vyžadovať, aby ste zašifrovali úložisko zariadenia (niekedy to môže byť potrebné aj pre pripojenie k nabíjačke). Vyberte preferovaný typ šifrovania a pokračujte podľa pokynov na obrazovke.

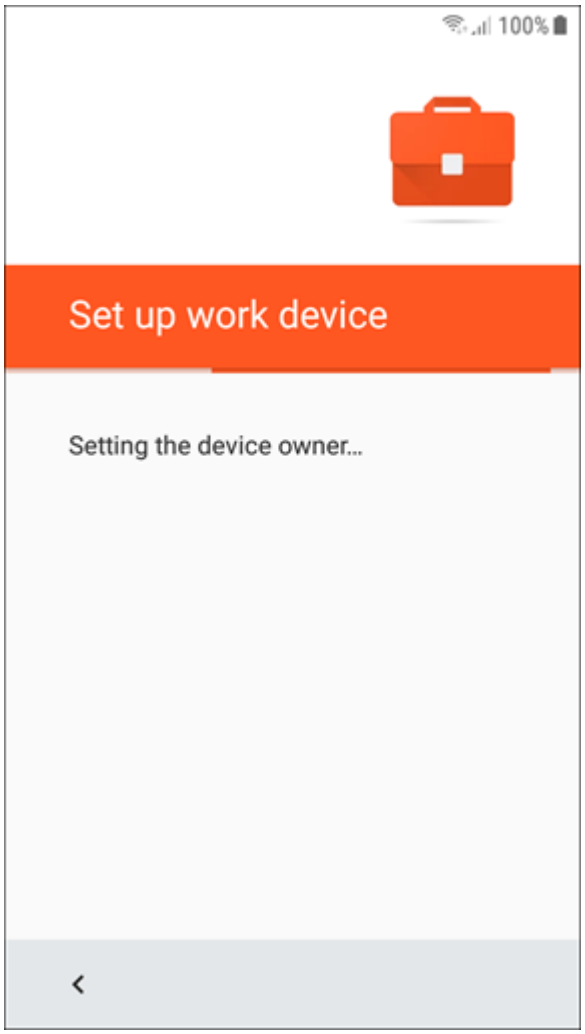
5. Vyberte internetové pripojenie. Toto pripojenie bude použité na stiahnutie čítačky QR kódov, ktorá bude potrebná v ďalšom kroku.



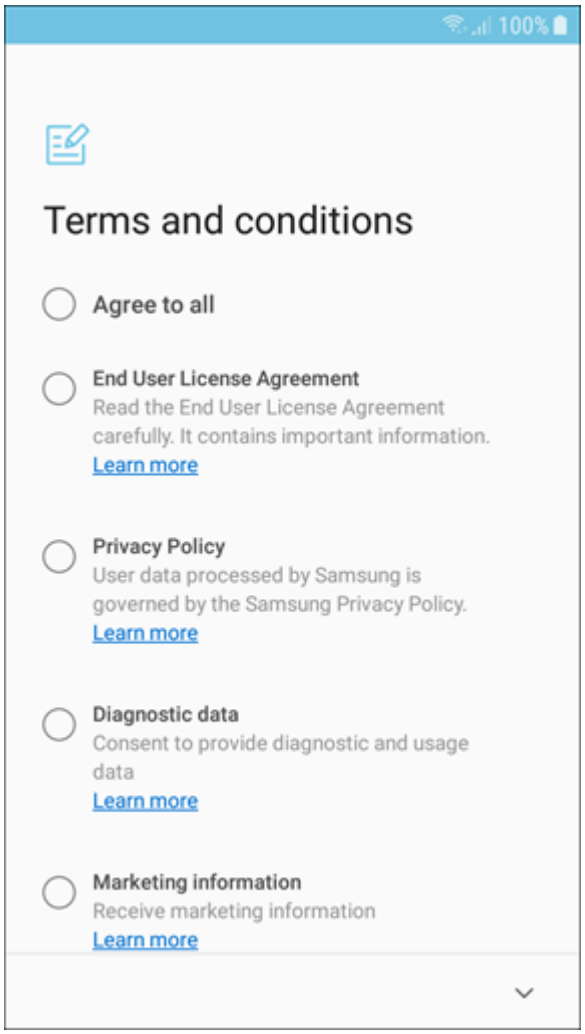
6. Teraz sa nainštaluje čítačka QR kódov. Po dokončení inštalácie naskenujte QR kód, ktorý bol vygenerovaný v nástroji ESMC Web Console.
7. Budete vyzvaný, aby ste potvrdili, že rozumiete, že udeľujete správcovi vyššie práva (Vlastník zariadenia). Pokračujte ťuknutím na **OK**.



8. Teraz sa nainštaluje aplikácia ESET Endpoint Security pre Android a zároveň sa aplikujú požadované povolenia.



9. Ťuknutím na **Agree to all** vyjadríte súhlas s Licenčnou dohodou s koncovým používateľom a Zásadami ochrany osobných údajov, ako aj so zasielaním diagnostických dát a prijímaním marketingových dát.

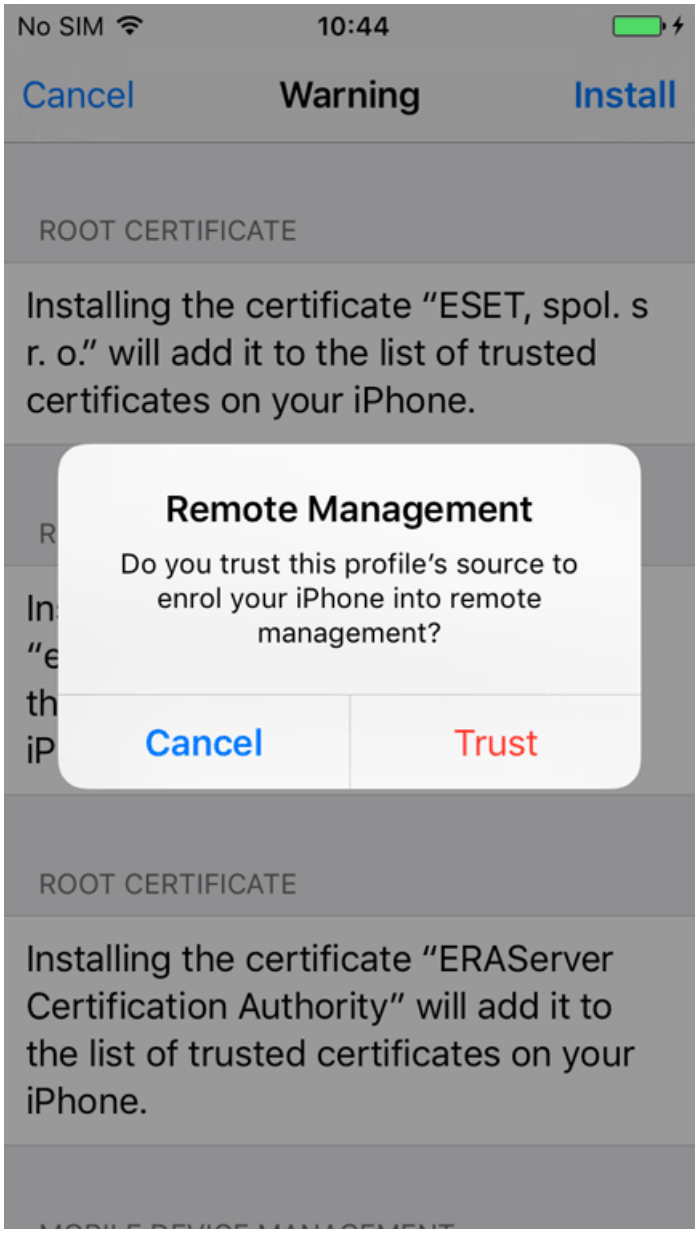


10. Zariadenie je odteraz registrované v režime Vlastník zariadenia.

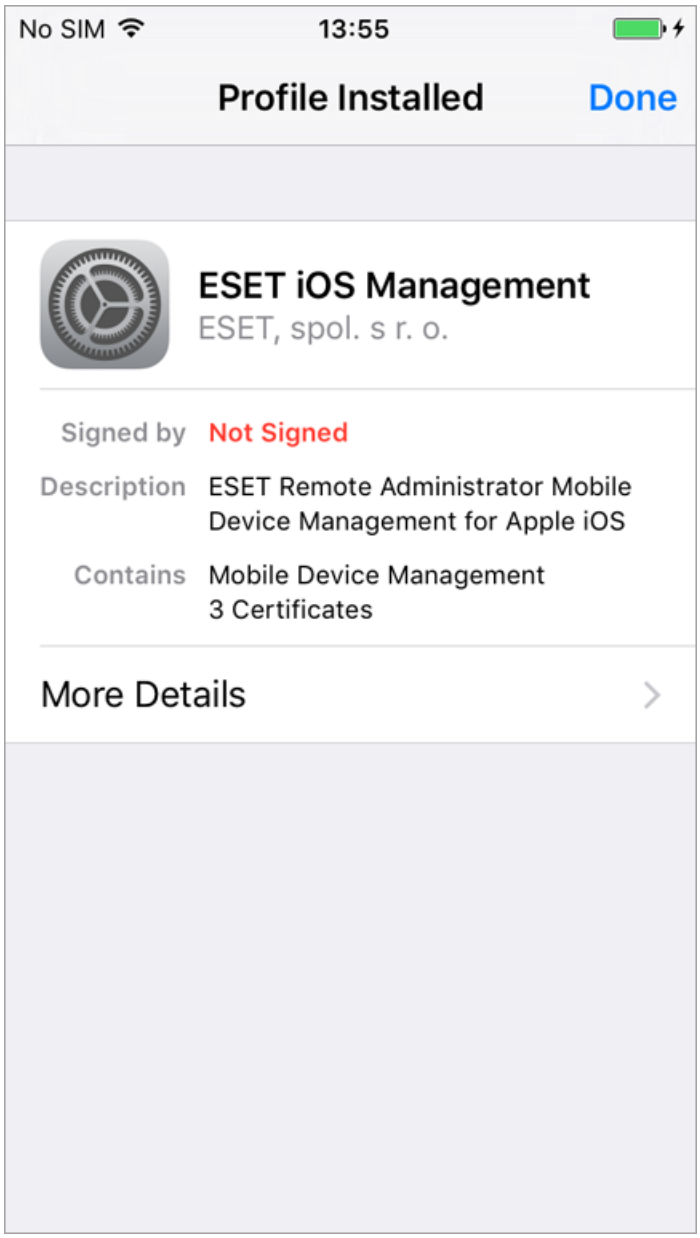
5.2.2 Registrácia zariadení iOS

Poznámka:
Ak registrujete iOS zariadenia prostredníctvom programu Apple Device Enrollment Program (DEP), prejdite na túto kapitolu.

1. Na zariadení ťuknite na registračný URL odkaz (vrátane čísla portu) alebo ho manuálne zadajte do prehliadača (napr. *https://eramdm:9980/<token>*). Môžete tiež použiť uvedený **QR kód**.
2. Pre pokračovanie ťuknite na **Inštalovať** na obrazovke **Inštalovať profil** v rámci MDM registrácie.

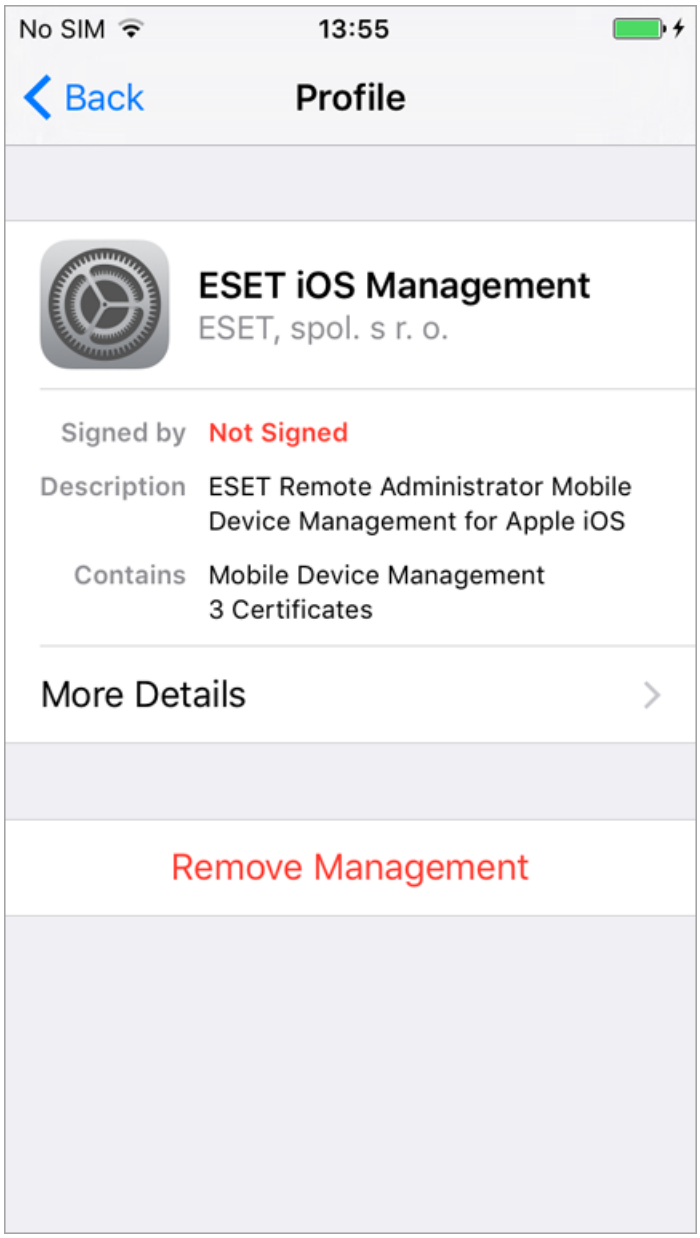


4. Po nainštalovaní nového profilu sa zobrazí informácia, že profil **nie je podpísaný**. Lenže iOS zariadenie tento certifikát nedokáže rozpoznať. Ak chcete mať registračný profil podpísaný, použite HTTPS certifikát vydaný autoritou, ktorej dôveruje spoločnosť Apple. Prípadne si tiež môžete certifikát podpísať.



5. Tento profil vám umožní nastaviť zariadenia, ako aj bezpečnostné politiky pre používateľov a skupiny.

Dôležité:
Odstránením tohto registračného profilu sa vymažú všetky firemné nastavenia (pošta, kalendár, kontakty atď.) a iOS mobilné zariadenie nebude spravované. Ak používateľ odstráni registračný profil, ESMC túto skutočnosť nezistí a stav zariadenia sa zmení na . Po 14 dňoch, počas ktorých sa zariadenie nebude pripájať k ESMC, sa stav zariadenia zmení na . Nebude poskytnutá žiadna ďalšia indícia, že registračný profil bol odstránený.

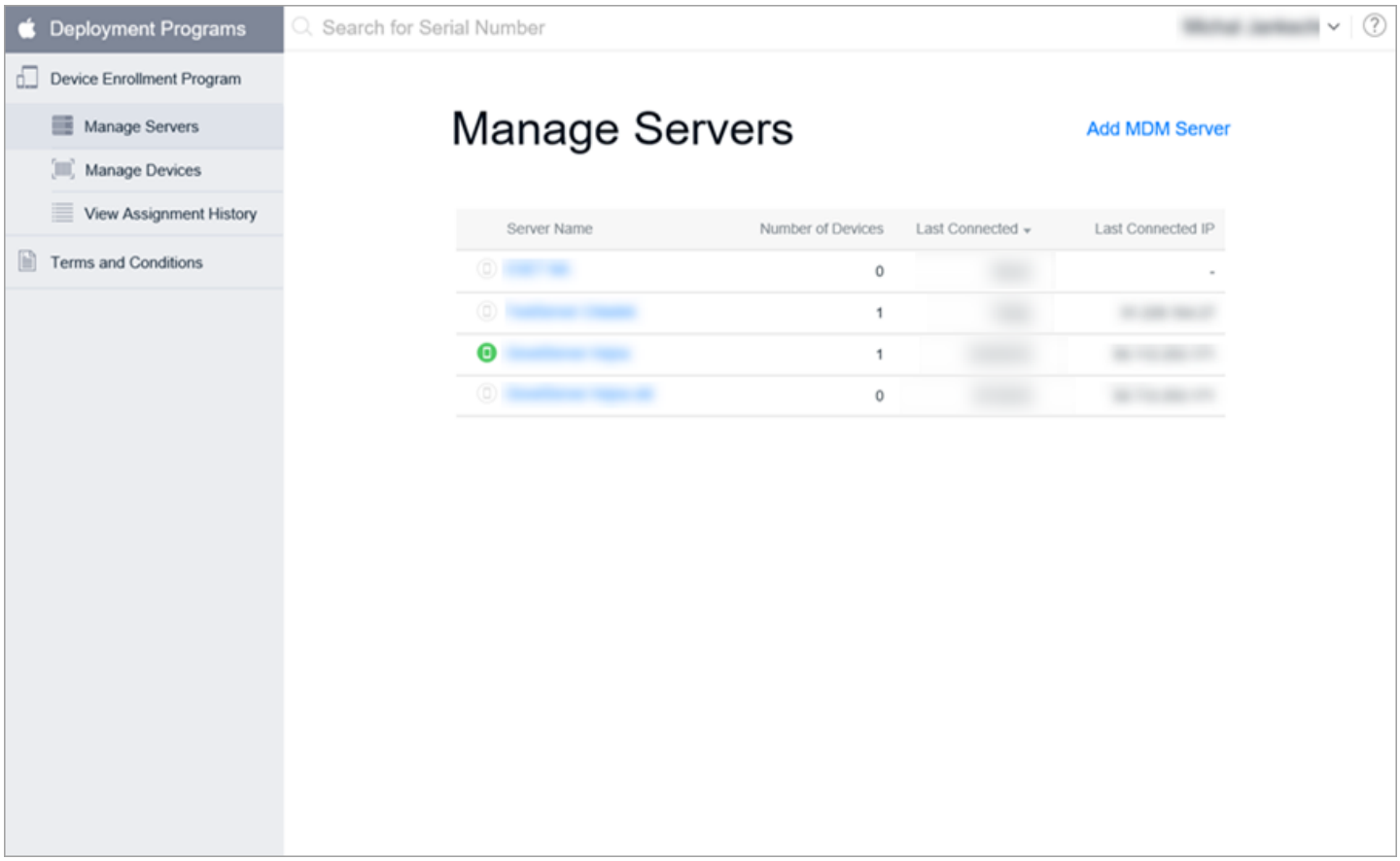


5.2.2.1 Registrácia zariadení iOS prostredníctvom programu DEP

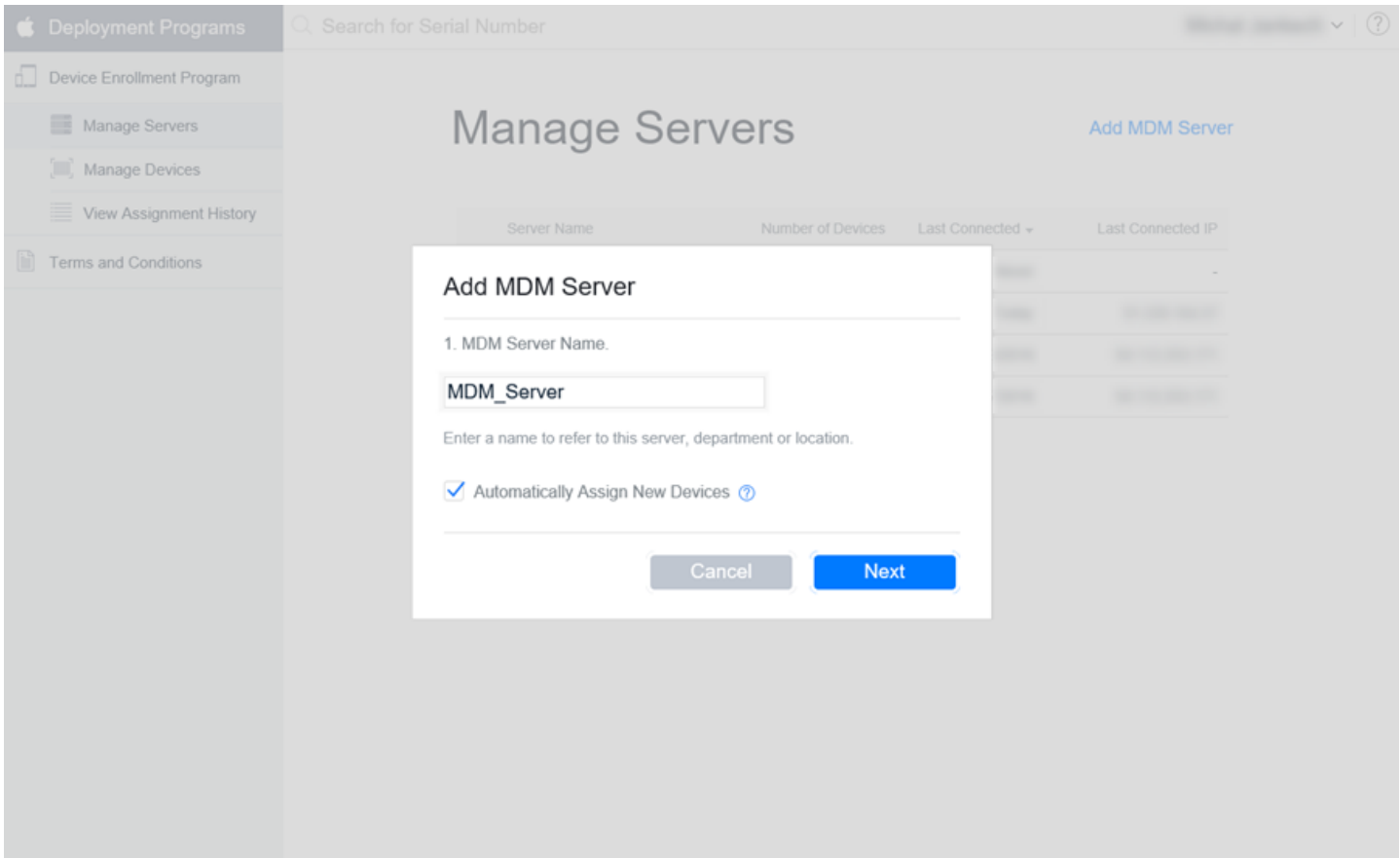
Device Enrollment Program (DEP) je program vytvorený spoločnosťou Apple, ktorý prináša nový spôsob registrácie firemných zariadení iOS. Prostredníctvom programu DEP môžete zariadenia iOS registrovať na diaľku bez potreby priameho kontaktu so zariadením a taktiež pri minimálnej interakcii používateľa. Apple DEP registrácia poskytuje správcom možnosť upravovať nastavenia zariadení iOS. Ponúka tiež možnosť zabrániť používateľovi odstrániť zo zariadenia MDM profil. Prostredníctvom programu DEP môžete zaregistrovať svoje existujúce zariadenia iOS (pokiaľ spĺňajú požiadavky na DEP registráciu), ako aj zariadenia iOS, ktoré vaša firma zakúpi v budúcnosti. Viac informácií o programe Apple DEP nájdete v príslušnej príručke a dokumentácii.

Pripojte svoj ESMC MDM Server k Apple DEP serveru:

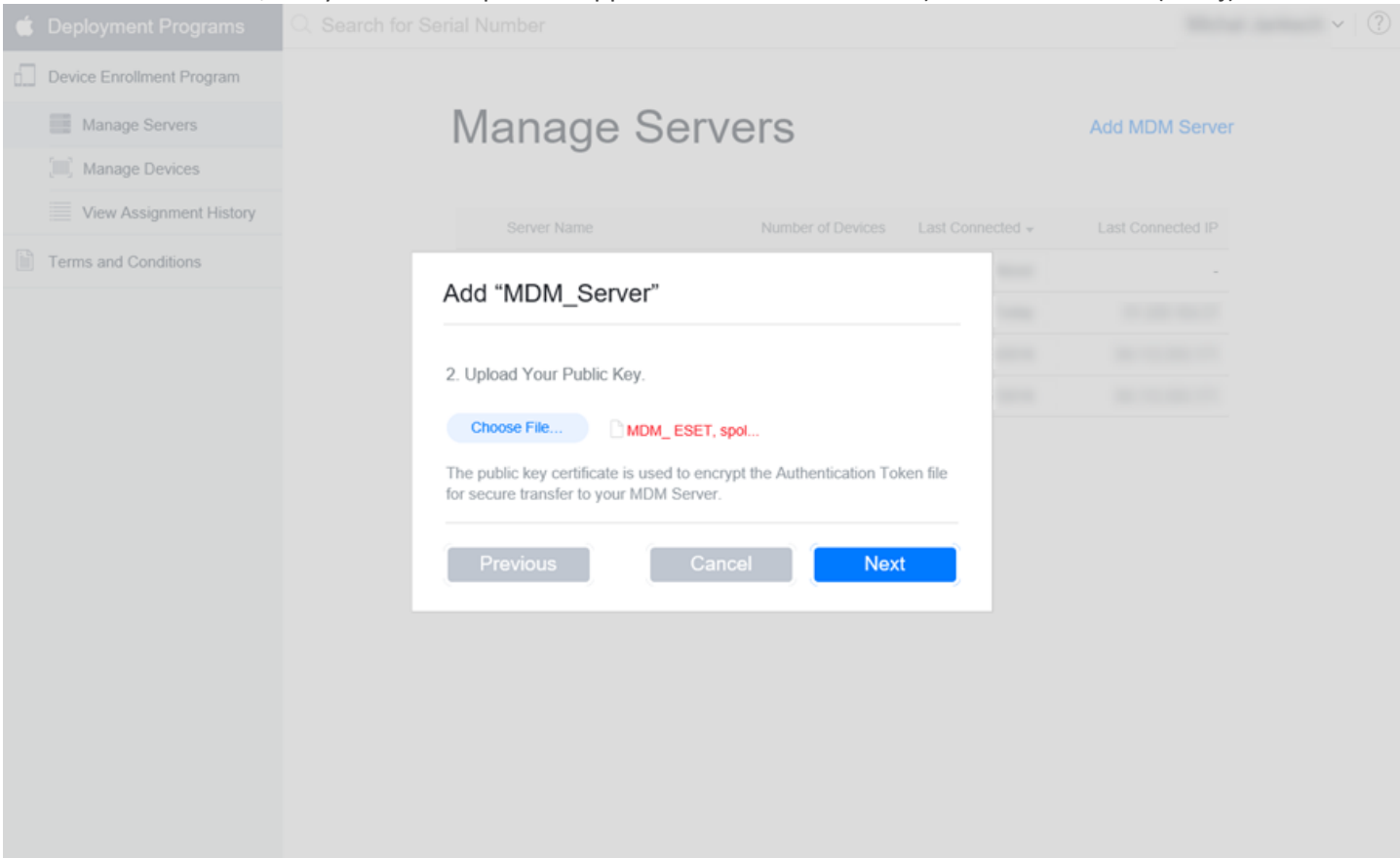
1. Uistite sa, že sú splnené všetky Apple DEP požiadavky týkajúce sa účtu i zariadení, ktoré chcete registrovať.
- Účet programu DEP:
  - Program DEP je dostupný len v niektorých krajinách. Informáciu o dostupnosti programu DEP v jednotlivých krajinách nájdete na webovej stránke Apple DEP.
  - Požiadavky týkajúce sa účtu programu DEP nájdete na nasledujúcich webových stránkach: požiadavky pre Apple Deployment Program a požiadavky pre Apple Device Enrollment Program.
  - Podrobné informácie o požiadavkách na registrované zariadenia nájdete na tejto stránke.
2. Prihláste sa do vášho Apple DEP účtu (pokiaľ ešte nemáte vytvorený Apple DEP účet, môžete si ho vytvoriť tu).
3. Z ponuky **Device Enrollment Program** na ľavej strane obrazovky zvoľte možnosť **Manage Servers** (Spravovať servery).



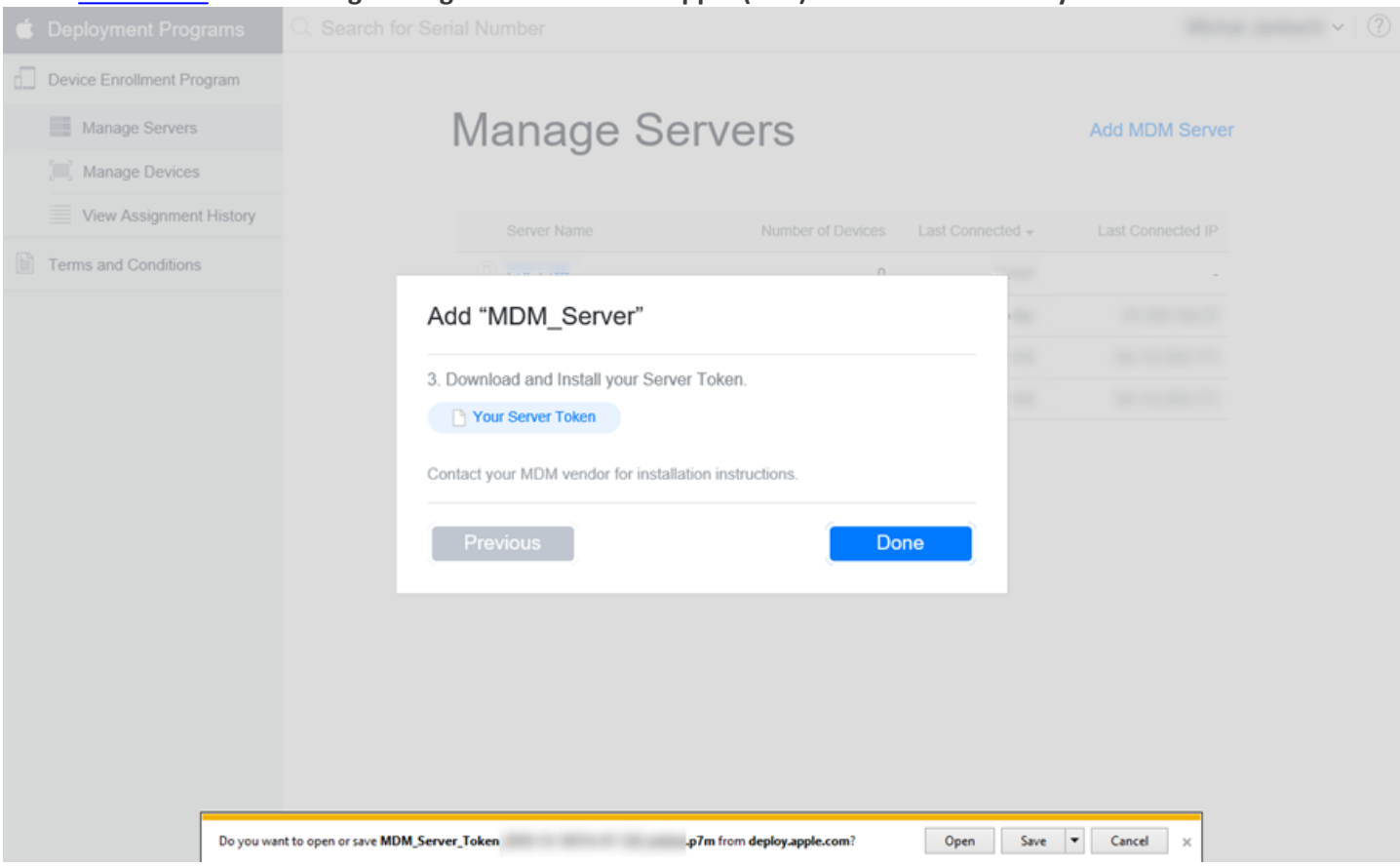
4. Kliknite na **Add MDM Server** (Pridať MDM Server) a otvorí sa okno pre pridanie MDM Servera.
5. Do prázdneho poľa zadajte názov **MDM Servera**, napr. „MDM_Server“, a kliknite na **Next**.



6. Nahrajte svoj verejný kľúč do portálu DEP. Kliknite na tlačidlo **Choose File**, vyberte súbor verejného kľúča (t. j. APNS certifikát, ktorý ste stiahli z portálu Apple Push Certificate Portal) a kliknite na **Next** (Ďalej).

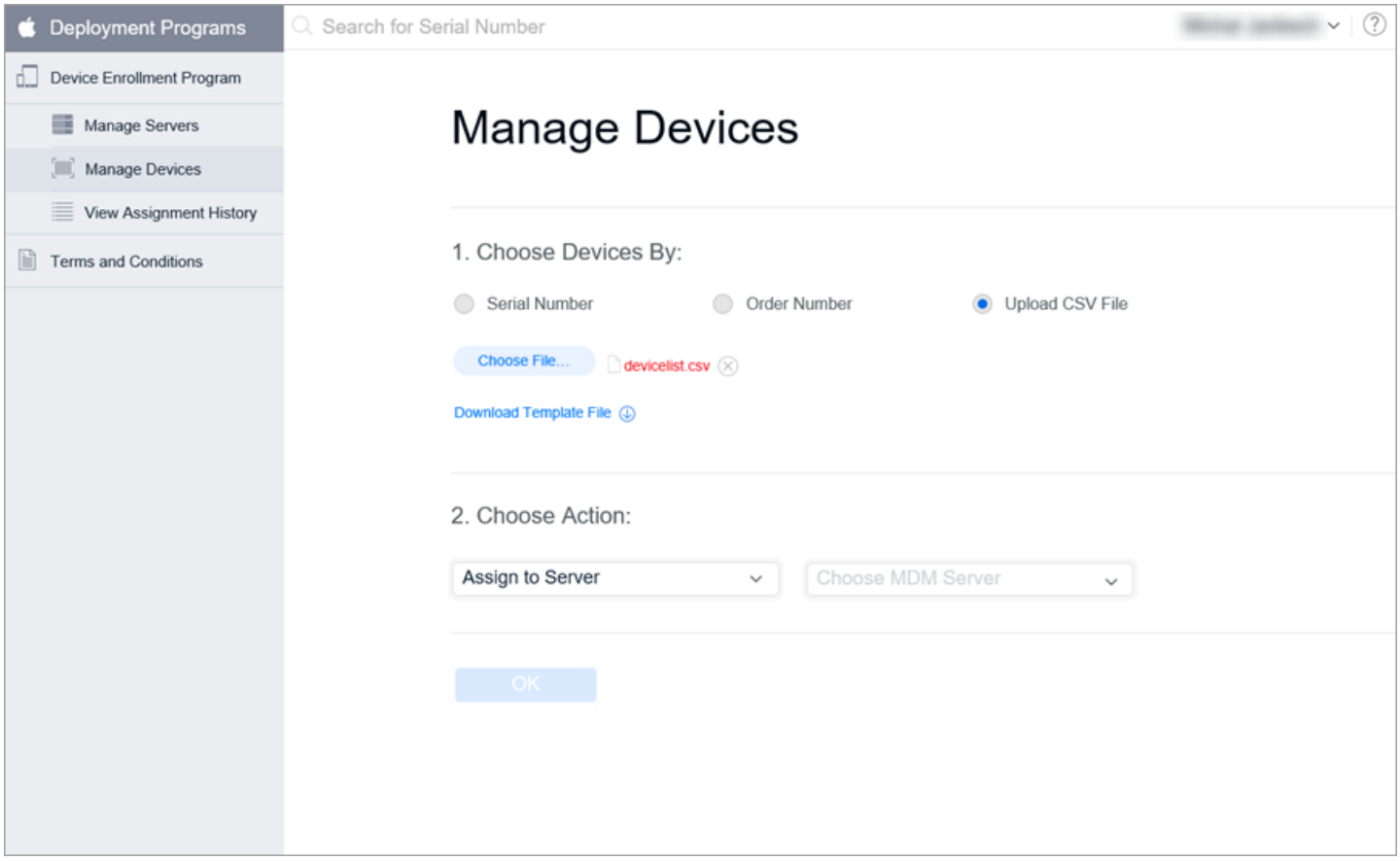


7. Teraz si môžete stiahnuť váš Apple DEP token. Tento súbor bude potrebné nahrať pri vytváraní politiky pre ESMC MDC v sekcii **Program registrácie zariadení Apple (DEP)** -> **Nahrať autorizačný token**.



Pridanie zariadení iOS do programu Apple DEP:

Ďalším krokom je priradenie zariadení iOS k vášmu virtuálnemu MDM Serveru na Apple DEP portáli. Pridať zariadenia iOS je možné na základe sériového čísla, čísla objednávky alebo nahraním zoznamu sériových čísel cieľových zariadení vo formáte CSV. Pri každej z týchto možností je potrebné zariadenie iOS priradiť k virtuálnemu MDM Serveru (ktorý ste vytvorili v predchádzajúcich krokoch).



Upozornenie:
Ak zariadenie odstránite z portálu DEP, bude odstránené natrvalo a nebude možné ho pridať späť.

Po priradení zariadení k MDM Serveru môžete odísť z Apple DEP portálu a prejsť do ESMC Web Console.

Upozornenie:
Ak registrujete firemné zariadenia iOS, ktoré sa už používajú (a ktoré spĺňajú požiadavky pre DEP registráciu), nové nastavenia upravené politikou budú na tieto zariadenia aplikované až po obnovení výrobných nastavení na príslušných cieľových zariadeniach.

Pre dokončenie procesu registrácie je potrebné nahrať APNS certifikát do politiky pre MDC, ktorá bude priradená k MDM Serveru. (Táto MDC politika bude upravovať nastavenia MDM Servera.)

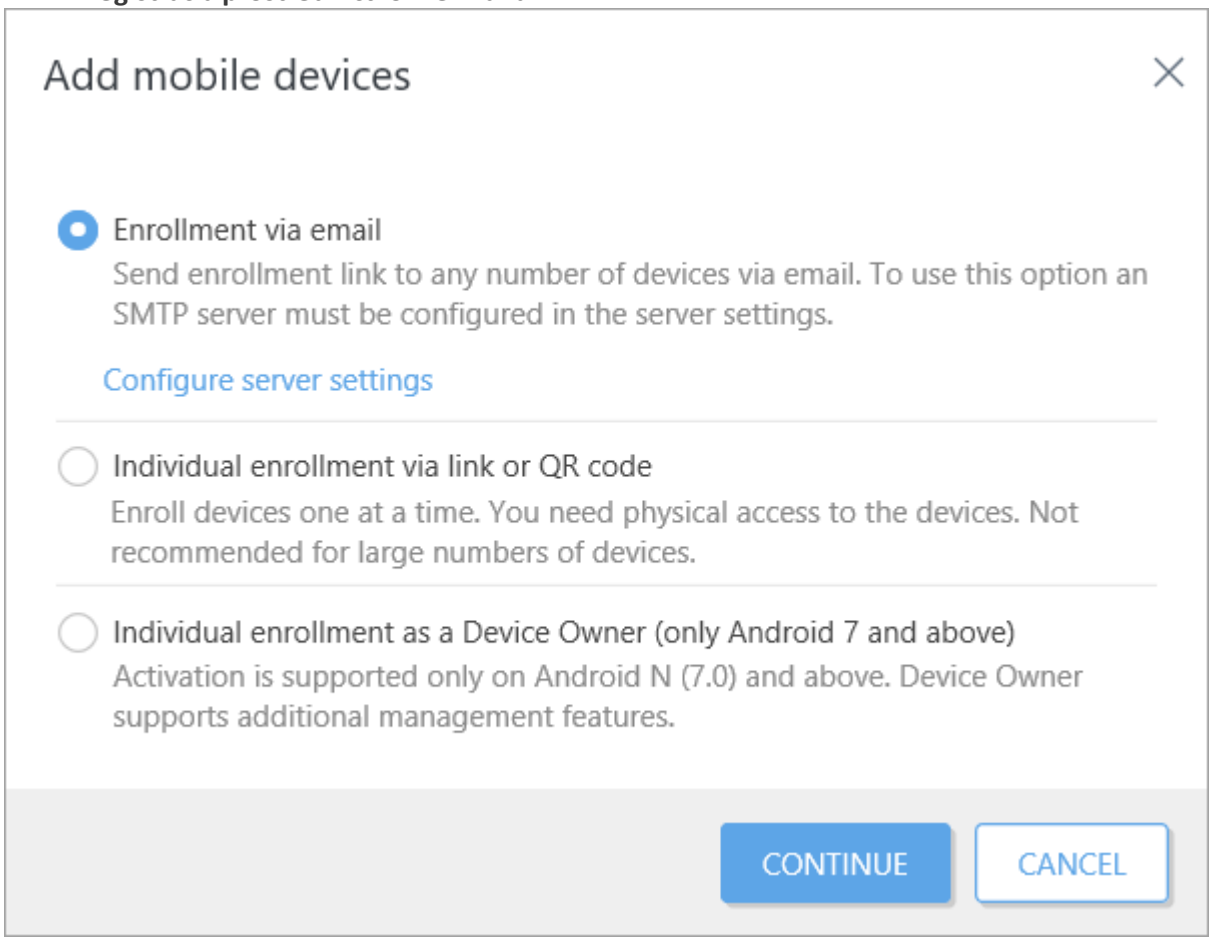
Poznámka:
Ak zariadenie iOS pri registrácii zobrazí chybové hlásenie, že sa nepodarilo stiahnuť registračný profil ESET, uistite sa, že MDM server je v rámci portálu DEP správne nakonfigurovaný (má správne certifikáty) a že ste k vášmu ESMC MDM Serveru na Apple DEP portáli priradili správne zariadenie iOS.

5.2.3 Registrácia prostredníctvom e-mailu

Táto metóda je optimálna pre hromadnú registráciu väčšieho počtu mobilných zariadení. Registračný odkaz môžete poslať na akýkoľvek počet zariadení prostredníctvom e-mailu. Každé mobilné zariadenie obdrží jedinečný jednorázový token podľa e-mailovej adresy.

Dôležité:
Je nutné nakonfigurovať SMTP server pre hromadnú registráciu prostredníctvom e-mailu. Prejdite do Nastavení servera, rozbaľte časť **Pokročilé nastavenia** a špecifikujte podrobnosti SMTP servera.

1. Pre pridanie nových mobilných zariadení prejdite do časti **Počítače** alebo **Viac** > **Skupiny**. Vyberte **Statickú skupinu**, do ktorej chcete pridať mobilné zariadenia a kliknite na **Pridať nový** > **Mobilné zariadenia** > **Registrácia prostredníctvom e-mailu**.



2. **Mobile Device Connector** – bude vybraný automaticky. Ak máte viac ako jeden MDC, vyberte FQDN názov toho MDC, ktorý chcete použiť. Ak ešte nemáte nainštalovaný Mobile Device Connector, postupujte podľa časti Inštalácia Mobile Device Connector – Windows alebo Linux, kde nájdete inštalačné inštrukcie.
3. **Licencia (voliteľná)** – kliknite na Vybrať a zvoľte licenciu, ktorá bude použitá pre aktiváciu. Pre mobilné zariadenie sa vytvorí úloha pre klienta Aktivácia produktu. Bude použitá licenčná jednotka (jedna pre každé mobilné zariadenie).
4. **Nadradená skupina** – ak nemáte špecifikovanú statickú skupinu pre mobilné zariadenia, odporúčame vám vytvoriť **Novú statickú skupinu** (nazvanú napr. **Mobilné zariadenia**). Ak už skupinu máte, kliknite na **/Všetko/**. Otvorí sa okno, kde môžete vybrať statickú skupinu.
5. **Zoznam zariadení** – špecifikujte zariadenia, ktoré chcete zaregistrovať. Pre pridanie mobilných zariadení môžete použiť nasledujúce funkcie:
   - **Pridať zariadenie** – jednotlivé zadanie, budete musieť manuálne zadať e-mailovú adresu priradenú k mobilnému zariadeniu, na ktoré bude odoslaný registračný e-mail. Ak tiež priradíte používateľa k mobilnému zariadeniu kliknutím na **Párovať** a vybratím konkrétneho používateľa, e-mailová adresa bude prepísaná adresou špecifikovanou v Správe používateľov. Ak chcete pridať ďalšie mobilné zariadenie, znova kliknite na **Pridať zariadenie** a zadajte požadované informácie.
   - **Pridať používateľa** – zariadenia môžete pridať označením príslušných používateľov zobrazených v sekcii Používatelia počítača. Kliknite na **Zrušiť párovanie**, ak chcete vykonať zmeny v zozname mobilných zariadení, ktoré budú registrované. Keď zrušíte priradenie používateľa k zariadeniu, bude tento používateľ označený ako nespárovaný. Kliknutím na **Párovať** môžete k nespárovanému zariadeniu priradiť požadovaného používateľa. Ak chcete niektorú položku vymazať, kliknite na ikonu **Odpadkového koša**.
   - **Import CSV** – metóda, ktorá uľahčuje pridanie veľkého množstva mobilných zariadení. Odovzdajte `.csv` súbor obsahujúci zoznam zariadení, ktoré majú byť pridané. Viac informácií nájdete v časti Import CSV.
   - **Skopírovať a vložiť** – pomocou tejto funkcie môžete importovať vlastný zoznam adries oddelených vlastnými oddeľovačmi (táto funkcia funguje podobne ako CSV import).

Poznámka:
Odporúčame, aby ste v prípade použitia metódy importu súboru CSV špecifikovali pre každú položku **Názov zariadenia**. Ide o názov zariadenia zobrazený v sekcii **Počítače**. Ak ponecháte pole **Názov zariadenia** prázdne, bude použitá e-mailová adresa a zobrazí sa ako názov zariadenia v častiach **Počítače** a **Skupiny**. Toto môže byť do určitej miery mätúce, obzvlášť v prípade, ak používate rovnakú e-mailovú adresu pre registráciu viacerých zariadení. Takáto e-mailová adresa bude zobrazená niekoľkokrát, čím sa sťaží rozpoznávanie individuálnych zariadení.

Dôležité:
Odporúčame, aby ste k mobilnému zariadeniu priradili aspoň jedného používateľa. Ak chcete používať prispôsobené politiky na iOS, k zariadeniu musí byť pridelený používateľ.

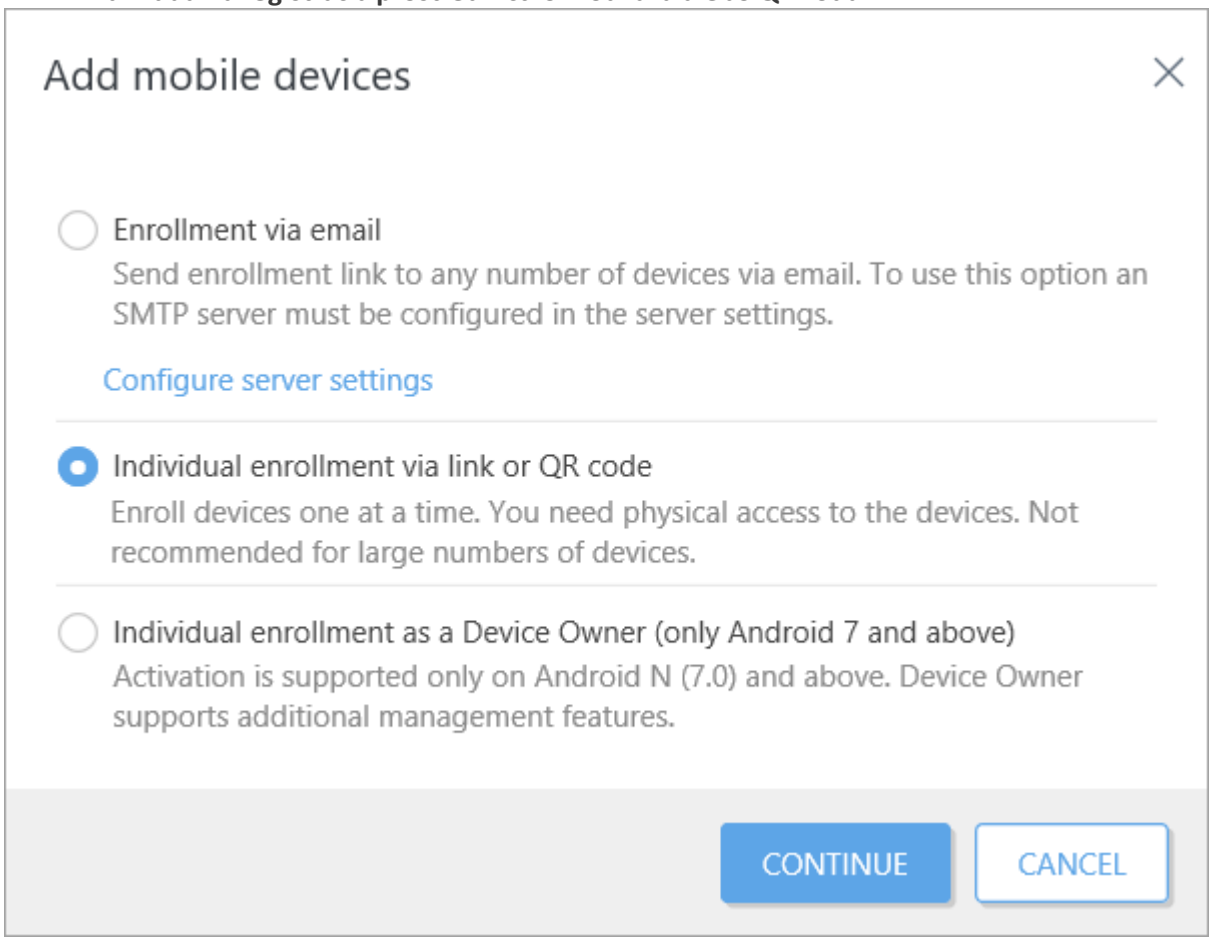
6. **E-mailová registračná správa** – prednastavená šablóna správy obsahujúca podrobnosti, ktoré sú väčšinou postačujúce, pričom môžete upraviť **Predmet** a **Obsah** doplnením ďalších informácií pre používateľov. **Inštrukcie** sú v registračnom e-maile zobrazené pod **obsahom** správy a obsahujú **Názov zariadenia** (alebo e-mailovú adresu) s registračným odkazom (URL). Ak používate na registráciu viacerých mobilných zariadení jednu e-mailovú adresu, zobrazí sa zoznam zariadení, pričom každé zariadenie bude mať svoj vlastný registračný odkaz (URL). Sú tam tiež inštrukcie, podľa ktorých musí používateľ mobilného zariadenia (iOS a Android) postupovať pre dokončenie registrácie.
7. Keď kliknete na **Registrovať**, na každú e-mailovú adresu bude odoslaný e-mail s príslušným registračným odkazom a inštrukciami.
8. Pre dokončenie registrácie mobilných zariadení postupujte podľa nasledujúcich krokov, prípadne vykonanie týchto úkonov prenechajte na používateľov/majiteľov daných mobilných zariadení:
   - Registrácia zariadení Android
   - Registrácia zariadení iOS

5.2.4 Individuálna registrácia prostredníctvom odkazu alebo QR kódu

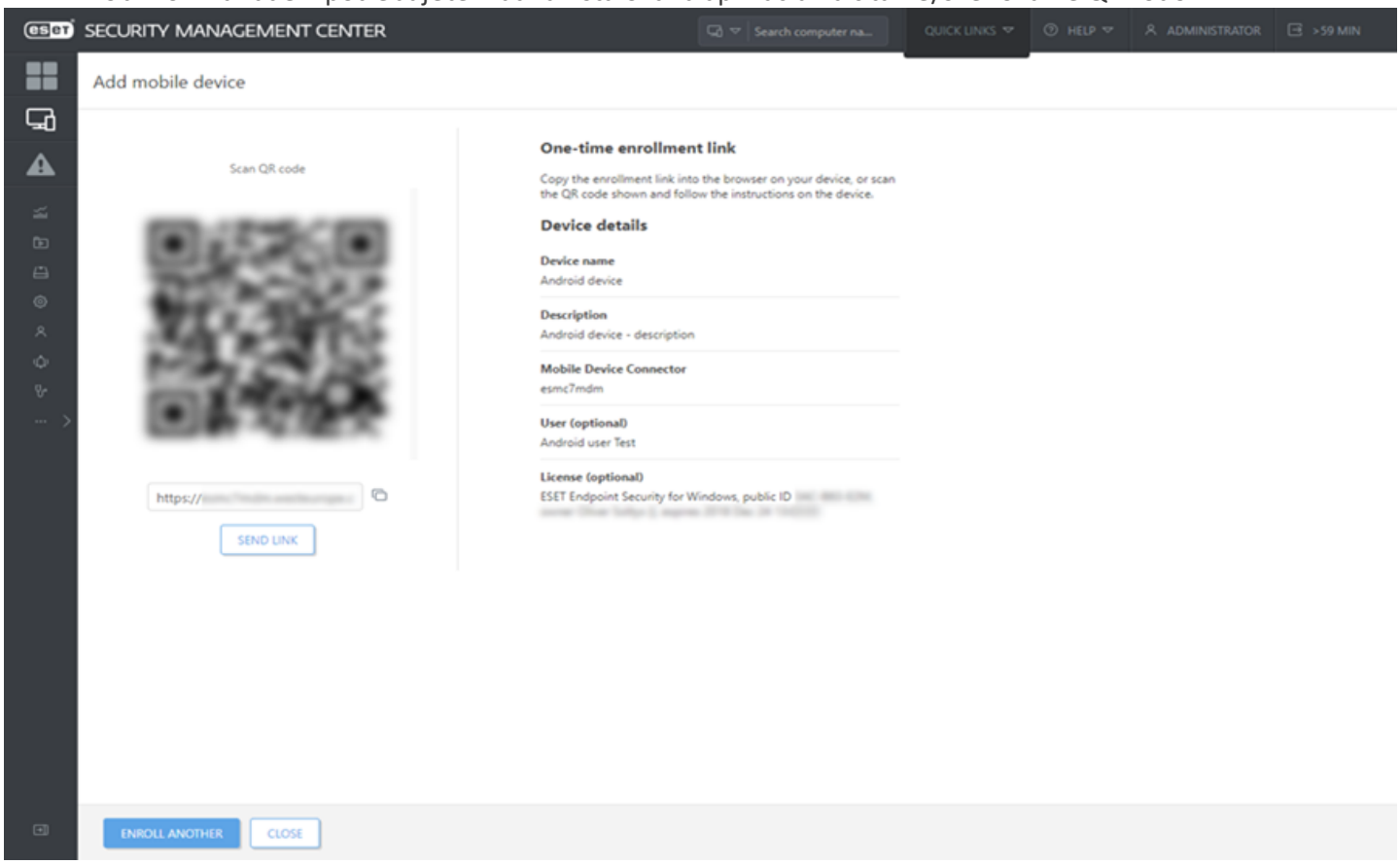
Pri registrácii mobilného zariadenia pomocou registračného odkazu alebo QR kódu budete potrebovať fyzický prístup k danému zariadeniu. Pre použitie QR kódu je tiež potrebné mať na mobilnom zariadení nainštalovanú aplikáciu na čítanie/skenovanie QR kódov.

POZNÁMKA:
Na registráciu väčšieho množstva mobilných zariadení odporúčame použiť Registráciu prostredníctvom e-mailu.

1. Pre pridanie nového mobilného zariadenia prejdite do časti **Počítače** alebo **Viac** > **Skupiny**. Vyberte **Statickú skupinu**, do ktorej chcete pridať mobilné zariadenie a kliknite na **Pridať nový** > **Mobilné zariadenia** > **Individuálna registrácia prostredníctvom odkazu alebo QR kódu**.



2. **Názov zariadenia** – zadajte **Názov** mobilného zariadenia (tento názov sa ukáže v zozname Počítače), prípadne zadajte aj **Popis**.
3. **Používateľ (voliteľný)** – odporúčame vám priradiť používateľa k mobilnému zariadeniu. Je to vyžadované pre iOS zariadenia, avšak voliteľné pre Android.
4. **Mobile Device Connector** – bude vybraný automaticky. Ak máte viac ako jeden MDC, vyberte si zo zoznamu kliknutím na FQDN. Ak ešte nemáte nainštalovaný Mobile Device Connector, postupujte podľa časti Inštalácia Mobile Device Connector – Windows alebo Linux, kde nájdete inštalačné inštrukcie.
5. **Licencia (voliteľná)** – kliknite na **Vybrať** a zvoľte licenciu, ktorá bude použitá pre aktiváciu. Pre mobilné zariadenie sa vytvorí úloha pre klienta Aktivácia produktu. Bude použitá licenčná jednotka (jedna pre každé mobilné zariadenie).
6. **Nadradená skupina** – ak nemáte špecifikovanú statickú skupinu pre mobilné zariadenia, odporúčame vám vytvoriť **Novú statickú skupinu** (nazvanú napr. „Mobilné zariadenia“). Ak už skupinu máte, kliknite na **/Všetko**. Otvorí sa okno, kde môžete vybrať statickú skupinu.
7. Po kliknutí na **Ďalej** sa zobrazí registračný **Odkaz** (URL) a **QR kód**. Manuálne zadajte celú URL adresu do webového prehliadača mobilného zariadenia (napr. *https://eramdm:9980/token*, pričom token bude odlišný pre každé mobilné zariadenie) alebo pošlite túto URL adresu na mobilné zariadenie iným spôsobom. Môžete tiež použiť uvedený **QR kód**, čo môže byť jednoduchšie ako manuálne zadávanie URL adresy, avšak na danom mobilnom zariadení potrebujete mať nainštalovanú aplikáciu na čítanie/skenovanie QR kódov.



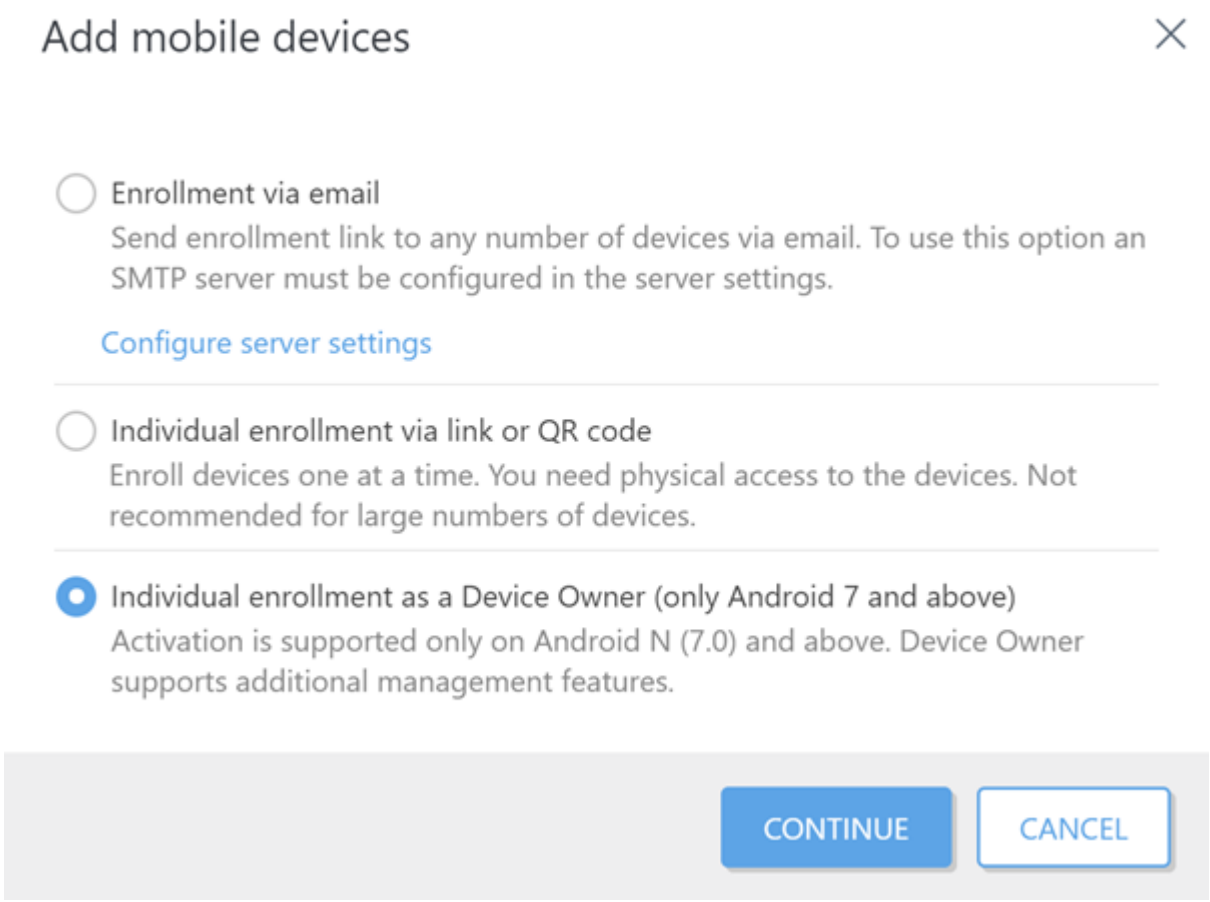
8. Pre pridanie ďalšieho mobilného zariadenia kliknite na **Registrovať ďalšie**. Otvorí sa nové okno pre pridanie mobilného zariadenia, ktoré si pamätá predchádzajúce výbery položiek v rámci sekcie „Všeobecné“. Budete teda musieť zadať iba názov zariadenia a priradiť používateľa. Kliknite na **Ďalej** a postupujte podľa inštrukcií v kroku č. 7. Po vygenerovaní registračných odkazov a QR kódov kliknite na **Zatvoriť**, čím sa vrátite do predchádzajúceho okna.
9. Pre vykonanie samotnej registrácie mobilných zariadení postupujte podľa nasledujúcich inštrukcií:
   - Registrácia zariadení Android
   - Registrácia zariadení iOS

5.2.5 Individuálna registrácia v rámci režimu Vlastník zariadenia

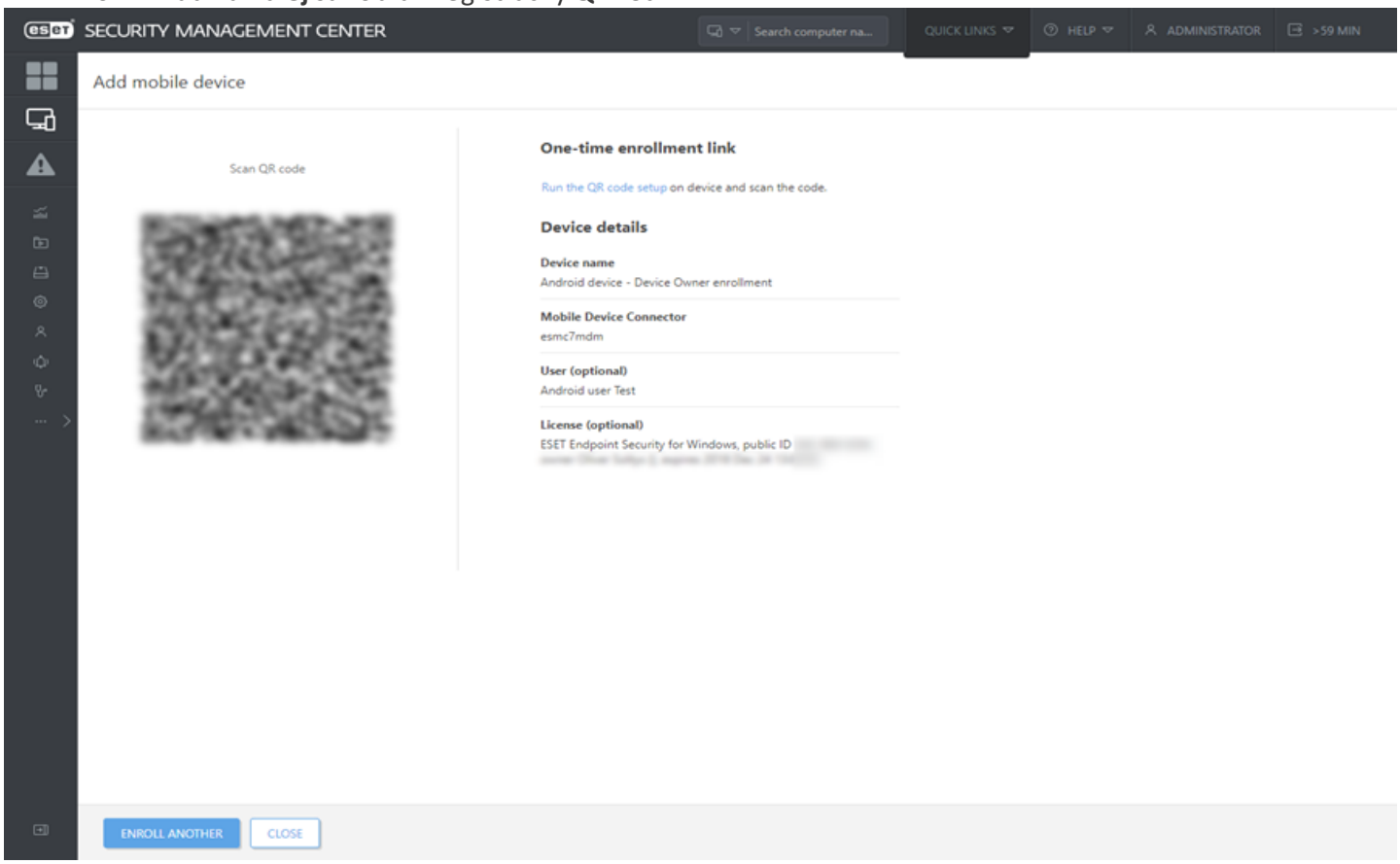
Pri registrácii mobilného zariadenia Android pomocou registračného QR kódu budete potrebovať fyzický prístup k danému zariadeniu. Túto registráciu je tiež možné vykonať iba na zariadení, ktoré je nové, prípadne bolo vymazané alebo na ňom boli obnovené výrobné nastavenia.

POZNÁMKA:
Nie je možné použiť metódu registrácie prostredníctvom e-mailu pre hromadnú registráciu zariadení Android v rámci režimu Vlastník zariadenia.

1. Pre pridanie nového mobilného zariadenia prejdite do časti **Počítače** alebo **Viac** > **Skupiny**. Vyberte **Statickú skupinu**, do ktorej chcete pridať mobilné zariadenie a kliknite na **Pridať nový** > **Mobilné zariadenia** > **Individuálna registrácia ako vlastník zariadenia (iba Android 7 a vyššie)**.



2. **Názov zariadenia** – zadajte **Názov** mobilného zariadenia (tento názov sa ukáže v zozname Počítače).
3. **Používateľ (voliteľný)** – odporúčame vám priradiť používateľa k mobilnému zariadeniu. Je to vyžadované pre iOS zariadenia, avšak voliteľné pre Android.
4. **Mobile Device Connector** – bude vybraný automaticky. Ak máte viac ako jeden MDC, vyberte si zo zoznamu kliknutím na FQDN. Ak ešte nemáte nainštalovaný Mobile Device Connector, postupujte podľa časti Inštalácia Mobile Device Connector – Windows alebo Linux, kde nájdete inštalačné inštrukcie.
5. **Licencia (voliteľná)** – kliknite na **Vybrať** a zvoľte licenciu, ktorá bude použitá pre aktiváciu. Pre mobilné zariadenie sa vytvorí úloha pre klienta Aktivácia produktu. Bude použitá licenčná jednotka (jedna pre každé mobilné zariadenie).
6. **Nadradená skupina** – ak nemáte špecifikovanú statickú skupinu pre mobilné zariadenia, odporúčame vám vytvoriť **Novú statickú skupinu** (nazvanú napr. Mobilné zariadenia). Ak už skupinu máte, kliknite na **/Všetko**. Otvorí sa okno, kde môžete vybrať statickú skupinu.
7. Po kliknutí na **Ďalej** sa zobrazí registračný **QR kód**.



8. Pokračujte na zariadení Android podľa týchto krokov.
9. Pre pridanie ďalšieho mobilného zariadenia kliknite na **Registrovať ďalšie**. Otvorí sa nové okno pre pridanie mobilného zariadenia, ktoré bude obsahovať predchádzajúce výbery položiek v rámci sekcie „Všeobecné“. Budete teda musieť zadať iba názov zariadenia a priradiť používateľa. Kliknite na **Ďalej** a postupujte podľa inštrukcií v kroku č. 7. Po vygenerovaní registračných QR kódov kliknite na **Zatvoriť**, čím sa vrátite do predchádzajúceho okna.

5.3 Príklady nastavenia politík

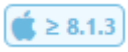
5.3.1 Vytvorenie politiky pre iOS MDM – Exchange ActiveSync účet

Politika pre iOS MDM umožňuje upravovať nastavenia zariadení iOS. Môže ísť rovnako o zariadenia iOS registrované v programe DEP, ako aj o zariadenia registrované klasickým spôsobom.

- Niektoré nastavenia sú označené ikonou DEP 

. Tieto nastavenia budú politikou aplikované len na zariadeniach iOS, ktoré boli zaregistrované do portálu Apple DEP. Odporúčame vám tieto nastavenia neupravovať, pokiaľ vytvárate politiku pre zariadenia iOS, ktoré nie sú registrované v programe DEP.
- Niektoré nastavenia môžu byť politikou aplikované len na zariadenia s určitou verziou operačného systému iOS. Tieto nastavenia sú označené ikonou, ktorá predstavuje príslušnú verziu operačného systému iOS.
  - iOS vo verzii 9.0 a vyššej 

  - iOS vo verzii 9.3 a vyššej 

  - iOS vo verzii 8.1.3 a vyššej 

  - iOS vo verzii 11.0 a vyššej 

- Pokiaľ sú pri určitom nastavení zobrazené oba druhy ikon (ikona DEP aj ikona verzie iOS), zariadenie na ktoré chcete aplikovať politiku musí spĺňať obe požiadavky, v opačnom prípade úpravu daného nastavenia nebude možné aplikovať.

Prezrite si ukážkový scenár uvedený nižšie, ktorý popisuje použitie politiky pre iOS MDM na nastavenie poštového konta Microsoft Exchange:

Túto politiku môžete použiť na konfiguráciu poštového konta Microsoft Exchange, kontaktov a kalendára na iOS mobilných zariadeniach používateľov. Výhodou používania takejto politiky je, že stačí vytvoriť len jednú politiku, ktorú potom aplikujete na viaceré iOS mobilné zariadenia bez potreby konfigurovať každé zariadenie samostatne. Toto je možné pomocou používateľských atribútov Active Directory. Bude potrebné špecifikovať premennú, napr. `${exchange_login/exchange}` a táto premenná bude nahradená hodnotou z AD pre príslušného používateľa.

Ak nepoužívate Microsoft Exchange alebo Exchange ActiveSync, môžete každú službu nastaviť manuálne (**Poštové účty**, **Kontaktové účty**, **LDAP účty**, **Kalendárové účty** a **Odoberané kalendárové účty**).

Nasleduje príklad vytvorenia a aplikovania novej politiky pre automatické nastavenie pošty, kontaktov a kalendára pre každého používateľa na iOS mobilnom zariadení pomocou Exchange ActiveSync (EAS) protokolu určeného na synchronizáciu týchto služieb.

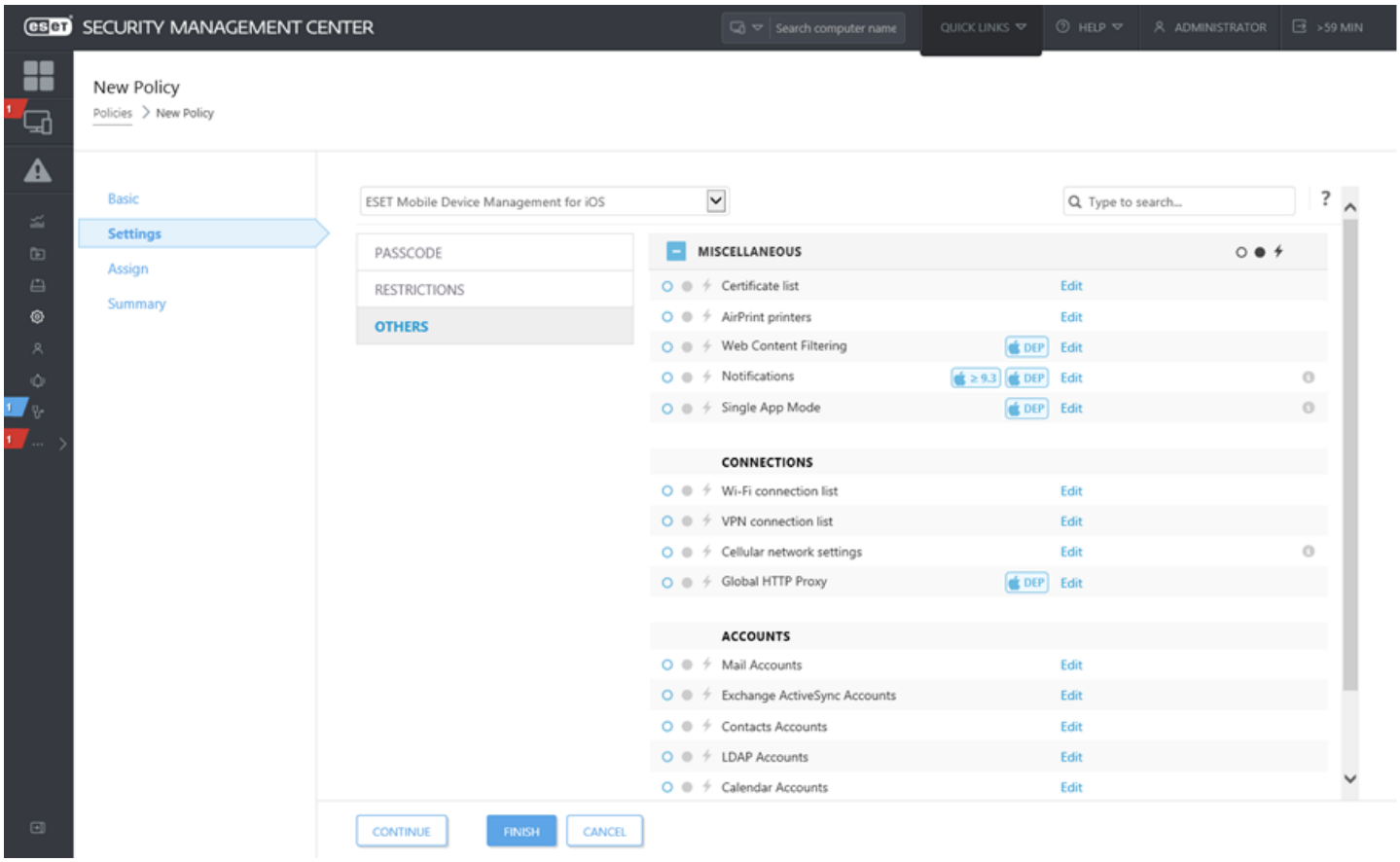
Poznámka:
Predtým, ako začnete nastavovať túto politiku, sa uistite, že ste už vykonali kroky popísané v časti Správa mobilných zariadení.

Základné

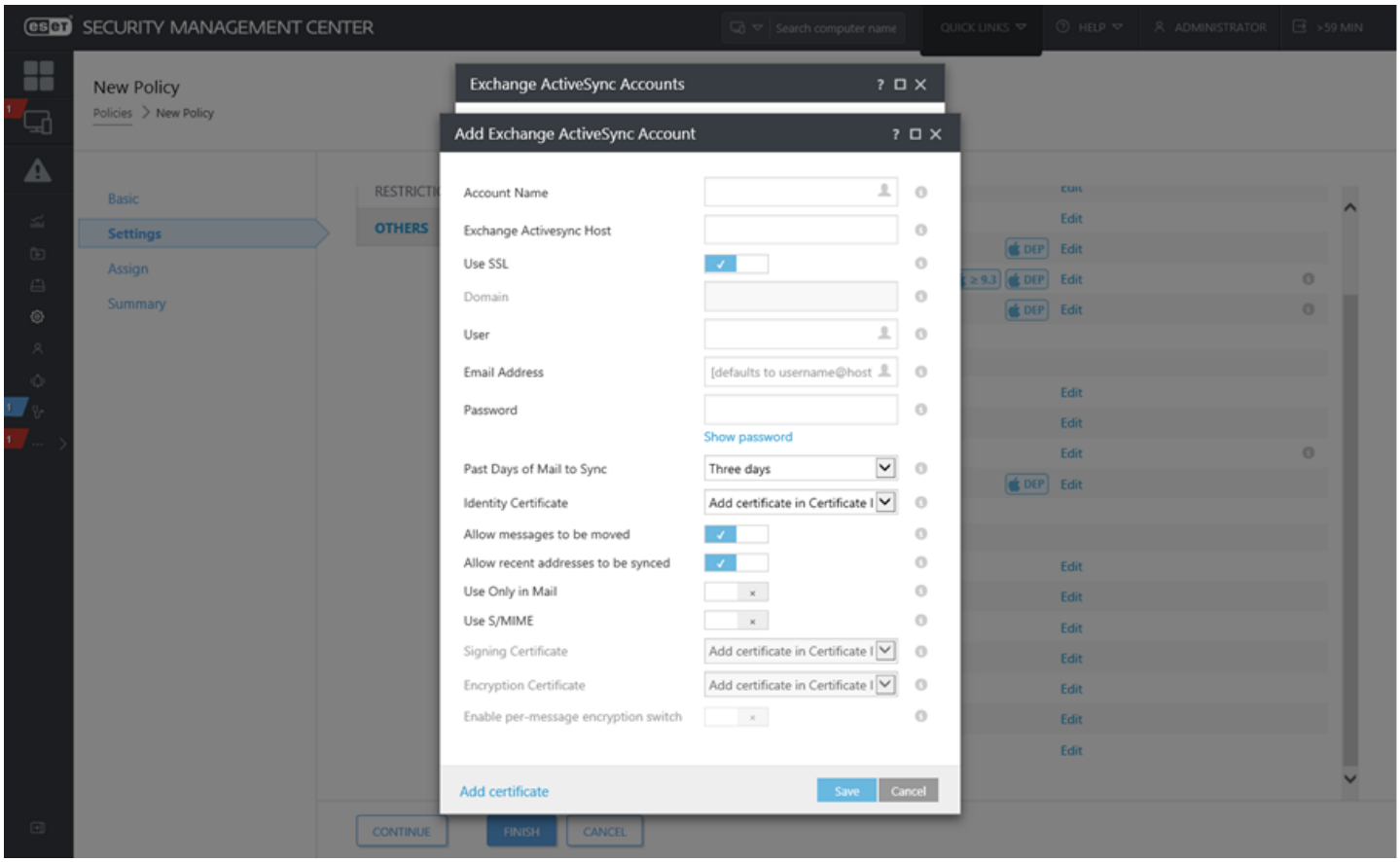
Zadajte **Názov** politiky. Pole **Popis** je voliteľné.

Nastavenia

Z roletového menu vyberte možnosť **ESET Mobile Device Management pre iOS**, kliknite na **Iné** pre rozbalenie kategórií a potom kliknite na **Upraviť** vedľa položky **Exchange ActiveSync účty**.

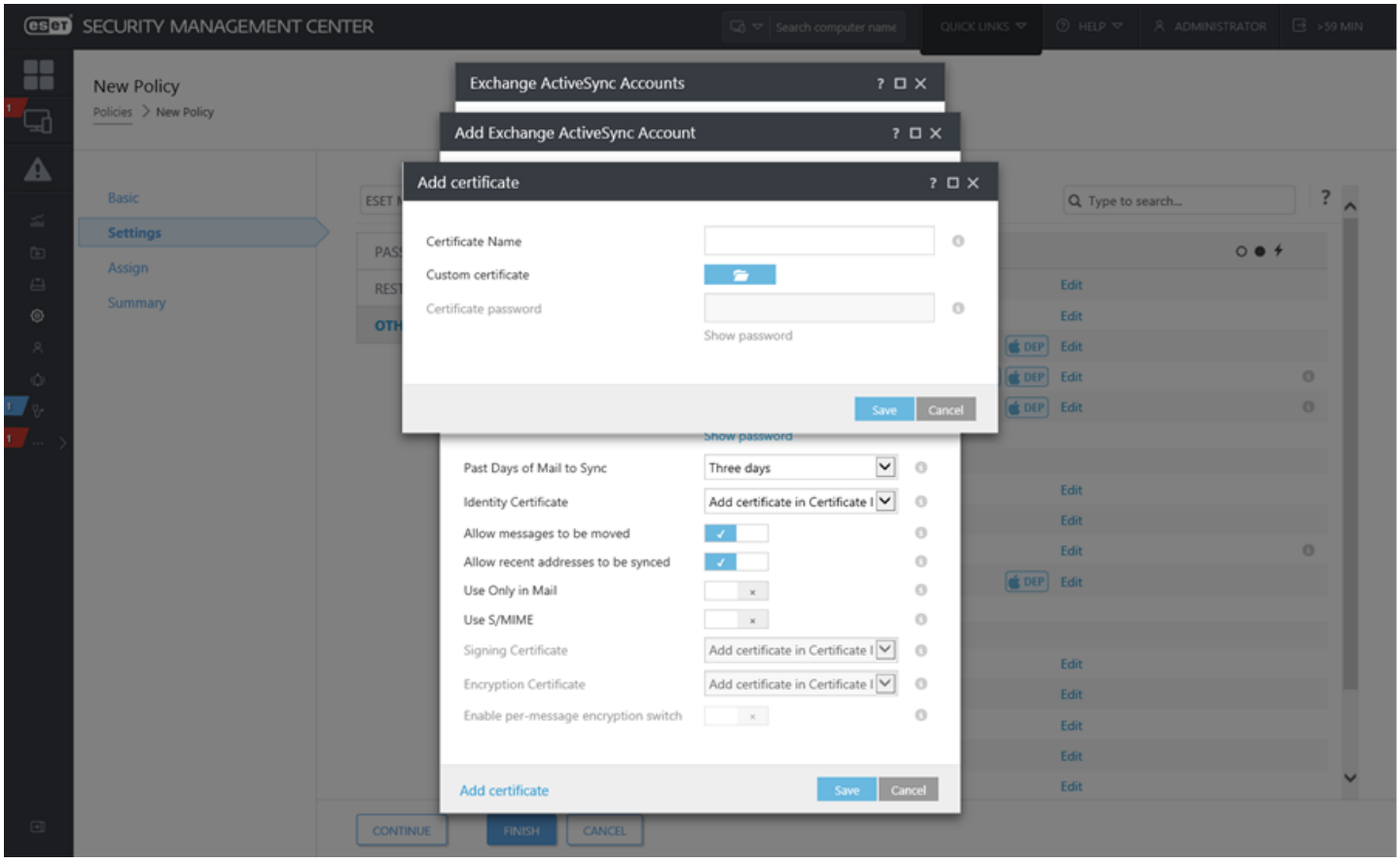


Kliknite na **Pridať** a upresnite podrobnosti vášho Exchange ActiveSync účtu. V určitých poliach môžete použiť premenné (podľa zoznamu v roletovom menu), napr. pre položky Používateľ alebo E-mailová adresa. Tieto premenné budú nahradené skutočnými hodnotami zo sekcie Používatelia počítača pri aplikovaní politiky.



- **Názov účtu** – zadajte názov účtu Exchange.
- **Exchange ActiveSync Host** – upresnite názov hostiteľa alebo IP adresu pre Exchange Server.
- **Použiť SSL** – táto možnosť je predvolene povolená. Poskytuje informácie o tom, či Exchange Server využíva v rámci overovania Secure Sockets Layer (SSL).
- **Doména** – toto pole je voliteľné. Môžete zadať doménu, do ktorej daný účet patrí.
- **Používateľ** – prihlasovacie meno pre Exchange. Z roletového menu vyberte formát, ktorý bude následne doplnený z atribútov používateľa v Active Directory.
- **E-mailová adresa** – z roletového menu vyberte formát, ktorý bude následne doplnený z atribútov používateľa v Active Directory.
- **Používateľské heslo** – voliteľné. Odporúčame ponechať toto pole prázdne. Ak ostane prázdne, používatelia budú vyzvaní na vytvorenie ich vlastných hesiel.
- **Synchronizovať e-maily za počet uplynulých dní** – vyberte počet dní, za ktoré sa majú synchronizovať e-maily.
- **Certifikát identity** – údaje pre pripojenie do ActiveSync.
- **Povoliť presúvanie správ** – ak je táto možnosť povolená, správy môžu byť presunuté z jedného účtu na druhý.
- **Povoliť súčasným adresám synchronizáciu** – ak je táto možnosť povolená, používateľovi je umožnené vykonávať synchronizáciu naposledy použitých e-mailových adries medzi zariadeniami.
- **Použiť len v aplikácii Mail** – túto možnosť povoľte, ak chcete umožniť odosielanie e-mailových správ z tohto účtu len prostredníctvom aplikácie Mail.
- **Použiť S/MIME** – ak povolíte túto možnosť, odchádzajúce e-mailové správy budú šifrované pomocou S/MIME.
- **Podpisový certifikát** – údaje pre podpisovanie MIME dát.
- **Šifrovací certifikát** – údaje pre šifrovanie MIME dát.
- **Povoliť výber šifrovania pre každú správu zvlášť** – povolením tejto možnosti bude môcť o šifrovaní správ rozhodnúť používateľ.

Poznámka:
Ak nezadáte hodnotu a necháte pole prázdne, používatelia mobilných zariadení budú vyzvaní na zadanie danej hodnoty. Jedným z príkladov môže byť napr. **Heslo**.

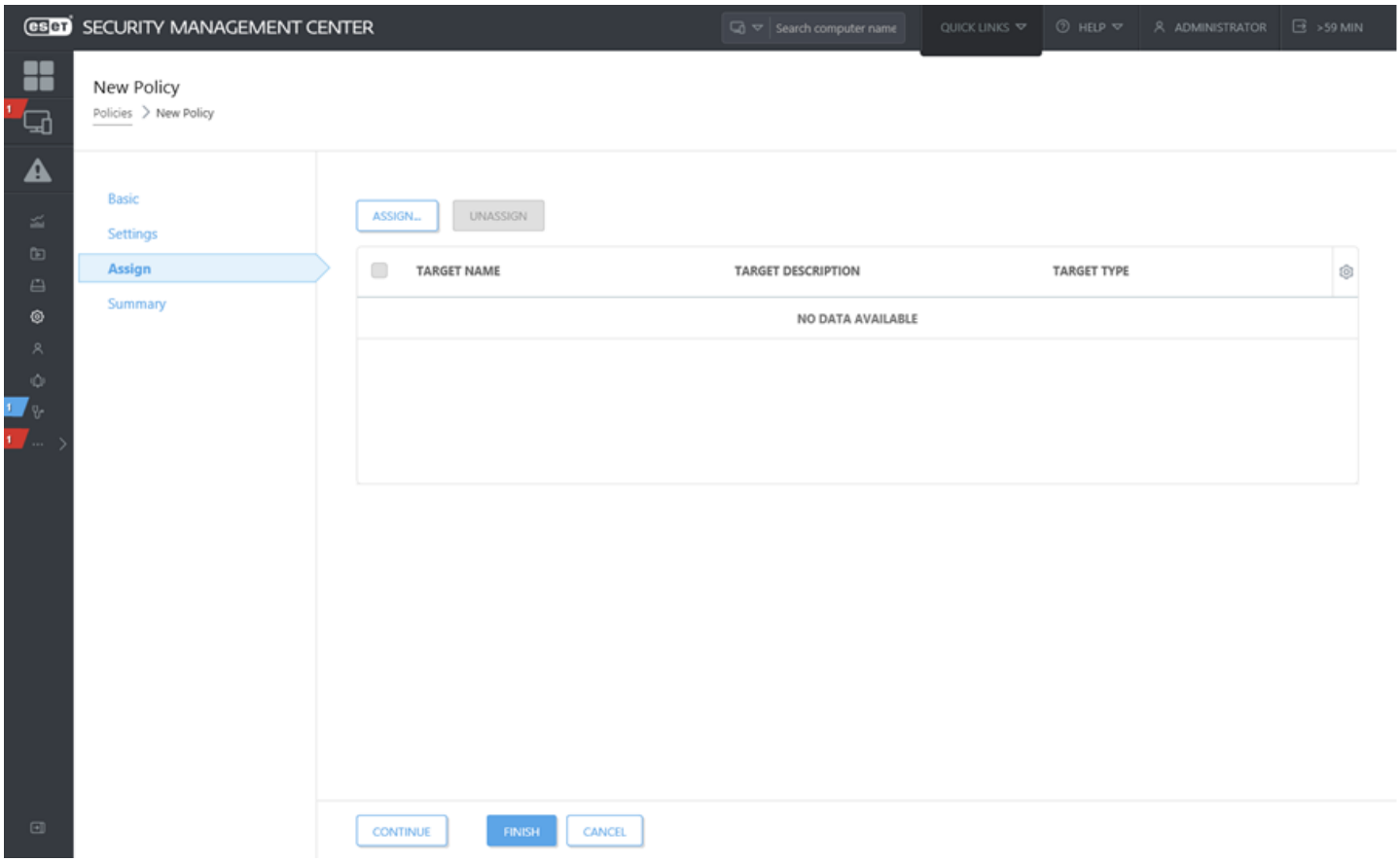


- **Pridať certifikát** – môžete v prípade potreby pridať konkrétne Exchange certifikáty (identita používateľa, digitálny podpis alebo šifrovací certifikát).

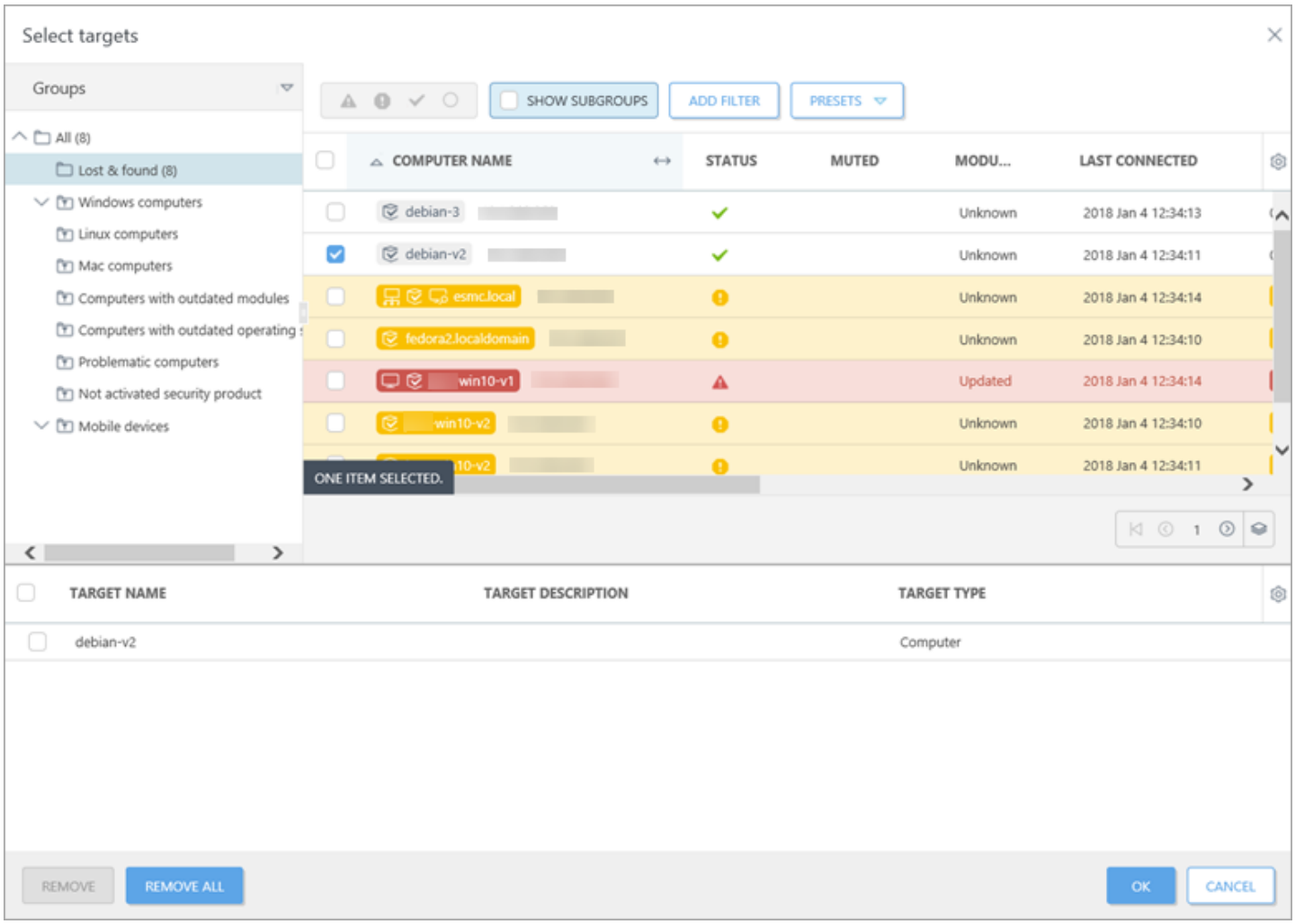
Poznámka:
Pomocou krokov uvedených vyššie môžete v prípade potreby pridať viacero Exchange ActiveSync účtov. To znamená, že na jednom mobilnom zariadení bude nastavených viacero účtov. Taktiež môžete upravovať už existujúce účty.

Priradiť

Zvoľte klientov (individuálne počítače/mobilné zariadenia alebo celé skupiny), ku ktorým bude priradená daná politika.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte požadované klientske zariadenia a kliknite na **OK**.



Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

5.3.2 Vytvorenie politiky pre MDC na aktiváciu APNS/DEP pre umožnenie registrácie zariadení iOS

Dôležité:
Pri zmene HTTPS certifikátu používaného v rámci vašej politike pre MDC postupujte podľa nasledujúcich krokov, aby sa zabránilo odpájaniu mobilných zariadení z vášho MDM:

1. Vytvorte a aplikujte novú politiku, ktorá používa nový HTTPS certifikát.

2. Počkajte, kým sa zariadenia pripoja k MDM serveru a prijmú novú politiku.

3. Overte, či zariadenia používajú nový HTTPS certifikát.

4. Počkajte aspoň 72 hodín, kým sa nová politika dostane na všetky zariadenia. Ak už všetky zariadenia prijali novú politiku (služba MDM Core prestane zobrazovať upozornenie „Prebieha zmena HTTPS certifikátu. Ešte sa používa pôvodný certifikát.“), môžete odstrániť starú politiku.

V nasledujúcom príklade vytvoríme novú politiku pre nástroj ESET Mobile Device Connector na aktiváciu APNS (Apple Push Notification Services) a pre umožnenie registrácie zariadení iOS. Vytvorenie tejto politiky je nevyhnutným krokom pre registráciu iOS zariadení. Pred tým, ako nastavíte túto politiku, vytvorte nový APN certifikát. Tento certifikát musí byť podpísaný spoločnosťou Apple v portáli Apple Push Certificates, aby sa z neho stal podpísaný certifikát alebo **APNS certifikát**. Podrobné inštrukcie nájdete v časti APN certifikát.

Základné

Zadajte **Názov** politiky. Pole **Popis** je voliteľné.

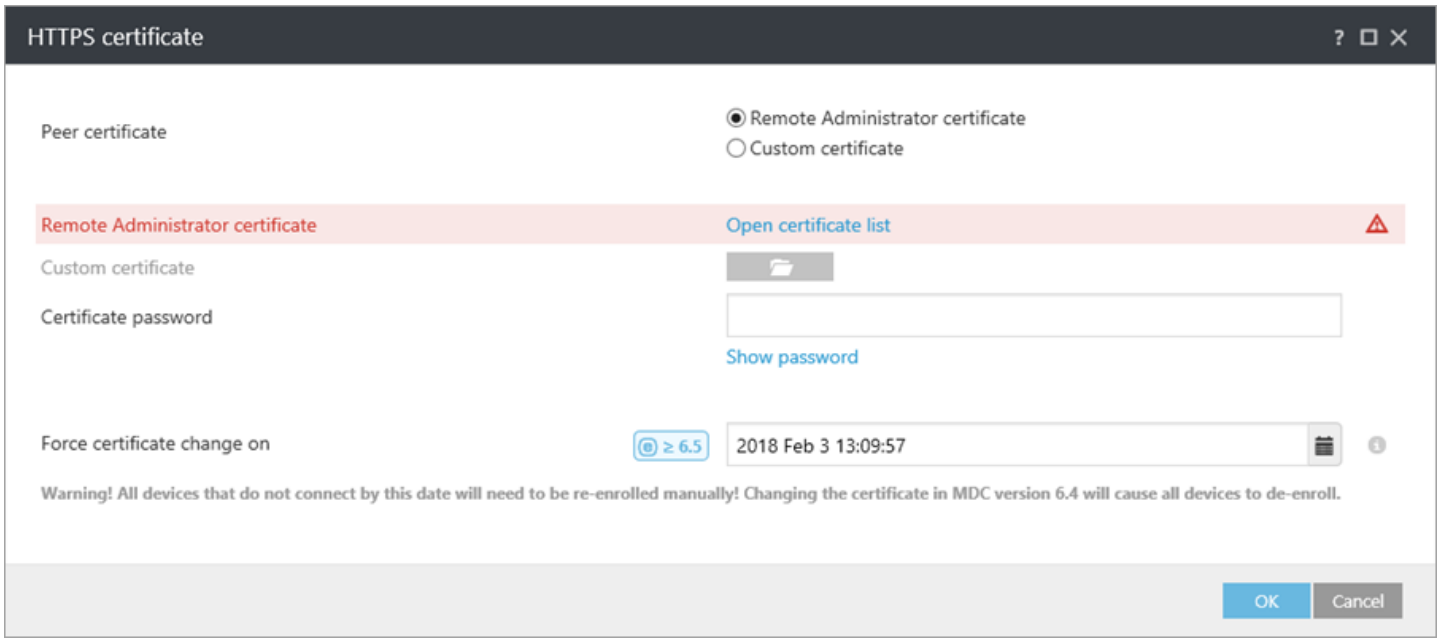
Nastavenia

Z roletového menu vyberte možnosť **ESET Mobile Device Connector**.

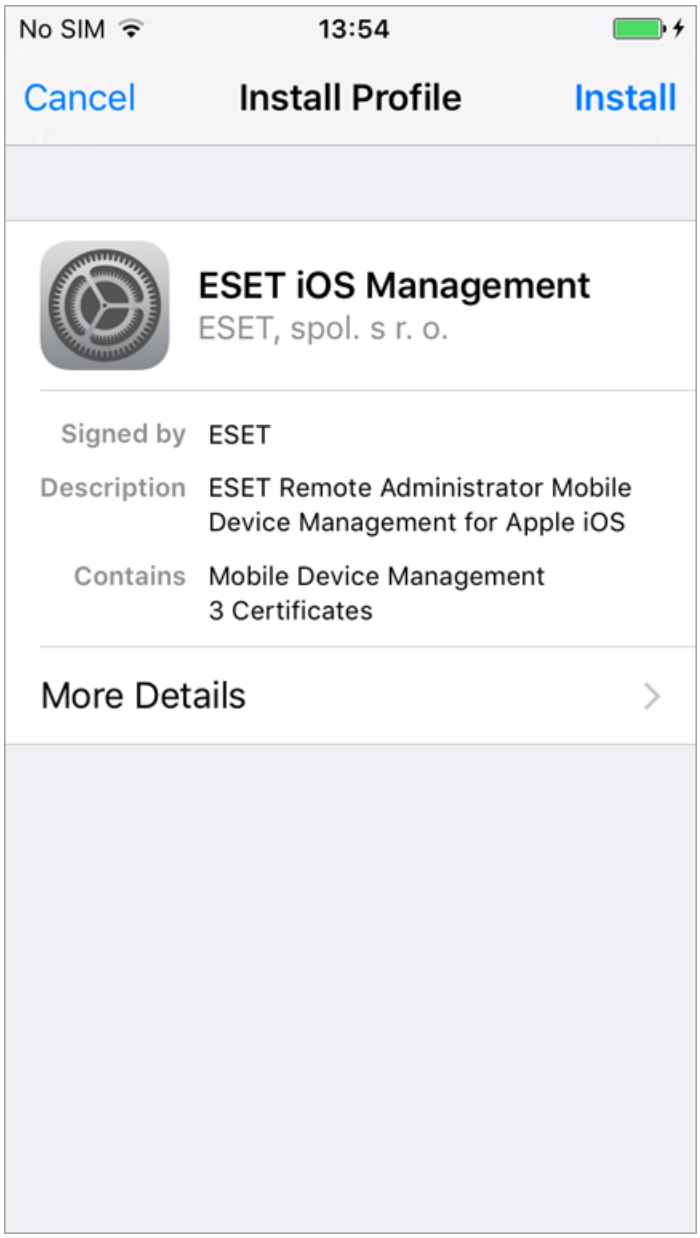
Dôležité:
Ak ste nainštalovali MDM Server pomocou all-in-one inštalátora (teda nie ako samostatný komponent), HTTPS certifikát bol vygenerovaný automaticky počas samotnej inštalácie. Toto sa vzťahuje len na inštalátor pre ERA 6.5 a novšie verzie. Vo všetkých ostatných prípadoch budete musieť použiť vlastný HTTPS certifikát. Viac informácií nájdete v bode č. 1 kapitoly Správa mobilných zariadení.

Môžete použiť ESMC certifikát (podpísaný certifikačnou autoritou ESMC) alebo vlastný certifikát. Pomocou funkcie **Vynútiť zmenu certifikátu** môžete zadať dátum a čas, kedy bude potrebné certifikát zmeniť. Viac informácií nájdete v popise umiestnenom vedľa tohto nastavenia.

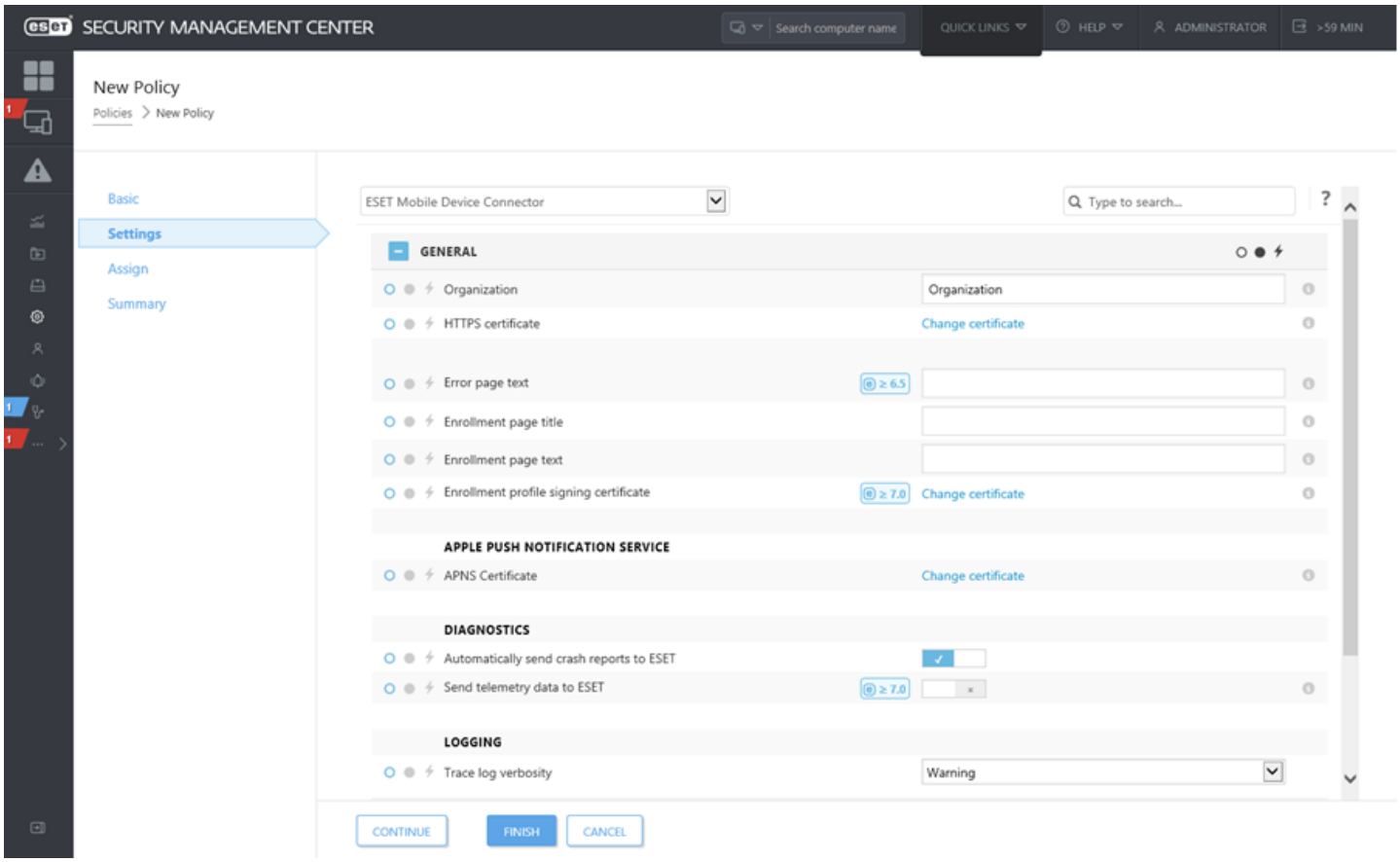
Poznámka:
Do poľa vedľa položky **Organizácia** zadajte názov vašej spoločnosti. Tento názov je následne použitý generátorom registračného profilu, ktorý túto informáciu uvedie v profile.



V sekcii **Všeobecné** môžete odovzdať HTTPS certifikát, ktorý bude použitý na podpísanie registračného profilu – možnosť **Podpisový certifikát profilu pre nasadenie** (toto má vplyv iba na registráciu mimo programu DEP). Týmto zabezpečíte, že na zariadeniach iOS bude počas registrácie uvedená informácia, že daný profil je podpísaný.

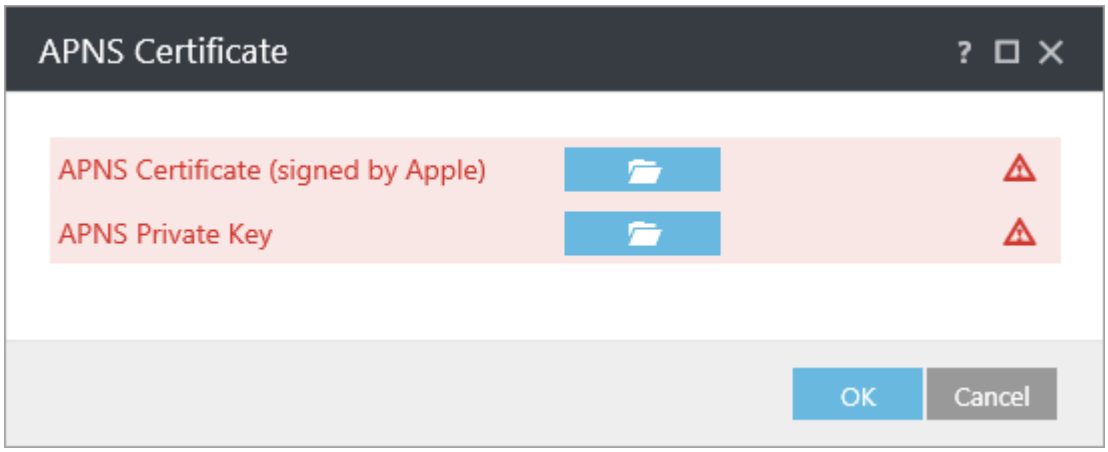


Odovzdajte certifikáty Apple pre registráciu zariadení iOS – prejdite do sekcie **Apple Push Notification Service** a odovzdajte **APNS certifikát** a **APNS privátny kľúč**.



APNS certifikát (podpísaný spoločnosťou Apple) – kliknite na ikonu priečinka a vyberte cestu k APNS certifikátu. APNS certifikát je súbor, ktorý ste stiahli z portálu Apple Push Certificates Portal.

APNS privátny kľúč – kliknite na ikonu priečinka a vyberte cestu k APNS privátnemu kľúču. APNS privátny kľúč je súbor, ktorý ste stiahli pri vytváraní APN/DEP certifikátu.



Program zlepšovania produktov – môžete zapnúť alebo vypnúť odosielanie správ o zlyhaní programu a anonymných telemetrických údajov do spoločnosti ESET.

Zapisovanie do protokolov – môžete nastaviť úroveň podrobnosti protokolov, čím určíte úroveň informácií, ktoré budú zhromažďované a zapisované do protokolov – od úrovne **Sledovanie** (informačné) až po **Závažné** (najdôležitejšie, kritické informácie).

Ak vytvárate túto politiku pre registráciu zariadení iOS prostredníctvom programu Apple DEP, prejdite do sekcie **Program registrácie zariadení Apple (DEP)**.

Program registrácie zariadení Apple (DEP) – tieto nastavenia sa týkajú len programu Apple DEP a zariadení iOS registrovaných cez tento program. DEP

Upozornenie:
Ak po počiatočnej konfigurácii dôjde k zmene v niektorom z týchto nastavení, bude potrebné obnoviť výrobné nastavenia a znova zaregistrovať všetky dotknuté zariadenia iOS, aby sa prejavili vykonané zmeny.

Nahrať autorizačný token – kliknite na ikonu priečinka a vyberte cestu k Apple DEP tokenu. DEP token je súbor, ktorý ste stiahli pri vytváraní virtuálneho MDM Servera na Apple DEP portáli.

Povinná inštalácia – používateľ nebude môcť používať zariadenie bez nainštalovania MDM profilu.

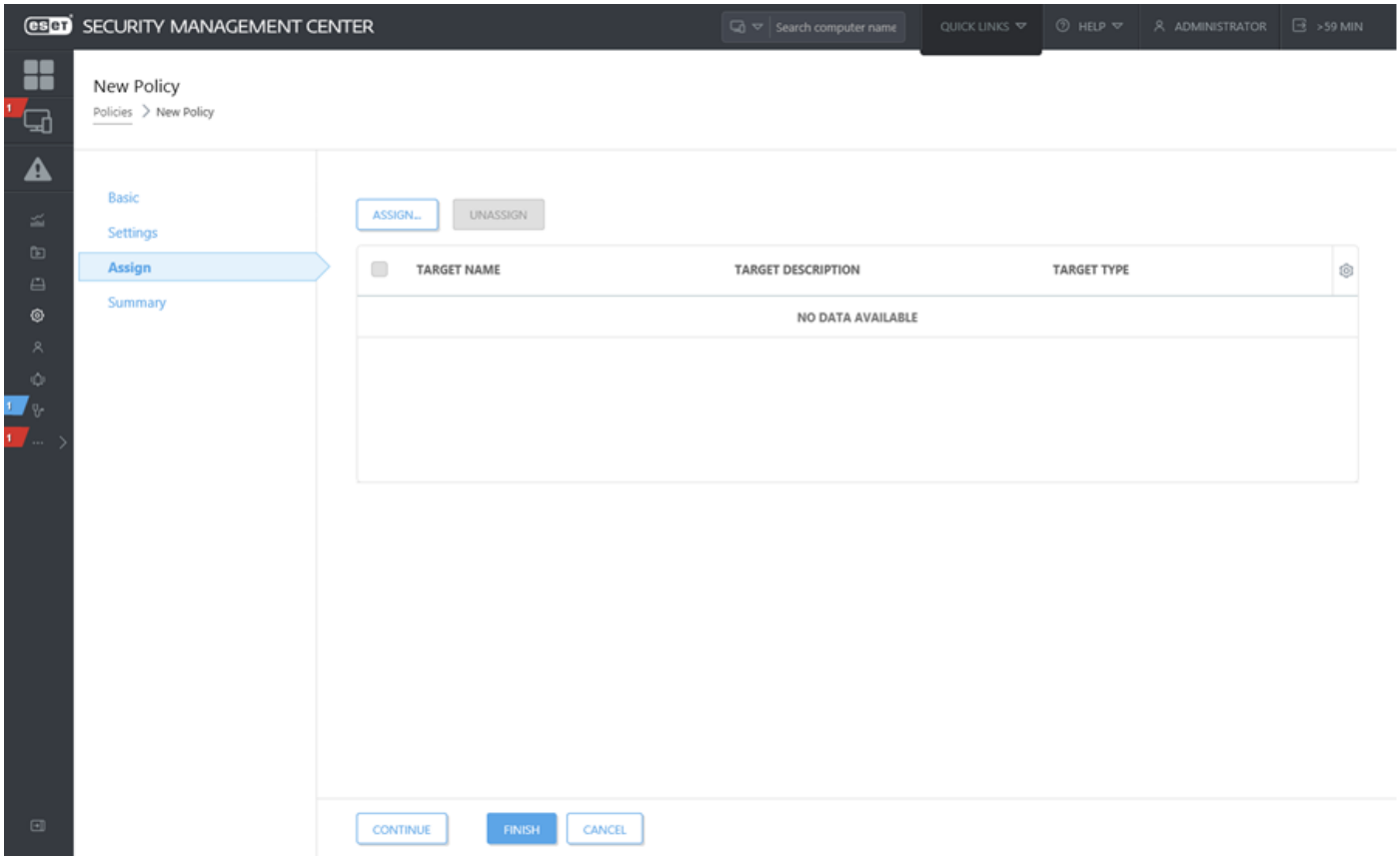
Povoliť odstránenie MDM profilu používateľom – zariadenie musí byť v režime pod dozorom, aby bolo možné zabrániť používateľovi v odstránení MDM profilu.

Vyžadovať prihlásenie do domény – od používateľa sa bude v sprievodcovi inštaláciou zariadenia vyžadovať zadanie platných prihlasovacích údajov do domény.

Preskočiť položky inštalácie – toto nastavenie vám umožňuje zvoliť, ktoré kroky počiatočnej konfigurácie zariadenia iOS budú preskočené. Podrobné informácie o jednotlivých krokoch počiatočnej konfigurácie zariadenia iOS nájdete v tomto článku Databázy znalostí spoločnosti Apple.

Priradiť

Vyberte zariadenie, na ktorom je spustený MDM server, pre ktorý je daná politika určená.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte inštanciu nástroja Mobile Device Connector, na ktorú chcete politiku aplikovať, a kliknite na **OK**.

Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

5.3.3 Vytvorenie politiky pre obmedzenie iOS zariadení a nastavenie Wi-Fi

Môžete vytvoriť politiku pre iOS mobilné zariadenia na účely vynútenia určitých obmedzení. Môžete tiež zadefinovať viacero Wi-Fi pripojení, aby sa napr. používatelia mohli automaticky pripájať na podnikovú Wi-Fi sieť z rôznych pobočiek. To isté platí pre VPN pripojenia.

Obmedzenia, ktoré môžete aplikovať na iOS mobilné zariadenie, sú uvedené v kategóriách. Napríklad, môžete zakázať FaceTime a používanie kamery, ako aj určité funkcie služby iCloud, prípadne vyladiť nastavenia bezpečnosti a súkromia alebo zakázať určité aplikácie.

Poznámka:
Obmedzenia, ktoré môžu alebo nemôžu byť aplikované, závisia od verzie systému iOS používaného klientskymi zariadeniami. Podporovaný je iOS 8.x a novšie.

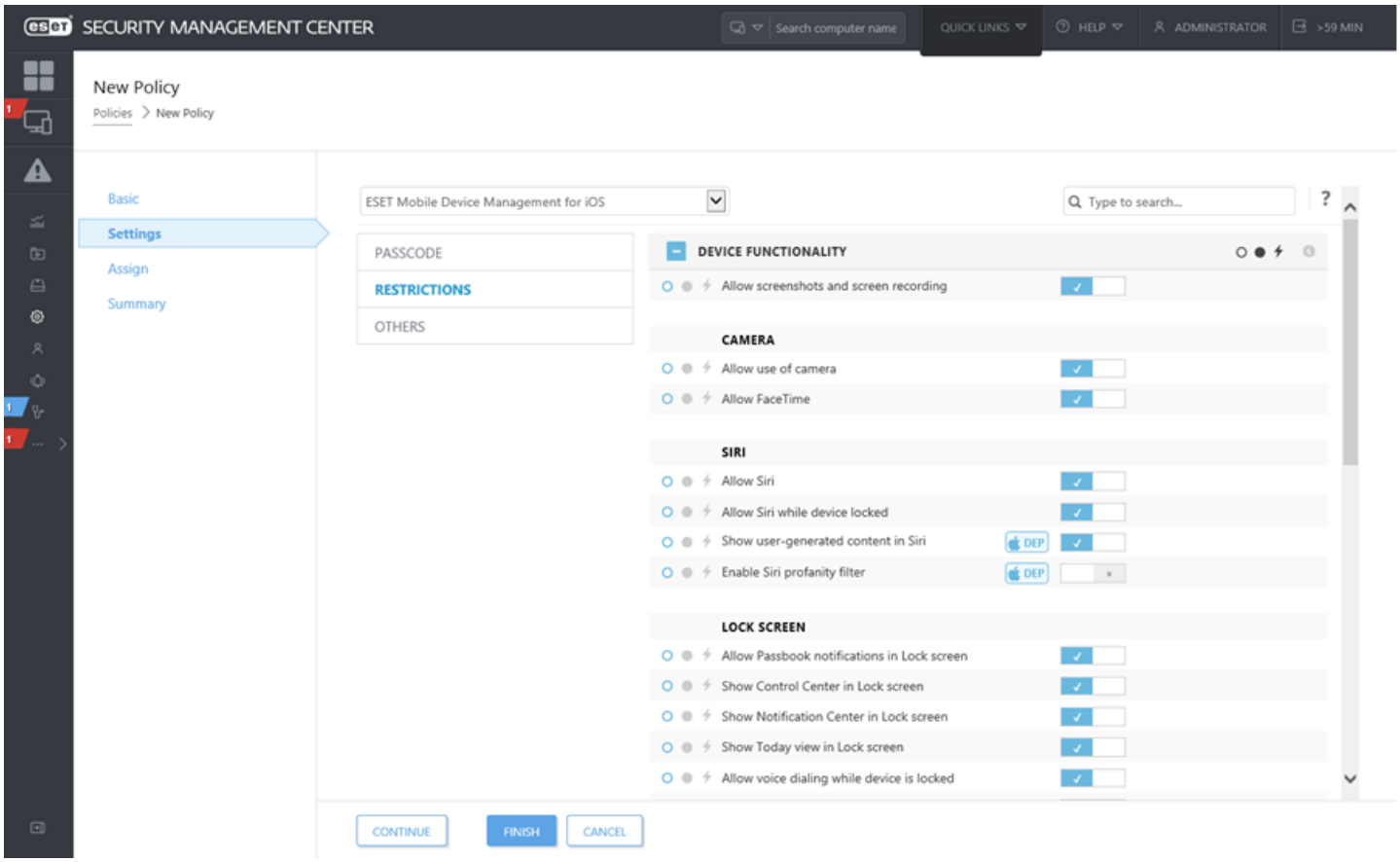
Nasleduje príklad, ktorý vysvetľuje, ako zakázať **fotoaparát** a **FaceTime** a pridať do zoznamu podrobnosti o Wi-Fi pripojení, aby sa iOS mobilné zariadenie pripájalo na Wi-Fi sieť vždy, keď je daná sieť nájdená. Ak použijete funkciu automatického pripojenia, iOS mobilné zariadenia sa predvolene pripoja na túto sieť. Toto nastavenie politiky prepíše manuálny výber Wi-Fi siete používateľa, pretože politika je vždy nadradená nastaveniam používateľa.

Základné

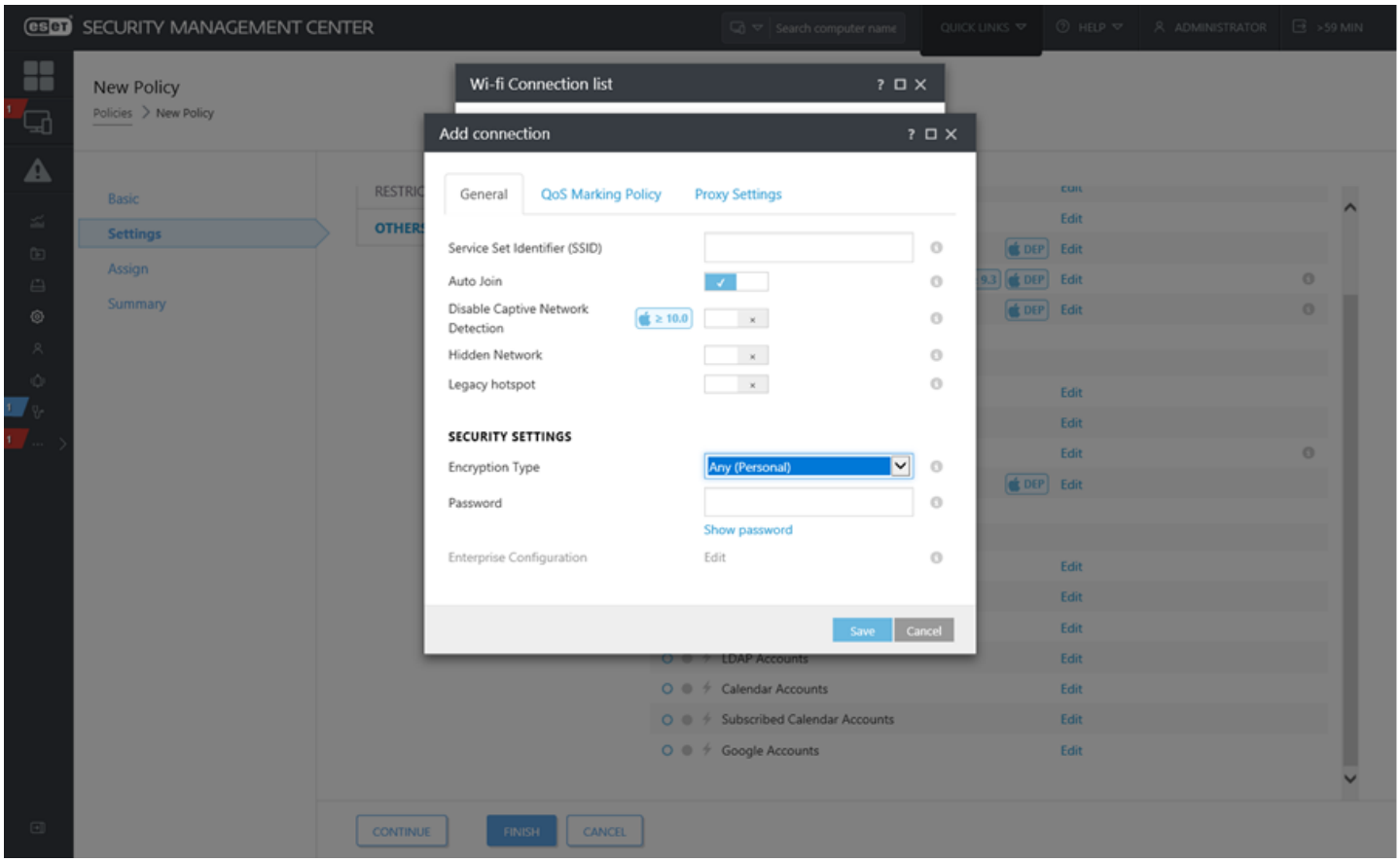
Zadajte **Názov** politiky. Pole **Popis** je voliteľné.

Nastavenia

Vyberte možnosť **ESET Mobile Device Management pre iOS** a kliknite na **Obmedzenia** pre zobrazenie kategórií. Použite tlačidlo prepínača vedľa položky **Povoliť používanie fotoaparátu**, čím zakážete používanie fotoaparátu. Keďže je teraz fotoaparát zakázaný, FaceTime bude takisto automaticky zakázaný. Ak si želáte zakázať iba aplikáciu FaceTime, nechajte fotoaparát povolený a použite tlačidlo vypínača vedľa položky **Povoliť FaceTime**.



Po nastavení **Obmedzení** kliknite na **Iné** a potom na **Upraviť** vedľa položky **Zoznam Wi-Fi pripojení**. Otvorí sa okno so zoznamom Wi-Fi pripojení. Kliknite na **Pridať** a upresnite podrobnosti pripojenia pre Wi-Fi sieť, ktorú chcete pridať. Kliknite na **Save**.



- **Service Set Identifier (SSID)** – SSID vašej Wi-Fi siete.
- **Automatické pripojenie sa** – voliteľné (prednastavene povolené), zariadenie sa automaticky pripojí na túto sieť.

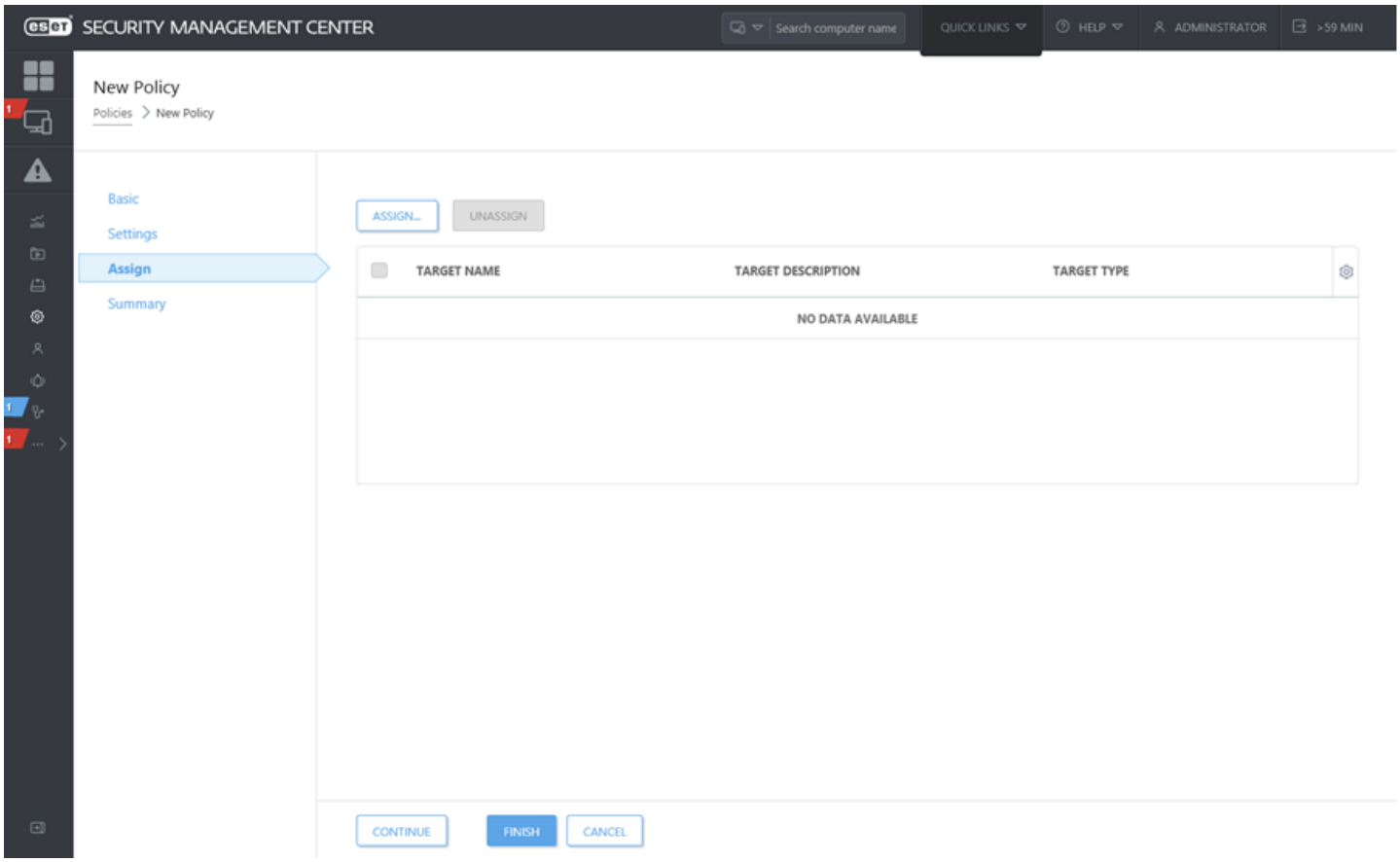
Bezpečnostné nastavenia:

- **Typ šifrovania** – vyberte si vhodný typ šifrovania z roletového menu a uistite sa, že táto hodnota presne zodpovedá možnostiam danej Wi-Fi siete.
- **Používateľské heslo** – zadajte heslo, ktoré bude použité na overovanie pri pripájaní sa k Wi-Fi sieti.

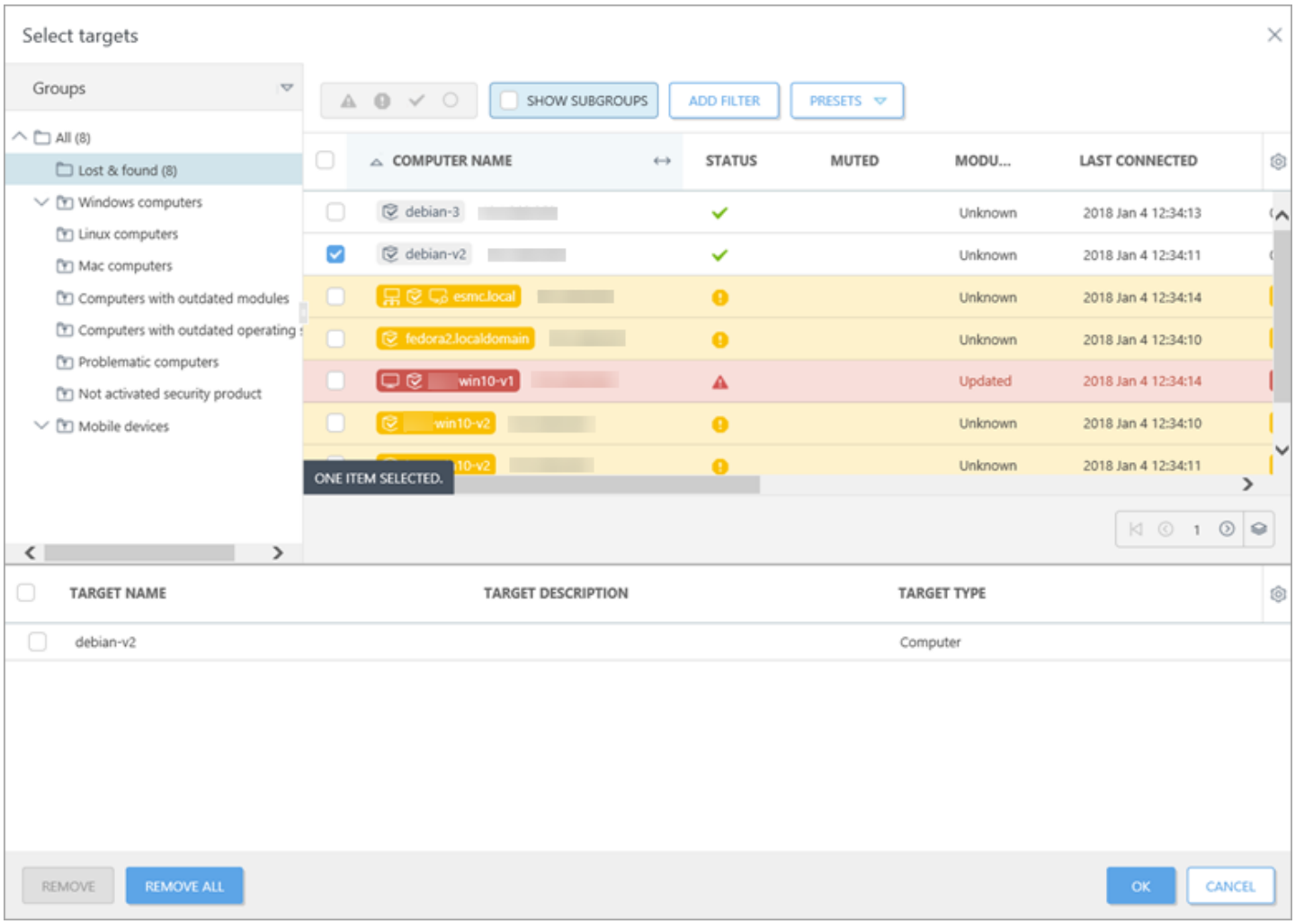
Nastavenia proxy – voliteľné. Ak vaša sieť využíva proxy, zadajte príslušné hodnoty.

Priradiť

Zvoľte klientov (individuálne počítače/mobilné zariadenia alebo celé skupiny), ku ktorým bude priradená daná politika.



Kliknite na **Priradiť** pre zobrazenie všetkých statických a dynamických skupín vrátane zariadení, ktoré do týchto skupín patria. Vyberte požadované klientske zariadenia a kliknite na **OK**.



Súhrn

Skontrolujte nastavenia danej politiky a kliknite na **Dokončiť**.

5.3.3.1 MDM konfiguračné profily

Môžete nastaviť profil, ktorý bude slúžiť na aplikovanie politík a obmedzení na spravované mobilné zariadenia.

Názov profilu	Krátky popis
Prístupový kód	Od koncových používateľov sa vyžaduje, aby chránili svoje zariadenia prístupovými kódmi vždy, keď sa zariadenia vrátia zo stavu nečinnosti do aktívneho režimu. Týmto sa zaručí, že všetky citlivé podnikové informácie budú na spravovaných zariadeniach chránené. Ak na jednom zariadení vynútia zadanie prístupových kódov viaceré profily, bude uplatnená najprísnejšia politika.
Obmedzenia	Profily obmedzení obmedzujú funkcie dostupné pre používateľov spravovaných zaradení tým, že obmedzujú určité povolenia týkajúce sa funkčnosti zariadenia, aplikácií, služby iCloud, bezpečnosti a súkromia.
Zoznam Wi-Fi pripojení	Wi-Fi profily odosielajú podnikové Wi-Fi nastavenia priamo na spravované zariadenia pre získanie okamžitého prístupu.
Zoznam VPN pripojení	VPN profily odosielajú podnikové nastavenia virtuálnej súkromnej siete na podnikové zariadenia, aby mali používatelia bezpečný prístup do podnikovej infraštruktúry zo vzdialených lokalít. **Názov pripojenia** – zobrazenie názvu pripojenia zobrazeného na zariadení. **Typ pripojenia** – vyberte typ pripojenia povoleného týmto profilom. Každý typ pripojenia ponúka rôzne možnosti. **Server** – zadajte názov hostiteľa alebo IP adresu servera, na ktorý sa pripájate.
Poštové účty	Táto funkcia umožňuje správcovi nastaviť IMAP/POP3 e-mailové účty.
Exchange ActiveSync účty	Exchange ActiveSync profily poskytujú koncovým používateľom prístup do podnikovej e-mailovej infraštruktúry založenej na báze „push“ (doručenie bez vyžiadania). Berte, prosím, na vedomie, že sa tam nachádzajú predvyplnené polia hľadaných hodnôt a možnosti, ktoré sa vzťahujú len na iOS 5+.
CalDAV – Kalendárové účty	CalDAV ponúka možnosti konfigurácie, ktorej cieľom je umožniť používateľom bezdrôtovú synchronizáciu s podnikovým CalDAV serverom.
CardDAV – Kontaktové účty	Táto časť umožňuje špecifickú konfiguráciu služieb CardDAV.
Odoberané kalendárové účty	Možnosť odoberania kalendárov umožňuje aj konfiguráciu kalendára.

5.4 Riešenie problémov s MDM

1. Čo mám robiť, keď sa mi zobrazilo chybové hlásenie: „Registračný token sa už používa alebo nie je platný.“?

Pravdepodobne sa pokúšate zariadenie zaregistrovať so starým registračným tokenom. Vygenerujte nový token pre opätovnú registráciu prostredníctvom Web Console a použite ho namiesto starého tokenu. Je tiež možné, že medzi predchádzajúcim pokusom o opätovnú registráciu a aktuálnym pokusom uplynulo príliš krátke časové obdobie. Skontrolujte, či sa váš aktuálny token pre opätovnú registráciu líši od tokenu, ktorý bol vygenerovaný pri predchádzajúcom pokuse. Ak tomu tak nie je, počkajte pár minút a pokúste sa vygenerovať nový token pre opätovnú registráciu.

2. Čo mám robiť, keď sa mi zobrazilo chybové hlásenie: „Overenie certifikátu služby zlyhalo.“?

Toto chybové hlásenie signalizuje, že ide o problém s vaším certifikátom služby APNS alebo GCM. Informácia o tomto probléme sa zobrazuje v ESMC Web Console ako jedno z nasledujúcich upozornení v rámci MDM Core výstrah:

- **Overenie certifikátu služby GCM zlyhalo** (0x0000000100001002)
- **Overenie certifikátu služby APNS zlyhalo** (0x0000000100001000)
- **Overenie certifikátu služby spätnej väzby APNS zlyhalo** (0x0000000100001004)

Uistite sa, že máte na vašom systéme dostupnú správnu certifikačnú autoritu:

- Certifikačná autorita služby APNS: **Entrust Certification Authority**, je potrebné overiť certifikát z gateway.push.apple.com:2195;
- Certifikačná autorita služby spätnej väzby APNS: **Entrust Certification Authority**, je potrebné overiť certifikát z feedback.push.apple.com:2196;
- Certifikačná autorita služby GCM: **GeoTrust Global CA**, je potrebné overiť certifikát z android.googleapis.com:443.

Požadovaná certifikačná autorita by mala byť obsiahnutá v úložisku certifikátov na MDM hostiteľskom počítači. Na systéme Windows môžete vyhľadať výraz „spravovať dôveryhodné koreňové certifikáty“. Na systéme Linux je umiestnenie certifikátov závislé od distribúcie, ktorú používate. Niektoré príklady cieľových umiestnení úložiska certifikátov:

- na systémoch Debian a CentOS: */usr/lib/ssl/cert.pem*, */usr/lib/ssl/certs*,
- na systéme Red Hat: */usr/share/ssl/cert.pem*, */usr/share/ssl/certs*,
- príkaz `openssl version -d` zvyčajne vráti požadovanú cestu.

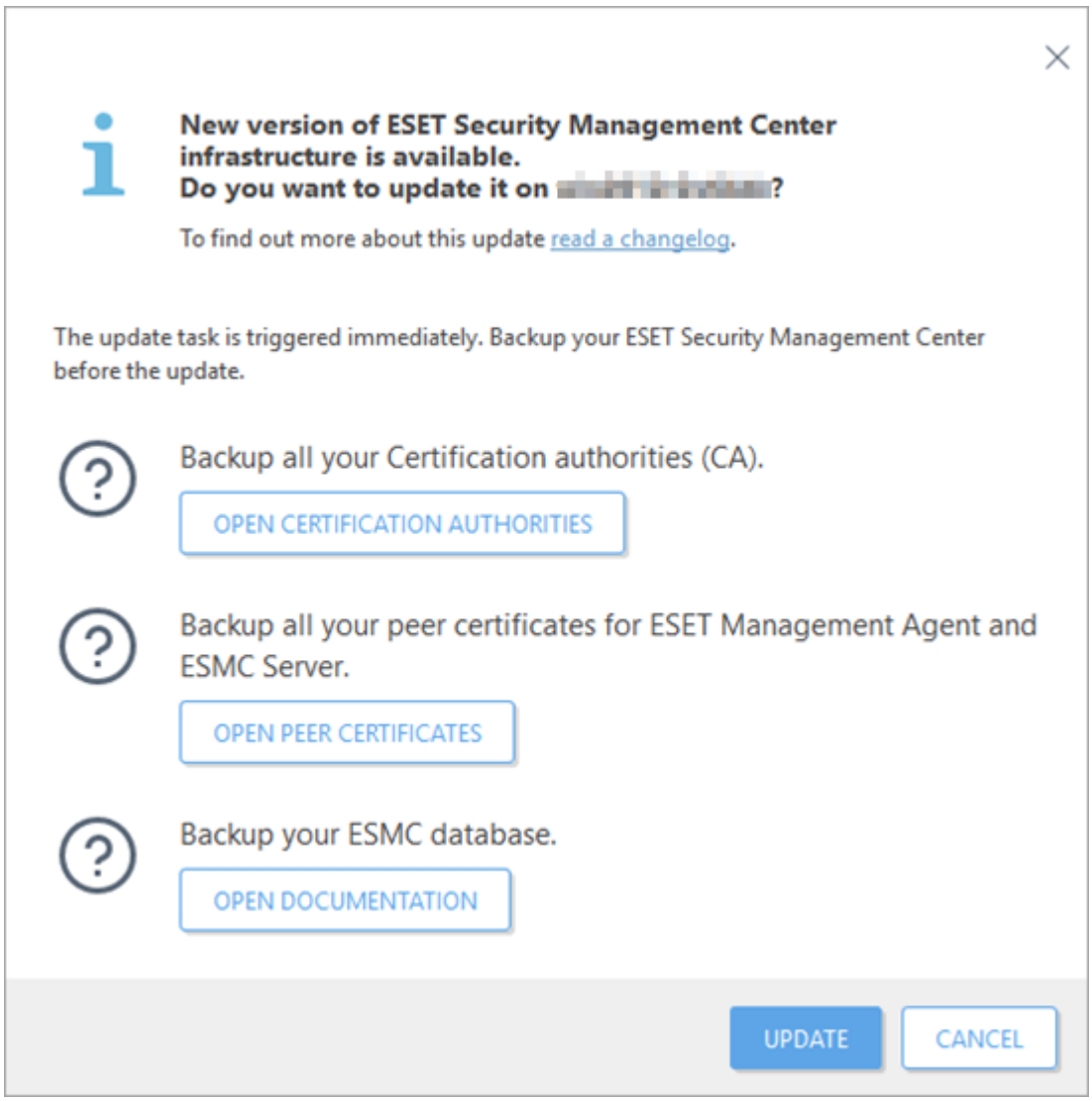
V prípade, že požadovaná certifikačná autorita nie je nainštalovaná na systéme, kde beží služba MDM Core, nainštalujte ju. Po vykonaní inštalácie reštartujte službu ESMC MDC.

Upozornenie:
Postupujte opatrne, pretože overenie certifikátu je bezpečnostná funkcia, čo znamená, že ak sa vo Web Console vyskytne upozornenie, mohlo by ísť aj o signalizovanie bezpečnostnej hrozby.

6. Aktualizácia ESMC

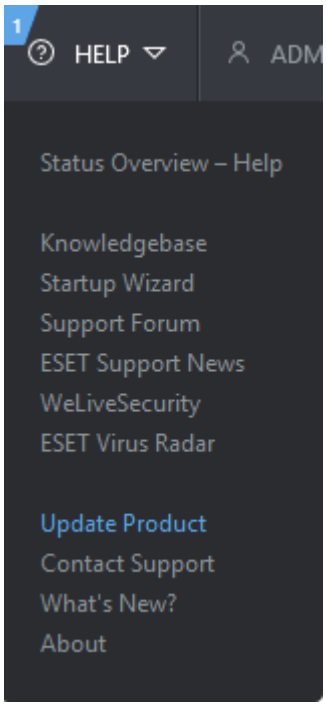
ESET Security Management Center Server pravidelne kontroluje dostupnosť aktualizácií infraštruktúry ESMC.

V prípade, že je dostupná aktualizácia, sa zobrazí nasledujúce okno:



O zmenách, ktoré sú súčasťou danej aktualizácie ESMC, sa dočítate v **protokole zmien**.

Ak sa rozhodnete nevykonať aktualizáciu, toto okno môžete znova zobraziť kliknutím na **Pomocník** > **Aktualizovať produkt**:



Poznámka:
Oznámenie o dostupnosti novej verzie sa zobrazí len tým používateľom, ktorí majú oprávnenie spúšťať úlohu pre klienta Aktualizácia súčastí Security Management Center.

1. Kliknite na **Otvoriť certifikačné autority** a zálohujte si všetky svoje certifikačné autority.
2. Kliknite na **Otvoriť partnerské certifikáty** a zálohujte si všetky svoje certifikáty.
3. Kliknite na **Otvoriť dokumentáciu** a zálohujte ESMC databázu.
4. Kliknite na tlačidlo **Aktualizovať**. Aktualizácia vášho ESMC Servera je naplánovaná – medzi úlohami pre klienta nájdete novú úlohu, ktorá vykonáva aktualizáciu komponentov ESMC na počítači, kde je nainštalovaný ESMC Server. Ak chcete na zariadeniach pripojených k ESMC Serveru aktualizovať na najnovšiu verziu ostatné komponenty ESMC, môžete spustiť úlohu **Aktualizácia súčastí Security Management Center** priamo z aktualizačného okna.

Poznámka:
Viac informácií nájdete v časti Aktualizácia súčastí.

7. Najčastejšie otázky

Zoznam otázok

Otázka: Ako vyriešim chybové hlásenie „Prihlásenie zlyhalo: Pripojenie zlyhalo so stavom **Nepripojený**“?

Odpoveď: Uistite sa, že služba ESMC Server (prípadne MS SQL Server) je spustená. Ak nie, spustite ju. Ak je spustená, reštartujte túto službu, obnovte stránku Web Console a skúste sa znova prihlásiť. Viac informácií nájdete v kapitole Riešenie problémov – Web Console.

Otázka: Na čo slúži skupina „**Stratené a nájdené**“?

Odpoveď: Počítače, ktoré sa pripájajú na ESMC Server, ale nie sú zaradené v žiadnej inej statickej skupine, sú automaticky zobrazené v skupine Stratené a nájdené. S touto skupinou a počítačmi v nej môžete pracovať tak, ako s ktoroukoľvek inou statickou skupinou. Túto skupinu je možné premenovať alebo presunúť do inej skupiny, avšak nie je možné ju odstrániť.

Otázka: Ako vytvorím dvojitý aktualizačný profil?

Odpoveď: Podrobné inštrukcie nájdete v našom článku databázy znalostí.

Otázka: Ako obnovím informácie na konkrétnej stránke alebo v sekcii bez toho, aby som obnovil celé okno/kartu prehliadača?

Odpoveď: Kliknite na možnosť **Obnoviť** v kontextovom menu v pravom hornom rohu danej sekcie stránky.

Otázka: Ako spustiť tichú inštaláciu ESET Management Agenta?

Odpoveď: Pomocou nasledujúcich metód môžete vykonať tichú inštaláciu:

- GPO – spúšťací skript
- Úloha nasadenia agenta
- Nástroj na nasadenie (Deployment Tool)

Otázka: RD Sensor nedetegoval všetky klientske zariadenia v sieti.

Odpoveď: RD Sensor načúva v sieti pasívne. Ak počítač nekomunikuje, nemôže byť zachytený pomocou nástroja RD Sensor. Skontrolujte nastavenia DNS a uistite sa, že nenastala chyba v DNS lookup, ktorá by bránila komunikácii.

Otázka: Ako vynulujem počet aktívnych hrozieb zobrazených v ESMC po vykonaní liečenia hrozieb?

Odpoveď: Pre vynulovanie počtu aktívnych hrozieb je potrebné cez ESMC na cieľovom počítači spustiť hĺbkovú kontrolu. Ak ste liečenie hrozby vykonali manuálne, môžete výstrahu aktívnej hrozby potlačiť.

Otázka: Je možné pre interval pripojenia ESET Management Agenta k ESMC Serveru použiť CRON výraz?

Odpoveď: Áno, parameter P_REPLICATION_INTERVAL prijíma hodnoty zadefinované prostredníctvom CRON výrazu.

Štandardný výraz „R R/20 * * * ? *“ znamená pripájanie v náhodnej sekunde (R=0-60) každých 20 minút (napríklad 3, 23, 43 alebo 17,37,57). Použitie náhodných hodnôt zabezpečí vyvažovanie záťaže, keďže sa každý ESET Management Agent bude pripájať na server v rozdielnom čase. Ak je použitý presný CRON výraz, napríklad „0 * * * * ? *“, všetky agenty s týmto nastavením sa budú na server pripájať v rovnakom čase (každú minútu v čase :00), čo môže spôsobiť vyťaženie siete a serveru v danom čase. Viac informácií nájdete v kapitole CRON výraz.

Otázka: Ako vytvorím novú dynamickú skupinu pre automatické nasadenie?

Odpoveď: Podrobné inštrukcie nájdete v našom článku databázy znalostí.

Otázka: Aký je formát súboru pre importovanie zoznamu počítačov do ESMC?

Odpoveď: Súbor musí obsahovať riadky v nasledujúcej podobe:

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX
All (Všetko) je požadovaný názov koreňovej skupiny.

Otázka: Ktoré certifikáty tretích strán môžu byť použité na podpísanie ESMC certifikátov?

Odpoveď: Na podpísanie certifikátov možno použiť len certifikačné autority (alebo sprostredkujúce certifikačné autority) s kľúčovým príznakom ‚keyCertSign‘ a obmedzením ‚keyUsage‘. To znamená, že s nimi možno podpísať iné certifikáty.

Otázka: Ako **vynulujem heslo správcu** pre Web Console (heslo zadané pri počiatočnom nastavení na operačnom systéme Windows)?

Odpoveď: Zmena tohto hesla je možná pri opätovnom spustení inštalátora a zvolení možnosti **Opraviť**. Môže byť vyžadované aj heslo k ESMC databáze, ak ste nepoužili Windows Authentication pri vytvorení databázy. Viac informácií nájdete v tomto článku databázy znalostí.

Poznámka:
Pri vykonávaní opráv je potrebné zvýšiť pozornosť, pretože niektoré opravy môžu viesť k vymazaniu uložených údajov.

Otázka: Ako **vynulujem heslo správcu** pre Web Console (heslo zadané pri počiatočnom nastavení na operačnom systéme Linux)?

Odpoveď: Ak je v ESMC ďalší používateľský účet s dostatočnými oprávneniami, mali by ste byť schopný cez tento účet vynulovať a znovu nastaviť heslo správcovského účtu. Ak je správcovský účet jediným účtom v systéme (ako je to po inštalácii), heslo nie je možné vynulovať.

- Budete musieť preinštalovať ESMC, vyhľadať v databáze záznam pre účet správcu a následne tento záznam upraviť. Vo všeobecnosti je najvhodnejšie zálohovať si prihlasovacie údaje k správcovskému účtu „Administrator“ na bezpečnom mieste a vytvoriť si ďalšie účty s oprávneniami správcu. Správcovský účet „Administrator“ by mal byť používaný výhradne na vytvorenie a správu ďalších používateľských účtov pre individuálnych správcov.
- Viac informácií nájdete v tomto článku databázy znalostí.

Otázka: Ako postupovať v prípade, že nástroj **RD Sensor** nedeteguje žiadne zariadenia v sieti?

Odpoveď: Ak je váš operačný systém zachytený ako sieťové zariadenie, nástroj RD Sensor ho nenahlási do ESMC ako počítač. Sieťové zariadenia (tlačiareň, router) sú odfiltrované. Nástroj RD Sensor bol kompilovaný s knižnicou *libpcap vo verzii 1.3.0*. Uistite sa, že je táto verzia nainštalovaná na vašom počítači. Ak je RD Sensor nainštalovaný na virtuálnom počítači, je nutné sieťový adaptér nastaviť do režimu Bridged. Ak sú tieto požiadavky splnené a chyba pretrváva, spustite nástroj nmap na detegovanie operačných systémov (http://nmap.org/book/osdetect-usage.html), aby ste zistili, či je možné detegovať operačný systém na vašom počítači.

Otázka: Prečo sa v sekcii Šablóny dynamických skupín nezobrazujú žiadne položky?

Odpoveď: Daný používateľ pravdepodobne nemá pridelené príslušné povolenia. Používatelia môžu šablóny vidieť len v prípade, že sú zahrnuté v statickej skupine, v ktorej má používateľ pridelené povolenia aspoň na **čítanie** pre Šablóny dynamických skupín.

Otázka: Prečo sa v sekcii Riadiaci panel nezobrazujú žiadne informácie?

Odpoveď: Daný používateľ pravdepodobne nemá pridelené príslušné povolenia. Používateľovi sa informácie v sekcii Riadiaci panel zobrazia len za predpokladu, že mu boli pridelené povolenia na prístup k Počítačom a k Riadiacemu panelu. Pozrite si tento príklad vytvorenia a pridelenia sady povolení.

Otázka: Ako môžem aktualizovať svoj bezpečnostný produkt ESET?

Odpoveď: Na aktualizáciu bezpečnostných produktov ESET je potrebné použiť úlohu Inštalácia softvéru a vybrať produkt, ktorý bude aktualizovaný.

8. O programe ESET Security Management Center

Okno **O programe** otvoríte kliknutím na **Pomocník** > **O programe**. V tomto okne nájdete podrobné informácie o nainštalovanej verzii programu ESET Security Management Center, ako aj zoznam nainštalovaných modulov programu. Vrchná časť okna obsahuje informácie o operačnom systéme a systémových prostriedkoch. Je tu tiež zobrazená licencia používaná na sťahovanie aktualizácií modulov ESMC (licencia, ktorá bola použitá na aktiváciu ESMC). Informácie o vašej databáze, ako napr. názov, verzia, veľkosť, hostiteľský názov a používateľ, sú zobrazené v tomto okne.

POZNÁMKA:

Ak chcete zistiť, akú verziu má konkrétny ESMC komponent, postupujte podľa inštrukcií v našom článku databázy znalostí.