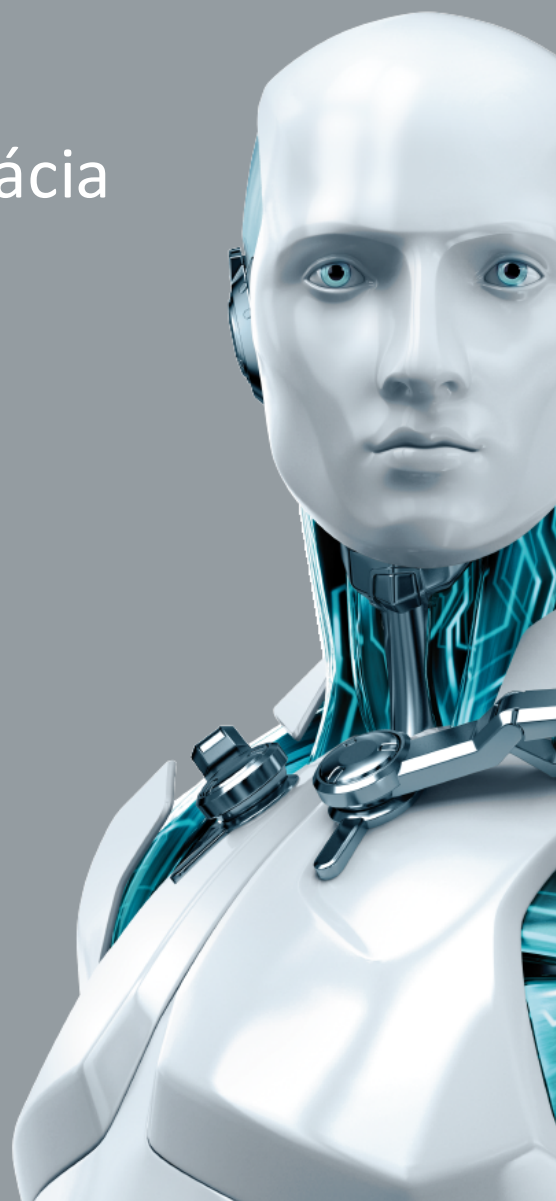




SECURITY MANAGEMENT CENTER

Inštalácia, aktualizácia a migrácia

[Pre stiahnutie najnovšej verzie tohto dokumentu kliknite sem](#)



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 reprodukováná 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

1. O tejto príručke	6
2. Inštalácia/aktualizácia	8
2.1 Nové funkcie	9
2.2 Architektúra	10
2.2.1 Server	11
2.2.2 Web Console	12
2.2.3 Agent	12
2.2.4 Proxy	13
2.2.5 Rogue Detection Sensor	15
2.2.6 Mobile Device Connector	17
2.2.7 Apache HTTP Proxy	18
2.3 Scenáre nasadenia – najvhodnejšie postupy	21
2.3.1 Praktické príklady nasadenia (Windows)	22
2.3.2 Nasadenie vo veľkých podnikoch (200 000 klientov)	24
2.3.3 Rozdiely medzi Apache HTTP Proxy, nástrojom Mirror Tool a priamym pripojením na internet	25
2.3.3.1 Kedy sa oplatí používať Apache HTTP Proxy?	26
2.3.3.2 Kedy sa oplatí používať Mirror Tool?	27
2.4 Škálovateľnosť ESMC infraštruktúry	27
2.5 Čo je nové v nástroji ESET Security Management Center 7.0	31
3. Systémové požiadavky	33
3.1 Podporované operačné systémy	33
3.1.1 Windows	33
3.1.2 Linux	35
3.1.3 macOS	36
3.1.4 Mobilné zariadenia	36
3.2 Podporované Desktop Provisioning prostredia	37
3.3 Hardvér	37
3.4 Databáza	38
3.5 Podporované verzie Apache Tomcat	38
3.6 Sieť	39
3.6.1 Používané porty	39
4. Inštalácia	41
4.1 All-in-one inštalácia na systéme Windows	42
4.1.1 Inštalácia ESMC Servera	43
4.1.2 Inštalácia komponentu ESMC Mobile Device Connector (samostatne)	53
4.1.3 Inštalácia ESMC na Windows SBS/Essentials	57
4.1.4 Odinštalovanie súčastí	60
4.2 Inštalácia na Microsoft Azure	61
4.3 Inštalácia súčastí na systéme Windows	62
4.3.1 Inštalácia servera	63
4.3.1.1 Prerekvizity servera – Windows	66
4.3.2 Požiadavky pre Microsoft SQL Server	67
4.3.3 Inštalácia a konfigurácia MySQL Servera	68
4.3.4 Vyhradený používateľský účet databázy	69
4.3.5 Inštalácia agenta	69
4.3.5.1 Serverom asistovaná inštalácia agenta	70
4.3.5.2 Offline inštalácia agenta	71

4.3.5.3	Odiňštalovanie agenta a riešenie problémov	71
4.3.5.4	Nástroj na nasadenie	72
4.3.5.4.1	Požiadavky pre nástroj na nasadenie	72
4.3.5.4.2	Výber počítačov z Active Directory	73
4.3.5.4.3	Vyhľadávanie počítačov v lokálnej sieti	75
4.3.5.4.4	Importovanie zoznamu počítačov	77
4.3.5.4.5	Manuálne pridanie počítačov	79
4.3.5.4.6	Riešenie problémov	81
4.3.6	Inštalácia Web Console – Windows	82
4.3.7	Inštalácia proxy	83
4.3.8	Inštalácia nástroja RD Sensor – Windows	84
4.3.8.1	Prerekvizity pre RD Sensor	84
4.3.9	Mirror Tool	84
4.3.10	Inštalácia komponentu Mobile Device Connector	87
4.3.10.1	Prerekvizity pre Mobile Device Connector	90
4.3.10.2	Aktivácia komponentu Mobile Device Connector	92
4.3.10.3	MDM funkcia licencovania iOS zariadení	92
4.3.10.4	Požiadavky HTTPS certifikátu	92
4.3.11	Apache HTTP Proxy – inštalácia a ukladanie do vyrovnávacej pamäte	93
4.3.12	Inštalácia Squid a vyrovnávacia pamäť HTTP Proxy	96
4.3.13	Offline repozitár	96
4.3.14	Failover klaster	98
4.4	Inštalácia súčastí na systéme Linux	99
4.4.1	Podrobná inštalácia ESMC Servera na systéme Linux	99
4.4.2	Inštalácia a konfigurácia MySQL	101
4.4.3	Inštalácia a konfigurácia ODBC ovládača	102
4.4.4	Inštalácia servera – Linux	103
4.4.4.1	Prerekvizity servera – Linux	106
4.4.5	Inštalácia agenta – Linux	108
4.4.5.1	Prerekvizity agenta – Linux	111
4.4.6	Inštalácia Web Console – Linux	111
4.4.6.1	Prerekvizity ESMC Web Console – Linux	112
4.4.7	Inštalácia proxy – Linux	113
4.4.8	Inštalácia nástroja RD Sensor a prerekvizity inštalácie – Linux	114
4.4.9	Inštalácia komponentu Mobile Device Connector – Linux	114
4.4.9.1	Prerekvizity pre Mobile Device Connector – Linux	116
4.4.10	Inštalácia Apache HTTP Proxy – Linux	117
4.4.11	Inštalácia Squid HTTP Proxy – Ubuntu Server	120
4.4.12	Mirror Tool	120
4.4.13	Failover klaster – Linux	123
4.4.14	Odiňštalovanie alebo preinštalovanie komponentu – Linux	125
4.5	Inštalácia súčastí na systéme macOS	126
4.5.1	Inštalácia agenta – macOS	126
4.6	Databáza	127
4.6.1	Záloha a obnova databázy	127
4.6.2	Aktualizácia databázového servera	128
4.7	Obraz ISO	129
4.8	DNS servisný záznam	129
4.9	Scenár offline inštalácie ESMC	130

5.	Aktualizácia, migrácia a preinštalovanie	132
-----------	---	------------

Obsah

5.1 Aktualizácia súčastí	132
5.1.1 Aktualizácia v rámci infraštruktúry s ERA 6.5 Proxy	136
5.2 Migrácia z ERA 5.x	138
5.2.1 Asistent migrácie	139
5.2.2 Nástroj na migráciu	148
5.2.2.1 Scenár migrácie 1	149
5.2.2.2 Scenár migrácie 2	153
5.2.2.3 Scenár migrácie 3	160
5.2.3 Migrácia z predchádzajúcej verzie na novú – Linux	165
5.2.4 Nastavenie HTTP Proxy	165
5.3 Migrácia na iný server	165
5.3.1 Čistá inštalácia – rovnaká IP adresa	166
5.3.2 Čistá inštalácia – odlišná IP adresa	167
5.3.3 Migrácia databázy – rovnaká IP adresa	168
5.3.4 Migrácia databázy – odlišná IP adresa	169
5.3.5 Odinštalovanie starého ESMC Servera	170
5.4 Migrácia ESMC databázy	170
5.4.1 Migračný proces pre MS SQL Server	171
5.4.2 Migračný proces pre MySQL Server	179
5.5 Migrácia MDM	180
5.6 Aktualizácia nástroja ERA nainštalovaného na Failover klastrí na systéme Windows	181
5.7 Aktualizácia Apache HTTP Proxy	181
5.7.1 Inštrukcie pre Windows (all-in-one inštalátor)	181
5.7.2 Inštrukcie pre Windows (manuálna aktualizácia)	183
5.8 Aktualizácia Apache Tomcat	184
5.8.1 Inštrukcie pre Windows (all-in-one inštalátor)	184
5.8.2 Inštrukcie pre Windows (manuálna aktualizácia)	186
5.8.3 Inštrukcie pre Linux	187
5.9 Zmena názvu hostiteľa alebo IP adresy ESMC Servera	188
5.10 Aktualizácia nástroja ERA nainštalovaného na Failover klastrí na systéme Linux	189
6. Riešenie problémov	190
6.1 Aktualizácia komponentov ESMC v offline prostredí	190
6.2 Najčastejšie problémy s inštaláciou	191
6.3 Protokoly	195
6.4 Diagnostický nástroj	196
6.5 Problémy po aktualizácii/migrácii ESMC Servera	198
6.6 Protokolovanie MSI	199
7. Prvé kroky a najvhodnejšie postupy	200
7.1 Otvorenie ESMC Web Console	200
7.2 Interval pripájania klientov	202
8. ESET Security Management Center API	203
9. Časté otázky	204

1. O tejto príručke

Táto inštalčná príručka bola napísaná, aby vám pomohla s inštaláciou a aktualizáciou nástroja ESET Security Management Center a zároveň poskytla potrebné inštrukcie týkajúce sa celého procesu.

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 ukázkový 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.
<i>Kurzíva</i>	Zástupné symboly pre údaje, ktoré máte poskytnúť. Napríklad, <i>file name</i> alebo <i>path</i> 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.

2. Inštalácia/aktualizácia

ESET Security Management Center (ESMC) je nástroj, ktorý vám umožňuje spravovať produkty spoločnosti ESET na klientských staniciach, serveroch a mobilných zariadeniach v zosieťovanom prostredí z jednej centrálnej lokality. ESET Security Management Center vám pomocou zabudovaného spravovania úloh umožňuje inštalovať bezpečnostné produkty spoločnosti ESET na vzdialené počítače a okamžite reagovať na nové problémy a hrozby.

ESET Security Management Center sám o sebe neposkytuje ochranu proti škodlivému kódu. Ochrana vášho prostredia závisí od bezpečnostných produktov spoločnosti ESET, napríklad: ESET Endpoint Security na pracovných staniciach a mobilných zariadeniach alebo ESET File Security pre Microsoft Windows Server nainštalovaný na serverových zariadeniach.

ESET Security Management Center je postavený na dvoch základných princípoch:

1. **Centralizovaný manažment** – celú sieť môžete konfigurovať, spravovať a sledovať z jedného miesta.
2. **Škálovateľnosť** – systém môže byť nasadený na malú sieť, ako aj na veľké siete vo veľkých podnikoch. ESET Security Management Center je navrhnutý tak, aby jednoducho zvládol rast infraštruktúry podnikovej siete.

ESET Security Management Center podporuje najnovšiu generáciu bezpečnostných produktov spoločnosti ESET a je kompatibilný aj s [predchádzajúcimi generáciami produktov](#).

! Dôležité:

Inštalácia/aktualizačná príručka popisuje mnoho spôsobov, ako nainštalovať ESET Security Management Center, a je určená najmä pre podnikových zákazníkov. Prečítajte si [príručku pre malé a stredné podniky](#), pokiaľ chcete nainštalovať ESET Security Management Center na platformu Windows a spravovať do 250 produktov od spoločnosti ESET, určených pre koncové zariadenia s operačným systémom Windows.

Pomocník k programu ESET Security Management Center obsahuje kompletný návod na inštaláciu a aktualizáciu:

- [Architektúra nástroja ESET Security Management Center](#)
- [Asistent migrácie](#)
- [Inštalácia](#)
- [ESET License Administrator](#)
- [Procesy nasadenia](#) a [nasadenie agenta pomocou GPO alebo SCCM](#)
- [Prvé kroky po inštalácii nástroja ESET Security Management Center](#)
- [Úlohy po inštalácii](#)
- [Príručka správcu](#)

2.1 Nové funkcie

Hlavné zmeny vo verzii 7.0:

- [Nový replikačný protokol pre ESET Management Agentu](#) – ESET Push Notification Service. Nový protokol umožňuje používať na preposielanie komunikácie služby proxy tretích strán, ako napr. [Apache HTTP Proxy](#).
- Podpora pre [VDI prostredia](#) – detekcia fungujúca na báze hardvérového odtlačku umožňuje rýchlo vyriešiť konflikty medzi klonovanými počítačmi.
- [Inventár hardvéru](#) – ESET Management Agent zozbiera informácie o hardvéri v rámci systémov Windows, macOS a Linux.
- Podpora pre nové produkty ESET:
 - [ESET Dynamic Threat Defense](#)
 - [ESET Enterprise Inspector](#)
 - Vylepšená ochrana pred ransomware ([Ransomware Shield](#)) v rámci produktov pre koncové zariadenia od verzie 7
- Výrazne prepracované rozhranie [Web Console](#):
 - Nová hlavná ponuka, prehľadnejšie používateľské rozhranie, nové ikony, prepracovaná sekcia rýchlych odkazov a sekcia odkazov na Online pomocníka.
 - Proaktívne oznámenia v prípade dostupnosti [novej verzie ESMC Servera](#).
 - Nový [riadiaci panel Prehľad](#) s rýchlou navigáciou jediným kliknutím a integráciou s informačným kanálom RSS (novinky z portálu WeLiveSecurity a novinky ohľadom produktov ESET).
 - Nový [riadiaci panel Prehľad incidentov](#) s rýchlou navigáciou k jednotlivým hrozbám.
 - ESET Endpoint Encryption (Deslock) a [Safetica](#) sú teraz hlásené ako produkty ESET. Safetica agent môže byť nasadený pomocou ESMC repozitára.
 - Položky sprievodcu majú nové rozloženie.
 - Vylepšené možnosti filtrovania v sekcii [Počítače](#).
 - Vylepšený sprievodca pre [odstránenie zariadení zo správy](#).
 - Nová obrazovka [Nasadiť agenta](#) s jednoduchým prehľadom možností nasadenia.
 - [All-in-one inštalátor](#) vám teraz umožňuje pri vytváraní nového inštalačného balíka vybrať možnosť **Iba agent**.
 - Nová funkcia [Zobraziť podrobnosti](#) zobrazuje informácie o dynamických skupinách a podrobnosti o hardvéri zariadenia.
 - Jediným kliknutím je teraz možné vykonať množstvo rôznych akcií a adresovať rôzne záležitosti, ako je aktivácia, reštart, aktualizácia operačného systému a problémy s ochranou.
 - Boli zavedené nové [interaktívne otázky](#) (modré príznaky) súvisiace s potenciálnymi problémami s klonovaním/duplikáciou/zmenou hardvéru.
 - Vylepšená správa hrozieb:
 - spracované hrozby sú automaticky označené ako vyriešené,
 - k dispozícii je kontrola pomocou jediného kliknutia s možnosťou liečenia,
 - hrozbu je možné pridať do politiky ako výnimku,
 - vylepšené filtrovanie hrozieb,
 - možnosť manuálneho [odoslania súboru do ESET Dynamic Threat Defense](#).
 - Nové rozloženie pre [správy](#) s možnosťou generovania správ jediným kliknutím, nové kategórie šablón správ pre ESET Enterprise Inspector, ESET Dynamic Threat Defense, [inventár hardvéru](#) a detekciu klonovania.
 - Dve nové úlohy pre klienta – [Diagnostika](#) a [Odoslať súbor do EDTD](#).
 - [Politiky](#) umožňujú povoliť vytváranie vlastných [lokálnych zoznamov](#) (lokálne konfigurované výnimky/pravidlá pre politiky).
 - Možnosť [synchronizácie používateľov](#) priamo cez Active Directory.
 - Prepracované [oznámenia](#) s novými predvolenými šablónami oznámení a možnosťou upraviť viacero oznámení súčasne. Oznámenia môžu byť vytvorené pre nové typy udalostí s pokročilými možnosťami filtrovania.
 - **Viac > Odoslané súbory** – nová sekcia s podrobnosťami o súboroch, ktoré boli odoslané do systémov ESET LiveGrid® a ESET Dynamic Threat Defense.
 - Podpora pre [licencie platené formou predplatného](#), lepšie popisy zobrazujúce aktuálne využitie licencie, prepracovaný sprievodca pre **pridanie licencie** s podporou pre [ESET Business Account](#) a aktivácia produktu jediným kliknutím.
 - Možnosť definovať [čistenie databázy](#) pre rôzne typy protokolov v časti **Viac > Nastavenia servera**.

- [Mobile Device Connector](#) je robustnejší a bezpečnejší.

2.2 Architektúra

ESET Security Management Center predstavuje novú generáciu nástroja vzdialenej správy, ktorá je výrazne odlišná od predchádzajúcich verzií. Keďže je architektúra úplne odlišná, nástroj ESET Security Management Center 7 je len čiastočne kompatibilný s ERA 6, pričom neexistuje spätná kompatibilita s ERA 5. Kompatibilita s predošlými verziami [bezpečnostných produktov spoločnosti ESET](#) je však zachovaná.

Spolu s novým nástrojom ESET Security Management Center vyvinula spoločnosť ESET aj novú generáciu bezpečnostných produktov s novým licenčným systémom.

Pre nasadenie bezpečnostných produktov spoločnosti ESET musia byť nainštalované nasledujúce komponenty (na platformách Linux a Windows):

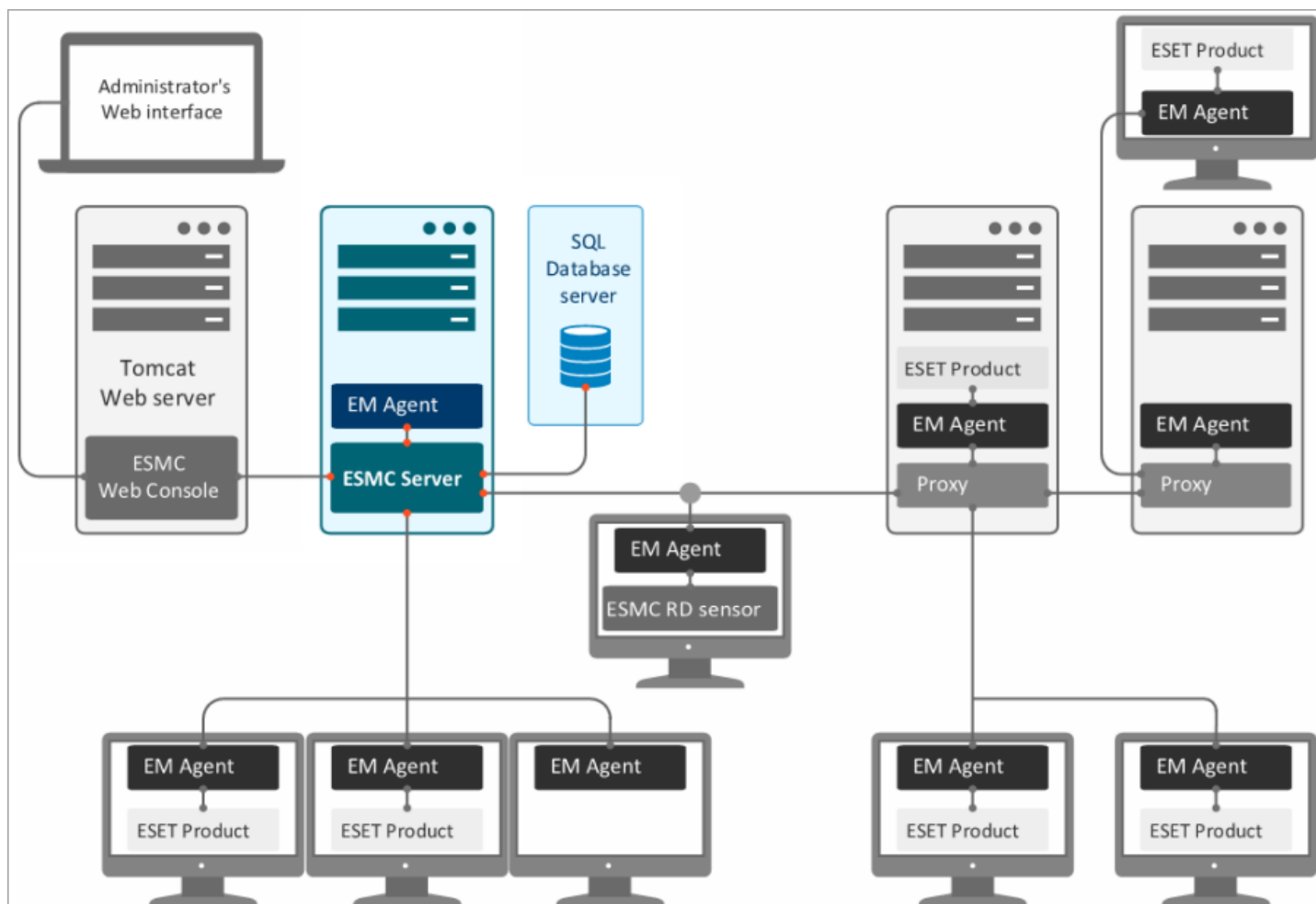
- [ESMC Server](#)
- [ESMC Web Console](#)
- [ESET Management Agent](#)

Nasledujúce komponenty sú voliteľné, avšak vo väčších sieťach odporúčame ich inštaláciu pre dosiahnutie maximálneho výkonu:

- [Proxy](#)
- [RD Sensor](#)
- [Apache HTTP Proxy](#)
- [Mobile Device Connector](#)

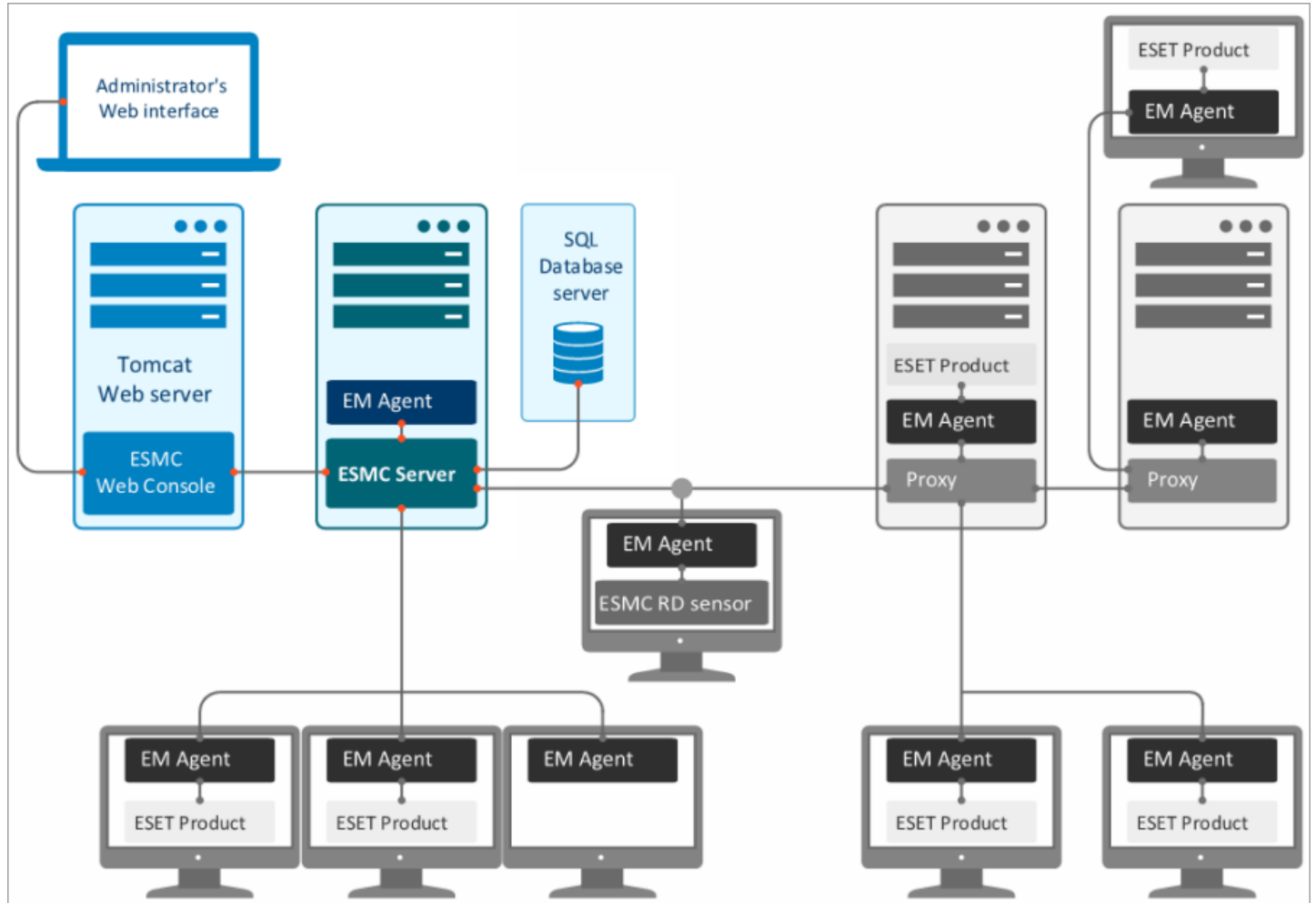
2.2.1 Server

ESET Security Management Center **Server (ESMC Server)** je aplikácia, ktorá spracováva všetky dáta prijaté z počítačov pripojených na server (pomocou ESET Management Agent alebo [Proxy](#)). Pre správne spracovanie dát vyžaduje server stabilné pripojenie na databázový server, kde sú uložené dáta. Pre optimalizáciu výkonu odporúčame nainštalovať databázový server na iný počítač.



2.2.2 Web Console

ESMC Web Console je webové rozhranie, ktoré vám umožňuje spravovať bezpečnostné produkty spoločnosti ESET vo vašej sieti z jedného miesta. Poskytuje prehľad klientov v sieti a zároveň sa dá využiť na vzdialenú inštaláciu bezpečnostných produktov spoločnosti ESET na klienty, ktoré ešte nie sú spravované prostredníctvom nástroja Web Console. Prístup do Web Console je možný prostredníctvom vášho webového prehliadača (pozrite si časť [Podporované webové prehliadače](#)). Ak sa rozhodnete sprístupniť webový server z internetu, budete môcť používať ESET Security Management Center prakticky z akéhokoľvek miesta a zariadenia.



2.2.3 Agent

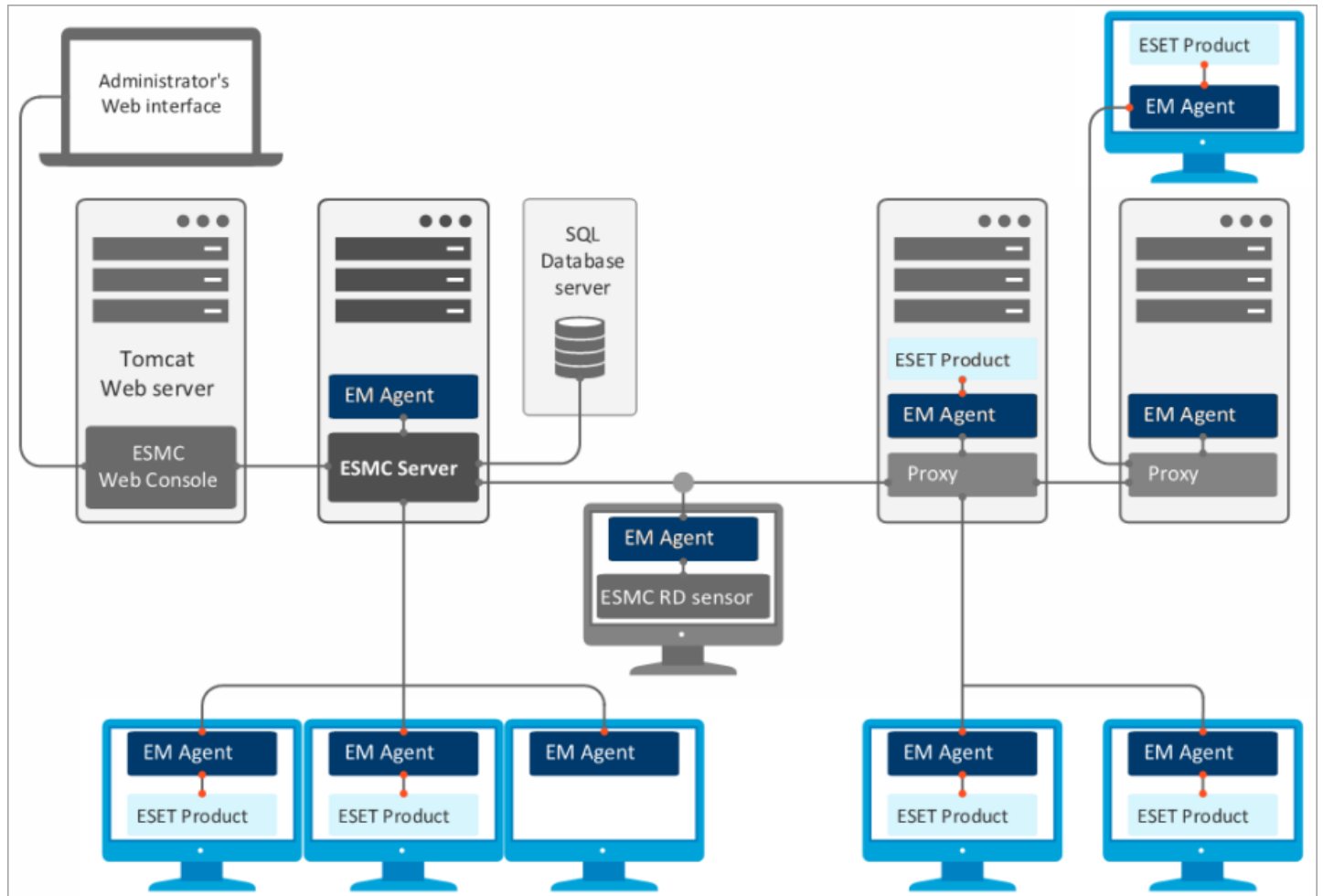
ESET Management Agent je dôležitou súčasťou nástroja ESET Security Management Center 7. Pôvodný názov komponentu z verzie 6.x (ERA Agent) bol zmenený, avšak tento komponent plní aj naďalej rovnaký účel. ESET Management Agent využíva nový, vylepšený komunikačný protokol.

Počítače nekomunikujú priamo so serverom, miesto toho túto komunikáciu sprostredkúva ESMC Agent. Agent zbiera informácie na klientskom počítači a odosiela ich na ESMC Server. Ak ESMC Server odosiela úlohu pre klienta, server najprv odošle úlohu agentu, ktorý ju následne odošle klientu.

Pre zjednodušenie implementácie ochrany vo firemnom prostredí je ESET Management Agent zahrnutý v ESMC suite. Je jednoduchý, modulárny, slúži na pokrytie všetkej komunikácie medzi ESMC Serverom a produktmi spoločnosti ESET alebo operačným systémom. Bezpečnostné produkty spoločnosti ESET nekomunikujú priamo so serverom ale prostredníctvom ESMC Agentu. Počítače, ktoré majú nainštalovaný ESET Management Agent a komunikujú s ESMC Serverom, sa označujú ako „spravované“ počítače. Agent môžete nainštalovať na akýkoľvek počítač bez ohľadu na to, či je na danom počítači nainštalovaný iný softvér od spoločnosti ESET.

Výhody:

- Jednoduchá inštalácia – agenta je možné nasadiť na klientske počítače vo firemnej sieti ako akýkoľvek iný softvér.
- Miestna správa bezpečnosti – prednastavením bezpečnostných scenárov pre agenta sa značne znižuje čas reakcie na hrozbu.
- Off-line správa bezpečnosti – agent môže reagovať na udalosti aj v čase, keď nie je pripojený na ESMC Server.



2.2.4 Proxy

Čo je proxy a ako by mohlo byť užitočné?

Proxy je komponent tretej strany a môže plniť dve hlavné úlohy:

- Ukladanie inštalátorov a aktualizácií produktov ESET do vyrovnávacej pamäte.
- Presmerovanie komunikácie agentov na ESMC Server v prostrediach, kde sa klientske počítače s nainštalovaným agentom nemôžu pripojiť na server.

Čo bolo ERA 6.x Proxy a prečo bolo odstránené?

ERA Proxy umožňovalo zhromažďovať dáta odosielané agentmi. Umožňovalo pripojiť viacero agentov na ERA Proxy, ktorých komunikáciu preposielalo na ERA Server. ESMC 7 využíva nový protokol replikácie, ktorý nám umožňuje preposielať replikáciu prostredníctvom nového proxy. ERA 6.x Proxy nedokáže čítať takýto protokol a preto nemôže byť používané s ESET Management Agentmi verzie 7.

Môže byť ERA 6.x Proxy použité s ESMC 7?

Áno, avšak len v určitom rozsahu. ERA 6.x Proxy dokáže preposielať komunikáciu agentov verzie 6.x na ESMC Server verzie 7, ale ESET Management Agenty sa nedokážu pripojiť na ERA 6.x Proxy. Agenty verzie 7 sa nedokážu pripojiť na ERA Server verzie 6.x. Túto zmenu je potrebné brať na vedomie pri vykonávaní [aktualizácie infraštruktúry](#) z verzie 6.x.

Ako funguje proxy v rámci nástroja ESET Security Management Center?

ESMC 7 využíva prispôsobenú verziu [Apache HTTP Proxy](#) ako proxy komponent. Po správnej konfigurácii môže Apache HTTP Proxy slúžiť ako proxy pre ESET Management Agency. Proxy neotvára a neukladá komunikáciu do vyrovnávacej pamäte, iba ju preposiela.

Môžem použiť iné riešenie proxy ako [Apache HTTP Proxy](#)?

Môže byť použité akékoľvek riešenie proxy, ktoré spĺňa nasledujúce požiadavky:

- dokáže preposielať SSL komunikáciu,
- podporuje HTTP CONNECT,
- nepoužíva overovanie, čiže používateľské meno a heslo.

V čom je odlišný nový protokol replikácie?

Nový protokol replikácie využíva TLS a HTTP2 protokoly a komunikáciu je možné presmerovať pomocou proxy serverov. Okrem toho disponuje novým self-recovery mechanizmom a využíva perzistentné spojenie, ktoré zvyšuje celkový výkon.

Aký to bude mať dopad na výkon?

Použitie HTTP Proxy nebude mať žiadny väčší vplyv na výkon. Používateľ môže tiež použiť politiku na nastavenie viacerých HTTP Proxy serverov pre každého agenta a použiť ich ako failover.

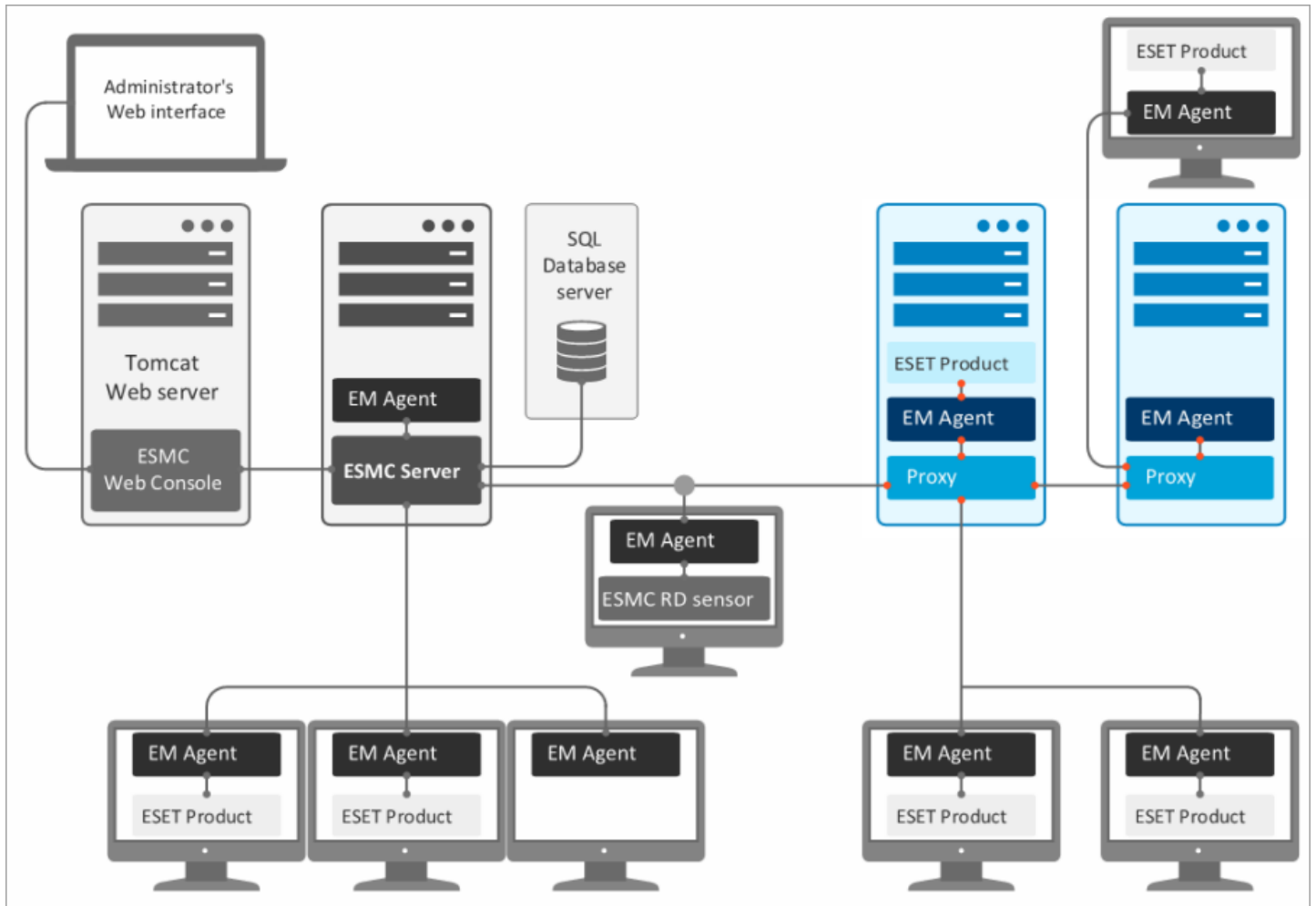
Kedy je vhodné použiť proxy?

Proxy odporúčame použiť v prípade, že vaše sieťové prostredie spĺňa jednu alebo viac podmienok spomenutých nižšie:

- Ak sa vaše klientske počítače s nainštalovanými agentmi nemôžu pripojiť priamo na ESMC Server.
- Ak má vaša firma vzdialené pobočky a vy chcete prostredníctvom proxy zabezpečiť spojenie medzi:
 - ESMC Serverom a proxy,
 - proxy a klientskymi počítačmi vo vzdialenej pobočke.

i Poznámka:

- Aké sú ostatné funkcie [Apache HTTP Proxy](#)?
- [Aké sú rozdiely medzi rôznymi proxy?](#)
- [Ako vykonať aktualizáciu](#) na ESMC 7 v rámci infraštruktúry s ERA 6.x Proxy?

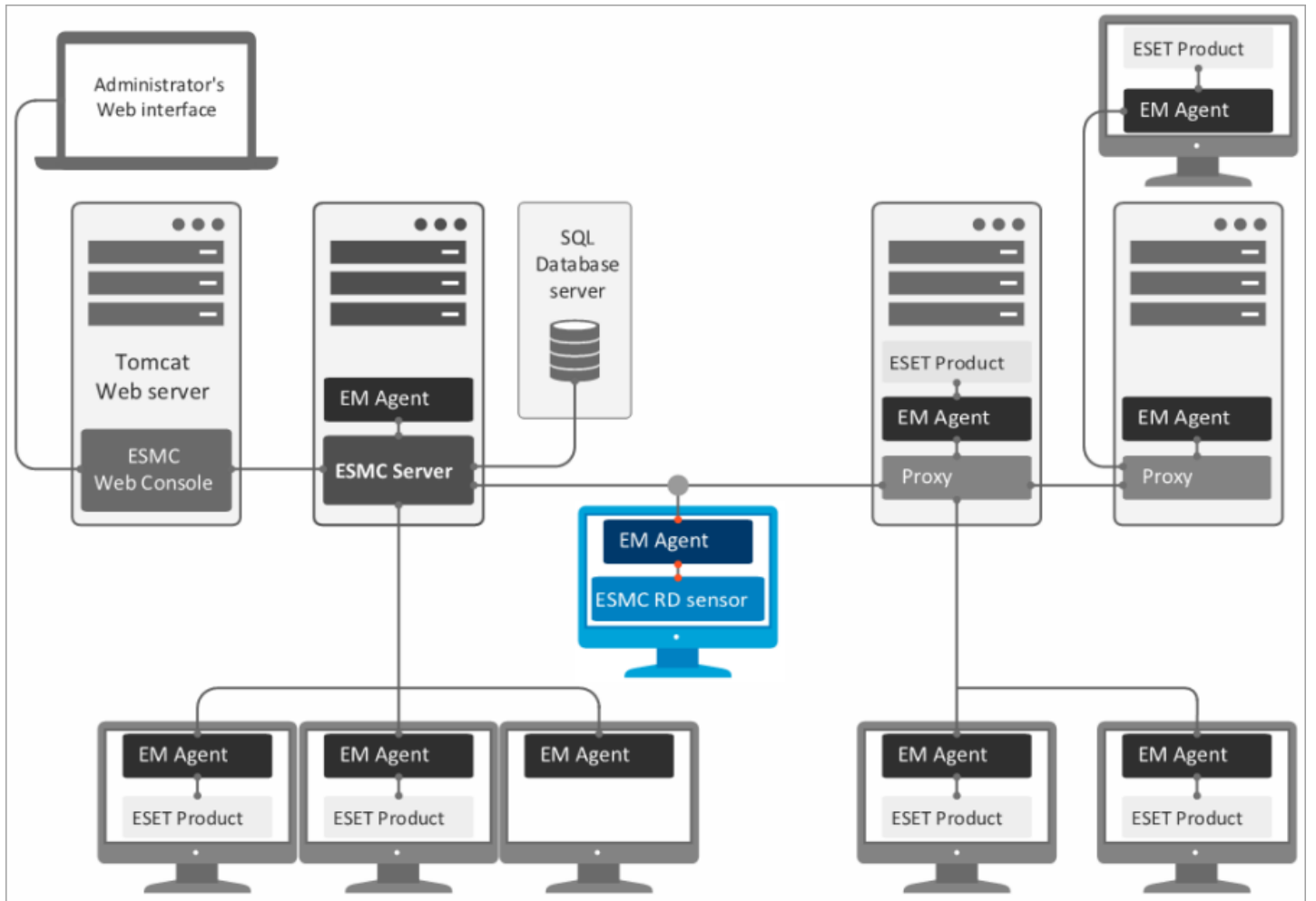


2.2.5 Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) je nástroj na vyhľadávanie počítačov v sieti. Poskytuje pohodlný spôsob pridávania nových počítačov do štruktúry ESET Security Management Center bez potreby manuálneho vyhľadávania a pridávania. Nájdené počítače budú nahlásené v preddefinovanej správe, čím sa umožní ich presunutie do statickej skupiny a následné spúšťanie úloh.

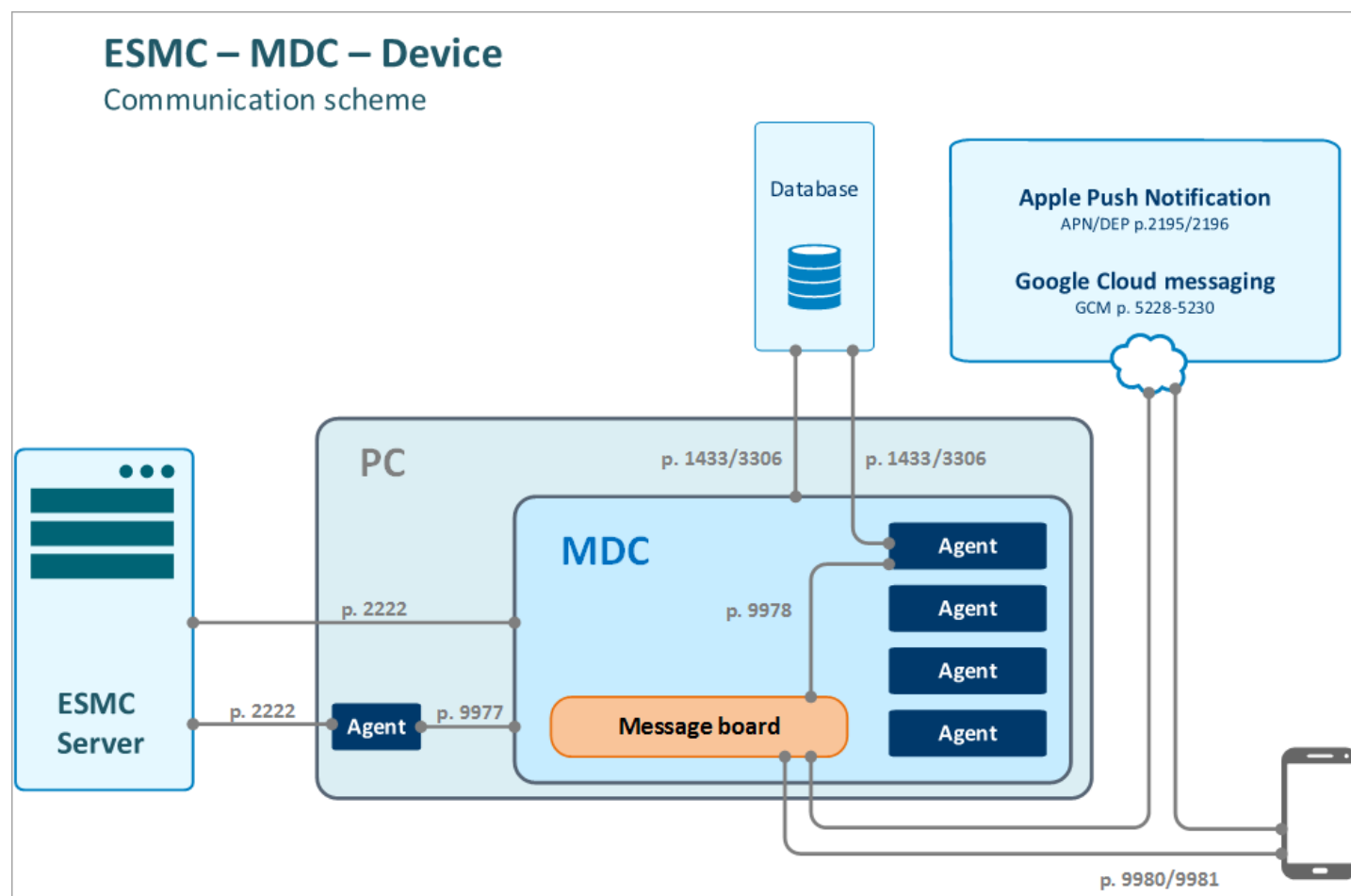
RD Sensor je pasívny prijímač, ktorý deteguje počítače, ktoré sú v sieti, a odosiela informácie o nich na ESMC Server. ESMC Server potom posudzuje, či sú tieto počítače na sieti neznáme, alebo ich už spravuje.

Každý počítač v sieti (doméne, LDAP, sieti Windows) je automaticky pridaný do zoznamu počítačov ESMC Servera prostredníctvom synchronizačnej úlohy. Použitie nástroja RD Sensor je pohodlným spôsobom detekcie počítačov, ktoré nie sú v doméne alebo inej sieti, a pridania ich do štruktúry ESET Security Management Center Servera. RD Sensor si pamätá počítače, ktoré už boli nájdené a nebude odosielať duplicitné informácie.



2.2.6 Mobile Device Connector

ESET Security Management Center Mobile Device Connector je komponent, ktorý umožňuje správu mobilných zariadení pomocou nástroja ESET Security Management Center. Umožňuje vám spravovať mobilné zariadenia (Android a iOS) a ESET Endpoint Security pre Android.



i Poznámka:

Odporúčame vám nasadiť komponent MDM na osobitné hostiteľské zariadenie, nie na zariadenie, na ktorom beží ESMC Server.

Odporúčané hardvérové nároky pre zhruba 80 spravovaných mobilných zariadení:

Hardvér	Odporúčaná konfigurácia
Procesor	4 jadrá, 2,5 GHz
RAM	4 GB (odporúčané)
HDD	100 GB

Pre viac ako 80 spravovaných mobilných zariadení však hardvérové nároky nie sú omnoho vyššie. Časové oneskorenie medzi odoslaním úlohy z ESMC a jej následným vykonaním na mobilnom zariadení sa zvýši proporcionálne v závislosti od toho, koľko zariadení je vo vašom prostredí.

2.2.7 Apache HTTP Proxy

Apache HTTP Proxy je služba, ktorá môže byť použitá na distribúciu aktualizácií na klientske počítače. Apache HTTP Proxy má podobnú úlohu ako funkcia mirror servera v ERA 5 a starších verziách.

Používanie Apache HTTP Proxy má nasledujúce výhody:

sťahovanie a ukladanie do vyrovnávacej pamäte,

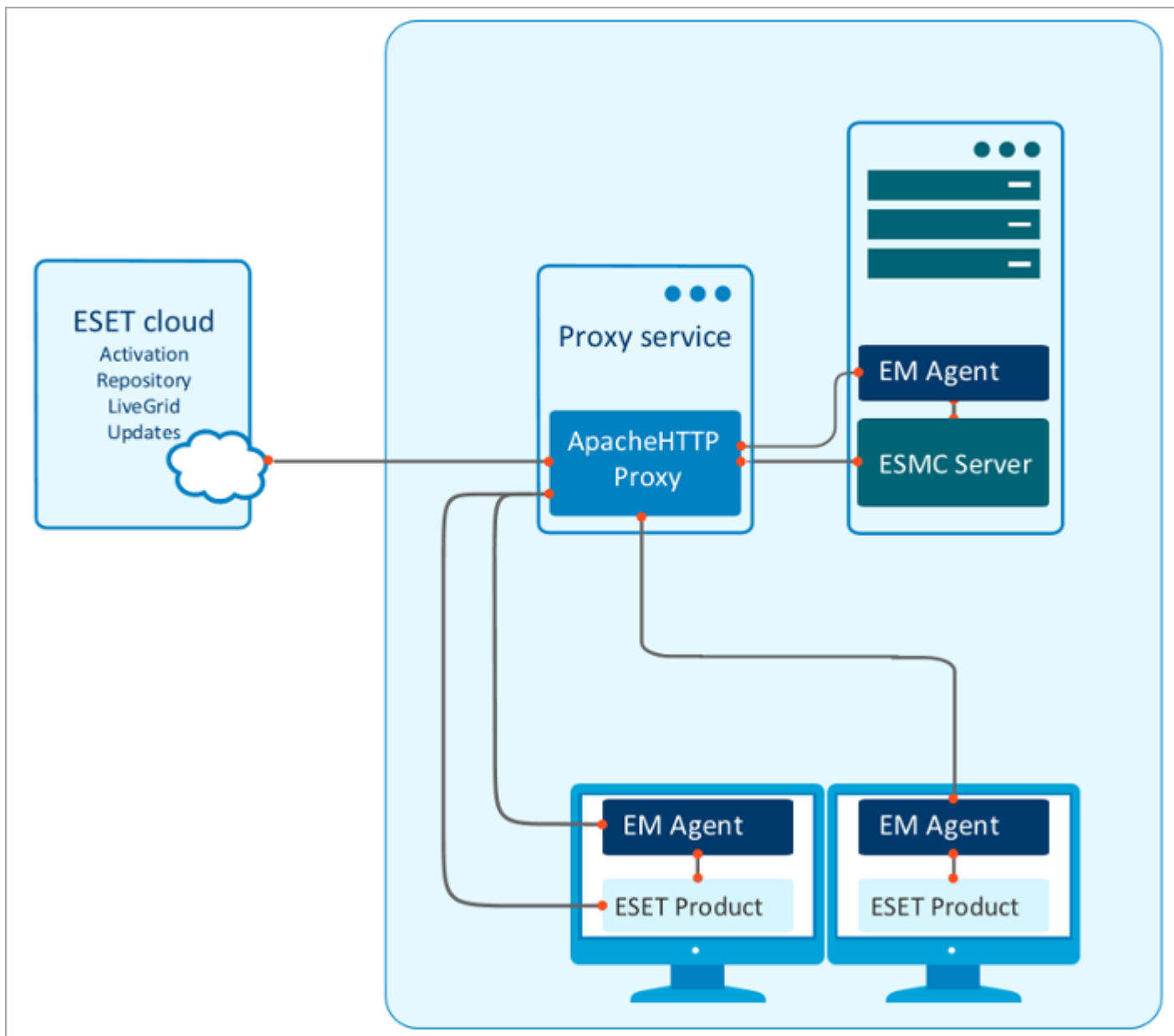
- aktualizácie detekčného jadra,
- úlohy aktivácie produktu – komunikácia s aktivačnými servermi a ukladanie licenčných údajov,
- dáta v ESMC repozitári,
- aktualizácie komponentov produktu,
- následná distribúcia na klienty v sieti.

Znižuje prenosové zaťaženie internetu vo vašej sieti.

Na rozdiel od nástroja Mirror Tool, ktorý z aktualizáčnych serverov spoločnosti ESET sťahuje všetky dostupné dáta, Apache HTTP Proxy sťahuje s cieľom znížiť zaťaženie siete len dáta vyžiadané komponentmi ESMC alebo produktmi ESET pre koncové zariadenia. Pokiaľ klient vyžaduje aktualizáciu, Apache HTTP Proxy ju stiahne z aktualizáčnych serverov spoločnosti ESET, uloží ju do adresára vyrovnávacej pamäte a distribuuje na daného klienta. Ak tú istú aktualizáciu požaduje ďalší klient, Apache HTTP Proxy ju poskytne priamo z vyrovnávacej pamäte, aby sa nemusela opätovne sťahovať z aktualizáčnych serverov spoločnosti ESET.

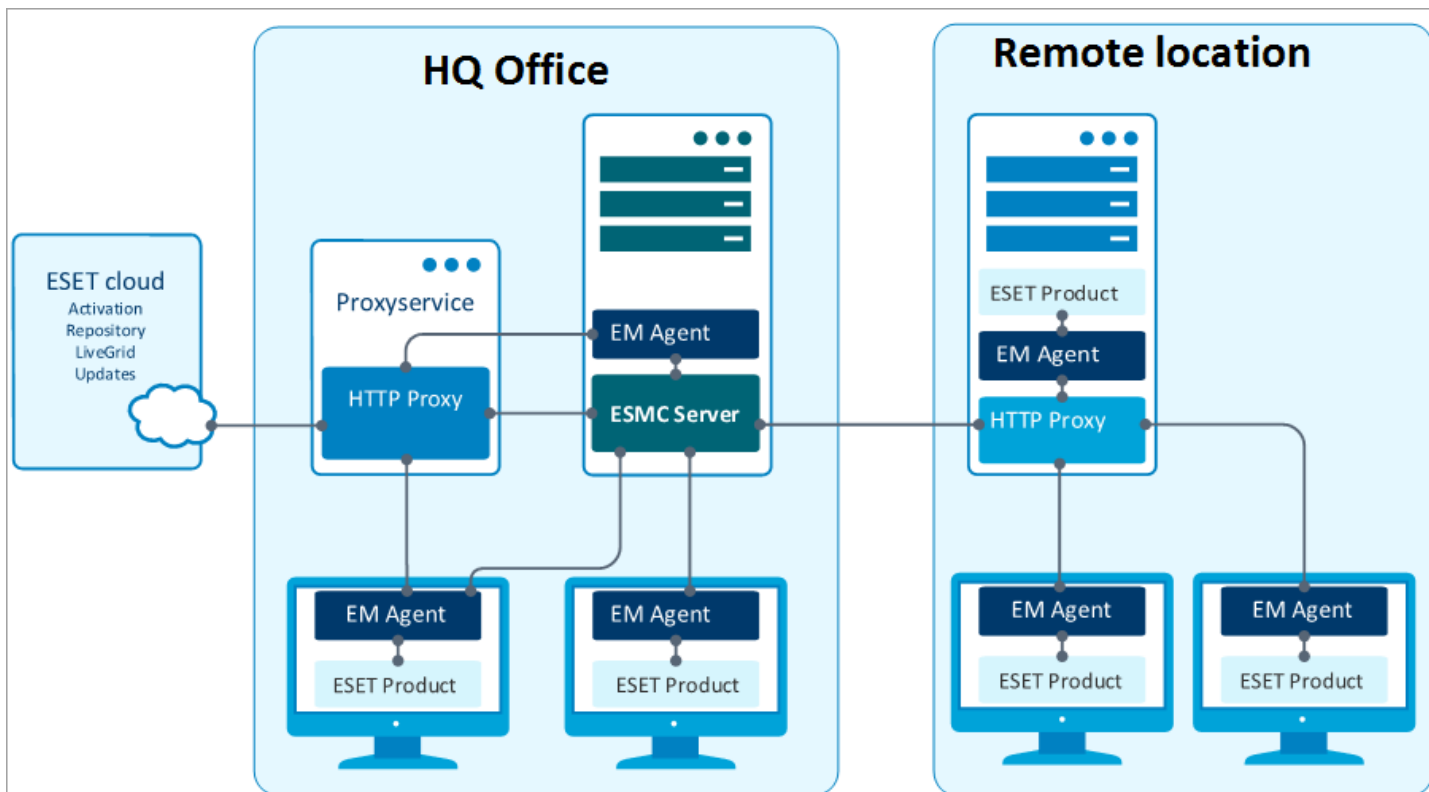
Pri správnom nastavení môže byť Apache HTTP Proxy použité na zozbieravanie a preposielanie dát z komponentov ESMC vo vzdialenej lokalite. Ide o funkciu podobnú funkcii komponentu ERA 6.x Proxy. (Komponent ERA 6.x Proxy nie je kompatibilný s ESET Management Agentmi.) Viac o funkcii proxy sa dozviete na nasledujúcom [odkaze](#).

Nasledujúca schéma zobrazuje použitie proxy servera (Apache HTTP Proxy) na prenos informácií z ESET cloudu na jednotlivé komponenty ESMC a produkty ESET pre koncové zariadenia.



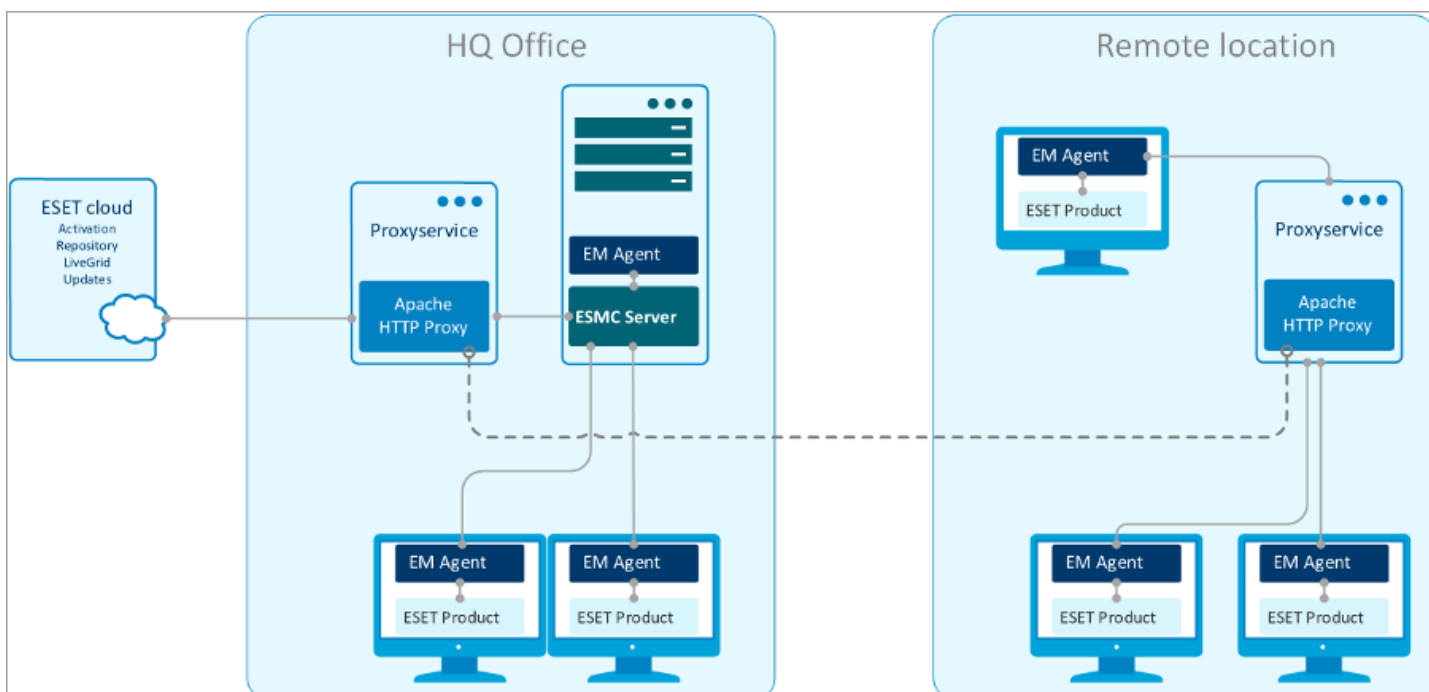
i Poznámka:

[Aké sú rozdiely medzi rôznymi proxy?](#)



! Dôležité:

Použitím [proxy chain](#) (reťazenia proxy) môžete do vzdialenej lokality pridať ďalšiu službu proxy. Majte na pamäti, že ESMC nepodporuje proxy chaining v prípade, že proxy vyžadujú autentifikáciu. Môžete použiť vlastný transparentný proxy server – avšak v tomto prípade bude pravdepodobne potrebné upraviť jeho konfiguráciu nad rámec toho, čo spomíname v tejto kapitole.



i Poznámka:

Pre offline aktualizáciu detekčného jadra použite namiesto Apache HTTP Proxy nástroj [Mirror tool](#). Tento nástroj je dostupný pre obe platformy ([Windows](#) a [Linux](#)).

2.3 Scenáre nasadenia – najvhodnejšie postupy

Nasledujúca sekcia pojednáva o rozličných scenároch nasadenia pre rôzne sieťové prostredia.

Najvhodnejšie postupy pre nasadenie ESET Security Management Center

Počet klientov	Do 1 000 klientov	1 000 – 5 000 klientov	5 000 – 10 000 klientov	10 000 – 50 000 klientov	50 000 – 100 000 klientov	100 000 a viac klientov**
ESMC Server a databázový server na tom istom zariadení	OK	OK	OK	Nie	Nie	Nie
Použitie MS SQL Express	OK	OK	OK	Nie	Nie	Nie
Použitie MS SQL	OK	OK	OK	OK	OK	OK
Použitie MySQL	OK	OK	OK	Nie	Nie	Nie
Použitie virtuálneho zariadenia ESMC	OK	OK	Neodporúča sa	Nie	Nie	Nie
Použitie virtuálneho počítača	OK	OK	OK	Voliteľné	Nie	Nie
Odporúčaný interval replikácie (v priebehu nasadenia)	60 sekúnd*	5 minút	10 minút	15 minút	20 minút	25 minút
Odporúčaný interval replikácie (po nasadení, počas bežného používania)	10 minút	10 minút	20 minút	30 minút	40 minút	60 minút

* Predvolený interval replikácie ESET Management Agent. Bližšie informácie o tom, ako upraviť interval replikácie tak, aby vyhovoval vašej infraštruktúre, nájdete v [tejto kapitole](#). Pre vysoko výkonnú konfiguráciu hardvéru odporúčame ponechať celkový počet pripojení agenta k serveru pod úrovňou 1000 za sekundu.

** O odporúčaných požiadavkách na hardvér sa dočítate v kapitole [Škálovateľnosť ESMC infraštruktúry](#).

Jeden server (malé spoločnosti)

Na správu malých sietí (1000 a menej klientov) stačí mať ESMC Server a všetky súvisiace komponenty ESMC nainštalované na jednom zariadení. Ide vlastne o jeden server alebo samostatne nainštalovaný komponent.

Vzdialené pobočky s Proxy

Ak klientske počítače nie sú priamo viditeľné na ESMC Serveri, použite [proxy](#) na presmerovanie komunikácie. Proxy neagreguje komunikáciu a neznižuje počet replikácií.

Podniková sieť (Enterprise)

V podnikovej sieti (napríklad so 100 000 klientmi) by mali byť využité ďalšie komponenty ESMC:

- [RD Sensor](#) pomáha pri vyhľadávaní nových počítačov vo vašej sieti.
- SQL databáza môže byť zavedená na osobitný server alebo Failover klaster.
- ESMC Server môže byť nainštalovaný na Failover klastri.

2.3.1 Praktické príklady nasadenia (Windows)

Pre čo najlepší výkon odporúčame použiť Microsoft SQL Server ako databázu pre ESET Security Management Center. Napriek tomu, že ESET Security Management Center je kompatibilný s MySQL, používanie MySQL môže mať negatívny dopad na výkon systému pri práci s veľkým množstvom dát. Rovnaký hardvér pri použití Microsoft SQL Servera dokáže spravovať 10-krát viac klientov ako pri použití MySQL.

Za účelom testovania každý klient ukladá do databázy 30 protokolov. Microsoft SQL Server používa veľké množstvo RAM pamäte pre ukladanie databázy do vyrovnávacej pamäte, odporúčame preto mať aspoň toľko pamäte, akú veľkosť predstavuje Microsoft SQL Server na disku.

Neexistuje žiadny jednoduchý výpočet na zistenie presného množstva prostriedkov použitých produktom ESET Security Management Center, pretože táto veľkosť sa mení v závislosti od konfigurácie siete. Nasledujú výsledky testov pre bežné sieťové konfigurácie:

- [Testovací prípad – maximálne 5000 klientov pripojených na ESMC Server](#)
- [Testovací prípad – maximálne 100 000 klientov pripojených na ESMC Server](#)

Pre dosiahnutie optimálnej konfigurácie odporúčame vykonávať testy s nízkym počtom klientov a pomalším hardvérom a následne na základe výsledkov testovania odvodiť vaše systémové požiadavky.

TESTOVACÍ PRÍPAD (5000 KLIENTOV)

Hardvér/softvér

- Windows Server 2012 R2, 64-bitová architektúra procesora
- Microsoft SQL Server Express 2014
- Intel Core2Duo E8400 @3 GHz
- 4 GB RAM
- Seagate Barracuda 7200 rpm, 1 TB, 16 MB cache, SATA 3,0 Gb/s

Výsledok

- ESMC Web Console reaguje do 5 sekúnd
- Priemerná spotreba pamäte:
 - Apache Tomcat 200 MB
 - ESMC Server 200 MB
 - SQL Server databáza 2 GB
- Výkon replikácie servera je 10 replikácií za sekundu
- Veľkosť databázy na disku je 2 GB (5000 klientov, každý s 30 protokolmi v databáze)

Pre tento príklad bol použitý SQL Server Express 2014. Napriek svojim obmedzeniam (10 GB databáza, 1CPU a 1 GB používanej RAM pamäte) bola táto konfigurácia funkčná a mala dobrý výkon. Pri použití SQL Server Express odporúčame menej ako 5000 klientov. Ak po nasadení SQL Server Express budete potrebovať pracovať s väčšími databázami, môžete prejsť na plnú verziu Microsoft SQL Servera.

Výkon replikácie servera udáva interval replikácie pre klientov. 10 replikácií za sekundu znamená 600 replikácií za minútu. V ideálnom prípade by mal byť interval replikácie na všetkých 5000 klientoch 8 minút, avšak len pri 100 % zaťažení servera, preto je v tomto prípade potrebný dlhší interval. V tomto prípade je odporúčaný interval replikácie 20 – 30 minút.

TESTOVACÍ PRÍPAD (100 000 KLIENTOV)

Hardvér/softvér

- Windows Server 2012 R2 Datacenter, 64-bitová architektúra procesora
- Microsoft SQL Server 2012
- Intel Xeon E5-2650v2 @2.60GHz
- 64 GB RAM
- Sieťový adaptér Intel NIC/PRO/1000 PT Dual
- 2x Micron RealSSD C400 256 GB SSD disky (jeden pre systém + softvér, druhý pre dátové súbory SQL Servera)

Výsledok

- Web Console reaguje do 30 sekúnd
- Priemerná spotreba pamäte
 - Apache Tomcat 1 GB
 - ESMC Server 2 GB
 - SQL Server databáza 10 GB
- Výkon replikácie servera je 80 replikácií za sekundu
- Veľkosť databázy na disku je 10 GB (100 000 klientov, každý s 30 protokolmi v databáze)

V tomto prípade sme pre test kapacity ESMC Servera nainštalovali Apache Tomcat + ESMC Web Console, ESMC Server na jeden počítač a SQL Server na druhý počítač.

Vysoký počet klientov sa prejavil na zvýšenom zaťažení pamäte a diskov databázovým systémom Microsoft SQL Server. Pre optimálny výkon SQL Server načíta do vyrovnávacej pamäte skoro celú databázu. Apache Tomcat (Web Console) a ESMC Server tiež používajú vyrovnávaciu pamäť, čo vysvetľuje väčšie vyťaženie pamäte v tomto prípade.

ESMC Server je schopný vykonať 80 replikácií za sekundu (288 000 za hodinu), čiže v ideálnom prípade by mal byť interval replikácie na všetkých 100 000 klientoch nastavený na každých cca 30 minút (zaťaženie 200 000 replikácií za hodinu). To by však znamenalo 100 % vyťaženie servera, preto najlepší interval replikácie je v tomto prípade 1 hodina (100 000 replikácií za hodinu).

Vyťaženie siete závisí od počtu protokolov získaných z klientskych počítačov. Pri tomto teste bol počet 20 KB na replikáciu, čiže 80 replikácií za sekundu vykazuje rýchlosť siete okolo 1600 KB/s (20 Mbit/s).

2.3.2 Nasadenie vo veľkých podnikoch (200 000 klientov)

Našu odporúčanú systémovú konfiguráciu pre nasadenie ESMC Servera a jeho komponentov v podnikovom prostredí s 200 000 klientmi nájdete nižšie.

! Dôležité:

Odporúčaná konfigurácia pre ESMC sa môže líšiť v závislosti od mnohých faktorov, ako napríklad veľkosť infraštruktúry, jej zloženie, geografická distribúcia klientov a kvalita pripojenia v rôznych častiach podnikovej siete.

ESMC Server

Hardvér/softvér	Odporúčaná konfigurácia
Operačný systém	Windows Server 2012 R2 a novšie verzie, 64-bitová architektúra procesora
Procesor	8 jadier
RAM	16 GB (minimum), 64 GB (odporúčané)
Typ a veľkosť disku	128 GB SSD (minimum), 256 GB SSD (odporúča sa)

ESMC databáza (MSSQL)

Hardvér/softvér	Odporúčaná konfigurácia
Operačný systém	Windows Server 2012 R2 a novšie verzie, 64-bitová architektúra procesora
Databáza	Microsoft SQL Server 2012 a novšie verzie
Procesor	32 jadier
RAM	128 GB (minimum), 512 GB (odporúčané)
Typ a veľkosť disku	1 TB ¹ SSD (minimum), 2 TB ¹ SSD (odporúčané)

¹ Predpokladaná doba uchovávanía protokolov je 6 mesiacov.

HTTP proxy²

Hardvér/softvér	Odporúčaná konfigurácia
Operačný systém	Windows Server 2012 R2 a novšie verzie, 64-bitová architektúra procesora
Procesor	2 jadrá
RAM	2 GB (minimum), 4 GB (odporúčané)
Typ a veľkosť disku	128 GB SSD (minimum), 256 GB SSD (odporúča sa)

² HTTP proxy odporúčame používať len na ukladanie aktualizácií bezpečnostných produktov ESET do vyrovnávacej pamäte. Neodporúčame používať HTTP proxy na preposielanie komunikácie ESET Management Agentov na ESMC Server, pokiaľ to nie je v rámci vašej siete nevyhnutné.

i Poznámka:

Pre zabezpečenie vysokej miery dostupnosti a spoľahlivosti vo vašom podnikovom prostredí vám odporúčame postupovať podľa inštrukcií týkajúcich sa [inštalácie nástroja ESET Security Management Center na Failover klaster](#). ESMC Server môžete tiež [pripojiť](#) ku klastrovej databáze.

2.3.3 Rozdiely medzi Apache HTTP Proxy, nástrojom Mirror Tool a priamym pripojením na internet

Komunikácia prebiehajúca v produktoch ESET zahŕňa preberanie aktualizácií detekčného jadra a modulov programu, overovanie licenčných údajov a taktiež výmenu dát v rámci technológie [ESET Live Grid](#) (pozrite si [tabuľku](#) nižšie).

ESET Security Management Center sťahuje inštalačné balíky pre najnovšie verzie produktov, ktoré sa majú distribuovať na klientske počítače, z repozitára spoločnosti ESET. Akonáhle je na cieľový počítač distribuovaný inštalačný balík, môže byť daný produkt nasadený na počítač.

Po inštalácii musí byť bezpečnostný produkt spoločnosti ESET aktivovaný, čo znamená, že produkt musí overiť vaše licenčné údaje na licenčnom serveri. Aktivovaný produkt pravidelne aktualizuje detekčné jadro a moduly programu.

[ESET LiveGrid® Early Warning System](#) pomáha zabezpečiť, aby bola spoločnosť ESET okamžite a nepretržite informovaná o nových infiltráciách a mohla tak pohotovo chrániť svojich zákazníkov. Tento systém umožňuje odosielanie hrozieb priamo do laboratória ESET Threat Lab, kde sú analyzované a spracované.

Najväčšiu časť komunikácie na sieti predstavujú aktualizácie modulov produktu. Bezpečnostný produkt ESET v priebehu mesiaca obyčajne stiahne približne 23,9 MB aktualizácií modulov programu.

[ESET LiveGrid®](#) dáta (približne 22,3 MB) a súbor aktualizovanej verzie (do 11 kB) sú jedinými distribuovanými súborami, ktoré nie je možné uložiť do vyrovnávacej pamäte.

Existujú dva typy aktualizácií – *level* a *nano*. [Pre viac informácií o typoch aktualizácií si prečítajte tento článok databázy znalostí.](#)

Znížiť zaťaženie siete pri distribúcii aktualizácií na klientske počítače je možné dvomi spôsobmi – prostredníctvom [Apache HTTP Proxy](#) alebo nástroja [Mirror Tool](#).

Typy komunikácie produktov spoločnosti ESET

Typ komunikácie	Frekvencia komunikácie	Vplyv na sieťovú komunikáciu	Komunikácia prostredníctvom proxy	S využitím proxy cache ¹	S využitím Mirror Toolu ²	Funkčnosť v offline prostredí
Nasadenie agenta (Push/Live inštalátory z repozitára)	jedenkrát	približne 50 MB na klienta	áno	áno ³	nie	áno (GPO/SSCM, upravené live inštalátory) ⁴
Inštalácia produktu ESET Endpoint (z repozitára)	jedenkrát	približne 100 MB na klienta	áno	áno ³	nie	áno (GPO/SSCM, inštalácia z URL) ⁴
Aktualizácia detekčného jadra/modulov programu	šesť a viackrát denne	23,9 MB za mesiac ⁵	áno	áno	áno	áno (offline Mirror Tool a vlastný HTTP Server) ⁶
Overenie verzie stiahnutím súboru update.ver	~8-krát denne	2,6 MB za mesiac ⁷	áno	nie	-	-

Typ komunikácie	Frekvencia komunikácie	Vplyv na sieťovú komunikáciu	Komunikácia prostredníctvom proxy	S využitím proxy cache ¹	S využitím Mirror Toolu ²	Funkčnosť v offline prostredí
Aktivácia/kontrola licencie	4-krát denne	zanedbateľný	áno	nie	nie	áno (offline licenčné súbory získané cez ESET Business Account) ⁸
LiveGrid overovanie reputácie	priebežne	11 MB za mesiac	áno	nie	nie	nie

1. O vplyve a výhodách používania vyrovnávacej pamäte (proxy cache) si prečítajte v kapitole [Kedy sa oplatí používať Apache HTTP Proxy?](#)
2. O výhodách používania nástroja Mirror Tool sa dočítate v kapitole [Kedy sa oplatí používať Mirror Tool?](#)
3. Pri inštalácii/aktualizácii odporúčame najskôr nasadiť jedného agenta/produkt určený pre koncové zariadenia, aby sa inštalátor uložil do vyrovnávacej pamäte.
4. Nasadenie ESET Management Agentu vo veľkých sieťach je popísané v kapitole [Nasadenie agenta pomocou GPO alebo SCCM](#).
5. Počiatočná aktualizácia detekčného jadra môže byť aj väčšia v závislosti od toho, aký starý je inštalačný balík (keďže sa budú musieť stiahnuť všetky novšie moduly programu, resp. aktualizácie detekčného jadra). Odporúčame bezpečnostný produkt najskôr nainštalovať na jedného klienta a nechať prebehnúť aktualizáciu, aby sa súbory aktualizácie detekčného jadra a modulov programu uložili do vyrovnávacej pamäte.
6. Bez pripojenia na internet nástroj Mirror tool nedokáže stiahnuť aktualizácie detekčného jadra. Môžete použiť Apache Tomcat ako HTTP server pre sťahovanie aktualizácií do adresára dostupného pre [Mirror Tool](#).
7. Pri každej kontrole verzie detekčného jadra a dostupnosti aktualizácií sa sťahuje a spracováva súbor *update.ver*. Podľa predvolených nastavení plánovač v produkte ESET určenom pre koncové zariadenia kontroluje dostupnosť aktualizácií každú hodinu. Predpokladáme pritom, že bežný firemný počítač je zapnutý 8 hodín denne. Veľkosť súboru *update.ver* je približne 11 kB.
8. [Stiahnite si offline licenčné súbory ako vlastník licencie](#) alebo ako [bezpečnostný správca](#).

i Poznámka:

Prostredníctvom Apache HTTP Proxy nie je možné do vyrovnávacej pamäte ukladať aktualizácie pre produkty ESET vo verziách 4 a 5. Distribuovať aktualizácie pre takéto produkty je možné použitím nástroja [Mirror Tool](#), prípadne môžete na jednom počítači s danou verziou produktu ESET určeného pre koncové zariadenia [vytvoriť mirror server](#).

2.3.3.1 Kedy sa oplatí používať Apache HTTP Proxy?

Naše testy ukázali, že komponent Apache HTTP Proxy sa oplatí používať hlavne v sieťach s 37 a viac počítačmi.

V sieti s 1000 počítačmi, v ktorej prebehlo aj niekoľko inštalácií a odinštalácií, sme zisťovali, aké množstvo dát bolo stiahnutých z internetu pre potreby aktualizácií v priebehu jedného mesiaca.

- Jeden počítač s priamym pripojením na internet (bez použitia Apache HTTP Proxy) stiahol na účely [aktualizácie](#) za mesiac v priemere 23,9 MB dát.
- Pri použití Apache HTTP Proxy dosiahol objem stiahnutých dát v celej sieti iba 900 MB za mesiac.

V tabuľke nižšie uvádzame porovnanie objemu stiahnutých dát aktualizácií za mesiac pri použití priameho pripojenia na internet a pri využití Apache HTTP Proxy:

Počet klientov vo vašej firemnej sieti	25	36	50	100	500	1 000
--	----	----	----	-----	-----	-------

Priame pripojenie na internet (MB/mesiac)	375	900	1 250	2 500	12 500	25 000
Apache HTTP Proxy (MB/mesiac)	30	50	60	150	600	900

2.3.3.2 Kedy sa oplatí používať Mirror Tool?

Ak využívate offline prostredie, t. j. počítače vo vašej sieti sa dlhodobo (mesiace či roky) nepripájajú na internet, je používanie nástroja [Mirror Tool](#) jediným možným spôsobom, ako distribuovať aktualizácie modulov produktu na jednotlivé klientske počítače v sieti, keďže tento nástroj pri každej žiadosti o aktualizovanie sťahuje a lokálne ukladá všetky dostupné level a nano aktualizácie.

Hlavným rozdielom medzi Apache HTTP Proxy a nástrojom Mirror Tool je to, že Apache HTTP Proxy sťahuje len chýbajúce aktualizácie (napríklad aktualizáciu Nano 3), zatiaľ čo Mirror Tool sťahuje všetky dostupné [level and nano aktualizácie](#) bez ohľadu na to, čo daný modul produktu potrebuje aktualizovať a čo nie.

Na vzorke 1000 počítačov, rovnakej ako pri teste [Apache HTTP Proxy](#), sme otestovali efektivitu nástroja Mirror Tool. Zistili sme, že v priebehu jedného mesiaca bolo z internetu v rámci aktualizácií stiahnutých 5500 MB dát. Množstvo stiahnutých dát ani po pridaní ďalších počítačov do siete ďalej nerástlo. V porovnaní so situáciou, keď sa klienty pripájajú do siete internet priamo, ide aj v prípade nástroja Mirror Tool o výrazné zníženie zaťaženia siete, avšak efektivitu Apache HTTP Proxy nedosahuje.

Počet klientov vo vašej firemnej sieti	25	36	50	100	500	1 000
Priame pripojenie na internet (MB/mesiac)	375	900	1 250	2 500	12 500	25 000
Mirror Tool (MB/mesiac)	5 500	5 500	5 500	5 500	5 500	5 500

i Poznámka:

Ani v prípade sietí s viac ako 1000 počítačmi by množstvo dát stiahnutých z internetu pre potreby aktualizácie výrazne nevrástlo, a to ani pri používaní Apache HTTP Proxy, ani nástroja Mirror Tool.

2.4 Škálovateľnosť ESMC infraštruktúry

i Poznámka:

Používate nástroj ESMC v prostredí malého alebo stredného podniku (MSP)? Kliknite sem...

Pre používanie nástroja ESET Security Management Center na správu menšej siete vám postačí [jeden server](#). Prečítajte si [príručku pre malé a stredné podniky](#), pokiaľ chcete nainštalovať ESET Security Management Center na platformu Windows a spravovať do 250 produktov od spoločnosti ESET, určených pre koncové zariadenia s operačným systémom Windows.

Pred inštaláciou ESET Security Management Center je dôležité oboznámiť sa s [architektúrou produktu](#) a zistiť, čo má vplyv na výkon ESMC Servera a SQL databázy:

Hardvér použitý pre ESMC Server

Predtým, ako budete pokračovať, vám odporúčame preštudovať si kapitolu o [minimálnych požiadavkách na hardvér](#). Na základe [praktických príkladov nasadenia](#) a nasledujúcej tabuľky môžete zvoliť také hardvérové vybavenie, aby ste zaistili optimálny výkon ESET Security Management Center.

Tabuľka pre malé a stredné podniky (MSP)

Počet klientov	ESMC Server + SQL databázový server		
	Počet CPU	RAM (GB)	HDD (GB)
Do 1 000	2	4	100

1 000 – 5 000	4	4 – 8	150
5 000 – 10 000	4	4 – 8	200

Tieto odporúčania platia pri použití vhodného nastavenia [intervalu pripájania klientov](#).

Tabuľka pre väčšie podniky (Enterprise)

Počet klientov	ESMC Server			SQL databázový server*		
	Počet CPU	RAM (GB)	HDD (GB)	Počet CPU	RAM (GB)	HDD (GB)
10 000 – 50 000	4+	4+	40	8+	8+	250+
50 000 – 100 000	8+	4+	80	8+	16+	250+
100 000+	8+	8+	80	8+	32+	250+

Tieto odporúčania platia pri použití vhodného nastavenia [intervalu pripájania klientov](#).

* SQL Server môže byť nainštalovaný na rovnakom serveri ako ESMC Server a zdieľať rovnaké prostriedky. V takomto prípade by sa mal použiť hardvér rovnať súčtu požiadaviek pre SQL Server a ESMC Server.

** V enterprise prostredí je potrebné SSD s vysokým IOPS.

Konfigurácia Web Console v rámci riešení pre väčšie podniky

Predvolená konfigurácia nástroja Web Console môže byť nestabilná pri práci s vysokým počtom objektov (napríklad vyriešenie 100 000 hrozieb). Aby ste predišli nedostatku pamäte, zmeňte nastavenia pre Tomcat.

• Windows

1. Spustíte súbor `tomcat7w.exe` alebo spustíte aplikáciu `Configure Tomcat`.
2. Prejdíte na kartu Java.
3. Zmeňte hodnotu **Initial memory pool** na 512 a hodnotu **Maximum memory pool** na 2048.
4. Reštartujete službu Tomcat.

• Virtuálne zariadenie ESMC/CentOS Linux

1. Otvorte virtuálny počítač a spustíte terminál.
2. Otvorte súbor `/etc/sysconfig/tomcat`.
3. Do súboru pridajte nasledujúci riadok:
`JAVA_OPTS="-Xms512m -Xmx2048m"`
4. Uložte súbor a reštartujte službu Tomcat.
`service tomcat restart`

• Debian Linux

1. Spustíte terminál ako root používateľ alebo použijete `sudo`.
5. Otvorte súbor `/etc/default/tomcat8`.
6. Do súboru pridajte nasledujúci riadok:
`JAVA_OPTS="-Xms512m -Xmx2048m"`
7. Uložte súbor a reštartujte službu Tomcat.
`service tomcat restart`

SQL databázový server

Požiadavky na databázový server pre ESET Security Management Center nájdete v [tejto kapitole](#). Na vás je rozhodnutie, či SQL databázový server nainštalujete na rovnaký počítač ako ESMC Server alebo preň vyhradíte samostatný server.

Pokiaľ vo vašej sieti spravujete viac ako 10 000 klientov, odporúčame vám použiť vyhradené zariadenie/zariadenia s vyhradenými prostriedkami.

Databáza	Malé a stredné podniky (MSP)	Veľké podniky (Enterprise)	Maximálny počet klientov	Windows	Linux
MS SQL Express	✓	(voliteľné)	5 000	✓	
MS SQL Server	✓	✓	Bez obmedzenia (až 100 000)	✓	
MySQL	✓	✓	10 000	✓	✓

Sieťová architektúra a rýchlosť pripojenia na internet

Požiadavky na sieťové prostredie sú popísané v [tejto kapitole](#). Prečítať si môžete aj o [rozdieloch medzi Apache HTTP Proxy, nástrojom Mirror Tool a priamym pripojením na internet](#).

Interval pripájania klientov

Vplyv na výkon ESMC Servera má aj to, s akým časovým intervalom sa ESET Management Agenty pripájajú na ESMC Server (alebo ERA Proxy). Viac informácií o nastavení intervalu pripájania klientov nájdete v [tejto kapitole](#).

Priemerný počet udalostí hlásených klientmi

Pri vypuknutí malware nákazy alebo preťažení servera (napr. keď pripojíme 20 000 klientov na server, ktorý dokáže pri desaťminútovom intervale zvládnuť pripojenie len 10 000 klientov) môže dôjsť k tomu, že niektoré klienty nebudú pripojené na server. Agenty na týchto nepripojených klientoch sa na ESMC Server pokúsia pripojiť neskôr.

Vplyv komunikácie medzi ESET Management Agentom a ESMC Serverom na prenosové zaťaženie siete

Aplikácie na klientských počítačoch nekomunikujú s ESMC Serverom priamo, miesto toho túto komunikáciu sprostredkúva ESET Management Agent. Takéto riešenie sa jednoduchšie spravuje a vytvára nižšie zaťaženie z hľadiska prenosu dát v sieti. Objem prenesených dát v sieti závisí od toho, ako je nastavený interval pripájania klientov, ako aj od typu úloh, ktoré sú na klientoch spúšťané. ESET Management Agent nadviaže komunikáciu s ESMC Serverom vždy aspoň raz počas stanoveného intervalu pripájania klienta, a to i v tom prípade, že na klientskom počítači nie je naplánovaná ani spúšťaná žiadna úloha. Každé pripojenie predstavuje určitý prenos dát v sieti. Konkrétne príklady prenosu dát nájdete v nasledujúcej tabuľke:

Typ akcie	Množstvo prenesených dát v rámci jedného intervalu pripojenia
Úloha pre klienta: Kontrolovať bez liečenia	4 kB
Úloha pre klienta: Aktualizácia modulov	4 kB
Úloha pre klienta: Vyžiadať SysInspector protokol	300 kB
Politika: Antivírus – Maximálna bezpečnosť	26 kB

Interval pripájania ESET Management Agentu	Množstvo dát vygenerované pripájajúcim sa, no inak nečinným ESET Management Agentom za jeden deň
1 minúta	16 MB
15 minút	1 MB
30 minút	0,5 MB
1 hodina	144 kB
1 deň	12 kB

Ak chcete vypočítať približné množstvo prenesených dát pri sieťovej komunikácii ESET Management Agentov s vaším ESMC Serverom, použite nasledujúci vzorec:

*počet klientov * (denné množstvo dát nečinného agenta + (množstvo prenesených dát pre určitú úlohu * počet opakovaní danej úlohy za deň))*

Počet ESET Management Agentov a klientských počítačov vo vašej sieti

Pre viac informácií si prečítajte kapitolu [Scénare nasadenia – najvhodnejšie postupy](#).

2.5 Čo je nové v nástroji ESET Security Management Center 7.0

Funkcia	ERA 6.x	ESET Security Management Center 7
Konzola	Web Console (vo webovom prehliadači).	Web Console vo webovom prehliadači s výrazne prepracovanou hlavnou ponukou, rozložením sprievodcu, ikonami a akciami, ktoré je možné vyvolať jediným kliknutím. Vyžaduje sa Java 8.
Súčasti	Server, Web Console (webové rozhranie, vyžaduje Java a Apache Tomcat), Agent, Proxy, Rogue Detection Sensor, Mobile Device Connector, Apache HTTP Proxy pre ukladanie aktualizácií do vyrovnávacej pamäte.	ERA Proxy bolo odstránené. Apache HTTP Proxy teraz umožňuje ukladanie aktualizácií produktov do vyrovnávacej pamäte a zároveň preposiela komunikáciu ESET Management Agentov.
Databáza	Pripojenie k jedinej databáze servera.	Možnosť pripojenia k databáze s vysokou dostupnosťou v rámci Failover klastra a pomenovaných inštancií.
Oznámenia	Oznámenia môžu byť doručované prostredníctvom SNMP Trap, e-mailu a Syslogu.	Pribudli nové upraviteľné textové oznámenia, ktoré podporujú premenné. Takisto pribudli nové oznámenia pre klonované počítače a VDI prostredia.
Ransomware Shield	Hlásenia o ransomware nie sú dostupné v ERA 6.x.	Hrozby ransomware sú hlásené ako hrozby HIPS od 7. a vyššej verzie bezpečnostných produktov ESET určených pre firmy.
ESET Dynamic Threat Defense	Integrácia s ESET Dynamic Threat Defense nie je možná v rámci ERA 6.x.	Integrácia s ESET Dynamic Threat Defense je dostupná pre bezpečnostné produkty ESET určené pre firmy verzie 7 – môžete odoslať súbory do ESET Dynamic Threat Defense na analýzu, pozrieť si podrobnosti o daných súboroch a dozvedieť sa výsledky analýzy malvéru. Môžete si tiež prezrieť zoznam všetkých súborov odoslaných na servery spoločnosti ESET.
Správa inventára hardvéru	V sekcii „Podrobnosti o počítači“ sú dostupné len základné informácie o hardvéri zariadenia.	Sú dostupné podrobné informácie o hardvéri pripojeného zariadenia. Môžete si vytvoriť vlastné správy o inventári hardvéru a dynamické skupiny na základe podrobností inventára hardvéru pripojených zariadení. Pre každý počítač s podporovaným operačným systémom je vytvorený hardvérový odtlačok. Tento odtlačok sa používa na identifikáciu počítačov po klonovaní.
Virtualizované prostredia	Podpora pre väčšinu nástrojov hypervisor, obmedzená podpora pre virtualizované prostredia (úloha „Obnoviť klonovaného agenta“).	Podpora pre VDI prostredia, automatická detekcia klonovania počítačov a zmien v hardvéri. Sú podporované systémy s non-perzistentnými diskami.
Inštalátory	K dispozícii sú možnosti lokálneho a vzdialeného nasadenia.	Možnosť vytvorenia all-in-one inštalátorov v rozhraní Web Console, pričom pribudla možnosť vytvorenia inštaláčného balíka pre samostatného ESET Management Agentu.
Replikačný protokol	ERA Agenty vyžadovali vo väčších sieťach ERA Proxy na agregáciu a preposielanie komunikácie na server.	ESET Management Agenty používajú vylepšený protokol, ktorý nevyžaduje agregáciu a komunikácia môže byť preposielaná pomocou proxy riešenia tretej strany.

Integrácia s nástrojom ESET Enterprise Inspector	ERA 6.5 zobrazuje hrozby hlásené nástrojom ESET Enterprise Inspector.	Hrozby zistené nástrojom ESET Enterprise Inspector je možné vyriešiť priamo z ESMC Web Console. K dispozícii je spoločné prihlásenie pre EEI a ESMC.
Mobile Device Connector	ERA MDM 6.5 umožňuje registráciu pre Android, iOS a iOS DEP. Sekcia „Podrobnosti o počítači“ pre mobilné zariadenia je podobná tej istej sekcii pre klientske počítače.	ESET Security Management Center MDM 7 podporuje registráciu zariadení v rámci režimu Vlastník zariadenia Android, čo umožňuje riešeniam ESET získať vyššie práva na správu zariadení. Sekcia „Podrobnosti o počítači“ pre mobilné zariadenia je odlišná od tej istej sekcie pre spravované počítače.

3. Systémové požiadavky

Existujú určité [hardvérové](#), [databázové](#) a [softvérové](#) podmienky, ktoré musia byť splnené pre inštaláciu produktu ESET Security Management Center a jeho správne fungovanie.

Bližšie informácie o [hardvérových požiadavkách](#) a [scenároch nasadenia](#) nájdete v predchádzajúcich kapitolách.

3.1 Podporované operačné systémy

V nasledujúcich častiach sú podľa konkrétnych komponentov nástroja ESET Security Management Center uvedené podporované verzie operačných systémov [Windows](#), [Linux](#) a [macOS](#), ako aj podporované verzie operačných systémov pre [mobilné zariadenia](#).

3.1.1 Windows

Nasledujúca tabuľka zobrazuje podporované operačné systémy Windows pre každý ESET Security Management Center komponent:

Operačný systém	Server	Agent	RD Sensor	MDM
Windows Home Server 2003 SP2		X	X	
Windows Home Server 2011 x64		X	X	
Windows Server 2003 x86 SP2		X	X	
Windows Server 2003 x64 SP2		X	X	
Windows Server 2003 x86 R2 SP2		X	X	
Windows Server 2003 x64 R2 SP2		X	X	
Windows Server 2008 x64 R2 SP1	X	X	X	X
Windows Server 2008 x64 R2 CORE	X	X	X	X
Windows Server 2008 x86 SP2		X	X	X***
Windows Server 2008 x64 SP2		X	X	X***
Windows Storage Server 2008 x64 R2	X	X	X	X
Windows Server 2012 x64	X	X	X	X
Windows Server 2012 x64 CORE	X	X	X	X
Windows Server 2012 x64 R2	X	X	X	X
Windows Storage Server 2012 x64 R2	X	X		
Windows Server 2012 x64 R2 CORE	X	X	X	X
Windows Storage Server 2012 x64 R2	X	X	X	X
Windows Server 2016 x64	X	X	X	X
Windows Storage Server 2016 x64	X	X	X	X
Microsoft SBS 2003 x86 SP2 **		X	X	
Microsoft SBS 2003 x86 R2 **		X	X	
Microsoft SBS 2008 x64 SP2 **		X	X	X
Microsoft SBS 2011 x64 Standard	X	X	X	X
Microsoft SBS 2011 x64 Essentials	X	X	X	X
Operačný systém	Server	Agent	RD Sensor	MDM

Windows XP x86 SP3		X	X	
Windows XP x64 SP2		X	X	
Windows Vista x86 SP2		X	X	
Windows Vista x64 SP2		X	X	
Windows 7 x86 SP1	X*	X	X	X*
Windows 7 x64 SP1	X*	X	X	X*
Windows 8 x86	X*	X	X	X*
Windows 8 x64	X*	X	X	X*
Windows 8.1 x86	X*	X	X	X*
Windows 8.1 x64	X*	X	X	X*
Windows 10 x86	X*	X	X	X*
Windows 10 x64	X*	X	X	X*

* Inštalácia súčastí ESMC na klientsky operačný systém nemusí byť v súlade s licenčnou politikou spoločnosti Microsoft. Overte si licenčnú politiku spoločnosti Microsoft, prípadne sa poraďte s vaším dodávateľom softvéru. V malých a stredne veľkých sieťach odporúčame zvážiť inštaláciu ESMC na systéme Linux, prípadne na [virtuálnom zariadení](#).

** Microsoft SQL Server Express ako súčasť Microsoft Small Business Server (SBS) nie je podporovaný produktom ESET Security Management Center. Ak sa rozhodnete používať ESMC databázu na vašom SBS, musíte použiť novšiu verziu Microsoft SQL Server Express alebo MySQL. Bližšie informácie a inštrukcie nájdete v časti [Inštalácia na Windows SBS/Essentials](#).

*** Inštalácia komponentu MDM je v rámci operačného systému Windows Server 2008 SP2 podporovaná len pomocou samostatného [all-in-one inštalátora](#).

Upozornenie: Staršie systémy MS Windows

- Na systéme Windows Server 2003 napríklad nie je zo strany systému plne podporované šifrovanie protokolov. V takýchto prípadoch bude použité TLSv1.0 namiesto TLSv1.2 (TLSv1.0 je považované za menej bezpečné ako novšie verzie). Tento problém môže tiež nastať, ak operačný systém podporuje TLSv1.2, ale klient ho nepodporuje. V takom prípade bude komunikácia prebiehať pomocou TLSv1.0. Na zaistenie najbezpečnejšej komunikácie odporúčame používať novšie operačné systémy (minimálne Windows Server 2008 R2 pre server a Windows Vista pre klienty).
- Vždy majte nainštalovaný najnovší balík service pack, obzvlášť na starších systémoch, ako Server 2003, 2008, Windows XP a Windows Vista.
- Pre správne fungovanie nástroja ESMC Web Console je potrebná Java vo verzii 8. Pozrite si oficiálny zoznam [podporovaných operačných systémov](#).

Poznámka:

Je možné nainštalovať [VMware Player](#) na klientsky operačný systém a nasadiť [virtuálne zariadenie ESMC](#). To vám umožní používať ESET Security Management Center na operačnom systéme, ktorý nie je určený pre servery, bez potreby vlastniť virtuálne prostredie VMware ESXi.

3.1.2 Linux

Nasledujúca tabuľka zobrazuje podporované operačné systémy Linux pre každý ESET Security Management Center komponent:

Operačný systém	Server	Agent	RD Sensor	MDM
Ubuntu 12.04 LTS x86 Desktop	X	X	X	X
Ubuntu 12.04 LTS x86 Server	X	X	X	X
Ubuntu 12.04 LTS x64 Desktop	X	X	X	X
Ubuntu 12.04 LTS x64 Server	X	X	X	X
Ubuntu 14.04 LTS x86 Desktop	X	X	X	X
Ubuntu 14.04 LTS x86 Server	X	X	X	X
Ubuntu 14.04 LTS x64 Desktop	X	X	X	X
Ubuntu 14.04 LTS x64 Server	X	X	X	X
Ubuntu 16.04.1 LTS x86 Desktop	X	X	X	X
Ubuntu 16.04.1 LTS x86 Server	X	X	X	X
Ubuntu 16.04.1 LTS x64 Desktop	X	X	X	X
Ubuntu 16.04.1 LTS x64 Server	X	X	X	X
RHEL 5 x86		X		
RHEL 5 x64		X		
RHEL Server 6 x86	X	X	X	X
RHEL Server 6 x64	X	X	X	X
RHEL Server 7 x86	X	X	X	X
RHEL Server 7 x64	X	X	X	X
CentOS 5 x86		X		
CentOS 5 x64		X		
CentOS 6 x86	X	X	X	X
CentOS 6 x64	X	X	X	X
CentOS 7 x86	X	X	X	X
CentOS 7 x64	X	X	X	X
SLED 11 x86	X	X	X	X
SLED 11 x64	X	X	X	X
SLED 12 x86	X	X	X	X
SLED 12 x64	X	X	X	X
SLES 11 x86	X	X	X	X
SLES 11 x64	X	X	X	X
SLES 12 x86	X	X	X	X
SLES 12 x64	X	X	X	X
OpenSUSE 13 x86	X	X	X	X
OpenSUSE 13 x64	X	X	X	X
Debian 7 x86	X	X	X	X
Debian 7 x64	X	X	X	X
Debian 8 x86	X	X	X	X
Debian 8 x64	X	X	X	X

Fedora 19 x86	X	X	X	X
Fedora 19 x64	X	X	X	X
Fedora 20 x86	X	X	X	X
Fedora 20 x64	X	X	X	X
Fedora 23 x86	X	X	X	X
Fedora 23 x64	X	X	X	X

3.1.3 macOS

Operačný systém	Agent
OS X 10.7 Lion	X
OS X 10.8 Mountain Lion	X
OS X 10.9 Mavericks	X
OS X 10.10 Yosemite	X
OS X 10.11 El Capitan	X
macOS 10.12 Sierra	X
macOS 10.13 High Sierra	X

Poznámka:

MacOS je podporovaný len ako klient. [ESET Management Agent](#) a [produkty spoločnosti ESET pre macOS](#) môžu byť nainštalované na macOS, avšak ESMC Server na macOS nainštalovaný byť nemôže.

3.1.4 Mobilné zariadenia

Operačný systém	EESA	EESA – režim Vlastník zariadenia	MDM iOS	MDM iOS DEP
Android v5.x+	x			
Android v6.x+	x			
Android v7.x+	x	x		
Android v8.x+	x	x		
iOS 9.x+			x	x
iOS 10.x+			x	x
iOS 11.x+			x	x

* Služba iOS DEP je dostupná len vo [vybraných krajinách](#).

Dôležité:

Odporúčame udržiavať operačný systém vášho mobilného zariadenia vždy v najnovšej verzii, aby bolo možné dostávať dôležité bezpečnostné aktualizácie.

3.2 Podporované Desktop Provisioning prostredia

Desktop Provisioning predstavuje spôsob, ako čo najrýchlejšie a najjednoduchšie spravovať zariadenia a poskytnúť počítač koncovému používateľovi.

Provisioned prostredia sú zvyčajne fyzické alebo virtuálne. Pre virtualizované prostredia využívajúce tzv. OS-streaming (provisioning služby od spoločnosti Citrix) si pozrite nižšie uvedený zoznam podporovaných nástrojov hypervisor a ich rozšírení.

ESET Security Management Center verzie 7 a novšej [podporuje](#):

- systémy s non-perzistentnými diskami,
- VDI prostredia,
- identifikáciu klonovaných počítačov.

Podporované nástroje hypervisor

- Citrix XenServer
- Microsoft Hyper-V
- VMware vSphere
- VMware ESXi
- VMware Workstation
- VMware View

Podporované rozšírenia nástrojov hypervisor

- Citrix VDI-in-a-box
- Citrix XenDesktop

Nástroje

(platí pre virtuálne aj fyzické počítače)

- Microsoft SCCM
- Windows Server 2012 Server Manager

3.3 Hardvér

Pre bezproblémový chod produktu ESET Security Management Center je potrebné splniť nasledujúce hardvérové požiadavky:

Pamäť	4 GB RAM
Pevný disk	Minimálne 20 GB voľného miesta
Procesor	Dvojjadrový, s taktom aspoň 2,0 GHz
Sieťové pripojenie	1 Gbit/s

3.4 Databáza

ESET Security Management Center podporuje dva druhy databázových serverov:

- Microsoft SQL Server (vrátane edície Express a ostatných štandardných edícií) 2008, 2008 R2, 2012, 2014, 2016, 2017
- MySQL (verzie 5.5 a novšie, dôrazne však odporúčame používať aspoň verziu 5.6)

Databázový server si môžete vybrať pri inštalácii ESMC Servera. Microsoft SQL Server Express sa podľa predvolených nastavení nainštaluje a je súčasťou [all-in-one inštalátora](#). Môžete používať vlastný Microsoft SQL Server spustený vo vašom prostredí, musí však spĺňať minimálne požiadavky.

Požiadavky na hardvér databázového servera:

Pamäť	2 GB RAM
Pevný disk	Minimálne 10 GB voľného miesta
Rýchlosť procesora	Procesor typu x86: 1,3 GHz Procesor typu x64: 1,6 GHz POZNÁMKA: Pre optimálny výkon je odporúčaný procesor s taktom aspoň 2,0 GHz.
Typ procesora	Procesor typu x86: Pentium IV-kompatibilný procesor a rýchlejší Procesor typu x64: AMD Opteron, AMD Athlon 64, Intel Xeon s podporou Intel EM64T, Intel Pentium IV s podporou EM64T

Ďalšie informácie

- **Microsoft SQL Server Express má veľkosť obmedzenú na 10 GB** pre každú relačnú databázu a nemôže byť nainštalovaný na doménový riadič. Neodporúčame používať Microsoft SQL Server Express vo veľkých sieťach alebo podnikoch. Ak používate [Microsoft SBS](#), odporúčame vám nainštalovať ESET Security Management Center na iný server alebo [neoznačiť SQL Server Express komponent](#) počas inštalácie (toto vyžaduje existujúci SQL alebo MySQL server pre spustenie ESMC databázy).
- Ak plánujete použiť **vyhradený používateľský účet databázy**, ktorý bude mať prístup len do ESMC databázy, musíte pred inštaláciou vytvoriť používateľský účet so špecifickými oprávneniami. Bližšie informácie nájdete v časti [Vyhradený používateľský účet databázy](#). Budete takisto musieť vytvoriť prázdnu databázu, ktorú bude ESET Security Management Center využívať.
- Pozrite si tiež inštrukcie, ako nainštalovať a nakonfigurovať [MySQL pre Windows](#) a [MySQL pre Linux](#) tak, aby bolo zabezpečené ich správne fungovanie s nástrojom ESET Security Management Center. Berte na vedomie, že databázový server MariaDB **nie je podporovaný** nástrojom ESET Security Management Center.
- [MS SQL Server](#) pre Linux nie je podporovaný.
- **ESMC Server nevykonáva zálohu databázy**. V rámci zníženia rizika straty dát odporúčame preto pravidelne [zálohovať](#) databázový server.

3.5 Podporované verzie Apache Tomcat

Podporovaný je Apache Tomcat 7.x a novšie verzie (32-bitová aj 64-bitová verzia). Apache Tomcat je nevyhnutný komponent potrebný pre fungovanie nástroja ESMC Web Console.

ESET Security Management Center nepodporuje alfa/beta/RC verzie Apache Tomcat.

3.6 Sieť

Je dôležité, aby ESMC Server aj klientske počítače spravované nástrojom ESMC mali internetové pripojenie, aby bol zabezpečený prístup na repozitáre a aktivačné servery spoločnosti ESET. Ak si neželáte, aby boli klientske počítače pripojené na internet priamo, môžete použiť proxy server (avšak nie rovnaký ako Apache HTTP Proxy) pre umožnenie komunikácie s vašou sieťou a internetom.

Počítače spravované nástrojom ESMC by sa mali pripájať na rovnakú sieť LAN a by mali byť v rovnakej doméne služby *Active Directory* ako váš ESMC Server. ESMC Server musí byť viditeľný pre klientske počítače. Navyše, klientskym počítačom musí byť umožnená komunikácia s vaším ESMC Serverom pre vzdialené nasadenie a funkciu pokynu na zobudenie.

Používané porty

Ak vaša sieť používa firewall, pozrite si náš zoznam možných [portov sieťovej komunikácie](#), ktoré sa používajú, keď je vo vašej infraštruktúre nainštalovaný ESET Security Management Center a jeho súčasti.

3.6.1 Používané porty

Nižšie uvedené tabuľky obsahujú všetky porty, ktoré pri sieťovej komunikácii využíva ESET Security Management Center a jeho súčasti. Ostatná komunikácia prebieha cez štandardné procesy operačného systému (napríklad NetBIOS cez TCP/IP).

ESMC Server:

Protokol	Port	Použitie	Popis
TCP	2222	ESMC Server načúva	Komunikácia medzi ESET Management Agentmi a ESMC Serverom
TCP	2223	ESMC Server načúva	Komunikácia medzi ESMC Web Console a ESMC Serverom, používaná na asistovanú inštaláciu

ESMC Web Console bežiaci na Apache Tomcat:

Protokol	Port	Použitie	Popis
TCP	443	Načúva	HTTP SSL Web Console volanie

Apache HTTP Proxy:

Protokol	Port	Použitie	Popis
TCP	3128	Načúva	Apache HTTP Proxy (ukladanie aktualizácií do vyrovnávacej pamäte a replikácia)

ESET Management Agent:

Protokol	Port	Použitie	Popis
MQTT	8883	Načúva	Komunikácia s EPNS Serverom (volania na prebudenie)
TCP	2222		Komunikácia s ESMC Serverom

Mobile Device Connector:

Protokol	Port	Použitie	Popis
TCP	9977		Interná komunikácia medzi ESET Management Agentmi a nástrojom Mobile Device Connector

Protokol	Port	Použitie	Popis
TCP	9978		Interná komunikácia medzi ESET Management Agentmi a nástrojmi Mobile Device Connector
TCP	9980	Načúva	Registrácia mobilných zariadení
TCP	9981	Načúva	Komunikácia mobilných zariadení
TCP	5223		Externá komunikácia so službou Apple Push Notification
TCP	2195		Odosielanie oznámení služby Apple Push Notification
TCP	2196		Služba spätnej väzby Apple Push Notification
TCP	443		Možnosť prepnutia na Wi-Fi, keď zariadenie nedokáže nadviazať spojenie so servermi APN na porte 5223. Pripojenie zariadenia s operačným systémom Android ku GCM serveru. Pripojenie k licenčnému serveru ESET. Pripojenie zariadenia s operačným systémom Android k licenčnému portálu (edf.eset.com).
TCP	5228, 5229, 5230		Odosielanie oznámení do Google Cloud Messaging

ESET Management Agent – využitie pri vzdialenom nasadení ESET Management Agentu na cieľové počítače s operačným systémom Windows:

Protokol	Port	Použitie	Popis
TCP	139	Cieľový port zo strany komponentu ESMC Server	Zdieľanie ADMIN\$
TCP	445	Cieľový port zo strany komponentu ESMC Server	Priamy prístup k zdieľaným zdrojom pomocou TCP/IP počas vzdialenej inštalácie (alternatíva k TCP 139)
UDP	137	Cieľový port zo strany komponentu ESMC Server	Preklad IP adries počas vzdialenej inštalácie
UDP	138	Cieľový port zo strany komponentu ESMC Server	Prehľadávanie počas vzdialenej inštalácie

Vopred definované porty 2222 a 2223 môžu byť zmenené, ak sú používané inými aplikáciami.

i Poznámka:

- Pre správne fungovanie nástroja ESET Security Management Center sa uistite, že žiadne z uvedených portov nie sú používané inými aplikáciami.
- Uistite sa, že váš firewall je nastavený tak, aby povoľoval komunikáciu cez tieto porty.

4. Inštalácia

! Dôležité:

Inštrukcie týkajúce sa aktualizácie vašej súčasnej verzie nástroja ESMC nájdete v kapitole [Aktualizácia, migrácia a preinštalovanie](#).

Inštalátory nástroja ESET Security Management Center sú dostupné k stiahnutiu na [webovej stránke spoločnosti ESET](#) v sekcii Stiahnuť ESET Security Management Center. Sú dostupné v niekoľkých formách. Štandardne je vybraná karta **All-in-one inštalátor**. Ak si prajete stiahnuť virtuálne zariadenie alebo samostatný inštalátor, kliknite na príslušnú kartu. Sú dostupné tieto možnosti:

- [All-in-one inštalátor](#) nástroja ESMC pre systém Windows (zip súbor).
- Obraz ISO, ktorý obsahuje všetky inštalátory nástroja ESET Security Management Center (okrem virtuálneho zariadenia ESMC).
- Súbor (OVA) virtuálneho zariadenia. Nasadenie virtuálneho zariadenia ESMC sa odporúča pre používateľov, ktorí chcú používať ESET Security Management Center vo virtuálnom prostredí alebo dávajú prednosť jednoduchšej inštalácii. Podrobné inštrukcie nájdete v [príručke nasadenia virtuálneho zariadenia ESMC](#).
- Samostatné inštalátory pre individuálne komponenty – pre [Windows](#) a [Linux](#).

Ďalšie metódy inštalácie:

- [Inštalácia na Microsoft Azure](#)
- Podrobné inštrukcie pre [inštaláciu na systéme Linux](#)

! Dôležité:

Po inštalácii nemeňte názov počítača, na ktorom beží ESMC Server. Viac informácií nájdete v kapitole [Zmena názvu hostiteľa alebo IP adresy ESMC Servera](#).

Prehľad inštaláčnych metód

i Poznámka:

Prečítajte si tiež kapitolu [Škálovateľnosť ESMC infraštruktúry](#).

Ak potrebujete pomôcť s výberom toho najvhodnejšieho spôsobu inštalácie nástroja ESET Security Management Center, môžete sa obrátiť na nasledujúcu tabuľku, vďaka ktorej ľahko zistíte, aká inštaláčna metóda bude pre vaše konkrétne prostredie najlepšia:

Napríklad: Nevyberajte si inštaláciu nástroja ESMC na cloud (napríklad na cloudovú platformu Windows Azure) v prípade, že je vaše internetové pripojenie pomalé.

Napríklad: Ak plánujete použiť nástroj ESMC v prostredí malého alebo stredného podniku (MSP), vyberte si all-in-one inštaláciu.

Metóda inštalácie	Typ zákazníka		Migrácia		Prostredie pre inštaláciu nástroja ESMC					Internetové pripojenie		
	Malé a stredné podniky (MSP)	Veľké podniky	Áno	Nie	Bez servera	Vyhradený server	Zdieľaný server	Virtualizačná platforma	Cloudový server	Žiadne	Dobré	Slabé
All-in-one inštalácia na Windows Server	X	X	X			X	X		X	X	X	X

All-in-one inštalácia na Windows Desktop	X		X		X				X	X	X
Virtuálne zariadenie	X		X					X	X	X	X
Microsoft Azure VM	X			X				X		X	
Inštalácia komponentov – Linux		X	X			X	X	X	X	X	X
Inštalácia komponentov – Windows		X	X			X	X	X	X	X	X

4.1 All-in-one inštalácia na systéme Windows

ESET Security Management Center môže byť nainštalovaný rôznymi spôsobmi. Zvoľte si typ inštalácie, ktorá je najvhodnejšia pre vaše prostredie. Najjednoduchší spôsob je použiť all-in-one inštalátor nástroja ESET Security Management Center. Táto metóda umožňuje nainštalovať ESMC a jeho súčasti na jeden počítač.

Inštalácia komponentov (súčastí) umožňuje nainštalovať rôzne komponenty nástroja ESET Security Management Center na rôzne počítače. To vám umožňuje prispôbiť si inštaláciu. Môžete nainštalovať každý komponent na akýkoľvek počítač za predpokladu, že daný počítač spĺňa systémové požiadavky.

ESMC môžete nainštalovať pomocou:

- all-in-one inštalácie – [ESMC Server](#), [Apache HTTP Proxy](#) alebo [Mobile Device Connector](#),
- [samostatných inštalátorov](#) pre súčasti ESMC (inštalácia komponentov).

Vlastné inštalčné scenáre zahŕňajú:

- inštaláciu na [Windows Small Business Server/Essentials](#),
- inštaláciu s [vlastnými certifikátmi](#),
- inštaláciu na [Failover klaster](#).

Väčšina inštalčných scenárov vyžaduje inštaláciu rôznych komponentov nástroja ESET Security Management Center na rôzne počítače v závislosti od sieťovej architektúry, výkonnostných požiadaviek atď. Pre jednotlivé komponenty nástroja ESET Security Management Center sú dostupné nasledujúce inštalčné balíky:

Základné súčasti

- [ESMC Server](#)
- [ESMC Web Console](#)
- [ESET Management Agent](#) – musí byť nainštalovaný na klientských počítačoch, voliteľne aj na ESMC Serveri.

Voliteľné súčasti

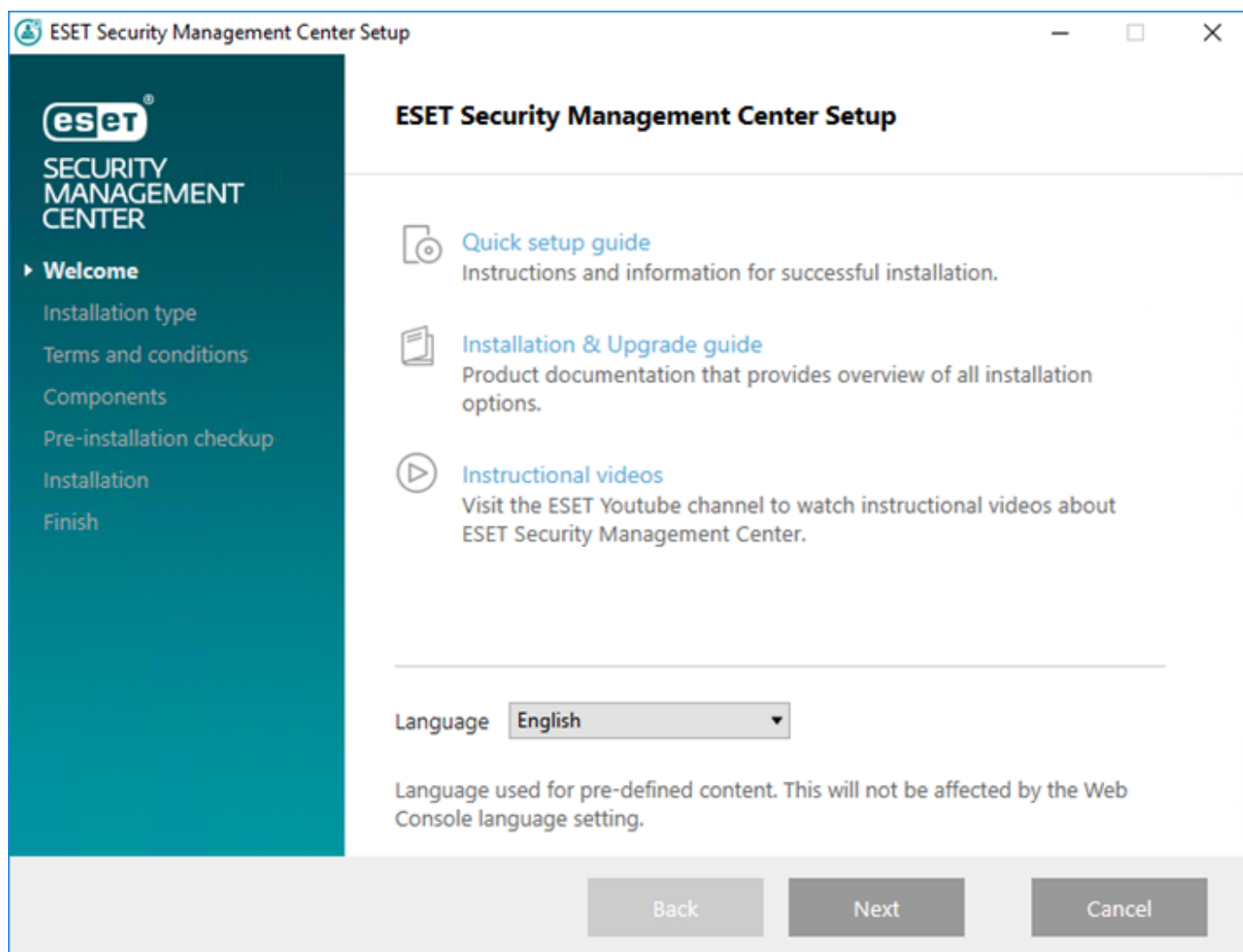
- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Apache HTTP Proxy](#)
- [Mirror Tool](#)

Ak chcete aktualizovať ESET Remote Administrator na najnovšiu verziu (ESMC 7.0), prečítajte si náš [článok databázy znalostí](#).

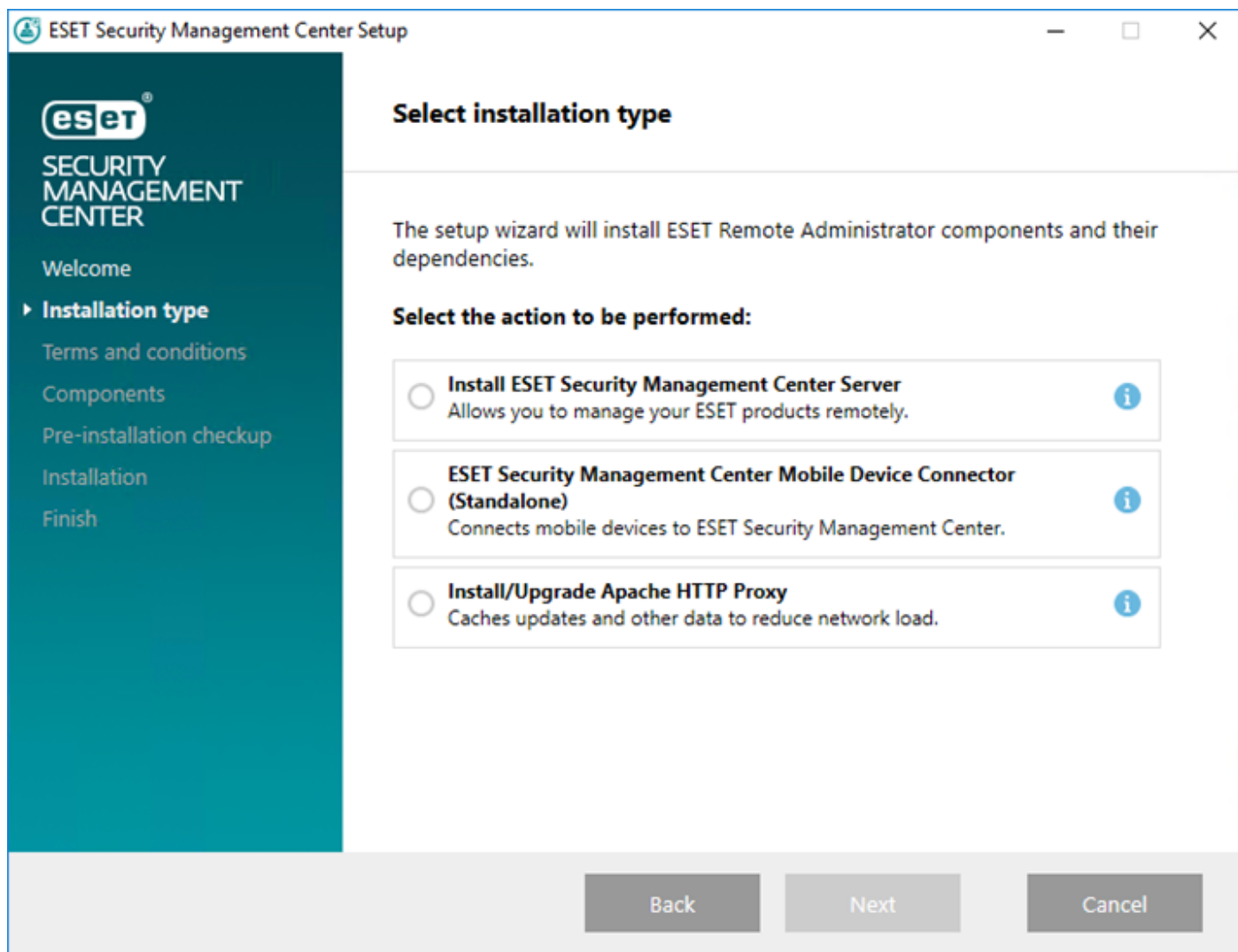
4.1.1 Inštalácia ESMC Servera

[All-in-one inštalátor nástroja ESMC](#) je dostupný len pre operačné systémy Windows. Tento inštalátor vám umožňuje nainštalovať všetky súčasti nástroja ESMC prostredníctvom sprievodcu.

1. Spustíte inštalračný balík a na úvodnej obrazovke kliknete na tlačidlo **Ďalej**. Predtým, ako budete pokračovať, môžete v prípade potreby zmeniť nastavenie jazyka v roletovom menu **Jazyk**.



2. Zvoľte možnosť **Nainštalovať ESET Security Management Server** a kliknite na **Ďalej**.



3. 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.
4. Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**. Vyberte požadované súčasti nástroja ESMC a kliknite na **Inštalovať**.

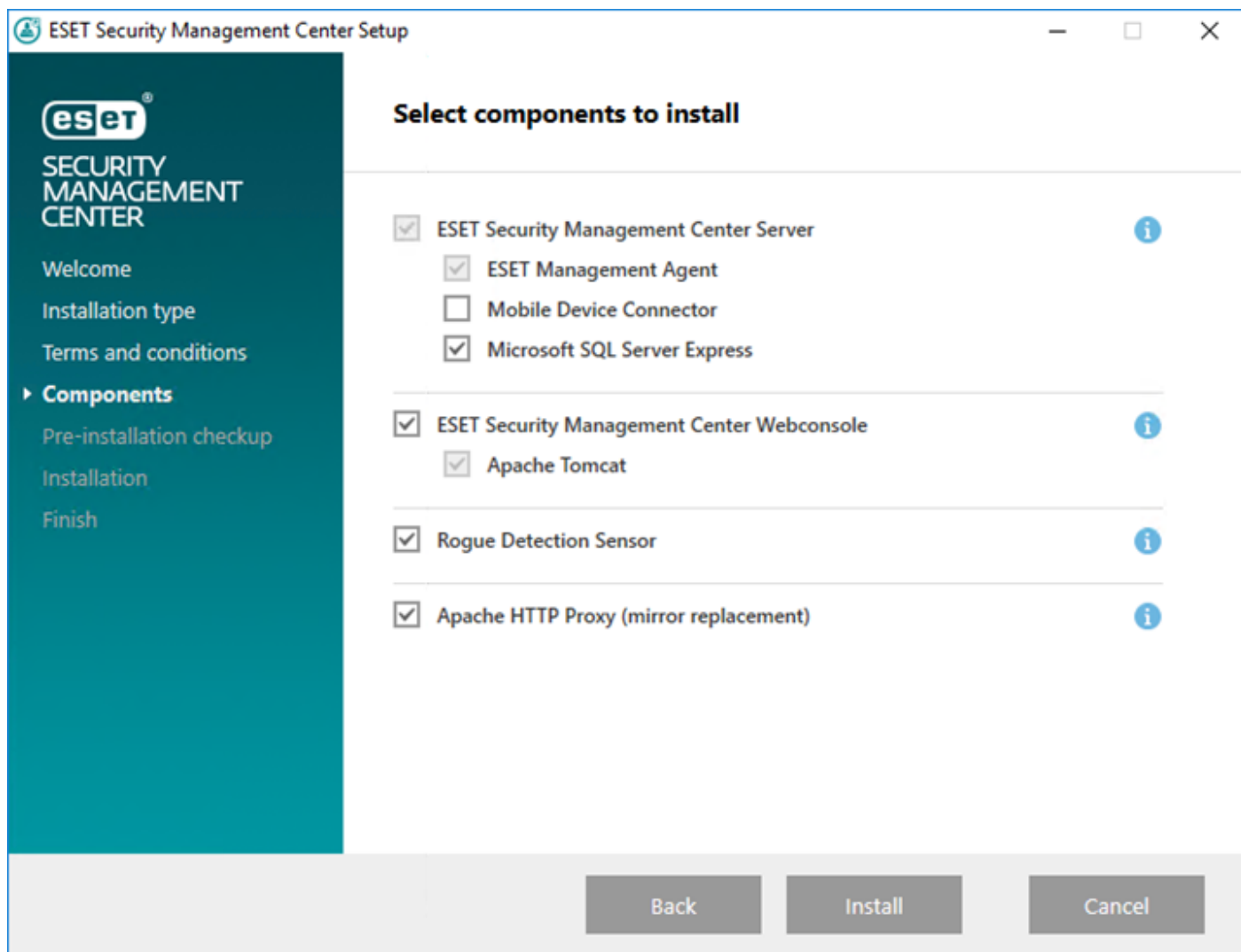
Microsoft SQL Server Express:

- Ak už máte nainštalovanú inú verziu Microsoft SQL servera alebo MySQL, alebo plánujete pripojenie na iný SQL server, zrušte výber tohto komponentu.
- Nebudete môcť nainštalovať Microsoft SQL Server Express na doménový radič (Domain Controller), napríklad ak používate Windows SBS/Essentials. Odporúčame vám nainštalovať ESET Security Management Center na iný server, prípadne použiť Microsoft SQL Server alebo MySQL Server pre spustenie ESMC databázy. Pre viac informácií kliknite [sem](#).

! DÔLEŽITÁ INFORMÁCIA O APACHE HTTP PROXY:

Možnosť **Apache HTTP Proxy** je určená len pre menšie alebo centralizované siete, bez roamingových klientov. Ak je táto možnosť označená, klienty budú predvolene nastavené tak, aby prepájali komunikáciu s ESET prostredníctvom služby proxy spustenej na rovnakom počítači ako ESMC Server. Toto spojenie nebude fungovať, ak medzi klientmi a ESMC Serverom nie je priama sieťová viditeľnosť.

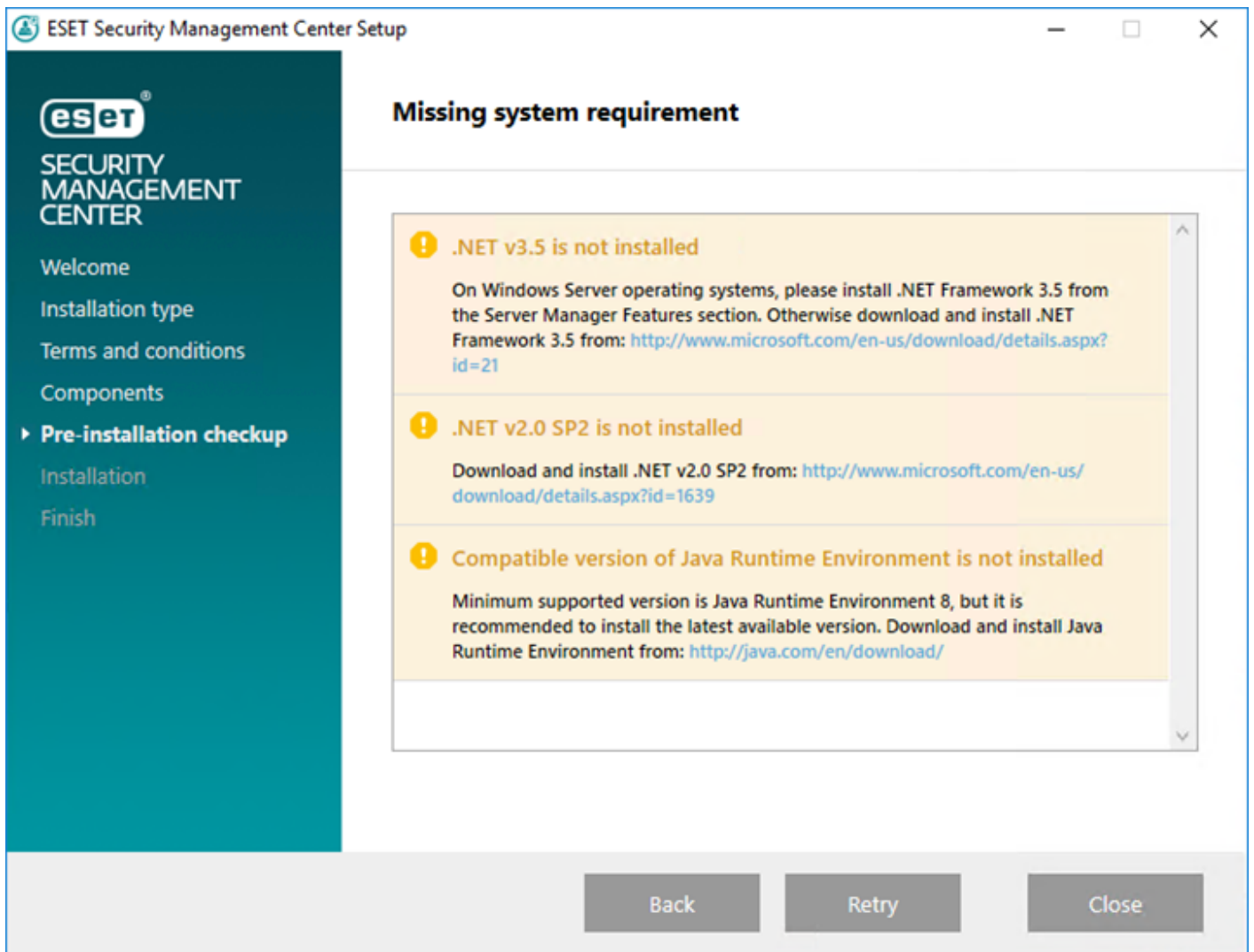
- Pre viac informácií si prečítajte kapitoly o [Apache HTTP Proxy](#) a o [rozdieloch medzi Apache HTTP Proxy, nástrojom Mirror Tool a priamym pripojením na internet](#).



Označte možnosť **Apache HTTP Proxy** pre inštaláciu Apache HTTP Proxy a pre vytvorenie a aplikovanie politík (pod názvom **Využitie HTTP proxy** a s aplikovaním na skupinu **Všetko**) pre nasledujúce produkty:

- ESET Endpoint pre Windows
- ESET Endpoint pre macOS (OS X) a Linux
- ESET Management Agent
- ESET File Security pre Windows Server (V6+)
- ESET Shared Local Cache
- Vytvorená politika aktivuje HTTP Proxy pre príslušné produkty. Ako hostiteľ proxy sa nastaví lokálna IP adresa ESMC Servera a port 3128. Autentifikácia nebude aktívna. V prípade potreby môžete tieto nastavenia skopírovať do iných politík a použiť ich pre ďalšie produkty.
- Používanie HTTP Proxy môže zredukovať množstvo dát stiahnutých z internetu a zvýšiť rýchlosť sťahovania aktualizácií. Odporúčame označiť možnosť **Apache HTTP Proxy**, ak plánujete prostredníctvom nástroja ESMC spravovať viac ako 37 počítačov. Ak chcete, môžete [Apache HTTP Proxy nainštalovať](#) aj neskôr.

4. Ak sú počas kontroly zistené chyby, opravte ich. Uistite sa, že váš systém spĺňa všetky [prerekvizity](#).



Ak nemáte na disku dostatok miesta pre inštaláciu ESMC, môže sa zobrazíť nasledujúce oznámenie:

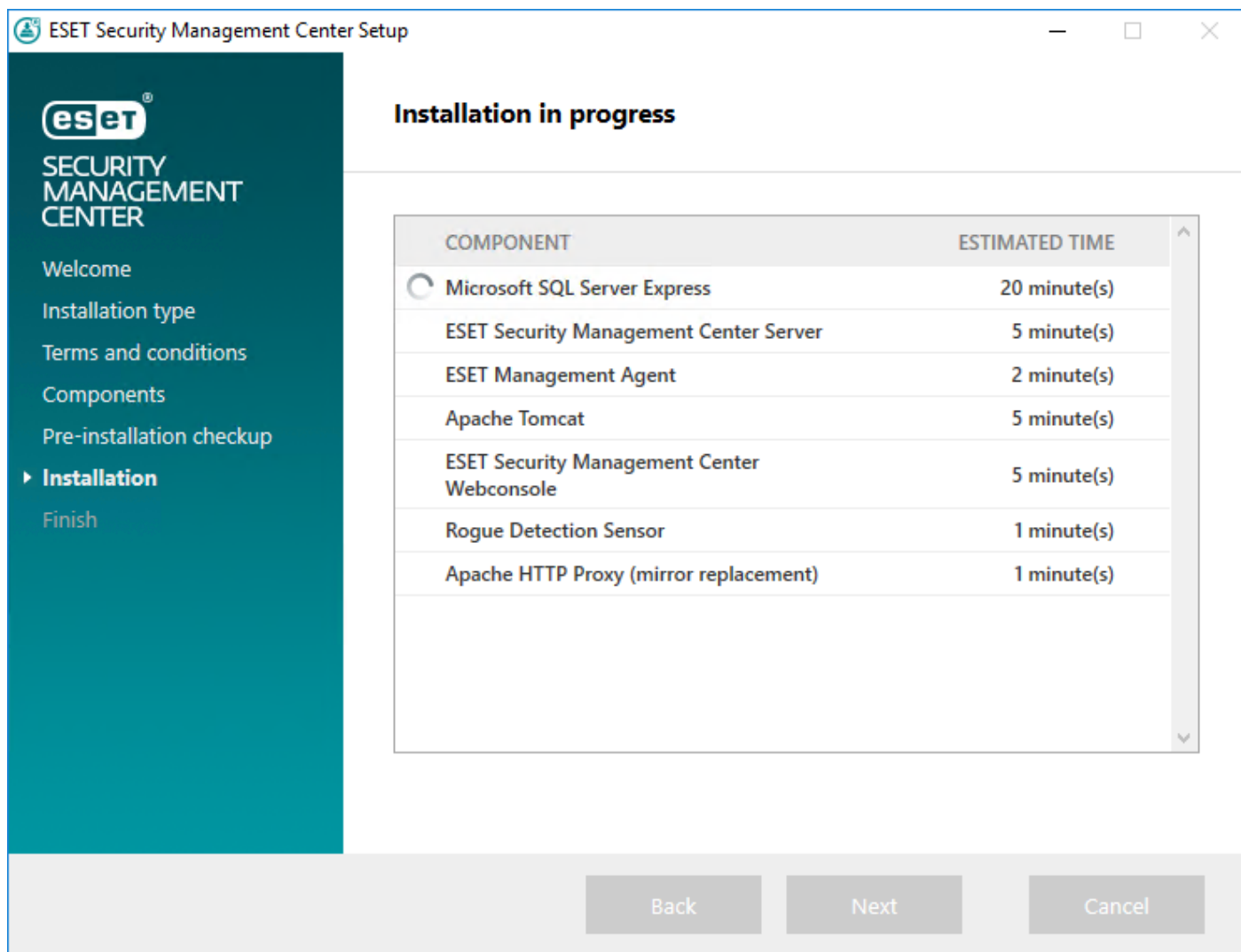
⚠ Na disku je voľných len 32 MB.

Pre inštaláciu ESMC musí byť na disku aspoň 5000 MB voľného miesta.

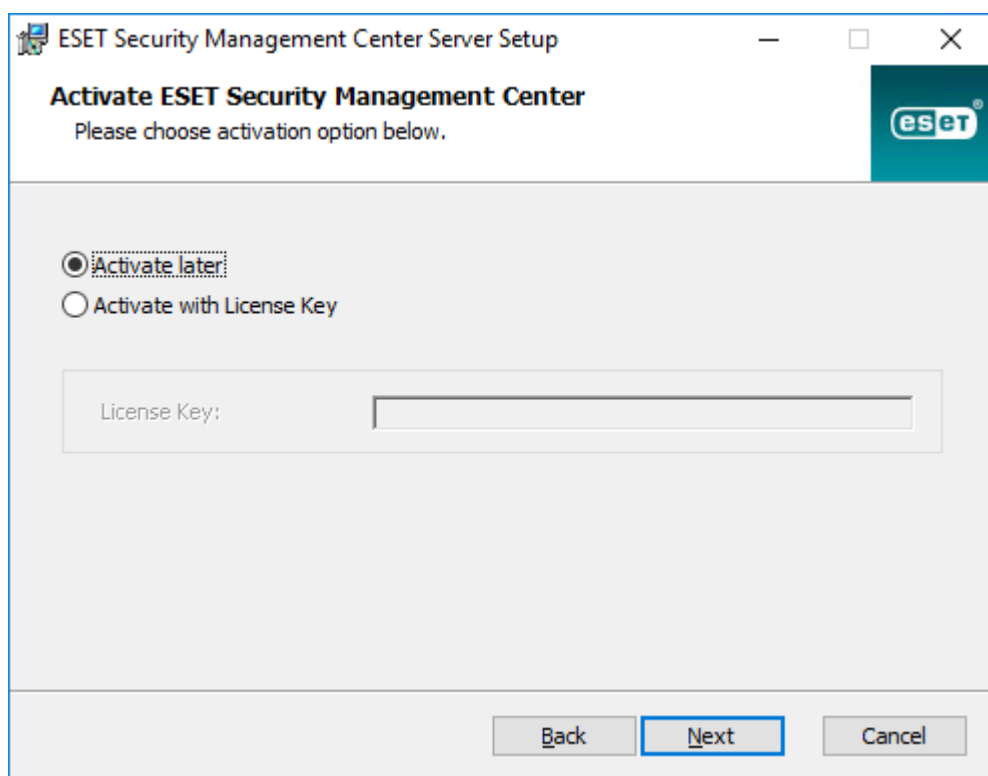
5. Keď skončí kontrola prerekvizít a vaše prostredie spĺňa všetky [požiadavky](#), začne sa inštalácia.

i Poznámka:

Ak práve prebieha inštalácia, sprievodca inštaláciou nástroja ESMC nereaguje a nie je možné ho ovládať.



6. Zadať platný **Licenčný kľúč** (je súčasťou e-mailu o kúpe produktu, ktorý ste dostali od spoločnosti ESET) a kliknite na **Ďalej**. Ak používate staršie licenčné údaje (používateľské meno a heslo), [prekonvertujte](#) tieto údaje na licenčný kľúč. Môžete tiež zvoliť možnosť **Aktivovať neskôr**. Ak zvolíte možnosť **Aktivovať neskôr**, prečítajte si kapitolu [Aktivácia](#) pre podrobnejšie inštrukcie.



7. Ak ste si v kroku 2 zvolili inštaláciu **Microsoft SQL Server Express**, bude vykonaná kontrola pripojenia databázy – prejdite na krok č. 9 ([Používateľ Web Console & pripojenie k serveru](#)). Ak už máte spustený databázový server, budete v ďalšom kroku zadávať údaje potrebné na pripojenie k tomuto serveru.
8. Ak používate existujúci SQL Server alebo MySQL, zadajte nastavenia pripojenia. Zadajte **Názov databázy**, **Názov hostiteľa**, číslo **Portu** (tieto informácie môžete nájsť v nástroji Microsoft SQL Server Configuration Manager) a údaje **Účtu databázy (Prihlasovacie meno a Heslo)** do príslušných polí a kliknite na **Ďalej**. Následne bude overený prístup k databáze. Ak už máte ESMC databázu (z predošlej inštalácie ERA 6) na vašom databázovom serveri, bude táto skutočnosť zistená. Môžete zvoliť možnosť **Použiť existujúcu databázu a aplikovať aktualizáciu** alebo možnosť **Odstrániť existujúcu databázu a nainštalovať novú verziu**.

Použití inštanciu s názvom – ak používate MS SQL databázu, môžete označiť možnosť **Použití inštanciu s názvom**. Následne budete môcť použiť vlastnú inštanciu databázy zadaním názvu hostiteľa v tvare *HOSTNAME\DB_INSTANCE*, napríklad: *192.168.0.10\ESMC7SQL*. Pre klastrovú databázu použijete len názov klastra. Ak je zvolená táto možnosť, nebude možné zmeniť port, ktorý bude použitý – systém použije porty predvolené spoločnosťou Microsoft.

i Poznámka:

Ak zvolíte možnosť **Použití inštanciu s názvom**, ESMC Server môžete pripojiť aj k MS SQL databáze, ktorá je nainštalovaná na Failover klastri. Do poľa **Názov hostiteľa** zadajte názov klastra.

i Poznámka:

Existujú dve možnosti zadania údajov **Účtu databázy**. Môžete použiť **vyhradený používateľský účet databázy**, ktorý bude mať prístup len do ESMC databázy, prípadne **SA účet** (MS SQL) alebo **root účet** (MySQL). Keď sa rozhodnete, že chcete použiť vyhradený používateľský účet, musí byť tento účet vytvorený s určitými právami. Bližšie informácie nájdete v časti [Vyhradený používateľský účet databázy](#). Ak neplánujete použiť vyhradený používateľský účet, zadajte účet správcu (SA alebo root).

ESET Security Management Center Server Setup

Database server connection
Please enter database server connection.

Database: MS SQL Server

ODBC driver: MS SQL Server

Database name: jera_db

Hostname: localhost

Use Named Instance:

Port: 1433

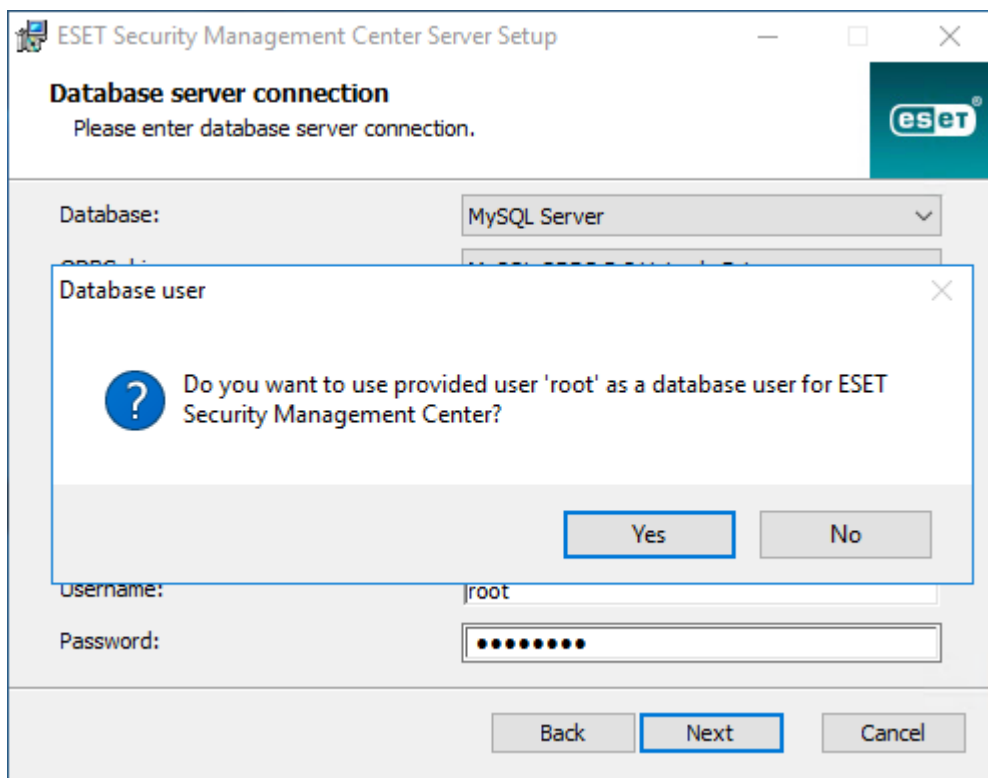
Database account

Username:

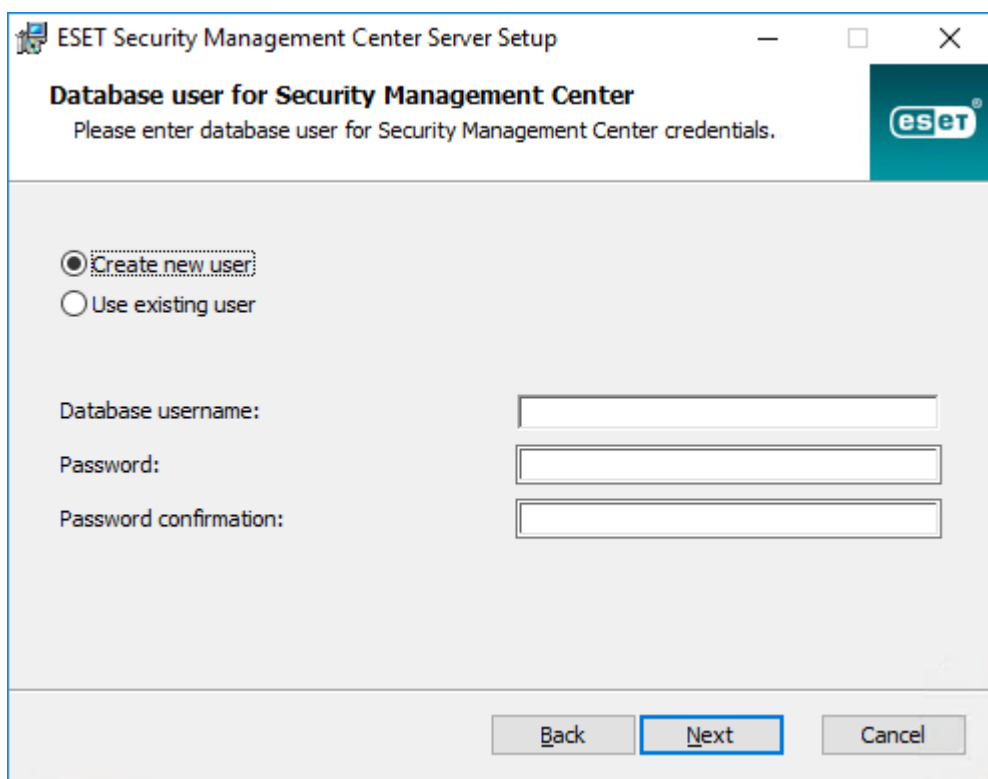
Password:

Back Next Cancel

Ak ste v predchádzajúcom okne zadali **SA účet** alebo **root účet**, kliknite na **Áno** pre pokračovanie v používaní účtu SA/root ako používateľ databázy pre ESET Security Management Center.



Ak kliknete na **Nie**, musíte vybrať možnosť **Vytvoriť nového používateľa** alebo **Použiť existujúceho používateľa** (ak máte vyhradený používateľský účet databázy, ako sa spomína [tu](#)).



9. Budete vyzvaný na zadanie hesla účtu správcu Web Console. Toto heslo je dôležité, pretože ho budete používať na prihlásenie do [ESMC Web Console](#). Kliknite na **Ďalej**.

The screenshot shows the 'Web Console user & server connection' step of the ESET Security Management Center Server Setup. The window title is 'ESET Security Management Center Server Setup'. The subtitle is 'Web Console user & server connection' and the instruction is 'Please enter Web Console user password and server connection.' The ESET logo is in the top right corner. The form contains the following fields: 'Web Console user:' with the value 'Administrator'; 'Password:' and 'Password confirmation:' both with masked input fields (dots); 'Agent port:' with the value '2222'; and 'Console port:' with the value '2223'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

10. Tieto polia môžete nechať nevyplnené, prípadne môžete vyplniť podnikové údaje, ktoré sa zobrazia v podrobnostiach certifikátov ESET Management Agent a ESMC Servera. Ak sa rozhodnete zadať heslo do poľa **Heslo authority**, uistite sa, že si ho zapamätáte. Kliknite na **Ďalej**.

The screenshot shows the 'Certificate information' step of the ESET Security Management Center Server Setup. The window title is 'ESET Security Management Center Server Setup'. The subtitle is 'Certificate information' and the instruction is 'Please enter common certificate information below.' The ESET logo is in the top right corner. The form contains the following fields: 'Organizational unit:', 'Organization:', 'Locality:', 'State / Country:', 'Certificate validity: *' (with a value of '10' and a 'Years' dropdown), 'Authority common name: *' (with the value 'Server Certification Authority'), and 'Authority password:'. At the bottom left, there is a note '* required fields'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted with a blue border), and 'Cancel'.

11. Zobrazia sa informácie o priebehu inštalácie.



SECURITY MANAGEMENT CENTER

Welcome

Installation type

Terms and conditions

Components

Pre-installation checkup

► **Installation**

Finish

Installation in progress

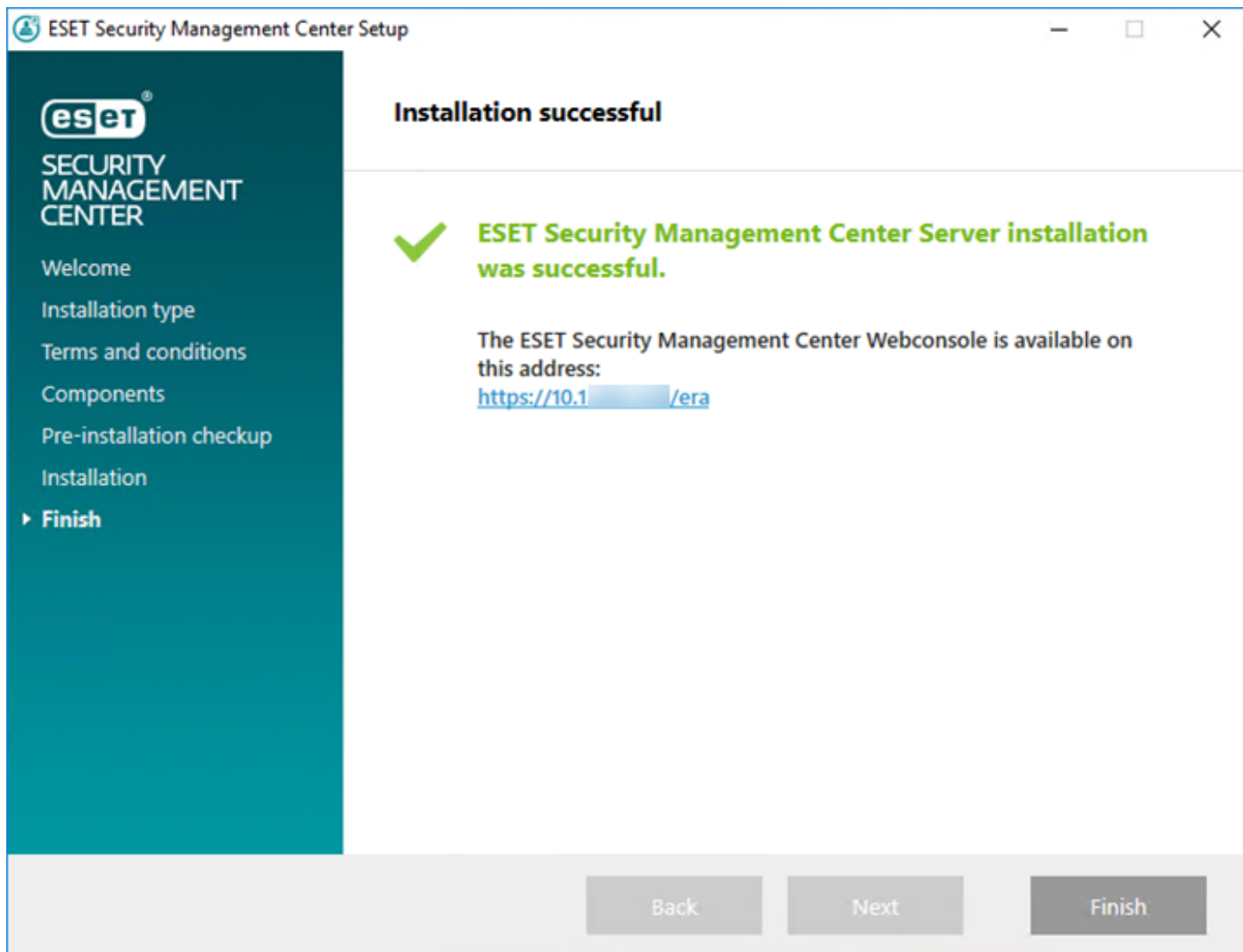
COMPONENT	ESTIMATED TIME
✓ Microsoft SQL Server Express	20 minute(s)
✓ ESET Security Management Center Server	5 minute(s)
⦿ ESET Management Agent	2 minute(s)
Apache Tomcat	5 minute(s)
ESET Security Management Center Webconsole	5 minute(s)
Rogue Detection Sensor	1 minute(s)
Apache HTTP Proxy (mirror replacement)	1 minute(s)

Back

Next

Cancel

12. Ak ste zvolili inštaláciu nástroja **Rogue Detection Sensor**, zobrazia sa inštalačné okná pre WinPcap ovládač. Uistite sa, že je označená možnosť **Automatically start the WinPcap driver at boot time**.
13. Po ukončení inštalácie sa zobrazí správa „Inštalácia ESET Security Management Center Server bola úspešná.“ spolu s URL adresou ESMC Web Console. Kliknite na URL adresu pre otvorenie [Web Console](#) alebo kliknite na **Dokončiť**.



V prípade neúspešnej inštalácie:

- Skontrolujte súbory protokolu inštalácie inštalačného balíka all-in-one. Protokoly sa nachádzajú v tom istom adresári ako all-in-one inštalátor, napr.:
C:\Users\Administrator\Downloads\x64\logs\
- Ďalšie pokyny pre vyriešenie vášho problému nájdete v časti [Riešenie problémov](#).

4.1.2 Inštalácia komponentu ESMC Mobile Device Connector (samostatne)

Ak si želáte nainštalovať Mobile Device Connector ako samostatný nástroj na iný počítač ako ten, na ktorom beží služba ESMC Server, postupujte podľa nasledujúcich krokov.

Upozornenie:

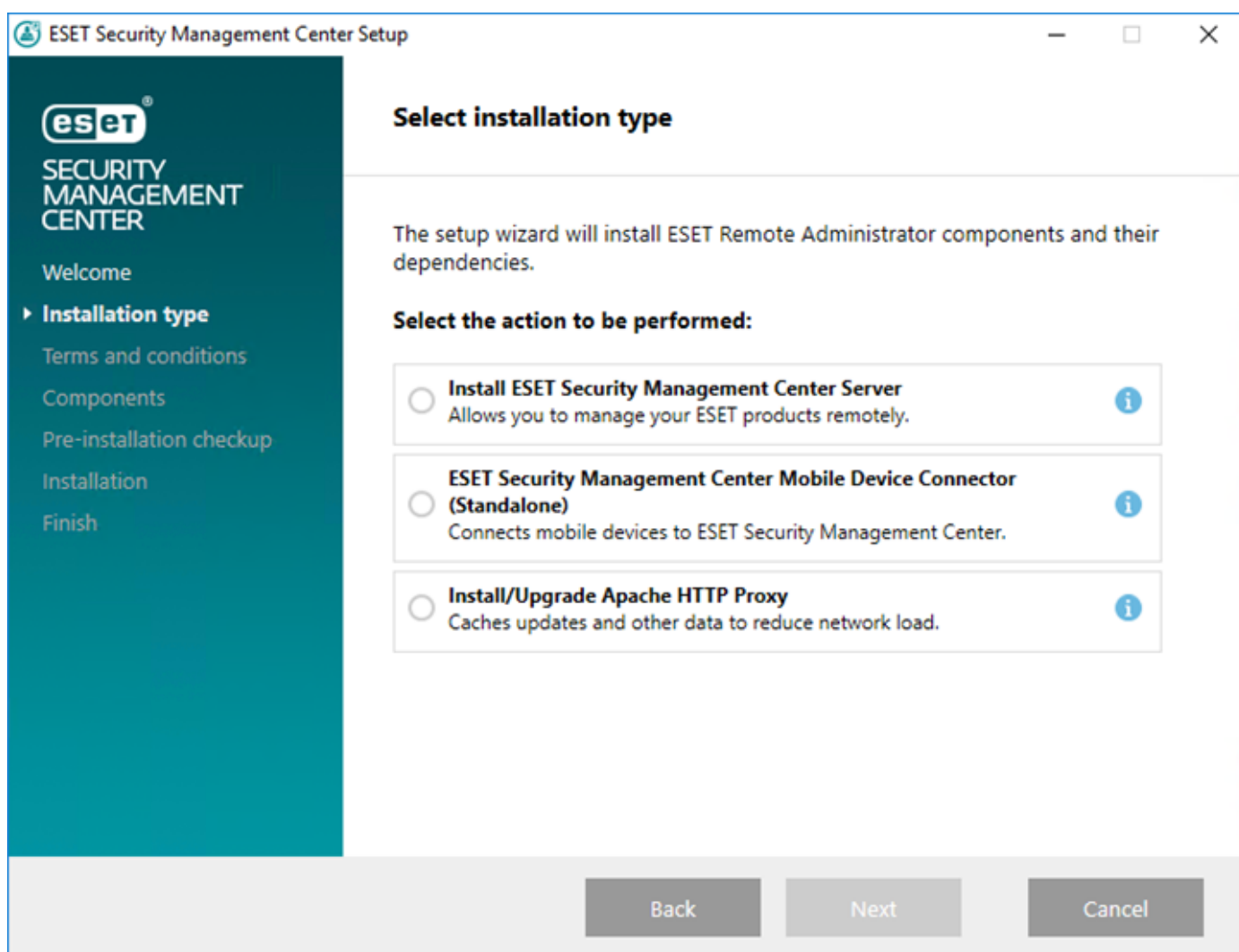
Aby mohli byť mobilné zariadenia spravované vždy bez ohľadu na ich polohu, Mobile Device Connector musí byť prístupný z internetu.

Poznámka:

Majte na pamäti, že mobilné zariadenia komunikujú s nástrojom Mobile Device Connector, čo ovplyvňuje množstvo prenesených dát. Väčšie množstvo prenesených dát môže byť nežiaduce najmä pri roamingu.

Pre inštaláciu komponentu Mobile Device Connector na operačnom systéme Windows postupujte podľa krokov uvedených nižšie:

1. Najprv si, prosím, prečítajte [prerekvizity](#) a uistite sa, že všetky sú splnené.
2. Dvojitým kliknutím spustíte inštalačný balík, vyberte **Nainštalovať Mobile Device Connector (Samostatný)** a kliknite na **Ďalej**.



3. 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.
4. Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**.
5. ESET Security Management Center Mobile Device Connector vyžaduje na fungovanie **databázu**. Ak chcete nainštalovať databázu, označte možnosť **Microsoft SQL Server Express**, v opačnom prípade ponechajte pole

prázdné. Ak sa chcete pripojiť k existujúcej databáze, príslušná možnosť bude dostupná počas inštalácie. Kliknite na **Inštalovať** pre pokračovanie v inštalácii.

6. Ak ste si v rámci tejto inštalácie zvolili nainštalovať databázu (krok č. 5), databáza bude nainštalovaná automaticky a vy môžete prejsť na krok č. 8. Ak ste si nezvolili nainštalovať databázu v kroku č. 5, budete vyzvaný na pripojenie komponentu MDM k svojej existujúcej databáze.

i Poznámka:

Môžete použiť rovnaký databázový server ako používate pre ESMC databázu, odporúčame však použiť iný databázový server, ak plánujete zaregistrovať viac ako 80 mobilných zariadení.

7. Inštalátor sa teraz musí pripojiť k existujúcej databáze, ktorá bude používaná komponentom Mobile Device Connector. Upresnite nasledujúce údaje o pripojení:
 - **Databáza:** MySQL Server/MS SQL Server/MS SQL Server cez Windows Authentication.
 - **ODBC ovládač:** MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 pre SQL Server.
 - **Názov databázy:** Ak je to možné, odporúčame používať predvolený názov databázy „era_mdm_db“.
 - **Názov hostiteľa:** názov hostiteľa alebo IP adresa vášho databázového servera.
 - **Port:** číslo portu používaného na pripojenie k serveru.
 - **Používateľské meno/heslo** k účtu správcu databázy.
 - **Použiť inštanciu s názvom** – ak používate MS SQL databázu, môžete označiť možnosť **Použiť inštanciu s názvom**. Následne budete môcť použiť vlastnú inštanciu databázy zadaním názvu hostiteľa v tvare `HOSTNAME\DB_INSTANCE`, napríklad: `192.168.0.10\ESMC7SQL`. Pre klastrovú databázu použijete len názov klastra. Ak je zvolená táto možnosť, nebude možné zmeniť port, ktorý bude použitý – systém použije porty predvolené spoločnosťou Microsoft.

i Poznámka:

Ak zvolíte možnosť **Použiť inštanciu s názvom**, ESMC Server môžete pripojiť aj k MS SQL databáze, ktorá je nainštalovaná na Failover klastri. Do poľa **Názov hostiteľa** zadajte názov klastra.

The screenshot shows a dialog box titled "ESET Security Management Center Mobile Device Connector...". The main heading is "Database server connection" with the instruction "Please enter database server connection." and the ESET logo in the top right corner. The dialog contains several fields and a dropdown menu:

- Database:** A dropdown menu with "MS SQL Server" selected.
- ODBC driver:** A dropdown menu with "MS SQL Server" selected.
- Database name:** A text field containing "era_mdm_db".
- Hostname:** A text field containing "localhost".
- Use Named Instance:** An unchecked checkbox.
- Port:** A text field containing "1433".
- Database account:** A section containing two empty text fields for "Username:" and "Password:".

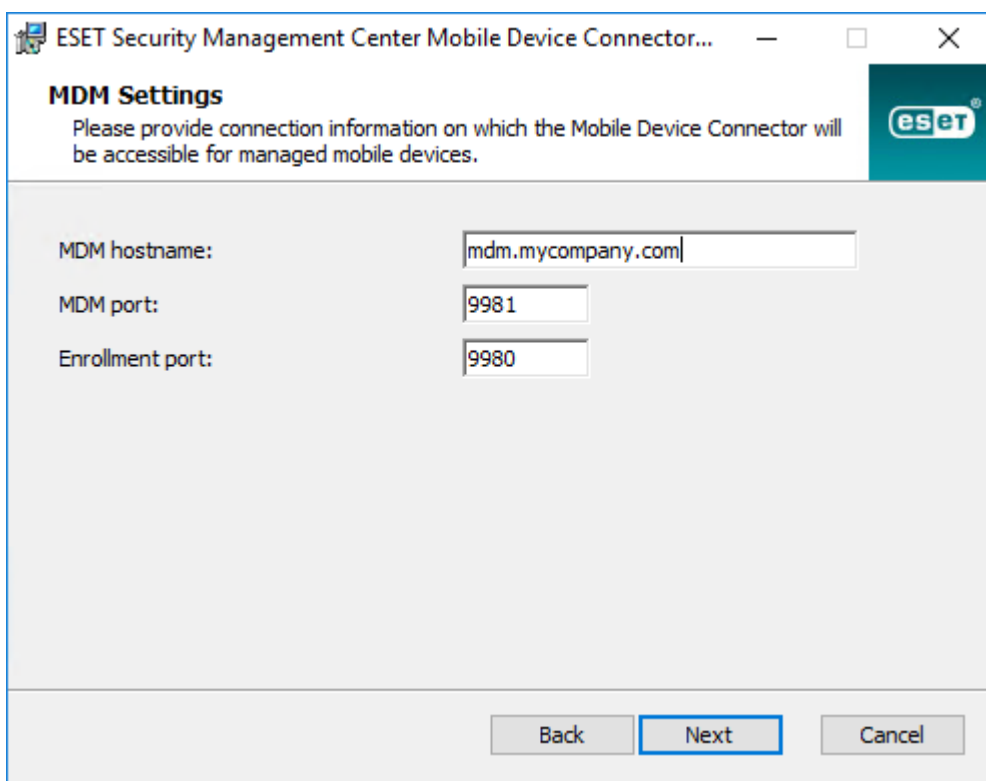
At the bottom of the dialog are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

8. Ak bolo pripojenie úspešné, budete vyzvaný na overenie, či chcete použiť poskytnutého používateľa ako používateľa databázy pre ESMC MDM.
9. Po úspešnej inštalácii novej databázy alebo úspešnom pripojení inštalátora k existujúcej databáze môžete pokračovať v inštalácii komponentu MDM. Uprávnite **MDM názov hostiteľa**: toto je verejná doména alebo verejná IP adresa vášho MDM servera a teda je dostupná pre mobilné zariadenia z internetu.

MDM názov hostiteľa musí byť zadaný v rovnakej podobe ako je uvedený vo vašom **HTTPS certifikáte servera**. V opačnom prípade iOS mobilné zariadenie odmietne nainštalovať [MDM profil](#). Napríklad, ak je v HTTPS certifikáte špecifikovaná IP adresa, zadajte túto IP adresu do poľa **MDM názov hostiteľa**. V prípade, že je špecifikované FQDN (napr. `mdm.mycompany.com`) v HTTPS certifikáte, zadajte toto FQDN do poľa **MDM názov hostiteľa**. Taktiež, ak je použitá hviezdička (*) (napr. `*.mycompany.com`) v HTTPS certifikáte, môžete do poľa **MDM názov hostiteľa** zadať `mdm.mycompany.com`.

Upozornenie:

V tomto kroku inštalácie buďte zvlášť opatrný pri vyplňaní poľa **MDM názov hostiteľa**. Ak bude zadaný údaj nesprávny alebo v nesprávnom formáte, MDM Connector nebude fungovať správne a jedinou možnosťou bude preinštalovať komponent.



10. V ďalšom kroku overte pripojenie k databáze kliknutím na **Ďalej**.
11. Pripojte MDM Connector k ESMC Serveru. Zadajte **Hostiteľa servera** a **Port servera** potrebný pre pripojenie k ESMC Serveru a pokračujte výberom buď **Serverom asistovanej inštalácie**, alebo **Offline inštalácie**:
 - **Serverom asistovaná inštalácia** – uveďte prístupové údaje správcu, ktoré používate na prihlásenie do ESMC Web Console, a inštalátor automaticky stiahne potrebné certifikáty. Skontrolujte tiež [požiadavky](#) pre serverom asistovanú inštaláciu.
 1. Zadajte **Hostiteľa servera** (názov alebo IP adresu vášho ESMC Servera) a **Port Web Console** (ponechajte prednastavený port 2223, ak nepoužívate vlastný port). Nezabudnite zadať aj prihlasovacie údaje (účet správcu) pre Web Console – **Používateľské meno/Heslo**.
 2. Kliknite na **Áno** v prípade, že ste boli vyzvaný na potvrdenie certifikátu. Prejdite na krok č. 11.
 - **Offline inštalácia** – uveďte **Proxy certifikát** a **Certifikačnú autoritu**, ktorú je možné [exportovať](#) z nástroja ESET Security Management Center. Môžete tiež použiť svoj [vlastný certifikát](#) a vhodnú certifikačnú autoritu.

1. Kliknite na **Prehľadávať** vedľa partnerského certifikátu a prejdite do umiestnenia, kde sa nachádza **Partnerský certifikát** (je to Proxy certifikát, ktorý ste exportovali z ESMC). Nechajte pole **Heslo certifikátu** prázdne, pretože tento druh certifikátu nevyžaduje heslo.
2. Zopakujte tento postup pre certifikačnú autoritu a pokračujte krokom č. 11.

i Poznámka:

Ak používate vlastné certifikáty pre ESMC (namiesto prednastavených, ktoré boli automaticky vygenerované pri inštalácii nástroja ESET Security Management Center), je potrebné ich zadať, keď budete vyzvaný poskytnúť Proxy certifikát.

12. Vyberte cieľový priečinok pre Mobile Device Connector (odporúčame použiť prednastavený), kliknite na **Ďalej** a potom na **Inštalovať**.

Po dokončení inštalácie MDM budete vyzvaný na inštaláciu agenta. Kliknite na **Ďalej** pre spustenie inštalácie, odsúhlaste Licenčnú dohodu s koncovým používateľom (EULA), ak s ňou súhlasíte, a postupujte podľa nasledujúcich krokov:

1. Zadajte **Hostiteľa servera** (názov hostiteľa alebo IP adresu vášho ESMC Servera) a **Port servera** (štandardný port servera je 2222, ak používate iný port, zadajte svoje číslo portu).

! Dôležité:

Uistite sa, že **Hostiteľ servera** zodpovedá aspoň jednej z hodnôt (ideálne FQDN) zadaných v poli **Hostiteľ** v časti **Certifikát servera**. V opačnom prípade sa zobrazí chybové hlásenie „Priятý certifikát servera nie je platný“. Ak zadáte v časti Certifikát servera hviezdičku (*) do poľa Hostiteľ, certifikát bude môcť fungovať s akýmkoľvek **Hostiteľom servera**.

2. Ak používate proxy, označte možnosť **Použiť proxy**. Po označení tejto možnosti bude inštalátor pokračovať v **offline inštalácii**.

i Poznámka:

Toto nastavenie proxy sa používa len na replikáciu medzi ESET Management Agentom a ESMC Serverom, nie na ukladanie aktualizácií do vyrovnávacej pamäte.

- **Názov hostiteľa proxy:** názov hostiteľa alebo IP adresa zariadenia s HTTP proxy.
- **Port proxy:** prednastavená hodnota je 3182.
- **Používateľské meno, Heslo:** zadajte prihlasovacie údaje používané vaším proxy, ak sa vyžaduje autentifikácia.

Nastavenia proxy môžete neskôr zmeniť vo vašej [politike](#). Najprv musíte nainštalovať [proxy](#), až potom môžete prostredníctvom neho nakonfigurovať spojenie medzi agentom a serverom.

3. Vyberte si jednu z nasledujúcich možností inštalácie a postupujte podľa jej krokov:

Serverom asistovaná inštalácia – budete musieť uviesť prístupové údaje správcu, ktoré používate pre prihlásenie do ESMC Web Console (inštalátor automaticky stiahne potrebné certifikáty).

Offline inštalácia – budete musieť zadať certifikát agenta a certifikačnú autoritu, ktoré je možné [exportovať](#) z nástroja ESET Security Management Center. Môžete tiež použiť váš [vlastný certifikát](#).

- Pre pokračovanie v **serverom asistovanej inštalácii agenta** postupujte podľa nasledujúcich krokov:
 1. Zadajte názov hostiteľa alebo IP adresu ESMC Web Console (rovnaké ako pre ESMC Server) do poľa **Hostiteľ servera**. **Web Console port** nechajte nastavený na štandardný port 2223, ak nepoužívate vlastný port. Nezabudnite tiež zadať prihlasovacie údaje pre Web Console do polí **Meno používateľa** a **Heslo**.

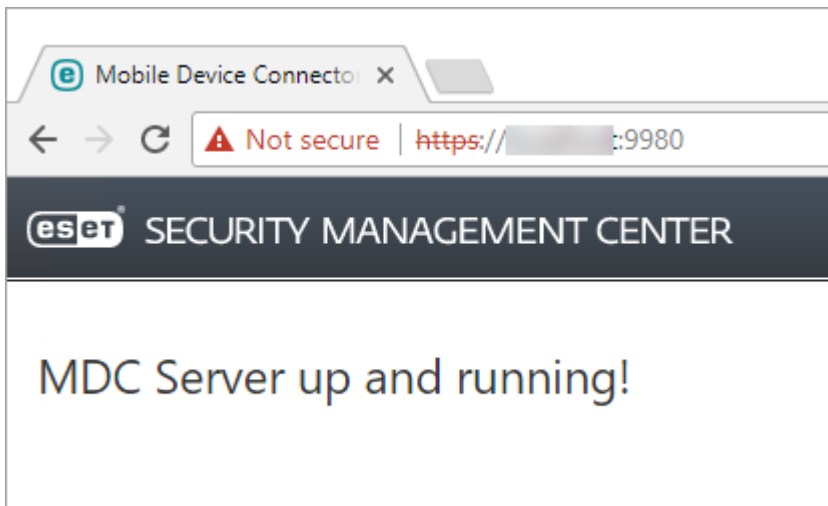
! Dôležité:

Uistite sa, že **Hostiteľ servera** zodpovedá aspoň jednej z hodnôt (ideálne FQDN) zadaných v poli **Hostiteľ** v časti **Certifikát servera**. V opačnom prípade sa zobrazí chybové hlásenie „Priятý certifikát servera nie je platný“. Ak zadáte v časti Certifikát servera hviezdičku (*) do poľa Hostiteľ, certifikát bude môcť fungovať s akýmkoľvek

Hostiteľom servera.

2. Kliknite na **Áno** v prípade, že ste boli vyzvaný na potvrdenie certifikátu.
 3. Zvoľte možnosť **Nevytvoriť počítač** alebo **Vybrať vlastnú statickú skupinu**. Ak kliknete na **Vybrať vlastnú statickú skupinu**, budete môcť zvoliť jednu skupinu zo zoznamu existujúcich statických skupín v ESMC. Do tejto skupiny bude pridaný počítač, na ktorý práve inštalujete agenta.
 4. Zvoľte cieľový priečinok pre ESET Management Agentu (odporúčame použiť predvolený priečinok), kliknite na tlačidlo **Ďalej** a potom na tlačidlo **Inštalovať**.
- Pre pokračovanie v **offline inštalácii agenta** postupujte podľa nasledujúcich krokov:
 1. Ak ste v predchádzajúcom kroku vybrali možnosť **Použiť proxy**, zadajte **Názov hostiteľa proxy**, **Port proxy** (predvolený port je 3128), **Používateľské meno** a **Heslo** a kliknite na **Ďalej**.
 2. Kliknite na **Prechádzať** a prejdite do umiestnenia vášho partnerského certifikátu (toto je certifikát agenta, ktorý ste exportovali z ESMC). Nechajte pole **Heslo certifikátu** prázdne, pretože tento druh certifikátu nevyžaduje heslo. Nemusíte hľadať **Certifikačnú autoritu** – nechajte toto pole prázdne.
- i Poznámka:**
Ak používate vlastný certifikát pre ESMC (namiesto prednastaveného, ktorý bol automaticky vygenerovaný pri inštalácii nástroja ESET Security Management Center), použite daný certifikát aj pri tejto inštalácii.
3. Pre inštaláciu do prednastaveného priečinka kliknite na **Ďalej**, prípadne kliknite na **Zmeniť** pre výber iného priečinka (odporúčame ponechať pôvodné umiestnenie).

Po dokončení inštalácie skontrolujte, či Mobile Device Connector pracuje správne otvorením adresy `https://váš-mdm-názovhostiteľa:registračný-port` (napr. `https://mdm.company.com:9980`) vo vašom webovom prehliadači alebo z mobilného zariadenia. Ak bola inštalácia úspešná, zobrazí sa nasledujúca správa:



Teraz môžete [aktivovať MDM pomocou nástroja ESET Security Management Center](#).

4.1.3 Inštalácia ESMC na Windows SBS/Essentials

Prerekvizity

Uistite sa, že všetky [požiadavky](#) sú splnené, obzvlášť požiadavky týkajúce sa [podporovaných operačných systémov](#).

i Poznámka:

Niektoré staršie verzie Microsoft SBS obsahujú Microsoft SQL Server Express vo verziách, ktoré nie sú podporované nástrojom ESET Security Management Center, napríklad:

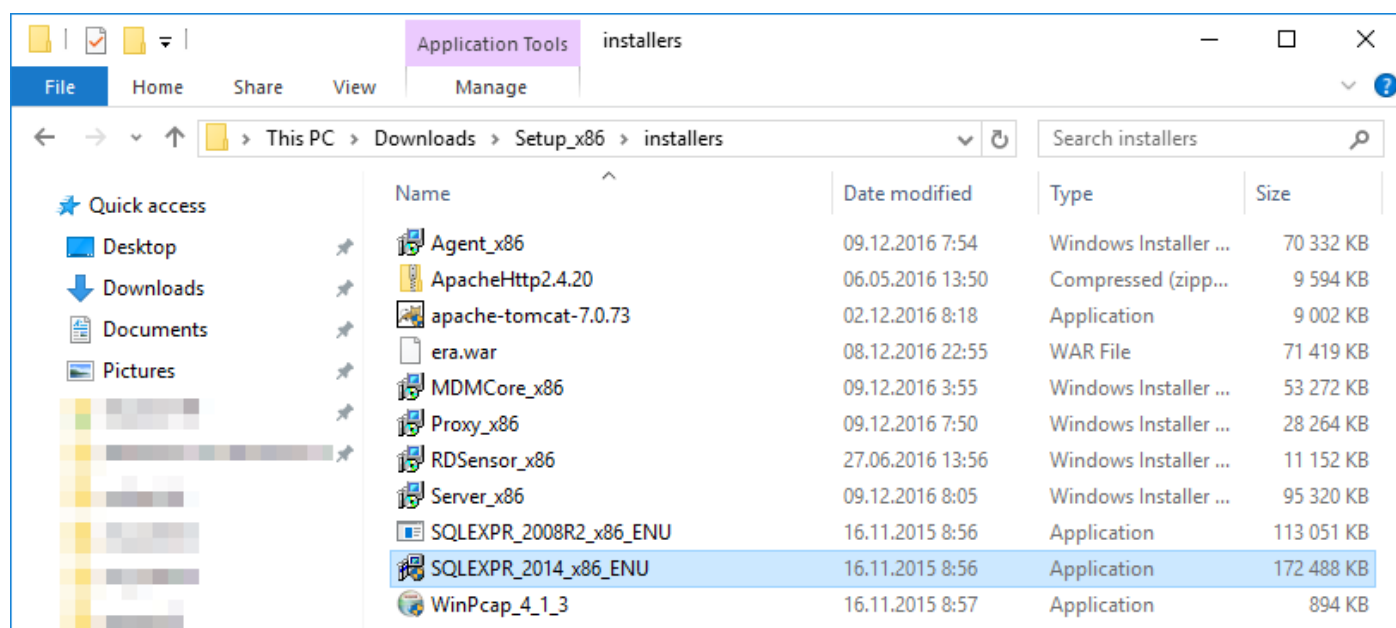
Microsoft SBS 2003 x86 SP2
Microsoft SBS 2003 x86 R2
Microsoft SBS 2008 x64 SP2

Ak používate niektorú z vyššie uvedených verzií Windows Small Business Server a rozhodnete sa inštalovať ESMC databázu na Microsoft SBS, musíte najprv aktualizovať Microsoft SQL Server Express na novšiu verziu.

- Ak nemáte nainštalovaný Microsoft SQL Express na svojom SBS systéme, postupujte podľa nasledujúcich krokov.
- Ak máte Microsoft SQL Express nainštalovaný na svojom SBS systéme, ale nepoužívate ho, odinštalujte ho a postupujte podľa krokov uvedených nižšie.
- Ak používate verziu Microsoft SQL Server Express, ktorá je štandardne dostupná na SBS, premigrujte svoju databázu na SQL Express kompatibilný s ESMC Serverom. Zálohujte si svoju databázu, odinštalujte predchádzajúcu verziu Microsoft SQL Server Express a postupujte podľa nasledujúcich krokov pre inštaláciu Microsoft SQL Server Express kompatibilného s ESMC Serverom. V prípade potreby tiež obnovte svoju pôvodnú databázu.

Inštalácia

1. Stiahnite si inštalčný balík pre ESMC (vo formáte .zip) [zo stránky spoločnosti ESET](#) v časti ESET Security Management Center.
2. Rozbaľte inštalčný súbor, otvorte priečinok **installers** a dvojitým kliknutím spustíte inštalátor pre Microsoft SQL Express. V našom príklade je to **SQLEXP_2014_x86_ENU**:



- Otvorí sa okno Installation Center. Pre spustenie inštalácie kliknite na **New installation or add features to an existing installation**.

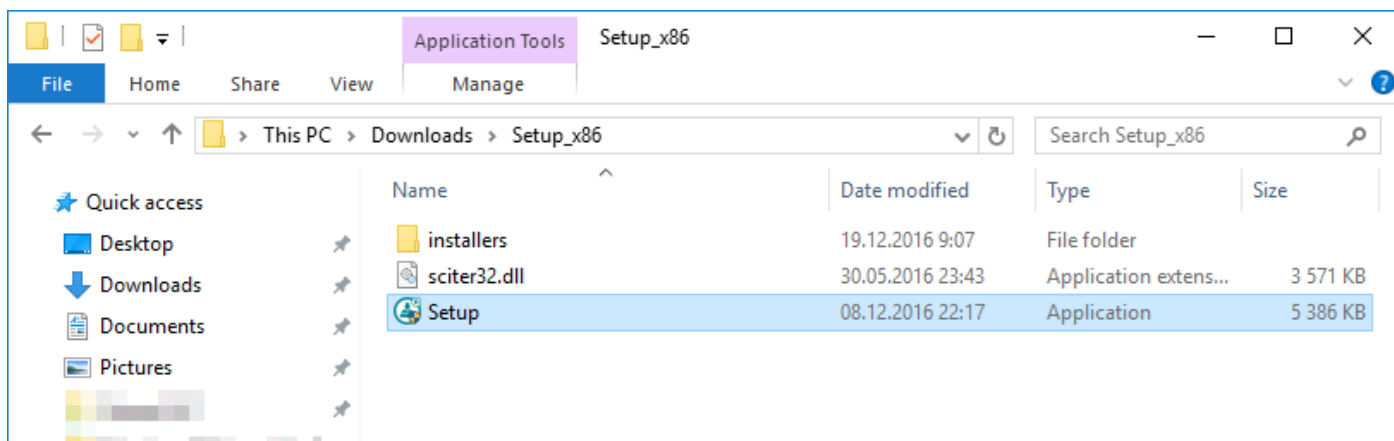
i Poznámka:

Počas [inštalácie](#) (krok č. 8) nastavte režim overovania (authentication mode) na **Mixed mode (SQL Server authentication and Windows authentication)**.

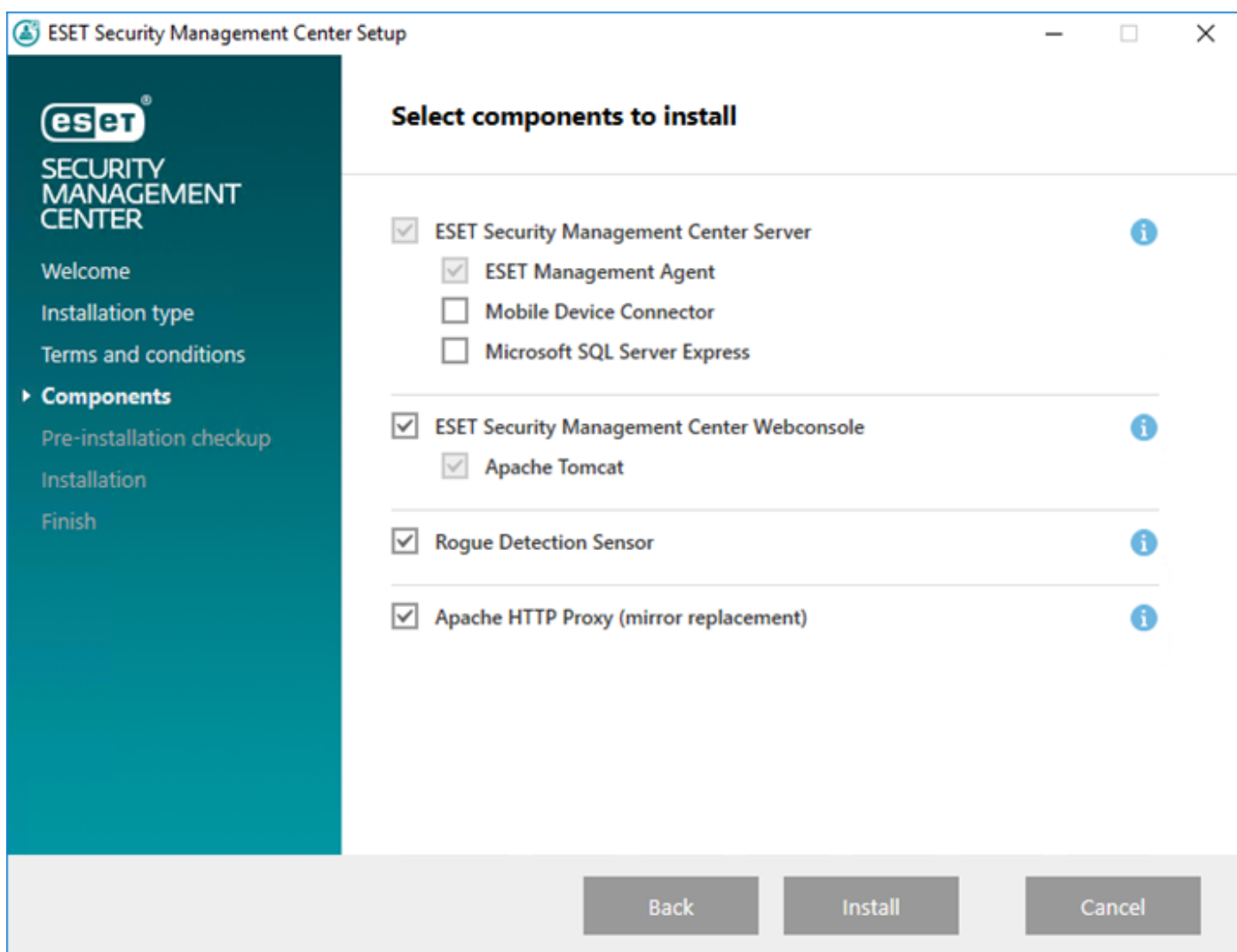
i Poznámka:

Pre inštaláciu ESMC Servera na SBS musíte [povoliť TCP/IP pripojenie na SQL Server](#).

3. Nainštalujte ESET Security Management Center spustením súboru **Setup.exe**:



4. Označte komponenty, ktoré chcete nainštalovať, **zrušte označenie pre Microsoft SQL Server Express** a kliknite na **Inštalovať**.



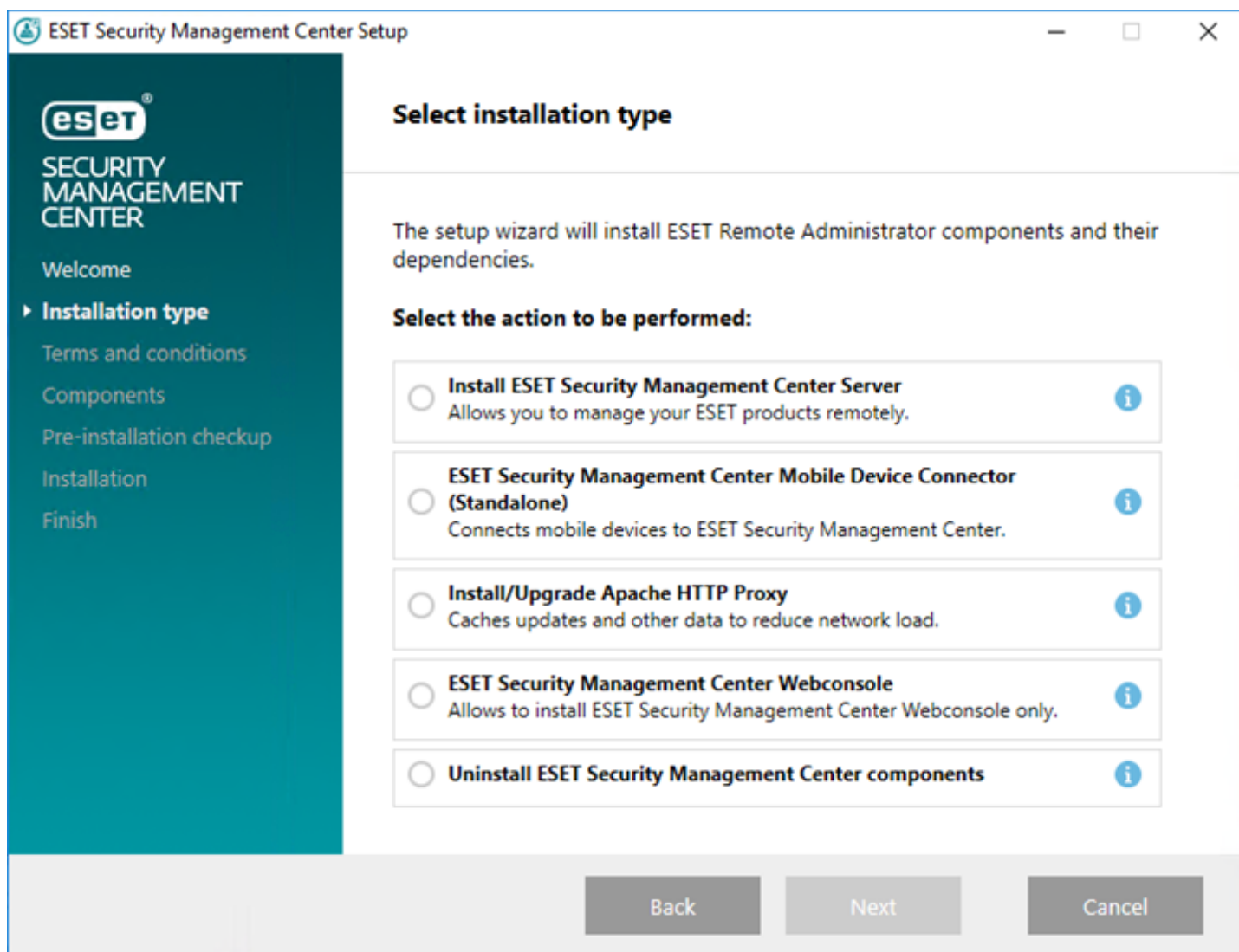
5. Prejdite na [Inštaláciu ESMC Servera](#).

4.1.4 Odinštalovanie súčastí

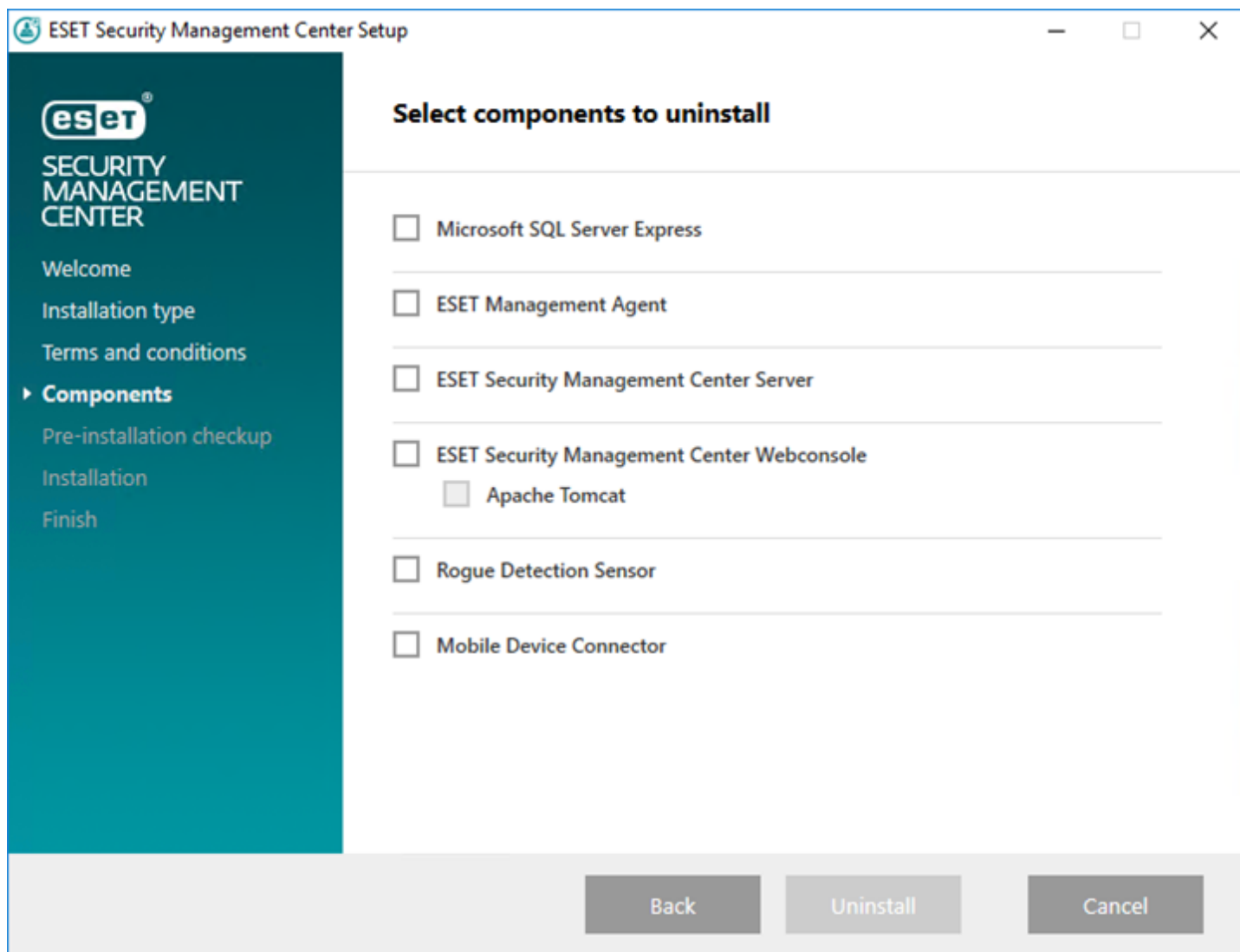
Pre odinštalovanie súčastí ESMC spustíte all-in-one inštalátor nástroja ESMC, ktorý ste použili počas [inštalácie ESMC](#), a vyberte možnosť **Odinštalovať súčasti ESET Security Management Center**. Pred pokračovaním v inštalácii si môžete v roletovom menu **Jazyk** vybrať požadovaný jazyk.

i Poznámka:

Pred odinštalovaním nástroja Mobile Device Connector si prečítajte kapitolu [MDM funkcia licencovania iOS zariadení](#).



Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**. Vyberte súčasti, ktoré chcete odinštalovať a kliknite na **Odinštalovať**.



i Poznámka:

- Pre dokončenie odinštalovania príslušných súčastí môže byť vyžadovaný reštart počítača.
- Prečítajte si tiež kapitolu [Odinštalovanie starého ESMC Servera](#).

4.2 Inštalácia na Microsoft Azure

Používateľom, ktorí uprednostňujú spravované riešenie pred prevádzkovaním nástroja ESMC na pôde firmy, ponúka spoločnosť ESET produkt ESET Security Management Center na cloudovej platforme [Microsoft Azure](#).

Viac informácií nájdete v našej databáze znalostí:

- [Ako začať s nástrojom ESET Security Management Center \(ESMC\) – Azure](#)
- [Často kladené otázky o ESET Security Management Center VM pre Microsoft Azure](#)
- [Ako nasadiť a nainštalovať ESET Security Management Center na Microsoft Azure?](#)

4.3 Inštalácia súčastí na systéme Windows

Väčšina inštalčných scenárov vyžaduje inštaláciu rôznych komponentov nástroja ESET Security Management Center na rôzne počítače v závislosti od sieťovej architektúry, výkonnostných požiadaviek atď. Pre jednotlivé komponenty nástroja ESET Security Management Center sú dostupné nasledujúce inštalčné balíky:

Základné súčasti

- [ESMC Server](#)
- [ESMC Web Console](#)
- [ESET Management Agent](#) – musí byť nainštalovaný na klientskych počítačoch, voliteľne aj na ESMC Serveri.

Voliteľné súčasti

- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Apache HTTP Proxy](#)
- [Mirror Tool](#)

Ak chcete aktualizovať ESET Remote Administrator na najnovšiu verziu (ESMC 7.0), prečítajte si náš [článok databázy znalostí](#).

Ak chcete spustiť inštaláciu v lokálnom jazyku, musíte spustiť MSI inštalátor konkrétneho komponentu ESMC cez príkazový riadok.

Nasleduje príklad, ako by malo vyzeráť spustenie inštalácie v slovenskom jazyku:

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The command prompt shows the command: `C:\install>msiexec /i Agent_x64.msi TRANSFORMS=":sk-SK.mst"`. The background of the command prompt is black, and the text is white.

Pre výber jazyka spustíte inštalátor s parametrom TRANSFORMS podľa nasledujúcej tabuľky:

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.

4.3.1 Inštalácia servera

Inštaláciu komponentu ESMC Server na operačnom systéme Windows vykonáte podľa nasledujúcich krokov:

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Uistite sa, že boli splnené všetky [požiadavky](#).
3. Spustíte inštalátor pre ESMC Server a potvrdíte Licenčnú dohodu s koncovým používateľom (EULA), ak s ňou súhlasíte.
4. Začiarkavacie políčko vedľa položky **Toto je inštalácia na klaster** nechajte prázdne a kliknite na **Ďalej**. Je toto klastrová inštalácia?

Dôležité:

Ak inštalujete ESMC Server na Failover klaster, označte možnosť **Toto je inštalácia na klaster**. Špecifikujte **Vlastnú cestu k dátam aplikácie** pre nasmerovanie k zdieľanému úložisku klastra. Dáta musia byť uložené v jednej lokalite, ktorá je dostupná pre všetky uzly klastra.

5. Vyberte **Používateľský účet služby**. Tento používateľský účet bude použitý na prevádzku služby ESET Security Management Center Server. Sú dostupné tieto možnosti:
 - Účet sieťovej služby
 - Zadané používateľom: DOMÉNA/PRIHLASOVACIE MENO

6. Pripojte sa k databáze. V databáze sú všetky dáta (vrátane hesiel do ESMC Web Console, protokolov z klientskych počítačov atď.):

- **Databáza:** MySQL Server/MS SQL Server/MS SQL Server cez Windows Authentication
- **ODBC ovládač:** MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server
- **Database name:** môžete ponechať preddefinované meno alebo ho zmeniť
- **Názov hostiteľa:** názov hostiteľa alebo IP adresa vášho databázového servera
- **Port:** číslo portu používaného na pripojenie k serveru
- **Prihlasovacie meno/Heslo** k účtu správcu databázy.
- **Použiť inštanciu s názvom** – ak používate MS SQL databázu, môžete označiť možnosť **Použiť inštanciu s názvom**. Následne budete môcť použiť vlastnú inštanciu databázy zadaním názvu hostiteľa v tvare *HOSTNAME\DB_INSTANCE*, napríklad: *192.168.0.10\ESMC7SQL*. Pre klastrovú databázu použite len názov klastra. Ak je zvolená táto možnosť, nebude možné zmeniť port, ktorý bude použitý – systém použije porty predvolené spoločnosťou Microsoft.

i Poznámka:

Ak zvolíte možnosť **Použiť inštanciu s názvom**, ESMC Server môžete pripojiť aj k MS SQL databáze, ktorá je nainštalovaná na Failover klastri. Do poľa **Názov hostiteľa** zadajte názov klastra.

The screenshot shows the 'Database server connection' dialog box in the ESET Security Management Center Server Setup. The dialog has a title bar with the ESET logo and window controls. Below the title bar, it says 'Please enter database server connection.' The main area contains several fields: 'Database:' with a dropdown menu showing 'MS SQL Server' selected; 'ODBC driver:' with a dropdown menu showing 'MS SQL Server' selected; 'Database name:' with a text box containing 'era_db'; 'Hostname:' with a text box containing 'localhost'; 'Use Named Instance:' with an unchecked checkbox; 'Port:' with a text box containing '1433'; 'Database account' section with 'Username:' and 'Password:' text boxes. At the bottom, there are three buttons: 'Back', 'Next', and 'Cancel'.

i Poznámka:

ESMC Server ukladá do databázy veľké bloky dát, preto je dôležité pre správne fungovanie ESMC [povoliť v MySQL akceptovanie veľkých dátových paketov](#).

Tento krok overí vaše pripojenie na databázu. Ak je pripojenie v poriadku, pokračujte na ďalší krok.

7. Vyberte používateľa pre ESET Security Management Center, ktorý má prístup do databázy. Môžete zadať existujúceho používateľa alebo vám inštalácia vytvorí nového.

8. Zadaťte heslo pre prístup do **Web Console**.

The screenshot shows a window titled "ESET Security Management Center Server Setup" with the subtitle "Web Console user & server connection". Below the subtitle, it says "Please enter Web Console user password and server connection." The ESET logo is in the top right corner. The form contains the following fields:

- Web Console user: Administrator
- Password: [Redacted with 10 dots]
- Password confirmation: [Redacted with 10 dots]
- Agent port: 2222
- Console port: 2223

At the bottom, there are three buttons: "Back", "Next" (highlighted with a blue border), and "Cancel".

9. ESET Security Management Center používa certifikáty na komunikáciu medzi serverom a klientom. Môžete vybrať svoje vlastné certifikáty alebo vám **Server** môže vytvoriť nový.

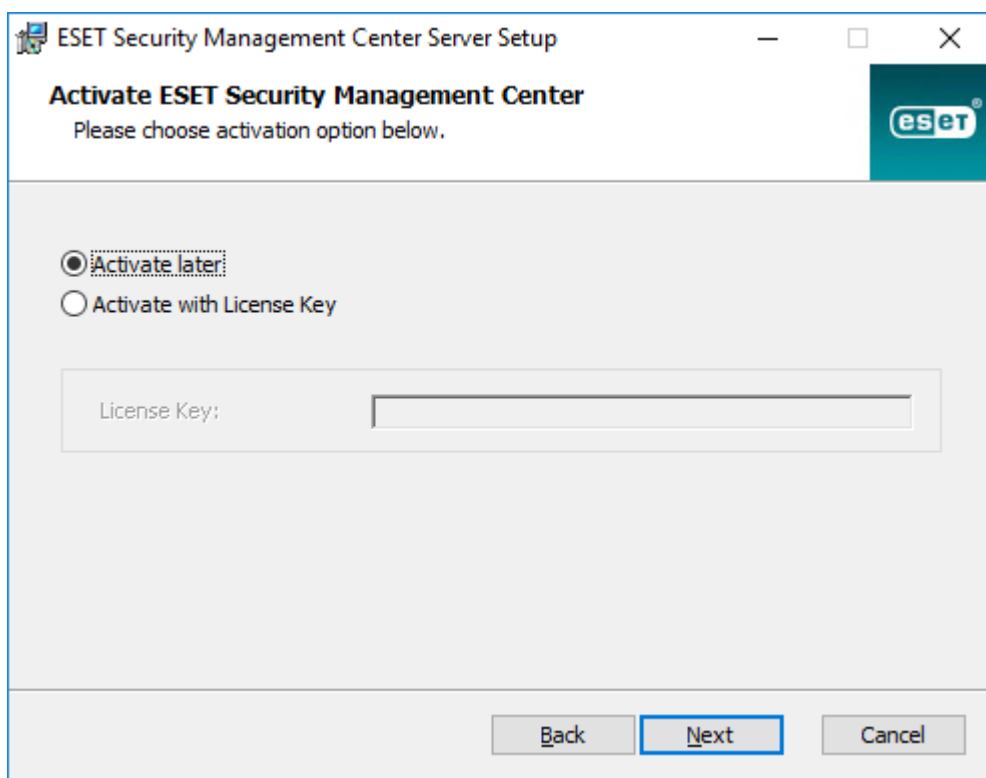
10. Vyplňte údaje pre všetky certifikáty a heslo pre **Certifikačnú autoritu**. Heslo si zapamätajte.

11. Bude vytvorený nový **Partnerský certifikát**, pre ktorý takisto vyberte heslo.

12. V ďalšom kroku vyberte heslo pre **Partnerské certifikáty** agenta a proxy. Môžete tiež prípadne upresniť dodatočné informácie o certifikátoch (nepovinné). Pole **Heslo authority** môžete ponechať prázdne, ak sa však rozhodnete heslo zadať, uistite sa, že si ho **zapamätáte**.

13. Inštalácia môže spustiť počítačnú úlohu [Synchronizácia statickej skupiny](#). Vyberte metódu (**Nesynchronizovať**, **Synchronizovať so sieťou Windows**, **Synchronizovať s Active Directory**) a kliknite na **Ďalej**.

14. Zadáte platný [licenčný kľúč](#) pre ESMC alebo vyberte možnosť **Aktivovať neskôr**.



15. Potvrďte alebo zmeňte adresár, do ktorého bude server nainštalovaný a kliknite **Ďalej**.

16. Kliknutím na **Inštalovať** spustíte inštaláciu servera.

i Poznámka:

Po dokončení inštalácie ESMC Servera môžete tiež nainštalovať [ESET Management Agentu](#) na rovnaký počítač (voliteľné). Týmto spôsobom budete môcť spravovať samotný server rovnako ako klientsky počítač.

4.3.1.1 Prerekvizity servera – Windows

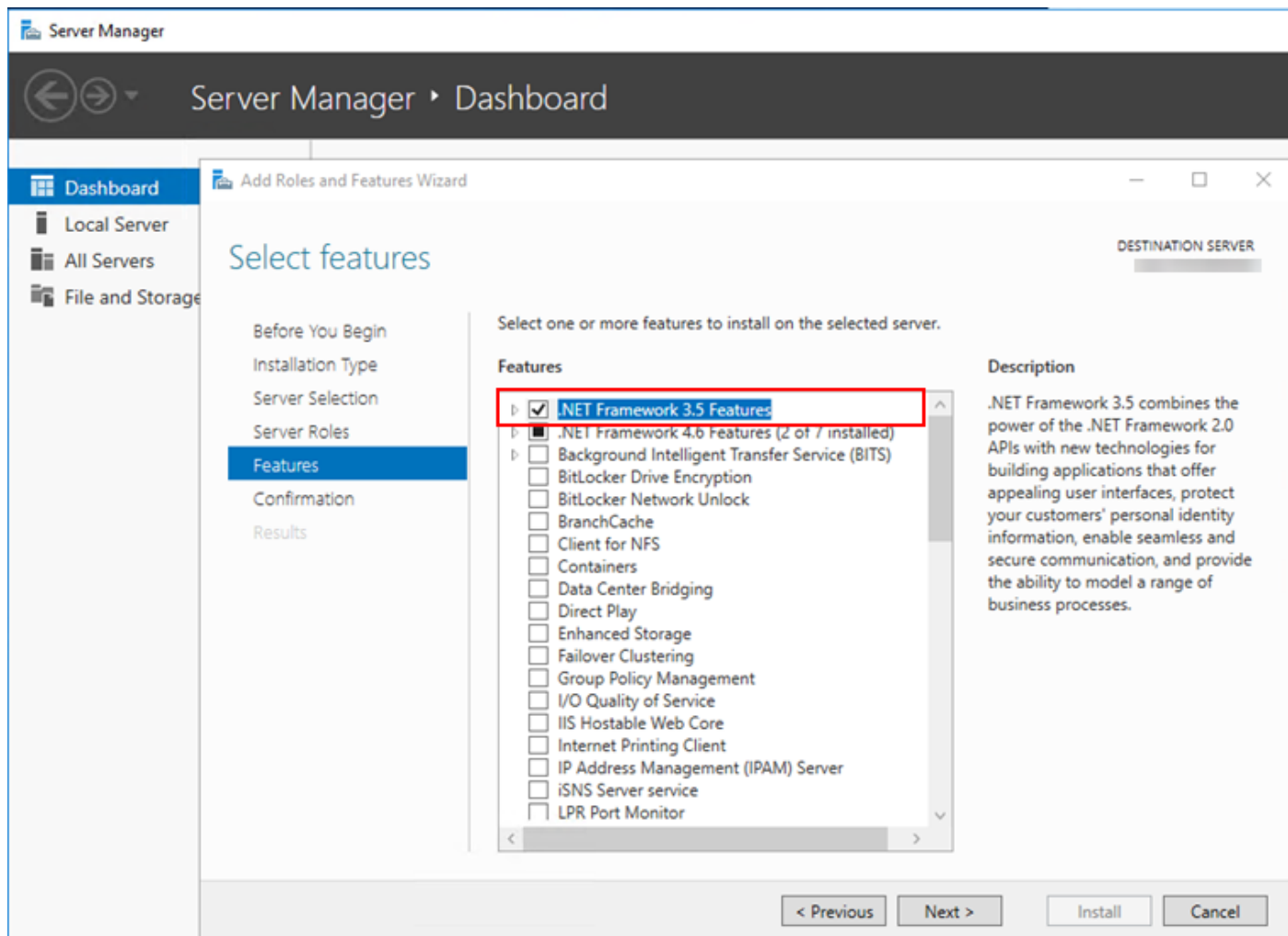
Pre inštaláciu komponentu ESMC Server na operačnom systéme Windows je potrebné splniť nasledujúce prerekvizity:

- Musíte mať platnú [licenciu](#).
- Potrebné porty musia byť otvorené a dostupné – podrobný zoznam portov môžete nájsť [tu](#).
- Databázový server (Microsoft SQL Server alebo MySQL) musí byť nainštalovaný a spustený. Pre viac informácií si pozrite [požiadavky na databázový server](#). Ak nemáte databázový server, odporúčame vám postupovať podľa [konfigurácie SQL Servera](#) pre správne nastavenie SQL pre používanie s nástrojom ESET Security Management Center. Databáza a používateľ databázy môže byť vytvorený buď počas inštalácie, alebo pred inštaláciou.

i Poznámka:

Podrobný návod, ako nastaviť vašu databázu a používateľský účet pre MS SQL a MySQL, nájdete v našom [článku databázy znalostí](#).

- Musíte si nainštalovať Java Runtime Environment (JRE) (môžete ho stiahnuť zo stránky <https://java.com/en/download/>). Vždy používajte najnovšiu oficiálne vydanú verziu Javy.
- Musí byť nainštalovaný Microsoft .NET Framework 3.5. Ak používate Windows Server 2008 a novšie verzie, nainštalujte ho pomocou **SPRIEVODCU ROLAMI A FUNKCIAMI SERVERA**. Ak používate Windows Server 2003, NET 3.5 môžete stiahnuť tu: <https://www.microsoft.com/en-us/download/details.aspx?id=21>



4.3.2 Požiadavky pre Microsoft SQL Server

Jednou z prekvizít pre inštaláciu ESMC je aj nainštalovanie a konfigurácia Microsoft SQL Servera. Je potrebné splniť nasledujúce požiadavky:

- Nainštalujte Microsoft SQL Server 2008 R2 alebo novší, prípadne môžete nainštalovať Microsoft SQL Server 2008 R2 Express alebo novší. Počas inštalácie vyberte pre autentifikáciu **Mixed mode**.
- Ak je Microsoft SQL Server už nainštalovaný, nastavte druh autentifikácie na **Mixed mode (SQL Server authentication and Windows authentication)**. Postupujte podľa inštrukcií v nasledujúcom [článku databázy znalostí](#).
- Povoľte TCP/IP pripojenie na SQL Server. Postupujte podľa inštrukcií v nasledujúcom [článku databázy znalostí](#) (časť II. **Povoľte TCP/IP pripojenie na SQL Server**).

i Poznámka:

- Na konfiguráciu a správu databázového systému Microsoft SQL Server si [stiahnite SQL Server Management Studio \(SSMS\)](#).
- Ak si počas inštalácie zvolíte nainštalovať Microsoft SQL Server Express, nebude možné ho nainštalovať na doménový radič. Toto je pravdepodobné v prípade, že používate Microsoft SBS. Ak používate Microsoft SBS, odporúčame vám nainštalovať ESET Security Management Center na iný server alebo nevybrať počas inštalácie komponent SQL Server Express (v takomto prípade musíte použiť na spustenie ESMC databázy svoj existujúci

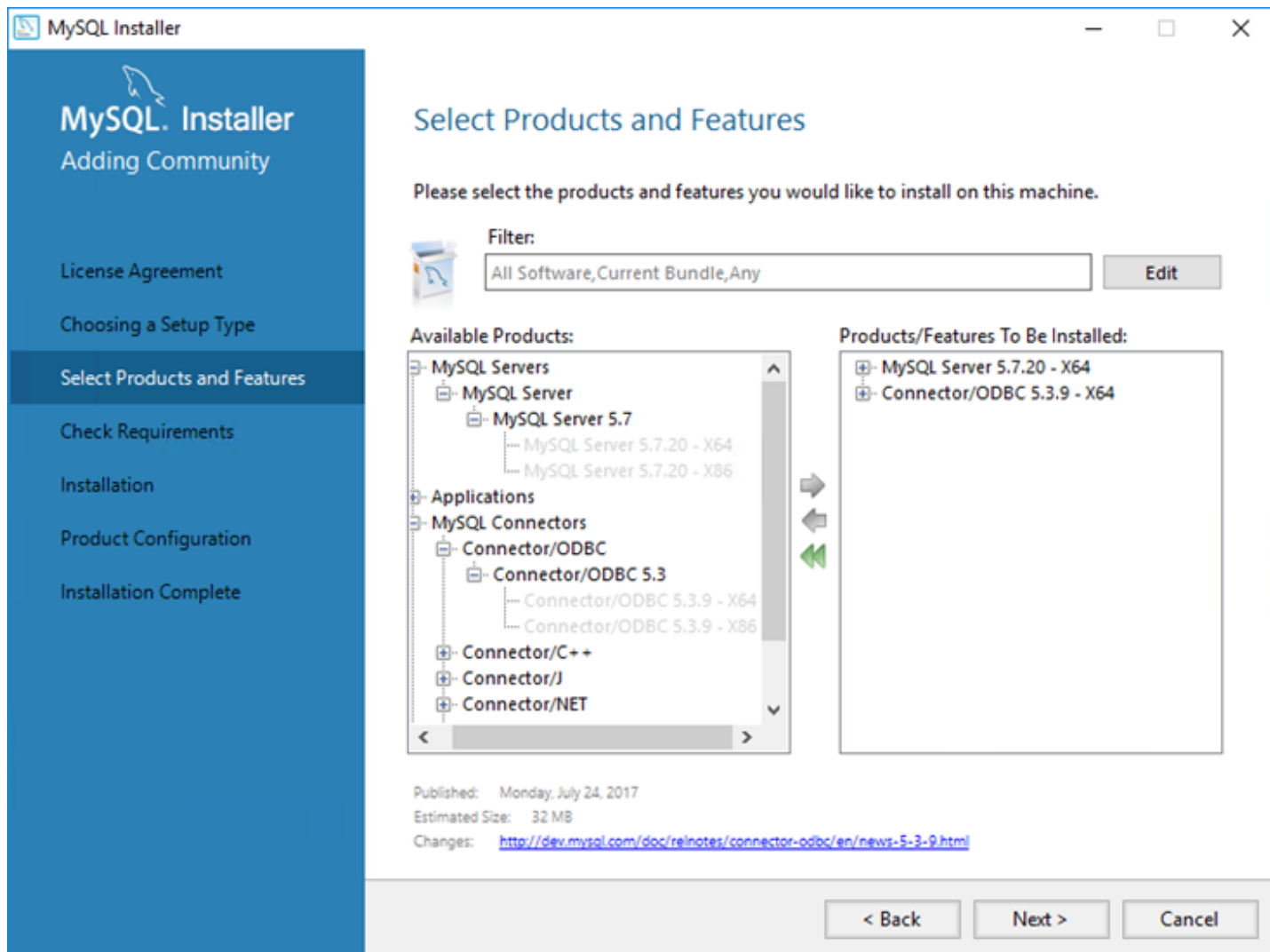
SQL Server alebo MySQL). Inštrukcie týkajúce sa inštalácie ESMC Servera na doménový radič nájdete v našom [článku databázy znalostí](#).

4.3.3 Inštalácia a konfigurácia MySQL Servera

Inštalácia

Stiahnite si MySQL Windows inštalátor z webovej stránky <https://dev.mysql.com/downloads/installer/> a spustite ho.

Počas inštalácie vyberte možnosť **Custom > MySQL Server a ODBC Connector**.



Konfigurácia

Otvorte nasledujúci súbor v textovom editore:

`C:\ProgramData\MySQL\MySQL Server 5.7\my.ini`

V súbore **my.ini** nájdite sekciu `[mysqld]` a pridajte do nej nasledujúce riadky:

`max_allowed_packet=33M`

- Pre MySQL 5.6.20 a 5.6.21 (verziu svojho MySQL môžete zistiť pomocou `mysql --version`):
 - `innodb_log_file_size` musí byť nastavené aspoň na **200 MB** (napr. `innodb_log_file_size=200M`)
- Pre MySQL 5.6.22 a novšie verzie:
 - `innodb_log_file_size*innodb_log_files_in_group` musí byť nastavené aspoň na **200 MB** (znak * predstavuje násobenie, súčin dvoch parametrov musí byť väčší ako 200 MB. Minimálna hodnota pre `innodb_log_files_in_group` je 2, pričom maximálna hodnota je 100 – musí byť použité celé číslo).

Napríklad:

```
innodb_log_file_size=100M  
innodb_log_files_in_group=2
```

Uložte zmeny a zatvorte súbor. Zadajte nasledujúci príkaz pre reštartovanie MySQL servera a aplikovanie nastavení (názov služby závisí od verzie MySQL, napr. verzia 5.7 = MySQL57 atď.):

```
net stop mysql57  
net start mysql57
```

Uistite sa, že inštalácia prebehla úspešne a služba je spustená pomocou zadania nasledujúceho príkazu do príkazového riadka:

```
sc query mysql57
```

4.3.4 Vyhradený používateľský účet databázy

Ak nechcete používať **SA účet** (MS SQL) alebo **root účet** (MySQL), môžete vytvoriť **vyhradený používateľský účet databázy**. Tento vyhradený účet bude používaný len na prístup do ESMC databázy. Odporúčame, aby ste si vytvorili vyhradený používateľský účet v rámci vašej databázy pred začatím inštalácie nástroja ESET Security Management Center. Budete tiež musieť pomocou vyhradeného používateľského účtu vytvoriť prázdnu databázu, ktorú bude ESET Security Management Center využívať.

i Poznámka:

- Je stanovená minimálna sada oprávnení, ktoré musia byť pridelené **vyhradenému používateľskému účtu databázy**.
- Podrobný návod, ako nastaviť vašu databázu a používateľský účet pre MS SQL a MySQL, nájdete v našom [článku databázy znalostí](#).
- MySQL oprávnenia používateľa:
ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER
- Microsoft SQL Server roly na úrovni databázy:
Používateľ ESMC databázy musí mať priradenú rolu **db_owner**.

4.3.5 Inštalácia agenta

Táto kapitola pojednáva o lokálnej inštalácii ESET Management Agent na pracovnej stanici.

i Poznámka:

Informácie o ďalších metódach inštalácie ESET Management Agent na pracovnej stanici nájdete v [príručke správcu](#) alebo našom [článku databázy znalostí](#).

Pre lokálnu inštaláciu komponentu ESET Management Agent na operačnom systéme Windows postupujte podľa nasledujúcich krokov:

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Spustíte inštalátor ESET Management Agent a odsúhlaste Licenčnú dohodu s koncovým používateľom (EULA).
3. 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.
4. Zadajte **Hostiteľa servera** (názov hostiteľa alebo IP adresu vášho ESMC Servera/ERA Proxy) a **Port servera** (štandardný port servera je 2222, ak používate iný port, zadajte vaše číslo portu).

! Dôležité:

Uistite sa, že **Hostiteľ servera** zodpovedá aspoň jednej z hodnôt (ideálne FQDN) zadaných v poli **Hostiteľ** v časti **Certifikát servera**. V opačnom prípade sa zobrazí chybové hlásenie „Priятý certifikát servera nie je platný“. Ak zadáte v časti Certifikát servera hviezdičku (*) do poľa Hostiteľ, certifikát bude môcť fungovať s akýmkoľvek **Hostiteľom servera**.

5. Ak používate na spojenie agenta so serverom proxy, označte možnosť **Použiť proxy**. Po označení tejto možnosti bude inštalátor pokračovať v [offline inštalácii](#).

i Poznámka:

Toto nastavenie proxy sa používa len na replikáciu medzi ESET Management Agentom a ESMC Serverom, nie na ukladanie aktualizácií do vyrovnávacej pamäte.

- **Názov hostiteľa proxy:** názov hostiteľa alebo IP adresa zariadenia s HTTP proxy.
- **Port proxy:** prednastavená hodnota je 3182.
- **Používateľské meno, Heslo:** zadajte prihlasovacie údaje používané vaším proxy, ak sa vyžaduje autentifikácia.

Nastavenia proxy môžete neskôr zmeniť vo vašej [politike](#). Najprv musíte nainštalovať [proxy](#), až potom môžete prostredníctvom neho nakonfigurovať spojenie medzi agentom a serverom.

6. Vyberte si jednu z nasledujúcich možností inštalácie a postupujte podľa jej krokov:

[Serverom asistovaná inštalácia](#) – budete musieť zadať prístupové údaje správcu, ktoré používate na prihlásenie do ESMC Web Console. Inštalátor automaticky stiahne potrebné certifikáty.

[Offline inštalácia](#) – budete musieť zadať certifikát agenta a certifikačnú autoritu. Certifikát agenta a certifikačnú autoritu je možné [exportovať](#) z nástroja ESET Security Management Center. Môžete tiež použiť svoj [vlastný certifikát](#).

4.3.5.1 Serverom asistovaná inštalácia agenta

Pre pokračovanie v **serverom asistovanej inštalácii agenta** postupujte podľa nasledujúcich krokov:

1. Zadajte názov hostiteľa alebo IP adresu ESMC Web Console (rovnaké ako pre ESMC Server) do poľa **Hostiteľ servera**. **Web Console port** nechajte nastavený na štandardný port 2223, ak nepoužívate vlastný port. Nezabudnite tiež zadať prihlasovacie údaje pre Web Console do polí **Meno používateľa a Heslo**.

! Dôležité:

Uistite sa, že **Hostiteľ servera** zodpovedá aspoň jednej z hodnôt (ideálne FQDN) zadaných v poli **Hostiteľ** v časti **Certifikát servera**. V opačnom prípade sa zobrazí chybové hlásenie „Priятý certifikát servera nie je platný“. Ak zadáte v časti Certifikát servera hviezdičku (*) do poľa Hostiteľ, certifikát bude môcť fungovať s akýmkoľvek **Hostiteľom servera**.

2. Kliknite na **Áno** v prípade, že ste boli vyzvaný na potvrdenie certifikátu.
3. Zvoľte možnosť **Nevytvoriť počítač** alebo **Vybrať vlastnú statickú skupinu**. Ak kliknete na **Vybrať vlastnú statickú skupinu**, budete môcť zvoliť jednu skupinu zo zoznamu existujúcich statických skupín v ESMC. Do tejto skupiny bude pridaný počítač, na ktorý práve inštalujete agenta.
4. Zvoľte cieľový priečinok pre ESET Management Agentu (odporúčame použiť predvolený priečinok), kliknite na tlačidlo **Ďalej** a potom na tlačidlo **Inštalovať**.

4.3.5.2 Offline inštalácia agenta

Pre pokračovanie v **offline inštalácii agenta** postupujte podľa nasledujúcich krokov:

1. Ak ste v predchádzajúcom kroku vybrali možnosť **Použiť proxy**, zadajte **Názov hostiteľa proxy**, **Port proxy** (predvolený port je 3128), **Používateľské meno** a **Heslo** a kliknite na **Ďalej**.
2. Kliknite na **Prechádzať** a prejdite do umiestnenia vášho partnerského certifikátu (toto je certifikát agenta, ktorý ste exportovali z ESMC). Nechajte pole **Heslo certifikátu** prázdne, pretože tento druh certifikátu nevyžaduje heslo. Nemusíte hľadať **Certifikačnú autoritu** – nechajte toto pole prázdne.

i Poznámka:

Ak používate vlastný certifikát pre ESMC (namiesto prednastaveného, ktorý bol automaticky vygenerovaný pri inštalácii nástroja ESET Security Management Center), použite daný certifikát aj pri tejto inštalácii.

3. Pre inštaláciu do prednastaveného priečinka kliknite na **Ďalej**, prípadne kliknite na **Zmeniť** pre výber iného priečinka (odporúčame ponechať pôvodné umiestnenie).

4.3.5.3 Odinštalovanie agenta a riešenie problémov

ESET Management Agent môže byť odinštalovaný niekoľkými spôsobmi.

Vzdialené odinštalovanie pomocou ESMC Web Console

1. [Prihláste sa do ESMC Web Console](#).
2. Na karte **Počítače** vyberte počítač, z ktorého chcete odstrániť ESET Management Agentu a kliknite na **Nová úloha**.
Prípadne vyberte viacero počítačov pomocou príslušných začiarkovacích políčok a kliknite na **Úlohy > Nová úloha**.
3. Zadajte **Názov** úlohy.
4. Z roletového menu **Kategória úlohy** vyberte ESET Security Management Center.
5. Z roletového menu **Úloha** vyberte **Ukončiť spravovanie (Odinštalovať ESET Management Agentu)**.
6. Skontrolujte **Súhrn** úlohy a kliknite na Dokončiť.

Spúšťač bude automaticky vytvorený s čo najskorším časom spustenia. Ak chcete zmeniť **Typ spúšťača**, kliknite na **Správca > Úlohy pre klienta**. Rozbaľte požadovanú úlohu pre klienta kliknutím na **+**. Následne pod úlohou kliknite na spúšťač a zvolte možnosť **Upraviť**.

i Poznámka:

Viac informácií sa dozviete v časti [Úloha pre klienta](#) v príručke správcu.

Lokálne odinštalovanie

1. Pripojte sa na koncový počítač, na ktorom chcete odstrániť ESET Management Agentu (napr. cez RDP).
2. Prejdite do **Ovládací panel > Programy a súčasti** a dvojitým kliknutím vyberte **ESET Management Agentu**.
3. Kliknite na **Ďalej > Odinštalovať** a postupujte podľa inštrukcií.

! Dôležité:

Ak ste pre ESET Management Agentu nastavili heslo pomocou politiky, budete ho musieť zadať počas odinštalovania. Druhou možnosťou je pred odinštalovaním ESET Management Agentu deaktivovať príslušnú politiku.

Riešenie problémov s odinštalovaním ESET Management Agentu

- Pozrite si časť [protokoly](#) (ESET Management Agent).

- ESET Management Agentu môžete odinštalovať použitím nástroja [ESET Uninstaller](#) alebo neštandardným spôsobom (napr. odstránením súborov, služby ESET Management Agent a položiek databázy Registry). Ak sa na rovnakom počítači nachádza aj produkt ESET určený pre koncové zariadenia, tento postup nebude možný, pretože agent je chránený funkciou [Self-Defense](#). Viac informácií nájdete v našom [článku databázy znalostí](#).

4.3.5.4 Nástroj na nasadenie

ESET Remote Deployment Tool je nástroj, ktorý vám umožňuje vzdialene nasadiť ESET Management Agentu prostredníctvom all-in-one inštalačného balíka vytvoreného cez ESMC. Tento nástroj na nasadenie sa spúšťa pod účtom s oprávneniami správcu, čo by malo pomôcť vyriešiť chyby zabezpečenia vyskytujúce sa na ESMC Serveroch bežiacich ako sieťová služba (Network Service), prípadne na virtuálnych zariadeniach ESMC Server bežiacich na operačnom systéme CentOS.

i Poznámka:

ESET Remote Deployment Tool je samostatný nástroj určený na nasadenie ESET Management Agentov na klientske počítače s operačným systémom Windows.

Pre nasadenie ESET Management Agentu pomocou tejto metódy postupujte podľa krokov nižšie:

1. Z webovej stránky spoločnosti ESET [stiahnite nástroj Deployment tool](#).
2. Uistite sa, že boli splnené všetky [požiadavky](#).
3. Spustíte nástroj ESET Remote Deployment Tool na klientskom počítači.
4. Vyberte si jednu z nasledujúcich možností nasadenia ESMC Agentov:
 - [Active Directory](#) – pri zvolení tejto možnosti bude potrebné zadať prihlasovacie údaje k Active Directory. Táto možnosť vám umožňuje exportovať štruktúru Active Directory a následne ju importovať do ESMC alebo ECA pre jednoduchý výber cieľových počítačov, na ktorých má prebehnúť nasadenie agentov.
 - [Scan Network](#) – prostredníctvom tejto možnosti môžete nájsť počítače v sieti zadaním konkrétneho rozsahu IP adries.
 - [Import list](#) – táto možnosť vám umožňuje importovať súbor so zoznamom názvov hostiteľov alebo IP adries.
 - [Add computers manually](#) – v rámci tejto možnosti je potrebné pridať zoznam názvov hostiteľov alebo IP adries manuálne.

i Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukázkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.1 Požiadavky pre nástroj na nasadenie

Pre použitie nástroja ESET Remote Deployment Tool na systéme Windows sa vyžaduje splnenie nasledujúcich požiadaviek:

! Dôležité:

- All-in-one inštalačný balík musí byť [vytvorený](#) a [pripravený](#) na lokálnom disku.
- Na [vytvorenie all-in-one inštalačného balíka](#) je potrebné mať príslušné povolenia.
- ESMC Server a ESMC Web Console musia byť nainštalované (na serverový počítač).
- Musia byť otvorené a dostupné potrebné porty. Pozrite si časť [ESET Management Agent – využitie pri vzdialenom nasadení ESET Management Agentu na cieľové počítače s operačným systémom Windows](#):
- V názve inštalačného balíka musí byť zahrnutý výraz "x86" alebo "x64". V opačnom prípade nasadenie balíka zlyhá.

i Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukázkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.2 Výber počítačov z Active Directory

Táto kapitola dopĺňa predchádzajúcu kapitolu a popisuje kroky, ktoré je potrebné dodržať pri nasadzovaní ESET Management Agentu:

1. Prečítajte si **Licenčnú dohodu s koncovým používateľom** (EULA), potvrdte ju, a následne kliknite na **Ďalej**.
2. Zadajte názov alebo IP adresu **Active Directory servera** a **Port**, na ktorom sa naň chcete pripojiť.
3. Zadajte prihlasovacie meno a heslo (**Username** a **Password**), ktoré chcete použiť na prihlásenie na Active Directory server. Ak označíte možnosť **Use current user credentials**, automaticky sa vyplnia prihlasovacie údaje aktuálne prihláseného používateľa.
4. Možnosť **Export computer list for Security Management Center** označte v prípade, že chcete exportovať štruktúru Active Directory na účely následného importu do ESMC.

Poznámka:

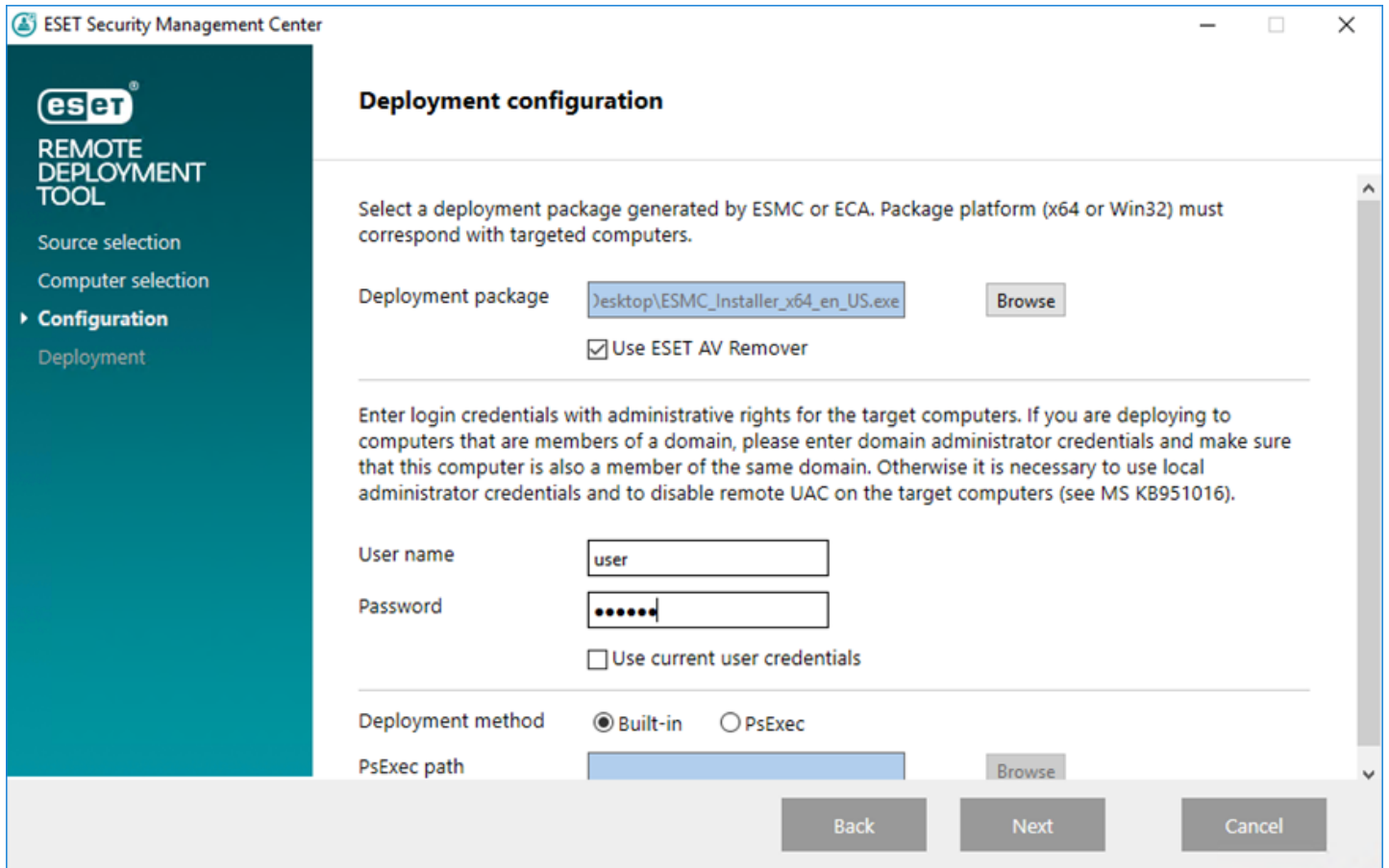
Ak sa počítač nachádza v Active Directory, kliknutím na **Next** budete automaticky prihlásený do prednastaveného doménového radiča.

5. Označte počítače, ktoré chcete pridať a kliknite na **Next**. Pre zobrazenie všetkých počítačov vo vybranej skupine označte možnosť **Include subgroups**.
6. Zobrazia sa vami zvolené počítače, na ktorých má prebehnúť vzdialené nasadenie. Uistite sa, že všetky počítače sú pridané a následne kliknite na **Next** (Ďalej).

Dôležité:

Všetky zvolené počítače musia mať rovnakú platformu (64-bitový alebo 32-bitový operačný systém).

7. Kliknite na tlačidlo **Browse** (Prehľadávať) a vyberte all-in-one inštalačný balík [vytvorený](#) cez ESMC Web Console. Pokiaľ na vašom lokálnom počítači nie je nainštalované žiadne iné bezpečnostné riešenie, zrušte označenie možnosti **Use ESET AV Remover** (Použiť ESET AV Remover). Nástroj ESET AV Remover dokáže odstrániť [niektoré aplikácie](#).
8. Zadajte prihlasovacie údaje k cieľovým počítačom. Pokiaľ sú počítače súčasťou domény, zadajte prihlasovacie údaje k účtu **doménového administrátora**. Pri použití **lokálneho administrátorského účtu** je potrebné [na cieľových počítačoch vypnúť Kontrolu používateľských kont \(UAC\)](#). Ak označíte možnosť **Use current user credentials**, automaticky sa vyplnia prihlasovacie údaje aktuálne prihláseného používateľa.
9. Vyberte spôsob vzdialeného nasadenia (deployment method), t. j. metódu umožňujúcu spúšťanie programov na vzdialených zariadeniach. **Built-in** metóda je predvoleným nastavením a podporuje chybové hlásenia systému Windows. Na nasadenie je možné použiť taktiež nástroj tretej strany **PsExec**. Vyberte jednu z týchto dvoch možností a kliknite na tlačidlo **Next** (Ďalej).



10. Akonáhle sa začne proces inštalácie, zobrazí sa správa „Success“ (Úspešné). Pre dokončenie nasadenia kliknite na tlačidlo **Finish** (Dokončiť). Pokiaľ nasadenie zlyhá, môžete vygenerovať zoznam počítačov, na ktorých sa inštalačný balík nepodarilo nasadiť. Urobiť tak môžete kliknutím na tlačidlo **Browse** (Prehľadávať) vedľa poľa **Export failed computers**, následným zvolením .txt súboru, do ktorého chcete zoznam uložiť, a kliknutím na tlačidlo **Export failed computer**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Správne fungovanie ESET Management Agentu na klientskom počítači si môžete overiť pomocou protokolu (umiestnený na klientskom počítači v `C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html`).

i Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukážkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.3 Vyhľadávanie počítačov v lokálnej sieti

Táto kapitola dopĺňa predchádzajúcu kapitolu a popisuje kroky, ktoré je potrebné dodržať pri nasadzovaní ESET Management Agentu:

1. Prečítajte si **Licenčnú dohodu s koncovým používateľom** (EULA), potvrdte ju, a následne kliknite na **Ďalej**.
2. Do poľa **IP Ranges** zadajte rozsah IP adries siete vo formáte *10.100.100.10-10.100.100.250*.
3. Vyberte si jednu z nasledujúcich možností vyhľadávania (**Scan methods**):
 - **Ping scan** – vyhľadá klientske počítače pomocou príkazu ping.
4. Pre vyhľadanie počítačov v sieti kliknite na **Start scan**.
5. Označte počítače, ktoré chcete pridať a kliknite na **Next**.
6. Zobrazia sa vami zvolené počítače, na ktorých má prebehnúť vzdialené nasadenie. Uistite sa, že všetky počítače sú pridané a následne kliknite na **Next** (Ďalej).

i Poznámka:

Majte na pamäti, že niektoré klientske počítače v tejto sieti nemusia na príkaz ping reagovať v závislosti od nastavení firewallu.

- **Port scan** – na vyhľadanie počítačov je použitá technika skenovania portov. V kapitole [Používané porty](#) nájdete informácie o portoch používaných na vzdialené nasadenie ESET Management Agentov. Štandardný port je 445.

! Dôležité:

Všetky zvolené počítače musia mať rovnakú platformu (64-bitový alebo 32-bitový operačný systém).

7. Kliknite na tlačidlo **Browse** (Prehľadávať) a vyberte all-in-one inštalačný balík [vytvorený](#) cez ESMC Web Console. Pokiaľ na vašom lokálnom počítači nie je nainštalované žiadne iné bezpečnostné riešenie, zrušte označenie možnosti **Use ESET AV Remover** (Použiť ESET AV Remover). Nástroj ESET AV Remover dokáže odstrániť [niektoré aplikácie](#).
8. Zadajte prihlasovacie údaje k cieľovým počítačom. Pokiaľ sú počítače súčasťou domény, zadajte prihlasovacie údaje k účtu **doménového administrátora**. Pri použití **lokálneho administrátorského účtu** je potrebné [na cieľových počítačoch vypnúť Kontrolu používateľských kont \(UAC\)](#). Ak označíte možnosť **Use current user credentials**, automaticky sa vyplnia prihlasovacie údaje aktuálne prihláseného používateľa.
9. Vyberte spôsob vzdialeného nasadenia (deployment method), t. j. metódu umožňujúcu spúšťanie programov na vzdialených zariadeniach. **Built-in** metóda je predvoleným nastavením a podporuje chybové hlásenia systému Windows. Na nasadenie je možné použiť taktiež nástroj tretej strany **PsExec**. Vyberte jednu z týchto dvoch možností a kliknite na tlačidlo **Next** (Ďalej).

ESET Security Management Center

eset
REMOTE DEPLOYMENT TOOL

Source selection
Computer selection
► **Configuration**
Deployment

Deployment configuration

Select a deployment package generated by ESMC or ECA. Package platform (x64 or Win32) must correspond with targeted computers.

Deployment package

Use ESET AV Remover

Enter login credentials with administrative rights for the target computers. If you are deploying to computers that are members of a domain, please enter domain administrator credentials and make sure that this computer is also a member of the same domain. Otherwise it is necessary to use local administrator credentials and to disable remote UAC on the target computers (see MS KB951016).

User name

Password

Use current user credentials

Deployment method Built-in PsExec

PsExec path

10. Akonáhle sa začne proces inštalácie, zobrazí sa správa „Success“ (Úspešné). Pre dokončenie nasadenia kliknite na tlačidlo **Finish** (Dokončiť). Pokiaľ nasadenie zlyhá, môžete vygenerovať zoznam počítačov, na ktorých sa inštalačný balík nepodarilo nasadiť. Urobiť tak môžete kliknutím na tlačidlo **Browse** (Prehľadávať) vedľa poľa **Export failed computers**, následným zvolením .txt súboru, do ktorého chcete zoznam uložiť, a kliknutím na tlačidlo **Export failed computer**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Správne fungovanie ESET Management Agentu na klientskom počítači si môžete overiť pomocou protokolu (umiestnený na klientskom počítači v `C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html`).

i Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukážkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.4 Importovanie zoznamu počítačov

Táto kapitola dopĺňa predchádzajúcu kapitolu a popisuje kroky, ktoré je potrebné dodržať pri nasadzovaní ESET Management Agent:

1. Prečítajte si **Licenčnú dohodu s koncovým používateľom** (EULA), potvrdte ju, a následne kliknite na **Ďalej**.
2. Vyberte si jednu z nasledujúcich možností:
 - Textový súbor: súbor obsahujúci názvy hostiteľov alebo IP adresy. Každá IP adresa alebo názov hostiteľa musí byť na osobitnom riadku.
 - Security Management Center export: súbor obsahujúci názvy hostiteľov alebo IP adresy, [exportovaný z ESMC Web Console](#).
3. Kliknite na **Browse**, vyberte súbor, ktorý chcete odovzdať, a kliknite na **Next**.
4. Zobrazia sa vami zvolené počítače, na ktorých má prebehnúť vzdialené nasadenie. Uistite sa, že všetky počítače sú pridané a následne kliknite na **Next** (Ďalej).

Dôležité:

Všetky zvolené počítače musia mať rovnakú platformu (64-bitový alebo 32-bitový operačný systém).

- Kliknite na tlačidlo **Browse** (Prehľadávať) a vyberte all-in-one inštalačný balík [vytvorený](#) cez ESMC Web Console. Pokiaľ na vašom lokálnom počítači nie je nainštalované žiadne iné bezpečnostné riešenie, zrušte označenie možnosti **Use ESET AV Remover** (Použiť ESET AV Remover). Nástroj ESET AV Remover dokáže odstrániť [niektoré aplikácie](#).
- Zadajte prihlasovacie údaje k cieľovým počítačom. Pokiaľ sú počítače súčasťou domény, zadajte prihlasovacie údaje k účtu **doménového administrátora**. Pri použití **lokálneho administrátorského účtu** je potrebné [na cieľových počítačoch vypnúť Kontrolu používateľských kont \(UAC\)](#). Ak označíte možnosť **Use current user credentials**, automaticky sa vyplnia prihlasovacie údaje aktuálne prihláseného používateľa.
- Vyberte spôsob vzdialeného nasadenia (deployment method), t. j. metódu umožňujúcu spúšťanie programov na vzdialených zariadeniach. **Built-in** metóda je predvoleným nastavením a podporuje chybové hlásenia systému Windows. Na nasadenie je možné použiť taktiež nástroj tretej strany **PsExec**. Vyberte jednu z týchto dvoch možností a kliknite na tlačidlo **Next** (Ďalej).

ESET Security Management Center

Deployment configuration

Select a deployment package generated by ESMC or ECA. Package platform (x64 or Win32) must correspond with targeted computers.

Deployment package:

Use ESET AV Remover

Enter login credentials with administrative rights for the target computers. If you are deploying to computers that are members of a domain, please enter domain administrator credentials and make sure that this computer is also a member of the same domain. Otherwise it is necessary to use local administrator credentials and to disable remote UAC on the target computers (see MS KB951016).

User name:

Password:

Use current user credentials

Deployment method: Built-in PsExec

PsExec path:

- Akonáhle sa začne proces inštalácie, zobrazí sa správa „Success“ (Úspešné). Pre dokončenie nasadenia kliknite na tlačidlo **Finish** (Dokončiť). Pokiaľ nasadenie zlyhá, môžete vygenerovať zoznam počítačov, na ktorých sa inštalačný balík nepodarilo nasadiť. Urobiť tak môžete kliknutím na tlačidlo **Browse** (Prehľadávať) vedľa poľa **Export failed computers**, následným zvolením .txt súboru, do ktorého chcete zoznam uložiť, a kliknutím na tlačidlo **Export failed computer**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Správne fungovanie ESET Management Agentu na klientskom počítači si môžete overiť pomocou protokolu (umiestnený na klientskom počítači v `C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html`).

Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukážkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.5 Manuálne pridanie počítačov

Táto kapitola dopĺňa predchádzajúcu kapitolu a popisuje kroky, ktoré je potrebné dodržať pri nasadzovaní ESET Management Agentu:

1. Prečítajte si **Licenčnú dohodu s koncovým používateľom** (EULA), potvrdte ju, a následne kliknite na **Ďalej**.
2. Zadajte názvy hostiteľov a IP adresy a následne kliknite na **Next** (Ďalej). Každá IP adresa alebo názov hostiteľa musí byť na osobitnom riadku.

Dôležité:

Všetky zvolené počítače musia mať rovnakú platformu (64-bitový alebo 32-bitový operačný systém).

3. Zobrazia sa vami zvolené počítače, na ktorých má prebehnúť vzdialené nasadenie. Uistite sa, že všetky počítače sú pridané a následne kliknite na **Next** (Ďalej).
4. Kliknite na tlačidlo **Browse** (Prehľadávať) a vyberte all-in-one inštalačný balík [vytvorený](#) cez ESMC Web Console. Pokiaľ na vašom lokálnom počítači nie je nainštalované žiadne iné bezpečnostné riešenie, zrušte označenie možnosti **Use ESET AV Remover** (Použiť ESET AV Remover). Nástroj ESET AV Remover dokáže odstrániť [niektoré aplikácie](#).
5. Zadajte prihlasovacie údaje k cieľovým počítačom. Pokiaľ sú počítače súčasťou domény, zadajte prihlasovacie údaje k účtu **doménového administrátora**. Pri použití **lokálneho administrátorského účtu** je potrebné [na cieľových počítačoch vypnúť Kontrolu používateľských kont \(UAC\)](#). Ak označíte možnosť **Use current user credentials**, automaticky sa vyplnia prihlasovacie údaje aktuálne prihláseného používateľa.
6. Vyberte spôsob vzdialeného nasadenia (deployment method), t. j. metódu umožňujúcu spúšťanie programov na vzdialených zariadeniach. **Built-in** metóda je predvoleným nastavením a podporuje chybové hlásenia systému Windows. Na nasadenie je možné použiť taktiež nástroj tretej strany **PsExec**. Vyberte jednu z týchto dvoch možností a kliknite na tlačidlo **Next** (Ďalej).

ESET Security Management Center

eset
REMOTE DEPLOYMENT TOOL

Source selection
Computer selection
► **Configuration**
Deployment

Deployment configuration

Select a deployment package generated by ESMC or ECA. Package platform (x64 or Win32) must correspond with targeted computers.

Deployment package

Use ESET AV Remover

Enter login credentials with administrative rights for the target computers. If you are deploying to computers that are members of a domain, please enter domain administrator credentials and make sure that this computer is also a member of the same domain. Otherwise it is necessary to use local administrator credentials and to disable remote UAC on the target computers (see MS KB951016).

User name

Password

Use current user credentials

Deployment method Built-in PsExec

PsExec path

7. Akonáhle sa začne proces inštalácie, zobrazí sa správa „Success“ (Úspešné). Pre dokončenie nasadenia kliknite na tlačidlo **Finish** (Dokončiť). Pokiaľ nasadenie zlyhá, môžete vygenerovať zoznam počítačov, na ktorých sa inštalačný balík nepodarilo nasadiť. Urobiť tak môžete kliknutím na tlačidlo **Browse** (Prehľadávať) vedľa poľa **Export failed computers**, následným zvolením .txt súboru, do ktorého chcete zoznam uložiť, a kliknutím na tlačidlo **Export failed computer**.

Progress	
COMPUTER	STATUS
✓ [blurred]	Success

Správne fungovanie ESET Management Agentu na klientskom počítači si môžete overiť pomocou protokolu (umiestnený na klientskom počítači v `C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html`).

i Poznámka:

Nasadenie môže zlyhať z niekoľkých dôvodov. V prípade akýchkoľvek problémov s nasadením si prečítajte kapitolu [Riešenie problémov](#) alebo [Ukážkové scenáre nasadenia ESET Management Agentu](#).

4.3.5.4.6 Riešenie problémov

Nasadenie môže zlyhať z niekoľkých dôvodov uvedených v tabuľke nižšie, pričom samotné zlyhanie je sprevádzané viacerými chybovými hláseniami:

Chybové hlásenie	Možná príčina
The network path was not found (error code 0x35)	<ul style="list-style-type: none"> Klient nie je dostupný v sieti, firewall blokuje komunikáciu. Prichádzajúca komunikácia na portoch 135, 137, 138, 139 a 445 nie je povolená vo firewallle. Nie je použitá výnimka povoľujúca prichádzajúce požiadavky na zdieľanie súborov a tlačiarň. Hostiteľský názov klienta sa nepodarilo rozpoznať. Použite platný FQDN názov počítača (úplný názov domény).
Access is denied (error code 0x5) The user name or password is incorrect (error code 0x52e)	<ul style="list-style-type: none"> Ak je aj server, aj klient pripojený k doméne, použite prihlasovacie údaje používateľa, ktorý je doménovým správcom, a to vo formáte doména\používateľ. 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.
The installation package is not supported by this processor type (error code 1633)	Inštalačný balík nie je určený pre túto platformu. Vytvorte v ESMC Web Console inštalačný balík pre správnu platformu (64-bitový alebo 32-bitový operačný systém).

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

Možná príčina	Riešenie problémov
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. Po úspešnom nasadení nie sú porty 2222 s 2223 otvorené vo firewallle. Povoľte tieto porty vo všetkých firewall riešeniach medzi klientom a serverom.
Hostiteľský názov klienta sa nepodarilo rozpoznať	Medzi možné riešenia problémov s DNS môže patriť: <ul style="list-style-type: none"> Použitie príkazu <code>nslookup</code> 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, <code>nslookup</code> pre názov hostiteľa by mal byť preložený na IP adresu, ktorú zobrazí príkaz <code>ipconfig</code> na danom hostiteľovi. Príkaz <code>nslookup</code> bude potrebné spustiť na klientských počítačoch a na serveri. Manuálne skontrolovať DNS záznamy pre duplikáty.
Účet správcu nemá nastavené heslo	Nastavte heslo pre účet správcu (nepoužívajte prázdne heslo).

Možná příčina	Riešenie problémov
Nedostatočné prístupové práva	<p>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.</p> <p>Na operačnom systéme Windows 7 a novších musí byť pred spustením úlohy nasadenia agenta aktivovaný účet správcu. Môžete vytvoriť lokálneho používateľa, ktorý bude členom skupiny správcov, alebo povoliť vstavaný účet správcu.</p> <p>Aktivácia účtu správcu:</p> <ol style="list-style-type: none"> Otvorte príkazový riadok. Zadajte nasledujúci príkaz: <code>net user administrator /active:yes</code>
Správcovské zdieľanie ADMIN\$ nie je dostupné	<p>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).</p>
Správcovské zdieľanie IPC\$ nie je dostupné	<p>Skontrolujte, či má server prístup do IPC\$ pomocou nasledujúceho príkazu spúšťaného v príkazovom riadku na serveri:</p> <pre>net use \\clientname\IPC\$ kde clientname je názov cieľového počítača.</pre>
Je aktívne zjednodušené zdieľanie súborov	<p>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:</p> <ul style="list-style-type: none"> Kliknite na Štart, do vyhľadávacieho poľa napíšte priečink a kliknite na Možnosti priečinka. Ďalej kliknite na kartu Zobrazenie a v dolnej časti sekcie Rozšírené nastavenia zrušte označenie možnosti Použiť Sprievodcu zdieľaním.

4.3.6 Inštalácia Web Console – Windows

i Poznámka:

Nástroj ESMC Web Console môžete nainštalovať aj na iný počítač ako ten, na ktorom je nainštalovaný ESMC Server.

Pre inštaláciu komponentu ESMC Web Console na operačnom systéme Windows postupujte podľa nasledujúcich krokov:

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Uistite sa, že boli splnené nasledujúce prerekvizity:
 - ESMC Server.
 - [Java](#) – vždy používajte najnovšiu oficiálnu verziu Javy (minimálna verzia Javy vyžadovaná nástrojom ESMC Web Console je verzia 8, avšak aj napriek tomu odporúčame, aby ste vždy používali najnovšiu verziu). Podrobnejšie informácie o inštalácii Javy nájdete v našom [článku databázy znalostí](#).
 - [Apache Tomcat](#) ([podporovaná](#) verzia). Odporúčame inštalovať Apache Tomcat pomocou inštalátora služieb pre systém Windows (.exe).
 - Web Console súbor (`era.war`) uložený na lokálnom pevnom disku.
3. Skopírujte `era.war` do Apache Tomcat priečinka s webovými aplikáciami: Prejdite do **Štart > Apache Tomcat > programový adresár Tomcat** a otvorte priečink **webapps** (na väčšine operačných systémov Windows je to `C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\`).
4. Počkajte, kým sa súbor extrahuje a prebehne inštalácia ESMC Web Console.

Ak ste nainštalovali ESMC Web Console na iný počítač ako ten, na ktorom je nainštalovaný ESMC Server, vykonajte nasledujúce kroky pre umožnenie komunikácie medzi ESMC Web Console a ESMC Serverom:

- I. Zastavte službu *Apache Tomcat*. Prejdite do sekcie **Štart > Apache Tomcat > Konfigurovať Tomcat** a kliknite na **Zastaviť**.
- II. Otvorte Poznámkový blok ako správca a upravte súbor `C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`.
- III. Vyhľadajte položku `server_address=localhost`.
- IV. Nahraďte `localhost` IP adresou vášho ESMC Servera a uložte súbor.
5. Reštartujte službu *Apache Tomcat*. **Štart > Apache Tomcat > Konfigurovať Tomcat**. Kliknite na **Zastaviť**, počkajte 30 sekúnd, a kliknite na **Štart**.
6. Otvorte ESMC Web Console vo svojom webovom prehliadači: <http://localhost/era/>. Zobrazí sa prihlasovacia obrazovka nástroja Web Console.

i Poznámka:

HTTP port, štandardne 8080, sa nastaví počas manuálnej inštalácie Apache Tomcat. Môžete tiež nastaviť [HTTPS pripojenie pre Apache Tomcat](#).

4.3.7 Inštalácia proxy

Ak vykonávate aktualizáciu v rámci existujúceho prostredia, riadte sa [nasledujúcim postupom](#). Pre vykonanie novej inštalácie proxy postupujte podľa nasledujúcich krokov:

1. [Nainštalujte Apache HTTP Proxy](#) na svoj počítač. Použite prednastavenú ESET verziu [Apache](#).
2. Upravte konfiguračný súbor *Apache HTTP Proxy – httpd.conf*, ktorý sa nachádza v `C:\Program Files\Apache HTTP Proxy\conf`. Štandardne sa používa port číslo 2222, ak ste však zmenili port počas inštalácie, použite vlastné číslo portu.
 - a. Pridajte nasledujúci riadok: `AllowCONNECT 443 563 2222`

```
<Proxy *>
Deny from all
</Proxy>
#*.eset.com:
AllowCONNECT 443 563 2222
<ProxyMatch>
```

- b. Do osobitného segmentu `ProxyMatch` pridajte:
 - i. adresu, ktorú používajú vaše agenty na pripojenie k ESMC Serveru,
 - ii. všetky možné adresy vášho ESMC Servera (IP, FQDN atď.).
Pridajte celý kód zobrazený nižšie, IP adresa 10.0.0.10 slúži len ako príklad a je potrebné nahradiť ju vašou vlastnou adresou.

```
</ProxyMatch>
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(10.0.0.10)>
Allow from all
</ProxyMatch>
```

- c. Reštartujte službu *Apache HTTP Proxy*.

4.3.8 Inštalácia nástroja RD Sensor – Windows

Pre inštaláciu nástroja RD Sensor na operačnom systéme Windows postupujte podľa nasledovných krokov:

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Uistite sa, že boli splnené všetky [požiadavky](#).
3. Inštaláciu spustíte dvojitým kliknutím na inštalačný balík.
4. Vyberte umiestnenie, kde bude nástroj RD Sensor nainštalovaný a kliknite na **Ďalej > Inštalovať**.

4.3.8.1 Prerekvizity pre RD Sensor

Pre inštaláciu nástroja RD Sensor na operačnom systéme Windows je potrebné splniť nasledujúce prerekvizity:

- [WinPcap](#) – použite najnovšiu verziu WinCap (minimálne 4.1.0).
- Sieť by mala byť správne nastavená (otvorené vhodné [porty](#), prichádzajúca komunikácia by nemala byť blokovaná firewallom atď.).
- ESMC Server musí byť dostupný.
- Pre správne fungovanie všetkých súčastí musí byť na lokálnom počítači nainštalovaný [ESET Management Agent](#).
- Protokol nástroja Rogue Detection Sensor sa nachádza v nasledujúcom umiestnení: C:
`\ProgramData\ESET\Rogue Detection Sensor\Logs\`

4.3.9 Mirror Tool

Mirror Tool je nástroj, ktorý sa používa na aktualizáciu detekčného jadra v offline prostredí. V prípade, že bezpečnostné produkty ESET na vašich klientskych počítačoch potrebujú aktualizácie detekčného jadra, no nemajú pripojenie na internet, môžete použiť nástroj Mirror Tool, ktorý sťahuje aktualizčné súbory z aktualizčných serverov spoločnosti ESET a ukladá ich lokálne.

Poznámka:

Mirror Tool sťahuje len aktualizácie detekčného jadra, nepodporuje aktualizácie programových súčastí (PCU) ani LiveGrid dáta. Nástroj Mirror Tool dokáže tiež vytvoriť [offline repozitár](#). Môžete sa tiež rozhodnúť aktualizovať produkty ESET individuálne.

Prerekvizity

Dôležité:

Nástroj Mirror Tool nepodporuje Windows XP a Windows Server 2003.

- Cieľový priečinok musí byť zdieľaný pomocou služieb Samba/Windows alebo HTTP/FTP.
- Musíte mať platný [offline licenčný súbor](#), ktorý obsahuje používateľské meno a heslo. Pri vytváraní licenčného súboru je potrebné označiť možnosť **Zahrnúť meno a heslo**. Musíte tiež zadať **Názov** licenčného súboru. Offline licenčný súbor je nevyhnutný pre aktiváciu nástroja Mirror Tool a vytvorenie aktivačného mirror servera.

Create offline license file

Product

- ESET Endpoint Antivirus for Windows
- ESET Endpoint Security for Windows
- ESET Endpoint Antivirus for Mac OS X
- ESET NOD32 Antivirus Business Edition for Linux Desktop
- ESET Endpoint Security for Mac OS X
- ESET Virtualization Security
- ESET Shared Local Cache
- ESET Virtual Agent Host
- ESET Mobile Device Connector

Name

Units count /9

Username and password

Include Username and Password
When included it is possible to update from ESET servers

Remote administrator

Allow management with Remote Administrator

ERA management token

GENERATE **CANCEL**

- Musíte mať k dispozícii súbor nástroja Mirror Tool. Nástroj je dostupný k stiahnutiu na [webovej stránke spoločnosti ESET](#) v sekcii **Samostatné inštalátory**.
- Na počítači, na ktorom bude používaný nástroj Mirror Tool, musíte mať nainštalovaný balík [Visual C++ Redistributable for Visual Studio 2010](#).
- Na počítači, na ktorom bude používaný nástroj Mirror Tool, musíte mať nainštalovaný balík [Visual C++ Redistributables for Visual Studio 2015](#).
- Nástroj pozostáva z dvoch súborov:
 - Windows: MirrorTool.exe a updater.dll
 - Linux: MirrorTool a updater.so

Použitie

- Pre zobrazenie pomocníka pre Mirror nástroj spustíte `MirrorTool --help`. Zobrazia sa všetky dostupné príkazy nástroja:

```
C:\Users\>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2017. All rights reserved.
Allowed options:
--mirrorType arg                [required for module update]
                                Type of mirror. Possible values (case
                                insensitive): regular, pre-release,
                                delayed.
--intermediateUpdateDirectory arg [required for module update]
                                Files will be downloaded to this
                                directory to create mirror in output
                                directory.
--offlineLicenseFilename arg    [required for module update]
                                Offline license file.
--updateServer arg              [optional]
                                Update server. (e.g.:
                                http://update.eset.com/eset_upd/ep6/)
                                Mirror will be created in output
                                directory, only specified path in
                                server will be mirrored.
--outputDirectory arg           [required for module update]
                                Directory where mirror will be created.
--proxyHost arg                 [optional]
                                Http proxy address (fqdn or IP).
--proxyPort arg                 [optional]
                                Http proxy port.
--proxyUsername arg             [optional]
                                Http proxy username.
--proxyPassword arg             [optional]
                                Http proxy password.
--networkDriveUsername arg      [optional]
                                Username used, when output directory is
                                accessed using smb(e.g:\\hostname).
--networkDrivePassword arg      [optional]
                                Password used, when output directory is
                                accessed using smb(e.g:\\hostname).
--excludedProducts arg          [optional]
                                Disable creating mirror for specified
                                products. Possible values: ep4 ep5 ep6
                                era6.
--repositoryServer arg          [required for repository update]
                                Repository server for repository
                                creation.
--intermediateRepositoryDirectory arg [required for repository update]
                                Files will be downloaded to this
                                directory to create offline mirror in
                                output directory.
--outputRepositoryDirectory arg [required for repository update]
                                Directory where offline repository will
                                be created..
--help                           [optional]
                                Display this help and exit
```

- Parameter `--updateServer` je voliteľný. Pri použití tohto parametra musíte zadať celú URL adresu aktualizáčného servera.

- Parameter `--offlineLicenseFilename` je povinný. Musíte zadať celú cestu k offline licenčnému súboru (ako je to popísané vyššie).
- Pre vytvorenie mirroru spustíte `MirrorTool` minimálne so všetkými povinnými parametrami. Príklad:
 - Windows:

```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

- Linux:

```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

Nástroj Mirror Tool a nastavenia aktualizácií

- Pre automatizáciu distribúcie aktualizácií vírusovej databázy môžete naplánovať spúšťanie nástroja Mirror Tool. Otvorte Web Console a prejdite do sekcie **Úlohy pre klienta > Operačný systém > Spustiť príkaz. Vyberte Príkazový riadok na spustenie** (vrátane cesty k súboru `MirrorTool.exe`) a spúšťač (napríklad CRON výraz pre každú hodinu `00 * * * ? *`). Na plánované spustenie môžete tiež použiť nástroj Plánovač úloh pre systém Windows alebo na systéme Linux použiť Cron.
- Pre zmenu nastavení aktualizácií na klientských počítačoch použijete novú politiku a nastavíte **Aktualizačný server** tak, aby odkazoval na adresu mirror serveru alebo zdieľaný priečinok.

4.3.10 Inštalácia komponentu Mobile Device Connector

Pre inštaláciu komponentu Mobile Device Connector pre ESET Security Management Center Server postupujte podľa nasledujúcich krokov.

Upozornenie:

Aby mohli byť mobilné zariadenia spravované vždy bez ohľadu na ich polohu, Mobile Device Connector musí byť prístupný z internetu.

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Najprv si však prečítajte [prerekvizity](#) a uistite sa, že všetky sú splnené.
3. Spustíte inštalátor komponentu Mobile Device Connector a potvrdíte Licenčnú dohodu s koncovým používateľom (EULA), ak s ňou súhlasíte.
4. Kliknite na **Prehľadávať**, prejdite do umiestnenia vášho [SSL certifikátu](#) používaného na komunikáciu cez HTTPS a zadajte heslo pre tento certifikát.

5. Uprávnite **MDM názov hostiteľa**: toto je verejná doména alebo verejná IP adresa vášho MDM servera a teda je dostupná pre mobilné zariadenia z internetu.

! Dôležité:

MDM názov hostiteľa musí byť zadaný v rovnakej podobe ako je uvedený vo vašom **HTTPS certifikáte servera**. V opačnom prípade iOS mobilné zariadenie odmietne nainštalovať [MDM profil](#). Napríklad, ak je v HTTPS certifikáte špecifikovaná IP adresa, zadajte túto IP adresu do poľa **MDM názov hostiteľa**. V prípade, že je špecifikované FQDN (napr. `mdm.mycompany.com`) v HTTPS certifikáte, zadajte toto FQDN do poľa **MDM názov hostiteľa**. Taktiež, ak je použitá hviezdica (*) (napr. `*.mycompany.com`) v HTTPS certifikáte, môžete do poľa **MDM názov hostiteľa** zadať `mdm.mycompany.com`.

7. Inštalátor sa teraz potrebuje pripojiť k existujúcej databáze, ktorá bude používaná komponentom Mobile Device Connector. Uprávnite nasledujúce údaje o pripojení:

- **Databáza:** MySQL Server/MS SQL Server/MS SQL Server cez Windows Authentication
- **ODBC ovládač:** MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server.
- **Názov databázy:** môžete ponechať preddefinovaný názov databázy alebo ho zmeniť. Ak je to možné, odporúčame používať predvolený názov databázy `era_mdm_db`.
- **Názov hostiteľa:** názov hostiteľa alebo IP adresa vášho databázového servera.
- **Port:** číslo portu používaného na pripojenie k serveru
- **Používateľské meno/heslo** k účtu správcu databázy.
- **Použiť inštanciu s názvom** – ak používate MS SQL databázu, môžete označiť možnosť **Použiť inštanciu s názvom**. Následne budete môcť použiť vlastnú inštanciu databázy zadaním názvu hostiteľa v tvare `HOSTNAME\DB_INSTANCE`, napríklad: `192.168.0.10\ESMC7SQL`. Pre klastrovú databázu použijete len názov klastra. Ak je zvolená táto možnosť, nebude možné zmeniť port, ktorý bude použitý – systém použije porty predvolené spoločnosťou Microsoft.

i Poznámka:

Ak zvolíte možnosť **Použiť inštanciu s názvom**, ESMC Server môžete pripojiť aj k MS SQL databáze, ktorá je nainštalovaná na Failover klastri. Do poľa **Názov hostiteľa** zadajte názov klastra.

i Poznámka:

Môžete použiť rovnaký databázový server ako používate pre ESMC databázu, odporúčame však použiť iný databázový server, ak plánujete zaregistrovať viac ako 80 mobilných zariadení.

6. Zadajte používateľské meno pre vytvorenú databázu nástroja Mobile Device Connector. Môžete **Vytvoriť nového používateľa** alebo **Použiť existujúceho používateľa databázy**. Zadajte heslo pre používateľa databázy.
7. Zadajte **Hostiteľa servera** (názov alebo IP adresu vášho ESMC Servera) a **Port servera** (prednastavený port je 2222, ak používate iný port, zadajte vaše číslo portu).
11. Pripojte MDM Connector k ESMC Serveru. Zadajte **Hostiteľa servera** a **Port servera** potrebný pre pripojenie k ESMC Serveru a pokračujte výberom buď **Serverom asistovanej inštalácie**, alebo **Offline inštalácie**:
- **Serverom asistovaná inštalácia** – uveďte prístupové údaje správcu, ktoré používate na prihlásenie do ESMC Web Console, a inštalátor automaticky stiahne potrebné certifikáty. Skontrolujte tiež [požiadavky](#) pre serverom asistovanú inštaláciu.
 1. Zadajte **Hostiteľa servera** (názov alebo IP adresu vášho ESMC Servera) a **Port Web Console** (ponechajte prednastavený port 2223, ak nepoužívate vlastný port). Nezabudnite zadať aj prihlasovacie údaje (účet správcu) pre Web Console – **Používateľské meno/heslo**.
 2. Kliknite na **Áno** v prípade, že ste boli vyzvaný na potvrdenie certifikátu. Prejdite na krok č. 11.
 - **Offline inštalácia** – uveďte **Proxy certifikát** a **Certifikačnú autoritu**, ktorú je možné [exportovať](#) z nástroja ESET Security Management Center. Môžete tiež použiť svoj [vlastný certifikát](#) a vhodnú certifikačnú autoritu.
 1. Kliknite na **Prehľadávať** vedľa partnerského certifikátu a prejdite do umiestnenia, kde sa nachádza **Partnerský certifikát** (je to Proxy certifikát, ktorý ste exportovali z ESMC). Nechajte pole **Heslo certifikátu** prázdne, pretože tento druh certifikátu nevyžaduje heslo.

2. Zopakujte tento postup pre certifikačnú autoritu a pokračujte krokom č. 11.

i Poznámka:

Ak používate vlastné certifikáty pre ESMC (namiesto prednastavených, ktoré boli automaticky vygenerované pri inštalácii nástroja ESET Security Management Center), je potrebné ich zadať, keď budete vyzvaný poskytnúť Proxy certifikát.

9. Vyberte cieľový priečinok pre Mobile Device Connector (odporúčame použiť prednastavený), kliknite na **Ďalej** a **Inštalovať**.
11. Po dokončení inštalácie skontrolujte, či Mobile Device Connector pracuje správne otvorením adresy `https://názov_vášho_servera:registračný_port` (napr. `https://mdm.company.com:9980`) vo vašom webovom prehliadači alebo z mobilného zariadenia. Ak bola inštalácia úspešná, zobrazí sa nasledujúca správa: MDM Server je pripravený a spustený
12. Teraz môžete [aktivovať MDM pomocou nástroja ESET Security Management Center](#).

4.3.10.1 Prerekvizity pre Mobile Device Connector

Pre inštaláciu komponentu Mobile Device Connector na operačnom systéme Windows je potrebné splniť nasledujúce prerekvizity:

- Verejná IP adresa/názov hostiteľa alebo verejná doména musia byť prístupné z internetu.

i Poznámka:

Ak potrebujete zmeniť názov hostiteľa pre váš MDM server, bude potrebné spustiť opravnú inštaláciu komponentu MDC. Ak zmeníte názov hostiteľa vášho MDM servera, bude následne potrebné importovať nový **certifikát HTTPS servera** (so zmeneným názvom hostiteľa).

- Otvorené a dostupné porty – pre kompletný zoznam portov kliknite [sem](#). Odporúčame používať vopred definované porty 9981 a 9980, ktoré však môžu byť zmenené pomocou konfiguračného súboru MDM servera. Uistite sa, že mobilné zariadenia sa dokážu cez dané porty pripájať. Toto umožníte zmenou nastavení pre firewall a/alebo sieť. Pre viac informácií o MDM architektúre [kliknite sem](#).
- Nastavenia pre Firewall – pri inštalácii nástroja Mobile Device Connector na OS, ktoré nie sú určené pre servery, ako napríklad Windows 7 (len na skúšobné účely), sa uistite, že sú povolené komunikačné porty vytvorením [pravidiel pre firewall](#), a to nasledovne:

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9980

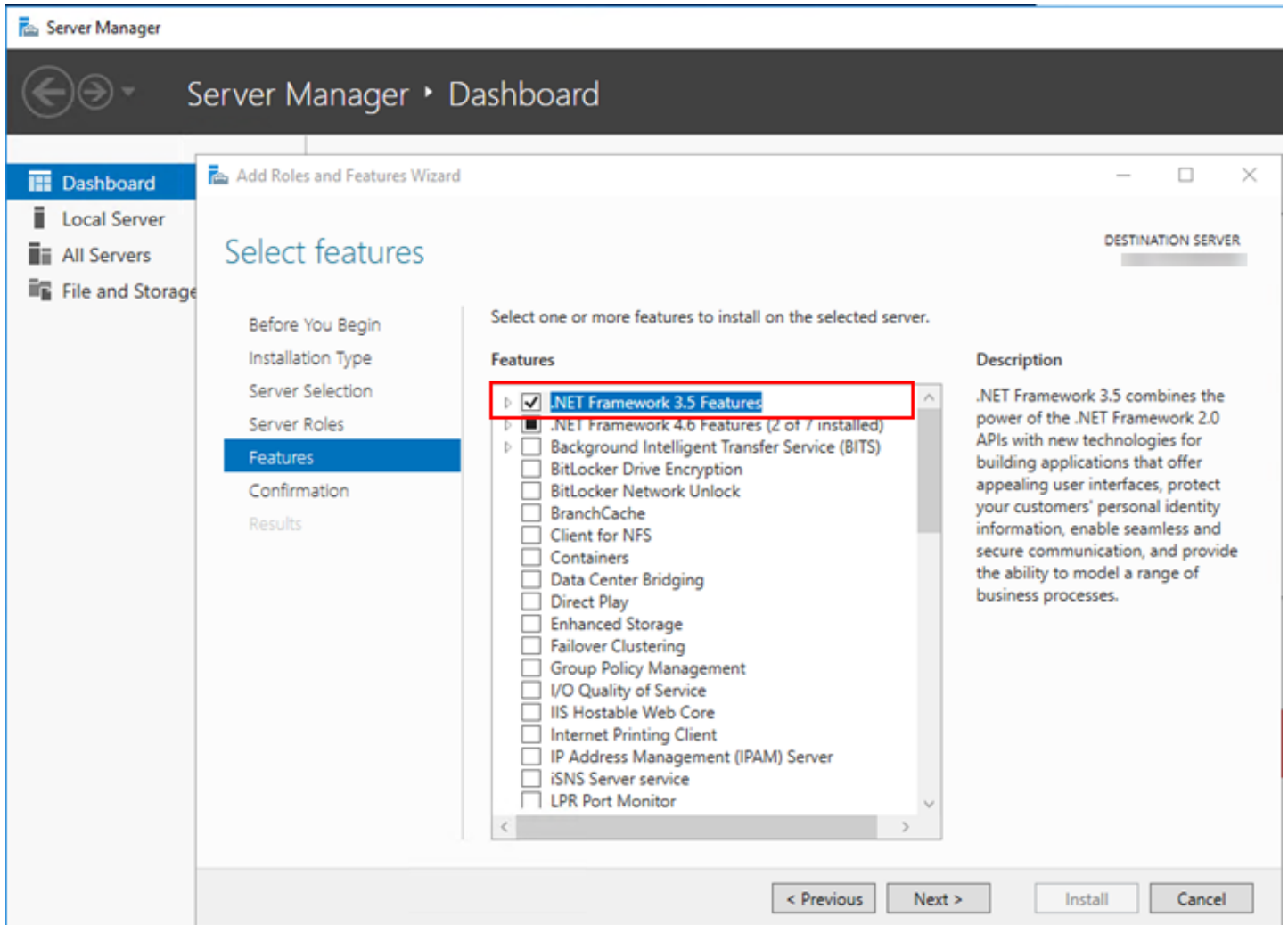
C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9981

C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP port 2222

i Poznámka:

Cesty k .exe súborom môžu byť rozdielne podľa toho, kde sú nainštalované jednotlivé súčasti ESMC.

- Databáza musí byť nainštalovaná a nastavená. Uistite sa, že spĺňate požiadavky pre [Microsoft SQL](#) alebo [MySQL](#).
- Využitie pamäte RAM nástrojom MDM Connector je optimalizované tak, aby mohlo byť súčasne spustených maximálne 48 procesov „ESET Security Management Center MDMCore Module“. Ak používateľ pripojí viac zariadení, procesy sa budú pravidelne meniť pre každé zariadenie, ktoré momentálne potrebuje využívať zdroje.
- Na serveri musí byť nainštalovaný Microsoft .NET Framework 3.5. V prípade operačného systému Windows Server 2008 a novších verzií môžete .NET 3.5 nainštalovať pomocou **Spríevodcu rolami a funkciami servera**. Ak používate Windows Server 2003, môžete .NET 3.5 stiahnuť z nasledujúceho odkazu: <https://www.microsoft.com/en-us/download/details.aspx?id=21>



POŽIADAVKY NA CERTIFIKÁT

! Dôležité:

Pre zabezpečenú komunikáciu cez HTTPS budete potrebovať **SSL certifikát** vo formáte .pfx. Odporúčame, aby ste použili certifikát poskytnutý vašou certifikačnou autoritou (certifikačná autorita ESMC alebo certifikačná autorita tretej strany). Neodporúčame používať certifikáty s vlastným podpisom, pretože niektoré mobilné zariadenia takéto certifikáty neakceptujú. Toto však nie je problém v prípade certifikátov podpísaných certifikačnou autoritou, pretože takéto certifikáty sú dôveryhodné a nevyžadujú povolenie od používateľa.

i Poznámka:

Je potrebné, aby ste mali certifikát podpísaný certifikačnou autoritou (certifikačná autorita ESMC alebo certifikačná autorita tretej strany) a príslušný privátny kľúč. Ďalej je potrebné zlúčiť certifikát podpísaný certifikačnou autoritou a privátny kľúč (pomocou OpenSSL) do jedného .pfx súboru:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCre`
Ide o štandardný postup pre väčšinu serverov, ktoré využívajú SSL certifikáty.

! Dôležité:

V prípade [offline inštalácie](#) budete tiež musieť [exportovať certifikát agenta](#) z nástroja ESET Security Management Center. Môžete tiež použiť svoj [vlastný certifikát](#).

4.3.10.2 Aktivácia komponentu Mobile Device Connector

Po úspešnej inštalácii komponentu Mobile Device Connector je potrebné aktivovať ho pomocou licencie ESET Endpoint, Business alebo Office:

1. Pridajte licenciu **ESET Endpoint, Business alebo Office** do správy licencií ESMC podľa krokov, ktoré sú uvedené [tu](#).
2. Aktivujte Mobile Device Connector pomocou úlohy pre klienta [Aktivácia produktu](#). Tento postup je rovnaký ako v prípade aktivácie akéhokoľvek produktu ESET na klientskom počítači – v tomto prípade je klientskym počítačom Mobile Device Connector.

4.3.10.3 MDM funkcia licencovania iOS zariadení

Keďže spoločnosť ESET neposkytuje žiadnu aplikáciu prostredníctvom App Store, všetky licenčné údaje pre iOS zariadenia uchováva Mobile Device Connector.

Každé zariadenie má samostatnú licenciu a môže byť aktivované pomocou [úlohy aktivácie produktu](#) (rovnako ako pre Android).

iOS licencie môžu byť deaktivované nasledujúcimi spôsobmi:

- Odstránením zariadenia zo správy pomocou úlohy Ukončiť spravovanie.
- Odinštalovaním MDC pomocou možnosti **Odstrániť databázu**.
- Deaktiváciou pomocou iných metód (deaktivácia v rámci ESMC alebo [deaktivácia pomocou EBA](#)).

Pretože MDC komunikuje s licenčnými servermi spoločnosti ESET v zastúpení iOS zariadení, EBA portál odráža stav MDC a nie stav jednotlivých zariadení. Aktuálne informácie o zariadení sú vždy dostupné v nástroji ESMC Web Console.

Pre zariadenia, ktoré nie sú aktivované, alebo zariadenia, ktorých platnosť licencie vypršala, bude zobrazený stav ochrany červenou farbou a hlásenie „Licencia nie je aktivovaná“. Takéto zariadenia nebudú vykonávať úlohy, nebudú sa na ne dať aplikovať politiky a nebudú doručovať iné než kritické upozornenia.

Ak je počas odinštalovania MDM zvolená možnosť **Neodstrániť databázu**, licencie nebudú deaktivované. Tieto licencie budú môcť byť použité znova, keď sa MDM na databáze preinštaluje, budú taktiež môcť byť odobraté prostredníctvom nástroja ESET Security Management Center alebo [deaktivované pomocou EBA](#). Pri presune na iný MDM Server budete musieť znova vykonať [úlohu aktivácie produktu](#).

4.3.10.4 Požiadavky HTTPS certifikátu

Ak chcete zaregistrovať mobilné zariadenie v nástroji ESET Mobile Device Connector, uistite sa, že HTTPS server vracia celý certifikačný reťazec.

Aby certifikát fungoval správne, musia byť splnené nasledujúce požiadavky:

- HTTPS certifikát (pkcs#12/pfx kontajner) musí obsahovať celý certifikačný reťazec.
- Ak je certifikát podpísaný sám sebou, musí tiež obsahovať koreňovú certifikačnú autoritu (CA).
- Certifikát musí mať definovaný rozsah platnosti (platný od – platný do).
- **CommonName** alebo **subjectAltName** sa musí zhodovať s hostiteľským názvom MDM.

i Poznámka:

Ak je **MDM názov hostiteľa** napr. hostname.mdm.domain.com, váš certifikát môže obsahovať názov serveru v niektorom z nasledujúcich formátov:

- hostname.mdm.domain.com
- *.mdm.domain.com

Nemôžete však použiť:

- *
- *.com
- *.domain.com

Hviezdička „*“ nenahradzuje časť s bodkou. Je to kvôli tomu, akým spôsobom iOS akceptuje certifikáty pre MDM.

4.3.11 Apache HTTP Proxy – inštalácia a ukladanie do vyrovnávacej pamäte

i Poznámka:

Ako alternatívu k Apache HTTP Proxy môžete nainštalovať [Squid](#).

Pre inštaláciu [Apache HTTP Proxy](#) na operačnom systéme Windows postupujte podľa nasledujúcich krokov:

! Dôležité:

Ak už máte Apache HTTP Proxy nainštalované na systéme Windows a chcete ho aktualizovať na najnovšiu verziu, prejdite na kapitolu [Aktualizácia Apache HTTP Proxy](#).

1. [Z webovej stránky spoločnosti ESET](#) si môžete stiahnuť samostatné inštalátory pre jednotlivé komponenty nástroja ESET Security Management Center.
2. Otvorte *ApacheHttp.zip* a extrahujte súbory do *C:\Program Files\Apache HTTP Proxy*

i Poznámka:

Ak chcete nainštalovať Apache HTTP Proxy na iný pevný disk, cesta *C:\Program Files* musí byť nahradená zodpovedajúcou cestou podľa inštrukcií uvedených nižšie a takisto je potrebné urobiť zmeny aj v súbore *httpd.conf*, nachádzajúcom sa v adresári *Apache HTTP Proxy\bin*. Napríklad, ak extrahujete obsah súboru *ApacheHttp.zip* do *D:\Apache Http Proxy*, potom cesta *C:\Program Files* musí byť nahradená cestou *D:\Apache Http Proxy*.

3. Otvorte príkazový riadok ako správca a zmeňte adresár na *C:\Program Files\Apache HTTP Proxy\bin*
4. Spustite nasledujúci príkaz:
`httpd.exe -k install -n ApacheHttpProxy`
5. Pomocou textového editora, napríklad Poznámkový blok, otvorte súbor *httpd.conf* a pridajte na koniec súboru nasledujúce riadky:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
```

```
</Directory>
```

```
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

i Poznámka:

Ak chcete, aby bol adresár vyrovnávacej pamäte umiestnený inde, povedzme na inej diskovej jednotke, napr. D:\Apache HTTP Proxy\cache, potom v poslednom riadku kódu uvedeného vyššie zmeňte "C:\Program Files\Apache HTTP Proxy\cache" na "D:\Apache HTTP Proxy\cache".

6. Spustíte službu **ApacheHttpProxy** pomocou nasledujúceho príkazu:

```
sc start ApacheHttpProxy
```

7. Skontrolujte, či je služba Apache HTTP Proxy spustená napr. pomocou modulu `services.msc` (hľadajte **ApacheHttpProxy**). Štandardne je služba nastavená na automatické spustenie.

Pomocou nasledujúcich krokov nastavte používateľské meno a heslo pre Apache HTTP Proxy (odporúčané):

1. Zastavte službu **ApacheHttpProxy** otvorením [príkazového riadka s oprávneniami správcu](#) a spustením nasledujúceho príkazu:

```
sc stop ApacheHttpProxy
```

2. Skontrolujte prítomnosť nasledujúcich modulov v `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf`:

```
LoadModule authn_core_module modules\mod_authn_core.dll
LoadModule authn_file_module modules\mod_authn_file.dll
LoadModule authz_groupfile_module modules\mod_authz_groupfile.dll
LoadModule auth_basic_module modules\mod_auth_basic.dll
```

3. Pridajte nasledujúce riadky do `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf` pod `<Proxy *>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
```

4. Použite príkaz `htpasswd` pre vytvorenie súboru pomenovaného `password.file` v priečinku `Apache HTTP Proxy\bin\` (budete vyzvaný na zadanie hesla):

```
htpasswd.exe -c ..\password.file username
```

5. Manuálne vytvorte súbor `group.file` v priečinku `Apache HTTP Proxy\` s nasledujúcim obsahom:

```
usergroup:username
```

6. Spustíte službu **ApacheHttpProxy** spustením nasledujúceho príkazu v príkazovom riadku bez obmedzených oprávnení:

```
sc start ApacheHttpProxy
```

7. Otestujte pripojenie na HTTP Proxy pomocou otvorenia nasledujúcej URL adresy vo vašom prehliadači:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)

i Poznámka:

Po úspešnej inštalácii Apache HTTP Proxy môžete povoliť komunikáciu iba produktom spoločnosti ESET (ostatná komunikácia bude prednastavene blokována) alebo povoliť všetku komunikáciu. Vykonajte potrebné zmeny v konfigurácii podľa:

- [Preposielanie iba pre ESET komunikáciu](#)
- [Proxy chaining \(všetka komunikácia\)](#)

Nasledujúci príkaz zobrazí zoznam obsahu vo vyrovnávacej pamäti:

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -a -p "C:\ProgramData\Apache HTTP Proxy\cache"
```

Vyrovnávaciu pamäť disku vyčistíte nástrojom [htcacheclean](#). Odporúčaný príkaz (veľkosť vyrovnávacej pamäte 10 GB a limit pre súbory ~12 000) je zobrazený nižšie:

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -n -t ^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l10000M -L12000
```

Pre naplánovanie spustenia čistenia vyrovnávacej pamäte každú hodinu spustíte nižšie uvedený príkaz:

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask ^  
/TR "\"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe\" ^  
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l10000M -L12000"
```

Ak povolíte všetku komunikáciu, odporúčané nastavenie je:

```
"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -n -t ^  
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l10000M
```

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask ^  
/TR "\"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe\" ^  
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l10000M"
```

i Poznámka:

Pre správne spustenie príkazov je nutné použiť na konci riadka znak ^. V opačnom prípade príkazy uvedené vyššie nebudú spustené správne.

Pre viac informácií navštívte náš [článok databázy znalostí](#) alebo [dokumentáciu Apache Authentication and Authorization](#).

4.3.12 Inštalácia Squid a vyrovnávacia pamäť HTTP Proxy

Squid je alternatívou k [Apache HTTP Proxy](#). Inštaláciu nástroja Squid na operačnom systéme Windows vykonáte podľa nasledujúcich krokov:

1. Stiahnite si Squid MSI inštalátor a nainštalujte Squid.
2. Kliknite na ikonu **Squid for Windows** na paneli úloh a vyberte možnosť **Stop Squid Service**.
3. Prejdite do inštaláčného priečinka Squid, napríklad C:\Squid\bin, a pomocou príkazového riadka spustíte nasledujúci príkaz:

```
squid.exe -z -F
```

Týmto vytvoríte swap adresáre pre vyrovnávaciu pamäť.

4. Kliknite na ikonu **Squid for Windows** na paneli úloh a vyberte možnosť **Open Squid Configuration**.
5. Nahraďte `http_access deny all` týmto: `http_access allow all`.
6. Povoľte ukladanie do vyrovnávacej pamäte na disku pridaním nasledujúceho riadka:
`cache_dir ufs C:/Squid/var/cache 300 16 256`

Poznámka:

V príklade uvedenom vyššie sa adresár vyrovnávacej pamäte nachádza v umiestnení C:\Squid\var\cache. Umiestnenie adresára vyrovnávacej pamäte môžete zmeniť podľa svojich požiadaviek. Môžete zmeniť aj celkovú veľkosť adresára (v tomto príklade je to 300 MB), počet podadresárov 1. úrovne (v tomto príklade 16) a počet podadresárov 2. úrovne (v tomto príklade 256).

7. Uložte a zatvorte konfiguračný súbor nástroja Squid `squid.conf`.
8. Kliknite na ikonu **Squid for Windows** na paneli úloh a vyberte možnosť **Start Squid Service**.
9. Skontrolujte, či je služba Squid spustená pomocou modulu `services.msc` (hľadajte **Squid for Windows**).

4.3.13 Offline repozitár

Od vydania ERA vo verzii 6.5 môže byť nástroj Mirror Tool použitý aj na vytvorenie offline repozitára (na systéme Windows). Toto je zvyčajne potrebné v prípade uzavretých počítačových sietí alebo sietí s obmedzeným prístupom na internet. Nástroj Mirror Tool môže byť použitý na vytvorenie kópie ESET repozitára v lokálnom priečinku. Tento klonovaný repozitár môže byť neskôr presunutý (napr. na externý disk) do umiestnenia v uzavretej sieti. Repozitár si môžete skopírovať na bezpečné miesto na lokálnej sieti a sprístupniť ho pomocou HTTP servera.

Aktualizácia offline repozitára je možná použitím toho istého príkazu (vrátane parametrov), ktorý slúži na jeho vytvorenie. Budú použité predošlé dáta z dočasného adresára a stiahnuté budú len zastarane súbory.

Dôležité:

Je potrebné mať na pamäti, že veľkosť repozitára je viac ako 70 GB a rovnako veľký je aj dočasný adresár. Pred tým, než začnete s vytváraním repozitára, sa preto uistite, že máte na disku aspoň **150 GB** voľného miesta.

Príklad postupu na systéme Windows

Časť I: Vytvorenie kópie repozitára

1. [Stiahnite si](#) nástroj Mirror Tool.
2. Extrahujte Mirror Tool zo stiahnutého `.zip` súboru.
3. Pripravte (vytvorte) priečinky pre:
 - dočasné súbory,
 - finálny repozitár.
4. Otvorte príkazový riadok a zmeňte adresár na priečinok, kde máte extrahovaný nástroj Mirror Tool (príkaz `cd`).
5. Spustíte nasledujúci príkaz (zmeňte dočasný a výstupný adresár repozitára na priečinky z kroku č. 3):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^  
--intermediateRepositoryDirectory C:\Intermediary ^  
--outputRepositoryDirectory C:\Repository
```


6. Po skopírovaní repozitára do priečinka `outputRepositoryDirectory` presuňte daný priečinok vrátane jeho obsahu na iné zariadenie, ktoré nemá prístup na internet a ktoré bude poskytovať offline repozitár.

Časť II: Nastavenie HTTP servera

7. V tejto časti je potrebný HTTP server bežiaci na zariadení v uzavretej sieti. Môžete použiť:
- Apache HTTP Proxy z [webovej stránky spoločnosti ESET](#),
 - iný HTTP server.
8. Otvorte `apachehttp.zip` a extrahujte súbory do `C:\Program Files\Apache HTTP Proxy`.
9. Otvorte príkazový riadok ako správca a zmeňte adresár na `C:\Program Files\Apache HTTP Proxy\bin` (príkaz `cd`).
10. Spustite nasledujúci príkaz:
- ```
httpd.exe -k install -n ApacheHttpProxy
```
11. Pomocou textového editora otvorte súbor `conf/httpd.conf` a pridajte na koniec súboru nasledujúce riadky:

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

12. Spustite službu **Apache HTTP Proxy** pomocou nasledujúceho príkazu:
- ```
sc start ApacheHttpProxy
```
13. Overtvorte, či je služba spustená otvorením adresy <http://YourIPAddress:80/index.html> vo vašom webovom prehliadači (nahraďte `YourIPAddress` IP adresou vášho počítača).

Časť III: Spustenie offline repozitára

14. Vytvorte nový priečinok pre offline repozitár, napríklad `C:\Repository`.

15. V súbore `httpd.conf` nahraďte riadky

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
```

adresou priečinka repozitára tak, ako je uvedené nižšie:

```
DocumentRoot "C:\Repository"
<Directory "C:\Repository">
```

16. Skopírujte stiahnutý repozitár do `C:\Repository`.
17. Reštartujte službu **ApacheHttpProxy** použitím nasledujúceho príkazu:
- ```
sc restart ApacheHttpProxy
```
18. Teraz je váš offline repozitár dostupný na adrese <http://YourIPAddress> (napr. `http://10.1.1.10`).
19. Nastavte novú adresu repozitára:

- a. V prípade [ESMC Servera](#) otvorte ESMC Web Console a kliknite na **Správca > Nastavenia servera**.
- b. V prípade [ESET Management Agentov](#) kliknite na **Správca > Politiky**.

#### 4.3.14 Failover klaster

Nižšie nájdete podrobný postup pre inštaláciu nástroja ESET Security Management Center na Failover klaster (klaster zabezpečený proti zlyhaniu).

##### **i Poznámka:**

Ďalšie informácie o inštalácii ESMC Servera v klastrovom prostredí nájdete v [tomto článku databázy znalostí](#).

1. Vytvorte Failover klaster so zdieľaným diskom:
  - a. [Vytvorenie Failover klastra na operačnom systéme Windows Server 2016](#)
  - b. [Vytvorenie Failover klastra na operačnom systéme Windows Server 2012](#)
  - c. [Vytvorenie Failover klastra na operačnom systéme Windows Server 2008](#)
2. V **sprievodcovi klastrom** zadajte (vytvorte) požadovaný názov hostiteľa a IP adresu.
3. Pripojte zdieľaný disk k uzlu node1 a [nainštalujte naň ESMC Server pomocou samostatného inštalátora](#). Uistite sa, že je počas inštalácie zvolená možnosť **Toto je inštalácia na klaster** a ako úložisko pre dáta aplikácie vyberte daný zdieľaný disk. Vytvorte názov hostiteľa a zadajte ho pre certifikát ESMC Servera vedľa predvyplnených názvov hostiteľov. Tento názov hostiteľa si zapamätajte a použite ho v kroku č. 6 pri vytváraní roly pre ESMC Server v Správcovi klastrov.
4. Zastavte službu ESMC Server na uzle node1, pripojte zdieľaný disk k uzlu node2 a [nainštalujte naň ESMC Server pomocou samostatného inštalátora](#). Opäť sa uistite, že je počas inštalácie zvolená možnosť **Toto je inštalácia na klaster**. Zvoľte zdieľaný disk ako úložisko pre dáta aplikácie. Údaje pre pripojenie do databázy a certifikáty ponechajte nezmenené, keďže už boli nastavené počas inštalácie komponentu ESMC Server na uzol node1.
5. Váš firewall nastavte tak, aby povoľoval prichádzajúcu komunikáciu cez všetky [porty](#) používané službou ESMC Server.
6. V Správcovi klastrov vytvorte a spustite rolu (*Configure Role > Select Role > Generic service ...*) pre službu ESMC Server. Zo zoznamu dostupných služieb vyberte službu ESET Security Management Center **Server**. Je veľmi dôležité, aby bol pre danú rolu použitý rovnaký názov hostiteľa, aký bol použitý v kroku č. 3 pre certifikát servera.

##### **i Poznámka:**

Pojem **Rola** sa používa iba v prostredí systému Windows Server 2016 a 2012. V systéme Windows Server 2008 R2 sa používa výraz **Služby a aplikácie**.

7. Nainštalujte ESET Management Agenta na všetky uzly prostredníctvom samostatného inštalátora. V častiach **Konfigurácia agenta** a **Pripojenie na ESET Security Management Center Server** použite hosťovský názov, ktorý ste použili v kroku č. 6. Dáta agenta uložte na lokálny uzol (**nie na zdieľaný disk**).
8. ESMC databáza a webový server (Apache Tomcat) nie sú podporované na klastri, čo znamená, že musia byť nainštalované na disk, ktorý nie je klastrový, alebo na iné zariadenie.

[Web Console je možné jednoducho nainštalovať](#) na samostatný počítač a nakonfigurovať pre pripojenie na klastrovú rolu vytvorenú pre službu ESMC Server. Po nainštalovaní Web Console nájdete konfiguračný súbor v nasledujúcej lokalite:

```
C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties
```

Súbor otvorte pomocou Poznámkového bloku alebo v akomkoľvek inom textovom editore. V riadku `server_address=localhost` nahraďte „localhost“ IP adresou alebo názvom hostiteľa klastrovej roly vytvorenej pre službu ESMC Server.

## 4.4 Inštalácia súčastí na systéme Linux

Vo väčšine inštalačných scenárov potrebujete nainštalovať rôzne súčasti nástroja ESET Security Management Center na rôzne počítače v závislosti od sieťovej architektúry, výkonnostných požiadaviek atď.

Pre podrobné inštrukcie k inštalácii ESMC Servera postupujte podľa tejto [sekcie](#).

Pre aktualizáciu nástroja ESET Security Management Center pre Linux na najnovšiu verziu si pozrite kapitolu [Aktualizácia súčastí](#) alebo náš [článok databázy znalostí](#).

### **i** Poznámka:

Berte, prosím, na vedomie, že Fedora vo verzii 22 a novších už nepoužíva príkaz `yum`. Tento príkaz bol nahradený `dnf` príkazom. Ak používate distribúciu Fedora vo verzii 22 a novších, použite príkaz `dnf` miesto príkazu `yum`.

### Základné súčasti

- [ESMC Server](#)
- [ESMC Web Console](#)
- [ESET Management Agent](#)
- [Databázový server](#)

### Voliteľné súčasti

- [RD Sensor](#)
- [Mobile Device Connector](#)
- [Apache HTTP Proxy](#)
- [Apache HTTP Proxy ako proxy pre pripojenie agent – server](#)
- [Mirror Tool](#)

#### 4.4.1 Podrobná inštalácia ESMC Servera na systéme Linux

V tomto inštalačnom scenári si podrobne ukážeme, ako nainštalovať ESMC Server a ESMC Web Console. Postup inštalácie si ukážeme na už spustenom MySQL.

### Pred vykonaním inštalácie

1. Uistite sa, že máte nainštalovaný [databázový server](#) a máte k nemu prístup. Ak nemáte nainštalovaný žiadny databázový server, musíte ho nainštalovať a nakonfigurovať.
2. Stiahnite si samostatné komponenty ESMC pre Linux (Agent, Server, Web Console). Inštalačné súbory nájdete na stránkach spoločnosti ESET v časti [ESMC Samostatné inštalátory](#).

### Inštalácia

#### **i** Poznámka:

Inštalácia vyžaduje, aby ste mali oprávnenie na použitie príkazu `sudo`, resp. aby ste mali root oprávnenia.

#### **i** Poznámka:

Ak chcete nainštalovať ESMC Server na SUSE Linux Enterprise Server (SLES), riadte sa pokynmi [v tomto článku databázy znalostí](#).

1. Nainštalujte [požadované balíky](#) ESMC Servera.
2. Prejdite do priečinka, kde ste stiahli ESMC Server a spustite inštalačný balík:

```
chmod +x server-linux-x86_64.sh
```

3. Nastavte pripojenie na MySQL Server podľa kapitoly [Inštalácia a konfigurácia MySQL](#).
4. Skontrolujte konfiguráciu MySQL ODBC ovládača (prečítajte si tiež kapitolu [Inštalácia a konfigurácia ovládača ODBC](#)):

Spustite nasledujúci príkaz pre otvorenie súboru **odbcinst.ini** v textovom editore:

```
sudo nano /etc/odbcinst.ini
```

Skopírujte nasledujúcu konfiguráciu do súboru **odbcinst.ini** (uistite sa, že cesta k **Driver** a **Setup** je správna) a potom uložte a zatvorte súbor:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

Ak používate 32-bitovú verziu Ubuntu, použite kľúče **Driver** a **Setup** a zmeňte cestu na:  
*/usr/lib/i386-linux-gnu/odbc/*

Cesta k ovládaču sa môže líšiť v závislosti od používanej distribúcie systému Linux. Ovládač môžete nájsť pomocou nasledujúceho príkazu:

```
sudo find /usr -iname "*libmyodbc*"
```

ESMC vyžaduje MySQL ovládač s podporou multi-threadingu (súbežné spracovanie vlákien). Túto požiadavku spĺňa ovládač unixODBC (2.3.0 a novšie verzie). Staršie verzie vyžadujú konfiguráciu. Ak máte staršiu verziu, (príkaz `odbcinst --version` vám ukáže verziu), pridajte nasledujúci parameter do súboru **odbcinst.ini**:

```
Threading = 0
```

Aktualizujte konfiguračné súbory, ktoré ovládajú prístup ODBC k databázovému serveru pomocou nasledujúceho príkazu:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

#### **i** Poznámka:

Odporúčame používať najnovšiu dostupnú verziu ODBC ovládača.

5. Upravte parametre inštalácie a spustite inštaláciu ESMC Servera. Pre viac informácií si pozrite kapitolu [Inštalácia servera – Linux](#).
6. Nainštalujte potrebné balíky **Java** a **Tomcat** pre ESMC Web Console podľa kapitoly [Prerekvizity ESMC Web Console – Linux](#).

Pred inštaláciou komponentu ESMC Web Console na systéme Linux je potrebné splniť nasledujúce prerekvizity:

- **Java** – vždy používajte najnovšiu oficiálne vydanú verziu Javy. ESMC Web Console vyžaduje minimálne verziu 8 (alebo openjdk), avšak aj napriek tomu odporúčame používať najnovšiu verziu. Podrobnejšie informácie o inštalácii Javy nájdete v našom [článku databázy znalostí](#).
- **Apache Tomcat** ([podporovaná](#) verzia).
- Web Console súbor (*era.war*) uložený na lokálnom pevnom disku.

Pre inštaláciu balíkov **Java** a/alebo **Apache Tomcat** použite nasledujúce príkazy podľa distribúcie systému Linux, ktorú používate:

|                                    |                                                         |
|------------------------------------|---------------------------------------------------------|
| <b>Debian a Ubuntu distribúcie</b> | <code>sudo apt-get install openjdk-8-jdk tomcat7</code> |
| <b>CentOS, Red Hat a</b>           | <code>sudo yum install java-1.8.0-openjdk tomcat</code> |

|                             |                                                            |
|-----------------------------|------------------------------------------------------------|
| <b>Fedora distribúcie</b>   |                                                            |
| <b>OpenSUSE distribúcia</b> | <code>sudo zypper install java-1_8_0-openjdk tomcat</code> |

7. Nasadíte a otestujete ESMC Web Console podľa kapitoly [Inštalácia ESMC Web Console – Linux](#). Ak máte problémy s HTTPS pripojením do ESMC Web Console, prečítajte si článok o [nastavení pripojenia HTTPS/SSL](#).

8. [Nainštalujte ESET Management Agentu](#) na server.

## 4.4.2 Inštalácia a konfigurácia MySQL

### Inštalácia

Ak ste už nainštalovali a nakonfigurovali MySQL, pokračujte na [nastavenia](#).

#### **Upozornenie:**

MariaDB je predvolená databáza vo väčšine súčasných linuxových prostredí a je súčasťou inštalácie MySQL.

Databázový server MariaDB nie je podporovaný nástrojom ESET Security Management Center.

#### **Dôležité:**

Pre správne fungovanie nástroja ESET Security Management Center nainštalujte MySQL. Pred inštaláciou databázy na systéme Linux pridajte MySQL repozitár:

- Debian, Ubuntu: [pridanie MySQL APT repozitára](#)
- CentOS, Red Hat, Fedora: [pridanie MySQL Yum repozitára](#)
- OpenSUSE, SUSE Linux Enterprise Server: [pridanie MySQL SLES repozitára](#)

Po pridaní MySQL repozitára môžete pokračovať v inštalácii MySQL.

Postup inštalácie MySQL sa odvíja od distribúcie a verzie systému Linux:

#### **Debian a Ubuntu distribúcie**

Pre inštaláciu MySQL použite nasledujúci príkaz:

```
sudo apt-get install mysql-server
```

Pokročilá inštalácia: <https://dev.mysql.com/doc/refman/5.7/en/linux-installation-apt-repo.html>

#### **CentOS, Red Hat a Fedora distribúcie**

Pre inštaláciu MySQL použite nasledujúci príkaz:

```
sudo yum install mysql-server
```

Pokročilá inštalácia: <https://dev.mysql.com/doc/refman/5.7/en/linux-installation-yum-repo.html>

#### **OpenSUSE distribúcia**

Pre inštaláciu MySQL použite nasledujúci príkaz:

```
sudo zypper install mysql-community-server
```

#### **Manuálna inštalácia**

Stiahnite si a nainštalujte MySQL Community Server edíciu na:

<http://dev.mysql.com/downloads/>

---

## Konfigurácia

Spustite nasledujúci príkaz pre otvorenie `my.cnf` (`my.ini` na systéme Windows) súboru v textovom editore:

```
sudo nano /etc/mysql/my.cnf
```

(ak ste požadovaný súbor nenašli, skúste umiestnenie `/etc/my.cnf`)

V sekcii [mysqld] súboru my.cnf nájdite nasledujúcu konfiguráciu a zmeňte hodnoty (ak sa v súbore parametre nenachádzajú, pridajte ich do sekcie [mysqld]):

```
max_allowed_packet=33M
```

- Pre MySQL 5.6.20 a 5.6.21 (verziu svojho MySQL môžete zistiť pomocou `mysql --version`):
  - `innodb_log_file_size` musí byť nastavené aspoň na **200 MB** (napr. `innodb_log_file_size=200M`)
- Pre MySQL 5.6.22 a novšie verzie:
  - `innodb_log_file_size*innodb_log_files_in_group` musí byť nastavené aspoň na **200 MB** (znak \* predstavuje násobenie, súčin dvoch parametrov musí byť väčší ako 200 MB. Minimálna hodnota pre `innodb_log_files_in_group` je 2, pričom maximálna hodnota je 100 – musí byť použité celé číslo).  
Napríklad:  
`innodb_log_file_size=100M`  
`innodb_log_files_in_group=2`

Uložte a zatvorte súbor a zadajte nasledujúci príkaz pre reštartovanie MySQL servera a aplikovanie nastavení (v niektorých prípadoch bude názov služby `mysqld`):

```
sudo service mysql restart
```

Spustite nasledujúci príkaz pre nastavenie MySQL vrátane oprávnení a hesla (tento krok je voliteľný a nemusí fungovať pre niektoré distribúcie systému Linux):

```
/usr/bin/mysql_secure_installation
```

Pomocou nasledujúceho príkazu skontrolujte, či je MySQL server spustený:

```
sudo netstat -tap | grep mysql
```

Ak je MySQL server spustený, zobrazí sa nasledujúci riadok. Berte, prosím, na vedomie, že identifikátor procesu – **PID (7668 v príklade nižšie)** bude odlišný:

```
tcp 0 0 localhost:mysql *.* LISTEN 7668/mysqld
```

### 4.4.3 Inštalácia a konfigurácia ODBC ovládača

#### Inštalácia

Pre inštaláciu **MySQL ODBC** (Open Database Connectivity) ovládača spustite nasledujúci príkaz z terminálu:

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Debian a Ubuntu distribúcie</b>          | <pre>sudo apt-get install libmyodbc libodbc1</pre> <p><b>i Poznámka:</b><br/>Od verzie Ubuntu 16.04.1 LTS a Debian 9 sa už balík <code>libmyodbc</code> v oficiálnom Ubuntu repozitári nenachádza. Odporúčame stiahnuť samostatný balík z <a href="#">oficiálnej webovej stránky</a> a <a href="#">nainštalovať</a> ho. Avšak, tento balík nebude aktualizovaný pomocou Ubuntu metódy <code>apt-get upgrade</code>, ale bude potrebná manuálna aktualizácia.</p> |
| <b>CentOS, Red Hat a Fedora distribúcie</b> | <pre>sudo yum install mysql-connector-odbc</pre>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>OpenSUSE distribúcia</b>                 | <pre>sudo zypper install myodbc-unixbox</pre>                                                                                                                                                                                                                                                                                                                                                                                                                    |

#### Konfigurácia

Spustite nasledujúci príkaz pre otvorenie súboru **odbcinst.ini** v textovom editore:

```
sudo nano /etc/odbcinst.ini
```

Skopírujte nasledujúcu konfiguráciu do súboru **odbcinst.ini** (uistite sa, že cesta k **Driver** a **Setup** je správna) a potom uložte a zatvorte súbor:

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

Ak používate 32-bitovú verziu Ubuntu, použite kľúče **Driver** a **Setup** a zmeňte cestu na:  
*/usr/lib/i386-linux-gnu/odbc/*

Cesta k ovládaču sa môže líšiť v závislosti od používanej distribúcie systému Linux. Ovládač môžete nájsť pomocou nasledujúceho príkazu:

```
sudo find /usr -iname "*libmyodbc*"
```

ESMC vyžaduje MySQL ovládač s podporou multi-threadingu (súbežné spracovanie vlákien). Túto požiadavku spĺňa ovládač unixODBC (2.3.0 a novšie verzie). Staršie verzie vyžadujú konfiguráciu. Ak máte staršiu verziu, (príkaz `odbcinst --version` vám ukáže verziu), pridajte nasledujúci parameter do súboru **odbcinst.ini**:

```
Threading = 0
```

Aktualizujte konfiguračné súbory, ktoré ovládajú prístup ODBC k databázovému serveru pomocou nasledujúceho príkazu:

```
sudo odbcinst -i -d -f /etc/odbcinst.ini
```

#### **i Poznámka:**

Odporúčame používať najnovšiu dostupnú verziu ODBC ovládača.

### 4.4.4 Inštalácia servera – Linux

Inštalácia komponentu ESMC Server na operačnom systéme Linux prebieha pomocou terminálu. Môžete si pripraviť inštalčný skript a spustiť ho s oprávneniami *sudo*. Predtým, ako začnete s inštaláciou, sa uistite, že boli splnené všetky [prerekvizity](#).

#### **i Poznámka:**

Ak chcete nainštalovať ESMC Server na SUSE Linux Enterprise Server (SLES), riadte sa pokynmi [v tomto článku databázy znalostí](#).

#### **Príklad inštalčného skriptu:**

(Nové riadky musia byť oddelené "\n" pre kopírovanie celého skriptu do terminálu.)

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-driver=MySQL \
--db-hostname=127.0.0.1 \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=Admin123 \
--server-root-password=Admin123 \
--db-user-username=root \
--db-user-password=Admin123 \
--cert-hostname="10.1.179.46;Ubuntu64-bb;Ubuntu64-bb.BB.LOCAL"
```

ESMC Server a služba `eraserver` budú nainštalované do nasledujúceho umiestnenia:  
*/opt/eset/RemoteAdministrator/Server*

Môžete zmeniť nasledujúce atribúty:

| Atribút                | Popis                                                                                                                                                                                                                                                                    | Vyžaduje sa |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| --uninstall            | <a href="#">Odištaluje</a> produkt.                                                                                                                                                                                                                                      | -           |
| --keep-database        | Počas <a href="#">odínštalovania</a> bude databáza zachovaná.                                                                                                                                                                                                            | -           |
| --locale               | Lokálny identifikátor (LCID) nainštalovaného servera (štandardne je to en_US). Viac informácií nájdete v časti <a href="#">podporované jazyky</a> .<br><b>POZNÁMKA:</b> Jazyk môžete nastaviť pre každú reláciu ESMC Web Console.                                        | Áno         |
| --skip-license         | Používateľovi sa počas inštalácie nezobrazí výzva na potvrdenie súhlasu s licenčnou dohodou.                                                                                                                                                                             | -           |
| --skip-cert            | Inštalátor preskočí generovanie certifikátu (použite s parametrom --server-cert-path).                                                                                                                                                                                   | -           |
| --license-key          | Licenčný kľúč ESET. Môže byť zadaný neskôr.                                                                                                                                                                                                                              | -           |
| --product-guid         | Globálny unikátny identifikátor produktu (GUID). Ak nie je zadefinovaný, bude vygenerovaný.                                                                                                                                                                              | -           |
| --server-port          | ESET Security Management Center (ESMC) Server port (štandardne je to 2222).                                                                                                                                                                                              | -           |
| --console-port         | ESET Security Management Center Web Console port (štandardne je to 2223).                                                                                                                                                                                                | -           |
| --server-root-password | Heslo do Web Console pre používateľský účet „Administrator“; minimálna dĺžka 8 znakov.                                                                                                                                                                                   | Áno         |
| --db-type              | Typ databázy, ktorý bude použitý (možné hodnoty: MySQL Server, MS SQL Server).                                                                                                                                                                                           | -           |
| --db-driver            | ODBC ovládač pre pripojenie do databázy (príkaz <code>odbcinst -q -d</code> zobrazí zoznam dostupných ovládačov, z ktorých použijete jeden, napr.: <code>--db-driver=MySQL</code> ).                                                                                     | Áno         |
| --db-hostname          | Názov alebo IP adresa databázového servera.                                                                                                                                                                                                                              | Áno         |
| --db-port              | Port databázového servera (štandardne je to 3306).                                                                                                                                                                                                                       | Áno         |
| --db-name              | Názov databázy ESMC Servera (štandardne je to <code>era_db</code> ).                                                                                                                                                                                                     | -           |
| --db-admin-username    | Používateľské meno správcu databázy (používané pri inštalácii pre vytvorenie a zmeny databázy). Tento parameter môžete vynechať, ak už je vytvorený používateľ databázy, ktorý je definovaný atribútmi <code>--db-user-username</code> a <code>--db-user-password</code> | Áno         |
| --db-admin-password    | Heslo správcu databázy. Tento parameter môžete vynechať, ak už je vytvorený používateľ databázy, ktorý je definovaný atribútmi <code>--db-user-username</code> a <code>--db-user-password</code>                                                                         | Áno         |
| --db-user-username     | Meno používateľa databázy ESMC Servera (používané ESMC Serverom na pripojenie do databázy); nemalo by mať viac ako 16 znakov.                                                                                                                                            | Áno         |
| --db-user-password     | Heslo používateľa databázy ESMC Servera.                                                                                                                                                                                                                                 | Áno         |
| --cert-hostname        | Obsahuje všetky možné mená a/alebo IP adresy počítača, na ktorom bude nainštalovaný ESMC Server. Musí byť zhodný s názvom servera zadaným v certifikáte agenta, ktorý sa pripája na server.                                                                              | Áno         |



| Atribút                    | Popis                                                                                                              | Vyžaduje sa |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|-------------|
| --server-cert-path         | Cesta k partnerskému certifikátu servera (použite túto možnosť, ak ste zadali aj parameter --skip-cert).           | -           |
| --server-cert-password     | Heslo partnerského certifikátu servera.                                                                            | -           |
| --agent-cert-password      | Heslo partnerského certifikátu agenta.                                                                             | -           |
| --cert-auth-password       | Heslo certifikačnej authority.                                                                                     | -           |
| --cert-auth-path           | Cesta k súboru certifikačnej authority servera.                                                                    | -           |
| --cert-auth-common-name    | Bežný názov certifikačnej authority (v úvodzovkách "").                                                            | -           |
| --cert-organizational-unit | -                                                                                                                  | -           |
| --cert-organization        | -                                                                                                                  | -           |
| --cert-locality            | -                                                                                                                  | -           |
| --cert-state               | -                                                                                                                  | -           |
| --cert-country             | -                                                                                                                  | -           |
| --cert-validity            | Platnosť certifikátu v dňoch alebo rokoch (udáva ju argument --cert-validity-unit).                                | -           |
| --cert-validity-unit       | Časové jednotky platnosti certifikátu; roky – „Years“ alebo dni – „Days“ (štandardná hodnota je Years).            | -           |
| --ad-server                | Active Directory server.                                                                                           | -           |
| --ad-user-name             | Meno používateľa s oprávneniami na prehľadávanie siete AD.                                                         | -           |
| --ad-user-password         | Active Directory heslo.                                                                                            | -           |
| --ad-cdn-include           | Strom Active Directory, ktorý bude synchronizovaný; pre synchronizáciu celého stromu použite prázdne úvodzovky "". | -           |
| --enable-imp-program       | Aktivácia programu zlepšovania produktov.                                                                          |             |
| --disable-imp-program      | Deaktivácia programu zlepšovania produktov.                                                                        |             |

## Protokol inštalácie

Protokol inštalácie je užitočný pri riešení problémov a nachádza sa v [súboroch protokolu](#).

Po inštalácii skontrolujte, či je služba ESMC Server spustená pomocou nasledujúceho príkazu:  
`service eraserver status`

```
root@localhost:~
File Edit View Search Terminal Help
[root@localhost ~]# service eraserver status
Redirecting to /bin/systemctl status eraserver.service
eraserver.service - ESET Remote Administrator Server
 Loaded: loaded (/etc/systemd/system/eraserver.service; enabled)
 Active: active (running) since Thu 2015-05-14 16:06:34 CEST; 5min ago
 Process: 5717 ExecStart=/opt/eset/RemoteAdministrator/Server/ERAServer --daemon --pidfile /var/run/eraserver.pid (code=exited, status=0/SUCCESS)
 Main PID: 5719 (ERAServer)
 CGroup: /system.slice/eraserver.service
 └─5719 /opt/eset/RemoteAdministrator/Server/ERAServer --daemon --p...

May 14 16:06:33 localhost.localdomain systemd[1]: Starting ESET Remote Admini...
May 14 16:06:34 localhost.localdomain systemd[1]: PID file /var/run/eraserver...
May 14 16:06:34 localhost.localdomain systemd[1]: Started ESET Remote Adminis...
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost ~]#
```

#### 4.4.4.1 Prerekvizity servera – Linux

Pre inštaláciu ESMC Servera na systéme Linux je potrebné splniť nasledujúce požiadavky:

- Musíte mať platnú [licenciu](#).
- [Databázový server musí byť nainštalovaný a nakonfigurovaný](#) s účtom root. Používateľský účet nemusí byť vytvorený pred inštaláciou, vie ho vytvoriť inštalátor.

##### **i** Poznámka:

ESMC Server ukladá do databázy veľké bloky dát, preto je dôležité pre správne fungovanie ESMC povoliť v MySQL [akceptovanie veľkých dátových balíkov](#).

- **ODBC ovládač** – ODBC ovládač sa používa na nadviazanie spojenia s [databázovým serverom](#) (MySQL).

##### **i** Poznámka:

Od verzie Ubuntu 16.04.1 LTS a Debian 9 sa už balík `libmyodbc` v oficiálnom Ubuntu repozitári nenachádza. Odporúčame stiahnuť samostatný balík z [oficiálnej webovej stránky](#) a [nainštalovať](#) ho. Avšak, tento balík nebude aktualizovaný pomocou Ubuntu metódy `apt-get upgrade`, ale bude potrebná manuálna aktualizácia.

- Inštalačný balík servera musí byť nastavený ako spustiteľný súbor. Použite nasledujúci príkaz:

```
chmod +x server-linux-x86_64.sh
```

- Minimálna podporovaná verzia openssl je **openssl-1.0.1e-30** (príkaz `openssl version` ukáže aktuálne používanú verziu).
- **Xvfb** – potrebné pre správnu tlač správ (úloha pre server [Generovať správu](#)) na systémoch Linux Server bez grafického používateľského rozhrania.
- **Cifs-utils** – potrebné pre správne nasadenie agenta v prostredí Windows OS.
- **Qt4 WebKit knižnice** – sú potrebné pre tlač správ vo formátoch PDF a PS (vyžaduje sa verzia 4.8, nie verzia 5). Všetky ostatné Qt4 závislosti sa nainštalujú automaticky. V prípade, že používate CentOS sa môže stať, že v oficiálnych repozitároch nebudú všetky požadované balíky. Môžete ich však [nainštalovať z repozitára tretích strán](#) (napr. EPEL repozitáre) alebo ich skompilovať priamo na počítači.


- **Kinit + klist** – používané pre overovanie pomocou protokolu Kerberos počas synchronizácie s AD a prihlasovania doménového používateľa. Vyžaduje sa tiež správna konfigurácia protokolu Kerberos (*/etc/krb5.conf*).
- **Wbinfo + ntlm auth** – používané pre overovanie pomocou doménového účtu a pre NTLM autentifikáciu pri SMTP serveri (odosielanie e-mailov).
- **Ldapsearch** – používané pri synchronizácii s AD.
- **Snmpttrap** – používané pre odosielanie SNMP trap správ. V prípade, že sa táto funkcia nebude používať, nie je jej inštalácia povinná. SNMP je tiež potrebné nakonfigurovať.
- **SELinux devel balík** – používa sa pri inštalácii produktov na vytváranie SELinux modulov politik. Toto sa vyžaduje len na systémoch, kde je aktivovaný SELinux (CentOS, Fedora, RHEL). Treba mať na pamäti, že SELinux môže spôsobovať problémy s ostatnými aplikáciami. Pre ESMC Server pritom nie je nevyhnutný.

Tabuľka nižšie obsahuje správne príkazy pre všetky balíky popísané vyššie pre distribúcie Debian a Ubuntu, ako aj pre distribúcie CentOS, Red Hat a Fedora:

| Debian a Ubuntu distribúcie                                                      | CentOS, Red Hat a Fedora distribúcie                                        | OpenSUSE distribúcia                                                                   |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>ODBC ovládač</b>                                                              |                                                                             |                                                                                        |
| <code>apt-get install unixodbc libmyodbc</code>                                  | <code>yum install mysql-connector-odbc</code>                               | <code>zypper install unixodbc myodbc-unixbox</code>                                    |
| <b>xvfb</b>                                                                      |                                                                             |                                                                                        |
| <code>apt-get install xvfb</code>                                                | <code>yum install xorg-x11-server-Xvfb</code>                               | <code>zypper install xorg-x11-server-extra</code>                                      |
| <b>cifs-utils</b>                                                                |                                                                             |                                                                                        |
| <code>apt-get install cifs-utils</code>                                          | <code>yum install cifs-utils</code>                                         | <code>zypper install cifs-utils</code>                                                 |
| <b>Qt4 WebKit knižnice</b>                                                       |                                                                             |                                                                                        |
| <code>apt-get install libqtwebkit4</code>                                        | Pozrite si náš <a href="#">článok databázy znalostí</a> .                   | <code>zypper install libqtwebkit4</code>                                               |
| <b>kinit+klist – voliteľné (potrebné pre službu Active Directory)</b>            |                                                                             |                                                                                        |
| <code>apt-get install krb5-user</code>                                           | <code>yum install krb5-workstation</code>                                   | <code>zypper install krb5</code>                                                       |
| <b>wbinfo + ntlm_auth</b>                                                        |                                                                             |                                                                                        |
| <code>apt-get install winbind</code>                                             | <code>yum install samba-winbind-clients</code>                              | <code>zypper install samba-winbind</code>                                              |
| <b>ldapsearch</b>                                                                |                                                                             |                                                                                        |
| <code>apt-get install ldap-utils libsasl2-modules-gssapi-mit</code>              | <code>yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap</code> | <code>zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop</code> |
| <b>snmptrap</b>                                                                  |                                                                             |                                                                                        |
| <code>apt-get install snmp</code>                                                | <code>yum install net-snmp-utils net-snmp</code>                            | <code>zypper install net-snmp</code>                                                   |
| <b>SELinux devel balík (voliteľné; Pre ESMC Server pritom nie je nevyhnutný.</b> |                                                                             |                                                                                        |

| Debian a Ubuntu distribúcie        | CentOS, Red Hat a Fedora distribúcie    | OpenSUSE distribúcia                |
|------------------------------------|-----------------------------------------|-------------------------------------|
| apt-get install selinux-policy-dev | yum install policycoreutils-devel       | zypper install selinux-policy-devel |
| <b>samba</b>                       |                                         |                                     |
| apt-get install samba              | yum install samba samba-winbind-clients | zypper install samba samba-client   |

#### 4.4.5 Inštalácia agenta – Linux

Inštalácia komponentu ESET Management Agent na operačnom systéme Linux prebieha pomocou terminálu. Uistite sa, že boli splnené všetky [požiadavky](#). Pripojenie na ESMC Server je umožnené parametrami --hostname a --port (port sa nepoužíva, ak je k dispozícii SRV záznam).  Možné formáty pripojenia.

- **Názov hostiteľa a port**
- **IPv4 adresa a port**
- **IPv6 adresa a port**
- **Servisný záznam (SRV záznam)** – pre konfiguráciu DNS zdrojového záznamu na Linuxe musí byť počítač v jednej doméne s funkčným DNS serverom. Pre viac informácií prejdite do kapitoly [DNS zdrojový záznam](#). SRV záznam musí začínať predponou „\_NAME.\_tcp“, kde „NAME“ predstavuje vlastné pomenovanie (napr. „era“).

#### Príklad inštaláčného skriptu:

(Nové riadky musia byť oddelené pomocou "\n" pre kopírovanie celého skriptu do terminálu.)

##### Serverom asistovaná inštalácia

```
./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.179.36 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

##### Offline inštalácia

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N31luI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

#### Parametre

| Atribút     | Popis                                                                                            | Vyžaduje sa   |
|-------------|--------------------------------------------------------------------------------------------------|---------------|
| --hostname  | Názov hostiteľa alebo IP adresa ESMC Servera (ERA Proxy).                                        | Áno           |
| --port      | Port ESMC Servera alebo ERA Proxy (prednastavená hodnota je 2222).                               | Áno           |
| --cert-path | Cesta k súboru certifikátu agenta (viac informácií o certifikátoch nájdete <a href="#">tu</a> ). | Áno (offline) |

| Atribút                            | Popis                                                                                                                                                                                                                                                                          | Vyžaduje sa         |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <code>--cert-auth-path</code>      | Cesta k súboru Certifikačnej autority servera (viac o certifikačných autoritách nájdete <a href="#">tu</a> ).                                                                                                                                                                  | Áno (offline)       |
| <code>--cert-password</code>       | Heslo certifikačnej autority. Musí sa zhodovať s heslom certifikátu agenta.                                                                                                                                                                                                    | Áno (offline)       |
| <code>--cert-auth-password</code>  | Heslo certifikačnej autority.                                                                                                                                                                                                                                                  | Áno (ak sa používa) |
| <code>--skip-license</code>        | Používateľovi sa počas inštalácie nezobrazí výzva na potvrdenie súhlasu s licenčnou dohodou.                                                                                                                                                                                   | Nie                 |
| <code>--product-guid</code>        | GUID produktu (ak nie je definované, vygeneruje sa).                                                                                                                                                                                                                           | Nie                 |
| <code>--cert-content</code>        | Base64 kódovaný obsah PKCS12 kódovaného verejného kľúča certifikátu a verejný kľúč použitý na nastavenie zabezpečenej komunikácie medzi serverom a agentmi. Použite len jednu z nasledujúcich možností: <code>--cert-path</code> alebo <code>--cert-content</code> .           | Nie                 |
| <code>--cert-auth-content</code>   | Base64 kódovaný obsah DER kódovaného súkromného kľúča certifikačnej autority použitého na overovanie komunikácie vzdialených klientov (proxy alebo server). Použite len jednu z nasledujúcich možností: <code>--cert-auth-path</code> alebo <code>--cert-auth-content</code> . | Nie                 |
| <code>--webconsole-hostname</code> | Názov hostiteľa alebo IP adresa používaná nástrojom Web Console na pripojenie na server (ponechaním prázdneho poľa bude použitá hodnota zadaná parametrom „hostname“).                                                                                                         | Nie                 |
| <code>--webconsole-port</code>     | Port používaný nástrojom Web Console na pripojenie na server (prednastavená hodnota je 2223).                                                                                                                                                                                  | Nie                 |
| <code>--webconsole-user</code>     | Používateľské meno používané nástrojom Web Console na pripojenie na server (prednastavená hodnota je Administrator).                                                                                                                                                           | Nie                 |
| <code>--webconsole-password</code> | Heslo používané nástrojom Web Console na pripojenie na server.                                                                                                                                                                                                                 | Áno (S-a)           |
| <code>--proxy-hostname</code>      | Názov hostiteľa HTTP Proxy pre pripojenie na server.                                                                                                                                                                                                                           | Ak sa používa proxy |
| <code>--proxy-port</code>          | Port HTTP Proxy pre pripojenie na server.                                                                                                                                                                                                                                      | Ak sa používa proxy |
| <code>--proxy-user</code>          | Používateľské meno pre HTTP Proxy.                                                                                                                                                                                                                                             | Ak sa používa proxy |
| <code>--proxy-password</code>      | Heslo pre HTTP Proxy.                                                                                                                                                                                                                                                          | Ak sa používa proxy |
| <code>--enable-imp-program</code>  | Aktivácia programu zlepšovania produktov.                                                                                                                                                                                                                                      | Nie                 |
| <code>--disable-imp-program</code> | Deaktivácia programu zlepšovania produktov.                                                                                                                                                                                                                                    | Nie                 |

## Pripojenie a certifikáty

- Údaje pre **Pripojenie na ESMC Server** musia byť zadané: `--hostname`, `--port` (port nie je potrebný, ak je použitý servisný záznam, štandardne je to 2222).
- Pre **Serverom asistovanú inštaláciu** zadajte nasledujúce údaje: `--webconsole-port`, `--webconsole-user`, `--webconsole-password`
- Pre **Offline inštaláciu** zadajte nasledujúce údaje : `--cert-path`, `--cert-password`  
Parametre inštalácie `--cert-path` a `--cert-auth-path` vyžadujú certifikačné súbory (`.pfx` a `.der`), ktoré je možné exportovať z ESMC Web Console. (Pre viac informácií si prečítajte o [exportovaní .pfx súboru](#) a [.der súboru](#).)

## Parametre typu hesla

Parametre typu hesla môžu byť zadané ako premenné prostredia, načítané zo `stdin`, alebo zadané ako text.  
Napríklad:

```
--password=env:SECRET_PASSWORD, kde SECRET_PASSWORD je premenná prostredia s heslom
--password=file:/opt/secret, kde prvý riadok textového súboru /opt/secret obsahuje vaše heslo
--password=stdin – inštalátor si prečíta heslo zo štandardného vstupu
--password="pass:PASSWORD" je rovnaký ako --password="PASSWORD" a je povinný v prípade, keď
aktuálne heslo je "stdin" (standard input) alebo reťazec začínajúci s "env:", "file:", prípadne "pass:"
```

## HTTP Proxy pripojenie

Ak používate HTTP Proxy, pomocou parametrov `--proxy-hostname`, `--proxy-port`, `--proxy-user` a `--proxy-password` definujte údaje pre pripojenie.

### PRÍKLAD: Offline inštalácia agenta s pripojením HTTP Proxy

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N31luI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
--proxy-user=Administrator \
--proxy-password=AdMiN_p1$$w0r4
```

## Protokol inštalácie

Protokol inštalácie je užitočný pri riešení problémov a nachádza sa v [súboroch protokolu](#).

Uistite sa, že inštalácia prebehla úspešne a služba je spustená pomocou nasledujúceho príkazu:  
`sudo service eraagent status`

## Aktualizácia a opravná inštalácia agenta na systéme Linux

Ak spúšťate inštaláciu agenta manuálne na systéme, kde je už agent nainštalovaný, môžu nastať nasledujúce scenáre:

- **Aktualizácia** – v prípade, že spustíte novšiu verziu inštalátora.
  - Serverom asistovaná inštalácia – aplikácia bude aktualizovaná a budú ponechané predošlé certifikáty.
  - Offline inštalácia – aplikácia bude aktualizovaná a budú použité nové certifikáty.
- **Opravná inštalácia** – v prípade, že spustíte rovnakú verziu inštalátora. Táto možnosť môže byť použitá na migráciu agenta na iný ESMC Server.
  - Serverom asistovaná inštalácia – aplikácia bude preinštalovaná a budú pre ňu použité súčasné certifikáty z ESMC Servera (definované parametrom `hostname`).
  - Offline inštalácia – aplikácia bude preinštalovaná a budú použité nové certifikáty.

Ak migrujete agenta zo staršieho servera na iný, novší ESMC Server manuálne a zároveň používate serverom asistovanú inštaláciu, spustíte inštalračný príkaz dvakrát. Najprv prebehne aktualizácia agenta a v druhom kroku budú získané nové certifikáty, aby sa agent mohol pripojiť na ESMC Server.

#### 4.4.5.1 Prerekvizity agenta – Linux

Pre inštaláciu ESET Management Agenta na operačnom systéme Linux je potrebné splniť nižšie uvedené prerekvizity.

##### Prerekvizity pre serverom asistovanú inštaláciu agenta:

- Serverový počítač musí byť dostupný zo siete a musia byť na ňom nainštalované [ESMC Server](#) a [ESMC Web Console](#).
- Inštalračný súbor ESET Management Agenta musí byť nastavený ako spustiteľný (toto nastavíte pomocou príkazu `chmod +x`).
- Musíte mať nainštalované *openssl* aspoň vo verzii `openssl-1.0.1e-30`

##### Prerekvizity pre offline inštaláciu agenta:

- Serverový počítač musí byť dostupný zo siete a musí byť na ňom nainštalovaný [ESMC Server](#).
- Musí byť vytvorený [certifikát](#) agenta.
- Musí byť vytvorený verejný kľúč [Certifikačnej autority](#) servera.
- Inštalračný súbor agenta musí byť nastavený ako spustiteľný (toto nastavíte pomocou príkazu `chmod +x`).
- Musíte mať nainštalované *openssl* aspoň vo verzii `openssl-1.0.1e-30`

##### Poznámka:

Pre Linux CentOS sa odporúča inštalácia balíka `policycoreutils-devel`. Pre inštaláciu balíka spustite nasledujúci príkaz:

```
yum install policycoreutils-devel
```

#### 4.4.6 Inštalácia Web Console – Linux

Pred inštaláciou komponentu ESMC Web Console sa uistite, že boli splnené všetky [prerekvizity](#). Pre inštaláciu ESMC Web Console postupujte podľa týchto krokov:

1. Spustíte nasledujúce príkazy pre skopírovanie súboru `era.war` do vybraného Tomcat priečinka:

|                                             |                                                         |
|---------------------------------------------|---------------------------------------------------------|
| <b>Debian a Ubuntu distribúcie</b>          | <code>sudo cp era.war /var/lib/tomcat7/webapps/</code>  |
| <b>CentOS, Red Hat a Fedora distribúcie</b> | <code>sudo cp era.war /var/lib/tomcat/webapps/</code>   |
| <b>OpenSUSE distribúcia</b>                 | <code>sudo cp era.war /usr/share/tomcat/webapps/</code> |

Prípadne môžete extrahovať obsah súboru `era.war` do priečinka `/var/lib/tomcat/webapps/era/`

2. Zadáte nasledujúci príkaz pre reštartovanie služby Tomcat a spustenie nasadenia súboru `.war`:

|                                    |                                           |
|------------------------------------|-------------------------------------------|
| <b>Debian a Ubuntu distribúcie</b> | <code>sudo service tomcat7 restart</code> |
|------------------------------------|-------------------------------------------|

|                                             |                                          |
|---------------------------------------------|------------------------------------------|
| <b>CentOS, Red Hat a Fedora distribúcie</b> | <code>sudo service tomcat restart</code> |
| <b>OpenSUSE distribúcia</b>                 | <code>sudo service tomcat restart</code> |

3. Ak ste nainštalovali ESMC Web Console na iný počítač ako ten, na ktorom je nainštalovaný ESMC Server, vykonajte nasledujúce kroky pre umožnenie komunikácie medzi ESMC Web Console a ESMC Serverom:

- I. Zastavte službu Tomcat: `sudo service tomcat7 stop`.
- II. Upravte súbor **EraWebServerConfig.properties** :

```
sudo nano /var/lib/tomcat/webapps/era\
/WEB-INF/classes/sk/eset/era/g2webconsole/server\
/modules/config/EraWebServerConfig.properties
```

Ak sa súbor **EraWebServerConfig.properties** nenachádza vo vyššie spomenutom umiestnení, môžete použiť nasledujúci príkaz:

```
find / -iname "EraWebServerConfig.properties"
```

- III. Vyhľadajte položku `server_address=localhost`.
- IV. Nahraďte `localhost` IP adresou vášho ESMC Servera a uložte súbor.
- V. Reštartujte službu Tomcat: `sudo service tomcat7 restart`.

Po dokončení inštalácie otestujte pripojenie do ESMC Web Console. Otvorte nasledujúci odkaz vo webovom prehliadači (zobrazí sa prihlasovacie okno):

<http://localhost:8080/era> alebo ak sa prihlasujete na vzdialený server,  
[http://IP\\_ADRESA\\_OR\\_HOSTNAME:8080/era](http://IP_ADRESA_OR_HOSTNAME:8080/era)

#### **i Poznámka:**

HTTP port, štandardne 8080, sa nastaví počas manuálnej inštalácie Apache Tomcat. Môžete tiež nastaviť [HTTPS pripojenie pre Apache Tomcat](#).

### **4.4.6.1 Prerekvizity ESMC Web Console – Linux**

Pred inštaláciou komponentu ESMC Web Console na systéme Linux je potrebné splniť nasledujúce prerekvizity:

- [Java](#) – vždy používajte najnovšiu oficiálne vydanú verziu Javy. ESMC Web Console vyžaduje minimálne verziu 8 (alebo `openjdk`), avšak aj napriek tomu odporúčame používať najnovšiu verziu. Podrobnejšie informácie o inštalácii Javy nájdete v našom [článku databázy znalostí](#).
- [Apache Tomcat](#) ([podporovaná](#) verzia).
- Web Console súbor (*era.war*) uložený na lokálnom pevnom disku.

Pre inštaláciu balíkov **Java** a/alebo **Apache Tomcat** použijete nasledujúce príkazy podľa distribúcie systému Linux, ktorú používate:

|                                             |                                                            |
|---------------------------------------------|------------------------------------------------------------|
| <b>Debian a Ubuntu distribúcie</b>          | <code>sudo apt-get install openjdk-8-jdk tomcat7</code>    |
| <b>CentOS, Red Hat a Fedora distribúcie</b> | <code>sudo yum install java-1.8.0-openjdk tomcat</code>    |
| <b>OpenSUSE distribúcia</b>                 | <code>sudo zypper install java-1_8_0-openjdk tomcat</code> |



## 4.4.7 Inštalácia proxy – Linux

V ESMC 7 bola funkcia ERA Proxy nahradená komponentom Apache HTTP Proxy, bežne distribuovaným v podobe `apache2` alebo `httpd` balíka. ESET Management Agency (od verzie 7) sa môžu pripájať na ESMC Server prostredníctvom Apache HTTP Proxy. Bližšie informácie o tom, ako proxy pracuje s ESET Management Agentmi, nájdete v [tejto kapitole](#).

Vyberte si scenár:

- [Nová inštalácia na systéme Linux](#)
- [Aktualizácia z predošlej verzie ERA Proxy nainštalovanej na systéme Linux](#)

### Nová inštalácia na systéme Linux

1. [Nainštalujte a nakonfigurujte komponent Apache HTTP Proxy.](#)
2. Nakonfigurujte Apache HTTP Proxy na preposielanie komunikácie agentov.
  - a. Na zariadení proxy otvorte konfiguračný súbor:
    - i. Debian distribúcie  
`/etc/apache2/mods-enabled/proxy.conf`
    - ii. Red Hat distribúcie  
`/etc/httpd/conf/httpd.conf`
  - b. Na koniec konfiguračného súboru pridajte riadok obsahujúci číslo portu, ktorý je používaný agentom na pripojenie na ESMC Server. Štandardne je to port 2222.  
`AllowCONNECT 443 563 2222`
  - c. Na zariadení proxy otvorte konfiguračný súbor:
    - i. Debian distribúcie  
`/etc/apache2/apache2.conf`
    - ii. Red Hat distribúcie  
`/etc/httpd/conf/httpd.conf`
  - d. Nájdite riadok  
`Listen 80`  
a zmeňte ho na  
`Listen 3128`
  - e. Ak ste v rámci nastavení proxy (krok č. 1) pridali obmedzenia pre IP adresy, musíte povoliť prístup na váš ESMC Server:
    - i. Do osobitného segmentu `ProxyMatch` pridajte:
      1. adresu, ktorú používajú vaše agenty na pripojenie k ESMC Serveru,
      2. všetky možné adresy vášho ESMC Servera (IP, FQDN atď.).Pridajte celý kód zobrazený nižšie, IP adresa 10.0.0.10 slúži len ako príklad a je potrebné nahradiť ju vašou vlastnou adresou.

```
</ProxyMatch>

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?(^[^@/]*@)?(10.0.0.10)>
Allow from all
</ProxyMatch>
```

- f. Reštartujte službu *Apache HTTP Proxy*.

### Aktualizácia z predošlej verzie ERA Proxy nainštalovanej na systéme Linux

Vykonanie aktualizácie v prostredí s ERA 6.x Proxy na systéme Linux je veľmi podobné [aktualizácii na systéme Windows](#) s výnimkou nastavenia ciest k súborom. Postupujte podľa inštrukcií uvedených v [tejto kapitole](#) a použite vhodný balík a cesty k súborom v závislosti od vašej distribúcie systému Linux.

#### 4.4.8 Inštalácia nástroja RD Sensor a prerekvizity inštalácie – Linux

Pre inštaláciu nástroja RD Sensor na operačnom systéme Linux postupujte podľa nasledujúcich krokov:

1. Uistite sa, že boli splnené všetky prerekvizity inštalácie:

- Sieť musí byť prehľadateľná (otvorené porty, firewall nastavený tak, aby neblokoval prichádzajúcu komunikáciu atď.).
- Server musí byť dostupný na sieti.
- Pre správne fungovanie všetkých súčastí musí byť na lokálnom počítači nainštalovaný [ESET Management Agent](#).
- Terminál musí byť otvorený.
- Inštalačný balík komponentu RD Sensor musí byť nastavený ako spustiteľný súbor:

```
chmod +x RDSensor-Linux-x86_64.sh
```

2. Spustíte nasledujúci príkaz pre spustenie inštalácie s oprávneniami sudo:

```
sudo ./RDSensor-Linux-x86_64.sh
```

3. Prečítajte si Licenčnú dohodu s koncovým používateľom (EULA). Pomocou **medzerníka** sa posuniete na ďalšiu stranu Licenčnej dohody s koncovým používateľom.

Budete vyzvaný na potvrdenie vášho súhlasu s licenciou. Stlačte kláves **Y** ak súhlasíte, ak nie, stlačte kláves **N**.

4. ESET Rogue Detection Sensor sa spustí po ukončení inštalácie.

5. Uistite sa, že inštalácia prebehla úspešne a služba je spustená pomocou nasledujúceho príkazu:

```
sudo service rdsensor status
```

6. Protokol k nástroju Rogue Detection Sensor sa nachádza v [Protokoloch](#):

```
/var/log/eset/RogueDetectionSensor/trace.log
```

#### 4.4.9 Inštalácia komponentu Mobile Device Connector – Linux

Mobile Device Connector môžete nainštalovať na iný server ako je ten, na ktorom beží váš ESMC Server. Takýto postup môže byť užitočný v prípade, ak sa napríklad rozhodnete sprístupniť Mobile Device Connector z internetu, aby mohli byť mobilné zariadenia spravované kedykoľvek.

Inštalácia komponentu ESMC Server na operačnom systéme Linux prebieha pomocou terminálu. Uistite sa, že boli splnené všetky [požiadavky](#). Môžete si pripraviť inštalačný skript a spustiť ho s oprávneniami *sudo*.

Je dostupné veľké množstvo inštalačných parametrov, niektoré sú však povinné.

Pri inštalácii sa vyžaduje váš [partnerský certifikát](#) ESMC. Môžete ho získať dvoma spôsobmi:

- **Serverom asistovaná inštalácia** – budete musieť uviesť prístupové údaje správcu, ktoré používate pre prihlásenie sa do ESMC Web Console (inštalátor automaticky stiahne potrebné certifikáty).
- **Offline inštalácia** – budete potrebovať partnerský certifikát (proxy certifikát [exportovaný](#) z nástroja ESET Security Management Center). Môžete tiež použiť váš [vlastný certifikát](#).

Je potrebné zadať nasledujúce inštalačné parametre:

HTTPS (Proxy) certifikát:

```
--https-cert-path=
```

```
--https-cert-password=
```

Partnerský Certifikát:

Pri **Serverom asistovanej inštalácii** sú potrebné aspoň tieto:

```
--webconsole-password=
```

Pri **Offline inštalácii** zadajte:

```
--cert-path=
--cert-password= (heslo nie je potrebné pre prednastavený certifikát agenta vytvorený počas prvej
inštalácie ESMC Servera)
```

Pripojenie na ESMC Server (názov alebo IP adresa):

```
--hostname=
```

Pre MySQL databázu je potrebné zadať:

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

Pre MySQL databázu je potrebné zadať:

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

### Príklad inštaláčného skriptu:

(Nové riadky musia byť oddelené pomocou "\" pre kopírovanie celého skriptu do terminálu.)

```
sudo ./mdmcore-linux-x86_64-0.0.0.0.sh \
--https-cert-path="./proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL" \
--db-driver="MySQL" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

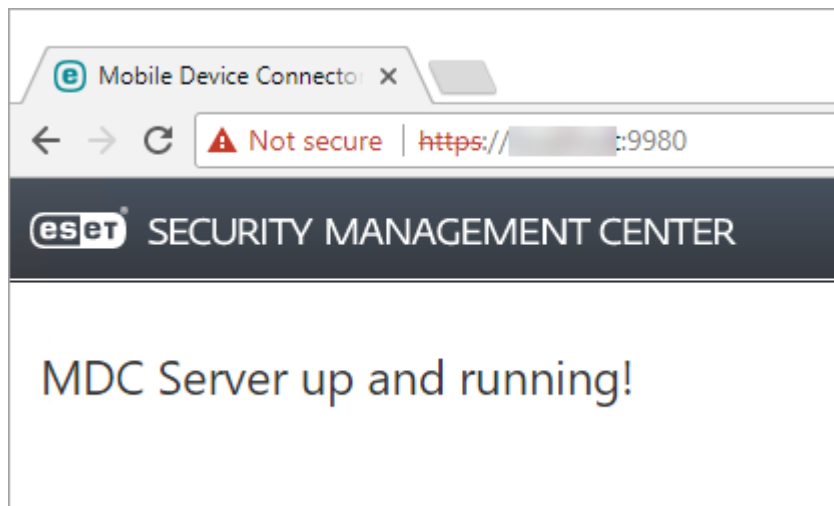
Pre úplný zoznam dostupných parametrov použite:

```
--help
```

### Protokol inštalácie

Protokol inštalácie je užitočný pri riešení problémov a nachádza sa v [súboroch protokolu](#).

Po dokončení inštalácie skontrolujte, či Mobile Device Connector funguje správne, a to otvorením adresy `https://váš-mdm-názovhostiteľa:registračný-port` (napr. `https://eramdm:9980`) vo vašom webovom prehliadači. Ak bola inštalácia úspešná, zobrazí sa nasledujúca správa:



Túto adresu môžete použiť aj na overenie dostupnosti MDM servera z internetu (po príslušnom nastavení) otvorením danej adresy na mobilnom zariadení. Ak sa vám stránka nezobrazuje, skontrolujte nastavenia firewallu vo vašej sieti.

#### 4.4.9.1 Prerekvizity pre Mobile Device Connector – Linux

Pre inštaláciu komponentu Mobile Device Connector na operačnom systéme Linux je potrebné splniť nasledujúce prerekvizity:

- Nainštalovaný a nakonfigurovaný databázový server s root účtom (používateľský účet nemusí byť vytvorený pred inštaláciou, vie ho vytvoriť inštalátor).
- Na počítači musí byť nainštalovaný ODBC ovládač pre pripojenie na [databázový server](#) (MySQL/MS SQL).  
`apt-get install unixodbc libmyodbc` (Debian a Ubuntu distribúcie)  
`yum install mysql-connector-odbc` (CentOS, Red Hat a Fedora distribúcie)  
`zypper install unixodbc myodbc-unixbox` (OpenSUSE distribúcie)

##### **i** Poznámka:

Mali by ste použiť balík **unixODBC\_23** (nie prednastavený unixODBC) pre bezproblémové pripojenie ESMC Servera na MySQL databázu. Platí to hlavne pre operačný systém SUSE Linux.

##### **i** Poznámka:

Od verzie Ubuntu 16.04.1 LTS a Debian 9 sa už balík `libmyodbc` v oficiálnom Ubuntu repozitári nenachádza. Odporúčame stiahnuť samostatný balík z [oficiálnej webovej stránky](#) a **nainštalovať** ho. Avšak, tento balík nebude aktualizovaný pomocou Ubuntu metódy `apt-get upgrade`, ale bude potrebná manuálna aktualizácia.

- Inštalačný balík MDMCore musí byť nastavený ako spustiteľný súbor:

```
chmod +x MDMCore-Linux-x86_64.sh
```

- Po úspešnej inštalácii sa uistite, že služba MDMCore je spustená.

```
service mdmcore status
```

- Musíte mať nainštalované OpenSSL minimálne vo verzii **openssl-1.0.1e-30**.

##### **i** Poznámka:

V prípade, že vaša MDM databáza na MySQL je príliš veľká (tisíce zariadení), znamená to, že prednastavená hodnota parametra `innodb_buffer_pool_size` je príliš malá. Viac informácií o optimalizácii databázy nájdete na nasledujúcom odkaze: <https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html>

### ! Dôležité:

Pre zabezpečenú komunikáciu cez HTTPS budete potrebovať **SSL certifikát** vo formáte `.pfx`. Odporúčame, aby ste použili certifikát poskytnutý certifikačnou autoritou (certifikačná autorita ESMC alebo certifikačná autorita tretej strany). Neodporúčame používať certifikáty s vlastným podpisom, pretože niektoré mobilné zariadenia takéto certifikáty neakceptujú. Toto však nie je problém v prípade certifikátov podpísaných certifikačnou autoritou, pretože takéto certifikáty sú dôveryhodné a nevyžadujú povolenie od používateľa.

### i Poznámka:

Je potrebné, aby ste mali certifikát podpísaný certifikačnou autoritou (certifikačná autorita ESMC alebo certifikačná autorita tretej strany) a príslušný privátny kľúč. Ďalej je potrebné zlúčiť certifikát podpísaný certifikačnou autoritou a privátny kľúč (pomocou OpenSSL) do jedného `.pfx` súboru:  
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCred.pfx`  
Ide o štandardný postup pre väčšinu serverov, ktoré využívajú SSL certifikáty.

### ! Dôležité:

Pre [Offline inštaláciu](#) budete potrebovať aj partnerský certifikát (**Certifikát agenta exportovaný** z nástroja ESET Security Management Center). Môžete tiež použiť váš [vlastný certifikát](#).

## 4.4.10 Inštalácia Apache HTTP Proxy – Linux

Postup inštalácie [Apache HTTP Proxy](#) zvolte podľa toho, akú distribúciu systému Linux používate na vašom serveri:

### Všeobecný postup inštalácie Apache HTTP Proxy na systéme Linux

1. Nainštalujte Apache HTTP Server (aspoň vo verzii 2.4.10).
2. Uistite sa, že sú načítané nasledujúce moduly:

`access_compat, auth_basic, authn_core, authn_file, authz_core, authz_groupfile, authz_host, proxy, proxy_http, proxy_connect, cache, cache_disk`

3. Pridajte konfiguráciu vyrovnávacej pamäte:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Ak adresár `/var/cache/apache2/mod_cache_disk` neexistuje, vytvorte ho a pridajte mu Apache oprávnenia (r, w, x).
5. Pridajte konfiguráciu Proxy:

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Povoľte pridanú vyrovnávaciu pamäť proxy a konfiguráciu (ak sa táto konfigurácia nachádza v hlavnom konfiguračnom súbore Apache, môžete tento krok vynechať).

7. Ak je to potrebné, zmeňte port pre proxy (predvolený port je 3128).

8. Voliteľné základné overovanie:

- Pridajte overovanie pre proxy:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

- Vytvorte súbor hesla pomocou `htpasswd.exe -c`

- Manuálne vytvorte súbor s názvom `group.file` a vložte doň `usergroup:username`

9. Reštartujte službu Apache HTTP Server.

## Inštalácia Apache HTTP Proxy na Ubuntu Server 14.10 a iné Debian distribúcie

1. Nainštalujte najnovšiu verziu Apache HTTP Server z apt repozitára:

```
sudo apt-get install apache2
```

2. Spustíte nasledujúci príkaz na načítanie potrebných Apache modulov:

```
sudo a2enmod access_compat auth_basic authn_core authn_file authz_core\
authz_groupfile authz_host proxy proxy_http proxy_connect cache cache_disk
```

3. Upravte konfiguračný súbor proxy cache:

```
sudo vim /etc/apache2/mods-available/cache_disk.conf
```

a do súboru vložte nasledujúce riadky:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 200000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Tento krok by nemal byť potrebný, no v prípade, že lokalita vyrovnávacej pamäte chýba, spustíte nasledujúce príkazy:

```
sudo mkdir /var/cache/apache2/mod_cache_disk
sudo chown www-data /var/cache/apache2/mod_cache_disk
sudo chgrp www-data /var/cache/apache2/mod_cache_disk
```

5. Upravte konfiguráciu Apache:

```
sudo vim /etc/apache2/conf-available/proxy.conf
```

a skopírujte nasledujúce nastavenia:

```
ProxyRequests On
ProxyVia On
<Proxy *>
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

6. Povoľte upravené konfiguračné súbory:

```
sudo a2enconf caching.conf proxy.conf
```

7. Zmeňte prijímajúci port pre Apache HTTP Server na port 3128. Upravte súbor */etc/apache2/ports.conf* a nahraďte riadok `Listen 80` riadkom `Listen 3128`.

8. Voliteľné základné overovanie:

```
sudo vim /etc/apache2/mods-enabled/proxy.conf
```

- o Skopírujte nasledujúce nastavenia pred reťazec `</Proxy>`:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /etc/apache2/password.file
AuthGroupFile /etc/apache2/group.file
Require group usergroup
```

- o Nainštalujte `apache2-utils` a vytvorte nový súbor hesla (napr. používateľ: `user`, skupina: `usergroup`):

```
sudo apt-get install apache2-utils
sudo htpasswd -c /etc/apache2/password.file user
```

- o Vytvorte súbor skupiny:

```
sudo vim /etc/apache2/group.file
```

a vložte doň nasledujúci riadok:

```
usergroup:user
```

9. Reštartujte Apache HTTP Server pomocou nasledujúceho príkazu:

```
sudo service apache2 restart
```

## Preposielanie iba pre ESET komunikáciu

Táto kapitola je dostupná len v [Online pomocníkovi](#).

## Proxy chaining (všetka komunikácia)

Majte na pamäti, že ESMC nepodporuje proxy chaining v prípade, že proxy vyžadujú autentifikáciu. Môžete použiť vlastný transparentný proxy server – avšak v tomto prípade bude pravdepodobne potrebné upraviť jeho konfiguráciu nad rámec toho, čo spomíname v tejto kapitole. Do konfigurácie proxy pridajte nasledujúci riadok (heslo funguje len pre podriadené proxy):

```
ProxyRemote * http://IP_ADDRESS:3128
```

Ak sa Proxy chaining používa na virtuálnom zariadení ESMC, je potrebné upraviť SELinux politiku. Na virtuálnom zariadení ESMC otvorte terminál a spustite príkaz:

```
/usr/sbin/setsebool -P httpd_can_network_connect 1
```

#### 4.4.11 Inštalácia Squid HTTP Proxy – Ubuntu Server

Na Ubuntu serveri môžete miesto Apache použiť Squid proxy. Inštalácia Squid na Ubuntu serveri (a podobných linuxových distribúciách založených na Debiane):

1. Nainštalujte balík Squid3:

```
sudo apt-get install squid3
```

2. Upravte konfiguračný súbor Squid `/etc/squid3/squid.conf` a nahraďte

```
#cache_dir ufs /var/spool/squid3 100 16 256
```

riadkom

```
cache_dir ufs /var/spool/squid3 5000 16 256 max-size=200000000
```

##### Poznámka:

5000 je veľkosť vyrovnávacej pamäte v MB.

3. Zastavte službu squid3.

```
sudo service squid3 stop
```

```
sudo squid3 -z
```

4. Znova upravte konfiguračný súbor Squid a pridajte `http_access allow all` pred `http_access deny all` pre umožnenie prístupu klientom k proxy.

5. Reštartujte službu squid3:

```
sudo service squid3 restart
```

#### 4.4.12 Mirror Tool

Mirror Tool je nástroj, ktorý sa používa na aktualizáciu detekčného jadra v offline prostredí. V prípade, že bezpečnostné produkty ESET na vašich klientských počítačoch potrebujú aktualizácie detekčného jadra, no nemajú pripojenie na internet, môžete použiť nástroj Mirror Tool, ktorý sťahuje aktualizčné súbory z aktualizčných serverov spoločnosti ESET a ukladá ich lokálne.

##### Poznámka:

Mirror Tool sťahuje len aktualizácie detekčného jadra, nepodporuje aktualizácie programových súčastí (PCU) ani LiveGrid dáta. Nástroj Mirror Tool dokáže tiež vytvoriť [offline repozitár](#). Môžete sa tiež rozhodnúť aktualizovať produkty ESET individuálne.

#### Prerekvizity

##### Dôležité:

Nástroj Mirror Tool nepodporuje Windows XP a Windows Server 2003.



- Cieľový priečinok musí byť zdieľaný pomocou služieb Samba/Windows alebo HTTP/FTP.
- Musíte mať platný [offline licenčný súbor](#), ktorý obsahuje používateľské meno a heslo. Pri vytváraní licenčného súboru je potrebné označiť možnosť **Zahrnúť meno a heslo**. Musíte tiež zadať **Názov** licenčného súboru. Offline licenčný súbor je nevyhnutný pre aktiváciu nástroja Mirror Tool a vytvorenie aktivačného mirror servera.

The screenshot shows a window titled "Create offline license file" with a close button (X) in the top right corner. The window is divided into several sections:

- Product:** A list of ESET products with checkboxes. "ESET Endpoint Antivirus for Windows" is checked. Other products include "ESET Endpoint Security for Windows", "ESET Endpoint Antivirus for Mac OS X", "ESET NOD32 Antivirus Business Edition for Linux Desktop", "ESET Endpoint Security for Mac OS X", "ESET Virtualization Security", "ESET Shared Local Cache", "ESET Virtual Agent Host", and "ESET Mobile Device Connector".
- Name:** A text input field containing "My custom name".
- Units count:** A numeric input field containing "1" and a spinner control, with a "/9" label to the right.
- Username and password:** A checkbox labeled "Include Username and Password" which is unchecked. Below it is the text "When included it is possible to update from ESET servers".
- Remote administrator:** A checkbox labeled "Allow management with Remote Administrator" which is checked and highlighted with a red box.
- ERA management token:** A text input field containing a long alphanumeric string: "00007987-68F6-2846-1890-83E2E5308893". This field is also highlighted with a red box.

At the bottom of the window, there are two buttons: "GENERATE" and "CANCEL".

- Musíte mať k dispozícii súbor nástroja Mirror Tool. Nástroj je dostupný k stiahnutiu na [webovej stránke spoločnosti ESET](#) v sekcii **Samostatné inštalátory**.
- Na počítači, na ktorom bude používaný nástroj Mirror Tool, musíte mať nainštalovaný balík [Visual C++ Redistributable for Visual Studio 2010](#).
- Na počítači, na ktorom bude používaný nástroj Mirror Tool, musíte mať nainštalovaný balík [Visual C++ Redistributables for Visual Studio 2015](#).
- Nástroj pozostáva z dvoch súborov:
  - Windows: MirrorTool.exe a updater.dll
  - Linux: MirrorTool a updater.so

## Použitie

- Pre zobrazenie pomocníka pre Mirror nástroj spustíte `MirrorTool --help`. Zobrazia sa všetky dostupné príkazy nástroja:

```
C:\Users\>MirrorTool.exe --help
Mirror Tool, Copyright (c) ESET, spol. s r.o. 1992-2017. All rights reserved.
Allowed options:
--mirrorType arg [required for module update]
 Type of mirror. Possible values (case
 insensitive): regular, pre-release,
 delayed.
--intermediateUpdateDirectory arg [required for module update]
 Files will be downloaded to this
 directory to create mirror in output
 directory.
--offlineLicenseFilename arg [required for module update]
 Offline license file.
--updateServer arg [optional]
 Update server. (e.g.:
 http://update.eset.com/eset_upd/ep6/)
 Mirror will be created in output
 directory, only specified path in
 server will be mirrored.
--outputDirectory arg [required for module update]
 Directory where mirror will be created.
--proxyHost arg [optional]
 Http proxy address (fqdn or IP).
--proxyPort arg [optional]
 Http proxy port.
--proxyUsername arg [optional]
 Http proxy username.
--proxyPassword arg [optional]
 Http proxy password.
--networkDriveUsername arg [optional]
 Username used, when output directory is
 accessed using smb(e.g:\\hostname).
--networkDrivePassword arg [optional]
 Password used, when output directory is
 accessed using smb(e.g:\\hostname).
--excludedProducts arg [optional]
 Disable creating mirror for specified
 products. Possible values: ep4 ep5 ep6
 era6.
--repositoryServer arg [required for repository update]
 Repository server for repository
 creation.
--intermediateRepositoryDirectory arg [required for repository update]
 Files will be downloaded to this
 directory to create offline mirror in
 output directory.
--outputRepositoryDirectory arg [required for repository update]
 Directory where offline repository will
 be created..
--help [optional]
 Display this help and exit
```

- Parameter `--updateServer` je voliteľný. Pri použití tohto parametra musíte zadať celú URL adresu aktualizáčného servera.

- Parameter `--offlineLicenseFilename` je povinný. Musíte zadať celú cestu k offline licenčnému súboru (ako je to popísané vyššie).
- Pre vytvorenie mirroru spustíte `MirrorTool` minimálne so všetkými povinnými parametrami. Príklad:
  - Windows:

```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

- Linux:

```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

## Nástroj Mirror Tool a nastavenia aktualizácií

- Pre automatizáciu distribúcie aktualizácií vírusovej databázy môžete naplánovať spúšťanie nástroja Mirror Tool. Otvorte Web Console a prejdite do sekcie **Úlohy pre klienta > Operačný systém > Spustiť príkaz. Vyberte Príkazový riadok na spustenie** (vrátane cesty k súboru `MirrorTool.exe`) a spúšťač (napríklad CRON výraz pre každú hodinu `00***?*`). Na plánované spustenie môžete tiež použiť nástroj Plánovač úloh pre systém Windows alebo na systéme Linux použiť Cron.
- Pre zmenu nastavení aktualizácií na klientských počítačoch použijete novú politiku a nastavíte **Aktualizačný server** tak, aby odkazoval na adresu mirror serveru alebo zdieľaný priečinok.

### 4.4.13 Failover klastr – Linux

Táto kapitola popisuje inštaláciu a konfiguráciu produktu ESET Security Management Center na Red Hat high-availability klastru.

#### Podpora klastra – Linux

Komponenty ESET Security Management Center Servera môžu byť nainštalované na **Red Hat Linux 6** klastru a novších. Failover klaster sú podporované iba v aktívnom/pasívnom režime vytvorené prostredníctvom `rgmanager`.

#### Prerekvizity

- Aktívny/pasívny klastr musí byť nainštalovaný a nastavený. Súčasne môže byť spustený len jeden uzol, ďalšie uzly musia byť v režime standby. Load balancing nie je podporované.
- Zdieľané úložiská – iSCSI SAN, NFS a iné sú podporované (každá technológia alebo protokol, ktorý pristupuje k zdieľanému úložisku po blokoch alebo súboroch a úložisko mapuje tak, že sa tvári ako lokálne pripojená jednotka). Zdieľané úložisko musí byť prístupné z každého aktívneho uzla klastra a musí mať správne inicializovaný súborový systém (napr. použitie súborového systému EXT3 alebo EXT4).

- Pre správu systému sú potrebné nasledujúce HA rozšírenia :
  - rgmanager
  - Conga
- rgmanager je tradičný Red Hat HA klaster stack. Je to povinný komponent.
- Grafické používateľské prostredie **Conga** je voliteľné. Failover klaster môže byť spravovaný bez tohto prostredia, odporúčame ho však nainštalovať. Pri použití tejto príručky ho treba mať nainštalované.
- **Fencing** musí byť správne nastavený, aby sa predišlo poškodeniu dát. Ak fencing ešte nie je nastavený, správca klastra ho musí nastaviť.

Ak ešte nemáte spustený klaster, pre vytvorenie a nastavenie high-availability failover klastra (aktívneho alebo pasívneho) použite nasledujúcu príručku spoločnosti Red Hat: [Red Hat Enterprise Linux 6 Cluster Administration](#).

## Rozsah

Súčasťou ESET Security Management Center, ktoré možno nainštalovať na **Red Hat Linux** HA klaster:

- ESMC Server a ESET Management Agent

### **i** Poznámka:

- ESET Management Agent musí byť nainštalovaný, pretože v opačnom prípade sa nespustí služba ESMC klaster.
- Inštalácia ESMC databázy na klaster je podporovaná len v prípade, že klaster je poskytnutý službou SQL a ESMC sa pripája na jednu adresu hostiteľa databázy.

Nasledujúci príklad je pre klaster s dvoma uzlami. Avšak, môžete použiť tento príklad aj ako referenciu pre inštaláciu nástroja ESET Security Management Center na klaster s viacerými uzlami. Uzly klastra sú v tomto príklade pomenované **node1** a **node2**.

## Kroky inštalácie

1. Nainštalujte [ESMC Server](#) na uzol node1.
  - Majte na pamäti, že certifikát servera musí v časti názov hostiteľa obsahovať externú IP adresu (alebo názov) rozhrania klastra (nie lokálnu IP adresu alebo názov uzla).
2. Zastavte a deaktivujte službu ESMC Server pomocou nasledujúcich príkazov:

```
service eraserver stop
chkconfig eraserver off
```

3. Pripojte zdieľané úložisko k uzlu node1. V tomto príklade je zdieľané úložisko pripojené ako `/usr/share/erag2cluster`.
4. V `/usr/share/erag2cluster` vytvorte nasledujúce adresáre:

```
/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/opt/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/log/eset/RemoteAdministrator/Server
/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator/Server
```

5. Rekurzívne skopírujte adresáre do nasledujúcich umiestnení (zdroj > destinácia):

| Zdroj:                                                | Destinácia:                                                           |
|-------------------------------------------------------|-----------------------------------------------------------------------|
| <code>/etc/opt/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/etc/opt/eset/RemoteAdministrator</code> |
| <code>/opt/eset/RemoteAdministrator/Server</code>     | <code>/usr/share/erag2cluster/opt/eset/RemoteAdministrator</code>     |
| <code>/var/log/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/var/log/eset/RemoteAdministrator</code> |
| <code>/var/opt/eset/RemoteAdministrator/Server</code> | <code>/usr/share/erag2cluster/var/opt/eset/RemoteAdministrator</code> |

6. Vytvorte symbolické odkazy (možno bude potrebné manuálne vytvoriť nové priečinky):  
Táto kapitola je dostupná len v [Online pomocníkovi](#).

7. Skript `eracluster_server`, ktorý sa nachádza v inštalačnom priečinku ESMC Servera, skopírujte do `/usr/share/cluster`. Skripty nepoužívajú v inštalačnom priečinku `.sh` príponu.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/e
```

8. Odpojte zdieľané úložisko z uzla node1.
9. Pripojte zdieľané úložisko na uzol node2 do rovnakého adresára ako pri node1 (`/usr/share/erag2cluster`).

10. V uzle node2 vytvorte nasledujúce symbolické odkazy:  
Táto kapitola je dostupná len v [Online pomocníkovi](#).

11. Skript `eracluster_server`, ktorý sa nachádza v inštalačnom priečinku ESMC Servera, skopírujte do `/usr/share/cluster`. Skripty v inštalačnom priečinku nepoužívajú `.sh` príponu.

```
cp /opt/eset/RemoteAdministrator/Server/setup/eracluster_server /usr/share/cluster/e
```

☐ Nasledujúce kroky treba vykonať v grafickom používateľskom rozhraní Conga Cluster Administration:

12. Vytvorte **skupinu služby**, napríklad `ESMCSERVICE`.

ESET Security Management Center klaster vyžaduje tri zdroje: IP adresu, súborový systém a skripty.

13. Vytvorte potrebné zdroje služby.

Pridajte IP adresu (externú IP adresu klastra, na ktorú sa budú pripájať Agenty), súborový systém a zdroj skriptov.

Súborový systém by mal odkazovať na zdieľané úložisko.

Bod pripojenia súborového systému by mal byť nastavený na `/usr/share/erag2cluster`.

Parameter „Full Path to Script File“ by mal byť nastavený na `/usr/share/cluster/eracluster_server`.

14. Tieto zdroje pridajte do skupiny `ESMCSERVICE`.

☐ Po úspešnom vytvorení a nastavení klastra [nainštalujte ESET Management Agentu](#) na oba uzly na lokálnom disku (nie na zdieľaný disk klastra). Pri použití príkazu `--hostname=` je nutné zadať externú IP adresu alebo hostiteľský názov rozhrania klastra (**nie parameter `localhost`**)!

#### 4.4.14 Odinštalovanie alebo preinštalovanie komponentu – Linux

Ak chcete preinštalovať alebo aktualizovať komponent na najnovšiu verziu, spustíte znova inštalačný skript.

Pre odinštalovanie komponentu (v tomto prípade je to ESMC Server) spustíte inštalátor s parametrom `--uninstall`:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

Ak chcete odinštalovať iný komponent, použite v príkaze príslušný názov inštalačného balíka. Napríklad ESET Management Agent:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

##### ⚠ Dôležité:

Pri odinštalovaní sa odstránia súbory databázy a nastavenia. Pre zachovanie súborov databázy vytvorte SQL dump databázy s parametrom `--keep-database`.

Po odinštalovaní skontrolujte, či boli odstránené:

- služba `eraserver`.
- priečinok `/etc/opt/eset/RemoteAdministrator/Server/`.

##### ℹ Poznámka:

Pred odinštalovaním odporúčame vytvoriť zálohu databázy pre prípad, že budete potrebovať obnoviť dáta.

Viac informácií týkajúcich sa preinštalovania agenta nájdete v tejto [kapitole](#).

## 4.5 Inštalácia súčastí na systéme macOS

Vo väčšine inštalčných scenárov potrebujete nainštalovať rôzne súčasti nástroja ESET Security Management Center na rôzne počítače v závislosti od sieťovej architektúry, výkonnostných požiadaviek atď.

### **i** Poznámka:

MacOS je podporovaný len ako klient. [ESET Management Agent](#) a [produkty spoločnosti ESET pre macOS](#) môžu byť nainštalované na macOS, avšak ESMC Server na macOS nainštalovaný byť nemôže.

### 4.5.1 Inštalácia agenta – macOS

Táto sekcia popisuje postup lokálnej inštalácie agenta.

1. Uistite sa, že boli splnené všetky **prerekvizity**:

- **ESMC Server** a **ESMC Web Console** sú nainštalované (na serveri).
- [Certifikát](#) agenta je vytvorený a pripravený na lokálnom disku.
- [Certifikačná autorita](#) je pripravená na vašom lokálnom disku (potrebné len pri nepodpísaných certifikátoch).

### **i** Poznámka:

Ak sa vyskytnú problémy pri vzdialenom nasadení ESET Management Agent (úloha pre server **Nasadenie agentov** skončí chybou), pozrite si kapitolu [Riešenie problémov s nasadením agenta](#).

2. Stiahnite si inštalčný súbor (samostatný inštalátor agenta *.dmg*) z [webovej stránky spoločnosti ESET](#) alebo alebo si ho vyžiadajte od svojho správcu systému.

3. Dvakrát kliknite na súbor *Agent-MacOSX-x86\_64.dmg* a spustíte inštaláciu dvojitém kliknutím na súbor *.pkg*.

4. Pokračujte v inštalácii. Po výzve zadajte parametre **pripojenia na server**:

- **Názov hostiteľského servera**: názov hostiteľa alebo IP adresa ESMC Servera.
- **Port servera**: port určený na komunikáciu agenta so serverom, predvolená hodnota je 2222.
- **Použiť proxy**: zvolte túto možnosť, ak chcete na spojenie medzi agentom a serverom používať HTTP proxy.

### **i** Poznámka:

Toto nastavenie proxy sa používa len na replikáciu medzi ESET Management Agentom a ESMC Serverom, nie na ukladanie aktualizácií do vyrovnávacej pamäte.

- **Názov hostiteľa proxy**: názov hostiteľa alebo IP adresa zariadenia s HTTP proxy.
- **Port proxy**: prednastavená hodnota je 3182.
- **Používateľské meno, Heslo**: zadajte prihlasovacie údaje používané vaším proxy, ak sa vyžaduje autentifikácia.

Nastavenia proxy môžete neskôr zmeniť vo vašej [politike](#). Najprv musíte nainštalovať [proxy](#), až potom môžete prostredníctvom neho nakonfigurovať spojenie medzi agentom a serverom.

5. Vyberte [Partnerský certifikát](#) a zvolte preň heslo. Môžete tiež pridať [Certifikačnú autoritu](#).

6. Skontrolujte cestu inštalácie a kliknite na **Inštalovať**. Agent bude nainštalovaný na váš počítač.

7. Protokol ESET Management Agent sa nachádza v nasledujúcom umiestnení:

```
/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log
```

## 4.6 Databáza

ESET Security Management Center používa databázu na uchovanie dát o pripojených zariadeniach. V nasledujúcich sekciách nájdete podrobné informácie o [zálohovaní](#), [aktualizácii](#) a [migrácii](#) databázy ESMC Servera (ERA Servera alebo služby ERA 6.x Proxy, ak používate verziu 6.x):

- Skontrolujte kompatibilitu databázy a [systémové požiadavky](#) pre ESMC Server.
- Ak nemáte nastavenú databázu pre použitie s ESMC Serverom, môžete nainštalovať **Microsoft SQL Server Express**, ktorý je zahrnutý v inštallačnom balíku.
- Ak používate Microsoft Small Business Server (SBS) alebo Essentials, odporúčame, aby ste sa uistili, že všetky [požiadavky](#) sú splnené a že používate [podporovaný operačný systém](#). Keď sú všetky požiadavky splnené, postupujte podľa [inštallačných inštrukcií pre Windows SBS/Essentials](#) pre inštaláciu ESMC na týchto operačných systémoch.
- Ak máte na vašom systéme nainštalovaný Microsoft SQL Server, skontrolujte požiadavky uvedené nižšie, aby ste sa uistili, že používate Microsoft SQL Server vo verzii, ktorá je podporovaná nástrojom ESET Security Management Center. Ak používate Microsoft SQL Server vo verzii, ktorá nie je podporovaná, [aktualizujte svoj SQL Server na kompatibilnú verziu](#).

### **i** Poznámka:

Komponent ERA Proxy z verzie 6 bol z dôvodu zmeny protokolu replikácie agenta nahradený službou [proxy](#) tretej strany. Nemigrujte databázu Proxy medzi verziami 6.x a 7.

[Vykonanie aktualizácie v prostredí s ERA Proxy](#)

Jednou z prerekvizít pre inštaláciu ESMC je aj nainštalovanie a konfigurácia Microsoft SQL Servera. Je potrebné splniť nasledujúce požiadavky:

- Nainštalujte Microsoft SQL Server 2008 R2 alebo novší, prípadne môžete nainštalovať Microsoft SQL Server 2008 R2 Express alebo novší. Počas inštalácie vyberte pre autentifikáciu **Mixed mode**.
- Ak je Microsoft SQL Server už nainštalovaný, nastavte druh autentifikácie na **Mixed mode (SQL Server authentication and Windows authentication)**. Postupujte podľa inštrukcií v nasledujúcom [článku databázy znalostí](#).
- Povoľte TCP/IP pripojenie na SQL Server. Postupujte podľa inštrukcií v nasledujúcom [článku databázy znalostí](#) (časť II. **Povoľte TCP/IP pripojenie na SQL Server**).

### **i** Poznámka:

- Na konfiguráciu a správu databázového systému Microsoft SQL Server si [stiahnite SQL Server Management Studio \(SSMS\)](#).
- Ak si počas inštalácie zvolíte nainštalovať Microsoft SQL Server Express, nebude možné ho nainštalovať na doménový radič. Toto je pravdepodobné v prípade, že používate Microsoft SBS. Ak používate Microsoft SBS, odporúčame vám nainštalovať ESET Security Management Center na iný server alebo nevybrať počas inštalácie komponent SQL Server Express (v takomto prípade musíte použiť na spustenie ESMC databázy svoj existujúci SQL Server alebo MySQL). Inštrukcie týkajúce sa inštalácie ESMC Servera na doménový radič nájdete v našom [článku databázy znalostí](#).

### 4.6.1 Záloha a obnova databázy

Všetky informácie a nastavenia produktu ESET Security Management Center sú uložené v databáze. Odporúčame preto pravidelne zálohovať túto databázu pre zníženie rizika straty dát. Postupujte podľa nasledujúcich návodov podľa typu vašej databázy:

### **i** Poznámka:

- Záloha sa tiež dá použiť neskôr pri migrácii produktu ESET Security Management Center na nový server.
- Názvy databáz a protokolov ostanú rovnaké aj po zmene názvu produktu z ESET Remote Administrator na ESET Security Management Center.

## Príklady zálohovania MS SQL databázy

Pri vytváraní záložného súboru MS SQL databázy sa môžete riadiť nižšie uvedenými príkladmi:

### ! Dôležité:

V rámci týchto príkladov sa používajú predvolené nastavenia (napr. predvolený názov databázy a predvolené nastavenia pripojenia k databáze). Skript použitý na zálohovanie budete musieť upraviť tak, aby odrážal všetky vaše zásahy do pôvodných nastavení.

### Jednorazová záloha databázy

Pre vytvorenie záložného súboru s názvom **BACKUPFILE** spustíte v príkazovom riadku systému Windows nasledujúci príkaz:

```
SQLCMD -S HOST\ERASQL -q "BACKUP DATABASE ERA_DB TO DISK = N'BACKUPFILE'"
```

### i Poznámka:

**HOST** je v tomto prípade IP adresa alebo názov hostiteľa a **ERASQL** je názov inštancie MS SQL servera. Od verzie produktu ESMC 7 môžete (ak používate MS SQL databázu) nainštalovať ESMC Server na SQL inštanciu, ktorú si pomenujete podľa seba. V takomto prípade je potrebné adekvátne upraviť zálohovacie skripty.

### Pravidelné zálohovanie databázy pomocou SQL skriptu

Táto kapitola je dostupná len v [Online pomocníkovi](#).

### Obnovenie MS SQL databázy

Táto kapitola je dostupná len v [Online pomocníkovi](#).

---

## Zálohovanie MySQL databázy

Táto kapitola je dostupná len v [Online pomocníkovi](#).

Ak si želáte obnoviť databázu zo zálohy, postupujte podľa nasledujúceho návodu:

### Obnovenie MySQL databázy

Táto kapitola je dostupná len v [Online pomocníkovi](#).

### i Poznámka:

Pre viac informácií o zálohovaní Microsoft SQL databázy navštívte [oficiálnu stránku spoločnosti Microsoft](#). Pre viac informácií o zálohovaní MySQL databázy si prečítajte [dokumentáciu pre databázový server MySQL](#).

## 4.6.2 Aktualizácia databázového servera

Aktualizáciu existujúcej Microsoft SQL Server inštancie na novšiu verziu pre použitie s ESMC Serverom vykonáte podľa nižšie uvedených inštrukcií:

1. **Zastavte** všetky spustené ESMC Server alebo ERA Proxy služby pripájajúce sa na databázový server, ktorý budete aktualizovať. Takisto zastavte všetky ostatné aplikácie, ktoré sa môžu pripájať na vašu Microsoft SQL Server inštanciu.
2. Bezpečne [zálohujte](#) všetky relevantné databázy predtým, ako budete pokračovať.
3. Zálohujte databázový server podľa inštrukcií dodávateľa databázy.
4. **Spustite** službu ESMC Server a skontrolujte sledovacie protokoly pre overenie, či databázové pripojenie funguje správne.



Pre viac informácií navštívte nasledujúce stránky podľa jednotlivých databáz:

- Aktualizácia SQL Servera: <https://msdn.microsoft.com/en-us/library/bb677622.aspx> (pre inštrukcie týkajúce sa aktualizácie na konkrétnu verziu SQL Servera kliknite na **Other Versions**)
- Aktualizácia MySQL Servera (na **verziu 5.6**): <http://dev.mysql.com/doc/refman/5.6/en/upgrading.html>

## 4.7 Obraz ISO

Obraz ISO je jeden z formátov, v ktorom môžete [stiahnuť](#) inštalačné súbory nástroja ESET Security Management Center. Obraz ISO obsahuje nasledovné:

- Inštalačný balík ESMC
- Samostatné inštalačné balíky pre všetky komponenty

Obraz ISO je užitočný v prípade, ak si želáte mať všetky inštalačné balíky nástroja ESET Security Management Center na jednom mieste. Pri jeho použití nemusíte inštalačné balíky sťahovať zo stránky spoločnosti ESET vždy, keď chcete spustiť inštaláciu. ISO obraz je tiež užitočný v prípade, že chcete nainštalovať ESET Security Management Center na virtuálny počítač.

## 4.8 DNS servisný záznam

**Nastavenie DNS zdrojového záznamu:**

1. Na vašom DNS serveri (DNS server na radiči domény) prejdite do sekcie **Control Panel > Administrative Tools**.
2. Vyberte DNS.
3. V nástroji DNS Manager označte `_tcp` v stromovej štruktúre a vytvorte nový záznam typu **Service location (SRV)**.
4. Zadajte názov služby do poľa **Service** podľa štandardných pravidiel DNS a na začiatku názvu použite podčiarkovník (`_`). Použite vlastný názov služby, napr. `_era`.
5. Zadajte tcp protokol do poľa **Protocol** v nasledujúcom formáte: `_tcp`.
6. Do poľa **Port number** zadajte číslo 2222.
7. Zadajte úplný názov domény (FQDN) pre ESMC Server do poľa **Host offering this service**.
8. Záznam uložte kliknutím na **OK > Done**. Nový záznam sa zobrazí v zozname.

**Overenie DNS záznamu:**

1. Prihláste sa na ktorýkoľvek počítač vo vašej doméne a otvorte príkazový riadok (cmd.exe).
2. Do príkazového riadka zadajte `nslookup` a stlačte **Enter**.
3. Zadajte `set querytype=srv` a stlačte **Enter**.
4. Zadajte `_era._tcp.domain.name` a stlačte **Enter**. Lokalita služby je zobrazená správne.

### **i** Poznámka:

Keď nainštalujete ESET Security Management Center Server na iný počítač, nezabudnite zmeniť hodnotu „Host offering this service:“ na úplný názov domény (FQDN) vášho nového servera.

## 4.9 Scenár offline inštalácie ESMC

V sieťach bez prístupu na internet môžete využiť metódu offline inštalácie nástroja ESMC a jeho komponentov. Postupujte podľa nasledujúcich krokov:

### ! Dôležité:

Inštrukcie pre aktualizáciu ESMC nájdete v kapitole [Aktualizácia komponentov ESMC v offline prostredí](#).

Inštalácia pomocou GPO/SCCM: Prečítajte si náš [článok databázy znalostí](#).

### Inštalácia z lokálneho repozitára

1. [Nainštalujte ESET Security Management Center](#). V priebehu inštalácie vyberte možnosť **Aktivovať neskôr a aktivujte ESMC** neskôr pomocou [offline licencie](#).
2. Vytvorte lokálny repozitár pre inštalačné balíky. Sú na to tri spôsoby:
  - a) Vytvorte lokálny repozitár prostredníctvom Apache Tomcat, ktorý bol nainštalovaný spolu s ESMC.
    - I. Prejdite do: `C:/Program Files (x86)/Apache Software Foundation/Tomcat 7.0/webapps/`
    - II. Pre lokálny repozitár vytvorte nový priečinok, napríklad `esmc_repository`.
    - III. Inštalačné balíky skopírujte do repozitára.
    - IV. Inštalačné balíky budú dostupné na tejto adrese:  
`https://tomcat_server:tomcat_port/esmc_repository/Agent_MacOSX-x86_64.dmg`
  - b) Vytvorte lokálny repozitár prostredníctvom Apache HTTP Proxy.
    - I. [Nainštalujte Apache HTTP Proxy](#).
    - II. Prejdite do nasledujúceho priečinka: `C:\Program Files\Apache HTTP Proxy\htdocs\` (umiestnenie je možné zmeniť v konfiguračnom súbore).
    - III. Skopírujte inštalačné balíky do tohto priečinka.
    - IV. Inštalačné balíky budú dostupné na tejto adrese:  
`http://proxy_server:proxy_port/Agent_MacOSX-x86_64.dmg`
  - c) Použite priečinok/disk zdieľaný na sieti.
3. Nainštalujte komponent ESET Management Agent prostredníctvom [live inštalátora agenta](#) – v inštalačnom skripte použite URL adresu inštalačného balíka agenta umiestneného v lokálnom repozitári. Viac informácií nájdete v našom [článku databázy znalostí](#).
4. Nasaďte bezpečnostné produkty ESET na koncové pracovné stanice vo vašej sieti pomocou [úlohy pre klienta „Inštalácia softvéru“](#). Pri vytváraní tejto úlohy zadajte príslušnú URL adresu inštalačného balíka agenta umiestneného v lokálnom repozitári. Inštalačné balíky sú dostupné k stiahnutiu na [webovej stránke spoločnosti ESET](#).
5. Aktivujte bezpečnostné produkty ESET použitím offline licencie:
  - [Ako aktivovať firemné produkty ESET bez internetového pripojenia?](#)
  - [Ako aktivovať firemné produkty ESET pomocou nástroja ESET Security Management Center?](#)
6. [Vypnite ESET Live Grid](#).
7. Aktualizáciu vírusovej databázy môžete riešiť dvoma spôsobmi (a, b):

### ! Dôležité:

Apache HTTP Proxy môže spĺňať funkciu aktualizáčného servera (mirror), avšak Apache Tomcat musí byť v tomto prípade nastavený tak, aby nepoužíval SSL. Pripojenie k ESMC Web Console bude bezpečné.

- a) V uzavretej sieti bez pripojenia na internet musí správca vytvoriť vlastný aktualizčný server – „mirror“ priečink, v ktorom budú uložené aktualizčné súbory pre klienty:
- I. Ak sa ako aktualizčný server použije Apache HTTP Proxy/Apache Tomcat, [klienty musia byť nakonfigurované tak, aby si aktualizácie sťahovali z vlastného aktualizčného serveru vytvoreného správcom](#) (nie proxy).
  - II. Ak sa ako mirror server použije produkt ESET Endpoint Security pre Windows, [klienty musia byť nakonfigurované tak, aby si aktualizácie sťahovali z daného mirroru](#).
- b) V prípade siete, kde má aspoň jeden počítač pripojenie na internet:
- I. Môžete použiť Apache HTTP Proxy a [nakonfigurovať klienty tak, aby používali proxy](#).
  - II. Ako aktualizčný server môžete použiť Tomcat + Mirror Tool a klienty nastaviť tak, aby [používali vlastný aktualizčný server](#).
  - III. Mirror môžete nastaviť pomocou produktu ESET Endpoint Security pre Windows a klienty nakonfigurovať tak, aby [sťahovali aktualizácie z daného mirroru](#).
8. Dôrazne odporúčame pravidelne aktualizovať moduly produktu. Ak moduly nie sú aktuálne, počítače zobrazené vo Web Console nesú označenie **Neaktualizovaný**. Toto upozornenie je v ESMC Web Console možné potlačiť – zo zoznamu vyberte daný počítač a následne v roletovom menu kliknite na možnosť **Potlačiť**.

## 5. Aktualizácia, migrácia a preinštalovanie

Táto kapitola popisuje rôzne metódy aktualizácie, migrácie a preinštalovania vášho ESET Security Management Center Servera a ostatných súčastí nástroja ESMC.

### 1. Aktualizácia z ERA 5

Aktualizácia/migrácia zo staršej generácie ERA 5 na ESMC 7 pomocou nástroja [Asistent migrácie](#).

Ak chcete nasadiť ESET Management Agentu pomocou nástroja ERA 5.x, prečítajte si [tento článok v databáze znalostí](#).

### 2. Aktualizácia z ERA 6.x na najnovšiu ESMC 7 verziu

[Aktualizácia súčastí](#) vašej ESET Security Management Center infraštruktúry.

#### Poznámka:

Pre zistenie verzie jednotlivých používaných súčastí ESMC si skontrolujte verziu svojho ESET Security Management Center Servera. V ESMC Web Console prejdite do časti [O programe](#), kde nájdete verziu svojho ESMC Servera. Verziu jednotlivých súčastí potom nájdete v nasledujúcom [článku databázy znalostí](#) podľa verzie ESMC Servera.

### 3. Migrácia alebo preinštalovanie nástroja ESMC 7 zo servera na server

Vykonanie [migrácie z jedného servera na druhý](#) alebo [preinštalovanie ESMC Servera](#).

#### Poznámka:

Ak sa chystáte migrovať ESMC Server na iný počítač, musíte exportovať/zálohovať všetky certifikačné authority, ako aj certifikát ESMC Servera. V opačnom prípade súčasti ESMC nebudú komunikovať s vašim novým ESMC Serverom.

### 4. Ďalšie postupy

Zmena [názvu hostiteľa alebo IP adresy](#) ESMC Servera.

#### Dôležité:

Po vykonaní aktualizácie zo starších verzií ERA (6.4 a staršie) na verziu 7.0 dôjde k viacerým zmenám týkajúcim sa používateľov a úloh. Bezpečnostný model v ESMC 7.0 je odlišný od predošlého, a preto je potrebná kontrola používateľských nastavení, skupín a úloh. Viac informácií nájdete v kapitole [Zmeny po aktualizácii zo staršej verzie ERA](#), nachádzajúcej sa v príručke správcu.

## 5.1 Aktualizácia súčastí

### Odporúčania:

Na aktualizáciu vašej ESMC infraštruktúry odporúčame použiť úlohu pre klienta **Aktualizácia súčastí**, ktorá je dostupná prostredníctvom rozhrania ESMC Web Console. Predtým, ako vykonáte aktualizáciu, si prečítajte inštrukcie.

[Vykonanie aktualizácie v prostredí s ERA Proxy](#)

#### Dôležité:

Iba ERA 6.3 a novšie verzie môžu byť aktualizované na ESMC 7.

Pred spustením aktualizáčnej úlohy si zálohujete nasledujúce dáta:

- Všetky certifikáty (certifikačná autorita, certifikát servera a certifikát agenta).
  1. Exportujte svoj verejný kľúč [certifikačnej autority](#) zo starého ESMC Servera ako `.der` súbor a uložte ho na externé ukladacie zariadenie.
  2. Exportujte svoje [klientske certifikáty](#) (pre ESET Management Agentu a ESMC Server) a súbor súkromného kľúča `.pfx` zo starého ESMC Servera a uložte ich na externé ukladacie zariadenie.
- [ERA/ESMC databázu](#).

### Odporúčaný postup aktualizácie:

1. Najprv aktualizujte ESMC Server (počítač, na ktorom beží ESMC Server).

#### **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.

2. Vyberte niekoľko klientskych počítačov, na ktorých skúšobne spustíte aktualizáciu úlohu (použite aspoň jedného klienta pre každý systém/bitovú verziu).
  - Pre zníženie zaťaženia siete odporúčame na distribúciu aktualizácií použiť [Apache HTTP Proxy](#) (alebo iný transparentný proxy server s aktívnym ukladaním do vyrovnávacej pamäte). Zvolené testovacie klienty spustia sťahovanie potrebných inštalátorov a ich uloženie do vyrovnávacej pamäte (cache). Pri ďalšom spustení aktualizácie úlohy už budú inštalátory na jednotlivé klientske počítače distribuované priamo z vyrovnávacej pamäte.
3. Po úspešnom otestovaní aktualizácie pokračujte v rovnakom postupe aj na zvyšných klientoch. Druhou možnosťou je ako cieľ úlohy nastaviť statickú skupinu *Všetko*. Klientske počítače, ktoré už boli aktualizované, po druhýkrát aktualizované nebudú.

### Zoznam súčastí, ktoré možno aktualizovať:

- ESMC Server
- ESET Management Agent (úloha aktualizuje všetky počítače na sieti, ktoré majú nainštalovaného ESET Management Agentu, ak sú zvolené ako ciele pre danú úlohu)
- ESMC Web Console (aktualizácia je možná len v prípade, že ste konzolu inštalovali pomocou ESMC all-in-one inštalátora, používate virtuálne zariadenie ESMC alebo ju máte na Linuxe v inštaláčnom priečinku: `/var/lib/tomcat8/webapps/`, `/var/lib/tomcat7/webapps/`, `/var/lib/tomcat/webapps/`)
- ESMC Mobile Device Connector. Odporúčame aktualizovať MDM z verzie 6.1 najskôr na verziu 6.4 a až potom vykonať aktualizáciu prostredia na verziu 7.

#### **Poznámka:**

ESMC vás automaticky upozorní na [dostupnosť novej verzie ESMC Servera](#).

### Nasledujúce súčasti je potrebné aktualizovať manuálne:

- Apache Tomcat (dôrazne odporúčame udržiavať Apache Tomcat aktuálny, pozrite si časť [Aktualizácia Apache Tomcat](#))
- Apache HTTP Proxy (aktualizáciu je možné vykonať pomocou all-in-one inštalátora, pozrite si časť [Aktualizácia Apache HTTP Proxy](#))
- ESMC [Rogue Detection Sensor](#)

#### **Dôležité:**

Na aktualizáciu bezpečnostných produktov ESET slúži úloha [Inštalácia softvéru](#). Spustite túto úlohu s použitím najnovšieho inštalátora, aby bola cez váš súčasný bezpečnostný produkt nainštalovaná najnovšia verzia programu.

### Predtým, ako začnete:

#### **Upozornenie:**

Ak zlyhá aktualizácia súčastí na počítači, na ktorom beží ESMC Server alebo Web Console, môže sa stať, že nebude možné vzdialené prihlásenie do Web Console. Pred začatím aktualizácie vám preto odporúčame nastaviť fyzický prístup k tomuto serveru. Ak nie je možné zriadiť fyzický prístup k serveru, uistite sa, že sa naň viete pripojiť ako správca pomocou vzdialenej pracovnej plochy. Odporúčame tiež pred aktualizáciou [zálohovať](#) databázy ESMC Servera a databázy komponentu Mobile Device Connector. Pre zálohovanie virtuálneho zariadenia vytvorte snímku (snapshot) alebo naklonujte vaše virtuálne zariadenie.

#### ☐ ESMC Server nainštalovaný na Failover klastri

Ak je váš ESMC Server nainštalovaný na Failover klastri, musíte aktualizovať komponent ESMC Server manuálne pre každý uzol. Po dokončení aktualizácie ESMC Servera spustíte úlohu [Aktualizácia súčastí](#) pre aktualizáciu celej infraštruktúry (napríklad ESET Management Agentov na klientskych počítačoch).

#### ☐ Dôležité informácie pred aktualizáciou Apache HTTP Proxy na systéme Microsoft Windows

Ak používate Apache HTTP Proxy a máte vlastné nastavenia v súbore `httpd.conf` (napr. prihlasovacie meno a heslo), zálohujte si váš pôvodný súbor `httpd.conf` (umiestnený v `C:\Program Files\Apache HTTP Proxy\conf\`). Ak nepoužívate vlastné nastavenia, nie je potrebné zálohovať súbor `httpd.conf`. Aktualizujte Apache HTTP Proxy na najnovšiu verziu ktorýmkoľvek zo spôsobov spomenutých v časti [Aktualizácia Apache HTTP Proxy](#).

#### **Upozornenie:**

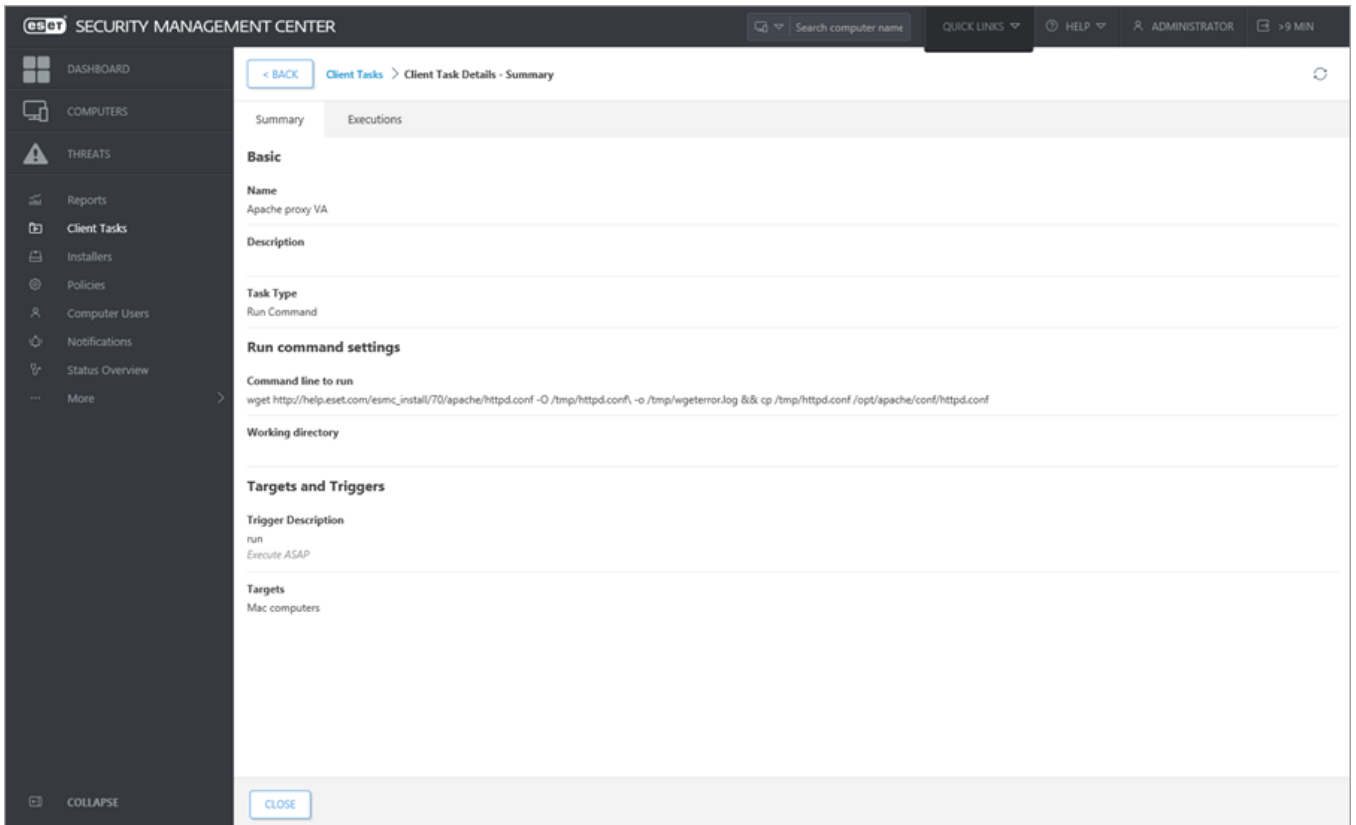
Keď ste úspešne aktualizovali Apache HTTP Proxy na systéme Windows a v pôvodnom súbore `httpd.conf` ste mali vlastné nastavenia (napr. prihlasovacie meno a heslo), skopírujte nastavenia zo zálohovaného súboru `httpd.conf` a do nového súboru `httpd.conf` pridajte len vaše vlastné nastavenia. Nepoužívajte váš pôvodný `httpd.conf` súbor s novou, aktualizovanou verziou Apache HTTP Proxy, pretože nebude správne fungovať. Skopírujte z neho len vaše vlastné nastavenia a použite nový `httpd.conf` súbor. Váš nový `httpd.conf` súbor si môžete prispôsobiť aj manuálne, nastavenia sú popísané v časti [Inštalácia Apache HTTP Proxy – Windows](#).

#### ☐ Dôležité informácie pred aktualizáciou Apache HTTP Proxy na virtuálnom zariadení

Ak používate **Apache HTTP Proxy** a máte vlastné nastavenia vo svojom `httpd.conf` súbore (napr. používateľské meno a heslo), zálohujte svoj pôvodný `httpd.conf` súbor (nachádzajúci sa v `/opt/apache/conf/`) a spustíte klientsku úlohu **Aktualizácia súčastí Security Management Center** pre aktualizáciu **Apache HTTP Proxy**. Ak nepoužívate vlastné nastavenia, nie je potrebné vytvoriť si zálohu súboru `httpd.conf`.

Po úspešnom dokončení úlohy Aktualizácia súčastí spustíte nižšie uvedený príkaz. Priradíte ho k počítaču, na ktorom je nainštalované Apache HTTP Proxy. Spustíte klientsku úlohu [Spustiť príkaz](#), čím sa aktualizuje `httpd.conf` súbor (je to potrebné pre správne fungovanie aktualizovanej verzie Apache HTTP Proxy):

```
wget https://help.eset.com/esmc_install/70/apache/httpd.conf -O\
/tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
/opt/apache/conf/httpd.conf
```



Ak Apache HTTP Proxy beží na vašom virtuálnom počítači, môžete spustiť rovnaký príkaz priamo z konzoly virtuálneho zariadenia ESMC. Ďalšou možnosťou je manuálne nahradenie konfiguračného súboru [httpd.conf](http://httpd.conf) pre Apache HTTP Proxy.

#### **⚠ Upozornenie:**

Ak máte vo vašom pôvodnom `httpd.conf` súbore vlastné nastavenia (napr. používateľské meno a heslo), skopírujte nastavenia zo zálohovaného `httpd.conf` súboru do nového `httpd.conf` súboru a pridajte doň len vaše vlastné nastavenia. Nepoužívajte váš pôvodný `httpd.conf` súbor s novou, aktualizovanou verziou Apache HTTP Proxy, pretože nebude správne fungovať. Skopírujte z neho len vaše vlastné nastavenia a použite nový `httpd.conf` súbor. Váš nový `httpd.conf` súbor si môžete prispôbiť aj manuálne, nastavenia sú popísané v časti [Inštalácia Apache HTTP Proxy – Linux](#).

Bližšie informácie týkajúce sa úlohy aktualizácie súčastí nástroja Security Management Center nájdete v [nasledujúcej kapitole online pomocníka](#). Ďalšie inštrukcie súvisiace s aktualizáciou nástroja ESET Security Management Center na najnovšiu verziu nájdete v našom [článku databázy znalostí](#).

#### **Riešenie problémov:**

- Skontrolujte, či máte [prístup do ESMC repozitára](#) z aktualizovaného počítača.
- Opätovné spustenie úlohy Aktualizácia súčastí nebude fungovať, ak už je aspoň jedna súčasť aktualizovaná na novú verziu.
- Ak nie je žiadny jasný dôvod zlyhania, môžete sa pokúsiť aktualizovať súčasti manuálne. Prečítajte si naše inštrukcie pre [Windows](#) alebo [Linux](#).
- Ďalšie informácie ohľadom riešení problémov s aktualizáciou nájdete v časti [Riešenie problémov](#).

### 5.1.1 Aktualizácia v rámci infraštruktúry s ERA 6.5 Proxy

Komponent ERA Proxy sa už v nástroji ESMC 7 nenachádza. Ak máte prostredie, v ktorom používate komponent proxy, postupujte podľa nasledujúcich krokov pre aktualizáciu vašej infraštruktúry na ESMC 7.0.

#### **Upozornenie:**

- Nižšie sú uvedené dôležité informácie týkajúce sa kompatibility:
  - ERA 6.x Agent sa dokáže pripojiť na ESMC 7 Server.
  - ESET Management Agent (verzie 7) sa nedokáže pripojiť na ESMC Server prostredníctvom ERA Proxy.
  - ESET Management Agent (verzie 7) sa nedokáže pripojiť k nástroju ERA.
- Nevykonávajte aktualizáciu ERA Agentov predtým, ako nakonfigurujete vhodné riešenie proxy.

1. Zálohujte si svoj ERA Server.
2. Aktualizujte ERA Server na ESMC 7 prostredníctvom úlohy **Aktualizácia súčastí Security Management Center**. Aktualizované budú komponenty Server, Agent a Web Console.
3. Počkajte približne 24 hodín a uistite sa, že aktualizácia prebehla úspešne.
4. Aktualizujte ERA Agentu na zariadení, kde beží ERA Proxy, pomocou úlohy **Aktualizácia súčastí Security Management Center**.
5. Nainštalujte *Apache HTTP Proxy* na zariadenie, kde je nainštalované ERA Proxy. Použite prednastavenú ESET verziu *Apache* (dostupná k stiahnutiu [tu](#)).
6. Upravte konfiguračný súbor *Apache HTTP Proxy* – `httpd.conf`, ktorý sa nachádza v `C:\Program Files\Apache HTTP Proxy\conf`. Štandardne sa používa port číslo 2222, ak ste však zmenili port počas inštalácie, použite vlastné číslo portu.
  - a. Pridajte nasledujúci riadok: `AllowCONNECT 443 563 2222`

```
<Proxy *>
Deny from all
</Proxy>
#*.eset.com:
AllowCONNECT 443 563 2222
<ProxyMatch>
```

- b. Do osobitného segmentu `ProxyMatch` pridajte:
  - i. adresu, ktorú používajú vaše agenty na pripojenie k ESMC Serveru,
  - ii. všetky možné adresy vášho ESMC Servera (IP, FQDN atď.).Pridajte celý kód zobrazený nižšie, IP adresa 10.0.0.10 slúži len ako príklad a je potrebné nahradiť ju vašou vlastnou adresou.

```
<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^\@/]*@)?(10.0.0.10)>
Allow from all
</ProxyMatch>
```

- c. Reštartujte službu *Apache HTTP Proxy*.



7. Vytvorte novú politiku na svojom ESMC Serveri.
  - a. V ESMC Web Console kliknite na **Politiky > Vytvoriť novú politiku**.
  - b. V sekcii **Základné** zadajte **Názov** politiky.
  - c. V sekcii **Nastavenia** vyberte možnosť ESET Management Agent.
  - d. Prejdite do sekcie **Pripojenie > Servery pre pripojenie > Upraviť zoznam serverov**.
  - e. Kliknite na **Pridať** a do poľa **Hostiteľ** zadajte adresu zariadenia, na ktorom beží služba proxy (zariadenie, na ktorom je nainštalované ERA Proxy). Kliknite na **OK**.
  - f. Zopakujte krok spomenutý vyššie a pridajte adresu svojho ESMC Servera (adresa sa musí zhodovať s konfiguráciou agenta).
  - g. Kliknite na **Uložiť**.
  - h. Prejdite do sekcie **Pokročilé nastavenia > HTTP proxy** a v rámci **Konfigurácie proxy** vyberte možnosť **Rôzne proxy pre každú službu**.
  - i. Kliknite na **Replikácia > Upraviť** a povoľte možnosť **Použiť proxy server**.
  - j. Zadajte IP adresu zariadenia s proxy do poľa **Hostiteľ**. IP adresa 10.0.1.10 na obrázku slúži len ako príklad a je potrebné nahradiť ju vašou vlastnou adresou.
  - k. V poli **Port** ponechajte pôvodnú hodnotu 3128.
  - l. Politiku uložte kliknutím na **Uložiť** a **Dokončiť**. Politiku zatiaľ nepriradíte k žiadnemu počítaču.

**! Dôležité:**

- Je absolútne nevyhnutné pridať do zoznamu adries v konfigurácii **obe IP adresy**. V prípade, že agent nedostane túto informáciu v rámci jednej politiky, nebude sa môcť po vykonaní aktualizácie pripojiť k proxy a serveru. V takomto prípade bude potrebné manuálne opraviť agenta vykonaním opravnej inštalácie a zadaním správnej adresy ESMC Servera.
- V prípade, že v politike nie je definovaná konfigurácia HTTP Proxy, agent sa nebude môcť pripojiť na ESMC Server. Manuálna opravná inštalácia pri riešení takejto situácie nepomôže.

8. Vyberte si jeden z počítačov pripojených prostredníctvom ERA Proxy a priradte k nemu novú politiku.
9. Počkajte niekoľko minút, kým sa politika aplikuje, a skontrolujte, či sa počítač naďalej pripája k ESMC Serveru.
10. Spustite úlohu **Aktualizácia súčastí Security Management Center** pre vykonanie aktualizácie klienta.
11. Po aktualizácii klienta na verziu 7 skontrolujte, či sa aj naďalej pripája k ESMC Serveru. Ak sa počítač po aktualizácii úspešne pripája k serveru, vykonajte aktualizáciu aj pre ostatné počítače.

**! Dôležité:**

Ak máte väčšiu sieť, začnite s aktualizáciou na pracovných staniciach, ktoré sa nachádzajú nablízku alebo v rámci oddelení so skúsenejšími používateľmi v oblasti IT. Uľahčí to riešenie prípadných problémov.

12. Aplikujte politiku (z kroku č. 5) na ostatné počítače, ktoré sa pripájajú prostredníctvom ERA Proxy.
13. Počkajte niekoľko minút, kým sa politika aplikuje, a skontrolujte, či sa počítače naďalej pripájajú k ESMC Serveru.
14. Na týchto počítačoch spustite úlohu **Aktualizácia súčastí Security Management Center**.
15. Ak sa po dokončení aktualizácie všetky klienty pripájajú na ESMC Server, môžete pokračovať pomocou ďalších krokov.
16. Upravte politiku (z kroku č. 5). Prejdite do sekcie **Politiky**, kliknite na ikonu vedľa politiky, ktorú chcete upraviť, a následne kliknite na možnosť **Upraviť**.
  - a. V sekcii **Nastavenia > Pripojenie** kliknite na **Upraviť zoznam serverov** a odstráňte adresu zariadenia s ERA Proxy.
  - b. Kliknite na **Uložiť**.
  - c. Politiku aplikujte a uložte kliknutím na **Dokončiť**.
17. Odstráňte ERA Proxy pomocou úlohy v sekcii **Úlohy pre klienta > Odinštalovanie softvéru**.

## 5.2 Migrácia z ERA 5.x

Ak chcete prejsť alebo migrovať zo staršej generácie ERA 5 na ESET Security Management Center 7, môžete použiť jednu z nasledujúcich samostatných aplikácií ESET:

- **Asistent migrácie (Migration Assistant)** – Asistent migrácie je určený pre malé a stredne veľké firmy. Úlohou Asistenta migrácie je nainštalovať nástroj ESET Security Management Center vo verzii 7.0, skontrolovať aktuálnu konfiguráciu, premigrovať dáta z ERA Servera verzie 5.x a nakoniec vypnúť ERA 5.x.
- **Nástroj na migráciu (Migration Tool)** – pomáha pri migrácii dát z ERA 5.x do prechodnej databázy, ktorá umožňuje importovanie dát do ESMC 7.x.

### **i** Poznámka:

Asistent migrácie a Nástroj na migráciu sú podporované len na počítačoch s operačným systémom Windows od spoločnosti Microsoft.

V nasledujúcej tabuľke nájdete porovnanie Asistenta migrácie s Nástrojom na migráciu z hľadiska migrovaných položiek a možností migrácie:

|                                                                               | Asistent migrácie | Nástroj na migráciu |
|-------------------------------------------------------------------------------|-------------------|---------------------|
| <b>Migrované položky:</b>                                                     |                   |                     |
| Statické skupiny <sup>1</sup>                                                 | ✓                 | ✓                   |
| Licencie                                                                      | ✓                 | ✗                   |
| Politiky <sup>2</sup>                                                         | ✓                 | ✓                   |
| HTTP proxy                                                                    | ✓ <sup>3</sup>    | ✗                   |
| Nastavenia aktualizácií                                                       | ✓                 | ✗                   |
| Počítače                                                                      | ✗                 | ✓                   |
| Správy                                                                        | ✗                 | ✗                   |
| Protokoly                                                                     | ✗                 | ✓ <sup>4</sup>      |
| Úlohy <sup>5</sup>                                                            | ✗                 | ✗                   |
| Hrozby                                                                        | ✗                 | ✗                   |
| Používatelia                                                                  | ✗                 | ✓                   |
| Parametrické skupiny <sup>5</sup>                                             | ✗                 | ✗                   |
| Server s podriadenými servermi <sup>6</sup>                                   | ✗                 | ✗                   |
| <b>Možnosti migrácie:</b>                                                     |                   |                     |
| Spustenie na počítači, na ktorom je nainštalovaný ERA Server 5.x <sup>7</sup> | ✓                 | ✓                   |
| Spustenie na počítači, kde bude bežať ESMC 7 <sup>7</sup>                     | ✓                 | ✓                   |
| Migrácia na rovnakom počítači <sup>7</sup>                                    | ✓                 | ✓                   |

|                                              | Asistent migrácie | Nástroj na migráciu |
|----------------------------------------------|-------------------|---------------------|
| Migrácia na inom počítači <sup>7</sup>       | ✓                 | ✓                   |
| Integrovaná inštalácia nového ESMC 7 Servera | ✓                 | ✗                   |

- Štruktúra statických skupín je zachovaná. Statické skupiny synchronizované z Active Directory sú však ignorované a nebudú migrované.
- Ak nie ste oboznámený s jednotlivými politikami nastavenými v rámci vášho nástroja ERA 5.x, môžete namiesto ich migrácie do ESMC 7 vytvoriť nové. Ak sa rozhodnete migrovať politiky, je dôležité brať na vedomie nasledovné:
  - Migrované sú len definície politik, nie však vzťahy medzi nimi.
  - Budete musieť manuálne priradiť migrované politiky ku skupinám.
  - Štruktúra politik je vynechaná. Príznak **Prepísať** bude v rámci politik ESMC 7 zmenený na príznak **Vynútiť**.
  - Ak sú v starom ERA v jednej politike nastavenia pre viaceré produkty, v ESMC 7 sa vytvoria politiky pre každý produkt samostatne.
- Nastavenia HTTP proxy sú z politik odstránené a proxy nainštalované spolu s novým ESMC Serverom je nastavené ako predvolené proxy.
- Migrácia bude vykonaná pre nasledujúce typy protokolov: protokoly hrozieb, protokoly kontroly, protokoly firewallu, protokoly správy zariadení, protokoly webovej kontroly a protokoly udalostí.
- Nie je možné preniesť parametrické skupiny a úlohy z ERA 5.x kvôli novému dizajnu a funkciám [dynamických skupín v ESMC 7](#) (prvýkrát predstavené v ERA 6.x).
- Migrácia ERA Serverov 5.x v stromovej štruktúre serverov nie je podporovaná.
- Ako Asistent migrácie, tak aj Nástroj na migráciu musí byť najprv spustený na počítači, kde je nainštalovaný ERA Server 5.x. Potom môžete pokračovať v migrácii v závislosti od toho, kde bude nainštalovaný ESMC Server 7.x: či už na tom istom počítači, kde bol nainštalovaný nástroj ERA 5.x, alebo na inom počítači.

### 5.2.1 Asistent migrácie

Ak sa chcete dozvedieť, ktoré nastavenia je možné premigrovať pomocou Asistenta migrácie, pozrite si toto [porovnanie](#) Asistenta migrácie a Nástroja na migráciu (Migration Tool).

#### Prerekvizity pre inštaláciu ESMC Servera

- Pre inštaláciu a konfiguráciu databázového systému Microsoft SQL Server Express je potrebné splniť nasledujúce podmienky:
  - Na serveri musí byť nainštalovaný Microsoft .NET Framework 3.5. V prípade operačného systému Windows Server 2008 alebo novších verzií môžete .NET 3.5 nainštalovať pomocou Sprievodcu rolami a funkciami servera. Ak používate Windows Server 2003, môžete .NET 3.5 stiahnuť z nasledujúceho odkazu: <http://www.microsoft.com/en-us/download/details.aspx?id=21>
  - Na serveri musí byť nainštalovaný [Java Runtime Environment](#) (JRE). Vždy používajte najnovšiu oficiálne vydanú verziu Javy.
- Pre použitie existujúcej inštancie MySQL alebo Microsoft SQL Server je potrebné [splniť nasledujúce podmienky](#).

#### Požiadavky na fungovanie Asistenta migrácie

Uistite sa, že v ERA 5.x sú zahrnuté všetky licencie k bezpečnostným produktom nainštalovaným na klientskych počítačoch. Overiť si to môžete nasledujúcimi spôsobmi:

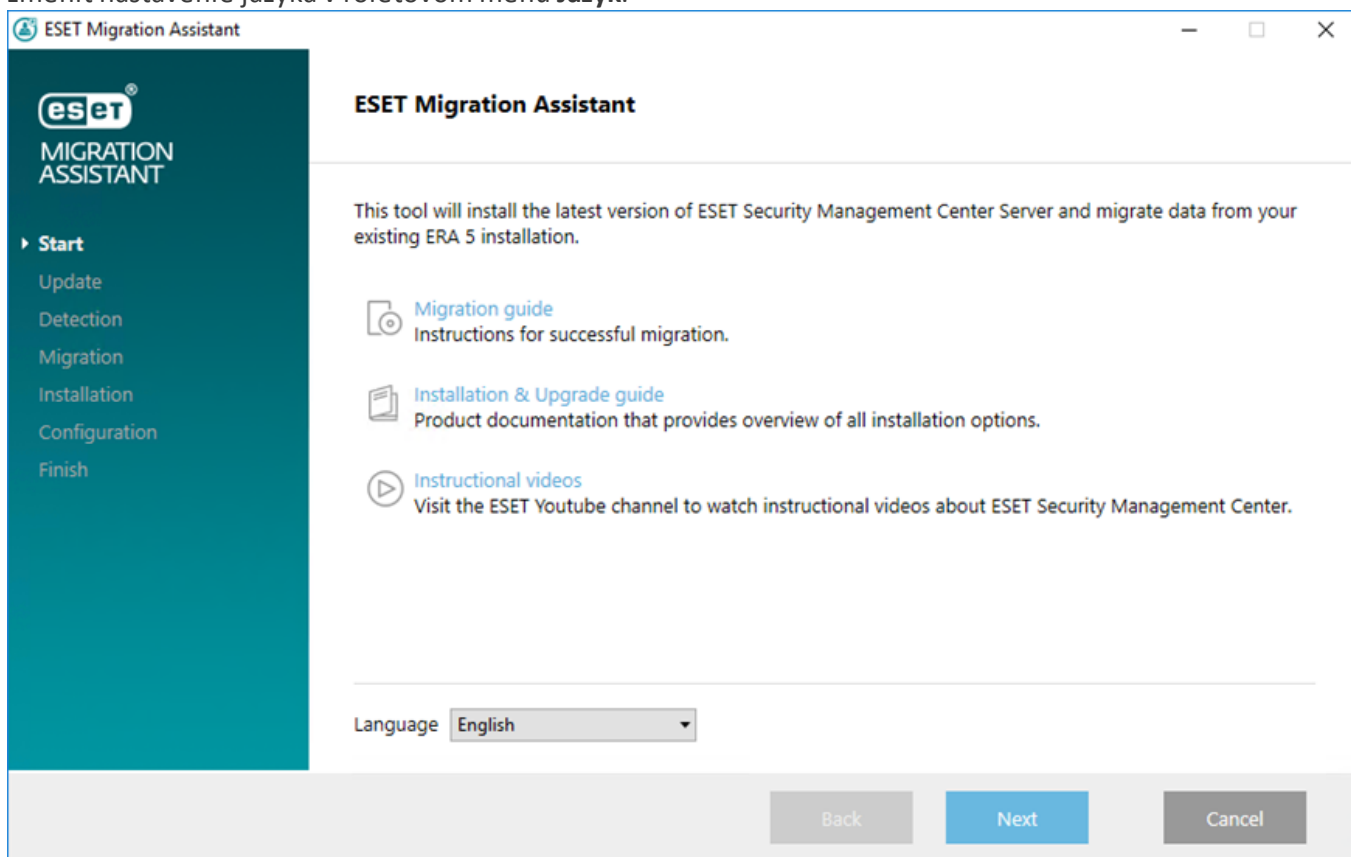
- Kliknite na klientsky počítač a vyžiadajte si príslušnú konfiguráciu kliknutím na **Request Data > Request Configuration**. Nastavenia produktu ESET určeného pre koncové zariadenia a nainštalovaného na klientskom počítači budú odoslané na ERA Server.
- Vytvorte novú konfiguračnú úlohu. Prejdite do sekcie **Update > Profiles > Settings** a zadajte vaše používateľské meno (**Username**) a heslo (**Password**).
- Prejdite do sekcie **Tools > Server Options**, kliknite na záložku **Updates** a zadajte vaše **Update username**.

## Postup migrácie dát prostredníctvom Asistenta migrácie

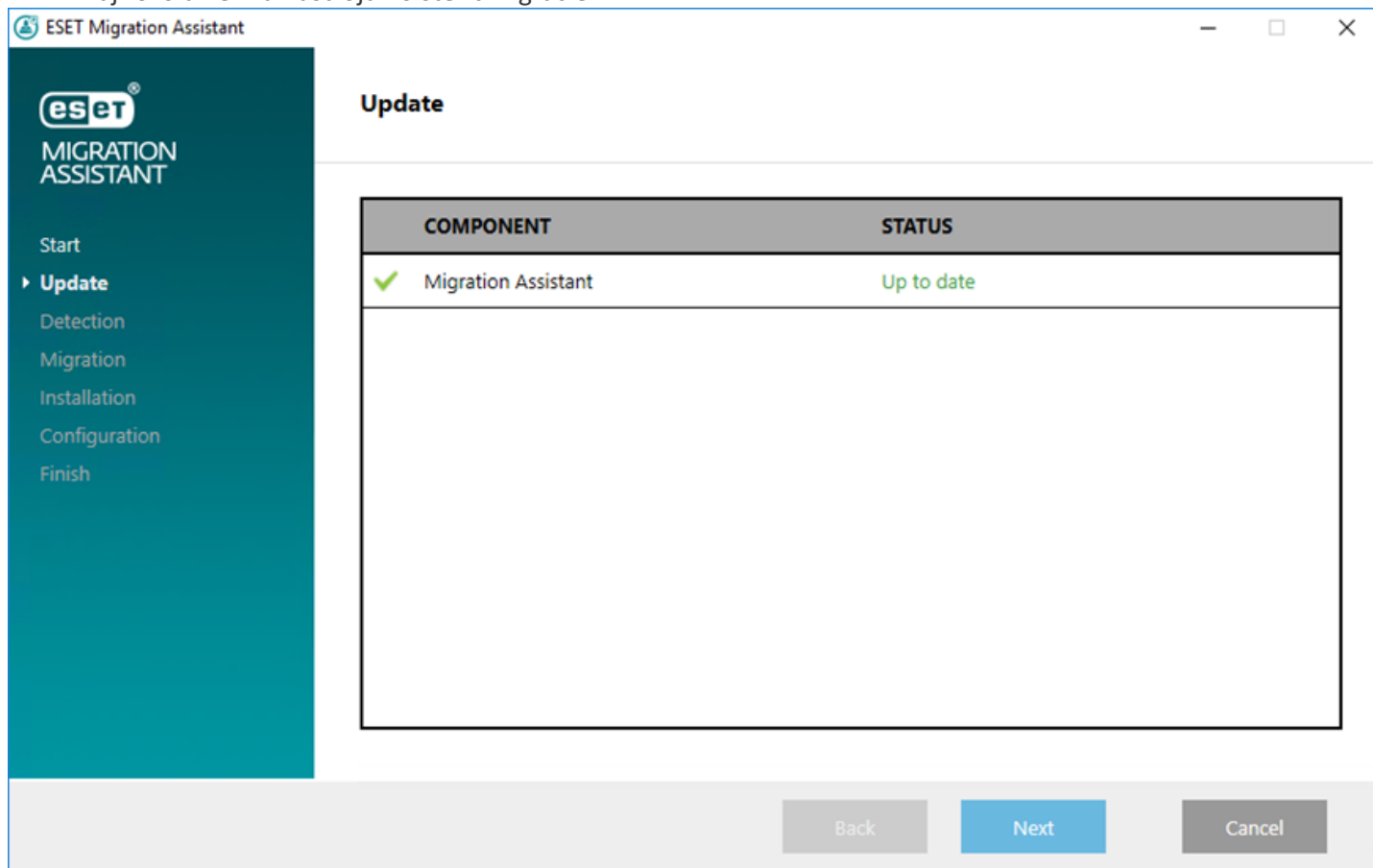
### ! Dôležité:

Pred spustením Asistenta migrácie si zálohujte vašu databázu.

1. Z [webovej stránky spoločnosti ESET](#) si stiahnite nástroj Asistent migrácie.
2. Z [webovej stránky spoločnosti ESET](#) si stiahnite all-in-one inštalátor nástroja ESMC. Vyberte si inštaláčny balík vhodný pre váš systém.
3. Extrahujte súbor .zip obsahujúci all-in-one inštalátor.
4. Skopírujte priečinok *Installers* umiestnený v priečinku All-in-one (x64/x86) do priečinka *MigrationAssistant*.
5. Prejdite do priečinka *MigrationAssistant* a dvojitým kliknutím spustíte aplikáciu Asistent migrácie. Zobrazí sa sprievodca nástroja ESET Migration Assistant.
6. Na úvodnej obrazovke kliknite na možnosť **Ďalej**. Predtým, ako budete pokračovať, môžete v prípade potreby zmeniť nastavenie jazyka v roletovom menu **Jazyk**.



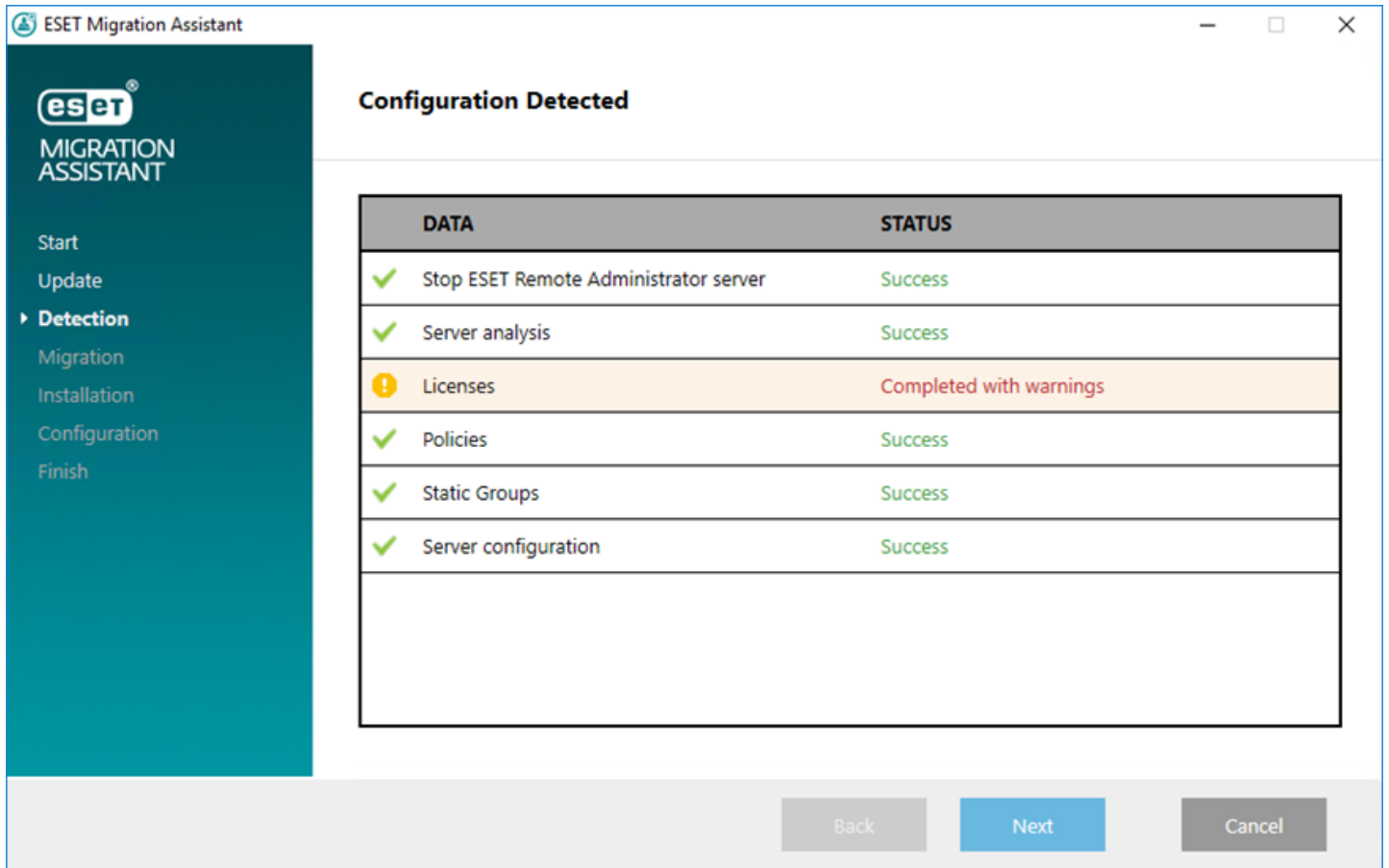
7. Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**.
8. Ak súhlasíte so zasielaním správ o zlyhaní programu a anonymných telemetrických údajov spoločnosti ESET, môžete označiť možnosť **Zúčastnite sa programu zlepšovania produktov**.
9. V sekcii **Aktualizácia** Asistent migrácie kontroluje dostupnosť aktualizácií. Odporúčame vždy používať najnovšiu verziu nástroja Asistent migrácie.



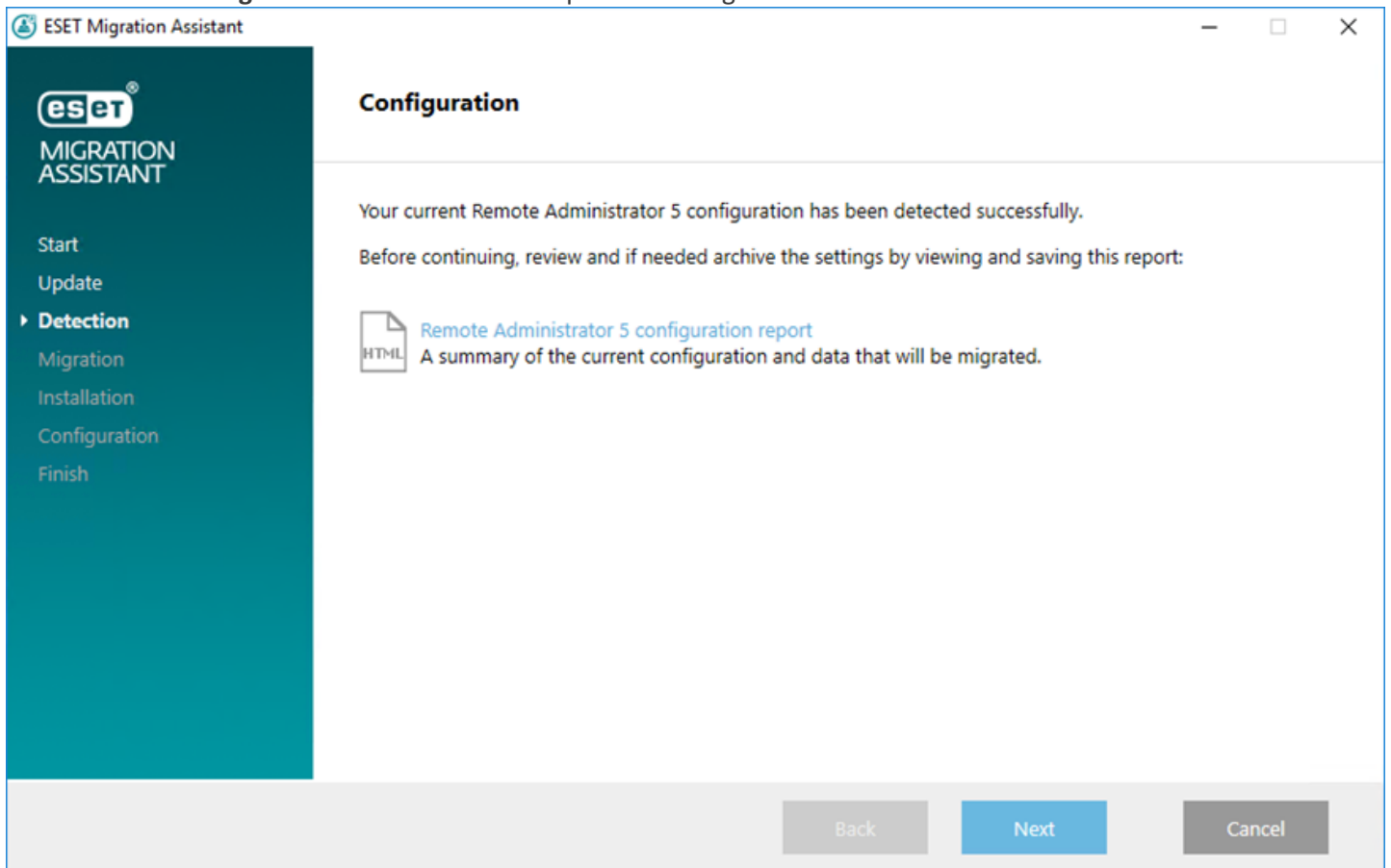
10. V sekcii **Detekcia** Asistent migrácie overuje konfiguráciu ERA Servera. Postupujte podľa krokov na obrazovke a držte sa odporúčaní uvedených v sprievodcovi nástroja Asistent migrácie.

**i Poznámka:**

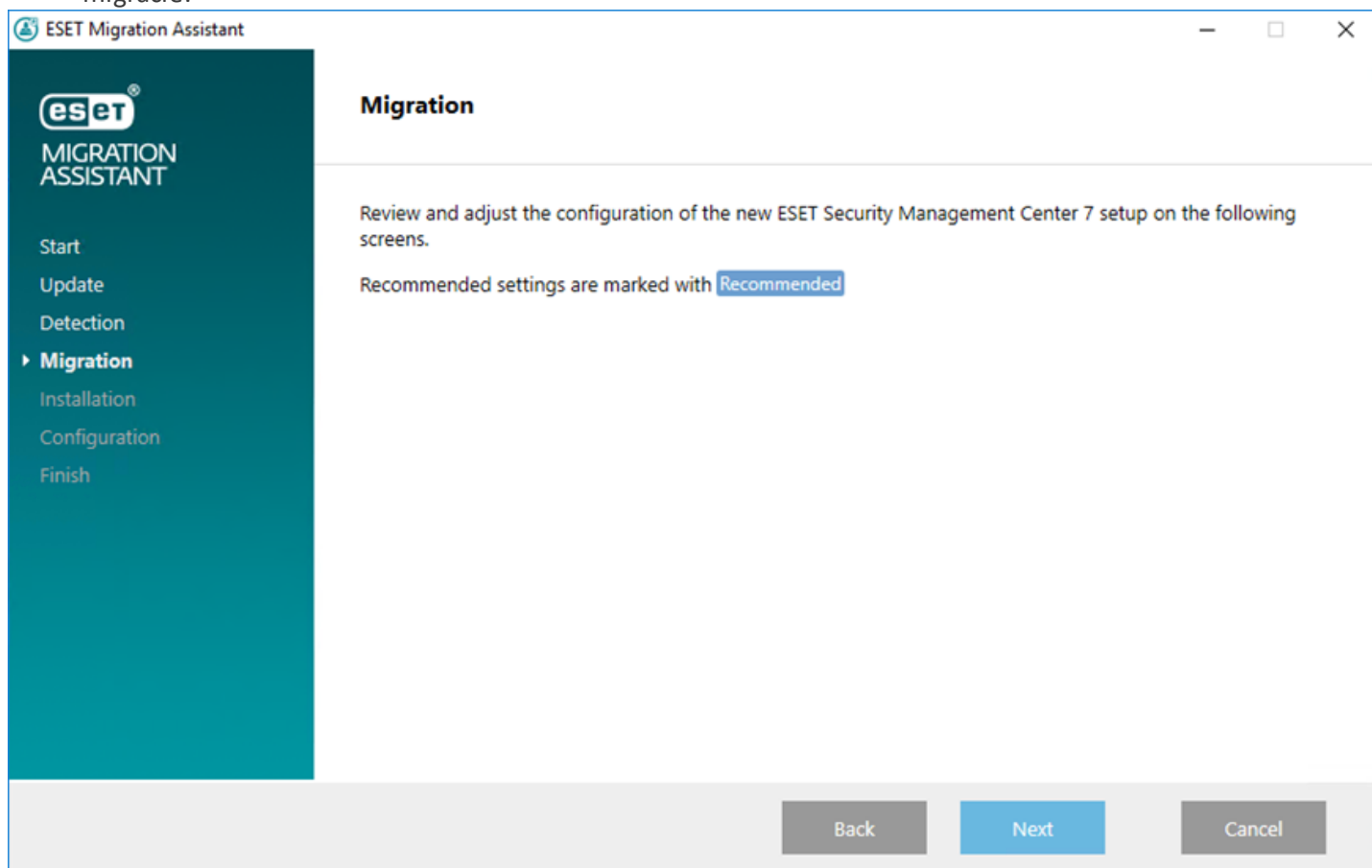
Asistent migrácie zastavuje službu ERA Server verzie 5.x. Ak sa rozhodnete zrušiť Asistenta migrácie, bude potrebné manuálne spustiť službu ERA Server.



11. V okne **Konfigurácia** si môžete stiahnuť správu o konfigurácii ERA 5.x vo formáte `html`.



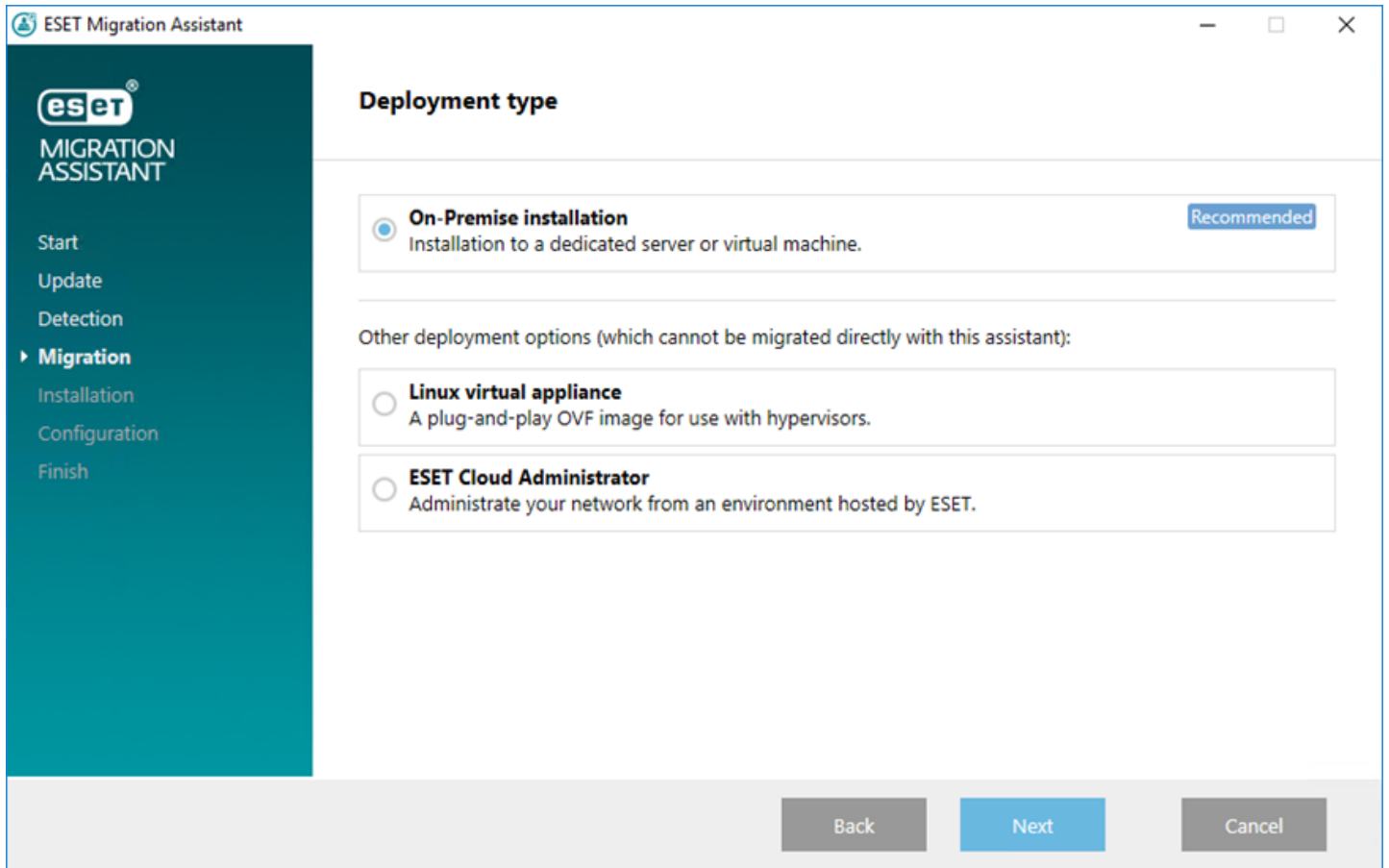
12. Skontrolujte a upravte konfiguráciu novej inštalácie ESMC. Môžete vychádzať z odporúčaní Asistenta migrácie.



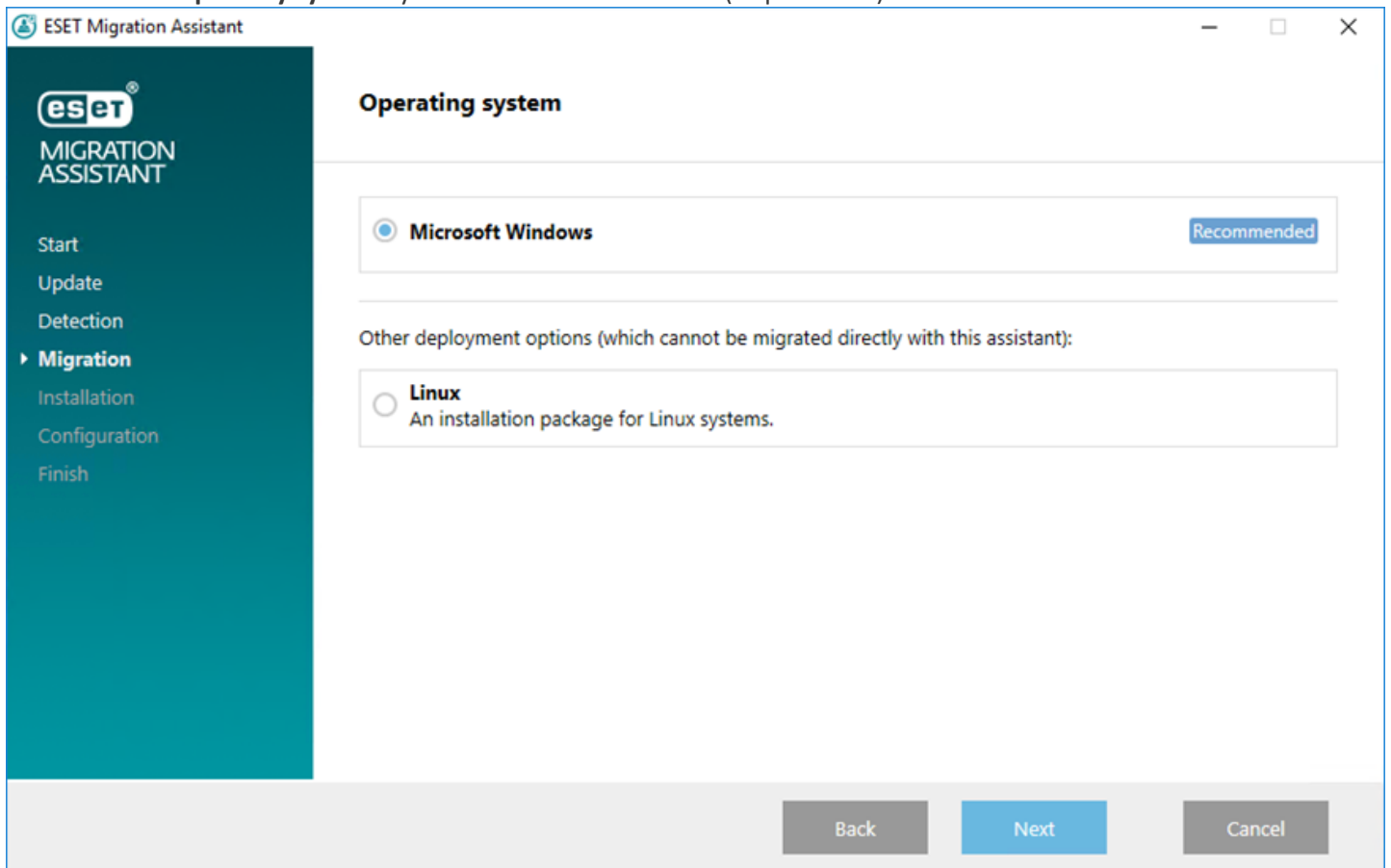
13. V okne Typ nasadenia vyberte možnosť **Lokálna inštalácia**.

**i Poznámka:**

Asistent migrácie podporuje iba migráciu na iný Windows server (fyzický alebo virtuálny). Asistent migrácie nepodporuje žiadne iné možnosti nasadenia.

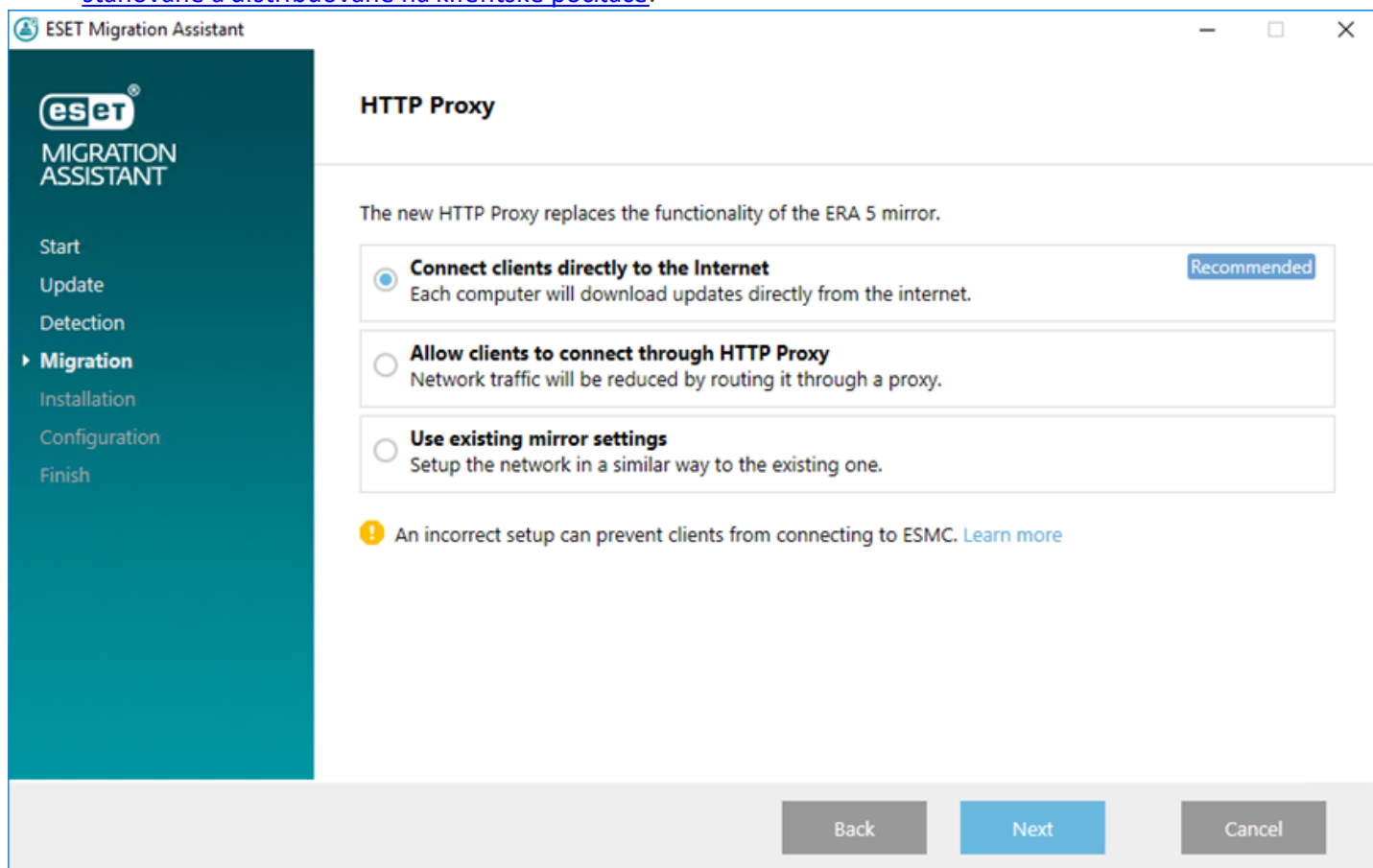


14. V okne **Operačný systém** vyberte **Microsoft Windows** (odporúčané).

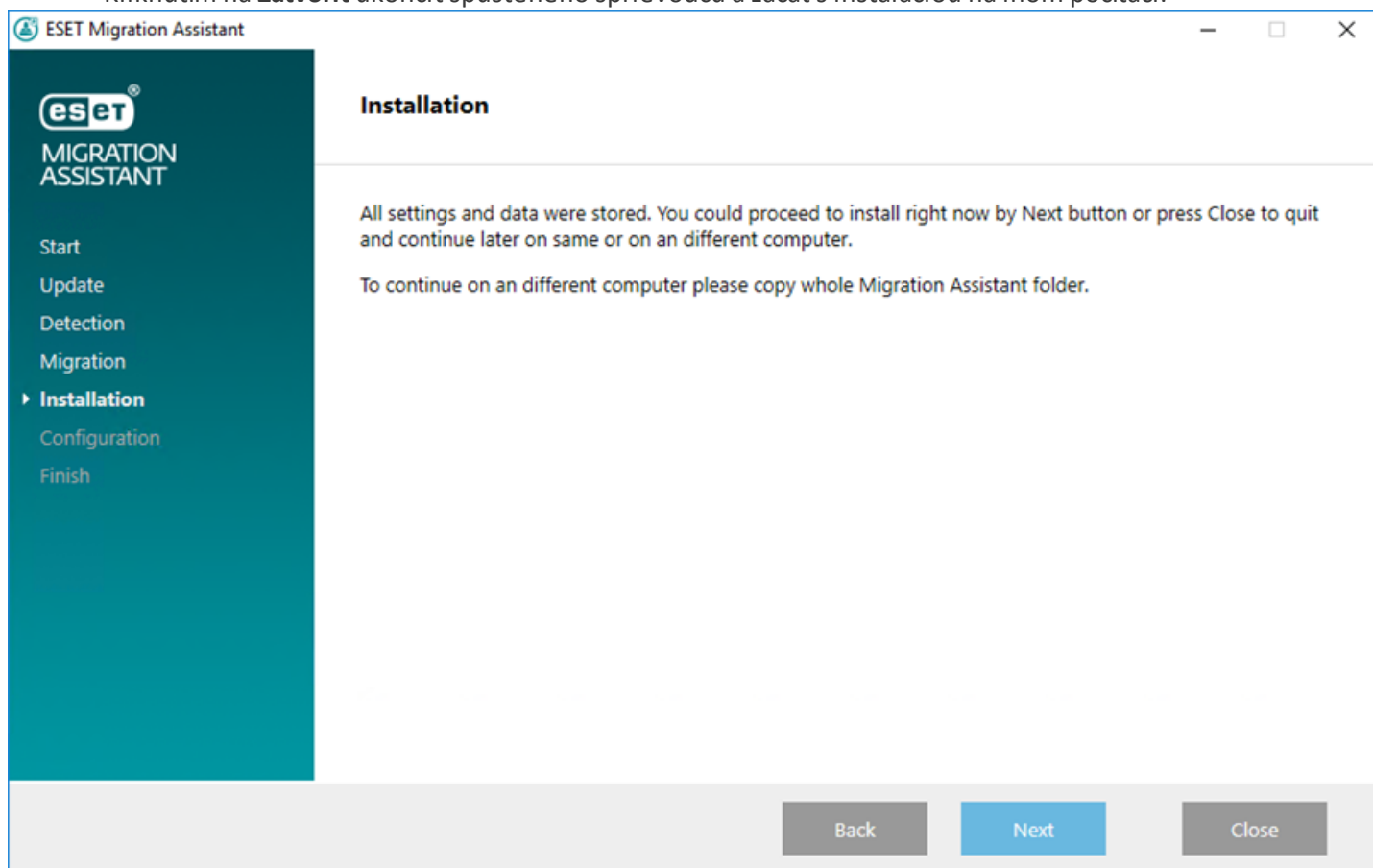




15. V okne **HTTP Proxy** výberom jednej z uvedených možností nastavíte [spôsob, akým budú aktualizácie sťahované a distribuované na klientske počítače](#).



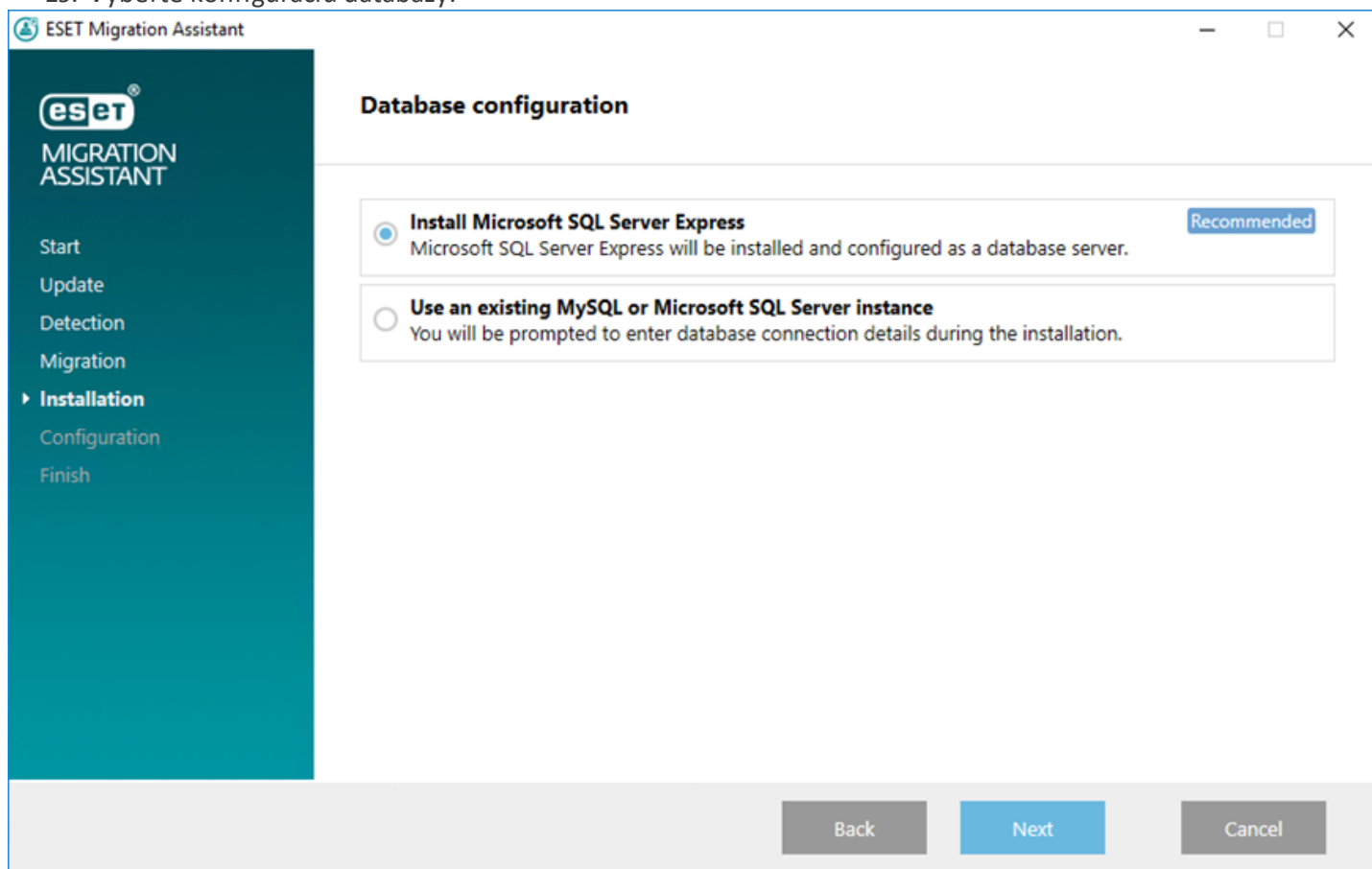
16. Označte začiarkavacie políčko vedľa licencií, ktoré chcete migrovať, a kliknite na **Ďalej**.
17. Označte začiarkavacie políčko vedľa všetkých politík, ktoré chcete migrovať, a kliknite na **Ďalej**.
18. Zobrazí sa okno Inštalácia. V tomto kroku sú k dispozícii dve možnosti:
  - Kliknutím na **Ďalej** začať s inštaláciou ESMC 7.0 na danom počítači.
  - Kliknutím na **Zatvoriť** ukončiť spusteného sprievodcu a začať s inštaláciou na inom počítači.



**i Poznámka:**

Ak chcete pokračovať s inštaláciou na inom počítači, kliknite na **Zatvoriť** a následne skopírujte celý priečinok *MigrationAssistant* na počítač, na ktorý chcete ESMC 7.0 nainštalovať. Pri spustení Asistenta migrácie na cieľovom počítači vyberte možnosť **Pokračovať s predchádzajúcou migráciou**.

## 19. Vyberte konfiguráciu databázy.



20. Sprievodca inštaláciou skontroluje, či sú splnené všetky požiadavky nevyhnutné pre inštaláciu ESMC 7.0.

21. Zadajte heslo pre ESMC Web Console a kliknite na **Ďalej**.

22. Počas inštalácie sa zobrazí okno ďalšieho sprievodcu, ktorý vás prevedie [nastavením ESMC Servera](#).

23. Po úspešnom nainštalovaní všetkých súčastí sa zobrazí správa „Migrácia bola úspešná“ spolu s URL adresou ESMC Web Console. Kliknite na URL adresu pre [otvorenie Web Console](#) alebo sprievodcu zatvorte kliknutím na **Dokončiť**.

## Ďalšie kroky

Po úspešnej migrácii nástroja ESET Remote Administrator je potrebné nasadiť ESET Management Agentu na klientske počítače vo vašej sieti. ESET Management Agentu odporúčame nasadiť jedným z nasledujúcich spôsobov:

- Použitím synchronizácie s Active Directory – synchronizácia s Active Directory sa vykoná po spustení úlohy pre server [Synchronizácia statickej skupiny](#).
- Použitím nástroja na nasadenie [ESET Remote Deployment tool](#) – tento nástroj vám umožňuje nasadiť all-in-one inštalačné balíky vytvorené cez ESMC Web Console.

Ďalšie metódy nasadenia ESET Management Agentu nájdete v [príručke správcu](#).

## Riešenie problémov

Počas migrácie sa v priečinku *MigrationAssistant* vytvorí nový priečinok s názvom *logs*. Tento priečinok obsahuje:

- *migration log* – zahŕňa informácie o procese migrácie.
- *migration\_report.html* – prehľad konfigurácie a dát, ktoré boli premigrované.

## 5.2.2 Nástroj na migráciu

Ak sa chcete dozvedieť, ktoré nastavenia je možné premigrovať pomocou Nástroja na migráciu, pozrite si toto [porovnanie](#) Asistenta migrácie a Nástroja na migráciu (Migration Tool).

### ! Dôležité:

Verzia nástroja na migráciu musí byť totožná s verziou ESMC, na ktorú sa chystáte migrovať. Pre zistenie potrebnej verzie nástroja na migráciu si pozrite nasledujúci [článok databázy znalostí](#).

### ⚠ Upozornenie:

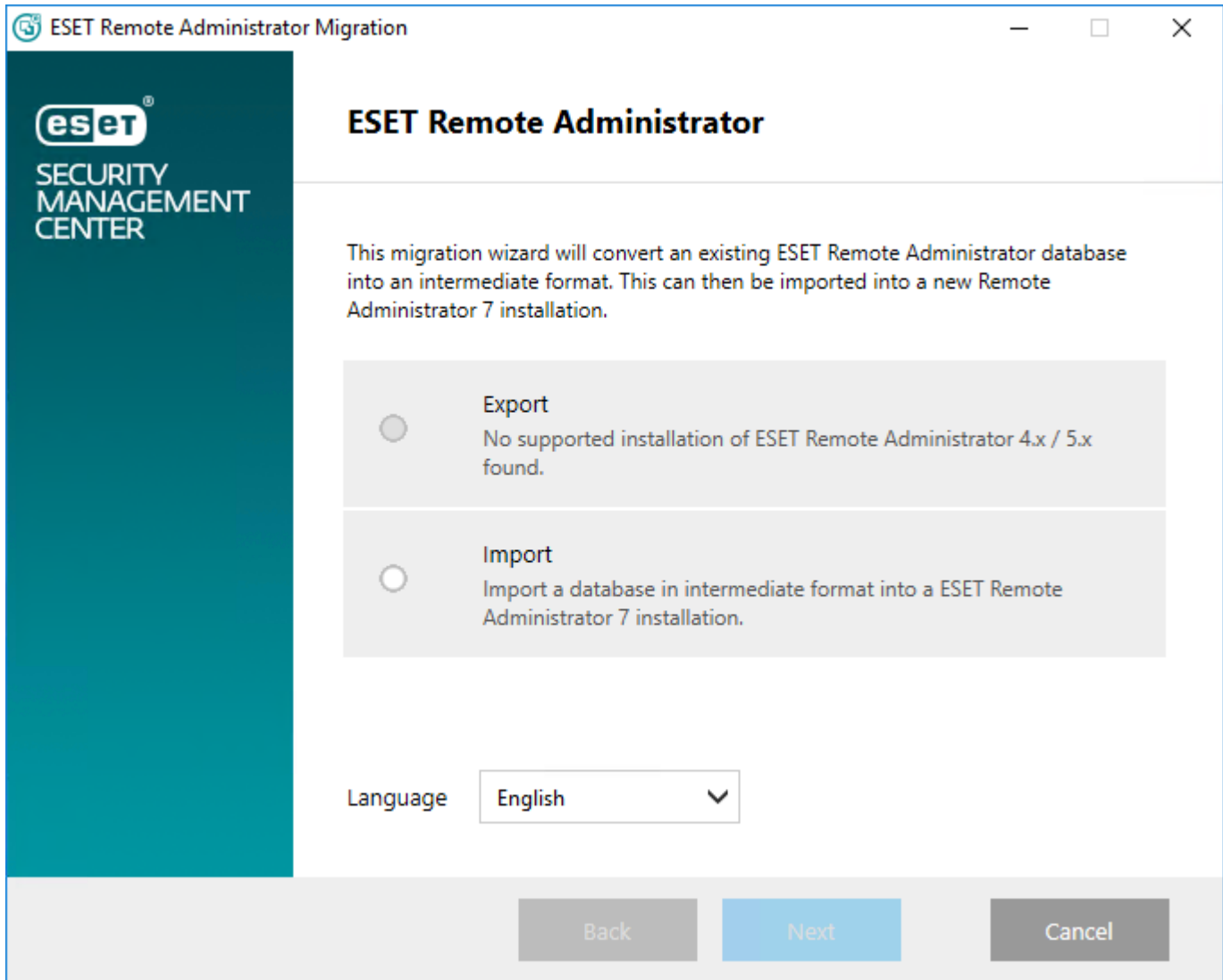
Ak sa ESET Management Agent verzie 7.x nainštaluje na klientsky počítač používajúci produkt pre koncové zariadenie verzie 5.x alebo staršej, nastavenie vzdialenej správy sa pre daného klienta automaticky zmení na `localhost / 2225`. V dôsledku toho sa po nainštalovaní agenta daný klient už nedokáže pripojiť k vášmu nástroju ERA 5.x.

Stiahnite si a spustite nástroj [ESET Remote Administrator Migration Tool](#).

- Nainštalujte si balík Microsoft Visual C++ 2015 x86, ktorý je nevyhnutný pre správne fungovanie nástroja na migráciu. Tento balík je súčasťou .zip súboru, ktorý obsahuje inštalátor pre samotný nástroj na migráciu.
- Spustite nástroj na migráciu ako správca lokálne na starom ERA Serveri verzie 5.x. Nástroj na migráciu nie je možné spustiť zo vzdialeného zariadenia.

### i Poznámka:

- Po migrácii odporúčame skontrolovať všetky položky (počítače, statické skupiny, politiky atď.) a uistiť sa, že migrácia prebehla podľa očakávania. Ak spozorujete nezrovnalosti, pravdepodobne bude potrebné pridať požadované položky manuálne.
- Ak sa pri migrácii vyskytne chyba, bude zapísaná v protokole `migration.log`, ktorý sa nachádza v rovnakom súbore ako nástroj na migráciu. Ak máte do tohto priečinka iba prístup na čítanie, otvorí sa len okno s protokolom. Podobne je to v prípade, keď nie je na disku dostatok miesta. Znamená to, že sa nevytvorí súbor protokolu, ale výsledok uvidíte len v okne protokolu.



Nasledujú migračné scenáre, ktoré vám pomôžu so samotným procesom migrácie:

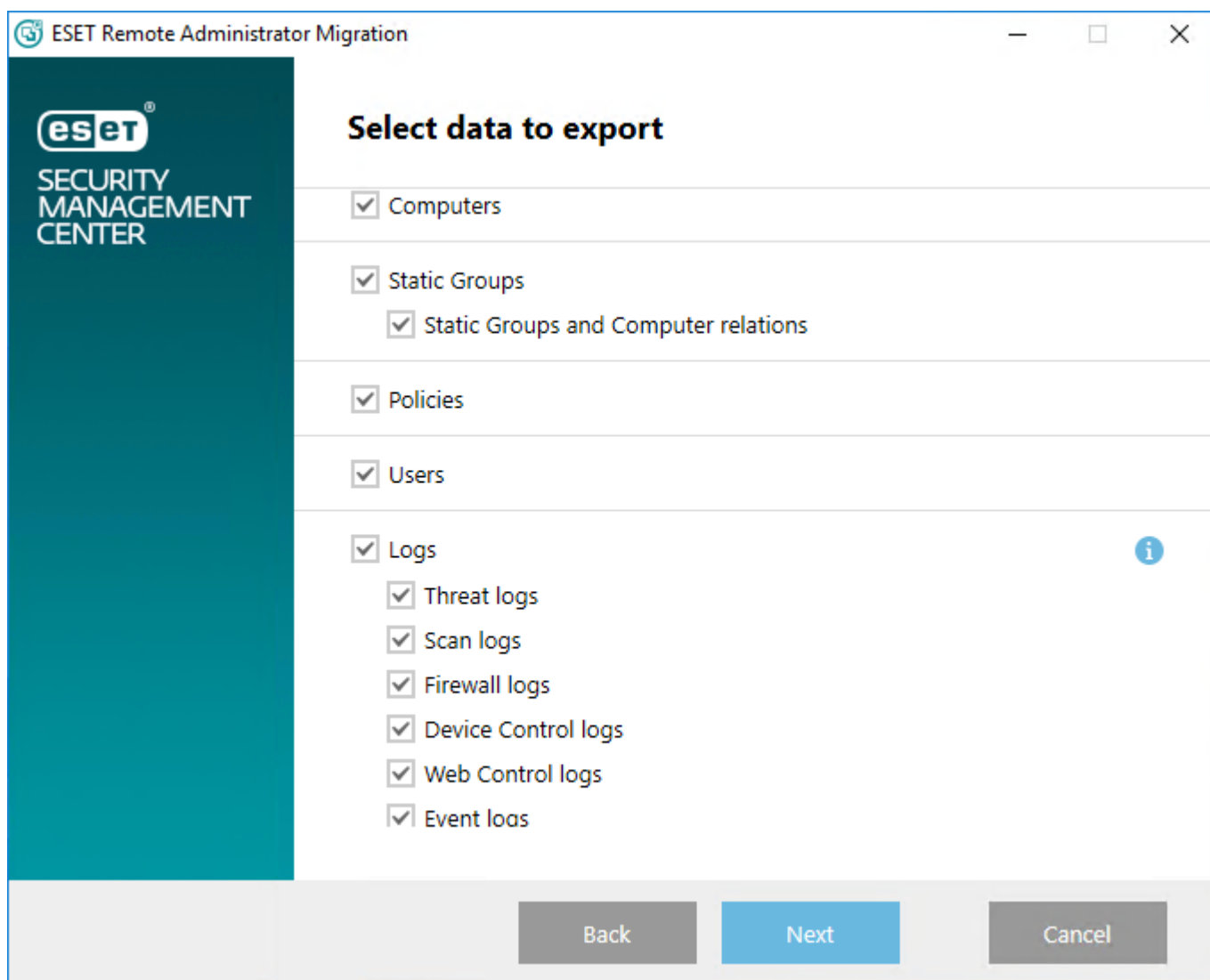
- [Scenár migrácie 1](#) – migrácia na ESMC 7.x bežiaci na inom počítači ako ERA 5.x.
- [Scenár migrácie 2](#) – migrácia na ESMC 7.x bežiaci na rovnakom počítači ako ERA 5.x.
- [Scenár migrácie 3](#) – migrácia na ESMC 7.x, kde sa koncové počítače ďalej pripájajú na starý ERA 5.x, až kým na ne nie je nasadený ESET Management Agent nástrojom ESMC 7.x.

### 5.2.2.1 Scenár migrácie 1

Tento scenár pokrýva migráciu na ESMC 7.x bežiaci na inom počítači ako ERA 5.x. Pre podrobné inštrukcie týkajúce sa inštalácie pomocou all-in-one inštalátora si môžete prečítať náš [článok databázy znalostí](#).

1. Uistite sa, že máte nástroj ESMC 7.x nainštalovaný a bežiaci na inom počítači.
2. Stiahnite si a spustite nástroj [ESET Remote Administrator Migration Tool](#).
  - Nainštalujte si balík Microsoft Visual C++ 2015 x86, ktorý je nevyhnutný pre správne fungovanie nástroja na migráciu. Tento balík je súčasťou .zip súboru, ktorý obsahuje inštalátor pre samotný nástroj na migráciu.
  - Spustite nástroj na migráciu ako správca lokálne na starom ERA Serveri verzii 5.x. Nástroj na migráciu nie je možné spustiť zo vzdialeného zariadenia.
3. Vyberte možnosť **Export** pre uloženie dát z ERA 5.x do prechodného databázového súboru.

4. Sprievodca migráciou dokáže preniesť len špecifické dáta. Vyberte dáta, ktoré chcete preniesť a kliknite na **Ďalej**.



Po vybraní adresára pre uloženie dočasnej databázy s dátami zobrazí sprievodca priebeh a stav načítavania informácií z databázy ERA 5.x.

Všetky dáta sú exportované do **prechodnej databázy**.

5. Po dokončení exportu dát si môžete vybrať jednu z dvoch možností:

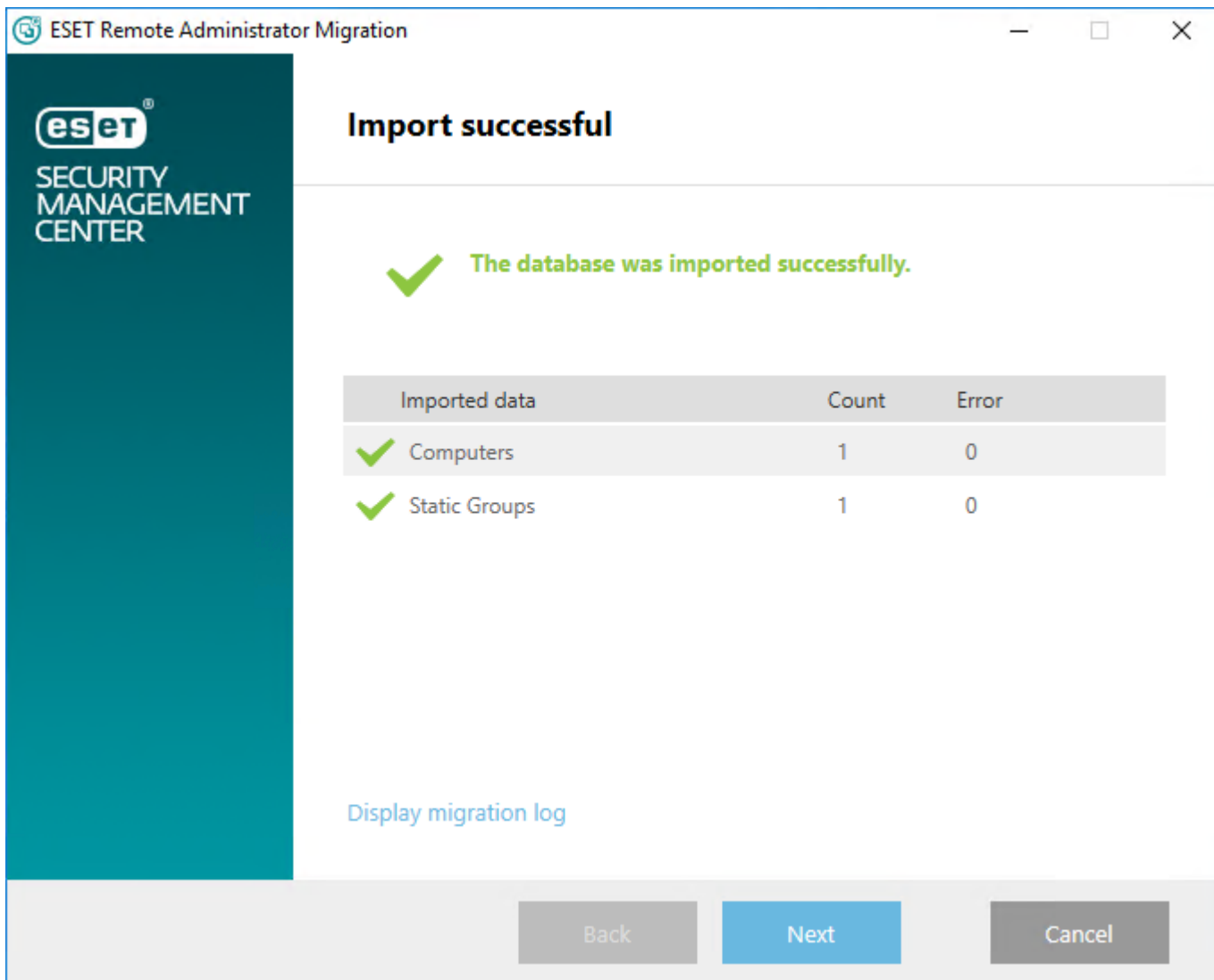
- Kliknúť na **Dokončiť** pre dokončenie exportu, **skopírovať** súbor prechodnej databázy na server, kde beží ESET Security Management Center 7.x, a následne importovať dáta pomocou nástroja na migráciu (Migration Tool).
- Použiť možnosť **Importovať teraz** a importovať dáta priamo do nástroja ESET Security Management Center 7.x prostredníctvom siete. Následne je potrebné zadať údaje o pripojení a prihlasovacie údaje pre nový ESMC Server.

**i Poznámka:**

Statické skupiny synchronizované z Active Directory sú ignorované a nebudú exportované.

6. Ak nastavenia servera nedovoľujú importovanie vybraných údajov, nástroj na migráciu Migration Tool vám umožní zmenu nastavení ESMC 7 pre vybrané komponenty.

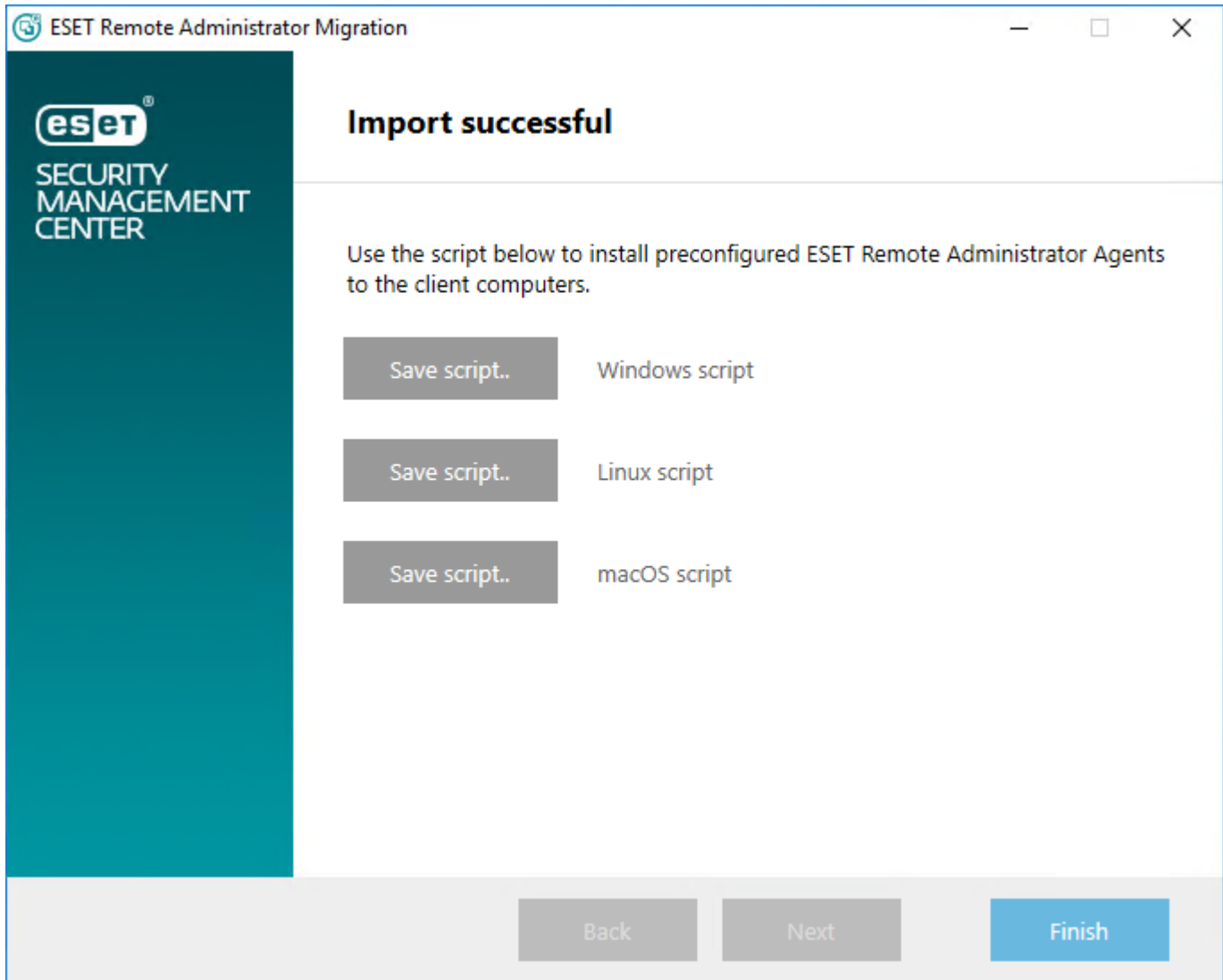
Každý komponent je potom importovaný. Pre každý komponent je dostupný **Protokol migrácie**. Po ukončení importu nástroj Migration tool zobrazí dialógové okno s výsledkom procesu importovania.



**! Dôležité:**

V prípade, že ste sa rozhodli migrovať používateľov, ich heslá boli vynulované a nahradené náhodne vygenerovanými heslami. Tieto vygenerované heslá budú dostupné na exportovanie vo formáte .CSV.

7. Nástroj na migráciu (Migration Tool) môžete použiť na vygenerovanie skriptu, ktorý umožňuje prednastaviť ESET Management Agency na klientských počítačoch. Tento skript je malý spustiteľný .bat súbor, distribuovateľný na klientske počítače.



Odporúčame skontrolovať migrované nastavenia a dáta a overiť si, či import prebehol úspešne. Potom môžete použiť skript na nasadenie ESET Management Agentov najprv na menšiu skupinu počítačov, aby ste sa uistili, že sa pripájajú na server správne.

Po úspešnom pripojení testovacej skupiny môžete nasadiť agenta na ostatné počítače v sieti (manuálne alebo použiť AD synchronizačnú úlohu na pridanie počítačov vo Web Console a následné nasadenie agenta).

**i Poznámka:**

Ak zlyhá niektorý z krokov migrácie, mali by ste vrátiť zmeny vykonané pre ESMC 7.x, pripojiť počítače späť na ERA 5.x, obnoviť zálohy dát z verzie ERA 5.x a kontaktovať technickú podporu spoločnosti ESET.

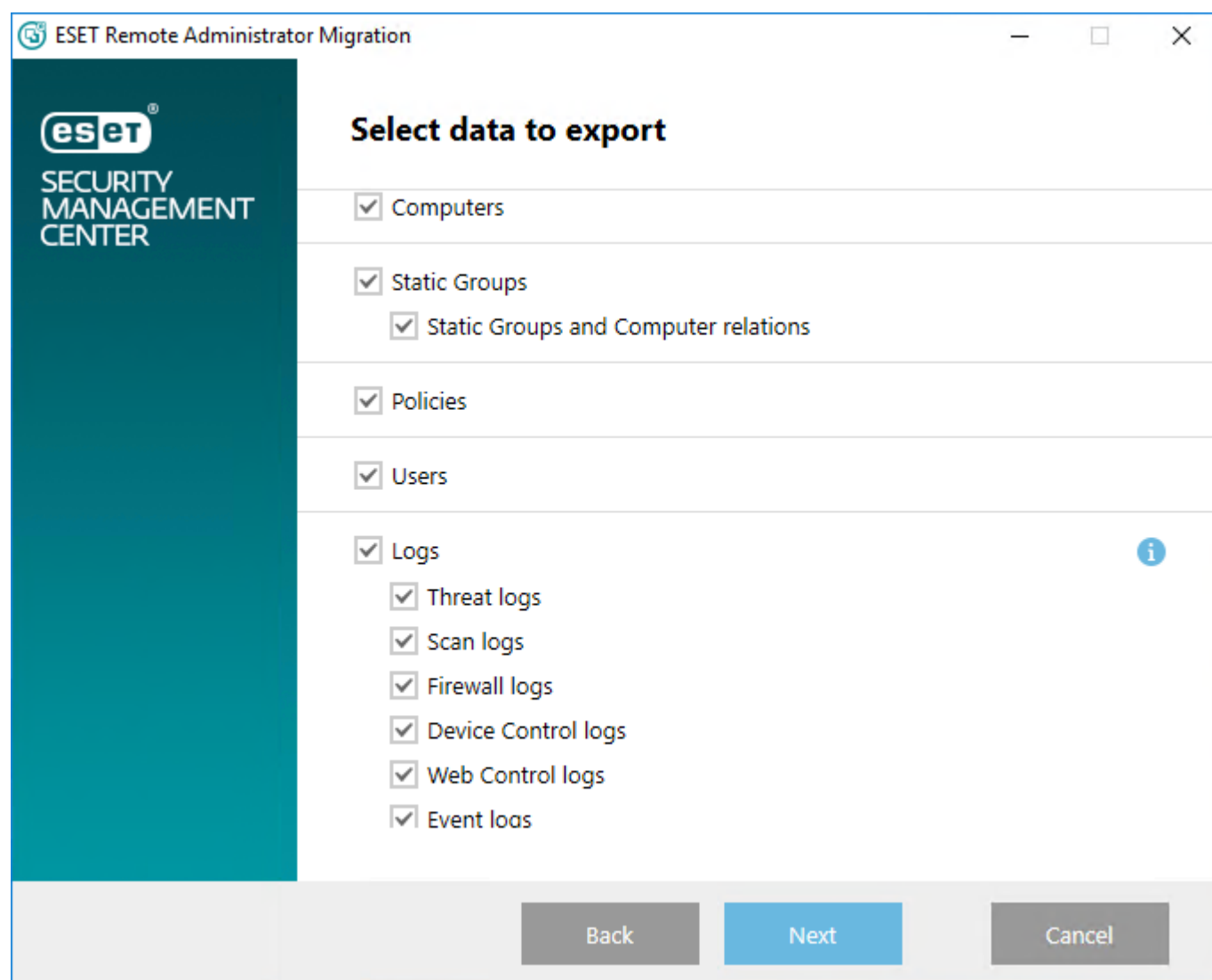


### 5.2.2.2 Scenár migrácie 2

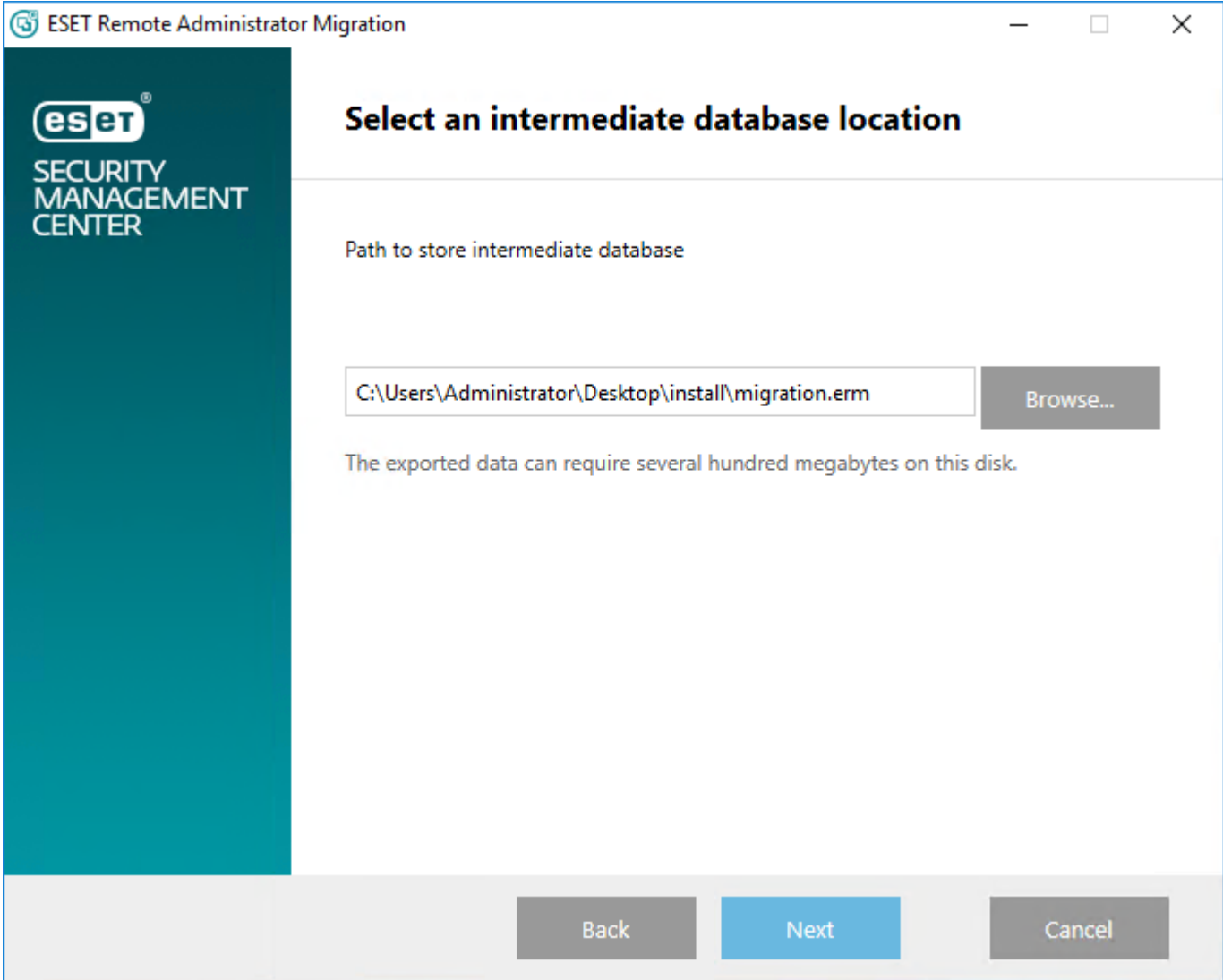
Tento scenár pokrýva migráciu na ESET Security Management Center 7.x bežiaci na rovnakom počítači ako ERA 5.x. Všetky ERA dáta musia byť zálohované (pomocou nástroja [ESET Maintenance tool](#)) a systémové služby ERA musia byť pred migráciou dát zastavené.

Pre podrobné inštrukcie týkajúce sa inštalácie pomocou all-in-one inštalátora si môžete pozrieť naše [video databázy znalostí](#) alebo náš [článok databázy znalostí](#).

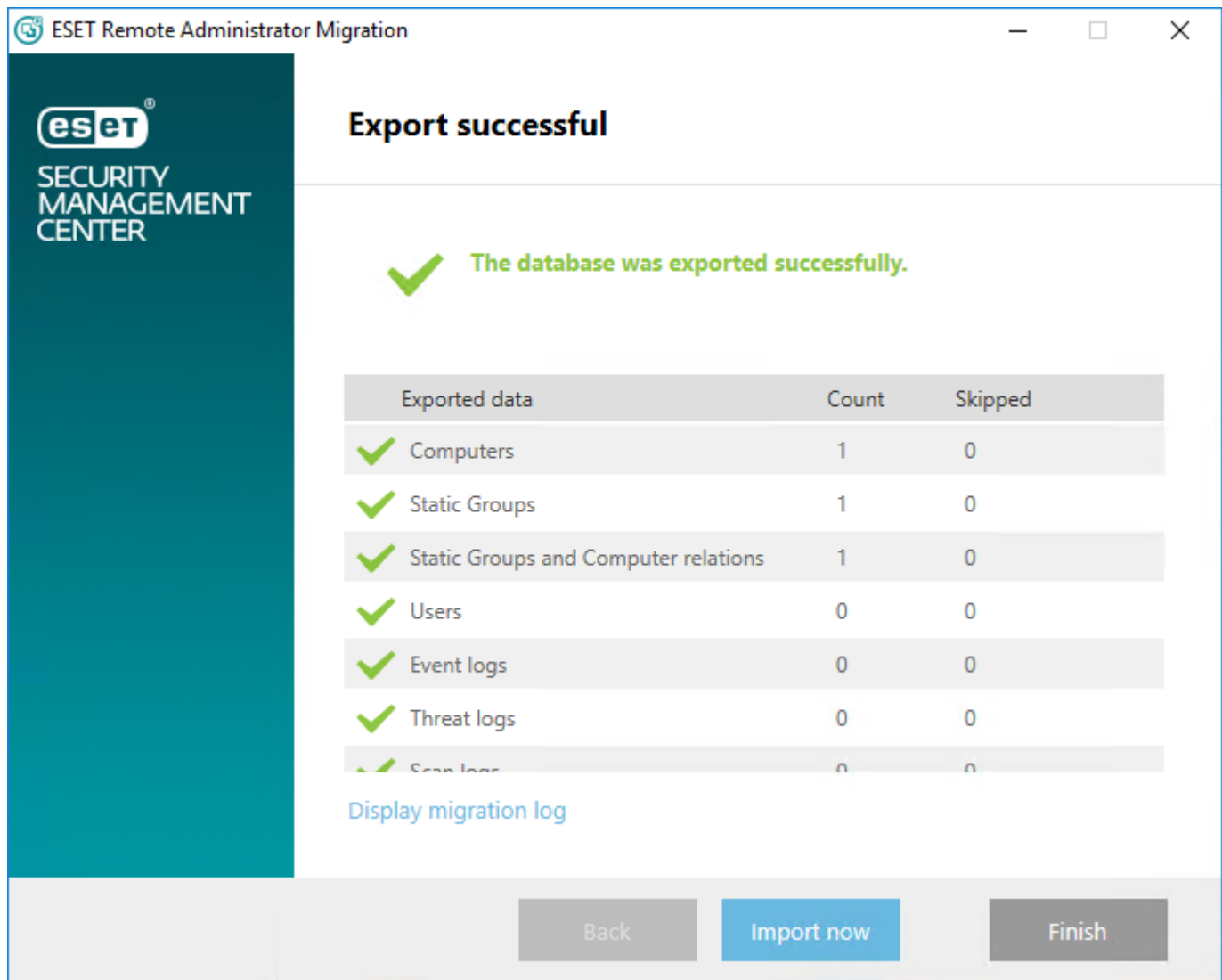
1. Stiahnite si a spustite nástroj [ESET Remote Administrator Migration Tool](#).
  - Nainštalujte si balík Microsoft Visual C++ 2015 x86, ktorý je nevyhnutný pre správne fungovanie nástroja na migráciu. Tento balík je súčasťou .zip súboru, ktorý obsahuje inštalátor pre samotný nástroj na migráciu.
  - Spustite nástroj na migráciu ako správca lokálne na starom ERA Serveri verzii 5.x. Nástroj na migráciu nie je možné spustiť zo vzdialeného zariadenia.
2. Vyberte možnosť **Export** pre uloženie dát z ERA 5.x do prechodného databázového súboru. Sprievodca migráciou dokáže preniesť len špecifické dáta:



3. Vyberte priečinok, kde bude uložená prechodná databáza.



4. Sprievodca zobrazí priebeh a stav načítavania informácií z databázy ERA 5.x.



The screenshot shows the 'ESET Remote Administrator Migration' window. The title bar includes the ESET logo and window controls. The main content area displays the ESET Security Management Center logo on the left and a large green checkmark with the text 'Export successful' and 'The database was exported successfully.' Below this is a table with three columns: 'Exported data', 'Count', and 'Skipped'. The table lists several data types, all with a count of 1 or 0 and 0 skipped. At the bottom of the window, there are three buttons: 'Back', 'Import now', and 'Finish'.

| Exported data                          | Count | Skipped |
|----------------------------------------|-------|---------|
| ✓ Computers                            | 1     | 0       |
| ✓ Static Groups                        | 1     | 0       |
| ✓ Static Groups and Computer relations | 1     | 0       |
| ✓ Users                                | 0     | 0       |
| ✓ Event logs                           | 0     | 0       |
| ✓ Threat logs                          | 0     | 0       |
| ✓ Scan logs                            | 0     | 0       |

5. Všetky dáta sú exportované do **prechodnej databázy**.

**! Dôležité:**

Po úspešnom exportovaní dát a pred nasadením ESMC 7.x musí byť nástroj ERA 5.x odinštalovaný. Odporúčame reštartovať počítač pred pokračovaním v inštalácii ESMC 7.x.

6. Po nainštalovaní ESMC 7.x importujte exportovanú databázu zo starších produktov pomocou nástroja na migráciu. Správca bude vyzvaný, aby zadal IP adresu počítača (tú, ktorá sa zobrazila pre ESMC Console po úspešnej inštalácii) do poľa **Hostiteľ**, heslo správcu nastavené počas inštalácie a takisto bude potrebné zvoliť uložený databázový súbor.

ESET Remote Administrator Migration


**eset**  
SECURITY  
MANAGEMENT  
CENTER

## Select new Remote Administrator 7.x

Network connection to ESET Remote Administrator 7

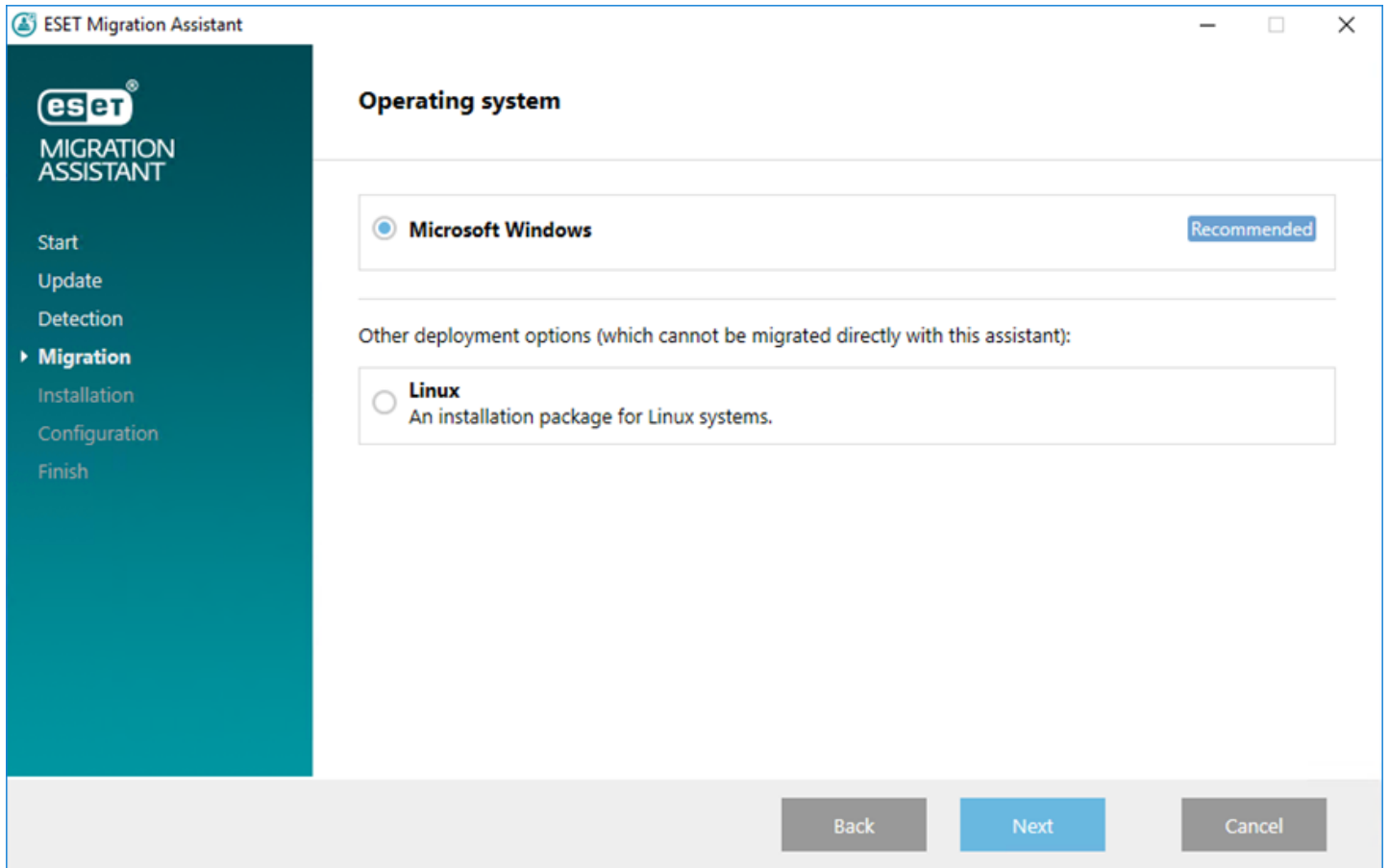
Host

Port

Administrator username  

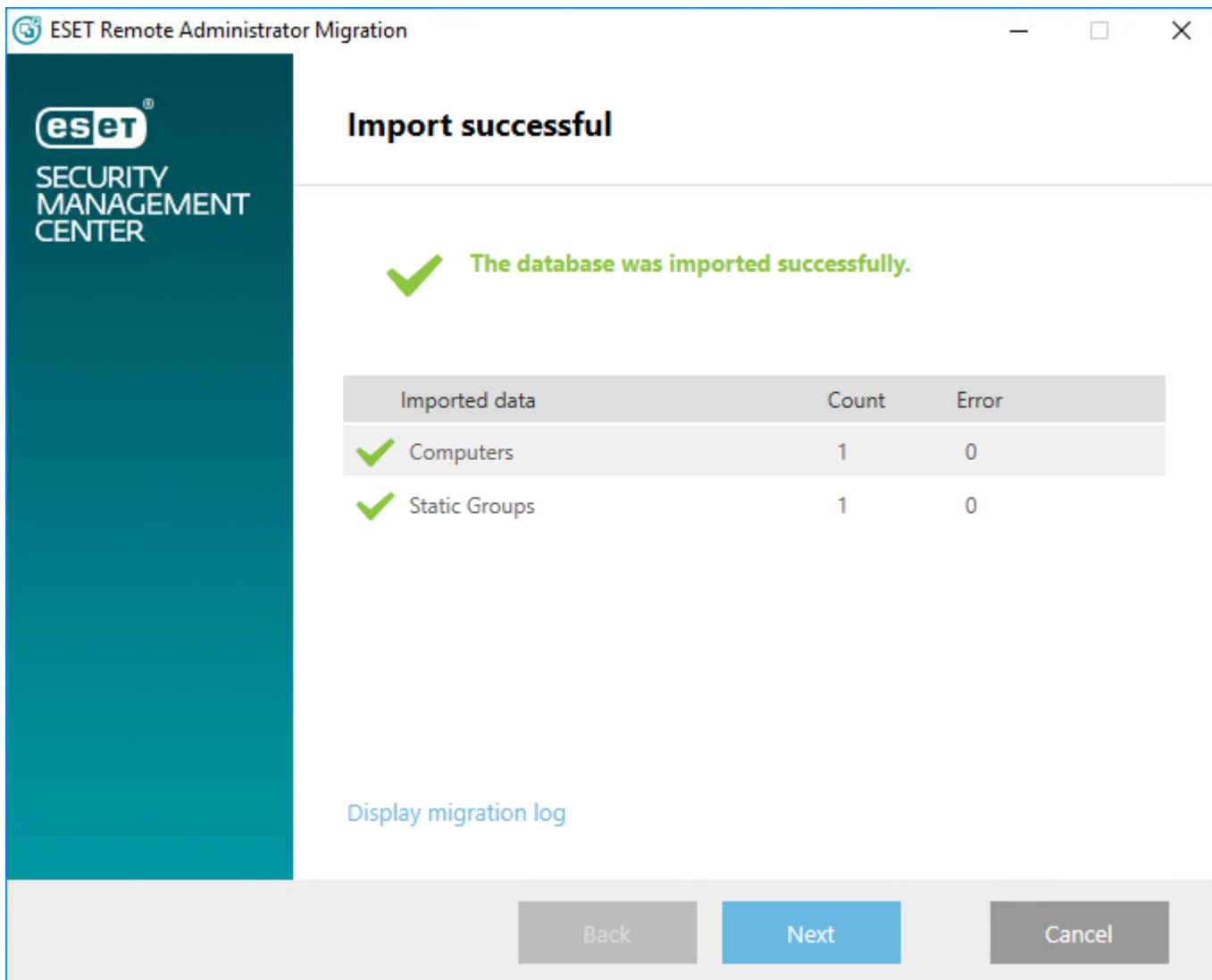
Password

7. Zvolte uložený databázový súbor.



8. Ak nastavenia servera nedovoľujú importovanie vybraných údajov, nástroj na migráciu Migration Tool vám umožní zmenu nastavení ESMC 7 pre vybrané komponenty.

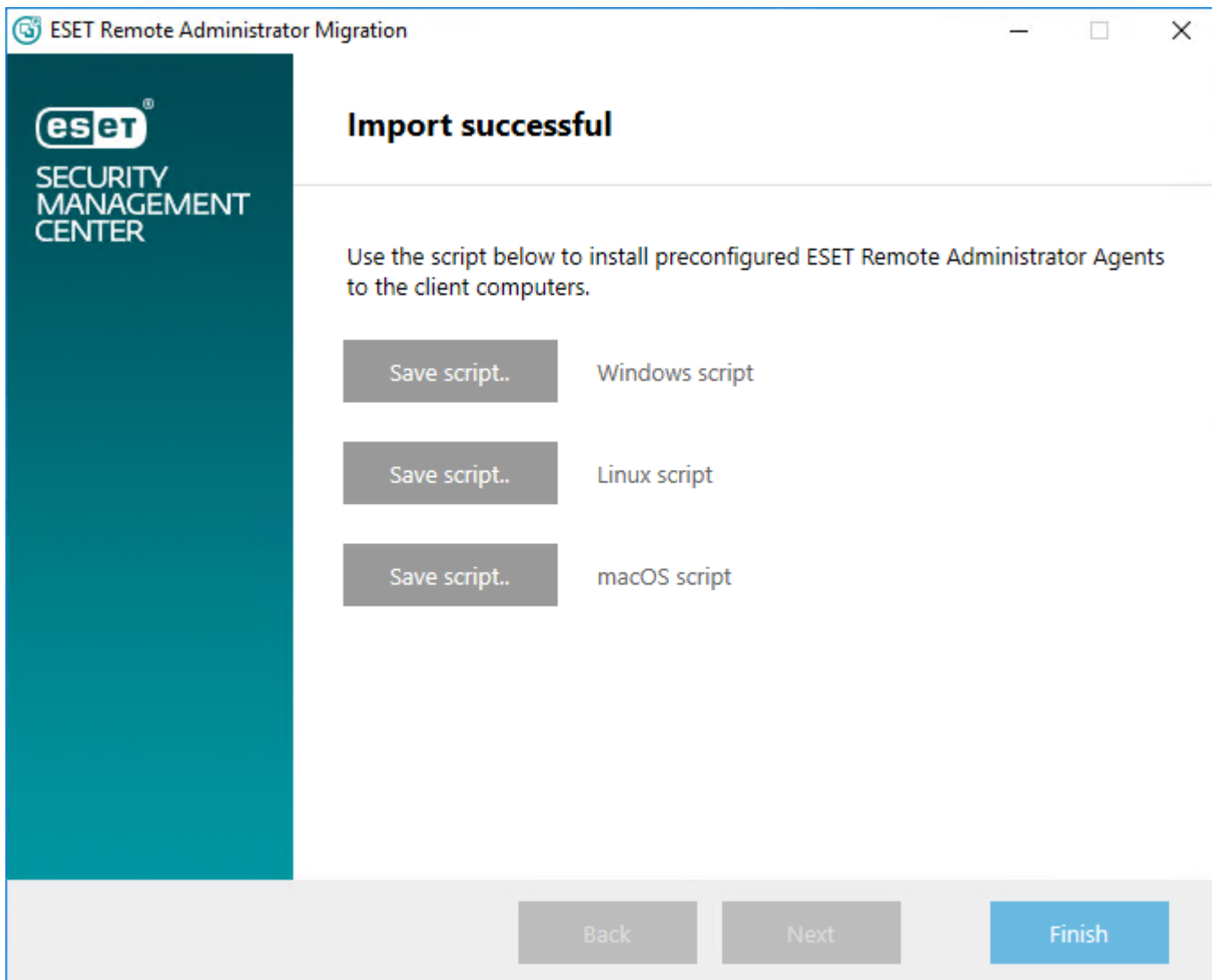
Každý komponent je potom importovaný. Pre každý komponent je dostupný **Protokol migrácie**. Po ukončení importu nástroj Migration tool zobrazí dialógové okno s výsledkom procesu importovania.



**! Dôležité:**

V prípade, že ste sa rozhodli migrovať používateľov, ich heslá boli vynulované a nahradené náhodne vygenerovanými heslami. Tieto vygenerované heslá budú dostupné na exportovanie vo formáte .CSV.

- Nástroj na migráciu (Migration Tool) môžete použiť na vygenerovanie skriptu, ktorý umožňuje prednastaviť ESET Management Agenty na klientských počítačoch. Tento skript je malý spustiteľný .bat súbor, distribuovateľný na klientske počítače.



Odporúčame skontrolovať migrované nastavenia a dáta a overiť si, či import prebehol úspešne. Potom môžete použiť skript na nasadenie ESET Management Agentov najprv na menšiu skupinu počítačov, aby ste sa uistili, že sa pripájajú na server správne.

Po úspešnom pripojení testovacej skupiny môžete nasadiť agenta na ostatné počítače v sieti (manuálne alebo použiť AD synchronizačnú úlohu na pridanie počítačov vo Web Console a následné nasadenie agenta).

**i Poznámka:**

Ak zlyhá niektorý z krokov migrácie, mali by ste vrátiť zmeny vykonané pre ESMC 7.x, pripojiť počítače späť na ERA 5.x, obnoviť zálohy dát z verzie ERA 5.x a kontaktovať technickú podporu spoločnosti ESET.

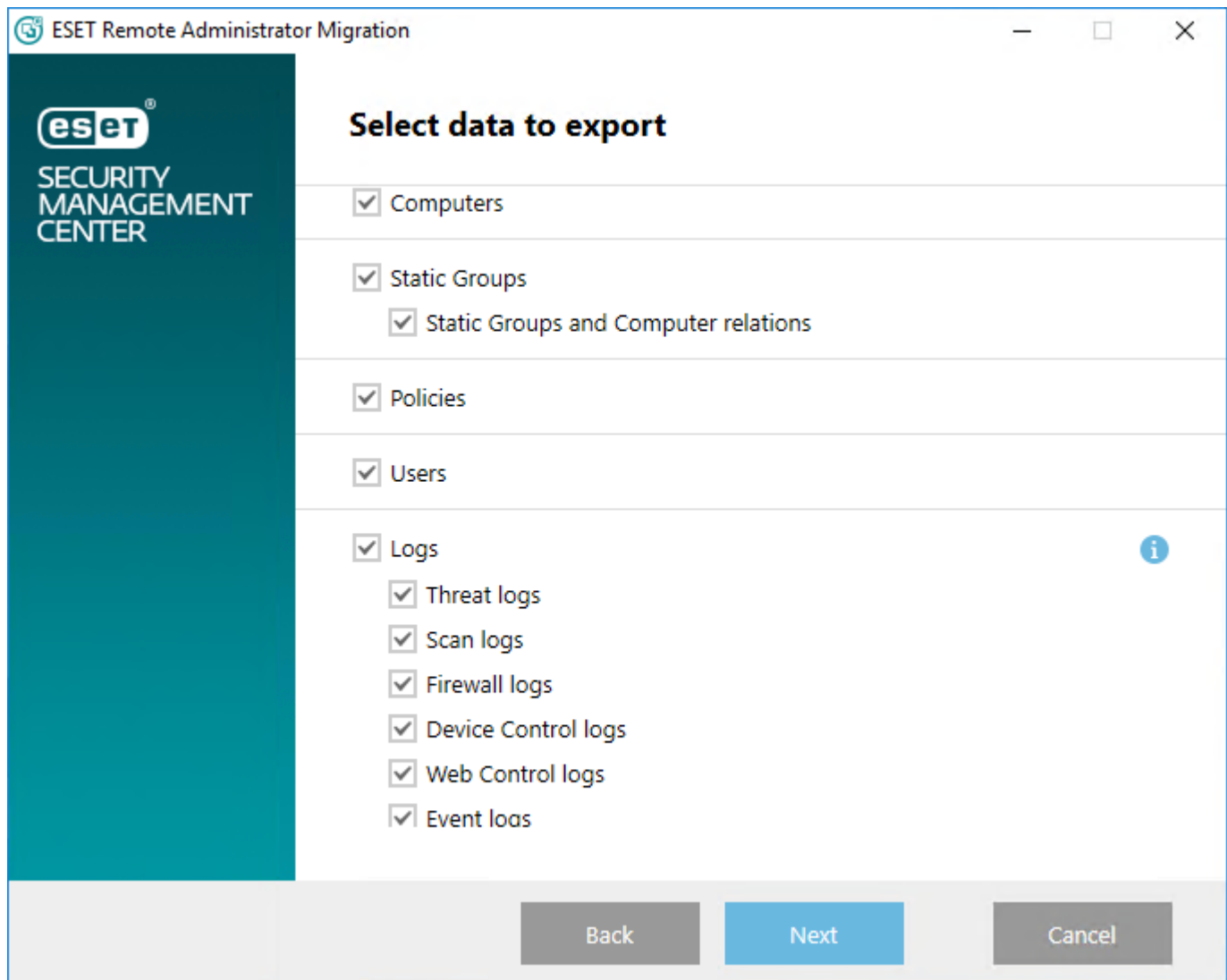
### 5.2.2.3 Scenár migrácie 3

Tento scenár pokrýva migráciu na ESMC 7.x, kde sa koncové počítače ďalej pripájajú na starý ERA 5.x, až kým na ne nie je nasadený ESET Management Agent nástrojom ESMC 7.x. Tento scenár môže pomôcť v prípade, že chcete zistiť, aké by bolo mať ESMC 7.x s dátami z ERA 5.x, pričom vaše koncové počítače by sa ešte stále pripájali na ERA 5.x.

#### **i** Poznámka:

Tento scenár je určený pre pokročilých používateľov. Neodporúčame používať tento typ migrácie, pokiaľ je iná možnosť.

1. Stiahnite si a spustite nástroj [ESET Remote Administrator Migration Tool](#).
  - Nainštalujte si balík Microsoft Visual C++ 2015 x86, ktorý je nevyhnutný pre správne fungovanie nástroja na migráciu. Tento balík je súčasťou .zip súboru, ktorý obsahuje inštalátor pre samotný nástroj na migráciu.
  - Spustite nástroj na migráciu ako správca lokálne na starom ERA Serveri verzii 5.x. Nástroj na migráciu nie je možné spustiť zo vzdialeného zariadenia.
2. Vyberte možnosť **Export** pre uloženie dát z ERA 5.x do prechodného databázového súboru. Sprievodca migráciou dokáže preniesť len špecifické dáta:



3. Vyberte priečinok, kde bude uložená prechodná databáza.





## Select an intermediate database location

Path to store intermediate database

C:\Users\Administrator\Desktop\install\migration.erm

Browse...

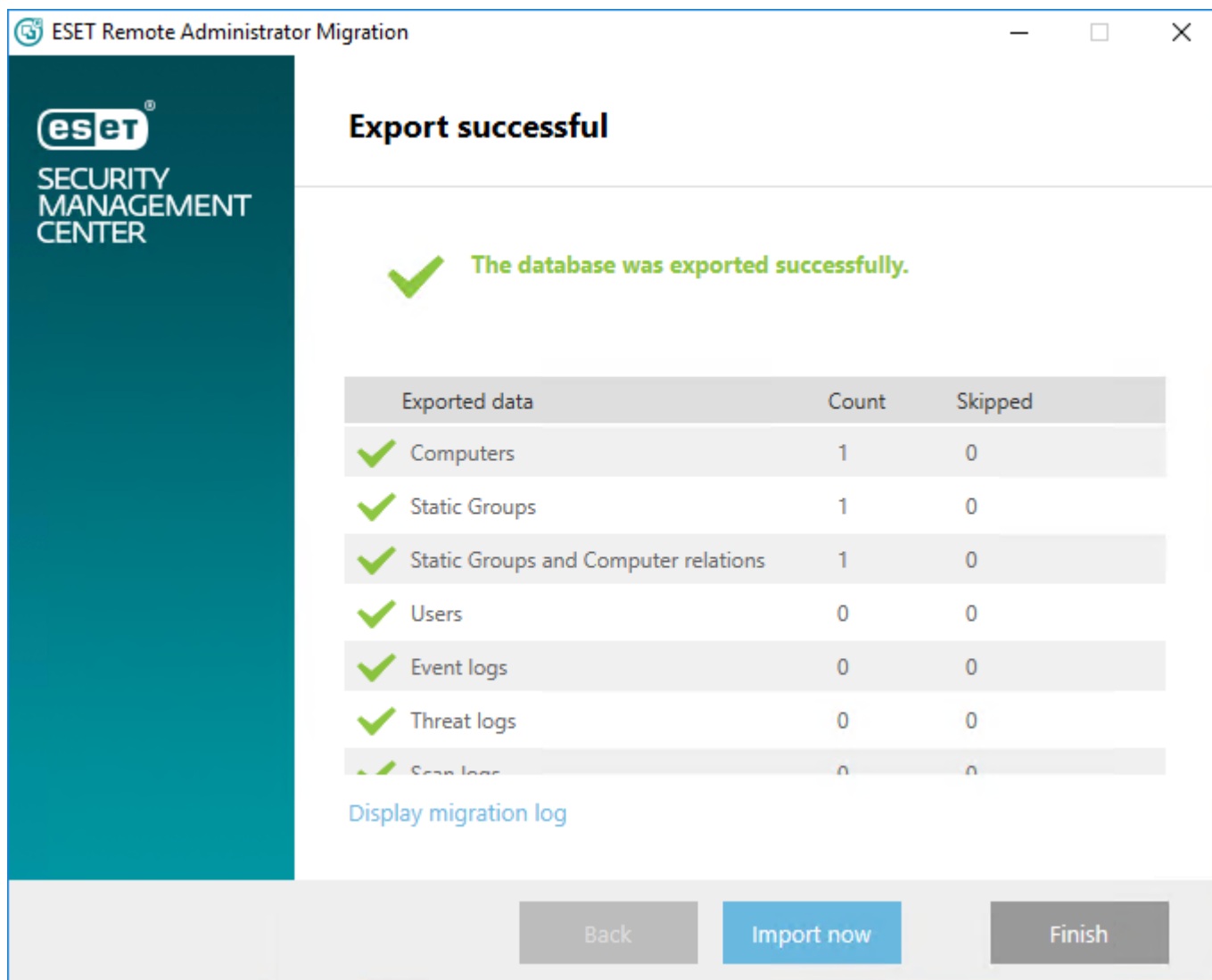
The exported data can require several hundred megabytes on this disk.

Back

Next

Cancel

4. Sprievodca zobrazí priebeh a stav načítavania informácií z databázy ERA 5.x.



5. Všetky dáta sú exportované do **prechodnej databázy**.

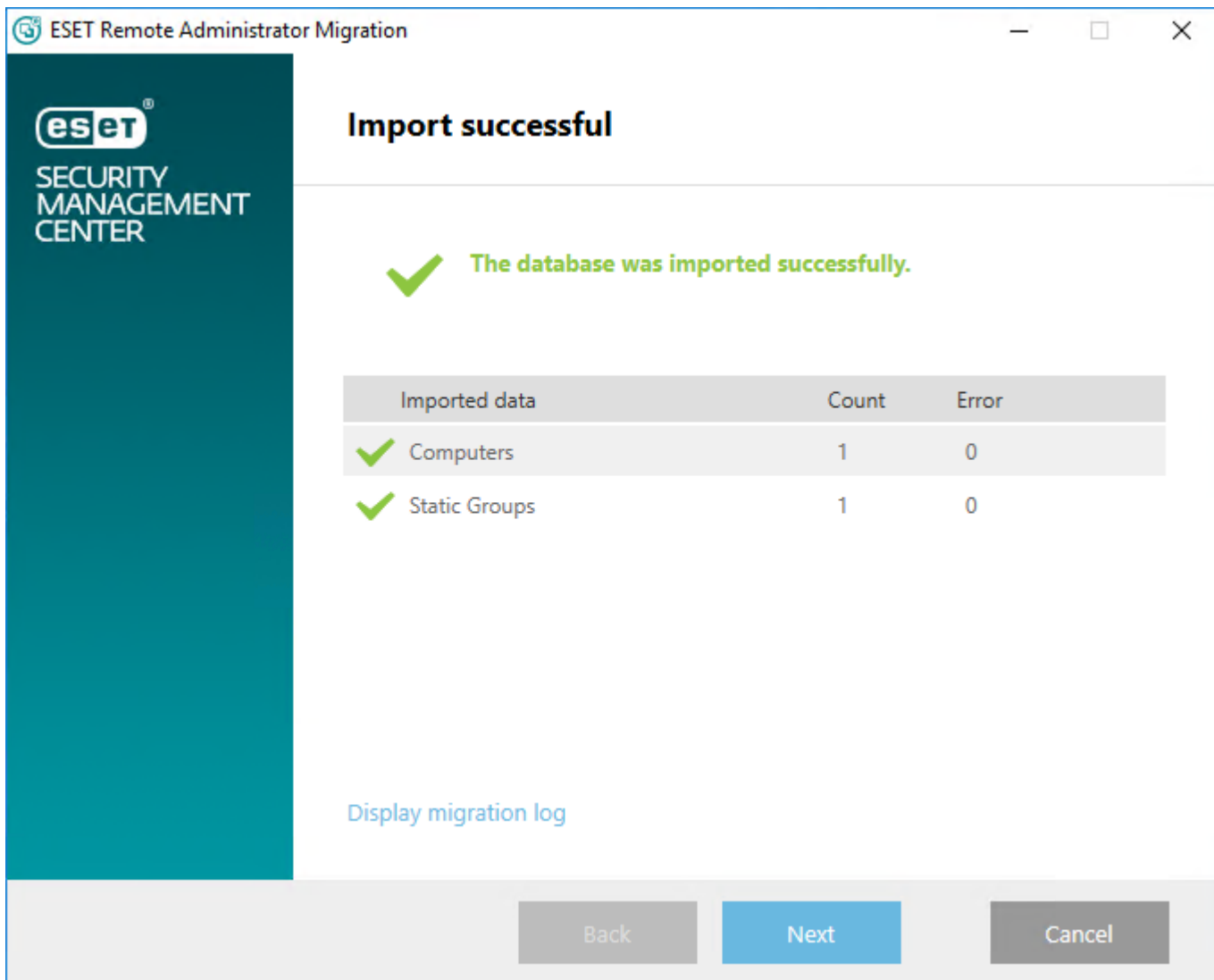
6. V prípade, že nástroj ESMC 7 bude nainštalovaný na rovnakom počítači ako ERA 5.x, musíte zmeniť svoje staré ERA porty a premenovať službu servera (`sc config ERA_SERVER DisplayName= "ESET Remote Administrator g1"`).

7. ESET Remote Administrator 5.x by mal byť po exportovaní dát znova spustený.

8. Nainštalujte ESMC 7 a importujte prechodnú databázu pomocou nástroja na migráciu. Budete vyzvaný, aby ste zadali IP adresu počítača (tú, ktorá sa zobrazila pre ESMC Console po úspešnej inštalácii) do poľa **Hostiteľ**, heslo správcu nastavené počas inštalácie a bude tiež potrebné zvoliť uložený databázový súbor.

9. Ak nastavenia servera nedovoľujú importovanie vybraných údajov, nástroj na migráciu Migration Tool vám umožní zmenu nastavení ESMC 7 pre vybrané komponenty.

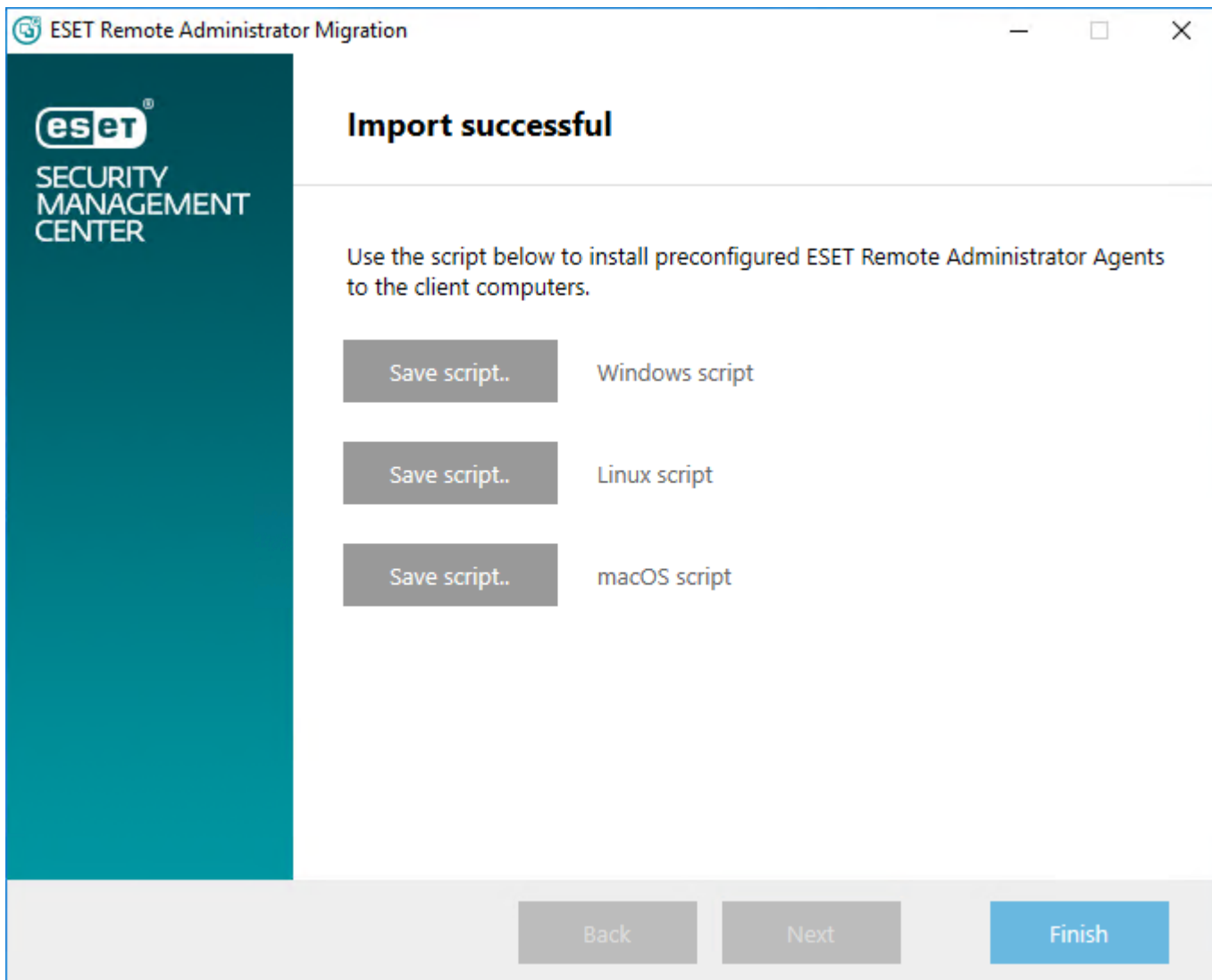
Každý komponent je potom importovaný. Pre každý komponent je dostupný **Protokol migrácie**. Po ukončení importu nástroj Migration tool zobrazí dialógové okno s výsledkom procesu importovania.



**! Dôležité:**

V prípade, že ste sa rozhodli migrovať používateľov, ich heslá boli vynulované a nahradené náhodne vygenerovanými heslami. Tieto vygenerované heslá budú dostupné na exportovanie vo formáte .CSV.

10. Nástroj na migráciu (Migration Tool) môžete použiť na vygenerovanie skriptu, ktorý umožňuje prednastaviť ESET Management Agency na klientských počítačoch. Tento skript je malý spustiteľný .bat súbor, distribuovateľný na klientske počítače.



Odporúčame skontrolovať migrované nastavenia a dáta a overiť si, či import prebehol úspešne. Potom môžete použiť skript na nasadenie ESET Management Agentov najprv na menšiu skupinu počítačov, aby ste sa uistili, že sa pripájajú na server správne.

Po úspešnom pripojení testovacej skupiny môžete nasadiť agenta na ostatné počítače v sieti (manuálne alebo použiť AD synchronizačnú úlohu na pridanie počítačov vo Web Console a následné nasadenie agenta).

**i Poznámka:**

Ak zlyhá niektorý z krokov migrácie, mali by ste vrátiť zmeny vykonané pre ESMC 7.x, pripojiť počítače späť na ERA 5.x, obnoviť zálohy dát z verzie ERA 5.x a kontaktovať technickú podporu spoločnosti ESET.

**! Dôležité:**

Pri tomto type migrácie nebudú exportované žiadne protokoly od zálohovania databázy ERA 5.x až po nasadenie agenta na klientsky počítač. Protokoly však zostanú uložené vo vašej starej kópii ERA 5.x.

### 5.2.3 Migrácia z predchádzajúcej verzie na novú – Linux

Asistent migrácie nepodporuje priamu migráciu z predchádzajúcej verzie nástroja ERA na novú verziu na operačných systémoch Linux.

Ak chcete migrovať nástroj ERA 5.x bežiaci na systéme Windows Server na nástroj ESMC 7.0 bežiaci na systéme Linux, postupujte podľa nasledujúcich inštrukcií:

1. Premigrujte ERA Server 5.x na operačnom systéme Windows použitím nástroja [ESET Asistent migrácie](#).
2. [Premigrujte ESMC zo systému Windows Server na virtuálne zariadenie ESMC](#).

#### **i** Poznámka:

Popísaný proces migrácie zahŕňa pokročilé úkony, a preto ho odporúčame vykonávať len naozaj skúseným správcom.

### 5.2.4 Nastavenie HTTP Proxy

HTTP Proxy nahrádza funkciu aktualizáčného mirror servera v ERA 5.x. HTTP Proxy môžete nastaviť niekoľkými spôsobmi.

#### **i** Poznámka:

Tieto nastavenia budú aplikované ako migrované politiky pre produkty **ESET Endpoint pre Windows**.

Ak je mirror priamo integrovaný do ERA Servera, k dispozícii sú nasledujúce možnosti:

- **Pripájať klienty priamo k internetu:** V migrovaných politikách pre koncové zariadenia bude v sekcii **Aktualizácia > Profily > HTTP Proxy > Režim proxy** zvolená možnosť **Použiť globálne nastavenie proxy servera**.
- **Pripájať klienty k internetu použitím HTTP Proxy:** V migrovaných politikách pre koncové zariadenia bude v sekcii **Aktualizácia > Profily > HTTP Proxy > Režim proxy** zvolená možnosť **Spojenie pomocou proxy servera**.

Pokiaľ ste v prostredí ERA 5.x ako mirror používali klienta, môžete tento mirror využívať aj naďalej – v tomto prípade zvolte možnosť **Použiť existujúce nastavenia mirror-a**.

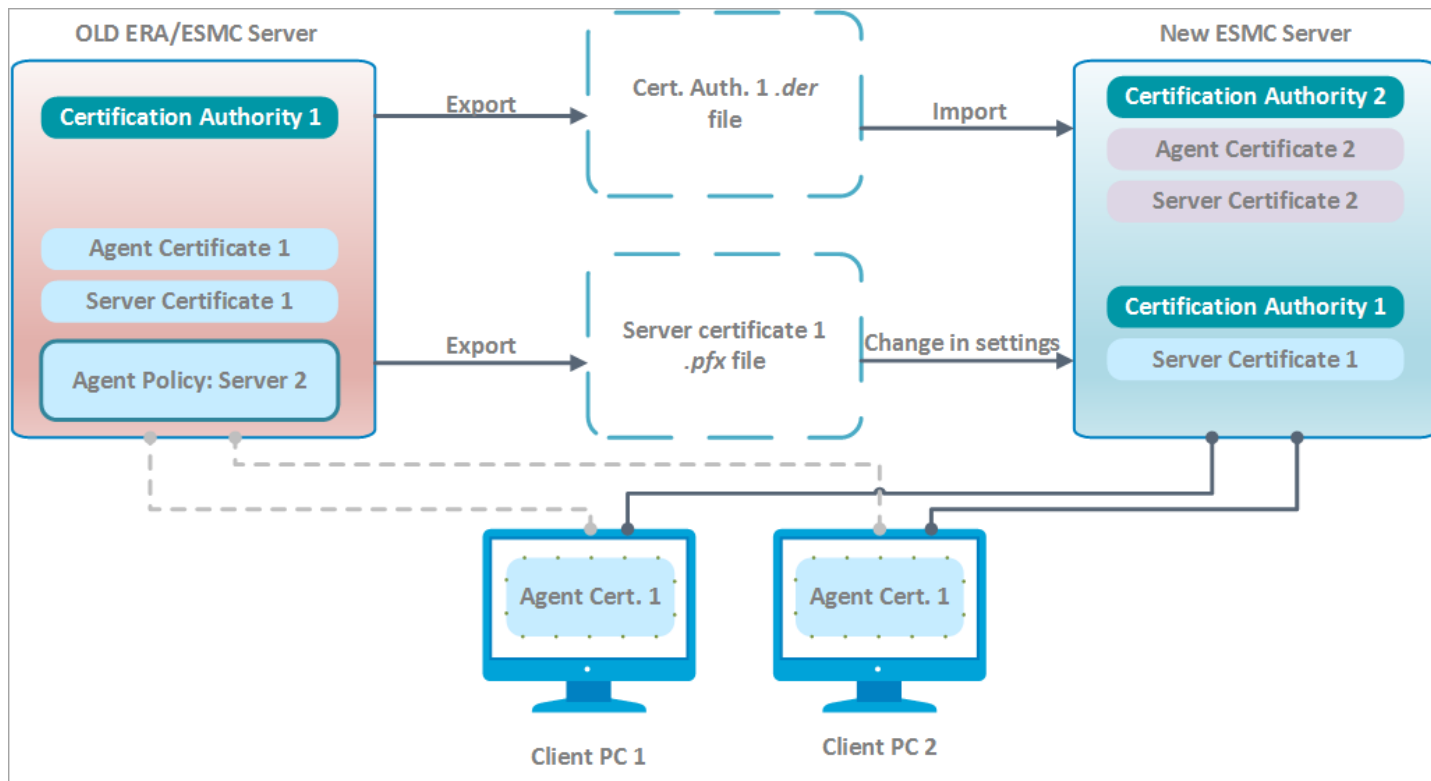
## 5.3 Migrácia na iný server

Existujú štyri spôsoby, ako migrovať ESET Security Management Center na iný server (tieto scenáre môžu byť použité pri preinštalovaní vášho ESMC Servera):

- [Čistá inštalácia – rovnaká IP adresa](#) – nová inštalácia nebude používať databázu z predošlého ESMC Servera a bude používať rovnakú IP adresu.
- [Čistá inštalácia – odlišná IP adresa](#) – nová inštalácia nebude používať databázu z predošlého ESMC Servera a bude používať odlišnú IP adresu.
- [Migrácia databázy – rovnaká IP adresa](#) – migrácia databázy môže byť vykonaná iba medzi dvomi podobnými typmi databázy (z MySQL na MySQL alebo z MSSQL na MSSQL) a podobnými verziami ESMC.
- [Migrácia databázy – odlišná IP adresa](#) – migrácia databázy môže byť vykonaná iba medzi dvomi podobnými typmi databázy (z MySQL na MySQL alebo z MSSQL na MSSQL) a podobnými verziami ESMC.

#### **i** Poznámka:

- Pri pridávaní nových klientskych počítačov použite na podpis certifikátov agentov novú certifikačnú autoritu. Importovaná certifikačná autorita nemôže byť použitá na podpisovanie nových partnerských certifikátov, môže byť použitá iba na overovanie ESET Management Agentov klientskych počítačov, ktoré boli migrované.



### 5.3.1 Čistá inštalácia – rovnaká IP adresa

Cieľom tohto postupu je nainštalovať úplne novú inštanciu ESMC Servera, ktorá nepoužíva predošlú databázu, ale ponecháva si záznamy pre klientske počítače. Nový ESMC Server bude mať **rovnakú IP adresu** ako váš predchádzajúci server, ale nebude používať databázu zo starého ESMC Servera.

#### ☐ Na vašom súčasnom (starom) ESMC Serveri:

1. **Exportujte** certifikát servera zo svojho súčasného ESMC Servera a **uložte** ho na externé ukladacie zariadenie.
  - Exportujte všetky [certifikáty certifikačnej autority](#) zo svojho ESMC Servera a uložte každý z nich ako `.der` súbor.
  - Exportujte [serverový certifikát](#) z vášho ESMC Servera vo formáte `.pfx`. Exportovaný `.pfx` súbor bude obsahovať aj súkromný kľúč.
2. **Zastavte** službu ESMC Server.
3. **Vypnite** zariadenie, ktoré slúži ako ESMC Server (voliteľné).

#### ⚠ Dôležité:

Zatiaľ neodinštalujte svoj starý ESMC Server.

#### ☐ Na vašom novom ESMC Serveri:

#### ⚠ Dôležité:

Uistite sa, že váš nový ESMC Server má rovnaké sieťové nastavenia (**IP adresa, FQDN, názov počítača, DNS SRV záznam**) ako váš starý ESMC Server.

1. **Nainštalujte** ESMC Server/MDM pomocou [all-in-one inštalátora](#) (Windows) alebo zvolte [iný spôsob inštalácie](#) – po jednotlivých komponentoch (Windows a Linux) alebo použite virtuálne zariadenie.
2. [Prihláste sa](#) do ESMC Web Console.
3. **Importujte všetky verejné kľúče certifikačnej autority**, ktoré ste exportovali z vášho starého ESMC Servera. Pre vykonanie tohto kroku postupujte podľa inštrukcií pre [importovanie verejného kľúča](#).

4. **Zmeňte** certifikát ESMC Servera v [nastaveniach servera](#) tak, aby sa používal certifikát vášho starého ESMC Servera (ten, ktorý bol exportovaný v kroku č. 1).
5. [Importujte všetky požadované ESET licencie](#) do ESMC.
6. **Reštartujte** službu ESMC Server. Viac informácií nájdete v nasledujúcom [článku databázy znalostí](#).

Klientske počítače by sa mali teraz pripojiť na váš nový ESMC Server pomocou ich pôvodného certifikátu ESET Management Agent, ktorý je overovaný certifikačnou autoritou importovanou zo starého ESMC Servera. Ak sa klientske počítače nepripájajú, pozrite si kapitolu [Problémy po aktualizácii/migrácii ESMC Servera](#).

#### **Odinštalovanie starého ESMC Servera/MDM**

Keď ste si istý, že na vašom novom ESMC Serveri funguje všetko správne, opatrne odinštalujte svoj starý ESMC Server/MDM podľa našich [podrobných inštrukcií](#).

### 5.3.2 Čistá inštalácia – odlišná IP adresa

Cieľom tohto postupu je nainštalovať úplne novú inštanciu ESMC Servera, ktorá nepoužíva predošlú databázu, ale ponecháva si záznamy pre klientske počítače. Nový ESMC Server bude mať **odlišnú IP adresu/názov hostiteľa**, ale nebude používať databázu zo starého ESMC Servera.

#### **Na vašom súčasnom (starom) ESMC Serveri:**

1. **Vygenerujte** [nový certifikát pre ESMC Server](#), ktorý bude obsahovať informácie o pripojení pre nový ESMC Server. V poli **Hostiteľ** ponechajte pôvodnú hodnotu (hviezdičku). Tým pádom certifikát nebude viazaný na konkrétny DNS názov alebo IP adresu a zároveň bude umožnená jeho bezproblémová distribúcia.
2. **Exportujte** certifikát servera zo svojho súčasného ESMC Servera a **uložte** ho na externé ukladacie zariadenie.
  - Exportujte všetky [certifikáty certifikačnej autority](#) zo svojho ESMC Servera a uložte každý z nich ako `.der` súbor.
  - Exportujte [serverový certifikát](#) z vášho ESMC Servera vo formáte `.pfx`. Exportovaný `.pfx` súbor bude obsahovať aj súkromný kľúč.
3. **Vytvorte** politiku, ktorá bude definovať [novú IP adresu ESMC Servera](#) a priradte ju k všetkým počítačom. Počkajte, kým sa politika aplikuje na všetky klientske počítače (počítače sa prestanú prihlasovať, keď dostanú informácie o novom serveri).
4. **Zastavte** službu ESMC Server.
5. **Vypnite** zariadenie, ktoré slúži ako súčasný ESMC Server (voliteľné).

#### **Dôležité:**

Zatiaľ neodinštalujte svoj starý ESMC Server.

#### **Na vašom novom ESMC Serveri:**

1. **Nainštalujte** ESMC Server/MDM pomocou [all-in-one inštalátora](#) (Windows) alebo zvolte [iný spôsob inštalácie](#) – po jednotlivých komponentoch (Windows a Linux) alebo použite virtuálne zariadenie.
2. [Prihláste sa](#) do ESMC Web Console.
3. **Importujte všetky verejné kľúče certifikačnej autority**, ktoré ste exportovali z vášho starého ESMC Servera. Pre vykonanie tohto kroku postupujte podľa inštrukcií pre [importovanie verejného kľúča](#).
4. **Zmeňte** certifikát ESMC Servera v [nastaveniach servera](#) tak, aby sa používal certifikát vášho starého ESMC Servera (ten, ktorý bol exportovaný v kroku č. 1). Nezastavujte službu ESMC Server až do kroku č. 6.
5. [Importujte všetky požadované ESET licencie](#) do ESMC.

6. **Reštartujte** službu ESMC Server. Viac informácií nájdete v nasledujúcom [článku databázy znalostí](#).

Klientske počítače by sa mali teraz pripojiť na váš nový ESMC Server pomocou ich pôvodného certifikátu ESET Management Agenta, ktorý je overovaný certifikačnou autoritou importovanou zo starého ESMC Servera. Ak sa klientske počítače nepripájajú, pozrite si kapitolu [Problémy po aktualizácii/migrácii ESMC Servera](#).

#### **Odinštalovanie starého ESMC Servera/MDM**

Keď ste si istý, že na vašom novom ESMC Serveri funguje všetko správne, opatrne odinštalujte svoj starý ESMC Server/MDM podľa našich [podrobných inštrukcií](#).

### 5.3.3 Migrácia databázy – rovnaká IP adresa

Cieľom tohto postupu je nainštalovať úplne novú inštanciu ESMC Servera a **zachovať vašu existujúcu ESMC databázu** vrátane existujúcich klientskych počítačov. Nový ESMC Server bude mať **rovnakú IP adresu** ako starý ESMC Server a databáza starého ESMC Servera bude importovaná na nový server predtým, ako začne inštalácia.

#### **Dôležité:**

- [Migrácia databáz](#) je podporovaná len medzi rovnakými typmi databáz (z MySQL na MySQL alebo z MSSQL na MSSQL).
- Pri migrácii databázy je možné migrovať len medzi inštaniami rovnakej verzie nástroja ESET Security Management Center. Pre inštrukcie, ako zistiť verzie vašich súčastí ESMC, si prečítajte náš [článok databázy znalostí](#). Po dokončení migrácie môžete v prípade potreby aktualizovať ESET Security Management Center.

#### **Na vašom súčasnom (starom) ESMC Serveri:**

1. **Exportujte** certifikát servera zo svojho súčasného ESMC Servera a **uložte** ho na externé ukladacie zariadenie.
  - Exportujte všetky [certifikáty certifikačnej autority](#) zo svojho ESMC Servera a uložte každý z nich ako `.der` súbor.
  - Exportujte [serverový certifikát](#) z vášho ESMC Servera vo formáte `.pfx`. Exportovaný `.pfx` súbor bude obsahovať aj súkromný kľúč.
2. **Zastavte** službu ESMC Server.
3. [Exportujte/zálohujte ESMC databázu](#).
4. **Vypnite** zariadenie, ktoré slúži ako súčasný ESMC Server (voliteľné).

#### **Dôležité:**

Zatiaľ neodinštalujte svoj starý ESMC Server.

#### **Na vašom novom ESMC Serveri:**

#### **Dôležité:**

Uistite sa, že váš nový ESMC Server má rovnaké sieťové nastavenia (**IP adresa, FQDN, názov počítača, DNS SRV záznam**) ako váš starý ESMC Server.

1. **Nainštalujte/spustite** [podporovanú](#) ESMC databázu.
2. **Importujte/obnovte** [ESMC databázu](#) z vášho starého ESMC Servera.
3. **Nainštalujte** ESMC Server/MDM pomocou [all-in-one inštalátora](#) (Windows) alebo zvolte [iný spôsob inštalácie](#) – po jednotlivých komponentoch (Windows a Linux) alebo použite virtuálne zariadenie. Počas inštalácie ESMC Servera upresnite nastavenia pripojenia na databázu.
4. [Prihláste sa](#) do ESMC Web Console.



5. **Importujte všetky verejné kľúče certifikačnej autority** exportované z vášho starého ESMC Servera. Pre vykonanie tohto kroku postupujte podľa inštrukcií pre [importovanie verejného kľúča](#).
6. **Reštartujte** službu ESMC Server. Viac informácií nájdete v nasledujúcom [článku databázy znalostí](#).

Klientske počítače by sa mali teraz pripojiť na váš nový ESMC Server pomocou ich pôvodného certifikátu ESET Management Agent, ktorý je overovaný certifikačnou autoritou importovanou zo starého ESMC Servera. Ak sa klientske počítače nepripájajú, pozrite si kapitolu [Problémy po aktualizácii/migrácii ESMC Servera](#).

#### **Odištalovanie starého ESMC Servera/MDM**

Keď ste si istý, že na vašom novom ESMC Serveri funguje všetko správne, opatrne odištalujte svoj starý ESMC Server/MDM podľa našich [podrobných inštrukcií](#).

### 5.3.4 Migrácia databázy – odlišná IP adresa

Cieľom tohto postupu je nainštalovať úplne novú inštanciu ESMC Servera a **zachovať vašu existujúcu ESMC databázu** vrátane existujúcich klientskych počítačov. Nový ESMC Server bude mať **inú IP adresu** ako starý ESMC Server a databáza starého ESMC Servera bude importovaná na nový server predtým, ako začne inštalácia.

#### **Dôležité:**

- [Migrácia databáz](#) je podporovaná len medzi rovnakými typmi databáz (z MySQL na MySQL alebo z MSSQL na MSSQL).
- Pri migrácii databázy je možné migrovať len medzi inštaniami rovnakej verzie nástroja ESET Security Management Center. Pre inštrukcie, ako zistiť verzie vašich súčastí ESMC, si prečítajte náš [článok databázy znalostí](#). Po dokončení migrácie môžete v prípade potreby aktualizovať ESET Security Management Center.

#### **Na vašom súčasnom (starom) ESMC Serveri:**

1. **Vygenerujte [nový certifikát pre ESMC Server](#)**, ktorý bude obsahovať informácie o pripojení pre nový ESMC Server. V poli **Hostiteľ** ponechajte pôvodnú hodnotu (hviezdičku). Tým pádom certifikát nebude viazaný na konkrétny DNS názov alebo IP adresu a zároveň bude umožnená jeho bezproblémová distribúcia.
2. **Exportujte** certifikát servera zo svojho súčasného ESMC Servera a **uložte** ho na externé ukladacie zariadenie.
  - Exportujte všetky [certifikáty certifikačnej autority](#) zo svojho ESMC Servera a uložte každý z nich ako `.der` súbor.
  - Exportujte [serverový certifikát](#) z vášho ESMC Servera vo formáte `.pfx`. Exportovaný `.pfx` súbor bude obsahovať aj súkromný kľúč.
3. **Vytvorte** politiku, ktorá bude definovať [novú IP adresu ESMC Servera](#) a priradte ju k všetkým počítačom. Počkajte, kým sa politika aplikuje na všetky klientske počítače (počítače sa prestanú prihlasovať, keď dostanú informácie o novom serveri).
4. **Zastavte** službu ESMC Server.
5. [Exportujte/zálohujte ESMC databázu](#).
6. **Vypnite** zariadenie, ktoré slúži ako súčasný ESMC Server (voliteľné).

#### **Dôležité:**

Zatiaľ neodinštalujte svoj starý ESMC Server.

#### **Na vašom novom ESMC Serveri:**

1. Nainštalujte/spustite [podporovanú ESMC databázu](#).

2. **Importujte/obnovte** [ESMC databázu](#) z vášho starého ESMC Servera.
3. **Nainštalujte** ESMC Server/MDM pomocou [all-in-one inštalátora](#) (Windows) alebo zvolte [iný spôsob inštalácie](#) – po jednotlivých komponentoch (Windows a Linux) alebo použite virtuálne zariadenie. Počas inštalácie ESMC Servera upresnite nastavenia pripojenia na databázu.
4. [Prihláste sa](#) do ESMC Web Console.
5. **Importujte všetky verejné kľúče certifikačnej autority** exportované z vášho starého ESMC Servera. Pre vykonanie tohto kroku postupujte podľa inštrukcií pre [importovanie verejného kľúča](#).
6. **Zmeňte** certifikát ESMC Servera v [nastaveniach servera](#) tak, aby sa používal certifikát vášho starého ESMC Servera (ten, ktorý bol exportovaný v kroku č. 1). Nezastavujte službu ESMC Server až do kroku č. 7.
7. **Reštartujte** službu ESMC Server. Viac informácií nájdete v nasledujúcom [článku databázy znalostí](#).

Klientske počítače by sa mali teraz pripojiť na váš nový ESMC Server pomocou ich pôvodného certifikátu ESET Management Agent, ktorý je overovaný certifikačnou autoritou importovanou zo starého ESMC Servera. Ak sa klientske počítače nepripájajú, pozrite si kapitolu [Problémy po aktualizácii/migrácii ESMC Servera](#).

#### **Odinštalovanie starého ESMC Servera/MDM**

Keď ste si istý, že na vašom novom ESMC Serveri funguje všetko správne, opatrne odinštalujte svoj starý ESMC Server/MDM podľa našich [podrobných inštrukcií](#).

### 5.3.5 Odinštalovanie starého ESMC Servera

Existuje niekoľko spôsobov, ako vyradiť váš starý ESMC Server/MDM z prevádzky:

#### **Dôležité:**

Uistite sa, že váš nový ESMC Server/MDM pracuje a klientske počítače a mobilné zariadenia sa pripájajú k ESMC správne.

1. V prípade, že si chcete ponechať operačný systém a znova ho použiť, môžete odinštalovať starú verziu ERA/ESMC MDM, avšak pred tým je potrebné vykonať nasledovné:
  - naplánujte reštart operačného systému svojho servera po odinštalovaní,
  - Uistite sa, že ostatné súčasti ESMC boli odinštalované (vrátane ESET Management Agent, Rogue Detection Sensor atď.),
  - neodinštalujte svoju databázu, ibaže od nej nie je závislý žiadny iný softvér.
2. Disk s ESMC Serverom môžete naformátovať, v tom prípade však stratíte všetky dáta uložené na disku vrátane operačného systému. Zároveň je to ale najjednoduchší spôsob odstránenia ERA/ESMC/MDM.

## 5.4 Migrácia ESMC databázy

Kliknite na príslušný odkaz nižšie pre pokyny k migrácii databázy ESMC Servera (ERA Server alebo služba ERA 6.x Proxy, ak používate verziu 6.x) alebo MDM databázy medzi rôznymi inštanciami SQL Servera (to platí aj pri prechode na inú verziu SQL Servera alebo pri prechode na SQL Server na inom počítači):

- [Migračný proces pre SQL Server](#)
- [Migračný proces pre MySQL Server](#)

Tento migračný proces je rovnaký pre **Microsoft SQL Server** a **Microsoft SQL Server Express**.

## 5.4.1 Migračný proces pre MS SQL Server

Tento migračný proces je rovnaký pre **Microsoft SQL Server** a **Microsoft SQL Server Express**.

Pre viac informácií si prečítajte nasledujúci článok: <https://msdn.microsoft.com/en-us/library/ms189624.aspx>.

### **i** Poznámka:

Komponent ERA Proxy z verzie 6 bol z dôvodu zmeny protokolu replikácie agenta nahradený službou [proxy](#) tretej strany. Nemigrujte databázu Proxy medzi verziami 6.x a 7.

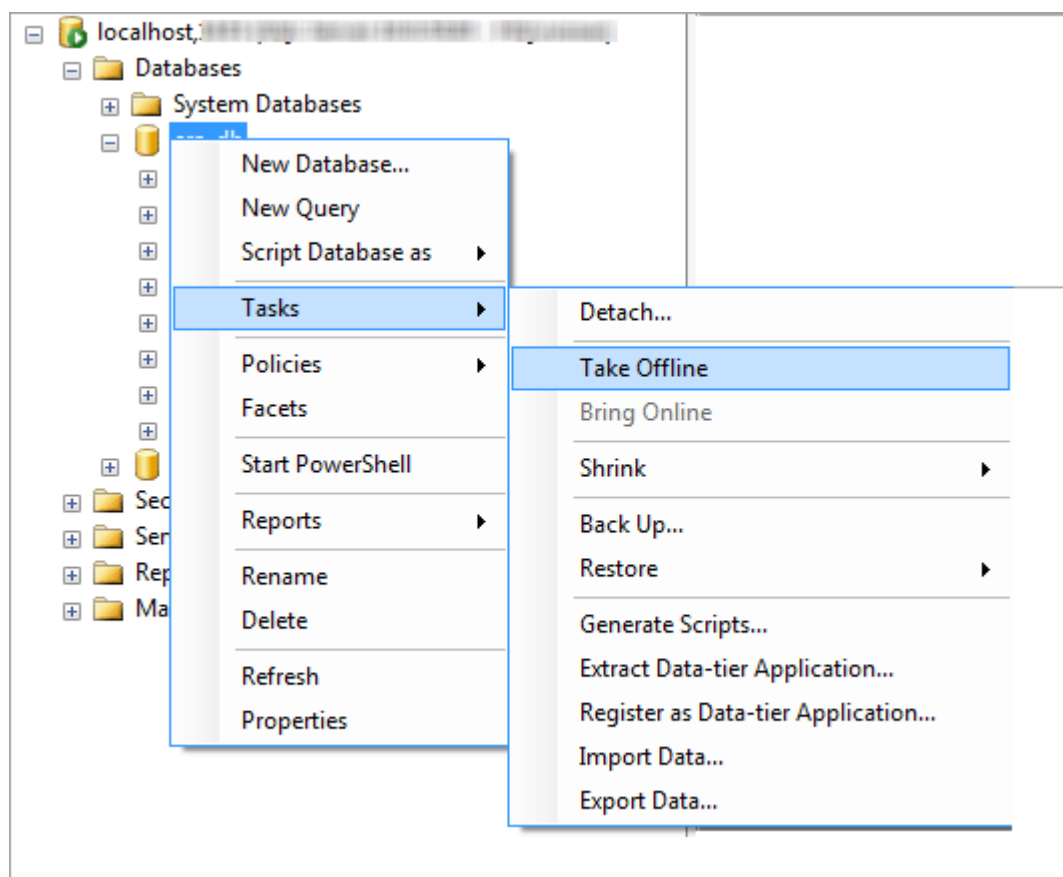
[Vykonanie aktualizácie v prostredí s ERA Proxy](#)

### Prerekvizity:

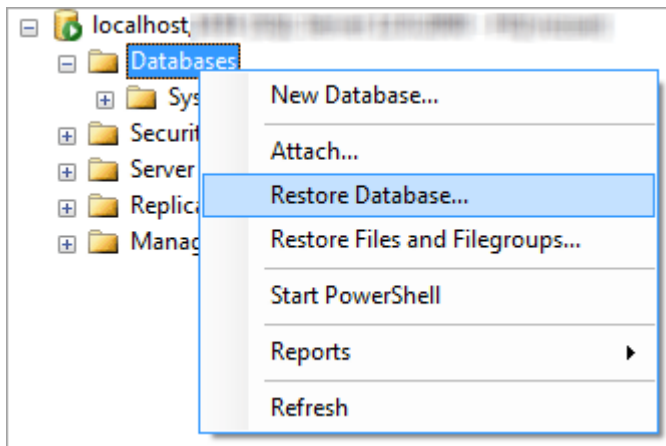
- Zdrojová a cieľová inštancia SQL servera musia byť nainštalované. Môžu byť umiestnené na odlišných zariadeniach.
- Cieľová inštancia SQL servera musí byť minimálne takej istej verzie ako zdrojová inštancia. **Prechod na nižšiu verziu nie je podporovaný!**
- **SQL Server Management Studio** musí byť nainštalované. Ak sa inštancie SQL servera nachádzajú na odlišných zariadeniach, je potrebné mať softvér SQL Server Management Studio nainštalovaný na každom z nich.

### Migrácia pomocou nástroja SQL Server Management Studio

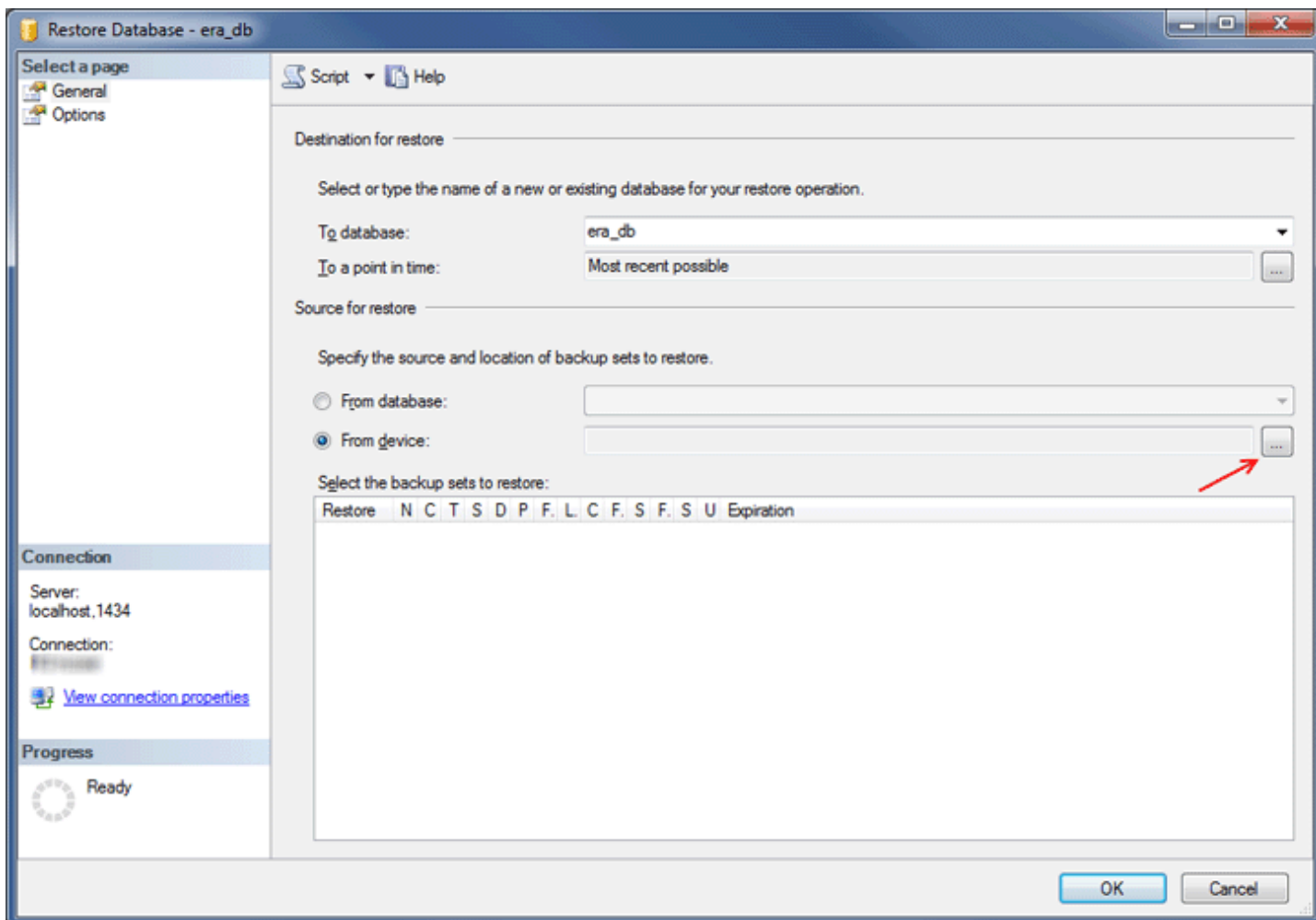
1. **Zastavte** službu ESMC Server (ERA Server alebo službu ERA 6.x Proxy, ak používate verziu 6.x), prípadne službu ESMC MDM.
2. Prihláste sa do zdrojovej inštancie SQL servera cez SQL Server Management Studio.
3. **Vytvorte úplnú zálohu databázy**, ktorú budete migrovať. Odporúča sa manuálne zadať úplne nový (doteraz nepoužitý) názov zálohy. Ak sa už daný názov zálohy použili v minulosti, nová záloha bude k starej zálohe pripojená, čo v konečnom dôsledku znamená zbytočne veľký súbor.
4. Zdrojovú databázu prepnete do offline režimu pomocou **Tasks > Take Offline**.



5. **Skopírujte** zálohu vytvorenú v kroku č. 3 (.bak súbor) na miesto, ktoré je dostupné pre cieľovú inštanciu SQL servera. Toto môže vyžadovať zmenu prístupových práv zálohového súboru alebo premiestnenie súboru na iný počítač.
6. **Znovu zapnite** zdrojovú databázu, ale zatiaľ **nespúšťajte ESMC Server alebo ESMC MDM!**
7. Prihláste sa do cieľovej inštancie SQL Servera pomocou nástroja SQL Server Management Studio.
8. [Obnovte vašu databázu](#) na cieľovú inštanciu SQL servera.

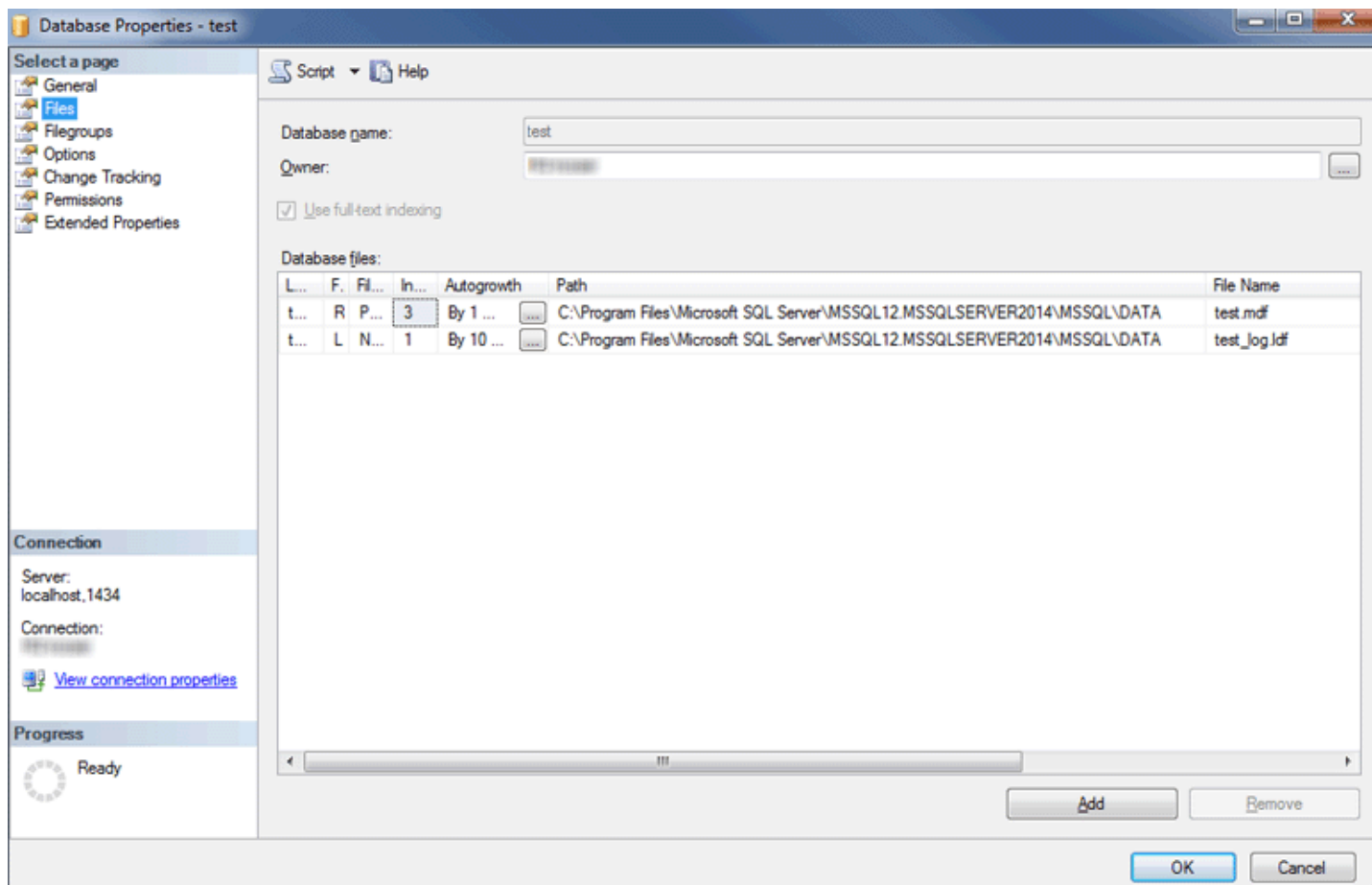


9. Zadáte nový názov databázy do poľa **To database**. Ak chcete, môžete použiť rovnaký názov ako názov vašej starej databázy.
10. Zvoľte možnosť „From device“ v časti **Specify the source and location of backup sets to restore** a kliknite na tlačidlo ...



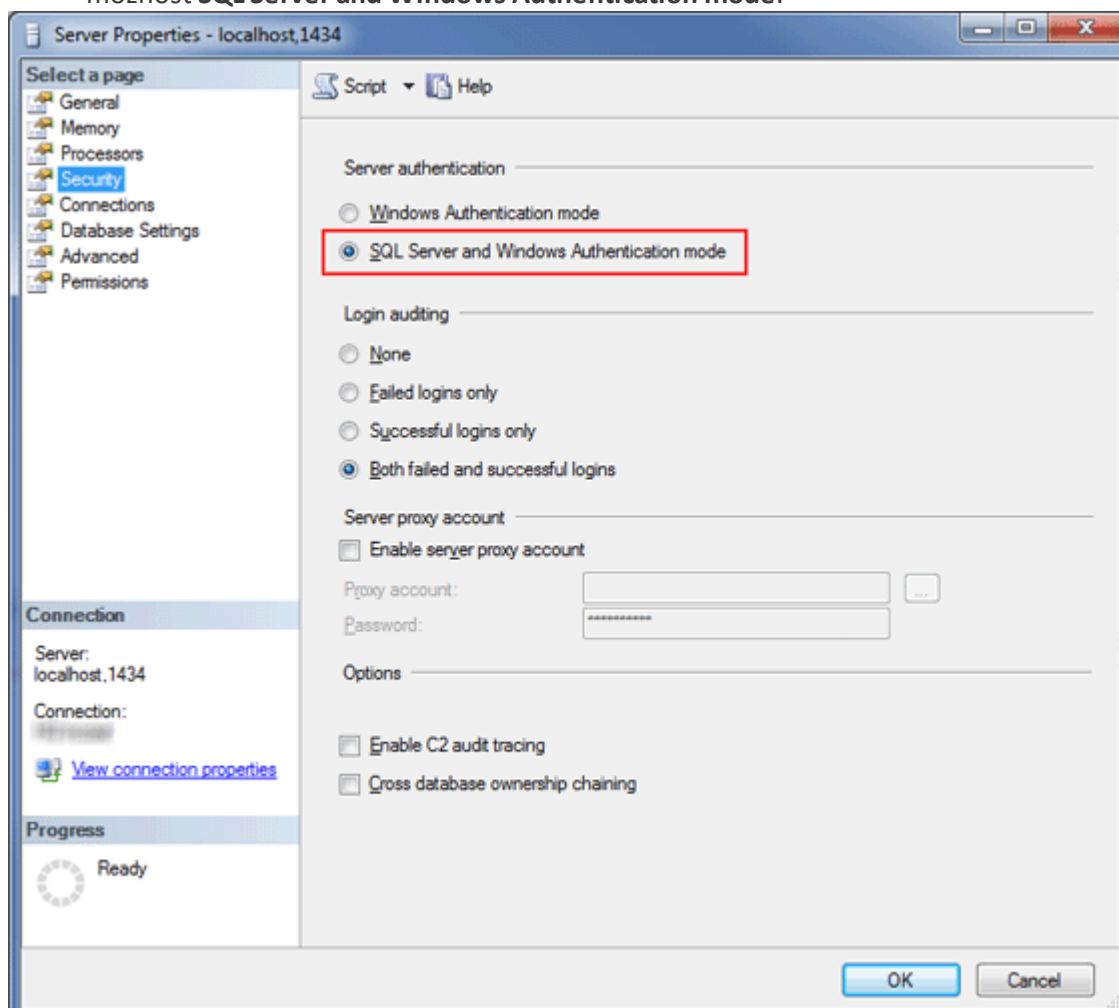
11. Kliknite na **Add**, nájdite súbor so zálohou databázy a otvorte ho.

12. Zvoľte najaktuálnejšiu zálohu (zálohový balík môže obsahovať viac záloh), z ktorej obnovíte databázu.
13. Kliknite na časť **Options** v sprievodcovi obnovou databázy. Môžete tiež prípadne zvoliť možnosť **Overwrite existing database** a uistiť sa, že miesta pre obnovenie databázy (.mdf) a protokolu (.ldf) sú správne. Ak prednastavené hodnoty necháte nezmenené, obnova s veľkou pravdepodobnosťou zlyhá, pretože pôvodné cesty pochádzajú zo zdrojového SQL servera.
  - Ak nie ste si istý umiestnením databázových súborov na cieľovej inštancii SQL Servera, kliknite pravým tlačidlom na existujúcu databázu, zvoľte **Properties** a kliknite na kartu **Files**. V stĺpci **Path** uvidíte cestu k adresáru, v ktorom sa databáza nachádza.



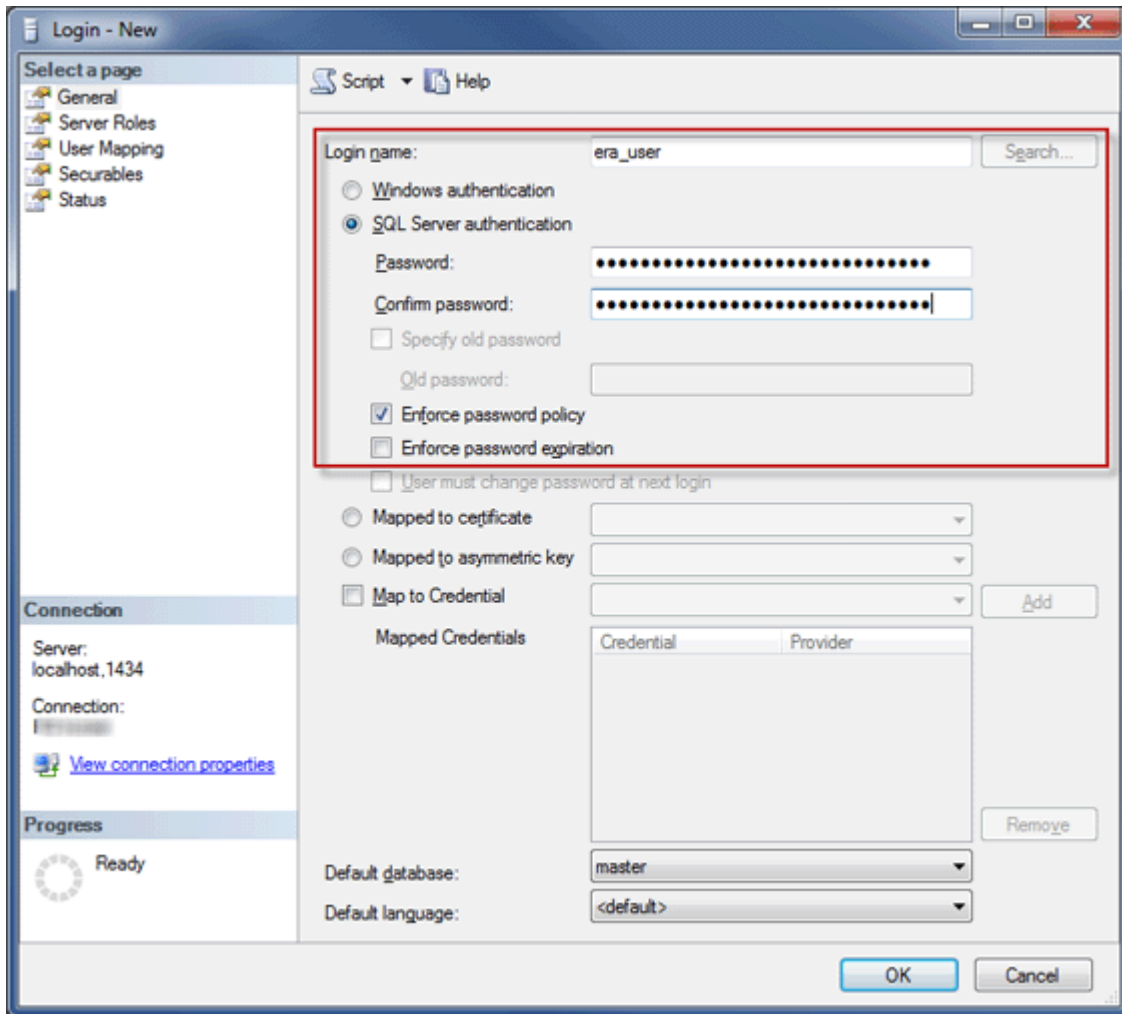
14. V okne sprievodcu obnovou databázy kliknite na tlačidlo **OK**.

15. Uistite sa, že nový databázový server má povolenú možnosť **SQL Server Authentication**. Aby ste tak učinili, kliknite pravým tlačidlom na server a zvolte **Properties**. V tomto okne zvolte **Security** a uistite sa, že je zvolená možnosť **SQL Server and Windows Authentication mode**.

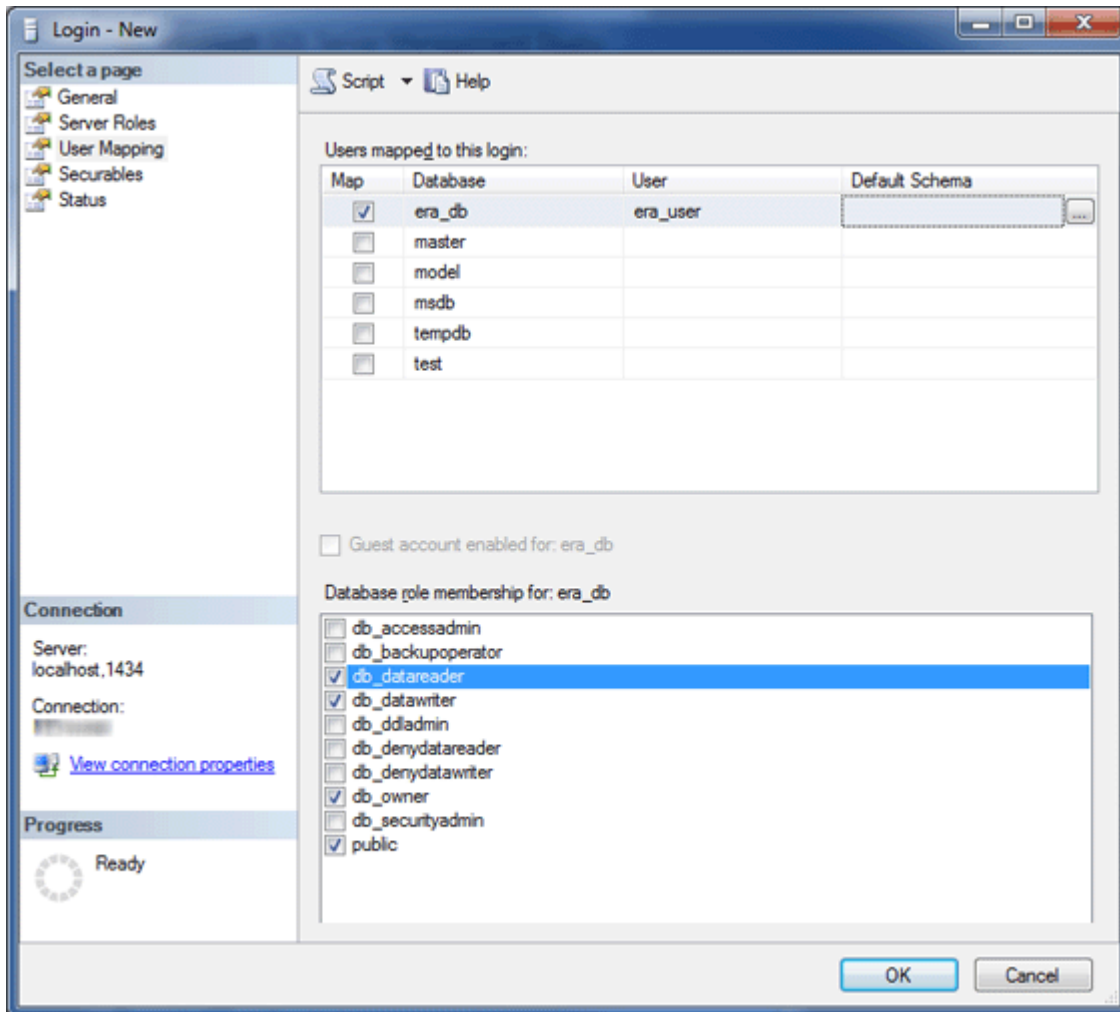


16. **Vytvorte nové prístupové údaje pre SQL server** (pre ESMC Server/ESMC MDM) na cieľovom SQL serveri, pričom zvolte možnosť **SQL Server authentication**, a potom priradte tieto prístupové údaje k používateľovi obnovenej databázy.

- Uistite sa, že možnosť „Enforce password expiration“ nie je zaškrtnutá!
- Odporúčané znaky pre meno používateľa:
  - Malé písmená zo znakovej sady ASCII, čísla a podčiarkovník " \_ "
- Odporúčané znaky pre heslo:
  - Iba znaky zo znakovej sady ASCII, malé aj veľké písmená zo znakovej sady ASCII, čísla, medzery, špeciálne znaky
- Nepoužívajte znaky, ktoré nepatria do znakovej sady ASCII, napr. zložené zátvorky { } alebo znak zavináč @.
- Berte, prosím, na vedomie, že ak nebudete postupovať podľa vyššie uvedených odporúčaní týkajúcich sa použiteľných znakov, môžete mať problémy s databázovým pripojením alebo budete musieť použiť tzv. „únikový znak“ (escape character) pri úprave reťazca pripojenia k databáze. Pravidlá použitia „únikových znakov“ nie sú súčasťou tejto dokumentácie.

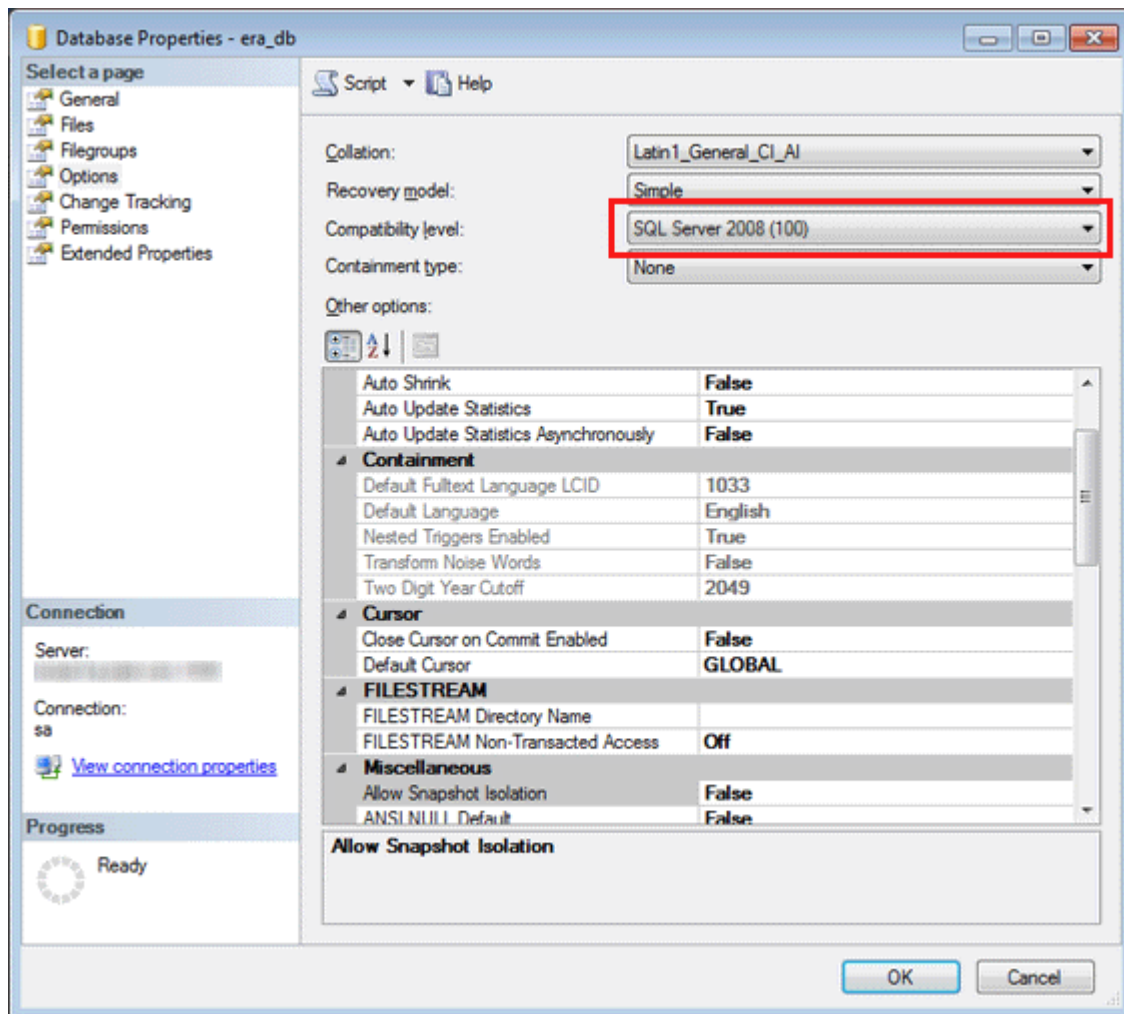


17. Priradíte prihlasovacie údaje k používateľovi cieľovej databázy. Uistite sa, že na karte **User Mapping** má používateľ priradené nasledovné roly: **db\_datareader**, **db\_datawriter** a **db\_owner**.





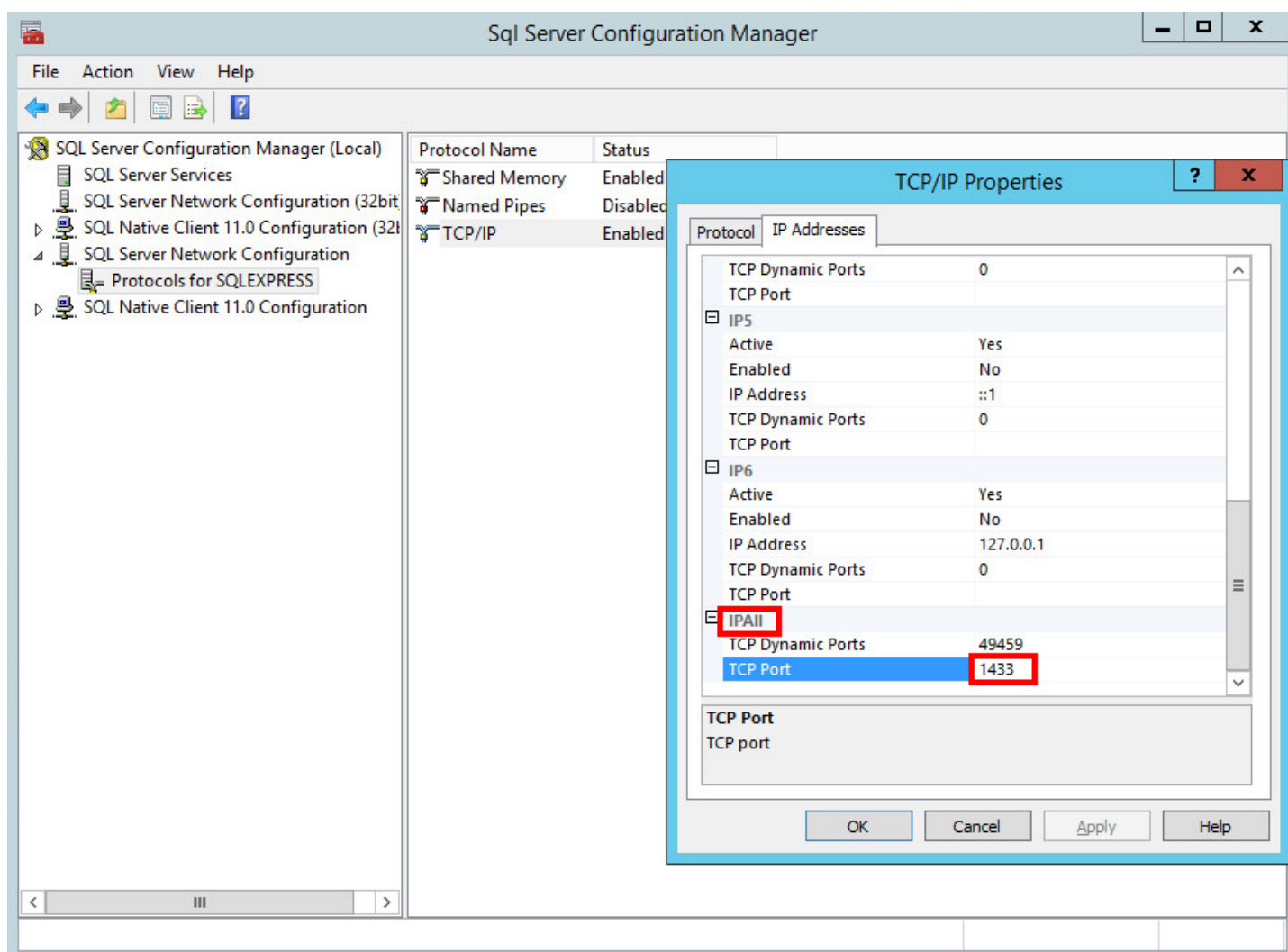
18. Následne nastavte **Compatibility level** pre obnovenú databázu na najnovšiu úroveň, aby boli povolené všetky funkcie databázového servera. Pre vykonanie tohto kroku kliknite pravým tlačidlom na novú databázu a zvolíte možnosť **Properties**.



**Poznámka:**

SQL Server Management Studio neumožňuje nastaviť vyššiu úroveň kompatibility ako je verzia, ktorú práve používate. Napríklad, ak používate SQL Server Management Studio 2008, nemôžete nastaviť úroveň kompatibility na SQL Server 2014.

19. Uistite sa, že **TCP/IP** protokol je **umožnený** pre „názov\_inštancie\_databázy“ (napr. SQLEXPRESS alebo MSSQLSERVER), a tiež že TCP/IP **port** je nastavený na **1433**. Toto môžete vykonať otvorením nástroja **Sql Server Configuration Manager** v časti **SQL Server Network Configuration > Protocols for „názov\_inštancie\_databázy“**, následným kliknutím praveho tlačidla na **TCP/IP** a zvolením možnosti **Enabled**. Potom dvakrát kliknite na **TCP/IP**, prejdite na kartu **Protocols**, posuňte sa nižšie na časť **IPAll** a do poľa **TCP Port** zadajte 1433. Kliknite na **OK** a reštartujte službu **SQL Server**.



20. **Nájdite** súbor *startupconfiguration.ini* na zariadení, na ktorom je nainštalovaná služba ESMC Server alebo ESMC MDM.

- Pre Windows Vista a novšie verzie operačného systému Windows:

Server:

% PROGRAMDATA %

|ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini

MDMCore:

% PROGRAMDATA %

|ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini

- Pre staršie verzie operačného systému Windows:

Server:

% ALLUSERSPROFILE %\ Application

Data\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini

MDMCore:

% ALLUSERSPROFILE %\ Application

Data\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configuration\startupconfiguration.ini

- Pre Linux:

Server:

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore:

```
/etc/opt/eset/RemoteAdministrator/MDMCore/StartupConfiguration.ini
```

21. **Zmeňte** reťazec pripojenia k databáze v súbore *startupconfiguration.ini* pre ESMC Server/MDM.

- Nastavte adresu a port nového databázového servera.
- Nastavte nové meno a heslo pre používateľa, ktorý má prístup k ESMC databáze.

- Výsledok by mal byť vyzeráť takto:

Táto kapitola je dostupná len v [Online pomocníkovi](#).

22. **Spustite** ESMC Server alebo ESMC MDM uistite sa, že tieto služby fungujú správne.

## 5.4.2 Migračný proces pre MySQL Server

### Prerekvizity

- Zdrojová a cieľová inštancia SQL servera musia byť nainštalované. Môžu byť umiestnené na odlišných zariadeniach.
- MySQL nástroje musia byť dostupné aspoň na jednom zo zariadení (`mysqldump` a `mysql` klient).

### Užitočné odkazy:

- <https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html>
- <https://dev.mysql.com/doc/refman/5.6/en/mysql.html>

### Migrácia SQL Servera

V príkazoch, konfiguračných súboroch alebo SQL príkazoch nižšie vždy zameňte:

- **SRCHOST** za adresu zdrojového databázového servera,
- **SRCROOTLOGIN** za používateľské meno root používateľa na zdrojovom MySQL serveri,
- **SRCERADBNAME** za názov zdrojovej databázy ESMC, ktorá sa má zálohovať,
- **BACKUPFILE** za cestu k súboru, kam sa uloží záloha,
- **TARGETHOST** za adresu cieľového databázového servera,
- **TARGETROOTLOGIN** za používateľské meno root používateľa na cieľovom MySQL serveri,
- **TARGETERADBNAME** za názov cieľovej databázy ESMC (po migrácii),
- **TARGETERALOGIN** za používateľské meno používateľa novej ESMC databázy na cieľovom MySQL serveri,
- **TARGETERAPASSWD** za heslo používateľa novej ESMC databázy na cieľovom MySQL serveri.

Nie je nevyhnutné spustiť nižšie uvedené príkazy cez príkazový riadok. Ak poznáte vhodný nástroj s grafickým rozhraním, môžete ho použiť miesto príkazov.

Nasledujúci postup je dostupný len v [Online pomocníkovi](#).

## 5.5 Migrácia MDM

Cieľom tohto postupu je premigrovať vašu existujúcu inštanciu ESMC MDM a zároveň **zachovať vašu existujúcu ESMC MDM databázu** vrátane registrovaných mobilných zariadení. Premigrovaný komponent ESMC MDM bude mať **rovnakú IP adresu/názov hostiteľa** ako starý ESMC MDM a databáza starého ESMC MDM bude importovaná na nového hostiteľa MDM predtým, ako začne inštalácia.

### ! Dôležité:

- [Migrácia databáz](#) je podporovaná len medzi rovnakými typmi databáz (z MySQL na MySQL alebo z MSSQL na MSSQL).
- Pri migrácii databázy je možné migrovať len medzi inštanciami rovnakej verzie nástroja ESET Security Management Center. Pre inštrukcie, ako zistiť verzie vašich súčastí ESMC, si prečítajte náš [článok databázy znalostí](#). Po dokončení migrácie môžete v prípade potreby aktualizovať ESET Security Management Center.

### ☐ Na vašom súčasnom (starom) ESMC MDM Serveri:

1. Prejdite do sekcie **Podrobnosti o počítači** na svojom súčasnom (starom) MDM Serveri a **exportujte z neho konfiguráciu**. Otvorte konfiguráciu a exportujte z nej nasledujúce položky na externé ukladacie zariadenie:
  - Presný názov hostiteľa svojho MDM Servera.
  - Zo svojho ESMC Servera exportujte v podobe súboru .pfx partnerské certifikáty, ktoré sú súčasťou politiky MDM. Exportovaný súbor .pfx bude obsahovať privátny kľúč a tiež nasledovné:
    - HTTPS certifikát,
    - podpisový certifikát profilu pre nasadenie,
    - APNS certifikát (exportujte APNS certifikát aj APNS privátny kľúč),
    - autorizačný token Programu registrácie zariadení Apple (DEP).
2. **Zastavte** službu ESMC MDM.
3. [Exportujte/zálohujte ESMC databázu](#).
4. **Vypnite** súčasné ESMC MDM zariadenie (voliteľné).

### ! Dôležité:

Zatiaľ neodinštalujte svoj starý ESMC MDM.

### ☐ Na vašom novom ESMC Serveri:

### ! Dôležité:

Uistite sa, že váš nový ESMC MDM Server má rovnaké sieťové nastavenia (**názov hostiteľa, ktorý ste exportovali z konfigurácie svojho starého MDM Servera**) ako váš starý ESMC MDM.

1. **Nainštalujte/spustite** [podporovanú](#) ESMC databázu.
2. **Importujte/obnovte** [ESMC databázu](#) zo svojho starého ESMC MDM.
3. **Nainštalujte** ESMC Server/MDM pomocou [all-in-one inštalátora](#) (Windows) alebo zvolte [iný spôsob inštalácie](#) – po jednotlivých komponentoch (Windows a Linux) alebo použite virtuálne zariadenie. Počas inštalácie ESMC MDM upresnite nastavenia pripojenia k databáze.
4. [Prihláste sa](#) do ESMC Web Console.
5. Vytvorte novú politiku MDM a importujte všetky certifikáty do príslušných umiestnení v rámci danej politiky.
6. **Reštartujte** službu ESMC MDM. Viac informácií nájdete v nasledujúcom [článku databázy znalostí](#).

Spravované mobilné zariadenia by sa odteraz mali pripájať na váš nový ESMC MDM Server pomocou svojho pôvodného certifikátu.

#### ❑ **Odinštalovanie starého ESMC Servera/MDM**

Keď ste si istý, že na vašom novom ESMC Serveri funguje všetko správne, opatrne odinštalujte svoj starý ESMC Server/MDM podľa našich [podrobných inštrukcií](#).

## 5.6 Aktualizácia nástroja ERA nainštalovaného na Failover klastrí na systéme Windows

Ak máte ESMC Server [nainštalovaný na Failover klastrí](#) na systéme Windows a želáte si ho aktualizovať, pokračujte podľa nasledujúcich krokov.

### **i Poznámka:**

Pojem **Rola** sa používa iba v prostredí systému Windows Server 2012 a 2016. V systéme Windows Server 2008 sa používa výraz **Služby a aplikácie**.

### **Aktualizácia z ERA 6.3 na najnovšiu verziu**

1. Zastavte klastrovú rolu vytvorenú pre službu ERA Server v Správcovi klastrov. Uistite sa, že služba **ESET Remote Administrator Server** je zastavená na všetkých klastrových uzloch.
2. Pripojte zdieľaný disk k uzlu node1 a aktualizujte ERA Server manuálne spustením najnovšieho inštalačného balíka *.msi* rovnako ako v prípade [inštalácie samostatného komponentu](#). Po dokončení inštalácie (aktualizácie) sa uistite, že služba **ESET Remote Administrator Server** je zastavená.
3. Pripojte zdieľaný disk k uzlu node2 a aktualizujte ESMC Server nainštalovaním najnovšej verzie tak ako v kroku č. 2.
4. Keď sa ESMC Server aktualizuje na všetkých klastrových uzloch, spustite klastrovú rolu vytvorenú pre službu ESMC Server v Správcovi klastrov.
5. Aktualizujte ESET Management Agentu manuálne spustením najnovšieho inštalačného balíka *.msi* na všetkých klastrových uzloch.
6. V nástroji ESMC Web Console skontrolujte, či verzie agenta a servera na všetkých uzloch ukazujú najnovšiu, aktualizovanú verziu.

[Manuálna aktualizácia nástroja ERA z verzie 6.1 alebo 6.2 na verziu 6.3](#)

## 5.7 Aktualizácia Apache HTTP Proxy

[Apache HTTP Proxy](#) je služba, ktorá môže byť používaná spolu s nástrojom ESET Security Management Center na distribúciu aktualizácií na klientske počítače a distribúciu inštalačných balíkov na ESET Management Agentu.

Ak ste nainštalovali Apache HTTP Proxy na Windows skôr a želáte si ho aktualizovať na najnovšiu verziu, máte dve možnosti vykonania aktualizácie, a to buď [manuálne](#), alebo pomocou [all-in-one inštalátora](#).

### 5.7.1 Inštrukcie pre Windows (all-in-one inštalátor)

Ak máte [ESMC all-in-one inštalátor](#) uložený na lokálnom disku, môžete použiť túto metódu pre rýchlu aktualizáciu Apache HTTP Proxy na najnovšiu verziu. Ak tento inštalátor nemáte, [manuálna aktualizácia Apache HTTP Proxy](#) je rýchlejšia.

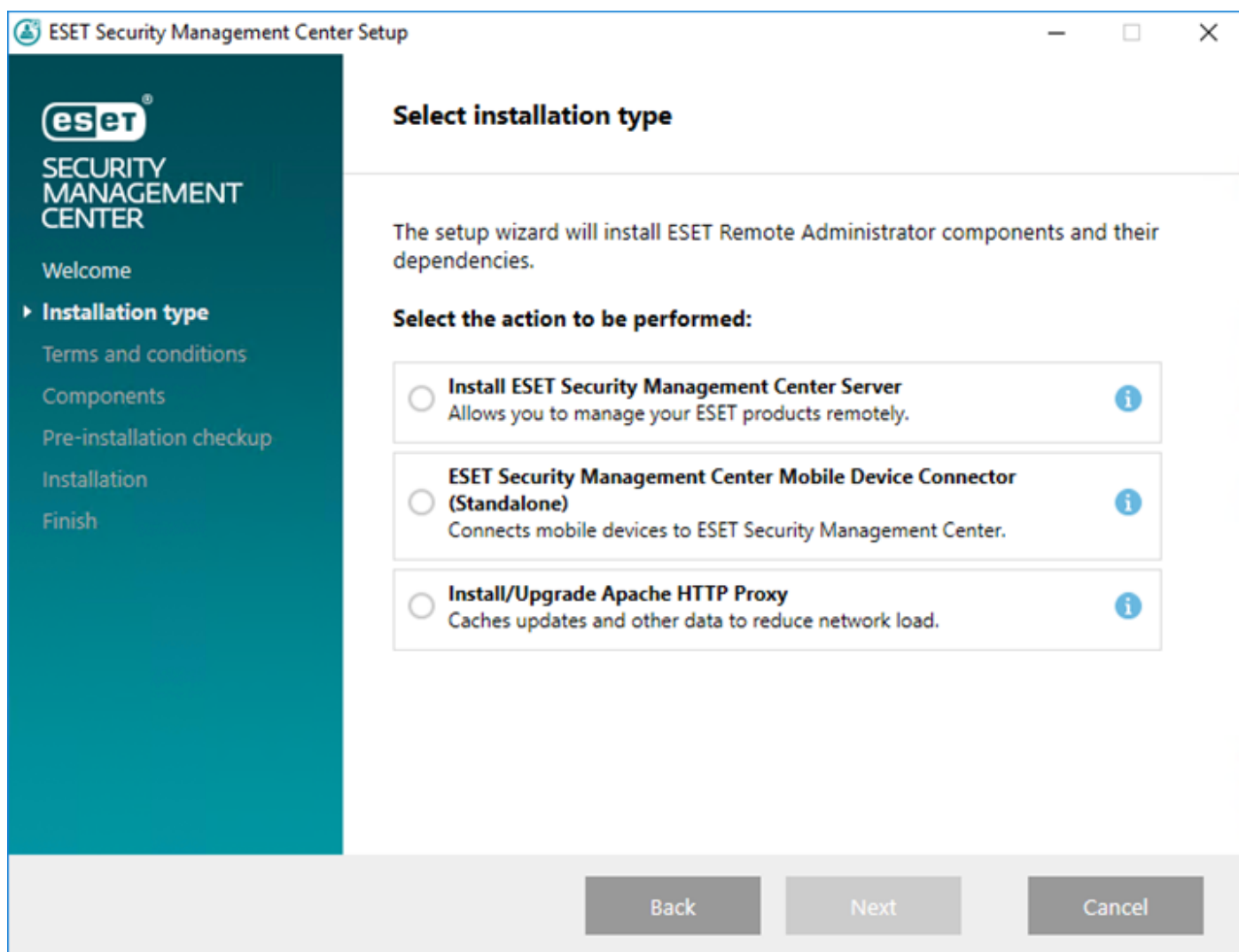
1. Zálohujte si nasledujúce súbory:

- *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf*
- *C:\Program Files\Apache HTTP Proxy\bin\password.file*
- *C:\Program Files\Apache HTTP Proxy\bin\group.file*

2. Zastavte službu **ApacheHttpProxy** otvorením [príkazového riadka s opávneniami správcu](#) a spustením nasledujúceho príkazu:

```
sc stop ApacheHttpProxy
```

3. Spustíte all-in-one inštalátor dvojitým kliknutím na súbor **setup.exe** a na úvodnej obrazovke kliknete na tlačidlo **Ďalej**.
4. Zvoľte možnosť **Inštalovať/aktualizovať Apache HTTP Proxy (náhrada mirror-a)** a kliknite na **Ďalej**.



Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**. Postupujte podľa inštrukcií na obrazovke pre dokončenie inštalácie a potom kliknite na **Dokončiť**.

Ak na prístup do Apache HTTP Proxy používate prihlasovacie meno a heslo (kapitola [Apache HTTP Proxy – inštalácia a ukladanie do vyrovnávacej pamäte](#)), nahraďte nasledujúcu časť kódu:

```
<Proxy *>
 Deny from all
</Proxy>
```

touto časťou (nachádza sa v zálohe súboru httpd.conf, vytvoreného v kroku č. 1):

```
<Proxy *>
AuthType Basic
AuthName "Password Required"
AuthUserFile password.file
AuthGroupFile group.file
Require group usergroup
Order deny,allow
Deny from all
Allow from all
</Proxy>
```

- Ak ste v súbore `httpd.conf` vykonali ďalšie zmeny na mieste vašej predchádzajúcej inštalácie Apache HTTP Proxy, môžete tieto úpravy skopírovať zo zálohovaného súboru `httpd.conf` do nového (aktualizovaného) súboru `httpd.conf`.

5. Uložte vaše zmeny a pustite službu **ApacheHttpProxy** pomocou nasledujúceho príkazu v [príkazovom riadku bez obmedzených oprávnení](#):

```
sc start ApacheHttpProxy
```

6. Otestujte pripojenie na Apache HTTP Proxy pomocou otvorenia nasledujúcej URL adresy vo vašom prehliadači:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)

V prípade riešenia problémov si pozrite [súbory protokolov Apache HTTP Proxy](#).

### 5.7.2 Inštrukcie pre Windows (manuálna aktualizácia)

Pre aktualizáciu Apache HTTP Proxy na najnovšiu verziu postupujte podľa krokov uvedených nižšie.

1. Zálohujte si nasledujúce súbory:

- `C:\Program Files\Apache HTTP Proxy\conf\httpd.conf`
- `C:\Program Files\Apache HTTP Proxy\bin\password.file`
- `C:\Program Files\Apache HTTP Proxy\bin\group.file`

2. Zastavte službu **ApacheHttpProxy** otvorením [príkazového riadka s opávneniami správcu](#) a spustením nasledujúceho príkazu:

```
sc stop ApacheHttpProxy
```

3. Stiahnite si inštalátor pre Apache HTTP Proxy zo [stránky](#) spoločnosti ESET a extrahujte obsah stiahnutého súboru do adresára `C:\Program Files\Apache HTTP Proxy\`. Pôvodné súbory počas extrahovania prepíšte.
4. Prejdite do adresára `C:\Program Files\Apache HTTP Proxy\conf`, kliknite pravým tlačidlom na súbor **httpd.conf** a z kontextového menu zvolte možnosť **Otvoriť v programe > Poznámkový blok**.
5. Na koniec súboru `httpd.conf` pridajte nasledujúci kód:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

6. Ak na prístup do Apache HTTP Proxy používate prihlasovacie meno a heslo (kapitola [Apache HTTP Proxy – inštalácia a ukladanie do vyrovnávacej pamäte](#)), nahraďte nasledujúcu časť kódu:

```
<Proxy *>
 Deny from all
</Proxy>
```

touto časťou (nachádza sa v zálohe súboru `httpd.conf`, zálohovaného v kroku č. 1):

```
<Proxy *>
 AuthType Basic
 AuthName "Password Required"
 AuthUserFile password.file
 AuthGroupFile group.file
 Require group usergroup
 Order deny,allow
 Deny from all
 Allow from all
</Proxy>
```

- Ak ste v súbore `httpd.conf` vykonali ďalšie zmeny na mieste vašej predchádzajúcej inštalácie Apache HTTP Proxy, môžete tieto úpravy skopírovať zo zálohovaného súboru `httpd.conf` do nového (aktualizovaného) súboru `httpd.conf`.

7. Uložte vaše zmeny a pustite službu **ApacheHttpProxy** pomocou nasledujúceho príkazu v [príkazovom riadku s oprávneniami správcu](#):

```
sc start ApacheHttpProxy
```

8. Otestujte pripojenie na Apache HTTP Proxy pomocou otvorenia nasledujúcej URL adresy vo vašom prehliadači:

[http://\[IP address\]:3128/index.html](http://[IP address]:3128/index.html)

V prípade riešenia problémov si pozrite [súbory protokolov Apache HTTP Proxy](#).

## 5.8 Aktualizácia Apache Tomcat

Ak prechádzate na najnovšiu verziu ESET Security Management Center alebo ste dlhší čas neaktualizovali Apache Tomcat, mali by ste zväziť aktualizáciu Apache Tomcat na najnovšiu verziu. Aktualizovanie verejne dostupných služieb, akými sú Apache Tomcat a podobne, znižuje bezpečnostné riziká pre vaše prostredie.

Pre aktualizáciu Apache Tomcat postupujte podľa inštrukcií v závislosti od vášho OS:

- [Inštrukcie pre Windows \(manuálna aktualizácia\)](#) alebo [Inštrukcie pre Windows \(all-in-one inštalátor\)](#)
- [Inštrukcie pre Linux](#)

### 5.8.1 Inštrukcie pre Windows (all-in-one inštalátor)

Ak máte [ESMC all-in-one inštalátor](#) uložený na lokálnom disku, môžete použiť túto metódu pre rýchlú aktualizáciu Apache Tomcat na najnovšiu verziu. Ak tento inštalátor nemáte, môžete si stiahnuť inštalátor pre Apache Tomcat a vykonať [manuálnu aktualizáciu](#).

V prípade, že máte all-in-one inštalátor uložený na lokálnom disku, postupujte podľa nasledujúcich inštrukcií:

#### **Upozornenie:**

Apache Tomcat podporuje aktualizácie len z verzie 7.x na verziu 7.x prostredníctvom ESMC all-in-one inštalátora vo verzii 6.3.12 a starších.



## ☐ Predtým, ako začnete s aktualizáciou

1. Uistite sa, že Java je na vašom systéme správne aktualizovaná. Pozrite si inštrukcie na [webovej stránke Javy](#).
2. Skontrolujte, aká verzia Apache Tomcat sa momentálne používa. Ak je dostupná novšia verzia, vykonajte aktualizáciu:
  - a. Otvorte dialógové okno Spustiť, zadajte `services.msc` a kliknite na **OK**.
  - b. Pravým tlačidlom kliknite na službu **Apache Tomcat**, vyberte možnosť **Vlastnosti** a na karte **Všeobecné** uvidíte číslo verzie (napr. 7.0.90).
3. Pozrite si náš zoznam [podporovaných verzií Apache Tomcat](#) a overte si, či je nová verzia kompatibilná s produktmi spoločnosti ESET.

## ☐ Ako vykonať aktualizáciu

1. Zastavte službu Apache Tomcat a ukončíte proces `Tomcat7w.exe`:
  - a. Otvorte dialógové okno Spustiť, zadajte `services.msc` a kliknite na **OK**.
  - b. Pravým tlačidlom kliknite na službu Apache Tomcat a kliknite na **Zastaviť**.
  - c. Na paneli úloh ukončíte proces `Tomcat7w.exe`.
2. Zálohujte si nasledujúce súbory (v niektorých prípadoch je názov priečinka *Tomcat 8.0*):  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\.keystore`  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\conf\server.xml`  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`
3. Z webovej stránky <http://tomcat.apache.org> si stiahnite inštalačný súbor (32-bitový/64-bitový inštalátor služieb pre systém Windows) `apache-tomcat-[verzia].exe` pre najnovšiu podporovanú verziu Apache Tomcat.
4. Odinštalujte vašu súčasnú verziu Apache Tomcat.
5. Vymažte nasledujúci priečinok v prípade, že sa ešte stále nachádza na vašom systéme:  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\`
6. Prejdite do priečinka, kde ste uložili all-in-one inštalátor.
7. Skopírujte `apache-tomcat-[verzia].exe` do adresára `./win32/installers` alebo `./x64/installers`. Starý inštalačný súbor Tomcat z tohto adresára vymažte.
8. Otvorte príkazový riadok, prejdite do priečinka all-in-one inštalátora a spustíte nasledujúci príkaz:  
`Setup.exe --mode webconsole`
9. V inštalačnom okne vyberte možnosť ESMC Web Console a kliknite na **Ďalej**.
10. Po odsúhlasení Licenčnej dohody s koncovým používateľom kliknite na **Ďalej**.
11. V okne súčastí (komponentov) kliknite na **Inštalovať**.
12. Obnovte súbory `.keystore`, `server.xml` a `EraWebServerConfig.properties` do ich pôvodného umiestnenia.
13. [Pripojte sa do ESMC Web Console](#) a uistite sa, že program funguje správne.

## 5.8.2 Inštrukcie pre Windows (manuálna aktualizácia)

V prípade, že nemáte ESET all-in-one inštalátor, postupujte podľa inštrukcií v tejto kapitole.

### ☐ Predtým, ako začnete s aktualizáciou

1. Uistite sa, že Java je na vašom systéme správne aktualizovaná. Pozrite si inštrukcie na [webovej stránke Javy](#).
2. Skontrolujte, aká verzia Apache Tomcat sa momentálne používa. Ak je dostupná novšia verzia, vykonajte aktualizáciu:
  - a. Otvorte dialógové okno Spustiť, zadajte `services.msc` a kliknite na **OK**.
  - b. Pravým tlačidlom kliknite na službu **Apache Tomcat**, vyberte možnosť **Vlastnosti** a na karte **Všeobecné** uvidíte číslo verzie (napr. 7.0.90).
3. Pozrite si náš zoznam [podporovaných verzií Apache Tomcat](#) a overte si, či je nová verzia kompatibilná s produktmi spoločnosti ESET.

### ☐ Ako vykonať aktualizáciu

1. Zastavte službu Apache Tomcat a ukončíte proces `Tomcat7w.exe`:
  - a. Otvorte dialógové okno Spustiť, zadajte `services.msc` a kliknite na **OK**.
  - b. Pravým tlačidlom kliknite na službu Apache Tomcat a kliknite na **Zastaviť**.
  - c. Na paneli úloh ukončíte proces `Tomcat7w.exe`.
2. Zálohujte si nasledujúce súbory (v niektorých prípadoch je názov priečinka *Tomcat 8.0*):  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\keystore`  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\conf\server.xml`  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties`
3. Z webovej stránky <http://tomcat.apache.org> si stiahnite inštalačný súbor (32-bitový/64-bitový inštalátor služieb pre systém Windows) `apache-tomcat-[verzia].exe` pre najnovšiu podporovanú verziu Apache Tomcat.
4. Odinštalujte vašu súčasnú verziu Apache Tomcat.
5. Vymažte nasledujúci priečinok v prípade, že sa ešte stále nachádza na vašom systéme:  
`C:\Program Files (x86)\Apache Software Foundation\Tomcat 7.0\`
6. Nainštalujte novú verziu Apache Tomcat, ktorú ste stiahli.
7. Po ukončení inštalácie zrušte výber začiarkavacieho políčka pre **Run Apache Tomcat**.
8. Obnovte zálohovaný `keystore` a `server.xml` do ich pôvodného umiestnenia (toto je možné len pri aktualizácii v rámci hlavnej verzie Apache Tomcat, napr. pri aktualizácii z verzie 7.x na verziu 7.x alebo z verzie 8.x na verziu 8.x). Môžete tiež prípadne manuálne nastaviť [HTTPS pripojenie pre Apache Tomcat](#) v rámci ESMC Web Console podľa inštrukcií, ktoré nájdete v databáze znalostí (odporúčané).
9. Nasadte ESMC Web Console podľa kapitoly [Inštalácia Web Console – Windows](#).
10. Obnovte `EraWebServerConfig.properties` do pôvodného umiestnenia.
11. Spustite Apache Tomcat a nastavte správnu verziu Java VM:
  - Kliknite na **Štart > Všetky programy > Apache Tomcat > Monitor Tomcat** a na karte **General** kliknite na **Start**.
  - Kliknite na kartu **Java**, zaškrtnite začiarkavacie políčko vedľa **Use default** a kliknite na **OK**. Pre viac informácií si pozrite [inštrukcie databázy znalostí](#).
12. [Pripojte sa do ESMC Web Console](#) a uistite sa, že program funguje správne.

## ☐ Riešenie problémov

- Ak sa vám nedarí nastaviť HTTPS pripojenie pre Apache Tomcat, môžete tento krok preskočiť a dočasne použiť HTTP pripojenie.
- Ak sa vám nedarí aktualizovať Apache Tomcat, nainštalujte vašu pôvodnú verziu a použite nastavenia z kroku č. 2.

### 5.8.3 Inštrukcie pre Linux

#### ☐ Predtým, ako aktualizujete Apache Tomcat

1. Uistite sa, že sa Java na vašom systéme aktualizuje správne.
  - Overte, či bol balík *openjdk* aktualizovaný (pozrite si tabuľku nižšie).
2. Skontrolujte, aká verzia Apache Tomcat sa momentálne používa. Ak je dostupná novšia verzia, vykonajte aktualizáciu:
  - Zadajte nasledujúci príkaz: `cd /usr/share/tomcat/bin && ./version.sh` (v niektorých prípadoch je názov priečinka `tomcat7` alebo `tomcat8`).
3. Pozrite si náš zoznam [podporovaných verzií Apache Tomcat](#) a overte si, či je nová verzia kompatibilná s produktmi spoločnosti ESET.
4. Zálohujte si konfiguračný súbor Tomcat `/etc/tomcat7/server.xml`.

#### ☐ Ako vykonať aktualizáciu

1. Zastavte službu Apache Tomcat:
  - Zadajte nasledujúci príkaz: `service tomcat stop` (v niektorých prípadoch je názov služby `tomcat7` alebo `tomcat8`).
2. Aktualizujte Apache Tomcat a Javu podľa používanej distribúcie systému Linux. V termináli spustíte nasledujúce príkazy:

|                                      |                                                                           |
|--------------------------------------|---------------------------------------------------------------------------|
| Debian a Ubuntu distribúcie          | <pre>sudo apt-get update sudo apt-get install openjdk-8-jdk tomcat7</pre> |
| CentOS, Red Hat a Fedora distribúcie | <pre>yum update yum install java-1.8.0-openjdk tomcat</pre>               |
| OpenSUSE                             | <pre>zypper refresh zypper install java-1_8_0-openjdk tomcat</pre>        |

3. Obnovte konfiguračný súbor Tomcat `server.xml` zo svojej zálohy.

#### ⚠ Dôležité:

Po aktualizácii Apache Tomcat na novšiu hlavnú verziu (napr. z verzie 7.x na 8.x):

- Pre zachovanie vlastných nastavení v ESMC Web Console znova nasadíte ESMC Web Console (pozrite si kapitolu [Inštalácia ESMC Web Console – Linux](#)) a použite súbor `%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties`.
- Pre Apache Tomcat nastavte [HTTPS pripojenie](#).

## 5.9 Zmena názvu hostiteľa alebo IP adresy ESMC Servera

Pre zmenu názvu hostiteľa alebo IP adresy vášho ESMC Servera postupujte podľa nasledujúcich krokov:

1. Ak certifikát vášho ESMC Servera obsahuje konkrétnu IP adresu a/alebo názov hostiteľa, [vytvorte nový certifikát servera](#) a použite danú IP adresu alebo názov hostiteľa. V prípade, že pre certifikát servera používate hviezdičku (\*) v poli „Hostiteľ“, **prejdite na krok č. 2**. Ak nie, vytvorte nový certifikát servera, použite novú IP adresu a názov hostiteľa (oddeľte ich čiarkou), pričom pridajte aj predošlú IP adresu a názov hostiteľa.
2. Nový certifikát podpíšte pomocou certifikačnej authority ESMC Servera.
3. Vytvorte politiku, pomocou ktorej zmeníte pripojenie klientov na novú IP adresu alebo názov hostiteľa (pokiaľ možno IP adresu). Pridajte aj alternatívne pripojenie na starú IP adresu alebo názov hostiteľa, aby sa mohol ESET Management Agent pripojiť na oba servery. Viac informácií nájdete v časti [Vytvorenie politiky pre pripojenie ESET Management Agentu na nový ESMC Server](#).
4. Aplikujte túto politiku na vaše klientske počítače a počkajte, kým prebehne replikácia ESET Management Agentov. Napriek tomu, že politika presmeruje klientov na nový server, ktorý nie je spustený, ESET Management Agenty budú používať na pripojenie na pôvodnú IP adresu alternatívny server.
5. [V nastaveniach servera nastavte váš nový certifikát servera](#).
6. Reštartujte službu ESMC Server a zmeňte IP adresu alebo názov hostiteľa.

Podrobné inštrukcie týkajúce sa zmeny IP adresy ESMC Servera nájdete v našom [článku databázy znalostí](#).

## 5.10 Aktualizácia nástroja ERA nainštalovaného na Failover klastrí na systéme Linux

Ak máte ESMC Server nainštalovaný na [Failover klastrí na systéme Linux](#) a želáte si ho aktualizovať, pokračujte podľa nasledujúcich krokov.

### [Vykonanie aktualizácie v prostredí s ERA Proxy](#)

#### Manuálna aktualizácia z verzie ERA 6.3 (a novšej) na najnovšiu verziu ESMC

1. V nástroji Conga (grafické používateľské rozhranie na správu klastrov) deaktivujte službu *EraService* v rámci **Service groups** a overte, či sú služby ERA Agent a ERA Server zastavené na oboch uzloch.
2. Aktualizujte komponent ESMC Server na uzle node1 podľa nasledujúcich pokynov:
  - a. Pripojte k tomuto uzlu zdieľané úložisko.
  - b. Manuálne aktualizujte komponent ERA Server na najnovšiu verziu spustením inštalačného skriptu `Server-Linux-x86_64.sh` s oprávneniami root alebo sudo.
  - c. Pôvodný skript klastra umiestnený v `/usr/share/cluster/eracluster_server.sh` nahraďte novým skriptom z priečinka `/opt/eset/RemoteAdministrator/Server/setup/eracluster_server`. Nemeňte názov súboru `eracluster_server.sh`.
  - d. Po skončení aktualizácie zastavte službu ERA Server (`stop eraserver`).
  - e. Deaktivujte samospúšťanie služby ERA Server premenovaním týchto dvoch súborov:
    - i. `mv /etc/init/eraserver.conf /etc/init/eraserver.conf.disabled`
    - ii. `mv /etc/init/eraserver-xvfb.conf /etc/init/eraserver-xvfb.conf.disabled`
  - f. Odpojte zdieľané úložisko z uzla node1.
3. Vyššie uvedené kroky zopakujte aj pre aktualizovanie ERA Servera na uzle node2.
4. V nástroji Conga (grafické používateľské rozhranie na správu klastrov) spustite v rámci skupín služieb *EraService*.
5. Aktualizujte komponent **ESET Management Agent** na všetkých klastrových uzloch.
6. V ESMC Web Console skontrolujte pripojenie jednotlivých uzlov a tiež to, či sa skutočne zobrazuje najnovšia verzia.

### [Manuálna aktualizácia z verzie 6.1 alebo 6.2 na verziu 6.3](#)

## 6. Riešenie problémov

ESET Security Management Center je komplexný produkt, ktorý využíva mnoho nástrojov tretích strán a podporuje niekoľko platforiem OS. Táto skutočnosť predstavuje potenciál, že sa stretnete s problémami, ktoré bude nutné odstrániť.

Dokumentácia spoločnosti ESET popisuje viacero metód riešenia problémov s nástrojom ESET Security Management Center. Riešenia najčastejších problémov s nástrojom ESET Security Management Center nájdete v kapitole [Najčastejšie problémy s inštaláciou](#).

### Neviete nájsť riešenie vášho problému?

- Každý komponent ESMC má svoj [protokol](#) s nastaviteľnou úrovňou zapisovania. Pomocou týchto protokolov môžete identifikovať problémy, prípadne dôjsť k vysvetleniu príčiny daného problému.
  - Úroveň zapisovania do protokolu pre jednotlivé komponenty sa nastavuje prostredníctvom [politiky](#) pre konkrétny komponent. Aby politika nadobudla účinnosť, musí byť aplikovaná na zariadenie.
    - [Politika pre ESET Management Agentu](#)
    - [RD Sensor](#)
    - [ESMC Server](#)
    - MDM Core
- Ak nedokážete vyriešiť váš problém, môžete navštíviť [bezpečnostné fórum spoločnosti ESET](#) a konzultovať konkrétny problém s komunitou ESET.
- Pri kontaktovaní [technickej podpory spoločnosti ESET](#) môžete byť požiadaný o poskytnutie protokolov. Získať potrebné protokoly môžete pomocou nástroja [ESET Log Collector](#) alebo prostredníctvom [Diagnostického nástroja](#). Dôrazne odporúčame, aby ste protokoly priložili už pri prvom kontaktovaní technickej podpory. Skrátime tým vybavovanie vašej požiadavky.

### 6.1 Aktualizácia komponentov ESMC v offline prostredí

Postupujte podľa nasledujúcich krokov, ak si prajete aktualizovať komponenty ESMC alebo produkty ESET určené pre koncové zariadenia bez prístupu na internet:

#### Dôležité:

V offline prostredí je možné použiť [úlohu pre aktualizáciu súčastí](#) len v prípade, že sú splnené nasledujúce požiadavky:

- k dispozícii je [offline repozitár](#),
- ako umiestnenie repozitára pre ESET Management Agentu je vybraná prístupná lokalita nastavená prostredníctvom [politiky](#).

1. Najskôr aktualizujte ESMC Server a Web Console:
  - a. [Skontrolujte, ktorá verzia nástroja ESMC](#) je spustená na serveri.
  - b. Skontrolujte dostupnosť [nových verzií komponentov ESMC](#).
  - c. Stiahnite si najnovšie samostatné inštalátory pre jednotlivé komponenty z [webovej stránky spoločnosti ESET](#).
  - d. [Vykonajte manuálnu aktualizáciu komponentov](#) ESMC Server a ESMC Web Console.
2. Teraz môžete prísť k offline aktualizácii bezpečnostných produktov ESET nainštalovaných na koncových pracovných staniciach:
  - a. Zistite, aké produkty sú nainštalované na klientskych zariadeniach: Otvorte ESMC Web Console a prejdite do sekcie **Riadiaci panel > ESET aplikácie**.
  - b. Skontrolujte dostupnosť [najnovších verzií produktov ESET určených pre koncové zariadenia](#).
  - c. Z [webovej stránky spoločnosti ESET](#) si stiahnite inštaláčne súbory do lokálneho repozitára, ktorý ste nakonfigurovali počas [offline inštalácie](#).
  - d. Spustite [úlohu pre inštaláciu softvéru](#) v ESMC Web Console.

## 6.2 Najčastejšie problémy s inštaláciou

Rozbalte príslušnú sekciu pre zobrazenie chybového hlásenia, ktoré chcete vyriešiť.

### ESMC Server

Služba ESMC Server sa nechce spustiť:

#### Poškodená inštalácia

Môže to byť zapríčinené chýbajúcimi kľúčmi v registri, chýbajúcimi súbormi alebo neplatnými povoleniami pre prístup k súborom.

All-in-one ESET inštalátor má [vlastný súbor protokolu](#). Ak inštalujete komponent manuálne, použite [MSI protokolovanie](#).

#### Port 2222 a 2223 sa už používa

Použite príslušný príkaz pre váš operačný systém:

- Windows:  

```
netstat -an | find "2222"
netstat -an | find "2223"
```
- Linux:  

```
netstat | grep 2222
netstat | grep 2223
```

#### Databáza nie je spustená/dostupná

- MS SQL Server: Overte, či je port 1433 dostupný pre databázový server, prípadne sa skúste prihlásiť prostredníctvom SQL Server Management Studio.
- MySQL: Overte, či je port 3306 dostupný pre databázový server, prípadne sa skúste prihlásiť do vášho databázového rozhrania (napr. prostredníctvom príkazového riadku MySQL alebo pomocou `phpmyadmin`).

#### Poškodená databáza

V prípade poškodenia databázy sa v súbore protokolu ESMC Servera zobrazí väčšie množstvo chýb. Odporúčame, aby ste si obnovili databázu zo zálohy. Ak zálohu nemáte, preinštalujte ESET Security Management Center.

#### Nedostatok systémových prostriedkov (RAM, miesto na disku)

Skontrolujte spustené procesy a výkon/zaťaženie systému:

- Používatelia systému Windows: pozrite sa do Správcu úloh, prípadne do Zobrazovača udalostí.
- Používatelia systému Linux môžu spustiť niektoré z nasledujúcich príkazov:  

```
df -h (pre informácie o voľnom mieste na disku)
cat /proc/meminfo (pre informácie o využití operačnej pamäte)
dmesg (pre informácie o stave systému Linux)
```

#### Chyba ODBC konektoru počas inštalácie ESMC Servera

Error: (Error 65533) ODBC connector compatibility check failed.  
Please install ODBC driver with support for multi-threading.

Nainštalujte ODBC ovládač, ktorý podporuje multi-threading (súbežné spracovanie vlákien) alebo prekonfigurujte súbor `odbcinst.ini` podľa kapitoly [Inštalácia a konfigurácia ODBC](#).

## Chyba pripojenia do databázy počas inštalácie ESMC Servera

Inštalácia ESMC Servera skončí všeobecným chybovým hlásením:

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

Chybové hlásenie v inštalačnom protokole:

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group
value 100663296 is too low.
```

Skontrolujte, či sa konfigurácia vášho databázového ovládača zhoduje s tým, čo je uvedené v kapitole [Inštalácia a konfigurácia ODBC ovládača](#).

### ☐ ESET Management Agent

#### Chybové hlásenie „Databázu nie je možné aktualizovať. Prosím, najprv odinštalujte produkt.“ sa zobrazuje počas odinštalovania agenta.

Oprava ESET Management Agenta:

1. Prejdite do **Ovládací panel > Programy a súčasti** a dvojitým kliknutím vyberte **ESET Management Agent**.
2. Kliknite na **Ďalej > Opraviť** a postupujte podľa inštrukcií.

#### Existujú aj iné možnosti odinštalovania ESET Management Agentu?

Všetky možnosti odinštalovania ESET Management Agentu sú popísané v [tejto kapitole](#).

#### Počas inštalácie agenta nastala chyba s kódom 1603

Táto chyba môže nastať vtedy, keď sa inštalačné súbory nenachádzajú na lokálnom disku. Riešením je skopírovať inštalačné súbory do lokálneho adresára a opätovne spustiť inštaláciu. Ak sa súbory na disku už nachádzajú alebo problém pretrváva, postupujte podľa inštrukcií [v článku databázy znalostí](#).

#### Počas inštalácie agenta na systéme Linux sa zobrazuje chybové hlásenie

Chybové hlásenie:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Možnou príčinou tohto problému je nesprávny názov súboru v inštalačnom príkaze. Majte na pamäti, že konzola rozlišuje veľké a malé písmená. Napríklad „Agent.pfx“ nie je to isté ako „agent.pfx“.

#### Vzdialené nasadenie zo systému Linux na Windows 8,1 (32-bitová verzia) zlyhalo

Ide o problém overovania spôsobený aktualizáciou KB3161949 od spoločnosti Microsoft. Jediným riešením je odstránenie tejto aktualizácie z počítačov, na ktorých nasadenie zlyháva.

### ☐ Web Console

#### Ako adresovať nasledujúce chybové hlásenia vo Web Console?

Prihlásenie zlyhalo: Pripojenie zlyhalo so stavom „Nepripojený“?

Skontrolujte, či je spustená služba ESMC Server a služba databázy. Tiež skontrolujte, či pripojenie nie je narušené. Ak tieto služby nie sú spustené, [reštartujte ich](#), obnovte stránku Web Console a skúste sa znova prihlásiť. Pre viac informácií skontrolujte súbory protokolu vašej služby databázy (MS SQL, MySQL).



Prihlásenie zlyhalo: Chyba komunikácie

Overte si, či Apache Tomcat funguje správne. Môžete tiež prípadne pre Apache Tomcat skontrolovať [súbory protokolu](#).

Pre viac informácií o tomto probléme si prečítajte nasledujúci [článok databázy znalostí](#).

### ESET Security Management Center Web Console sa nechce načítať

V prípadoch, keď sa ESET Security Management Center Web Console (ESMC Web Console) nenačíta alebo sa načítava príliš dlho a bez úspechu, postupujte podľa [inštrukcií databázy znalostí](#).

### Ako nastaviť HTTPS/SSL pripojenie do Web Console?

Chybové hlásenie:

Používate nešifrované pripojenie! Upravte, prosím, konfiguráciu webového servera tak, aby používal HTTPS

Ak máte problémy s HTTPS pripojením do Web Console, prečítajte si článok o [nastavení pripojenia HTTPS/SSL](#).

### Apache Tomcat nedokáže extrahovať obsah zo súboru 'era.war'

Chyba: Po nainštalovaní súčastí ESMC prostredníctvom all-in-one inštalátora sa súbor era.war neextrahuje a prístup do Web Console nie je možný. Pre vyriešenie tohto problému postupujte podľa inštrukcií v nasledujúcom [článku databázy znalostí](#).

## ☐ Apache HTTP Proxy

### Veľkosť vyrovnávacej pamäte má už niekoľko GB a stále rastie

Ak ste Apache HTTP Proxy inštalovali pomocou all-in-one inštalátora, je nastavené pravidelné čistenie. Ak čistenie nepracuje správne, [vykonajte čistenie manuálne alebo naplánujte úlohu čistenia](#).

### Aktualizácie detekčného jadra po inštalácii Apache HTTP Proxy nefungujú

Ak sa klientske stanice neaktualizujú, postupujte podľa databázy znalostí pre dočasné [deaktivovanie Apache HTTP Proxy na koncových stanicach](#). Po odstránení problémov s pripojením zvážte opätovné povolenie Apache HTTP Proxy.

### Vzdialená aktualizácia ESET Management Agent sa skončila chybou s kódom 20008

Vzdialená aktualizácia ESET Management Agent sa skončila nasledujúcim chybovým hlásením:  
*GetFile: Failed to process the HTTP request (error code 20008, url: 'http://repository.eset.com/v1//info.meta')*

V tomto prípade postupujte podľa inštrukcií v [kroku I - III v nasledujúcom článku databázy znalostí](#) pre vyriešenie problému s pripojením. Ak je počítač, na ktorom sa má aktualizovať ESET Management Agent, mimo dosahu vašej podnikovej siete, nastavte politiku pre tohto ESET Management Agent tak, aby na pripojenie do repozitára nepoužíval proxy server v prípadoch, keď je mimo dosahu podnikovej siete.

## ☐ ESET Rogue Detection Sensor

### Prečo sa v protokole služby ESET Rogue Detection Sensor (trace.log) neustále objavuje nasledujúce chybové hlásenie?

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} threw error:
Device open failed with error:Error opening adapter:
The system cannot find the device specified. (20)
```

Ide o problém s WinPcap. Zastavte službu ESET Rogue Detection Sensor, preinštalujte najnovšiu verziu WinPcap (aspoň 4.1.0) a reštartujte službu ESET Rogue Detection Sensor .

## Linux

### Chýbajúce závislosti libQtWebKit na systéme CentOS Linux

V prípade chybového hlásenia:

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

postupujte podľa inštrukcií v našom [článku databázy znalostí](#).

### Inštalácia služby ESMC Server na systéme CentOS 7 zlyhala

V prípade chybového hlásenia:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

je pravdepodobnou príčinou chybná konfigurácia lokálneho prostredia. Spustite nižšie uvedený skript a pokúste sa inštaláciu vykonať znova:

```
export LC_ALL="en_US.UTF-8"
```

## Microsoft SQL Server

### Počas inštalácie Microsoft SQL Server sa zobrazí chybové hlásenie -2068052081.

Reštartujte počítač a spustite inštaláciu znova. Ak problém pretrváva, odinštalujte SQL Server Native Client a spustite inštaláciu znova. Ak sa vám stále nepodarilo vyriešiť problém, odinštalujte všetky produkty Microsoft SQL Server, reštartujte počítač a spustite inštaláciu znova.

### Počas inštalácie Microsoft SQL Server sa zobrazí chybové hlásenie -2067922943.

Overte si, či váš systém spĺňa [požiadavky na databázu](#) pre ESMC.

### Počas inštalácie Microsoft SQL Server sa zobrazí chybové hlásenie -2067922934.

Uistite sa, že máte tie správne [oprávnenia pre používateľský účet](#).

### Web Console zobrazuje chybové hlásenie „Načítanie dát zlyhalo“.

MS SQL Server sa snaží využívať všetok dostupný priestor na disku na ukladanie protokolov transakcií. Ak chcete tieto súbory na disku prečistiť, [navštívte oficiálnu stránku spoločnosti Microsoft](#).

### Počas inštalácie Microsoft SQL Server sa zobrazí chybové hlásenie -2067919934.

Uistite sa, že všetky predchádzajúce kroky boli vykonané a dokončené správne. Tato chyba je zapríčinená nesprávnou konfiguráciou systémových súborov. Reštartujte počítač a spustite inštaláciu znova.

## 6.3 Protokoly

Každý komponent nástroja ESET Security Management Center vykonáva zapisovanie do protokolu. Komponenty ESMC zapisujú do protokolov informácie o určitých udalostiach. Umiestnenie protokolov závisí od konkrétneho komponentu. Nižšie je uvedený zoznam umiestnení protokolov:

### Windows

|                                          |                                                                                                                                                                                                          |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESMC Server                              | C:<br>\\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs\                                                                                                                       |
| ESET Management Agent                    | C:<br>\\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\                                                                                                                         |
| ESMC Web Console a Apache Tomcat         | C:\Program Files\Apache Software Foundation\Tomcat 7.0\Logs<br>Pozrite si tiež <a href="https://tomcat.apache.org/tomcat-7.0-doc/logging.html">https://tomcat.apache.org/tomcat-7.0-doc/logging.html</a> |
| Mobile Device Connector                  | C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs\                                                                                                                                                    |
| Rogue Detection Sensor                   | C:\ProgramData\ESET\Rogue Detection Sensor\Logs\                                                                                                                                                         |
| Apache HTTP Proxy                        | C:\Program Files\Apache HTTP Proxy\logs\<br>C:\Program Files\Apache HTTP Proxy\logs\errorlog                                                                                                             |
| Na starších operačných systémoch Windows | C:\Documents and Settings\All Users\Application Data\ESET\...                                                                                                                                            |

#### Poznámka:

C:\ProgramData je podľa predvolených nastavení skrytý priečinok.  Pre jeho zobrazenie...

1. Prejdite do **Štart > Ovládací panel > Možnosti priečinka > Zobrazenie**.
2. Vyberte možnosť **Zobrazíť skryté súbory a priečinky** a kliknite na **OK**.

### Linux

|                                  |                                                                                                                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESMC Server                      | /var/log/eset/RemoteAdministrator/Server/<br>/var/log/eset/RemoteAdministrator/EraServerInstaller.log                                                                                  |
| ESET Management Agent            | /var/log/eset/RemoteAdministrator/Agent/<br>/var/log/eset/RemoteAdministrator/EraAgentInstaller.log                                                                                    |
| Mobile Device Connector          | /var/log/eset/RemoteAdministrator/MDMCore/<br>/var/log/eset/RemoteAdministrator/MDMCore/Proxy/                                                                                         |
| Apache HTTP Proxy                | /var/log/httpd/                                                                                                                                                                        |
| ESMC Web Console a Apache Tomcat | /var/log/tomcat7/ alebo /var/log/tomcat8/<br>Pozrite si tiež <a href="https://tomcat.apache.org/tomcat-7.0-doc/logging.html">https://tomcat.apache.org/tomcat-7.0-doc/logging.html</a> |
| ESMC RD Sensor                   | /var/log/eset/RogueDetectionSensor/                                                                                                                                                    |

## Virtuálne zariadenie ESMC

|                      |                                                                 |
|----------------------|-----------------------------------------------------------------|
| Konfigurácia ESMC VA | <i>/root/appliance-configuration-log.txt</i>                    |
| ESMC Server          | <i>/var/log/eset/RemoteAdministrator/EraServerInstaller.log</i> |
| Apache HTTP Proxy    | <i>/var/log/httpd</i>                                           |

### macOS

*/Library/Application Support/com.eset.remoteadministrator.agent/Logs/  
/Users/%user%/Library/Logs/EraAgentInstaller.log*

## 6.4 Diagnostický nástroj

Diagnostický nástroj je súčasťou všetkých ESMC komponentov. Používa sa na zhromažďovanie a kompresiu protokolov, ktoré môžu pomôcť technickej podpore a vývojárom spoločnosti ESET vyriešiť problémy s komponentmi produktov.

**Diagnostický nástroj nájdete v nasledujúcom umiestnení:**

### Windows

V priečinku *C:\Program Files\ESET\RemoteAdministrator\<produkt>* nájdete súbor **Diagnostic.exe**.

### Linux

V adresári */opt/eset/RemoteAdministrator/<produkt>/* nájdete spustiteľný súbor **Diagnostic<produkt>** (jedno slovo, napr. **DiagnosticServer**, **DiagnosticAgent** a pod.).

### Použitie (Linux)

Spustite diagnostický spustiteľný súbor v termináli ako root používateľ a postupujte podľa pokynov na obrazovke.

### Použitie (Windows)

1. Spustíte nástroj pomocou príkazového riadka.
2. Zadáte cestu pre ukladanie protokolov (v našom príklade je to priečinok „logs“) a stlačíte **Enter**.
3. Zadáte informácie, ktoré chcete zhromažďovať (v našom príklade `1 trace status 3`). Pre viac informácií si pozrite časť **Akcie** nižšie v tejto kapitole.

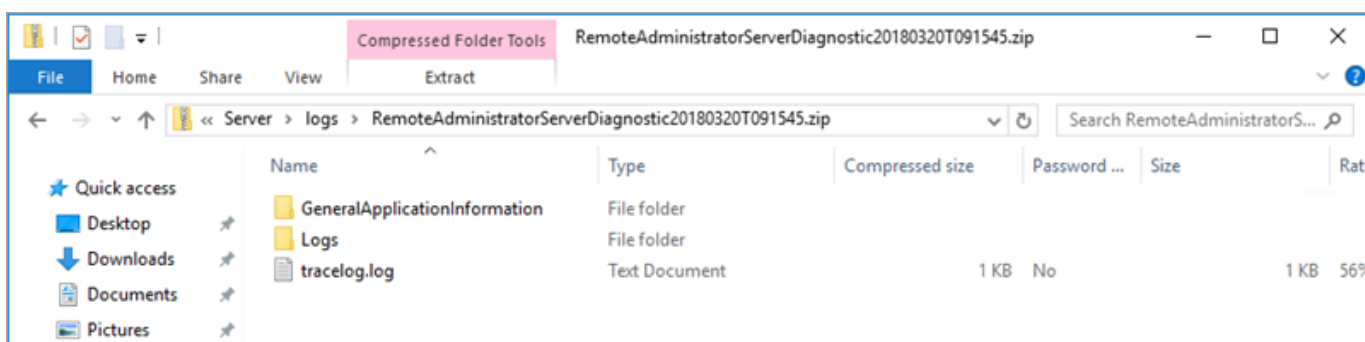
```

Administrator: Command Prompt
C:\Program Files\ESET\RemoteAdministrator\Server>Diagnostic.exe
Starting diagnostics for product type: Server
Provide path to folder, where ZIP file will be stored: logs
Actions:
1. ActionEraLogs. Get product logs. Specific log can be selected with options: trace,status,last-error,avremo
ver,software-install,software-uninstall,ra-upgrade-agent,ra-upgrade-infrastructure,ra-agent-uninstall.
2. ActionGetDumps. Dump process and get already created dumps.
3. ActionGeneralApplicationInformation. Get general application information.
4. ActionConfiguration. Get configuration.
Provide actions (numbers) and options (specified in actions) separated by spaces (example: 1 trace status 3):
1 trace status 3
Executing all actions.
Action: ActionEraLogs started.
Action: ActionEraLogs successfully finished.
Action: ActionGeneralApplicationInformation started.
Action: ActionGeneralApplicationInformation successfully finished.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation started.
Zip file: logs\RemoteAdministratorServerDiagnostic20180320T091545.zip creation finished.

C:\Program Files\ESET\RemoteAdministrator\Server>_

```

- Po dokončení môžete nájsť protokoly skomprimované v .zip súbore v adresári „logs“ v umiestnení Diagnostického nástroja.



## Akcie

- **ActionEraLogs** – vytvorí nový priečinok, do ktorého budú ukladané všetky protokoly. Pre špecifikovanie konkrétnych protokolov použite na ich oddelenie medzeru.
- **ActionGetDumps** – vytvorí sa nový priečinok. Dump súbor sa vo všeobecnosti vytvorí v prípade, že nastal problém. Ak sa vyskytne kritický problém, systém vytvorí dump súbor. Nájdete ho v súbore %temp% (Windows) alebo v súbore /tmp/ (Linux).

### Poznámka:

Počas získavania týchto dát musí byť služba komponentov (Agent, Server, RD Sensor) spustená.

- **ActionGeneralApplicationInformation** – vytvorí sa priečinok GeneralApplicationInformation a v ňom sa vytvorí súbor GeneralApplicationInformation.txt. Tento súbor obsahuje informácie o aktuálne nainštalovanom produkte spoločnosti ESET vrátane verzie.
- **ActionConfiguration** – vytvorí sa konfiguračný priečinok v umiestnení, kde je uložený súbor storage.lua.

## 6.5 Problémy po aktualizácii/migrácii ESMC Servera

V prípade, že nemôžete spustiť službu ESET Security Management Center Server z dôvodu poškodenej inštalácie a v protokole ste nenašli žiadne relevantné chybové hlásenia, vykonajte opravu podľa krokov uvedených nižšie:

### **Upozornenie:**

Odporúčame, aby ste pred samotnou opravou urobili [zálohu databázového servera](#).

1. Prejdite do **Štart > Ovládací panel > Programy a súčasti** a dvojitým kliknutím vyberte **ESET Security Management Center**.
2. Vyberte možnosť **Opraviť** a kliknite na **Ďalej**.
3. Použite vaše existujúce nastavenia pripojenia na databázu a kliknite na **Ďalej**. V prípade, že bude potrebné potvrdenie, kliknite na **Áno**.
4. Vyberte možnosť **Použite heslo správcu, ktoré je už uložené v databáze** a kliknite na **Ďalej**.
5. Vyberte možnosť **Ponechať aktuálne používané certifikáty** a kliknite na **Ďalej**.
6. Kliknite na **Opraviť**.
7. [Prihláste sa do Web Console](#) a skontrolujte, či je všetko v poriadku.

Ďalšie scenáre:

### **ESMC Server nebeží, ale máte zálohu databázy:**

1. Obnovte [zálohu databázy](#).
2. Uistite sa, že nový server používa rovnakú IP adresu alebo názov hostiteľa ako pôvodný, aby sa mohli agenti pripojiť.
3. Vykonajte opravnú inštaláciu ESMC Servera a použite obnovenú databázu.

### **ESMC Server nie je spustený, ale exportovali ste z neho certifikát servera a certifikačnú autoritu:**

1. Uistite sa, že nový server používa rovnakú IP adresu alebo názov hostiteľa ako pôvodný, aby sa mohli agenti pripojiť.
2. Vykonajte opravnú inštaláciu ESMC Servera použitím zálohovaných certifikátov (pri oprave vyberte možnosť **Načítať certifikáty zo súboru** a postupujte podľa inštrukcií).

### **ESMC Server nebeží a nemáte zálohu databázy, certifikát ESMC Servera ani certifikačnú autoritu:**

1. Vykonajte opravnú inštaláciu ESMC Servera.
2. Opravte ESET Management Agenty pomocou nasledujúcich metód:
  - live inštalátor agenta,
  - vzdialené nasadenie (bude potrebné vypnúť firewall na cieľových počítačoch),
  - manuálna inštalácia komponentu Agent.

## 6.6 Protokolovanie MSI

Protokolovanie MSI je užitočné v prípade, keď sa vám nedarí nainštalovať niektoré súčasti ESMC na systém Windows, napr. ESET Management Agent:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

## 7. Prvé kroky a najvhodnejšie postupy

Po úspešnej inštalácii nástroja ESET Security Management Center môžete začať s nastaveniami.

Otvorte vo svojom prehliadači [ESMC Web Console](#) a prihláste sa.

### Zoznámte sa s ESMC Web Console

Predtým, ako sa pustíte do prvého nastavovania, odporúčame, aby ste sa [zoznámili s ESMC Web Console](#), pretože je to rozhranie, ktoré budete používať na správu bezpečnostných riešení od spoločnosti ESET. Kapitola [Úlohy po inštalácii](#) vás prevedie odporúčanými krokmi pre optimálne nastavenia.

### Vytvorenie používateľského účtu

Počas inštalácie vytvoríte účet správcu. Odporúčame však, aby ste účet správcu nepoužívali na každodennú činnosť, ale aby ste si na správu klientov a nastavovanie ich oprávnení [vytvorili nový účet](#).

### Pridanie klientskych počítačov, serverov alebo mobilných zariadení do vašej infraštruktúry ESMC

Už počas inštalácie môžete vyhľadať počítače vo vašej sieti. Všetky nájdené počítače budú zobrazené v sekcii **Počítače** po tom, ako spustíte ESET Security Management Center. Ak sa v tejto sekcii počítače neukážu, spustíte úlohu [Synchronizácia statickej skupiny](#) pre vyhľadanie počítačov a ich zobrazenie v skupinách.

### Nasadenie agenta

Keď sa počítače nájdu, [nasadte na ne agenta](#). Agent sprostredkúva komunikáciu medzi nástrojom ESET Security Management Center a klientmi.

### Inštalácia bezpečnostného produktu spoločnosti ESET (vrátane aktivácie)

Pre zaistenie ochrany vašich klientov a siete použite úlohu [Inštalácia softvéru](#), pomocou ktorej nainštalujete produkty spoločnosti ESET.

### 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, že chcete uplatniť špecifickú konfiguráciu pre bezpečnostné produkty spoločnosti ESET na klientskych počítačoch. Politikou sa môžete vyhnúť potrebe nastaviť každý nainštalovaný bezpečnostný produkt manuálne na každom počítači. Po [vytvození novej politiky](#), ktorá obsahuje vaše nastavenia, ju môžete priradiť k skupine (statickej alebo dynamickej) pre aplikovanie vašich nastavení na všetky počítače v skupine.

### Priradenie politiky ku skupine

Pre aplikovanie politiky musí byť daná politika priradená k určitej skupine. To znamená, že na počítače patriace do skupiny bude politika aplikovaná. Politika bude aplikovaná vždy, keď sa agent pripojí na ESMC Server.

### Nastavenie oznámení a vytváranie správ

Ak chcete mať lepší prehľad o tom, čo sa deje s počítačmi vo vašej sieti, odporúčame použiť [Oznámenia](#) a [Správy](#). Napríklad, ak chcete byť upozornený na určitú udalosť alebo si chcete pozrieť alebo stiahnuť správu.

### 7.1 Otvorenie ESMC Web Console

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 vášho servera.
- Pre prihlásenie do **virtuálneho zariadenia** ESMC použite nasledujúcu URL adresu:  
*https://[IP address]*



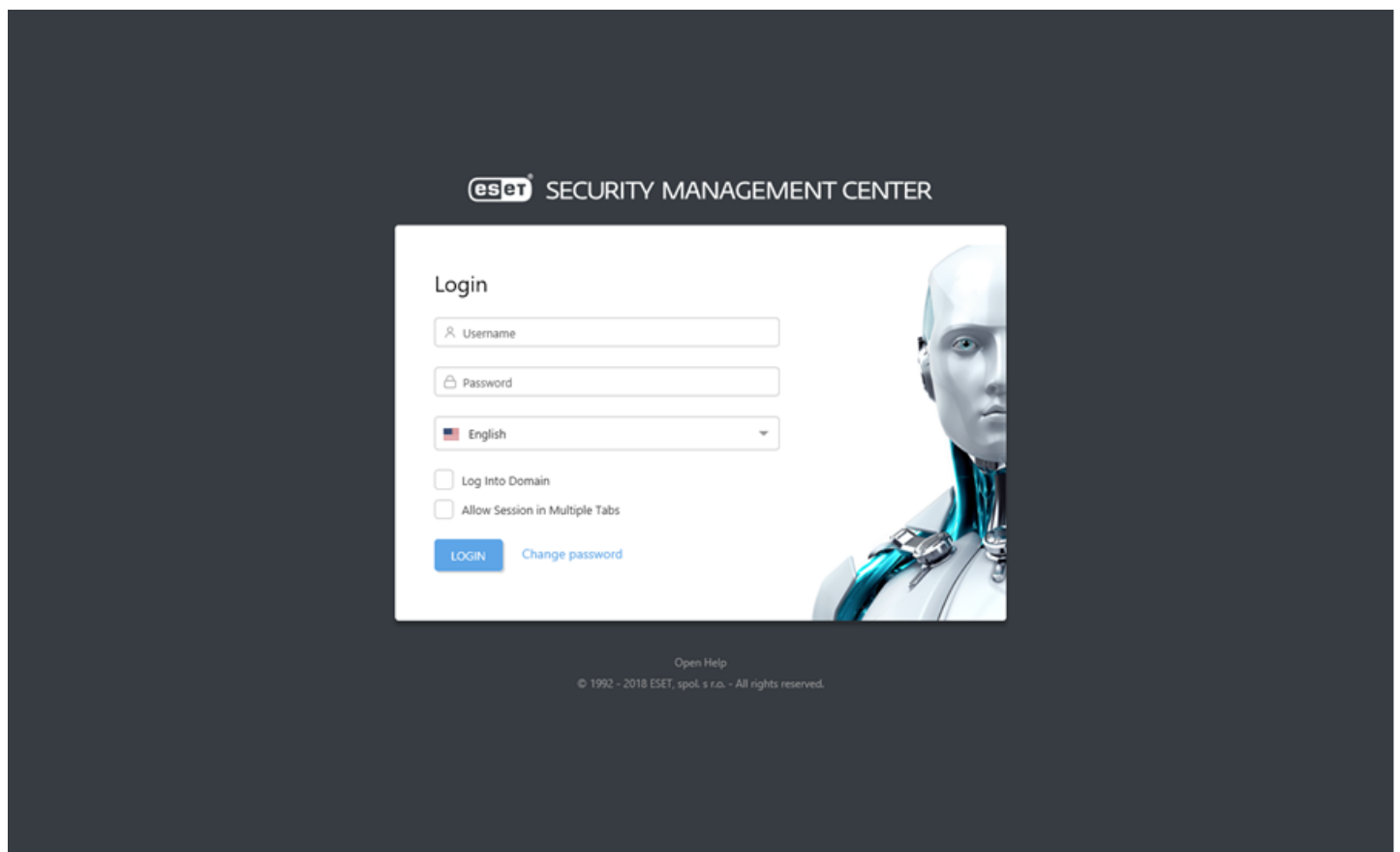
Nahradte „[IP address]“ IP adresou vášho virtuálneho počítača ESMC. Ak si nepamätáte IP adresu, postupujte podľa kroku č. 9 v časti obsahujúcej [inštrukcie nasadenia virtuálneho zariadenia](#).

- Na vašom lokálnom serveri (na ktorom sa nachádza Web Console) kliknite na **Štart > Všetky programy > ESET > ESET Security Management Center > ESET Security Management Center Webconsole** – otvorí sa prihlasovacie okno vo vašom predvolenom internetovom prehliadači. Toto sa nevzťahuje na virtuálne zariadenie ESMC.

#### **i Poznámka:**

Pretože Web Console používa protokol HTTPS, môže sa vo vašom webovom prehliadači zobrazíť správa o bezpečnosti certifikátu alebo nedôveryhodnom pripojení (presné znenie správy závisí od typu prehliadača). Váš internetový prehliadač chce skontrolovať 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 prístup do prostredia ESMC Web Console. Toto sa vzťahuje len na situáciu, kde sa snažíte pripojiť na adresu rozhrania ESET Security Management Center Web Console.

Ak je váš lokálny server (počítač s ESMC Web Console) spustený, zobrazí sa nasledujúca obrazovka:



Ak je toto vaše prvé prihlásenie, zadajte prihlasovacie údaje, ktoré ste zadali počas [inštalácie](#). Pre viac informácií si pozrite časť [Prihlasovacie okno Web Console](#).

#### **i Poznámka:**

Vo výnimočných prípadoch, kedy sa prihlasovacie okno nenačíta alebo sa načítava dlho, 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 Web Console.

## 7.2 Interval pripájania klientov

Predvolený interval pripájania ESET Management Agentu je 60 sekúnd. Po nainštalovaní nástroja ESET Security Management Center a nasadení ESET Management Agentov a produktov ESET určených pre koncové zariadenia na klientske počítače by ste túto hodnotu mali pomocou politik upravíť tak, aby zodpovedala [veľkosti vašej siete](#).

1. V ESMC Web Console prejdite do sekcie **Politiky**.
2. Vytvorte novú alebo upravte existujúcu politiku pre **ESET Management Agentu**.

### **Poznámka:**

Môžete použiť preddefinované politiky, napríklad politiku **Pripojenie - Pripojiť každých 20 minút**.

3. Kliknite na politiku, ktorú chcete upravovať, a následne na **Politiky > Upraviť**.
4. V sekcii **Nastavenia > Pripojenie** kliknite na **Zmeniť interval** vedľa položky **Interval pripojenia** a zadajte požadovanú hodnotu.
5. Zmeny uložte kliknutím na **Uložiť > Dokončiť**.
6. Politiku priradte ku všetkým agentom.

Pre viac informácií o vytváraní politik si prečítajte [tento článok databázy znalostí spoločnosti ESET](#) alebo [príslušnú kapitolu v príručke správcu](#).

## 8. ESET Security Management Center API

ESET Security Management Center ServerApi (`ServerApi.dll`) je rozhranie API; sada funkcií a nástrojov pre vytváranie vlastných softvérových aplikácií podľa vlastných požiadaviek. Prostredníctvom ServerApi môže vaša aplikácia poskytnúť vlastné rozhranie, funkcie a operácie, ktoré by ste za normálnych okolností vykonávali pomocou ESMC Web Console, ako je napr. správa nástroja ESET Security Management Center, vytváranie a prijímanie správ atď.

Pre viac informácií, príklady v jazyku C a zoznam dostupných JSON správ navštívte nasledujúcu webovú stránku:

[ESMC 7 API](#)

## 9. Časté otázky

**Prečo je na server potrebné nainštalovať Javu? Nepredstavuje Java potenciálne bezpečnostné riziko? Väčšina bezpečnostných spoločností a bezpečnostných systémov odporúča odinštalovať Javu z počítačov a obzvlášť zo serverov.**

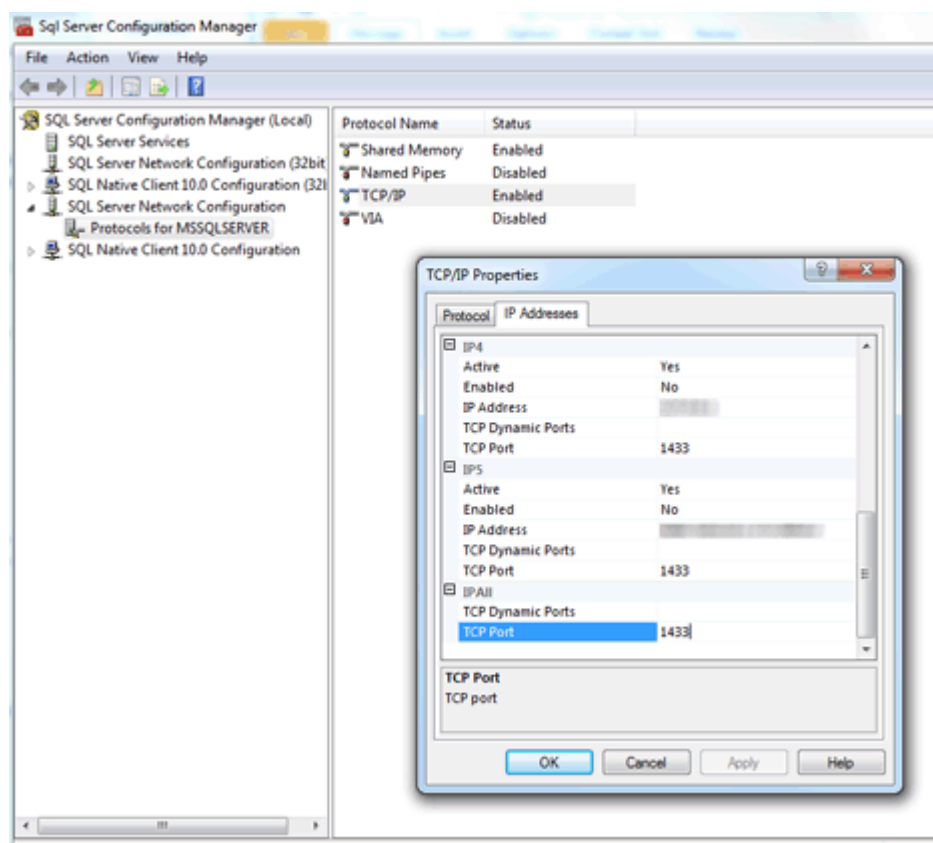
Pre správne fungovanie nástroja ESMC Web Console je potrebná Java. Java je priemyselný štandard pre webové konzoly a všetky významnejšie webové konzoly používajú Javu a webový server (Apache Tomcat), aby mohli správne fungovať. Java je tiež nevyhnutnou súčasťou podpory viacplatformového webového servera.

ESMC Web Console vyžaduje Javu aspoň vo verzii 8, napriek tomu však odporúčame vždy použiť najnovšiu oficiálne vydanú verziu platformy Java. Je možné nainštalovať webový server na vyhradený počítač v prípade, že pre vás Java predstavuje veľké bezpečnostné riziko.

---

### Ako zistím, ktorý port používa môj SQL server?

Sú rôzne možnosti, ako zistiť číslo portu SQL servera. Najlepšou možnosťou je zistiť číslo portu priamo cez nástroj SQL Server Configuration Manager. Na nasledujúcom obrázku je znázornené, kde sa v nástroji SQL Configuration Manager nachádza číslo portu.



Po nainštalovaní SQL Server Express (súčasť balíku ESMC) na Windows Server 2012 sa nepoužíva štandardný SQL port. Pravdepodobne sa používa iný ako štandardný port (1433).

---

### Ako nastavím MySQL na akceptovanie väčších paketov?

Pozrite si MySQL inštaláciu a konfiguráciu pre [Windows](#) alebo [Linux](#).

## Ak nainštalujem SQL samostatne, ako vytvorím databázu pre ESMC manuálne?

Databázu nemusíte vytvárať manuálne. Databáza sa vytvorí pomocou **SERVER.MSI** inštalátora, nie pomocou ESMC inštalátora. ESMC inštalátor je priložený pre zjednodušenie postupu. Inštaluje SQL server a databáza je potom vytvorená prostredníctvom inštalátora `Server.msi`.

---

## Dokáže ESMC inštalátor vytvoriť novú databázu na už existujúcom MS SQL serveri, ak pri inštalácii zadám platné prístupové údaje a potrebné údaje o pripojení k serveru? Aké verzie SQL servera (2008, 2014 atď.) sú podporované?

Databáza sa vytvorí pomocou inštalátora `Server.msi`. To znamená, že inštalátor pre vás môže vytvoriť ESMC databázu na samostatne nainštalovanom SQL serveri. Sú podporované verzie SQL Server 2008 a novšie.

---

## Mal by byť pri inštalácii na existujúci SQL server použitý vstavaný režim overovania systému Windows?

Nie, pretože režim overovania systému Windows môže byť zakázaný na SQL serveri a jediný spôsob prihlásenia sa na SQL server je pomocou prihlasovacieho mena a hesla SQL servera. Musíte použiť buď SQL Server autentifikáciu, alebo zmiešaný režim. Ak inštalujete SQL server manuálne, odporúčame vytvoriť root heslo (root používateľ je pomenovaný „sa“, čo je skratka pre security admin) a dobre si toto heslo uložiť na bezpečnom mieste. Root heslo môžete potrebovať pri aktualizácii ESMC Servera.

---

## Môžem použiť MariaDB miesto MySQL?

### Upozornenie:

MariaDB je predvolená databáza vo väčšine súčasných linuxových prostredí a je súčasťou inštalácie MySQL.

Databázový server MariaDB nie je podporovaný nástrojom ESET Security Management Center.

Pozrite si tiež kapitolu [Inštalácia a konfigurácia MySQL](#).

---

## Musím nainštalovať Microsoft .NET Framework 3.5, na čo ma upozornil ESMC inštalátor (<http://www.microsoft.com/en-us/download/details.aspx?id=21>). Toto však zlyhalo na novej inštalácii Windows Server 2012 R2 SP1.

Tento inštalátor nemôže byť použitý pri verzii Windows Server 2012, pretože bezpečnostná politika systému Windows Server 2012 to nepovoľuje. Microsoft .NET Framework musí byť nainštalovaný prostredníctvom **SPRIEVODCU ROLAMI A FUNKCIAMI SERVERA**.

---

## Microsoft .NET 4.5 framework je už na mojom systéme nainštalovaný. Pre nainštalovanie verzie .NET 3.5. som použil Sprievodcu rolami a funkciami servera. Prečo ESET Security Management Center nepodporuje .NET 4.5?

Pretože verzia .NET 4.5 nie je spätne kompatibilná s verziou .NET 3.5, ktorá je prerekvizitou pre inštaláciu SQL servera.

---

## Je náročné zistiť, či ešte stále prebieha inštalácia SQL servera. Ako to zistím, ak je inštalácia spustená už viac ako 10 minút?

Inštalácia SQL servera môže v zriedkavých prípadoch trvať aj 1 hodinu. Trvanie inštalácie závisí od výkonu vášho systému.

---

## Ako vynulujem heslo správcu pre Web Console (heslo bolo nastavené pri inštalácii)?

Zmena tohto hesla je možná pri opätovnom spustení inštalátora a zvolení možnosti **Opraviť**. Berte na vedomie, že na prístup do ESMC databázy môže byť potrebné heslo, ak ste pri vytvorení databázy nepoužili overovanie systému Windows.

### **i** Poznámka:

Buďte, prosím, opatrný, pretože niektoré opravy môžu viesť k vymazaniu uložených údajov.

---

## Aký je formát súboru pre importovanie zoznamu počítačov do ESMC?

Súbor musí obsahovať riadky v nasledujúcej podobe:

*All\Group1\GroupN\Computer1*

*All\Group1\GroupM\ComputerX*

All (Všetko) je požadovaný názov koreňovej skupiny.

---

## Môžem namiesto Apache použiť IIS, prípadne iný HTTP server?

IIS je HTTP server. Nástroj Web Console vyžaduje Java servlet container (napr. Tomcat), samotný HTTP server nestačí. Existujú riešenia premeny IIS na Java servlet container, tento postup však neodporúčame.

### **i** Poznámka:

Nepoužívame Apache HTTP Server, ale Apache Tomcat.

---

## Má ESMC vlastný príkazový riadok?

Áno, ponúkame ESET Security Management Center [ServerApi](#).

---

## Môžem nainštalovať ESMC na doménový radič?

ESMC Server je možné nainštalovať na doménový radič, môžu sa však vyskytnúť určité obmedzenia pri inštalácii MS SQL na Windows Domain Controller. Viac informácií nájdete v našom [článku databázy znalostí](#).

---

## Dá sa pre inštaláciu na doménový radič použiť sprievodca?

Môžete použiť na inštaláciu sprievodcu, musíte však zrušiť výber inštalácie SQL v okne výberu súčastí.

---

## Dokáže inštalácia ESMC Servera zistiť, či je SQL už nainštalované v systéme? Čo sa stane, ak je už SQL nainštalované? A ako to je s MySQL?

ESMC pri inštalácii kontroluje, či je v systéme spustené SQL v prípade, že ste použili inštalátor a vybrali možnosť inštalovať SQL Express. V prípade, že je už v systéme spustené SQL, inštalátor zobrazí oznámenie a vyzve vás k odinštalovaniu SQL a opätovnému spusteniu inštalácie alebo k inštalácii ESMC bez komponentu SQL Express. Pozrite si [požiadavky na databázu](#) pre ESMC.

---

## Kde nájdem informácie o verziách súčastí ESMC?

Viac informácií nájdete v našom [článku databázy znalostí](#).

---

## Ako aktualizujem ESET Security Management Center na najnovšiu verziu podľa jednotlivých súčastí?

Windows: <https://support.eset.com/kb6819/>

Linux: <https://support.eset.com/kb6734/>

---

## Ako aktualizujem produkt od spoločnosti ESET bez pripojenia na internet?

Pomocou HTTP proxy nainštalovaného na počítači, ktorý sa môže pripojiť na aktualizáčnne servery spoločnosti ESET a odkázať klienty na dané HTTP proxy na lokálnej sieti. Ak váš server nie je pripojený na internet, môžete v rámci produktu ESET určeného pre koncové zariadenia použiť na jednom počítači funkciu mirror, použiť USB kľúč na dodanie aktualizáčnych súborov na tento počítač a nastaviť ho ako aktualizáčny server pre ostatné počítače v sieti.

Podrobný postup týkajúci sa offline inštalácie nájdete v [týchto inštrukciách](#).

---

## Ako preinštalujem ESMC Server a pripojím ho na existujúci SQL server, ak konfigurácia SQL servera prebehla automaticky počas počiatocnej inštalácie ESMC ?

Ak inštalujete novú inštanciu ESMC Servera pomocou rovnakého používateľského účtu (napríklad účet správcu domény), pod ktorým ste nainštalovali pôvodný ESMC Server, môžete použiť **MS SQL Server cez overovanie systému Windows**.

---

## Ako vyriešim problémy so synchronizáciou Active Directory na Linuxe?

Uistite sa, že ste názov domény zadali veľkými písmenami (administrator@TEST.LOCAL miesto administrator@test.local).

---

## Môžem namiesto repozitára použiť vlastnú sieť (napríklad zdieľanie súborov cez SMB)?

Môžete zadať priamu cestu k súboru na sieti (URL adresu). Ak používate zdieľanie súborov, špecifikujte ho vo formáte: file:// a následne zadajte úplnú sieťovú cestu k súboru, napríklad:

## Ako vynulujem alebo zmením svoje heslo?

Ideálne by účet správcu mal byť používaný len na vytváranie ďalších správcovských účtov. Po vytvorení [úctu správcu](#) by malo byť heslo uložené a účet by nemal byť používaný. Takýto postup umožňuje, aby bol účet správcu používaný len na účely vynulovania hesla/zobrazenia podrobností účtu.

Ako vynulovať heslo pre účet správcu ESMC:

1. Otvorte **Programy a súčasti** (spustíte *appwiz.cpl*), nájdite v zozname ESET Security Management Center Server a kliknite naň pravým tlačidlom.
2. Z roletového menu vyberte možnosť **Zmeniť**.
3. Ďalej vyberte možnosť **Opraviť**.
4. Upresnite podrobnosti pripojenia na databázu.
5. Vyberte možnosť **Použiť existujúcu databázu a aplikovať aktualizáciu**.
6. Zrušte výber možnosti **Použite heslo správcu, ktoré je už uložené v databáze** a zadajte nové heslo.
7. Následne sa môžete prihlásiť do ESMC Web Console pomocou svojho nového hesla.

### **i** Poznámka:

Dôrazne odporúčame vytvoriť ďalšie používateľské účty, ktoré budú mať pridelené požadované povolenia umožňujúce vykonávanie len určitých činností.

---

## Ako zmením porty pre ESMC Server a ESMC Web Console?

Je potrebné zmeniť port v konfigurácii webového servera, aby sa webový server mohol pripojiť na nový port. Postupujte podľa nasledujúcich krokov:

1. Vypnite webový server.
  2. V konfigurácii webového servera zmeňte číslo portu.
    - a) Otvorte súbor *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
    - b) Nastavte nové číslo portu (napr. `server_port=44591`).
  3. Znova spustíte webový server.
- 

## Ako premigrujem ESMC Server na novú verziu?

Podrobnejšie informácie o migrácii nájdete na nasledujúcich odkazoch:

- [Aktualizácia z predošlej verzie ERA](#)
- 

## Môžem vykonať aktualizáciu nástroja ERA z verzie 5 na ESMC 7 priamo cez all-in-one inštalátor?

Priama aktualizácia nie je podporovaná, odporúčame preto použiť nástroj na migráciu (Migration Tool). Pre viac informácií si pozrite časť [Aktualizácia z predošlej verzie ERA](#) a nasledujúci článok databázy znalostí spoločnosti ESET: [Ako aktualizujem ESET Remote Administrator 5 na verziu 7?](#)

---



**Dostávam chybové hlásenia alebo mám problém s nástrojom ESET Security Management Center, čo mám robiť?**

Potrebné informácie nájdete v kapitole [Najčastejšie problémy s inštaláciou](#).