ESET PROTECT

Przewodnik instalacji uaktualniania i migracji

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

Prawa autorskie ©2023 ESET, spol. s r.o.

Produkt ESET PROTECT został opracowany przez ESET, spol. s r.o.

Aby uzyskać więcej informacji, odwiedź stronę https://www.eset.com.

Wszelkie prawa zastrzeżone. Żadna część tej dokumentacji nie może być powielana, przechowywana w systemie wyszukiwania lub przesyłana w jakiejkolwiek formie lub za pomocą jakichkolwiek środków elektronicznych, mechanicznych, fotokopiowania, nagrywania, skanowania lub w inny sposób bez pisemnej zgody autora.

Firma ESET, spol. s r.o. zastrzega sobie prawo do zmiany dowolnej z opisanych aplikacji bez uprzedniego powiadomienia.

Pomoc techniczna: https://support.eset.com

WER. 19.03.2023

1 Informacje o pomocy ... 1
2 Instalacja/Aktualizacja/Migracja ... 2
2.1 Nowe funkcje produktu ESET PROTECT 9.1 ... 2
2.2 Architektura ... 4
2.2 Serwer ... 5
2.2 Konsola internetowa ... 6
2.2 Serwer proxy HTTP ... 6
2.2 Serwer proxy Apache HTTP ... 8
2.2 Agent ... 12
2.2 Moduł Rogue Detection Sensor ... 13
2.2 Moduł zarządzania urządzeniami mobilnymi ... 14
2.3 Różnice pomiędzy serwerem proxy Apache HTTP, narzędziem Mirror Tool a połączeniem bezpośrednim ... 16
2.3 Kiedy zacząć używać serwera proxy Apache HTTP ... 18
2.3 Kiedy zacząć używać narzędzia Mirror Tool ... 18
3 Wymagania systemowe i rozmiary ... 19
3.1 Obsługiwane systemy operacyjne ... 19
3.1 System Windows ... 19
3.1 Linux ... 21
3.1 macOS ... 22
3.1 Urządzenie mobilne ... 22
3.2 Obsługiwane środowiska przydzielania komputerów ... 24
3.3 Rozmiar sprzętu i infrastruktury ... 25
3.3 Zalecenia dotyczące wdrażania ... 27
3.3 Wdrożenie dla 10 000 klientów ... 29
3.4 Baza danych ... 31
3.5 Obsługiwane wersje serwera Apache Tomcat i środowiska Java ... 33
3.6 Obsługiwane przeglądarki internetowe, produkty zabezpieczające firmy ESET i języki ... 33
3.7 Sieć ... 36
3.7 Używane porty ... 37
4 Procedura instalacji ... 41
4.1 Instalacja kompleksowa w systemie Windows ... 42
4.1 Instalowanie serwera ESET PROTECT ... 43
4.1 Instalowanie Modułu zarządzania urządzeniami mobilnymi ESET PROTECT (tryb autonomiczny) ... 56
4.2 Instalowanie na platformie Microsoft Azure ... 63
4.3 Instalacja komponentów w systemie Windows ... 63
4.3 Instalacja serwera — Windows ... 65
4.3 Wymagania dotyczące programu Microsoft SQL Server ... 72
4.3 Instalacja i konfiguracja programu MySQL Server ... 73
4.3 Dedykowane konto użytkownika bazy danych ... 75
4.3 Instalacja agenta — Windows ... 75
4.3 Wspomagana instalacja serwerowa agenta ... 78
4.3 Instalacja offline agenta ... 79
4.3 ESET Remote Deployment Tool ... 80
4.3 Instalacja konsoli internetowej — Windows ... 80
4.3 Instalacja konsoli internetowej przy użyciu instalatora kompleksowego ... 80
4.3 Ręczne instalowanie konsoli internetowej ... 86
4.3 Instalacja serwera proxy HTTP ... 87
4.3 Instalacja narzędzia RD Sensor — Windows ... 88
4.3 Narzędzie Mirror Tool — system Windows ... 89
4.3 Instalacja narzędzia Moduł zarządzania urządzeniami mobilnymi – Windows ... 96

4.3 Wymagania wstępne dotyczące komponentu Moduł zarządzania urządzeniami mobilnymi ... 98
4.3 Aktywacja Modułu zarządzania urządzeniami mobilnymi ... 101
4.3 Narzędzie MDM, funkcja licencjonowania urządzeń z systemem iOS ... 101
4.3 Wymagania dotyczące certyfikatu HTTPS ... 101
4.3 Instalacja i pamięć podręczna serwera proxy Apache HTTP ... 102
4.3 Konfiguracja serwera proxy Apache HTTP ... 103
4.3 Instalacja Squid — Windows (pamięć podręczna proxy HTTP) ... 107
4.3 Repozytorium offline — Windows ... 107
4.3 Klaster trybu failover — Windows ... 110
4.4 Instalacja komponentów w systemie Linux ... 111
4.4 Szczegółowa instrukcja instalacji ESET PROTECT w systemie Linux ... 112
4.4 Instalacja i konfiguracja oprogramowania MySQL ... 113
4.4 Instalacja i konfiguracja sterownika ODBC ... 115
4.4 Instalacja serwera — system Linux ... 117
4.4 Wymagania wstępne dotyczące serwera — system Linux ... 121
4.4 Instalacja agenta — system Linux ... 123
4.4 Instalacja konsoli internetowej — system Linux ... 128
4.4 Instalacja narzędzia rogue detection sensor – Linux ... 130
4.4 Instalacja narzędzia Moduł zarządzania urządzeniami mobilnymi — system Linux ... 131
4.4 Wymagania wstępne dotyczące komponentu Moduł zarządzania urządzeniami mobilnymi — system Linux ... 134
4.4 Instalacja serwera proxy Apache HTTP — system Linux ... 135
4.4 Instalowanie serwera proxy Squid HTTP w systemie Ubuntu Server ... 145
4.4 Narzędzie Mirror Tool — system Linux ... 145
4.5 Instalacja komponentów w systemie macOS ... 152
4.5 Instalacja agenta — system macOS ... 152
4.6 Obraz ISO ... 154
4.7 Rekord usługi DNS ... 154
4.8 Scenariusz instalacji offline programu ESET PROTECT ... 155
5 Procedury uaktualniania ... 156
5.1 Zadanie Uaktualnianie komponentów ESET PROTECT ... 156
5.2 Uaktualnianie za pomocą instalatora kompleksowego ESET PROTECT 9.1 ... 161
5.3 Uaktualnienie z wersji ERA 6.5 ... 164
5.4 Kopa zapasowa / aktualizacja serwera bazy danych ... 164
5.4 Tworzenie i przywracanie kopii zapasowej serwera bazy danych ... 165
5.4 Uaktualnianie serwera baz danych ... 167
5.5 Uaktualnianie programu ESMC/ESET PROTECT zainstalowanego w klastrze trybu failover w systemie Windows ... 168
5.6 Uaktualnianie serwera proxy Apache HTTP ... 168
5.6 Uaktualnianie serwera proxy Apache HTTP przy użyciu instalatora kompleksowego (system Windows) ... 168
5.6 Ręczne uaktualnianie serwera proxy Apache HTTP (system Windows) ... 171
5.7 Uaktualnianie serwera Apache Tomcat ... 173
5.7 Uaktualnianie serwera Apache Tomcat przy użyciu instalatora kompleksowego (system Windows) ... 173
5.7 Ręczne uaktualnianie serwera Apache Tomcat (system Windows) ... 177
5.7 Uaktualnianie serwera Apache Tomcat (system Linux) ... 179
6 Procedury migracji i ponownej instalacji ... 180
6.1 Migracja między serwerami ... 180
6.1 Czysta instalacja, ten sam adres IP ... 181
6.1 Migrowana baza danych — ten sam/inny adres IP ... 183
6.2 migracja bazy danych ESET PROTECT ... 184
6.2 Procedura migracji programu MS SQL Server ... 184
6.2 Procedura migracji programu MySQL Server ... 192

6.2 Łączenie serwera ESET PROTECT lub komponentu MDM z bazą danych 194
6.3 Migracja komponentu MDM 196
6.4 Zmienianie adresu IP lub nazwy hosta serwera ESET PROTECT po migracji 197
6.5 Migracja z programu ERA 5.x 198
7 Odinstalowywanie serwera ESET PROTECT i jego składników 198
7.1 Odinstaluj agenta ESET Management 198
7.2 Windows — odinstalowywanie serwera ESET PROTECT i jego składników 200
7.3 Linux — uaktualnianie, ponowne instalowanie lub odinstalowywanie składników ESET PROTECT 201
7.4 macOS — odinstalowywanie agenta ESET Management i produktu punktu końcowego firmy ESET 202
7.5 Likwidacja starego serwera ESMC / ESET PROTECT / MDM po migracji na inny serwer 204
8 Rozwiązywanie problemów 205
8.1 Uaktualnianie komponentów ESET PROTECT w środowisku offline 206
8.2 Rozwiązania częstych problemów z instalacją 206
8.3 Pliki dziennika 212
8.4 Narzędzie diagnostyczne 213
8.5 Problemy po uaktualnieniu/migracji serwera ESET PROTECT 215
8.6 Zapisywanie w dzienniku MSI 216
9 ESET PROTECT API 216
10 Często zadawane pytania 216
11 Umowa licencyjna użytkownika końcowego 224
12 Zasady ochrony prywatności 232

Informacje o pomocy

Ten podręcznik instalacji został napisany, aby pomóc w instalowaniu i uaktualnianiu programu ESET PROTECT. Zawiera też odpowiednie instrukcje.

Terminologia stosowana w tym podręczniku jest oparta na nazwach parametrów programu ESET PROTECT w celu zapewnienia spójności oraz uniknięcia pomyłek. Stosujemy również zestaw symboli do wyróżniania szczególnie ważnych tematów.

Ta sekcja zawiera przydatne informacje, na przykład dotyczące poszczególnych funkcji, lub łącza do tematów pokrewnych.

Informacje w tej sekcji należy uważnie przeczytać i nie należy ich pomijać. Nie mają one kluczowego znaczenia, są jednak ważne.

Kluczowe informacje, które należy przeczytać ze szczególną uwagą. Ostrzeżenia mają na celu zapobiegnięcie potencjalnie szkodliwym pomyłkom. Tekst w tej sekcji należy przeczytać ze zrozumieniem, ponieważ dotyczy on bardzo istotnych ustawień systemowych i ryzykownych czynności.

Przykładowy scenariusz przedstawia czynności użytkownika, które dotyczą omawianego tematu. Przykłady są używane do wyjaśniania bardziej skomplikowanych zagadnień.

Konwencja	Znaczenie
Pogrubienie	Nazwy elementów interfejsu, na przykład pola i przyciski opcji.
Kursywa	Elementy zastępcze oznaczające informacje podawane przez użytkownika. Na przykład nazwa pliku lub ścieżka oznacza, że użytkownik wpisuje rzeczywistą ścieżkę lub nazwę pliku.
`Courier New`	Przykłady kodu lub poleceń.
Hiperłącze	Zapewnia szybki i łatwy dostęp do wspomnianych tematów lub zewnętrznych stron internetowych. Hiperłącza są wyróżnione przy użyciu niebieskiego koloru i mogą być podkreślone.
%ProgramFiles%	Katalog w systemie Windows, w którym znajdują się zainstalowane programy systemu Windows oraz inne programy.

- Pomoc online to główne źródło pomocy. Najnowsza wersja pomocy online jest wyświetlana automatycznie, gdy działa połączenie z Internetem. Strony pomocy online programu ESET PROTECT zawierają cztery aktywne karty u góry nagłówka nawigacyjnego: Instalacja/Uaktualnienie, Administracja, Wdrażanie urządzenia wirtualnego oraz Poradnik dla małych i średnich przedsiębiorstw.

- Tematy w tym podręczniku zostały podzielone na kilka rozdziałów i podrozdziałów. Odpowiednie informacje można znaleźć, używając pola Szukaj u góry.

Po otwarciu Podręcznika użytkownika z poziomu paska nawigacyjnego u góry strony wyszukiwanie jest ograniczone do zawartości tego podręcznika. Jeśli na przykład zostanie otwarty Podręcznik administratora, tematy z podręczników dotyczących instalacji/uaktualniania i wdrażania urządzenia wirtualnego nie będą uwzględniane w wynikach wyszukiwania.

- Baza wiedzy firmy ESET zawiera odpowiedzi na najczęściej zadawane pytania, a także zalecane rozwiązania dotyczące różnych problemów. Jest ona regularnie aktualizowana przez specjalistów firmy ESET, dlatego stanowi najlepsze narzędzie do rozwiązywania rozmaitych dylematów.

- Forum ESET pozwala użytkownikom produktów firmy ESET w prosty sposób uzyskiwać pomoc i pomagać innym. Można na nim publikować pytania dotyczące dowolnych problemów lub używanych produktów firmy ESET.

Instalacja/Aktualizacja/Migracja

ESET PROTECT to aplikacja umożliwiająca zarządzanie produktami firmy ESET na klienckich stacjach roboczych, serwerach i urządzeniach mobilnych w środowisku sieciowym z jednej lokalizacji centralnej. Dzięki wbudowanemu systemowi zarządzania zadaniami dostępnemu w programie ESET PROTECT można instalować rozwiązania zabezpieczające firmy ESET na komputerach zdalnych i szybko reagować na nowe problemy i wykrycia.

Sam program ESET PROTECT nie zapewnia ochrony przed szkodliwym kodem. Ochrona środowiska użytkownika zależy od zainstalowanego na stacjach roboczych, serwerach lub urządzeniach mobilnych rozwiązania zabezpieczającego firmy ESET, takiego jak ESET Endpoint Security czy ESET Server Security dla systemu Windows Server.

W programie ESET PROTECT zastosowano dwie główne zasady:

- **Scentralizowane zarządzanie** — możliwość skonfigurowania całej sieci oraz zarządzania nią i monitorowania jej działania z jednego miejsca.

- **Skalowalność** — system można wdrażać zarówno w niewielkich sieciach, jak i w wielkich środowiskach firmowych. Program ESET PROTECT można dostosowywać do rozwoju infrastruktury.

Program ESET PROTECT obsługuje nową generację produktów zabezpieczających firmy ESET i jest także zgodny z poprzednią generacją tych produktów.

Strony pomocy programu ESET PROTECT zawierają instrukcje pełnej instalacji i uaktualniania:

- Architektura programu ESET PROTECT
- Procedura instalacji
- Procedury uaktualniania
- Procedury migracji
- Procedury dezinstalacji
- Zarządzanie licencjami
- Procedury wdrażania i Wdrażanie agenta przy użyciu obiektu GPO lub programu SCCM
- Pierwsze kroki po zainstalowaniu programu ESET PROTECT
- Podręcznik administracji

Nowe funkcje produktu ESET PROTECT 9.1

Prezentacja produktu

Dodaliśmy nową prezentację produktu, aby ułatwić Ci szybką nawigację po naszym rozwiązaniu i przyspieszyć proces wdrażania. Dowiedz się więcej

Zmiany w nazwach produktów

ESET Enterprise Inspector został przemianowany na ESET Inspect, a ESET Dynamic Threat Defense został przemianowany na ESET LiveGuard Advanced. Więcej informacji można znaleźć w tym artykule.

Ulepszone ponowne uruchamianie

W najnowszej wersji ESET Endpoint Security dla systemu Windows (9.1) przerobiliśmy restarty i wprowadziliśmy nowe opcje. Możesz teraz skonfigurować ponowne uruchamianie w taki sposób, aby użytkownicy końcowi mogli je odłożyć. Dowiedz się więcej

Łatwiejsze wdrażanie

Przerobiliśmy kreator tworzenia instalatora, aby był bardziej intuicyjny. W zadaniu Instalacja oprogramowania można teraz użyć specjalnego parametru „najnowszy”. który zapewnia, że utworzony instalator zawsze instaluje najnowszą wersję produktu po uruchomieniu. Dowiedz się więcej

Natywna obsługa ARM dla systemu macOS

Wraz z najnowszą wersją ESET Management Agent i ESET Endpoint Antivirus dla systemu macOS (v7) wprowadzamy natywną obsługę architektury ARM. Dowiedz się więcej

Obsługa aplikacji do uwierzytelniania dwuskładnikowego innych firm

Dodaliśmy obsługę aplikacji do uwierzytelniania dwuskładnikowego innych firm, które obsługują wymagany protokół TOTP, takich jak Google Authenticator, Microsoft Authenticator i Authy. Dowiedz się więcej

Filtry zaawansowane

Przedstawiamy nową koncepcję filtrowania danych, która ułatwi Ci filtrowanie odpowiednich urządzeń w większych środowiskach, ale nie tylko tam. Zawsze będziesz mieć statystyczny ogląd na liczbę urządzeń z określonymi atrybutami w swojej sieci i będziesz wiedzieć, ile wyników uzyskasz, zanim klikniesz filtr. Możesz teraz wypróbować nowe opcje filtrowania w sekcji Komputery. Dowiedz się więcej

Lepsza komunikacja automatycznych aktualizacji

Dodaliśmy nową niebieską sekcję do stanu wersji składnika na pulpicie nawigacyjnym Przegląd stanu, aby ułatwić identyfikację punktów końcowych z włączonymi automatycznymi aktualizacjami, które czekają na aktualizacje, ale mogą być również aktualizowane ręcznie z wyprzedzeniem. Dowiedz się więcej

Lista nieaktualnych komponentów

ESET PROTECT wykrywa teraz nieaktualne komponenty, wyświetla administratorowi konsoli listę nieaktualnych komponentów oraz instrukcje dotyczące ich uaktualniania. Dowiedz się więcej

Kontrola dostępu do stron internetowych dla MDM

Przenosimy funkcje kontroli dostępu do stron internetowych z Cloud MDM do wariantu lokalnego. Administrator może ograniczyć pracownikom dostęp do różnych kategorii treści lub konkretnych linków internetowych.

Inne ulepszenia i zmiany użyteczności

Więcej szczegółów można znaleźć w dzienniku zmian.

Architektura

ESET PROTECT to nowa generacja systemu zdalnego zarządzania.

Aby przeprowadzić całkowite wdrożenie produktów zabezpieczających firmy ESET, należy zainstalować następujące składniki (platformy Windows i Linux):

- Serwer ESET PROTECT
- Konsola internetowa ESET PROTECT
- Agent ESET Management

Wymienione niżej komponenty pomocnicze są opcjonalne. Zalecamy jednak zainstalowanie ich w celu zapewnienia optymalnej wydajności oprogramowania w sieci:

- Serwer proxy
- RD Sensor
- Serwer proxy Apache HTTP
- Moduł zarządzania urządzeniami mobilnymi

Komponenty ESET PROTECT komunikują się z serwerem ESET PROTECT za pomocą certyfikatów. Więcej informacji na temat certyfikatów w ESET PROTECT zawiera ten artykuł w bazie wiedzy.

Przegląd elementów infrastruktury

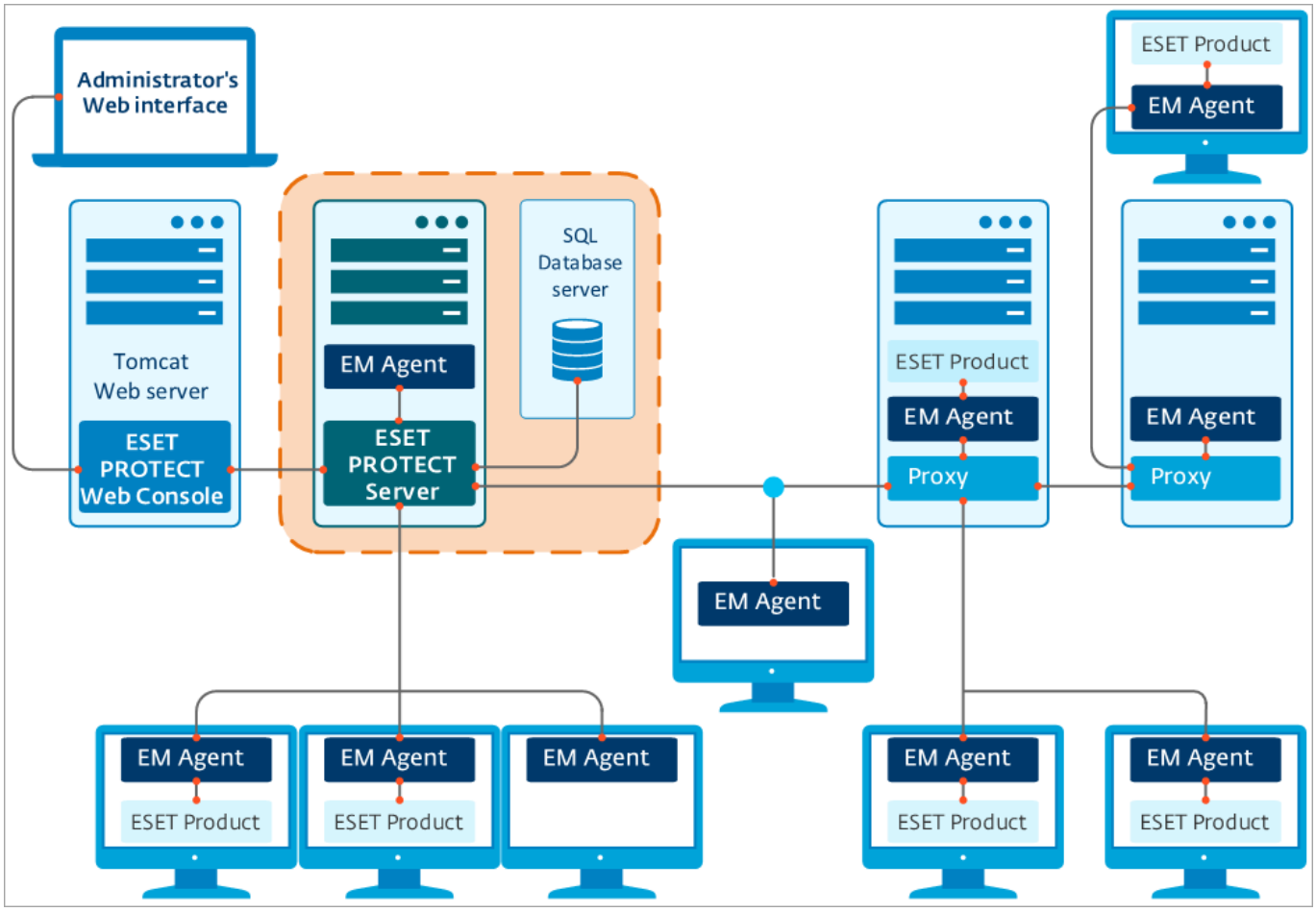
W poniższej tabeli przedstawiono przegląd elementów infrastruktury ESET PROTECT oraz ich najważniejsze funkcje:

Funkcjonalność	ESET PROTECTSerwer	Agent ESET Management	Produkt zabezpieczający ESET	Serwer proxy HTTP	Serwery ESET	Moduł zarządzania urządzeniami mobilnymi
Zdalne zarządzanie produktami zabezpieczającymi firmy ESET (tworzenie polityk, zadań, raportów itd.)	✔	X	X	X	X	X

Funkcjonalność	ESET PROTECTSerwer	Agent ESET Management	Produkt zabezpieczający ESET	Serwer proxy HTTP	Serwery ESET	Moduł zarządzania urządzeniami mobilnymi
Komunikacja z serwerem ESET PROTECT oraz zarządzanie produktem zabezpieczającym firmy ESET na urządzeniu klienckim	X	✔	X	X	X	✔
Udostępnianie aktualizacji, weryfikacja licencji	X	X	X	X	✔	X
Buforowanie i przekazywanie aktualizacji (silnik detekcji, instalatory, moduły)	X	X	✔	✔	X	X
Przekazywanie ruchu sieciowego pomiędzy agentem ESET Management a serwerem ESET PROTECT	X	X	X	✔	X	X
Zabezpieczanie urządzenia klienckiego	X	X	✔	X	X	X
Zdalne zarządzanie urządzeniami mobilnymi	X	X	X	X	X	✔

Serwer

Serwer ESET PROTECT to aplikacja wykonawcza przetwarzająca wszystkie dane odbierane od klientów łączących się z serwerem (za pośrednictwem agenta ESET Management lub serwera HTTP proxy). Aby poprawnie przetwarzać dane, serwer wymaga stabilnego połączenia z serwerem bazy danych, gdzie dane sieciowe są przechowywane. W celu uzyskania wyższej wydajności zalecane jest zainstalowanie serwera bazy danych na innym komputerze.

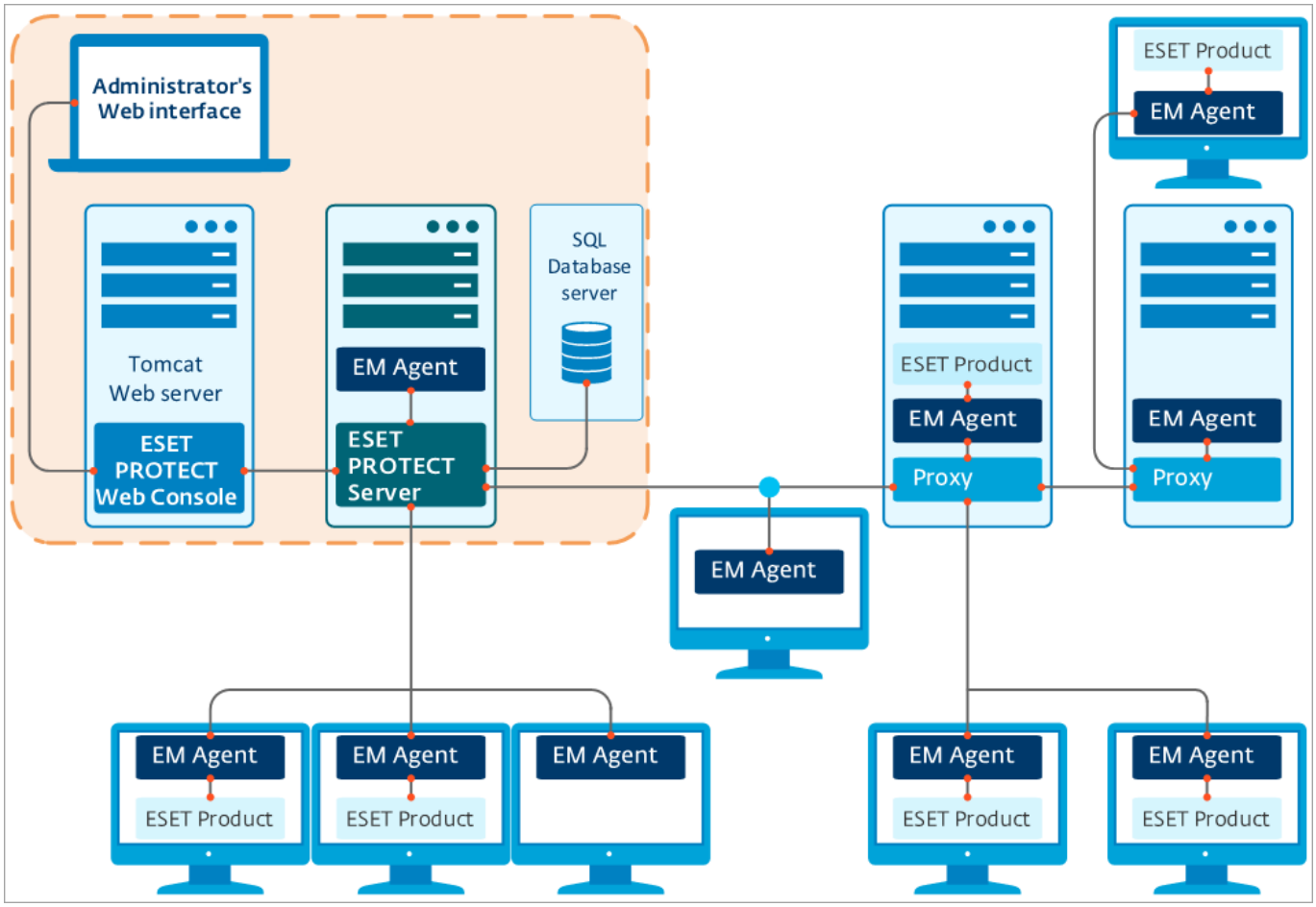


Konsola internetowa

Konsola internetowa ESET PROTECT to interfejs użytkownika obsługiwany w przeglądarce internetowej. Pozwala on na zarządzanie rozwiązaniami zabezpieczającymi firmy ESET w środowisku użytkownika. Umożliwia wyświetlanie podsumowania stanu klientów w danej sieci i może być używana do zdalnego wdrażania rozwiązań ESET na niezarządzanych komputerach. Dostęp do konsoli internetowej uzyskiwany jest przy użyciu przeglądarki internetowej (patrz Obsługiwane przeglądarki internetowe). Jeśli zdecydujesz się, by serwer sieciowy był dostępny przez Internet, możesz używać programu ESET PROTECT z praktycznie dowolnego miejsca, za pomocą dowolnego urządzenia.

Na potrzeby konsoli internetowej jako serwer HTTP używany jest serwer Apache Tomcat. W przypadku korzystania z serwera Tomcat dostępnego w pakiecie w instalatorze produktu ESET lub urządzenia wirtualnego w konsoli internetowej obsługiwane są wyłącznie połączenia w ramach protokołu TLS 1.2 i 1.3.

Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT.



Serwer proxy HTTP

Co to jest serwer proxy HTTP i do czego służy?

Serwer proxy HTTP służy do przekazywania komunikacji między agentami a serwerem ESET PROTECT w środowiskach, w których komputery agentów nie mogą nawiązać połączenia z serwerem.

Jak działa serwer proxy w programie ESET PROTECT?

ESET PROTECT 9 używa niestandardowej wersji usługi Apache HTTP Proxy jako komponentu serwera proxy. Po prawidłowym skonfigurowaniu usługa Apache HTTP Proxy może działać jako serwer proxy na potrzeby agentów ESET Management. Serwer proxy nie buforuje danych ani nie otwiera komunikacji. Przekazuje tylko dane.

Czy można używać serwera proxy innego niż Serwer proxy Apache HTTP?

Każde rozwiązanie serwera proxy, które spełnia poniższe warunki, może być używane z agentem ESET Management:

- Obsługa przekazywania komunikacji SSL
- Obsługa HTTP CONNECT
- Brak konieczności używania nazwy użytkownika i hasła

Czym różni się nowy protokół komunikacyjny?

Serwer ESET PROTECT komunikuje się z agentami ESET Management za pośrednictwem protokołu gRPC. Komunikacja wykorzystuje protokoły TLS i HTTP2, dzięki czemu może być przekazywana przez serwery proxy. Udostępnia też nowe funkcje automatycznego odzyskiwania i stałe połączenie, co usprawnia komunikację.

Jak to wpływa na wydajność?

Używanie serwera proxy HTTP nie ma poważnego wpływu na wydajność.

Kiedy należy korzystać z serwera proxy?

Korzystanie z serwera proxy jest zalecane, gdy infrastruktura spełnia co najmniej jeden z poniższych warunków:

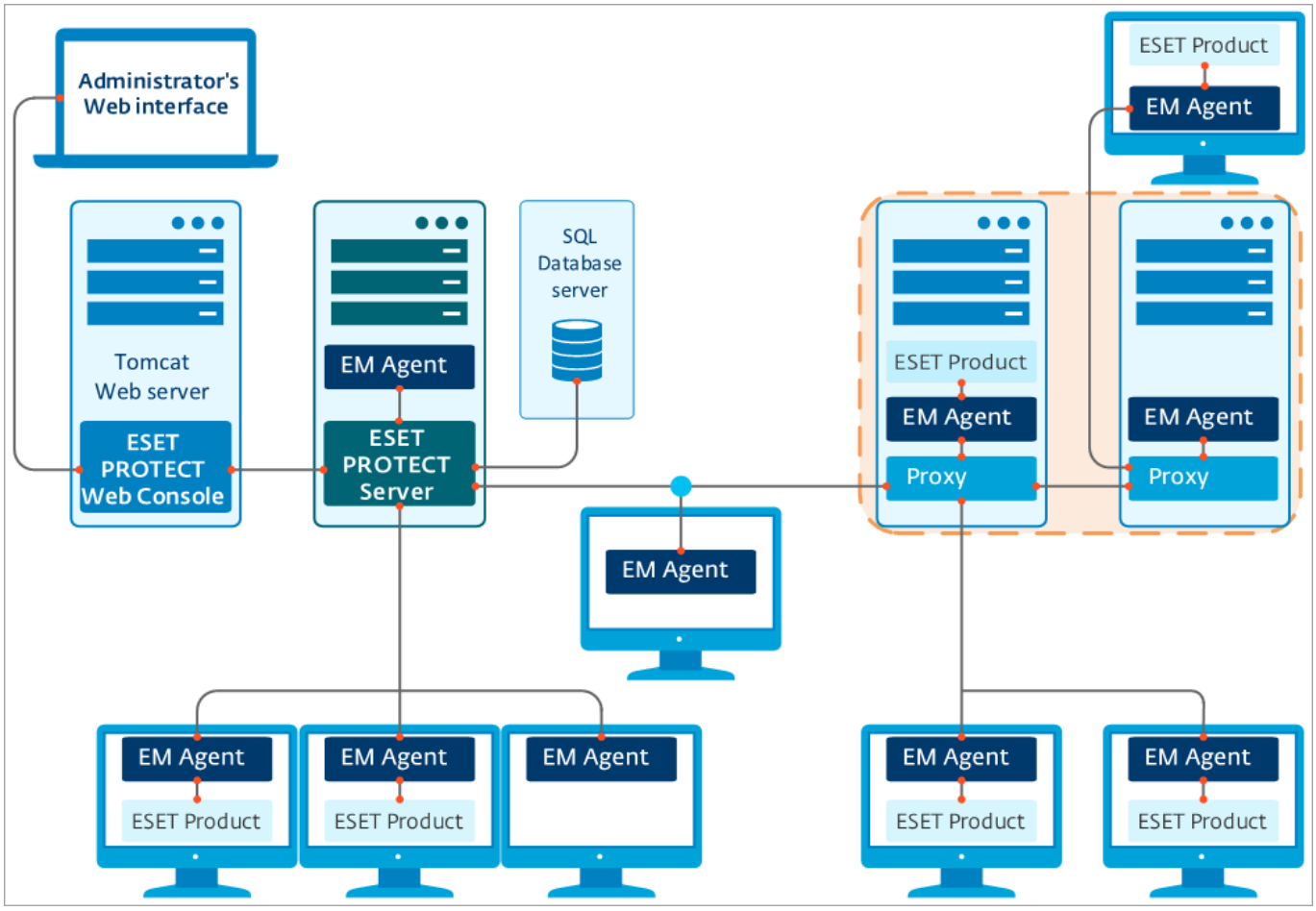
- Jeśli komputery agentów nie mogą nawiązać bezpośredniego połączenia z serwerem ESET PROTECT.
- W przypadku lokalizacji zdalnej lub oddziału serwer proxy może służyć do obsługi komunikacji:
  - omiędzy serwerem ESET PROTECT o serwerem proxy,
  - omiędzy serwerem proxy i komputerami klienckimi w lokalizacji zdalnej.

Jak skonfigurować serwer proxy HTTP

Aby można było korzystać z serwera proxy, należy skonfigurować nazwę hosta proxy HTTP w polityce agenta (**Ustawienia zaawansowane** > **Serwer proxy HTTP**). Do buforowania i przekazywania można używać różnych serwerów proxy. Zobacz ustawienia polityki poniżej:

- **Globalny serwer proxy** — będzie używane jedno rozwiązanie proxy do buforowania pobieranych plików i przekazywania komunikacji agenta.
- **Różne serwery proxy na usługę** — będą używane różne rozwiązania proxy do buforowania i przekazywania komunikacji.

Jakie inne funkcje udostępnia usługa Apache HTTP Proxy?



Serwer proxy Apache HTTP

Apache HTTP Proxy to usługa serwera proxy, z której można korzystać w celu dystrybuowania aktualizacji na komputerach klienckich.

Aby zainstalować usługę Apache HTTP Proxy, zapoznaj się z instrukcjami dla systemu Windows, systemu Linux lub urządzenia wirtualnego.

Funkcje Apache HTTP Proxy

Funkcja	Rozwiązanie proxy, które udostępnia tę funkcję
Buforowanie plików do pobrania i aktualizacji	Apache HTTP Proxy lub inne rozwiązanie proxy
Buforowanie wyników ESET LiveGuard Advanced	Tylko skonfigurowana usługa Apache HTTP Proxy
Komunikacja replikacji agenta ESET Management z serwerem ESET PROTECT	Apache HTTP Proxy lub inne rozwiązanie proxy

Funkcja pamięci podręcznej

Apache HTTP Proxypobieranie i zapisywanie w pamięci podręcznej:

- Aktualizacja modułów ESET

- Pakiety instalacyjne z serwerów repozytorium
- Aktualizacje komponentów produktów

Buforowane dane są dystrybuowane do klientów w punktach końcowych sieci. Buforowanie może znacznie zmniejszyć natężenie ruchu internetowego w sieci.

W odróżnieniu od narzędzia Mirror Tool, które pobiera wszystkie dane dostępne na serwerach aktualizacji ESET, Apache HTTP Proxy pobiera jedynie dane zgodne z żądaniami komponentów programu ESET PROTECT lub produktów ESET do obsługi punktów końcowych w celu zmniejszenia obciążenia sieci. Jeśli klient zainstalowany w punkcie końcowym wyśle żądanie aktualizacji, Apache HTTP Proxy pobierze aktualizację z serwerów aktualizacji ESET, zapisze aktualizację w swoim katalogu pamięci podręcznej i prześle ją do danego klienta zainstalowanego w punkcie końcowym. Jeśli inny klient zainstalowany w punkcie końcowym wyśle żądanie dotyczące tej samej aktualizacji, Apache HTTP Proxy prześle pliki do pobrania bezpośrednio z pamięci podręcznej, eliminując konieczność pobierania aktualizacji po raz kolejny z serwerów aktualizacji ESET.

Pamięć podręczna do produktu ESET Endpoint

Ustawienia pamięci podręcznej agenta i punktu końcowego ESET Management nie są takie same. Agent ESET Management może zarządzać ustawieniami produktów zabezpieczających ESET na urządzeniach klienckich. Serwer proxy na potrzeby rozwiązania ESET Endpoint Security można skonfigurować:

- lokalnie, z graficznego interfejsu użytkownika;
- z konsoli internetowej ESET PROTECT przy użyciu polityki (jest to zalecany sposób zarządzania ustawieniami urządzeń klienckich).

Buforowanie wyników z ESET LiveGuard Advanced

Apache HTTP Proxy może też buforować wyniki z ESET LiveGuard Advanced. Buforowanie wymaga określonej konfiguracji, która jest zawarta w rozwiązaniu Apache HTTP Proxy dystrybuowanym przez ESET. Zaleca się, by w miarę możliwości używać buforowania z ESET LiveGuard Advanced. Więcej informacji zawiera dokumentacja usługi.

Używanie oprogramowania Apache jako proxy HTTP do komunikacji agent-serwer

Po odpowiednim skonfigurowaniu można używać usługi Apache HTTP Proxy do gromadzenia i przekazywania danych z komponentów programu ESET PROTECT w lokalizacji zdalnej. Jednego rozwiązania proxy można używać do buforowania aktualizacji (zalecana jest usługa Apache HTTP Proxy), a drugiego — do komunikacji między agentem a serwerem. Usługi Apache HTTP Proxy można używać w obu celach jednocześnie, ale nie jest to zalecane w przypadku sieci mających ponad 10 000 komputerów klienckich na jeden komputer z serwerem proxy. W środowiskach korporacyjnych (w których liczba zarządzanych komputerów przekracza 1000) zalecamy korzystanie z dedykowanego serwera Apache HTTP Proxy.

Więcej informacji o funkcji proxy.

Jak skonfigurować serwer proxy HTTP

Aby można było korzystać z serwera proxy, należy skonfigurować nazwę hosta proxy HTTP w polityce agenta (**Ustawienia zaawansowane** > **Serwer proxy HTTP**). Do buforowania i przekazywania można używać różnych

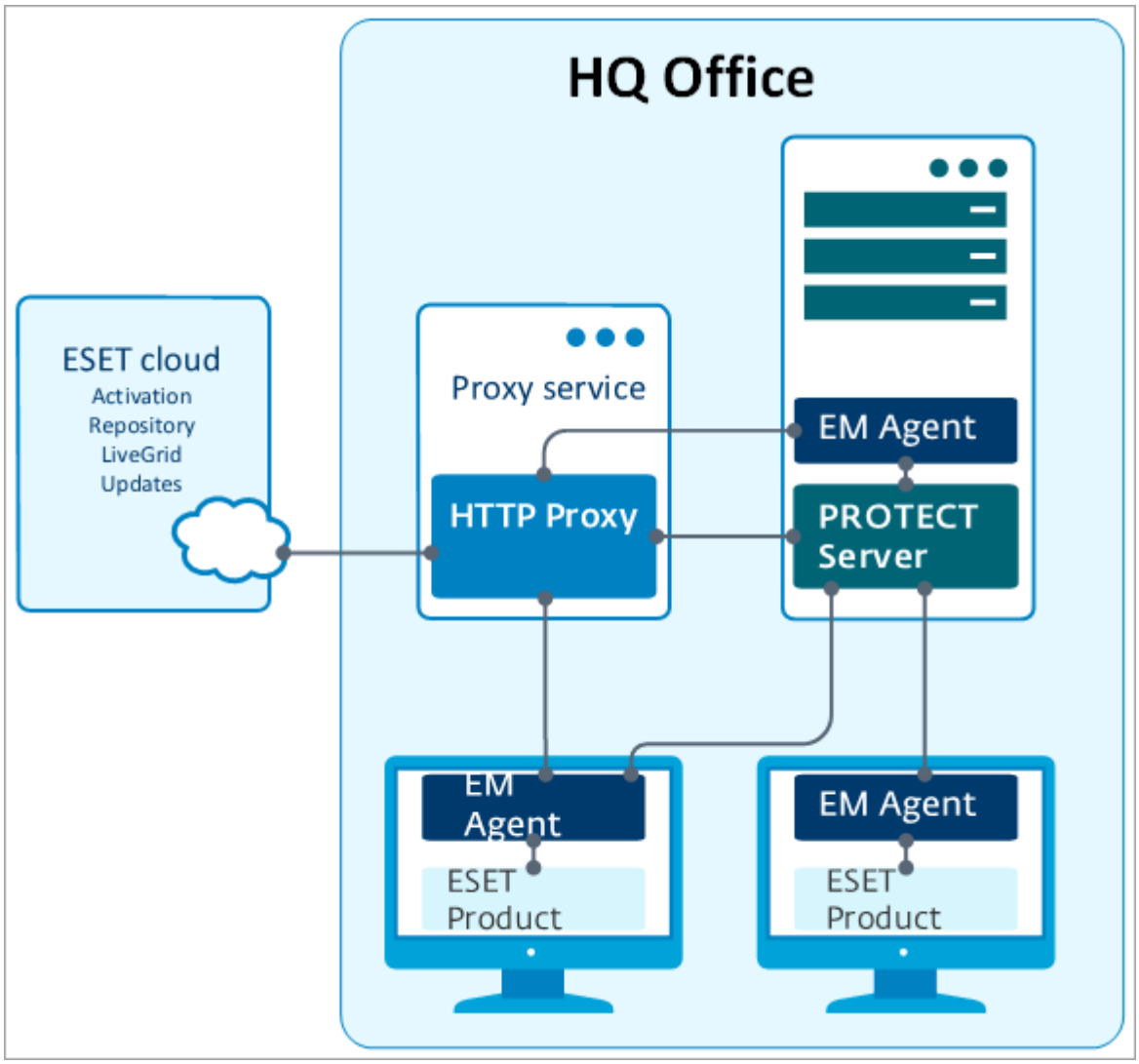
serwerów proxy. Zobacz ustawienia polityki poniżej:

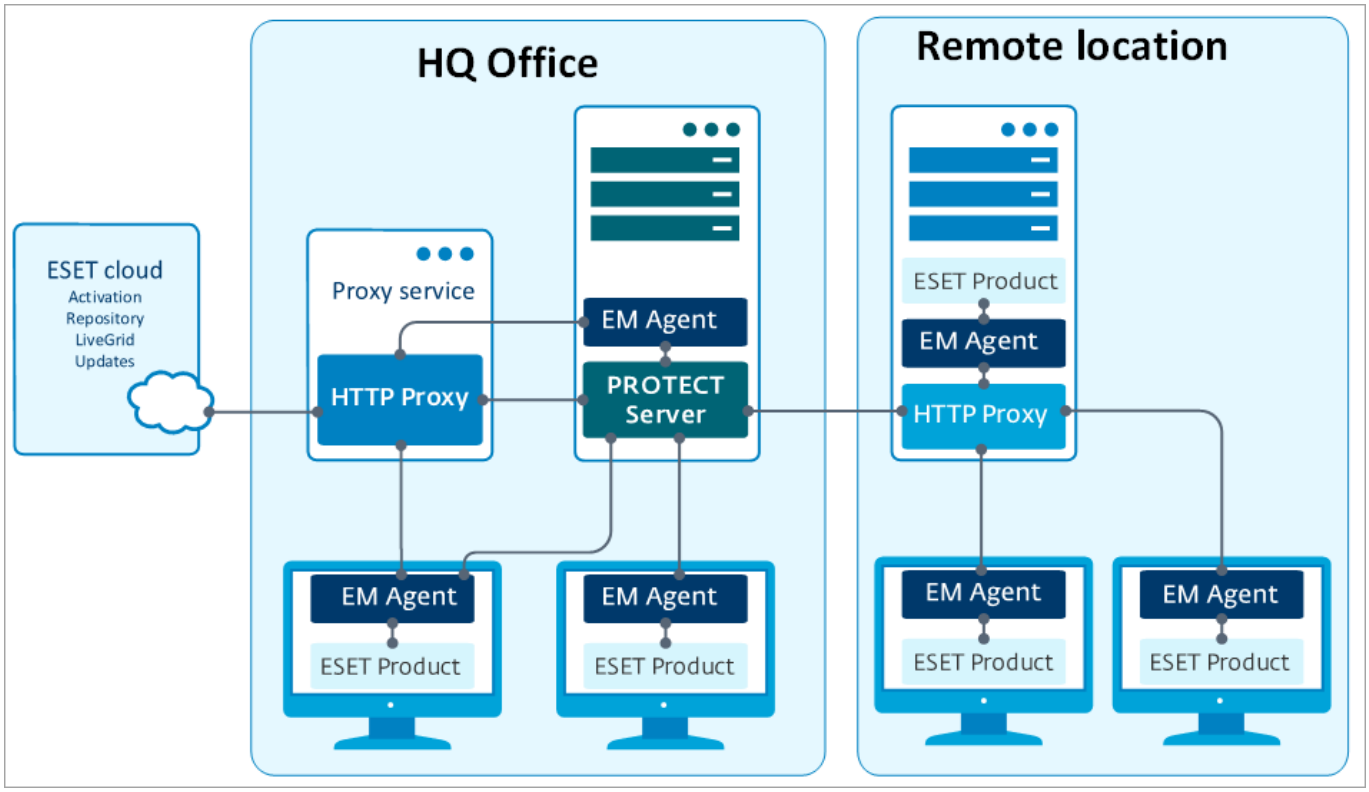
- **Globalny serwer proxy** — będzie używane jedno rozwiązanie proxy do buforowania pobieranych plików i przekazywania komunikacji agenta.

- **Różne serwery proxy na usługę** — będą używane różne rozwiązania proxy do buforowania i przekazywania komunikacji.

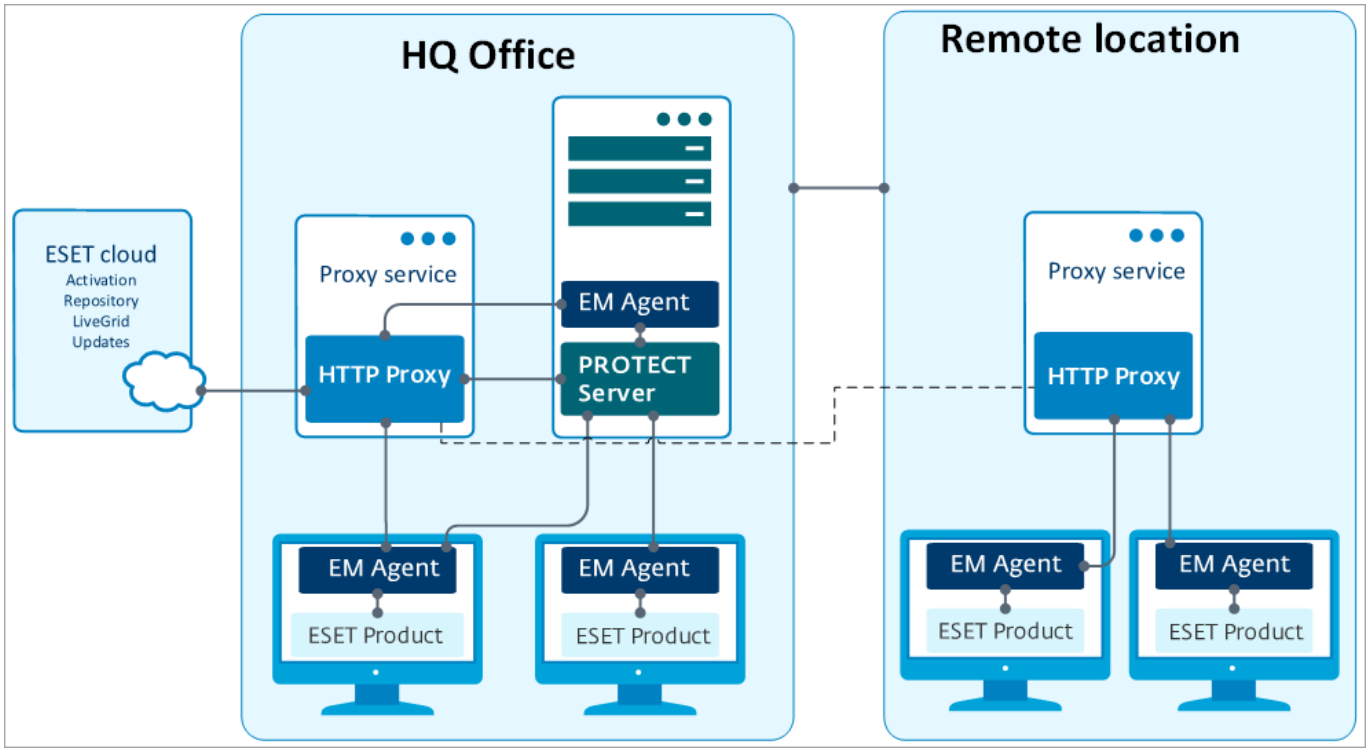
Serwer Apache HTTP Proxy w infrastrukturze

Poniższy diagram ilustruje działanie serwera proxy (Apache HTTP Proxy) używanego do dystrybucji ruchu sieciowego w chmurze ESET pomiędzy wszystkimi komponentami ESET PROTECT oraz produktami ESET do obsługi punktów końcowych.





W celu dodania kolejnej usługi proxy w lokalizacji zdalnej można posłużyć się łańcuchem serwerów proxy. Należy pamiętać, że ESET PROTECT nie obsługuje łańcuchów serwerów proxy, w których serwery proxy wymagają uwierzytelnienia. Można używać własnego transparentnego rozwiązania serwerów WWW proxy, jednak może ono wymagać dodatkowej konfiguracji, której nie omówiono w niniejszym dokumencie.



W przypadku aktualizacji silnika detekcji offline należy użyć narzędzia Mirror Tool (dostępnego dla systemu Windows i Linux) zamiast serwera proxy Apache HTTP.

Agent

Agent ESET Management to kluczowa część programu ESET PROTECT. Klienty nie komunikują się bezpośrednio z serwerem ESET PROTECT. Komunikacja ta odbywa się za pośrednictwem agenta. Agent gromadzi informacje pozyskiwane od klienta i wysyła je do serwera ESET PROTECT. Gdy serwer ESET PROTECT wysyła zadanie do klienta, trafia ono do agenta, który następnie przekazuje je do klienta. Agent ESET Management używa nowego, ulepszonego protokołu komunikacji.

W celu uproszczenia wdrażania rozwiązań do ochrony punktów końcowych do pakietu ESET ManagementESET PROTECT dołączany jest samodzielny agent . Jest to prosta usługa modułowa, która nie wymaga wielu zasobów i obsługuje całość komunikacji pomiędzy serwerem ESET PROTECT a dowolnymi produktami firmy ESET oraz systemami operacyjnymi. Zamiast komunikować się bezpośrednio z serwerem ESET PROTECT, produkty firmy ESET komunikują się za pośrednictwem agenta. Komputery klienckie z zainstalowanym agentem ESET Management, które są w stanie komunikować się z serwerem ESET PROTECT, nazywane są komputerami „zarządzanymi”. Agenta można zainstalować na dowolnym komputerze, niezależnie od tego, czy zainstalowano na nim inne oprogramowanie firmy ESET.

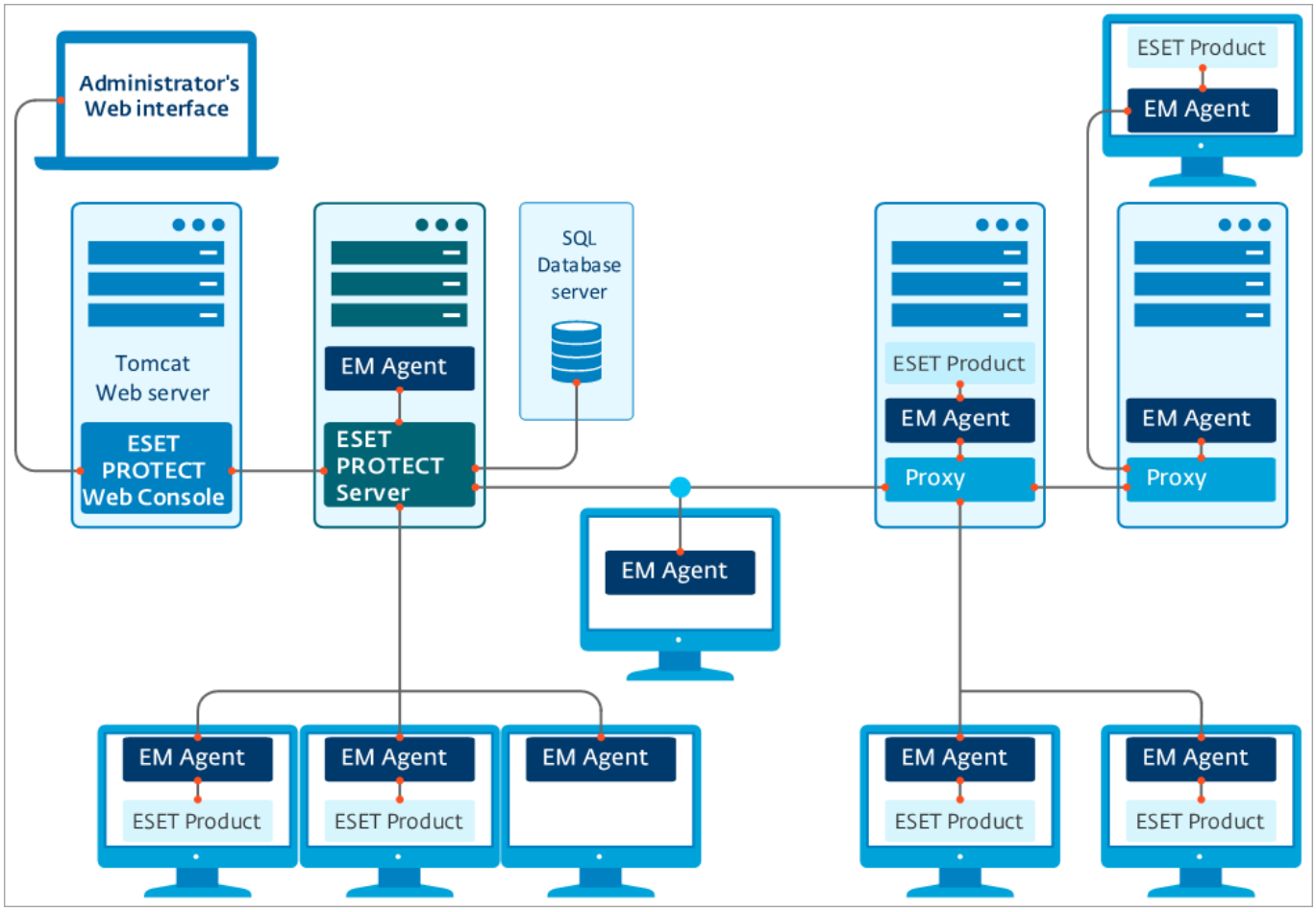
Wiążą się z tym następujące korzyści:

- Łatwość konfiguracji — możliwe jest wdrożenie agenta w ramach standardowej instalacji korporacyjnej.

- Zarządzanie zabezpieczeniami na miejscu — agenta można skonfigurować tak, aby przechowywał wiele scenariuszy zabezpieczeń, dlatego czas reakcji na wykrycie ulega znacznemu skróceniu.

- Zarządzanie zabezpieczeniami w trybie offline — agent może zareagować na zdarzenie nawet wtedy, gdy nie jest połączony z serwerem ESET PROTECT.

Protokół komunikacji między agentem a serwerem ESET PROTECT nie obsługuje uwierzytelniania. Żadne rozwiązanie proxy używane do przekazywania komunikacji agenta na serwer ESET PROTECT i wymagające uwierzytelniania nie będzie działać.
Jeśli port domyślny używany dla konsoli internetowej lub agenta zostanie zmieniony, może być konieczna korekta ustawień zapory. W przeciwnym razie instalacja może się nie powieść.



Moduł Rogue Detection Sensor

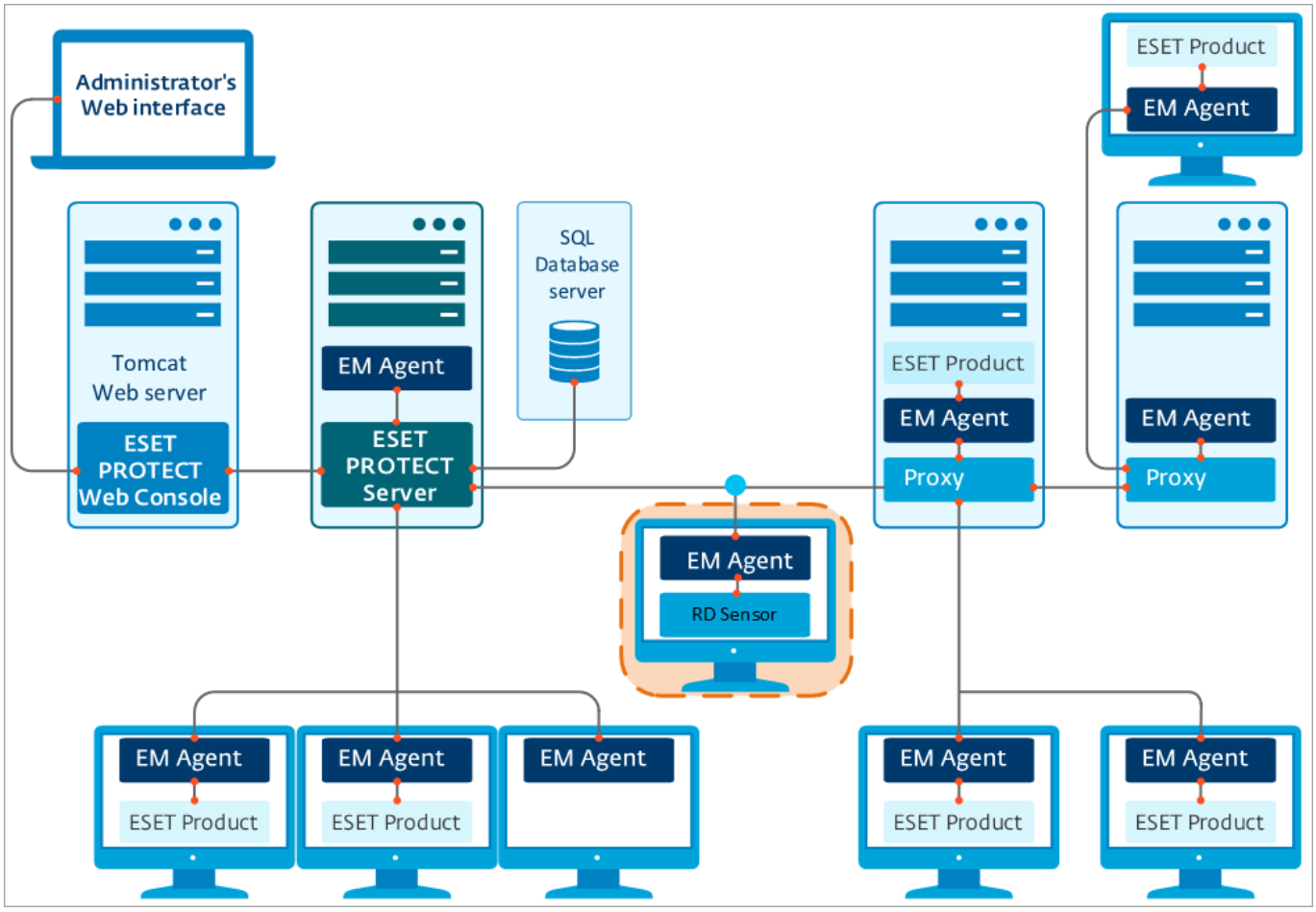
Rogue Detection Sensor (RD Sensor) to narzędzie systemowe do wykrywania komputerów w sieci użytkownika. Narzędzie RD Sensor stanowi udogodnienie, ponieważ umożliwia zlokalizowanie nowych komputerów w programie ESET PROTECT bez konieczności ich ręcznego wyszukiwania i dodawania. Wykryte urządzenia są natychmiast lokalizowane i uwzględniane we wstępnie zdefiniowanym raporcie, co umożliwia przeniesienie ich do określonych grup statycznych i przystąpienie do realizowania w odniesieniu do nich zadań związanych z zarządzaniem.

RD Sensor aktywnie nasłuchuje emisji ARP. Gdy RD Sensor wykryje nowy aktywny komponent sieci, wysyła emisje jednokrotne ARP, wykonuje odciski palców hosta (przy użyciu kilku portów) i wysyła informacje o wykrytych komputerach do serwera ESET PROTECT. Serwer ESET PROTECT dokonuje następnie oceny, czy komputery znalezione w sieci są nieznane na serwerze ESET PROTECT, czy może są już obsługiwane.

Nie można wyłączyć odcisków palców hosta, ponieważ jest to główna funkcja narzędzia RD Sensor.

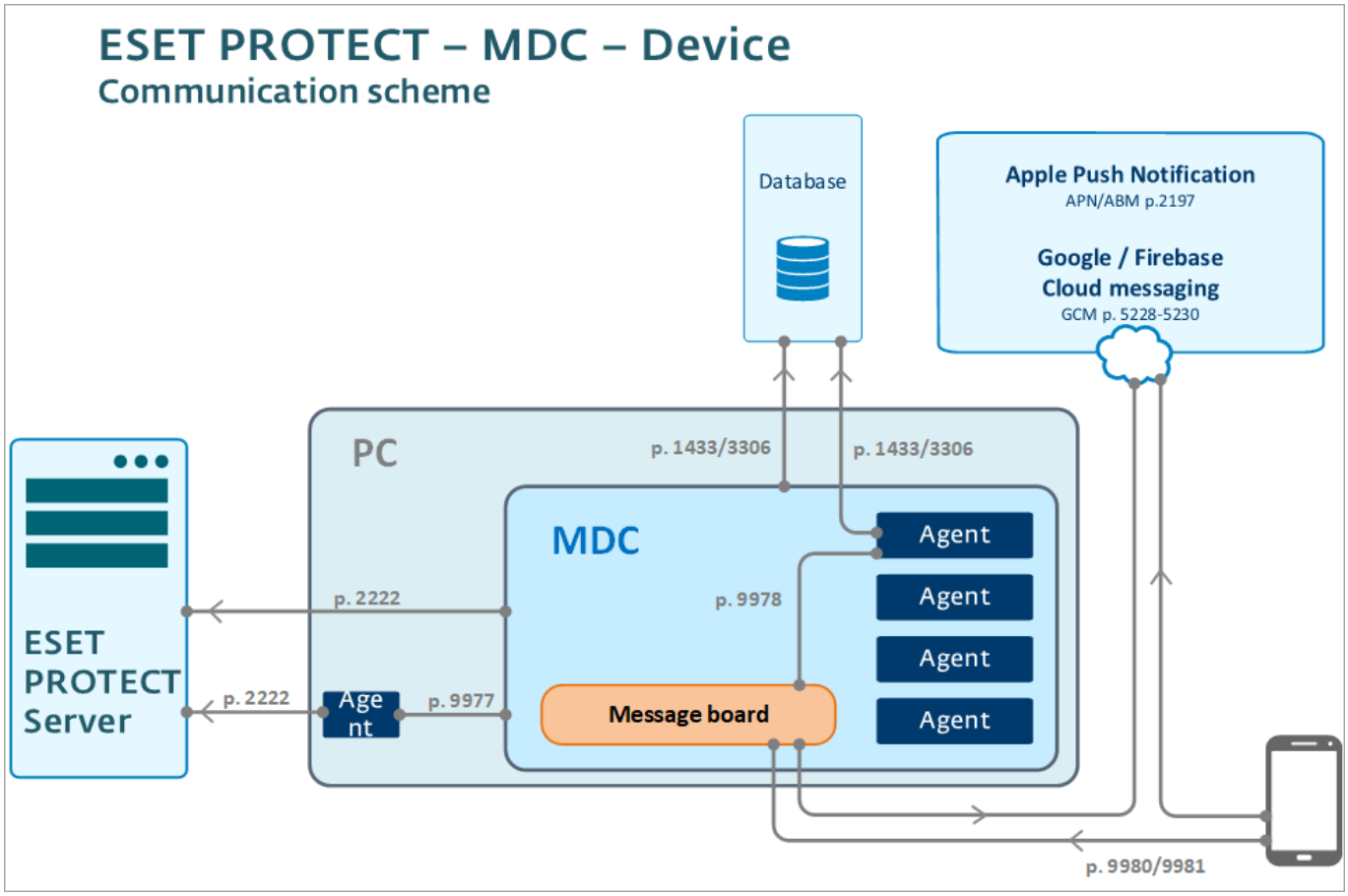
Jeśli istnieje wiele segmentów sieci, Rogue Detection Sensor musi być zainstalowany osobno w każdym segmencie sieci, aby uzyskać pełną listę wszystkich urządzeń w całej sieci.

Każdy komputer w ramach struktury sieci (domeny, usługi LDAP, sieci Windows) zostaje automatycznie dodany do listy komputerów na serwerze ESET PROTECT przy użyciu zadania synchronizacji serwera. Korzystanie z narzędzia RD Sensor to wygodny sposób wyszukiwania komputerów, które nie znajdują się w domenie ani innej strukturze sieci, oraz dodawania ich do serwera ESET PROTECT. Wykryte komputery są zapamiętywane w narzędziu RD Sensor i te same informacje nie są wysyłane ponownie.



Moduł zarządzania urządzeniami mobilnymi

Moduł zarządzania urządzeniami mobilnymi firmy ESET PROTECT to komponent umożliwiający zarządzanie urządzeniami mobilnymi z systemem Android lub iOS przy użyciu programu ESET PROTECT oraz administrowanie programem ESET Endpoint Security w systemie Android.



Powiększyć obraz

> Zalecamy wdrożenie komponentu MDM na innym urządzeniu hosta niż to, na którym jest hostowany serwer ESET PROTECT.

Poniżej prezentujemy zalecane wstępne wymagania sprzętowe na potrzeby około 80 zarządzanych urządzeń mobilnych:

Sprzęt	Zalecana konfiguracja
Procesor	4 rdzenie, 2,5 GHz
PAMIĘĆ RAM	4 GB (zalecane)
HDD	100 GB

W przypadku ponad 80 zarządzanych urządzeń mobilnych wymagania sprzętowe nie są dużo większe. Opóźnienie między przesłaniem zadania z programu ESET PROTECT a jego wykonaniem na urządzeniu mobilnym wzrasta proporcjonalnie do liczby urządzeń działających w środowisku.

Postępuj zgodnie z instrukcjami instalacji MDM dla systemu Windows(Instalator kompleksowy lub instalacja składników) lub Linux.

Różnice pomiędzy serwerem proxy Apache HTTP,

narzędziem Mirror Tool a połączeniem bezpośrednim

Komunikacja pomiędzy produktami ESET obejmuje aktualizacje silnika detekcji oraz modułów programów, a także wymianę danych ESET LiveGrid® (patrz poniższa tabela) oraz informacji dotyczących licencji.

Program ESET PROTECT pobiera najnowsze produkty, które następnie dystrybuuje pomiędzy komputerami klienckimi przy użyciu repozytorium. Po rozdystrybuowaniu produkt jest gotowy do wdrożenia na urządzeniu docelowym.

Po zainstalowaniu produktu zabezpieczającego ESET należy go aktywować, co oznacza konieczność zweryfikowania informacji dotyczących licencji poprzez porównanie ich z danymi na serwerze licencji. Po dokonaniu aktywacji silnik detekcji oraz moduły programu są regularnie aktualizowane.

System monitorowania zagrożeń ESET LiveGrid® umożliwia natychmiastowe i ciągłe informowanie programów ESET o nowych infekcjach w celu zapewnienia naszym klientom szybkiej ochrony. System ten umożliwia przesyłanie nowych wykryć do laboratorium firmy ESET, w którym są one analizowane i przetwarzane.

Większość ruchu sieciowego jest generowana przez aktualizacje modułów produktów. W ujęciu ogólnym produkt zabezpieczający ESET pobiera około 23,9 MB aktualizacji modułów programu miesięcznie.

Dane systemu ESET LiveGrid® (około 22,3 MB) oraz plik wersji aktualizacji (maks. 11 KB) to jedyne z dystrybuowanych plików, które nie mogą być zapisywane w pamięci podręcznej.

Istnieją dwa typy aktualizacji — aktualizacje poziomowe i nanoaktualizacje. Więcej informacji na temat typów aktualizacji zawiera ten artykuł bazy wiedzy.

Istnieją 2 sposoby na zmniejszenie obciążenia sieci podczas dystrybucji aktualizacji w ramach sieci komputerowej: serwer proxy Apache HTTP lub narzędzie Mirror Tool (dostępne dla systemów Windows i Linux).

> Zapoznaj się z tym artykułem z bazy wiedzy, aby skonfigurować tworzenie łańcucha przy użyciu narzędzia Mirror Tool (konieczne jest skonfigurowanie narzędzia Mirror Tool w taki sposób, aby pobierało aktualizacje z innego narzędzia Mirror Tool).

Typy komunikacji w produktach ESET

Typ komunikacji	Częstotliwość komunikacji	Wpływ na ruch sieciowy	Komunikacja przekazywana przez serwer proxy	Opcja buforowania serwera proxy1	Opcja kopii dystrybucyjnej2	Opcja środowiska offline
Wdrożenie agenta (instalacja wypychana lub instalatory live z repozytorium)	Jednorazowo	Około 50 MB na klienta	TAK	TAK3	NIE	TAK (GPO/SCCM, edytowane instalatory live)4

Typ komunikacji	Częstotliwość komunikacji	Wpływ na ruch sieciowy	Komunikacja przekazywana przez serwer proxy	Opcja buforowania serwera proxy1	Opcja kopii dystrybucyjnej2	Opcja środowiska offline
Instalacja w punkcie końcowym (instalacja oprogramowania z repozytorium)	Jednorazowo	Około 100 MB na klienta	TAK	TAK3	NIE	TAK (GPO / SCCM, instalacja na podstawie adresu URL pakietu)4
Aktualizacja modułu silnika detekcji/modułu programu	Ponad 6 razy dziennie	23,9 MB miesięcznie5	TAK	TAK	TAK	TAK (narzędzie działające w trybie offline Mirror Tool i niestandardowy serwer HTTP)6
Plik wersji aktualizacji update.ver	Około 8 razy dziennie	2,6 MB miesięcznie7	TAK	NIE	-	-
Aktywacja / weryfikacja licencji	4 razy dziennie	Zaniedbywalny	TAK	NIE	NIE	TAK (pliki w trybie offline generowane przez narzędzie ESET Business Account)8
Reputacja ESET LiveGrid® oparta na chmurze	Na bieżąco	11 MB miesięcznie	TAK	NIE	NIE	NIE

1.Informacje na temat buforowania serwera proxy i jego zalet można znaleźć w sekcji Kiedy zacząć używać serwera proxy Apache HTTP?

2.Informacje na temat kopii dystrybucyjnej można znaleźć w sekcji Kiedy zacząć używać narzędzia Mirror Tool?

3.Jednokrotnie w ramach instalacji lub uaktualnienia zalecamy wdrożenie na początku jednego agenta (po jednym dla danej wersji) / punktu końcowego, aby umożliwić zapisanie instalatora w pamięci podręcznej.

4.Informacje na temat wdrażania agenta ESET Management w dużej sieci można znaleźć w sekcji Wdrażanie agenta przy użyciu obiektu GPO lub programu SCCM.

5.Pierwsza aktualizacja silnika detekcji może być większa niż zwykle, w zależności od wieku pakietu instalacyjnego, ponieważ pobierane są wszystkie nowsze aktualizacje silnika detekcji i aktualizacje modułu. Zalecamy zainstalowanie na początek jednego klienta i umożliwienie mu przeprowadzenia aktualizacji, aby potrzebne aktualizacje silnika detekcji oraz modułów programu zostały zapisane w pamięci podręcznej.

6.W przypadku braku połączenia internetowego narzędzie Mirror Tool nie może pobierać aktualizacji silnika detekcji. Można skorzystać z serwera Apache Tomcat w charakterze serwera HTTP w celu pobrania aktualizacji do katalogu dostępnego w narzędziu Mirror Tool (dostępne dla systemów Windows i Linux).

7.Podczas sprawdzania aktualizacji silnika detekcji zawsze pobierany jest i analizowany plik *update.ver*. Domyślnie harmonogram będącego punktem końcowym produktu ESET co godzinę wysyła zapytania o nowe aktualizacje. Zakładamy, że kliencka stacja robocza jest włączona przez 8 godzin dziennie. Rozmiar

pliku *update.ver* to około 11 kB.

8.Pobierz pliki licencji offline z programu ESET Business Administrator.

W wersjach 4 i 5 produktów korzystających z serwera proxy Apache HTTP nie można buforować aktualizacji. Aby rozpowszechniać aktualizacje dla tych produktów, użyj narzędzia Mirror Tool.

Kiedy zacząć używać serwera proxy Apache HTTP

Na podstawie przeprowadzonych przez nas testów zalecamy wdrożenie serwera proxy Apache HTTP w przypadku sieci złożonych z co najmniej 37 komputerów.

Dla skutecznego buforowania niezbędne jest, aby data i godzina na serwerze proxy HTTP była poprawnie ustawiona. Kilkuminutowe różnice spowodowałyby, że mechanizm buforowania nie działałby skutecznie, pobierając więcej plików, niż jest to konieczne.

Na podstawie analiz wykorzystania przepustowości wyłącznie na potrzeby aktualizacji w sieci testowej złożonej z 1.000 komputerów, w której przeprowadzono kilka instalacji i dezinstalacji ustalono co następuje:

- jeden komputer pobiera średnio 23,9 MB aktualizacji miesięcznie, jeśli łączy się bezpośrednio z Internetem (bez zastosowania serwera proxy Apache HTTP);
- przy zastosowaniu serwera proxy Apache HTTP łączne pobrania w całej sieci wyniosły 900 MB miesięcznie.

Proste zestawienie ilości danych aktualizacji pobieranych miesięcznie w przypadku bezpośredniego połączenia z Internetem lub serwera proxy Apache HTTP w sieci komputerowej:

Liczba komputerów w sieci korporacyjnej	25	36	50	100	500	1.000
Bezpośrednie połączenie z Internetem (MB/mies.)	375	900	1.250	2.500	12.500	25 000
Serwer proxy Apache HTTP (MB/mies.)	30	50	60	150	600	900

Kiedy zacząć używać narzędzia Mirror Tool

W przypadku pracy w środowisku offline, w którym komputery w sieci nie łączą się z Internetem przez dłuższy czas (kilka miesięcy, rok), narzędzie Mirror Tool (dostępne dla systemów Windows i Linux) jest jedynym sposobem dystrybuowania aktualizacji modułów produktów, ponieważ umożliwia ono pobranie wszystkich dostępnych aktualizacji poziomowych i nanoaktualizacji po otrzymaniu każdego żądania dotyczącego informacji o udostępnieniu nowej aktualizacji.

Zapoznaj się z tym artykułem z bazy wiedzy, aby skonfigurować tworzenie łańcucha przy użyciu narzędzia Mirror Tool (konieczne jest skonfigurowanie narzędzia Mirror Tool w taki sposób, aby pobierało aktualizacje z innego narzędzia Mirror Tool).

Najważniejszą różnicą pomiędzy serwerem proxy Apache HTTP oraz narzędziem Mirror Tool jest fakt, że serwer proxy Apache HTTP pobiera wyłącznie brakujące aktualizacje (na przykład nanoaktualizację 3), natomiast narzędzie Mirror Tool pobiera wszystkie dostępne aktualizacje poziomowe i nanoaktualizacje (lub tylko

aktualizacje poziomowe, jeśli tak zostanie skonfigurowane), niezależnie od tego, której aktualizacji określonego modułu brakuje.

> Aktualizacje przesyłane strumieniowo nie są dostępne w narzędziu Mirror Tool. Zalecamy preferowanie aktualizacji za pośrednictwem serwera proxy HTTP z wykorzystaniem kopii dystrybucyjnych, jeśli to możliwe. Wybierz tę opcję nawet wtedy, gdy komputer jest w trybie offline, ale ma dostęp do innego komputera podłączonego do Internetu i może uruchamiać serwer proxy HTTP do buforowania plików aktualizacji.

Zastosowanie narzędzia Mirror Tool zamiast serwera proxy Apache HTTP przetestowaliśmy w tej samej sieci złożonej z 1.000 komputerów. Na podstawie analizy ustaliliśmy, że w miesiącu pobranych zostało 5500 MB aktualizacji. Wielkość pobieranych aktualizacji nie zwiększyła się w wyniku dodania do sieci kolejnych komputerów. Jest to w dalszym ciągu ogromne zmniejszenie obciążenia w porównaniu do konfiguracji, w której klienty łączą się bezpośrednio z Internetem, jednak poprawa wydajności nie jest tak znacząca jak w przypadku zastosowania serwera proxy HTTP.

Liczba komputerów w sieci korporacyjnej	25	36	50	100	500	1.000
Bezpośrednie połączenie z Internetem (MB/mies.)	375	900	1.250	2.500	12.500	25.000
Mirror Tool (MB/mies.)	5.500	5.500	5.500	5.500	5.500	5.500

> Nawet jeśli w sieci jest więcej niż 1.000 komputerów, wykorzystanie przepustowości w związku z aktualizacjami nie zwiększa się znacząco zarówno w przypadku zastosowania serwera proxy Apache HTTP, jak i narzędzia Mirror Tool.

Wymagania systemowe i rozmiary

Aby można było zainstalować i uruchomić ESET PROTECT, Twój system musi spełniać wymagania wstępne dotyczące sprzętu, bazy danych, sieci i oprogramowania.

Obsługiwane systemy operacyjne

W poniższych sekcjach opisano zgodność składników ESET PROTECT z poszczególnymi wersjami systemu Windows, Linux, macOS i mobilnymi systemami operacyjnymi.

System Windows

W poniższej tabeli wymieniono systemy operacyjne Windows obsługiwane przez poszczególne komponenty programu ESET PROTECT.

System operacyjny	Serwer	Agent	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1z zainstalowanymi poprawkami KB4474419 i KB4490628		✔	✔	
Windows Server 2008 R2 CORE x64z zainstalowanymi poprawkami KB4474419 i KB4490628		✔	✔	
Windows Storage Server 2008 R2 x64z zainstalowanymi poprawkami KB4474419 i KB4490628		✔	✔	

System operacyjny	Serwer	Agent	RD Sensor	MDM
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
Windows Server 2012 x64	✔	✔	✔	✔
Windows Server 2012 CORE x64	✔	✔	✔	✔
Windows Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2012 R2 CORE x64	✔	✔	✔	✔
Windows Storage Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2016 x64	✔	✔	✔	✔
Windows Storage Server 2016 x64	✔	✔	✔	✔
Windows Server 2019 x64	✔	✔	✔	✔
Windows Server 2022 x64	✔	✔	✔	✔

System operacyjny	Serwer	Agent	RD Sensor	MDM
Windows 7 x86 SP1 z najnowszymi aktualizacjami systemu Windows (co najmniej KB4474419 i KB4490628)		✔	✔	
Windows 7 x64 SP1 z najnowszymi aktualizacjami systemu Windows (co najmniej KB4474419 i KB4490628)		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64	*	✔	✔	*
Windows 8.1 x86		✔	✔	
Windows 8.1 x64	*	✔	✔	*
Windows 10 x86		✔	✔	
Windows 10 x64 (wszystkie oficjalne wersje)	*	✔	✔	*
Windows 10 na ARM		✔		
Windows 11 x64	*	✔	✔	*

* Instalowanie komponentów ESET PROTECT w systemie operacyjnym klienta może być niezgodne z zasadami licencjonowania firmy Microsoft. Aby uzyskać szczegółowe informacje, należy zapoznać się z zasadami licencjonowania firmy Microsoft lub skontaktować się z dostawcą oprogramowania. W małych i średnich firmach

oraz środowiskach z małymi sieciami zachęcamy do instalacji programu ESET PROTECT w wersji na system Linux lub urządzenia wirtualnego, gdy ma to zastosowanie.

W przypadku starszych systemów MS Windows:
• Musi być zawsze zainstalowana najnowsza wersja dodatku Service Pack, szczególnie w starszych systemach takich jak Server 2008 i Windows 7.
• ESET PROTECT nie obsługuje zarządzania komputerami z systemem Windows 7 (bez SP), Widows Vista ani Windows XP.
• Od 24 marca 2020 r. firma ESET nie będzie już oficjalnie obsługiwać ani zapewniać pomocy technicznej dla produktu ESET PROTECT (serwer i usługa MDM) zainstalowanego w następujących systemach operacyjnych Microsoft Windows: Windows 7, Windows Server 2008 (wszystkie wersje).
Nie obsługujemy nielegalnych lub pirackich systemów operacyjnych.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

Możesz uruchamiać ESET PROTECT na nieserwerowym systemie operacyjnym bez konieczności korzystania z oprogramowania ESXi. W systemie operacyjnym komputera stacjonarnego można zainstalować program VMware Player, a następnie wdrożyć urządzenie wirtualne ESET PROTECT.

Linux

W poniższej tabeli wymieniono systemy operacyjne Linux obsługiwane przez poszczególne komponenty programu ESET PROTECT:

System operacyjny	Serwer	Agent	RD Sensor	MDM
Ubuntu 16.04.1 LTS x86 Desktop		✔	✔	
Ubuntu 16.04.1 LTS x86 Server		✔	✔	
Ubuntu 16.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 16.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Desktop	✔	✔	✔	✔
Ubuntu 18.04.1 LTS x64 Server	✔	✔	✔	✔
Ubuntu 20.04 LTS x64	✔	✔	✔	✔
RHEL Server 7 x86		✔	✔	
RHEL Server 7 x64	✔	✔	✔	✔
RHEL Server 8 x64	✔*	✔		✔
CentOS 7 x64	✔	✔	✔	✔
SLED 15 x64	✔	✔	✔	✔
SLES 12 x64	✔	✔	✔	✔
SLES 15 x64	✔	✔	✔	✔
OpenSUSE Leap 15.2 x64	✔	✔	✔	✔

System operacyjny	Serwer	Agent	RD Sensor	MDM
Debian 9 x64	✔	✔	✔	✔
Debian 10 x64	✔	✔	✔	✔
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

* Red Hat Entreprise Linux Server 8.x nie obsługuje generowania raportów *.pdf* – więcej szczegółów znajdziesz w rozwiązaniach znanych problemów z produktem ESET PROTECT.

macOS

System operacyjny	Agent
macOS 10.12 Sierra	✔
macOS 10.13 High Sierra	✔
macOS 10.14 Mojave	✔
macOS 10.15 Catalina	✔
macOS 11.0 Big Sur	✔
macOS 12.0 Monterey	✔
macOS 13.0 Ventura	✔

System macOS jest obsługiwany wyłącznie w charakterze klienta. Agenta ESET Management i produkty ESET dla systemu macOS można zainstalować w systemie macOS. Jednak w systemie tym nie można zainstalować serwera ESET PROTECT.

Urządzenie mobilne

System operacyjny	EESA	Właściciel urządzenia z aplikacją EESA	Komponent MDM na urządzeniach z systemem iOS	MDM iOS ABM
Android 5.x+	✔			
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔			
iOS 9.x+			✔	*

System operacyjny	EESA	Właściciel urządzenia z aplikacją EESA	Komponent MDM na urządzeniach z systemem iOS	MDM iOS ABM
iOS 10.x+			✔	*
iOS 11.x+			✔	*
iOS 12.0.x			✔	*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔

* System iOS DEP jest dostępny w wybranych krajach.

Zalecamy zaktualizowanie systemu operacyjnego zainstalowanego na urządzeniu mobilnym do najnowszej wersji, aby otrzymywać ważne poprawki dotyczące bezpieczeństwa.

Wymagania dotyczące systemu iOS 10.3 lub nowszego:

Od czasu wydania systemu iOS w wersji 10.3 urząd certyfikacji zainstalowany w ramach profilu rejestracji może nie być automatycznie oznaczony jako zaufany. Aby rozwiązać ten problem, wykonaj następujące czynności:

a)Użyj certyfikatu wystawionego przez zaufanego wystawcę firmy Apple.

b)Zainstaluj ręcznie zaufanie certyfikatu przed rejestracją. Oznacza to konieczność ręcznego zainstalowania głównego urzędu certyfikacji na urządzeniu mobilnym przed rejestracją i włączenia pełnego zaufania dla zainstalowanego certyfikatu.

Wymagania dotyczące systemu iOS 12:

Zapoznaj się z wymaganiami dotyczącymi systemu iOS 10.3 lub nowszego.

- Połączenie musi korzystać z protokołu **TLS 1.2 lub nowszego**.
- Połączenie musi korzystać z szyfrowania symetrycznego **AES-128** lub **AES-256**. Zestaw szyfrowania negocjowanego połączenia TLS musi obsługiwać funkcję **doskonałego utajnienia przekazywania (PFS)** za pośrednictwem **wymiany kluczy ECDHE**. Musi to być jeden z poniższych zestawów:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

```
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- Wymagany jest podpis przy użyciu **klucza RSA** o długości **co najmniej 2048 bitów**. Algorytmem tworzenia wartości skrótu certyfikatu musi być algorytm **SHA-2 o długości skrótu** (nazywany czasem „odciskiem palca”) wynoszącej no najmniej 256 (czyli **SHA-256 lub większy**). Certyfikat spełniający te wymagania można wygenerować w programie ESET PROTECT z włączoną opcją Zaawansowane zabezpieczenia.

- Certyfikat musi obejmować **cały łańcuch certyfikatów, włącznie z głównym urzędem certyfikacji**. Główny urząd certyfikacji występujący w certyfikacie służy do ustanawiania zaufania z urządzeniami i jest instalowany w ramach profilu rejestracji MDM.

Wymagania dotyczące systemu iOS 13:

- Zarządzanie urządzeniami mobilnymi z systemem iOS 13 wymaga spełnienia nowych wymagań firmy Apple dla certyfikatów komunikacyjnych (MDM HTTPS). Certyfikaty wydane przed 1 lipca 2019 r. również muszą spełniać te kryteria.

- Certyfikat HTTPS podpisany przez urząd certyfikacji ESMC nie spełnia tych wymagań.

Stanowczo zaleca się, aby nie aktualizować urządzeń mobilnych do wersji iOS 13 przed spełnieniem wymogów firmy Apple dla certyfikatów komunikacyjnych. Takie działanie spowoduje, że urządzenia przestaną się łączyć z ESET PROTECT MDM.

- Jeśli przeprowadziłeś aktualizację, nie posiadając odpowiedniego certyfikatu, a Twoje urządzenia przestały się łączyć z ESET PROTECT MDM, musisz zmienić swój bieżący certyfikat HTTPS używany do komunikacji z urządzeniami z systemem iOS na taki, który spełnia wymogi firmy Apple dla certyfikatów komunikacyjnych (MDM HTTPS), a następnie ponownie zarejestrować swoje urządzenia z systemem iOS.

- Jeśli nie przeprowadziłeś jeszcze aktualizacji do systemu iOS 13, upewnij się, że Twój obecny certyfikat HTTPS serwera MDM używany do komunikacji z urządzeniami z systemem iOS spełnia wymogi firmy Apple dla certyfikatów komunikacyjnych (MDM HTTPS). Jeśli tak, możesz kontynuować uaktualnianie urządzeń z systemem iOS do systemu iOS 13. Jeśli nie, zmień swój bieżący certyfikat HTTPS używany do komunikacji z urządzeniami z systemem iOS na taki, który spełnia wymogi firmy Apple dla certyfikatów komunikacyjnych (MDM HTTPS), a następnie przejdź do aktualizacji swoich urządzeń do systemu iOS 13.

Obsługiwane środowiska przydzielania komputerów

Przydzielanie komputerów ułatwia zarządzanie urządzeniami i przyspiesza przekazanie komputerów osobistych użytkownikom końcowym.

Przekazane komputery osobiste są zazwyczaj fizyczne lub wirtualne. W przypadku środowisk zwirtualizowanych wykorzystujących systemy operacyjne przesyłane strumieniowo (usługi przydzielania Citrix) należy się zapoznać z listą obsługiwanych hiperwizorów.

ESET PROTECT obsługiwa:

- systemy z dyskami nietrwałymi,
- środowiska VDI,
- funkcję identyfikacji sklonowanych komputerów.

Obsługiwane hiperwizory i rozszerzenia hiperwizora

Hiperwizor	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔ (bezpieczny rozruch nie jest obsługiwany)
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMware Fusion	X	✔ (12.2.3)
Parallels	X	✔

Rozszerzenie hiperwizora	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

Narzędzia

(można ich używać zarówno na komputerach wirtualnych, jak i fizycznych)

- Microsoft SCCM
- Menedżer serwera Windows Server 2012/2016/2019/2022
- Windows Admin Center

Rozmiar sprzętu i infrastruktury

Serwer ESET PROTECT powinien spełniać następujące wymagania sprzętowe przedstawione w tabeli poniżej.

Liczba klientów	ESET PROTECTSerwer + serwer bazy danych SQL				
	Rdzenie CPU	Szybkość zegara procesora (GHz)	RAM (GB)	Dysk[1]	Operacje We/Wy na dysku [2]
Do 1.000	4	2.1	4	Pojedynczy	500
5.000	8	2.1	8		1.000

Liczba klientów	ESET PROTECTSerwer + serwer bazy danych SQL				
	Rdzenie CPU	Szybkość zegara procesora (GHz)	RAM (GB)	Dysk[1]	Operacje We/Wy na dysku [2]
10,000 [3]	4	2.1	16	Oddzielny	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10 000
100.000	16	2.1	64+		20.000

1 Pojedynczy / oddzielny napęd – zalecamy instalację bazy danych na osobnym dysku dla systemów z ponad 10.000 klientów.

2 operacje We/Wy (całkowita operacja we/wy na sekundę) — minimalna wymagana wartość.

- Zalecamy około 0,2 IOPS na podłączonego klienta, jednak liczba całkowita nie powinna być niższa niż 500.
- Liczbę IOPS dysku można sprawdzić za pomocą narzędzia diskspd, korzystając z polecenia:

Liczba klientów	Polecenie
Do 5.000 klientów	`diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat`
Powyżej 5000 klientów	`diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat`

3 Zobacz przykładowy scenariusz dla środowiska z 10 000 klientów.

Zalecenia dotyczące dysku

Dysk to czynnik mający największy wpływ na wydajność ESET PROTECT.

- Instancja serwera SQL może współużytkować zasoby z serwerem ESET PROTECT w celu zmaksymalizowania wydajności i zminimalizowania opóźnień. Uruchom serwer ESET PROTECT oraz serwer bazy danych na jednym urządzeniu, aby zwiększyć wydajność ESET PROTECT.
- Wydajność serwera SQL jest wyższa, jeśli pliki dziennika bazy danych oraz transakcji umieszczone są na osobnych dyskach, najlepiej oddzielnych fizycznych dyskach SSD.
- Jeśli masz jeden dysk, zalecamy użycie dysku SSD.
- Zalecamy korzystanie z architektury all-flash. Dyski półprzewodnikowe (SSD) są znacznie szybsze niż standardowe dyski HDD.
- Jeśli masz konfigurację z dużą ilością pamięci RAM, wystarczająca będzie konfiguracja SAS z R5. Testowana konfiguracja: Dyski 10x 1,2 TB SAS w R5 — dwie grupy parzystości w 4+1 bez dodatkowego buforowania.
- Wydajność nie poprawia się w przypadku korzystania z dysku SSD klasy korporacyjnej z wysokim parametrem IOPS.
- Pojemność 100 GB jest wystarczająca dla dowolnej liczby klientów. Jeśli często wykonujesz kopie zapasowe bazy danych, możesz potrzebować większej pojemności.
- Nie korzystaj z dysku sieciowego, ponieważ jego działanie spowolni ESET PROTECT.

• Jeśli masz działającą wielowarstwową infrastrukturę magazynowania, która umożliwia migrację magazynu online, zalecamy rozpoczęcie od udostępnionych wolniejszych warstw i monitorowanie wydajności ESET PROTECT. Jeśli zauważysz, że opóźnienie odczytu/zapisu wynosi ponad 20 ms, możesz wykonać niezakłócające pracy przejście warstwy pamięci masowej do szybszej warstwy, aby korzystać z najbardziej opłacalnego zaplecza. Możesz zrobić to samo w hiperwizorze (jeśli używasz ESET PROTECT jako maszyny wirtualnej).

Zalecenia dotyczące rozmiaru dla różnych liczb klientów

Poniżej znajdziesz wyniki wydajności dla środowiska wirtualnego z określoną liczbą klientów działającego przez jeden rok.

Baza danych i ESET PROTECT są uruchomione na oddzielnych maszynach wirtualnych z identycznymi konfiguracjami sprzętowymi.

Rdzenie CPU	Szybkość zegara procesora (GHz)	RAM (GB)	Wydajność		
			10 000 klientów	20 000 klientów	40 000 klientów
8	2.1	64	Wysokie	Wysokie	Normalny
8	2.1	32	Normalny	Normalny	Normalny
4	2.1	32	Normalny	Normalny	Niskie
2	2.1	16	Niskie	Niskie	Niewystarczająca
2	2.1	8	Bardzo niski (niezalecane)	Bardzo niski (niezalecane)	Niewystarczająca

Zalecenia dotyczące wdrażania

Najlepsze praktyki związane z wdrażaniem programu ESET PROTECT

Liczba klientów	Do 1.000	1 000 - 5 000	5.000 - 10.000	10 000 - 50 000	50.000 - 100.000	100 000+
Serwer i serwer bazy danych ESET PROTECT na tym samym komputerze	✔	✔	✔	X	X	X
Używanie programu MS SQL Express	✔	✔*	X	X	X	X
Używanie programu MS SQL	✔	✔	✔	✔	✔	✔
Używanie programu MySQL	✔	✔	✔	X	X	X
Używanie urządzenia wirtualnego ESET PROTECT	✔	✔	Niezalecane	X	X	X
Zastosowanie serwera wirtualnego	✔	✔	✔	Opcjonalnie	X	X
Zalecany interwał połączenia (na etapie wdrożenia)	60 s	5 min	10 min	15 min	20 min	25 min
Zalecany interwał połączenia (po wdrożeniu, przy standardowym użytkowaniu)	10 min	10 min	20 min	30 min	40 min	60 min

* Aby uniknąć wypełniania bazy danych ESET PROTECT, nie zalecamy tego scenariusza w przypadku korzystania również z programu ESET Inspect.

Interwał połączenia

Serwer ESET PROTECT łączy się z agentami ESET Management za pomocą połączeń stałych. Pomimo stałego połączenia transmisja danych odbywa się tylko raz w trakcie interwału połączenia. Na przykład jeśli interwał replikacji na 5.000 klientów jest ustawiony na osiem minut, istnieje 5.000 transmisji w 480 sekund, 10,4 na sekundę. Upewnij się, że ustawiony zostanie odpowiedni interwał połączenia klienta. W celu zapewnienia wydajnej pracy konfiguracji sprzętowej całkowita liczba połączeń między agentem a serwerem powinna być utrzymywana poniżej 1000 na sekundę.

W przypadku nadmiernego obciążenia serwera lub epidemii szkodliwego oprogramowania (np. przy podłączeniu 20.000 klientów do serwera, który może obsłużyć 10.000 klientów z interwałem 10 minut) serwer pomija niektóre podłączone klienty. Niepodłączone klienty podejmą próbę połączenia z serwerem ESET PROTECT później.

Pojedynczy serwer (małe firmy)

Do zarządzania niewielkimi sieciami (liczącymi maksymalnie 1000 klientów) wystarczy jeden komputer z zainstalowanym serwerem ESET PROTECT oraz wszystkimi komponentami ESET PROTECT. W małych i średnich firmach oraz środowiskach z małymi sieciami zachęcamy do instalacji programu ESET PROTECT w wersji na system Linux lub urządzenia wirtualnego, gdy ma to zastosowanie.

Odległe oddziały z serwerami proxy

Jeśli komputer kliencki nie widzą serwera programu ESET PROTECT, do celów komunikacji z produktami ESET należy korzystać z serwera proxy. Serwer proxy HTTP nie agreguje połączeń ani nie obniża natężenia ruchu związanego z replikacją.

Wysoka dostępność (środowisko firmowe)

W środowiskach korporacyjnych (ponad 10 000 klientów) należy wziąć pod uwagę następujące kwestie:

- Narzędzie RD Sensor pomaga przeszukiwać sieć i wykrywać nowe komputery.
- Serwer ESET PROTECT można zainstalować w klastrze trybu failover.
- Skonfiguruj swój serwer HTTP proxy dla wysokiej liczby klientów.

Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności

Domyślnie konsola internetowa ESET PROTECT zainstalowana za pośrednictwem instalatora kompleksowego dla systemu Windows rezerwuje limit pamięci 1024 MB dla serwera Apache Tomcat.

Domyślną konfigurację konsoli internetowej można zmienić w zależności od infrastruktury:

- W środowisku firmowym domyślna konfiguracja konsoli internetowej może być niestabilna w przypadku dużej liczby obiektów. Aby zapobiec sytuacjom, w których brakuje pamięci, należy zmienić ustawienia usługi

Tomcat. Przed wprowadzeniem tych zmian upewnij się, że system ma wystarczającą ilość pamięci RAM (16 GB lub więcej).

• Jeśli masz system o niskiej wydajności z ograniczonymi zasobami sprzętowymi, możesz zmniejszyć użycie pamięci serwera Tomcat.

Wartości pamięci podane poniżej są wartościami zalecanymi. Ustawienia pamięci serwera Tomcat można dostosować na podstawie zasobów sprzętowych.

System Windows

1.Uruchom plik *tomcat9w.exe* lub aplikację `Configure Tomcat`.

2.Przejdź na kartę **Java**.

3.Zmień użycie pamięci:

a.Zwiększenie (przedsiębiorstwo): Zmień wartości w polu **Pierwotna pula pamięci** na 2048 MB, a w polu **Maksymalna pula pamięci** — na 16384 MB.

b.Zmniejszenie (systemy o niskiej wydajności): Zmień wartości w polu **Pierwotna pula pamięci** na 256 MB, a w polu **Maksymalna pula pamięci** — na 2048 MB.

4.Uruchom ponownie usługę Tomcat.

Linux i urządzenie wirtualne ESET PROTECT

1.Otwórz terminal jako użytkownik root lub skorzystaj z programu `sudo`.

2.Otwórz plik

a.Urządzenie wirtualne ESET PROTECT / CentOS: `/etc/sysconfig/tomcat`

b.Debian: `/etc/default/tomcat9`

3.Dodaj do pliku następujący wiersz:

a.Zwiększenie zużycia pamięci (w przedsiębiorstwie): `JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.Zmniejszenie zużycia pamięci (systemy o niskiej wydajności): `JAVA_OPTS="-Xms256m -Xmx2048m"`

4.Zapisz plik i uruchom ponownie usługę Tomcat.
`service tomcat restart`

Wdrożenie dla 10 000 klientów

Poniżej znajdziesz wyniki wydajności dla środowiska wirtualnego z 10 000 klientów działającego przez jeden rok.

Konfiguracja serwera hiperwizora

Komponent	Wartość
VMware	ESXi 6.7 aktualizacja 2 lub nowsza (maszyna wirtualna w wersji 15)
Hiperwizor	VMware ESXi, 6.7.0
Procesory logiczne	112
Typ procesora	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

Test przebiegał na dedykowanych maszynach

Baza danych i ESET PROTECT są uruchomione na oddzielnych maszynach wirtualnych z identycznymi konfiguracjami sprzętowymi.

Oprogramowanie używane na maszynach wirtualnych

ESET PROTECT:

- System operacyjny: Microsoft Windows Server 2016 Standard (64-bit)

Baza danych:

- Database server: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- System operacyjny: Microsoft Windows Server 2016 Standard (64-bit)

Opis środowiska ESET PROTECT

- 10 000 łączących się klientów
- Około 2000 grup dynamicznych i 2000 szablonów dla grup dynamicznych
- Około 255 grup statycznych
- 20 użytkowników
- 15-minutowy interwał połączenia dla agentów ESET Management
- Po działaniu środowiska przez rok rozmiar bazy danych wynosi 15 GB

Liczba procesorów	RAM (GB)	Wydajność
8	64	Wysokie
4	32	Normalny
2	16	Niskie
2	8	Bardzo niski (niezalecane)

Baza danych

Należy określić serwer i łącznik bazy danych, które mają być używane podczas instalowania serwera ESET PROTECT. Można użyć istniejącego serwera bazy danych uruchomionego w środowisku, jednak musi on spełniać wymienione niżej wymagania.

W wersji ESET PROTECT 9.1 Instalator kompleksowy domyślnie instaluje produkt Microsoft SQL Server Express 2019.

- Jeśli używasz starszej wersji systemu Windows (Server 2012 lub SBS 2011), domyślnie zainstalowany zostanie produktMicrosoft SQL Server Express 2014.

- Instalator automatycznie generuje losowe hasło do uwierzytelniania bazy danych (przechowywane w pliku *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Program Microsoft SQL Server Express ma limit rozmiaru wynoszący 10 GB dla każdej relacyjnej bazy danych. Nie zalecamy korzystania z programu Microsoft SQL Server Express:
- w środowiskach firmowych lub dużych sieciach,
- Jeśli produkt ESET PROTECT ma być używany z ESET Inspect.

Obsługiwane serwery baz danych i łączniki bazy danych

Program ESET PROTECT obsługuje dwa typy serwerów baz danych: Microsoft SQL Server i MySQL.

ESET PROTECT nie obsługuje bazy danych MariaDB. MariaDB to domyślna baza danych w większości obecnych środowisk systemu Linux, która jest instalowana po wybraniu instalacji programu MySQL.

Obsługiwane serwery bazy danych	Obsługiwane wersje bazy danych	Obsługiwane łączniki bazy danych
Microsoft SQL Server	• Edycje Express i inne niż Express • 2014, 2016, 2017, 2019	• Serwer SQL • Klient macierzysty serwera SQL10.0 • Sterownik ODBC dla serwera SQL 11, 13, 17, 18
MySQL	• 5.6* • 5.7 • 8.0	Wersje sterowników MySQLODBC: • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27 Tylko system Windows

* Wsparcie dla produktu MySQL 5.6 zostało zakończone w lutym 2021. Zaleca się uaktualnienie serwera bazy danych MySQL do wersji 5.7 lub nowszej.

Następujące wersje sterowników MySQL ODBC nie są obsługiwane:
- 5.3.11 i późniejsze 5.3.x
- 8.0.0-8.0.15
- 8.0.18 i późniejsze

Wymagania sprzętowe dotyczące serwera bazy danych

Zobacz instrukcje dotyczące sprzętu i dostosowywania rozmiarów.

Zalecenia dotyczące wydajności

W celu uzyskania najwyższej wydajności zalecamy korzystanie z najnowszej obsługiwanej wersji programu Microsoft SQL Server jako bazy danych programu ESET PROTECT. Program ESET PROTECT jest wprawdzie zgodny z programem MySQL, jednak korzystanie z programu MySQL może negatywnie wpływać na wydajność systemu podczas pracy ze znacznymi ilościami danych związanych z panelami kontrolnymi, wykryciami i klientami. Ten sam sprzęt z programem Microsoft SQL Server może obsługiwać znacznie większą liczbę klientów niż w przypadku MySQL.

Można zdecydować, czy zainstalować serwer bazy danych SQL na:

- Tym samym urządzeniu co serwer ESET PROTECT.
- Tym samym urządzeniu, ale na osobnym dysku.
- Dedykowanym serwerze do instalacji serwera bazy danych SQL.

Zalecamy korzystanie z dedykowanych serwerów baz danych SQL z zastrzeżonymi zasobami w przypadku zarządzania więcej niż 10 000 klientów.

Baza danych	Klient SMB	Klient korporacyjny	Ograniczenie liczby klientów	System Windows	Linux
MS SQL Express	✔	(opcjonalnie)	5.000	✔	
MS SQL Server	✔	✔	Brak	✔	
MySQL	✔	✔	10 000	✔	✔

Informacje dodatkowe

Serwer ESET PROTECT nie używa zintegrowanej funkcji tworzenia kopii zapasowych. Zdecydowanie zalecamy utworzenie kopii zapasowej bazy danych serwera w celu uniknięcia utraty danych.

- Nie instaluj programu SQL Server na kontrolerze domeny (np. w przypadku korzystania z systemu Windows SBS/Essentials). Zalecamy zainstalowanie programu ESET PROTECT na innym serwerze lub niezaznaczanie komponentu SQL Server Express podczas instalacji (wymaga to uruchomienia bazy danych ESET PROTECT na istniejącym serwerze SQL lub MySQL).
- Jeśli ma być używane dedykowane konto użytkownika bazy danych z dostępem tylko do bazy danych ESET PROTECT, przed rozpoczęciem instalacji należy utworzyć konto użytkownika o określonych uprawnieniach. Więcej informacji zawiera sekcja Dedykowane konto użytkownika bazy danych. Ponadto musi zostać utworzona pusta baza danych na potrzeby programu ESET PROTECT.
- Należy zapoznać się z instrukcjami dotyczącymi instalowania i konfigurowania programu MySQL for Windows i MySQL for Linux na potrzeby prawidłowego współdziałania z programem ESET PROTECT.
- Program MS SQL Server dla systemu Linux nie jest obsługiwany. Można jednak połączyć serwer ESET

PROTECT w systemie Linux z programem MS SQL Server w systemie Windows.

- W przypadku instalacji serwerów ESET PROTECT i MS SQL Server na osobnych komputerach można włączyć zaszyfrowane połączenie z bazą danych.

- Klastrowa konfiguracja bazy danych w środowiskach z systemem Windows jest obsługiwana tylko w przypadku programu MS SQL Server (nie MySQL).

Obsługiwane wersje serwera Apache Tomcat i środowiska Java

Apache Tomcat

Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT.

ESET PROTECT jest zgodny tylko z Apache Tomcat 9.x (w wersji 64-bitowej). Zalecamy korzystanie z najnowszej wersji biblioteki Apache Tomcat 9.x.

Program ESET PROTECT nie obsługuje wersji alfa/beta/RC serwera Apache Tomcat.

Java

Apache Tomcat wymaga 64-bitowego Java/OpenJDK.

Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

⚠ Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

Obsługiwane przeglądarki internetowe, produkty zabezpieczające firmy ESET i języki

Program ESET PROTECT obsługuje następujące systemy operacyjne:

- Windows, Linux i macOS

Konsola internetowa ESET PROTECT działa w następujących przeglądarkach internetowych:

Przeglądarka internetowa
Mozilla Firefox
Microsoft Edge
Google Chrome

Przeglądarka internetowa
Safari
Opera

Aby jak najlepiej korzystać z konsoli internetowej ESET PROTECT, zalecamy regularną aktualizację przeglądarek internetowych.

Jeśli korzystasz z programu Internet Explorer, konsola internetowa ESET PROTECT powiadomi Cię, że używasz nieobsługiwanej przeglądarki internetowej.

Najnowsze wersje produktów firmy ESET, którymi można zarządzać przy użyciu programu ESET PROTECT 9.1

Produkt	Wersja produktu
ESET Endpoint Security dla systemu Windows	7.x, 8.x, 9.x
ESET Endpoint Antivirus dla systemu Windows	7.x, 8.x, 9.x
ESET Endpoint Security dla systemu macOS	6.8+
ESET Endpoint Antivirus dla systemu macOS	6.8+
ESET Endpoint Security dla systemu Android	2.x
ESET Server Security dla systemu Microsoft Windows Server	8.x, 9.x
ESET File Security dla systemu Microsoft Windows Server	7.x
ESET File Securityna platformie Microsoft Azure	7.x
ESET Mail Security dla oprogramowania Microsoft Exchange Server	7.x, 8.x, 9.x
ESET Security for Microsoft SharePoint Server	7.x, 8.x, 9x
ESET Mail Security dla środowiska IBM Domino Server	7.x, 8.x, 9.x
ESET File Security dla systemu Linux	7.x, 8.x
ESET Server Security dla systemu Linux	8.1+
ESET Endpoint Antivirus dla systemu Linux	7.x, 8.x, 9.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
ESET Full Disk Encryption dla systemu Windows	
ESET Full Disk Encryption dla systemu macOS	

Najnowsze wersje produktów firmy ESET, którymi można zarządzać przy użyciu programu ESET PROTECT 9.1

Produkt	Wersja produktu
ESET Endpoint Security dla systemu Windows	6.5 i nowsze wersje
ESET Endpoint Antivirus dla systemu Windows	6.5 i nowsze wersje
ESET File Security dla systemu Microsoft Windows Server	6.5
ESET File Securityna platformie Microsoft Azure	6.5
ESET Mail Security dla oprogramowania Microsoft Exchange Server	6.5

Produkt	Wersja produktu
ESET Mail Security dla IBM Lotus Domino	6.5
ESET Security for Microsoft SharePoint Server	6.5
ESET Mail Security for Linux/FreeBSD*	4.5.x
ESET File Security for Linux/FreeBSD*	4.5.x
ESET Gateway Security for Linux/FreeBSD*	4.5.x

* Nie można zarządzać tym produktem za pomocą agenta 9 ESET Management. Aby zarządzać produktem, użyj agenta ESET Management w wersji 8.1 lub starszej.

Wersje produktu zabezpieczającego ESET wcześniejsze niż te przedstawione w powyższej tabeli nie mogą być zarządzane przy użyciu produktu ESET PROTECT 9.
Aby uzyskać więcej informacji na temat zgodności, zobacz Politykę o końcu okresu użytkowania produktów biznesowych firmy ESET.

Produkty obsługujące aktywację przy użyciu licencji subskrypcyjnej

Produkt ESET	Dostępny od wersji
ESET Endpoint Antivirus/Security for Windows	7.0
ESET Endpoint Antivirus/Security for macOS	6.8.x
ESET Endpoint Security for Android	2.0.158
ESET Mobile Device Management for Apple iOS	7.0
ESET File Security dla systemu Microsoft Windows Server	7.0
ESET Mail Security for Microsoft Exchange	7.0
ESET File Security dla systemu Windows Server	7.0
ESET Mail Security dla środowiska IBM Domino	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security dla systemu Linux	7.0
ESET Endpoint Antivirus dla systemu Linux	7.0
ESET Server Security dla systemu Windows	8.0
ESET Server Security dla systemu Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect (z programem ESET Endpoint dla systemu Windows w wersji 7.3 i nowszych)	1.5

Obsługiwane języki

Język	Kod
Angielski (Stany Zjednoczone)	en-US
Arabski (Egipt)	ar-EG
Chiński uproszczony	zh-CN
Chiński tradycyjny	zh-TW
Chorwacki (Chorwacja)	hr-HR
Czeski (Czechy)	cs-CZ

Język	Kod
Francuski (Francja)	fr-FR
Francuski (Kanada)	fr-CA
Niemiecki (Niemcy)	de-DE
Grecki (Grecja)	el-GR
Węgierski (Węgry)*	hu-HU
Indonezyjski (Indonezja)*	id-ID
Włoski (Włochy)	it-IT
Japoński (Japonia)	ja-JP
Koreański (Korea)	ko-KR
Polski (Polska)	pl-PL
Portugalski (Brazylia)	pt-BR
Rosyjski (Rosja)	ru-RU
Hiszpański (Chile)	es-CL
Hiszpański (Hiszpania)	es-ES
Słowacki (Słowacja)	sk-SK
Turecki (Turcja)	tr-TR
Ukraiński (Ukraina)	uk-UA

* W tym języku jest dostępny jedynie produkt. Pomoc online jest niedostępna.

Sieć

Ważne, aby serwer ESET PROTECT i komputery klienckie zarządzane przez program ESET PROTECT miały działające połączenie z Internetem na potrzeby łączenia się z repozytorium i serwerami aktualizacji firmy ESET. Jeśli klienty nie powinny być połączone bezpośrednio z Internetem, można użyć serwera proxy (innego niż serwer proxy Apache HTTP Proxy), aby umożliwić komunikację z siecią i Internetem.

Komputery zarządzane przy użyciu programu ESET PROTECT powinny być podłączone do tej samej sieci LAN i/lub powinny należeć do tej samej domeny *Active Directory* co serwer ESET PROTECT. Serwer ESET PROTECT musi być widoczny dla komputerów klienckich. Ponadto komputery klienckie muszą mieć możliwość komunikacji z serwerem ESET PROTECT, aby możliwe było korzystanie z funkcji zdalnego wdrażania i sygnału wznowienia.

Program ESET PROTECT dla systemu Windows/Linux jest zgodny z protokołami internetowymi IPv4 i IPv6. Urządzenie wirtualne ESET PROTECT jest zgodne tylko z protokołem IPv4.

Używane porty

Jeśli w sieci jest stosowana zapora, należy się zapoznać z listą portów komunikacji sieciowej używanych w przypadku zainstalowania w infrastrukturze programu ESET PROTECT wraz z komponentami.

Wpływ serwera ESET PROTECT i komunikacji agenta ESET Management na

ruch sieciowy

Aplikacje na komputerach klienckich nie komunikują się bezpośrednio z serwerem ESET PROTECT. Komunikacja ta odbywa się za pośrednictwem agenta ESET Management. To rozwiązanie jest łatwiejsze w zarządzaniu i wymaga mniejszych transferów danych w sieci. Ruch sieciowy zależy od interwału połączenia klienta i typów zadań wykonywanych na klientach. Nawet jeśli na kliencie nie jest wykonywane żadne zadanie ani go na nim nie zaplanowano, agent ESET Management komunikuje się z serwerem ESET PROTECT raz na interwał połączenia. Każde połączenie generuje ruch. Poniższa tabela zawiera przykłady ruchu:

Typ czynności	Ruch w jednym interwale połączenia
Zadanie klienta: Skanowanie bez leczenia	4 KB
Zadanie klienta: Aktualizacja modułów	4 KB
Zadanie klienta: Żądanie dziennika programu SysInspector	300 KB
Polityka — Moduł antywirusowy — maksymalny poziom bezpieczeństwa	26 KB

ESET ManagementInterwał replikacji agenta	Dzienny ruch wygenerowany przez bezczynnego agenta ESET Management
1 minuta	16 MB
15 minut	1 MB
30 minut	0,5 MB
1 godzina	144 KB
1 dzień	12 KB

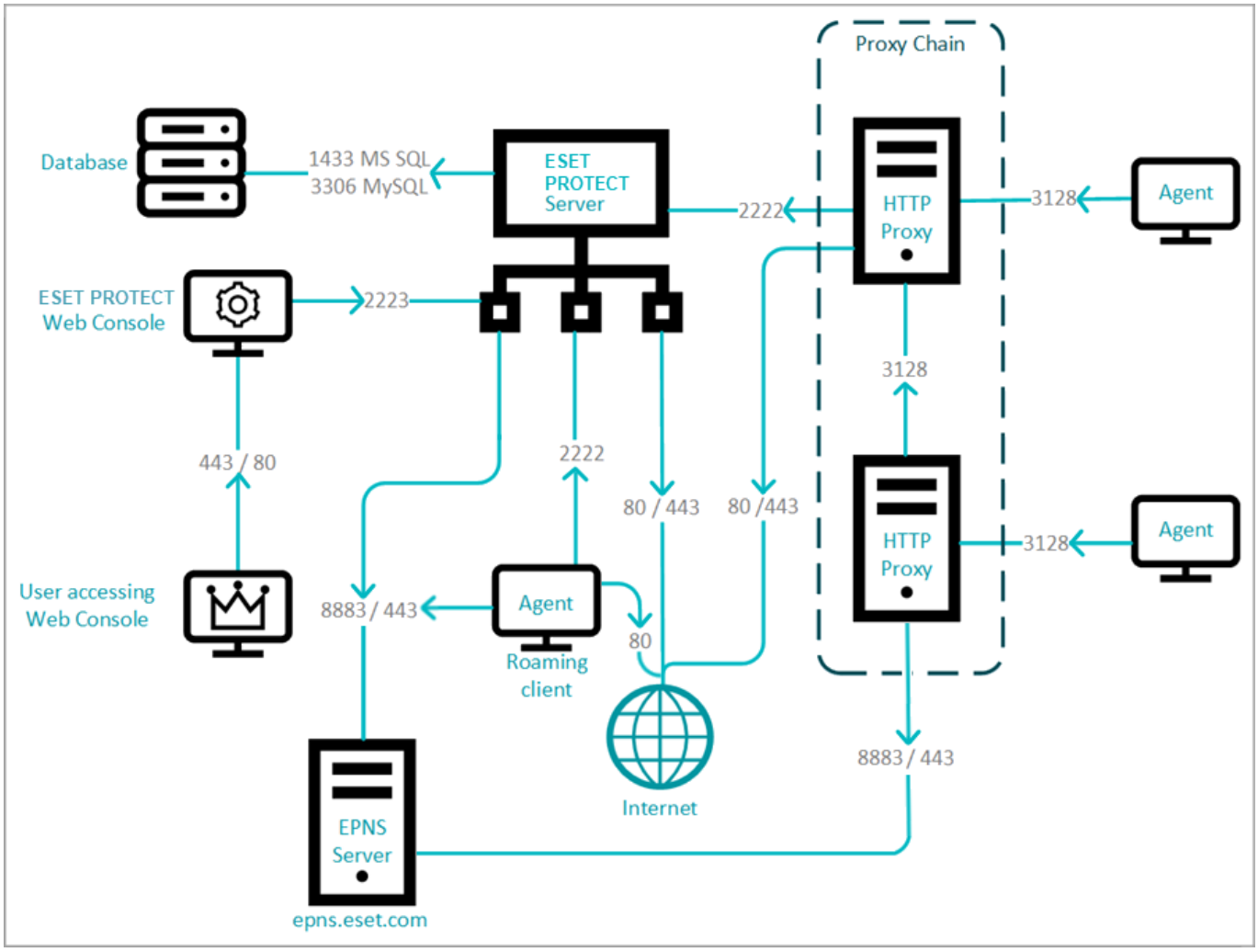
Aby oszacować łączny ruch generowany przez agenty ESET Management, należy użyć następującego wzoru:

*liczba klientów * (dzienny ruch bezczynnego agenta + (ruch w przypadku danego zadania * dzienne występowanie zadania))*

Jeśli używasz rozwiązania ESET Inspect, Connector ESET Inspect generuje dzienny ruch na poziomie 2-5 MB (w zależności od liczby zdarzeń).

Używane porty

Serwer ESET PROTECT można zainstalować na tym samym komputerze, na którym działa baza danych, konsola internetowa ESET PROTECT i serwer proxy Apache HTTP. Na poniższym diagramie przedstawiono osobną instalację i używane porty (strzałki wskazują ruch sieciowy):



W poniższych tabelach przedstawiono wszelkie możliwe porty komunikacji sieciowej używane wtedy, gdy ESET PROTECT oraz komponenty tego oprogramowania są zainstalowane w infrastrukturze. Inne rodzaje komunikacji są obsługiwane przez procesy zachodzące w macierzystym systemie operacyjnym (na przykład NetBIOS przez TCP/IP).

Aby oprogramowanie ESET PROTECT działało poprawnie, żaden z niżej wymienionych portów nie może być używany przez inne aplikacje.
Należy pamiętać o skonfigurowaniu zapór w sieci tak, by umożliwić komunikację z wymienionymi niżej portami.

Klient (agent ESET Management) lub komputer z serwerem proxy Apache HTTP

Protokół	Port	Opisy
TCP	2222	Komunikacja między agentami ESET Management i serwerem ESET PROTECT
TCP	80	Połączenie z repozytorium firmy ESET
MQTT	8883, 443	Usługa ESET Push Notification — sygnały wznowienia działania między serwerem ESET PROTECT a agentem ESET Management (port 443 to port awaryjny).
TCP	3128	Komunikacja z serwerem proxy Apache HTTP
TCP	443	Komunikacja z ESET LiveGuard Advanced (tylko serwer proxy)

Agent ESET Management — porty używane do zdalnego wdrożenia na komputerze docelowym

z systemem operacyjnym Windows

Protokół	Port	Opisy
TCP	139	Korzystanie z udziału ADMIN$
TCP	445	Bezpośredni dostęp do zasobów udostępnionych przy użyciu protokołu TCP/IP podczas instalacji zdalnej (alternatywa dla portu TCP 139)
UDP	137	Rozpoznawanie nazwy podczas zdalnej instalacji
UDP	138	Przeglądanie podczas zdalnej instalacji

Komputer z konsolą internetową ESET PROTECT (jeżeli nie jest komputerem, na którym działa serwer ESET PROTECT)

Protokół	Port	Opisy
TCP	2223	Komunikacja między konsolą ESET PROTECT a serwerem ESET PROTECT stosowana w ramach instalacji wspomaganej
TCP	443/80	Emisja Tomcat konsoli internetowej.
TCP	443	Kanał informacyjny RSS z wiadomościami pomocy technicznej: • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

Komputer serwera ESET PROTECT

Protokół	Port	Opisy
TCP	2222	Komunikacja między agentem ESET Management i serwerem ESET PROTECT
TCP	80	Połączenie z repozytorium firmy ESET
MQTT	8883	Usługa ESET Push Notification — sygnały wznowienia działania między serwerem ESET PROTECT a agentem ESET Management
TCP	2223	Obsługa DNS i rozwiązanie awaryjne MQTT
TCP	3128	Komunikacja z serwerem proxy Apache HTTP
TCP	1433 (MS SQL) 3306 (MySQL)	Łączność z zewnętrzną bazą danych (tylko wtedy, gdy baza danych jest na innym komputerze).
TCP	389	Synchronizacja LDAP. Otwórz ten port także na kontrolerze AD.
UDP	88	Bilety Kerberos (dotyczy tylko urządzenia wirtualnego ESET PROTECT)

RD Sensor

Protokół	Port	Opisy
TCP	22, 139	Wykrywanie systemu operacyjnego przy użyciu protokołów SMB (TCP 139) i SSH (TCP 22).
UDP	137	Rozpoznawanie nazwy hosta komputera przy użyciu systemu NetBIOS.

Komputer modułu zarządzania urządzeniami mobilnymi ESET PROTECT

Protokół	Port	Opisy
TCP	9977 9978	**Wewnętrzna** komunikacja między narzędziem Moduł zarządzania urządzeniami mobilnymi i agentem ESET Management
TCP	9980	Rejestracja urządzenia mobilnego
TCP	9981	Komunikacja z urządzeniami mobilnymi
TCP	2195	Wysyłanie powiadomień do usługi Apple Push Notification. (*gateway.push.apple.com*) do wersji ESMC 7.2.11.1
TCP	2196	Usługa Apple Feedback (*feedback.push.apple.com*) do wersji ESMC 7.2.11.1
HTTPS	2197	• Usługa informacji zwrotnych Apple Push Notification (*api.push.apple.com*) ESMC wersja 7.2.11.3 lub nowsza.
TCP	2222	Komunikacja (replikacja) między agentem ESET Management, modułem zarządzania urządzeniami mobilnymi a serwerem ESET PROTECT
TCP	1433 (MS SQL) 3306 (MySQL)	Łączność z zewnętrzną bazą danych (tylko wtedy, gdy baza danych jest na innym komputerze)

Urządzenie zarządzane przez MDM

Protokół	Port	Opisy
TCP	9980	Rejestracja urządzenia mobilnego
TCP	9981	Komunikacja z urządzeniami mobilnymi
TCP	5223	Komunikacja zewnętrzna z usługą Apple Push Notification (iOS)
TCP	443	• Rozwiązanie zastępcze tylko w sieci Wi-Fi, gdy urządzenia nie mogą się połączyć z punktami dostępu na porcie 5223 (iOS). • Połączenie urządzenia z systemem Android z serwerem GCM. • Połączenie z portalem licencyjnym firmy ESET. • ESET LiveGrid® (Android) (przychodzące: *https://i1.c.eset.com*; wychodzące: *https://i3.c.eset.com*) • Anonimowe informacje statystyczne wysyłane do laboratorium firmy ESET (Android) (*https://ts.eset.com*) • Kategoryzacja aplikacji zainstalowanych w urządzeniu. Używana z funkcją Kontrola aplikacji w przypadku gdy zdefiniowano blokowanie niektórych kategorie aplikacji. (Android) (*https://play.eset.com*) • Aby wysłać zgłoszenie do pomocy technicznej przy użyciu funkcji Zgłoszenie do działu obsługi klienta (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	Wysyłanie powiadomień do usługi Google Cloud Messaging (Android)* Wysyłanie powiadomień do usługi Firebase Cloud Messaging (Android)*
TCP	80	• Aktualizacja modułów (Android) (*http://update.eset.com*) • Używane tylko w wersji WWW. Informacje o najnowszej aktualizacji wersji aplikacji i pobieranie nowej wersji. (Android) (*http://go.eset.eu*)

* Usługa GCM (Google Cloud Messaging) została wycofana i została usunięta 11 kwietnia 2019 r. Zastąpiono ją usługą FCM (Firebase Cloud Messaging). Do tej daty w MDM v7 zastąpiono usługę GCM usługą FCM, a po tej dacie należało tylko zezwolić na komunikację usłudze FCM.

Wstępnie zdefiniowane porty 2222 i 2223 można zmienić w razie potrzeby.

Proces instalacji

Przewodnik po instalacji zawiera informacje o wielu sposobach instalowania programu ESET PROTECT i jest przeznaczonych głównie dla klientów korporacyjnych. Informacje o instalowaniu programu ESET PROTECT na platformie Windows na potrzeby zarządzania maksymalnie 250 produktami punktów końcowych ESET dla systemu Windows zawiera przewodnik dla małych i średnich firm.
Instrukcje dotyczące uaktualniania istniejącej instalacji programu ESET PROTECT zawiera sekcja Procedury uaktualniania.

Instalatory programu ESET PROTECT są dostępne w sekcji pobierania programu ESET PROTECT na stronie internetowej firmy ESET. Dostępne są w różnych formatach dostosowanych do różnych metod instalacji. Domyślnie wybrana jest karta **instalacji kompleksowej**. Aby pobrać urządzenie wirtualne lub instalator autonomiczny, kliknij odpowiednią kartę. Do pobrania dostępne są następujące pliki:

- Pakiet instalatora kompleksowego ESET PROTECT dla systemu Windows w postaci archiwum zip.
- Obraz ISO zawierający wszystkie instalatory programu ESET PROTECT (oprócz urządzeń wirtualnych ESET PROTECT).
- Urządzenia wirtualne (pliki OVA). Wdrożenie urządzenia wirtualnego ESET PROTECT jest zalecane w przypadku użytkowników, którzy chcą, aby program ESET PROTECT działał w środowisku zwirtualizowanym, albo preferują prostą instalację. Szczegółowe instrukcje zawiera Instrukcja wdrażania urządzenia wirtualnego ESET PROTECT.
- Pojedyncze instalatory komponentów — dla platformy Windows i Linux.

Dodatkowe metody instalacji:

- Instalowanie na platformie Microsoft Azure
- Szczegółowa instrukcja instalacji w systemie Linux

Po zakończeniu instalacji nie należy zmieniać nazwy komputera serwera ESET PROTECT. Więcej informacji zawiera sekcja Zmienianie adresu IP lub nazwy hosta serwera ESET PROTECT.

Poniższa tabela pozwala zdecydować, którą instalację programu ESET PROTECT odpowiednią dla używanego środowiska: Na przykład:

- W przypadku korzystania z programu ESET PROTECT w chmurze nie należy używać wolnego połączenia z Internetem.
- Instalator kompleksowy należy wybrać, gdy klientem jest mała lub średnia firma.

Patrz również Rozmiar sprzętu i infrastruktury.

Metoda instalacji	Typ klienta		Migracja		Środowisko instalacji programu ESET PROTECT					Połączenie internetowe		
	Mała i średnia firma	Przedsiębiorstwo	Tak	Nie	Brak serwera	Dedykowany serwer	Współużytkowany serwer	Platforma wirtualizacji	Serwer w chmurze	Brak	Dobre	Złe
Instalator kompleksowy w systemie Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
Instalator kompleksowy w systemie Windows Desktop	✓		✓		✓					✓	✓	✓
Urządzenie wirtualne	✓		✓					✓		✓	✓	✓
Maszyna wirtualna na platformie Microsoft Azure	✓			✓					✓		✓	
Komponent — Linux		✓	✓			✓	✓		✓	✓	✓	✓
Komponent — Windows		✓	✓			✓	✓		✓	✓	✓	✓

Instalacja kompleksowa w systemie Windows

ESET PROTECT można zainstalować na kilka różnych sposobów. Wybierz typ instalacji, który najlepiej odpowiada Twoim potrzebom i środowisku. Najprostszą metodą jest użycie instalatora kompleksowego programu ESET PROTECT. Ta metoda umożliwia zainstalowanie programu ESET PROTECT wraz z jego komponentami na pojedynczym komputerze.

Instalacja poszczególnych składników umożliwia dostosowanie instalacji i instalowanie różnych składników programu ESET PROTECT na różnych komputerach, pod warunkiem że spełnia on wymagania systemowe.

Sposoby instalowania programu ESET PROTECT:

- Instalacja kompleksowa pakietu serwera ESET PROTECT, serwera proxy Apache HTTP lub Modułu zarządzania urządzeniami mobilnymi
- Instalatory autonomiczne komponentów programu ESET PROTECT (instalacja komponentów)

Niestandardowe scenariusze instalacji:

- Instalacja przy użyciu certyfikatów niestandardowych
- Instalacja w klastrze trybu failover

Wiele scenariuszy instalacji wymaga zainstalowania różnych komponentów ESET PROTECT na różnych komputerach na potrzeby obsługi architektur sieci, w celu spełnienia wymagań dotyczących wydajności i z innych powodów. Poniższe pakiety instalacyjne są dostępne dla poszczególnych komponentów ESET PROTECT:

Instalacja komponentów podstawowych

- Serwer ESET PROTECT
- Konsola internetowa ESET PROTECT - Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT.

- Agent ESET Management (musi być zainstalowany na komputerach klienckich, może być zainstalowany na serwerze ESET PROTECT)

Instalacja komponentów opcjonalnych

- RD Sensor
- Moduł zarządzania urządzeniami mobilnymi
- Serwer proxy Apache HTTP
- Narzędzie Mirror Tool

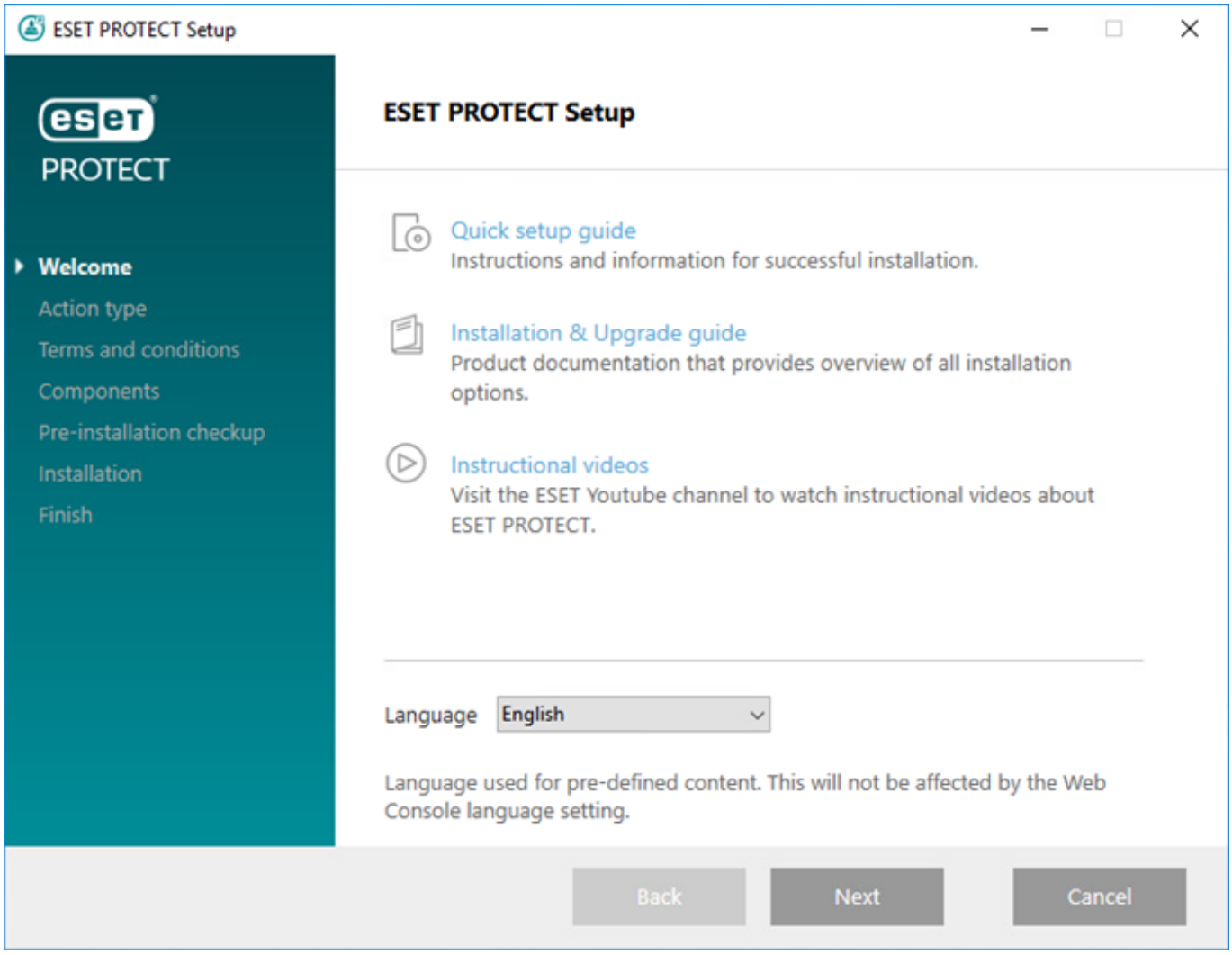
Zobacz także ESET PROTECT instalacja kompleksowa.

Dodatkowe instrukcje dotyczące uaktualniania programu ESMC do najnowszej wersji ESET PROTECT9.1 znajdziesz w procedurach aktualizacji.

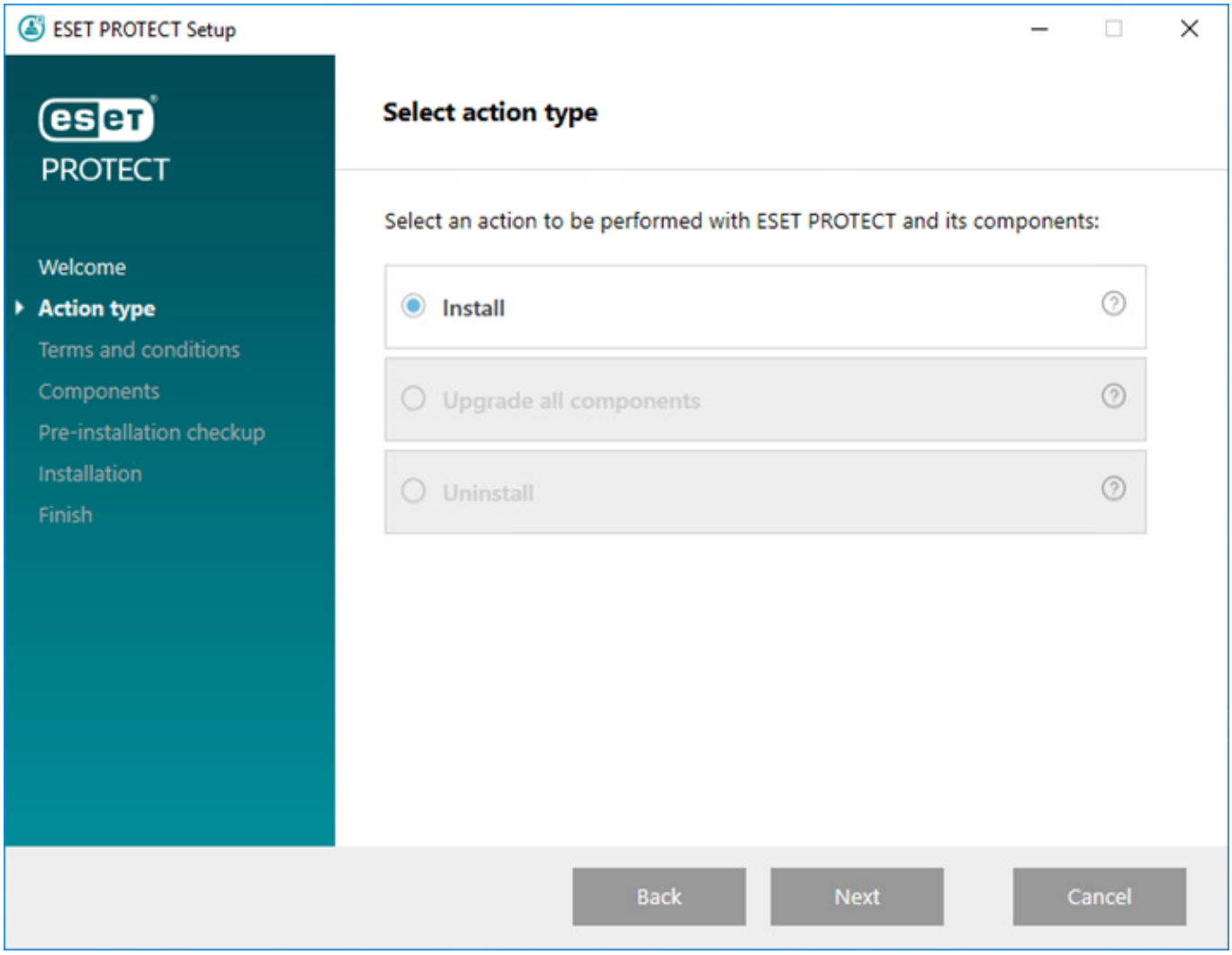
Instalowanie serwera ESET PROTECT

Instalator kompleksowy ESET PROTECT jest dostępny tylko dla systemów operacyjnych Windows. Instalator kompleksowy umożliwia zainstalowanie wszystkich komponentów produktu ESET PROTECT przy użyciu Kreatora instalacji ESET PROTECT.

1. Otwórz pakiet instalacyjny. Na ekranie powitalnym skorzystaj z menu rozwijanego **Język**, aby dostosować ustawienia języka. Kliknij przycisk **Dalej**, aby kontynuować.



2. Wybierz opcję **Zainstaluj** i kliknij przycisk **Dalej**.



3. Jeśli nie zgadzasz się na przesyłanie firmie ESET raportów o awariach i anonimowych danych telemetrycznych (takich jak rodzaj i wersja systemu operacyjnego, wersja produktu ESET i inne informacje dotyczące konkretnego produktu), usuń zaznaczenie pola wyboru **Weź udział w programie ulepszania produktu**. W przypadku niezaznaczenia tego pola wyboru dane telemetryczne i raporty o awariach będą przesyłane firmie ESET. Po zaakceptowaniu umowy EULA kliknij opcję **Dalej**.

4. Wybierz komponenty do zainstalowania i kliknij przycisk **Dalej**.

Microsoft SQL Server Express

- W wersji ESET PROTECT 9.1 Instalator kompleksowy domyślnie instaluje produkt Microsoft SQL Server Express 2019.
  - Jeśli używasz starszej wersji systemu Windows (Server 2012 lub SBS 2011), domyślnie zainstalowany zostanie produktMicrosoft SQL Server Express 2014.
  - Instalator automatycznie generuje losowe hasło do uwierzytelniania bazy danych (przechowywane w pliku *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

Program Microsoft SQL Server Express ma limit rozmiaru wynoszący 10 GB dla każdej relacyjnej bazy danych. Nie zalecamy korzystania z programu Microsoft SQL Server Express:
- w środowiskach firmowych lub dużych sieciach,
- Jeśli produkt ESET PROTECT ma być używany z ESET Inspect.

- Jeśli masz już zainstalowaną inną obsługiwaną wersję programu Microsoft SQL Server lub MySQL albo planujesz połączenie z innym serwerem SQL, usuń zaznaczenie pola wyboru **Microsoft SQL Server Express**.

- Nie instaluj programu SQL Server na kontrolerze domeny (np. w przypadku korzystania z systemu Windows SBS/Essentials). Zalecamy zainstalowanie programu ESET PROTECT na innym serwerze lub niezaznaczanie komponentu SQL Server Express podczas instalacji (wymaga to uruchomienia bazy danych ESET PROTECT na istniejącym serwerze SQL lub MySQL).

Dodaj niestandardowy certyfikat HTTPS dla konsoli internetowej

- Zaznacz tę opcję, jeśli chcesz użyć niestandardowego certyfikatu HTTPS dla konsoli internetowej ESET PROTECT.

- Jeśli ta opcja nie zostanie zaznaczona, instalator automatycznie wygeneruje nowy magazyn kluczy dla serwera Tomcat (samodzielnie podpisany certyfikat HTTPS).

Serwer proxy Apache HTTP

Opcja **Serwer proxy Apache HTTP** jest przeznaczona tylko dla mniejszych lub scentralizowanych sieci bez klientów mobilnych. Jeśli ta opcja zostanie wybrana, instalator skonfiguruje klienty do komunikacji tunelowej z programem ESET za pośrednictwem serwera proxy zainstalowanego na tym samym komputerze, co serwer ESET PROTECT. Połączenie to nie zadziała, jeśli nie ma bezpośredniej widoczności w sieci między klientami a serwerem ESET PROTECT.

- Korzystanie z serwera proxy HTTP pozwala znacząco obniżyć wykorzystanie przepustowości na potrzeby pobierania danych z Internetu oraz przyspieszyć pobieranie aktualizacji produktów. Zalecamy zaznaczenie pola wyboru **Serwer proxy Apache HTTP**, jeśli serwer ESET PROTECT ma służyć do zarządzania więcej niż 37 komputerami. Możesz też wybrać opcję zainstalowania serwera proxy Apache HTTP później.

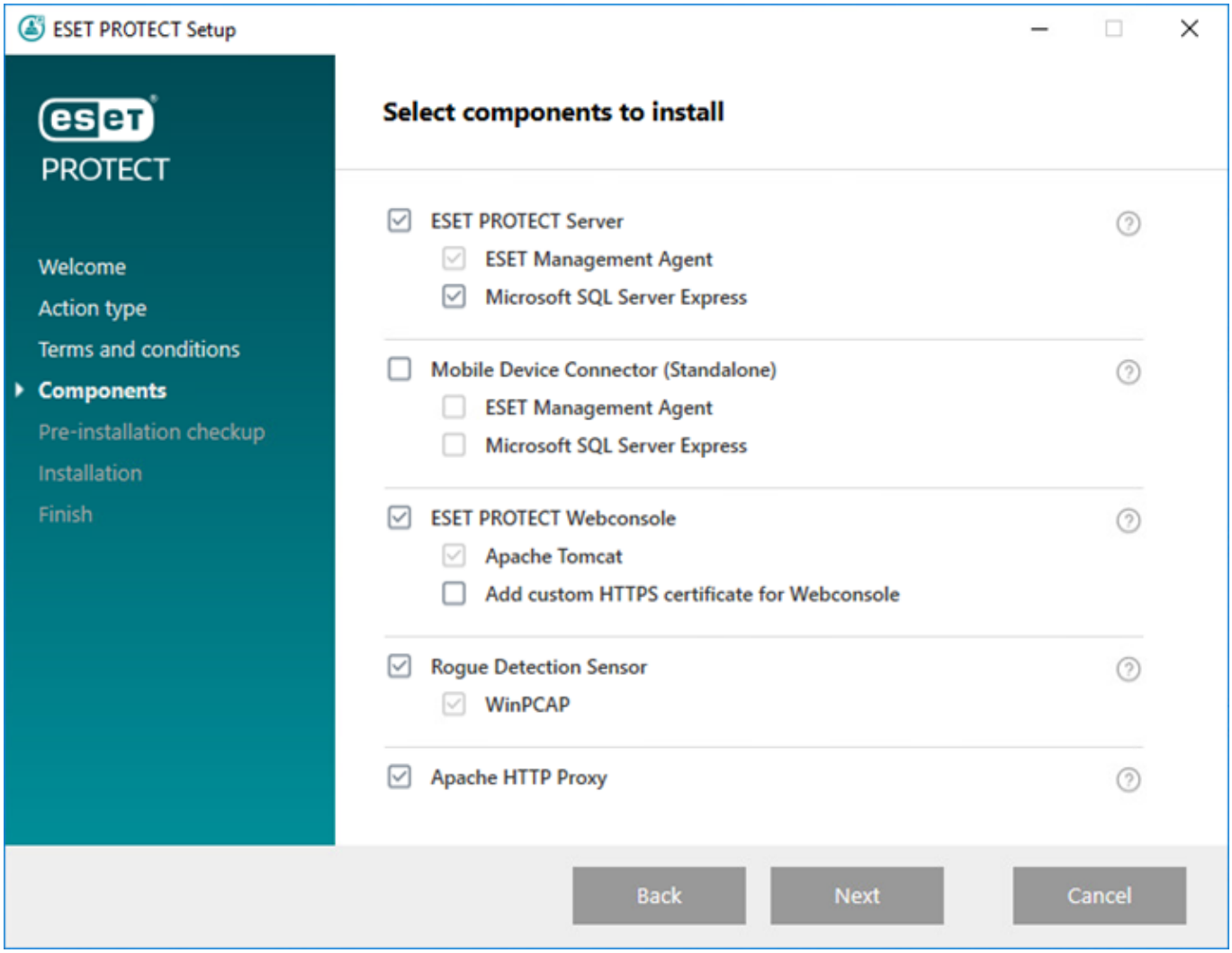
- Więcej informacji można znaleźć w sekcjach Co to jest serwer proxy Apache HTTP? oraz Różnice pomiędzy serwerem proxy Apache HTTP, narzędziem Mirror Tool a połączeniem bezpośrednim.

- Wybierz opcję **Serwer proxy Apache HTTP**, aby zainstalować serwer proxy Apache HTTP oraz utworzyć i zastosować polityki (o nazwie **Wykorzystanie serwera proxy apache HTTP**, przypisane do grupy **Wszystkie**) na potrzeby następujących produktów:

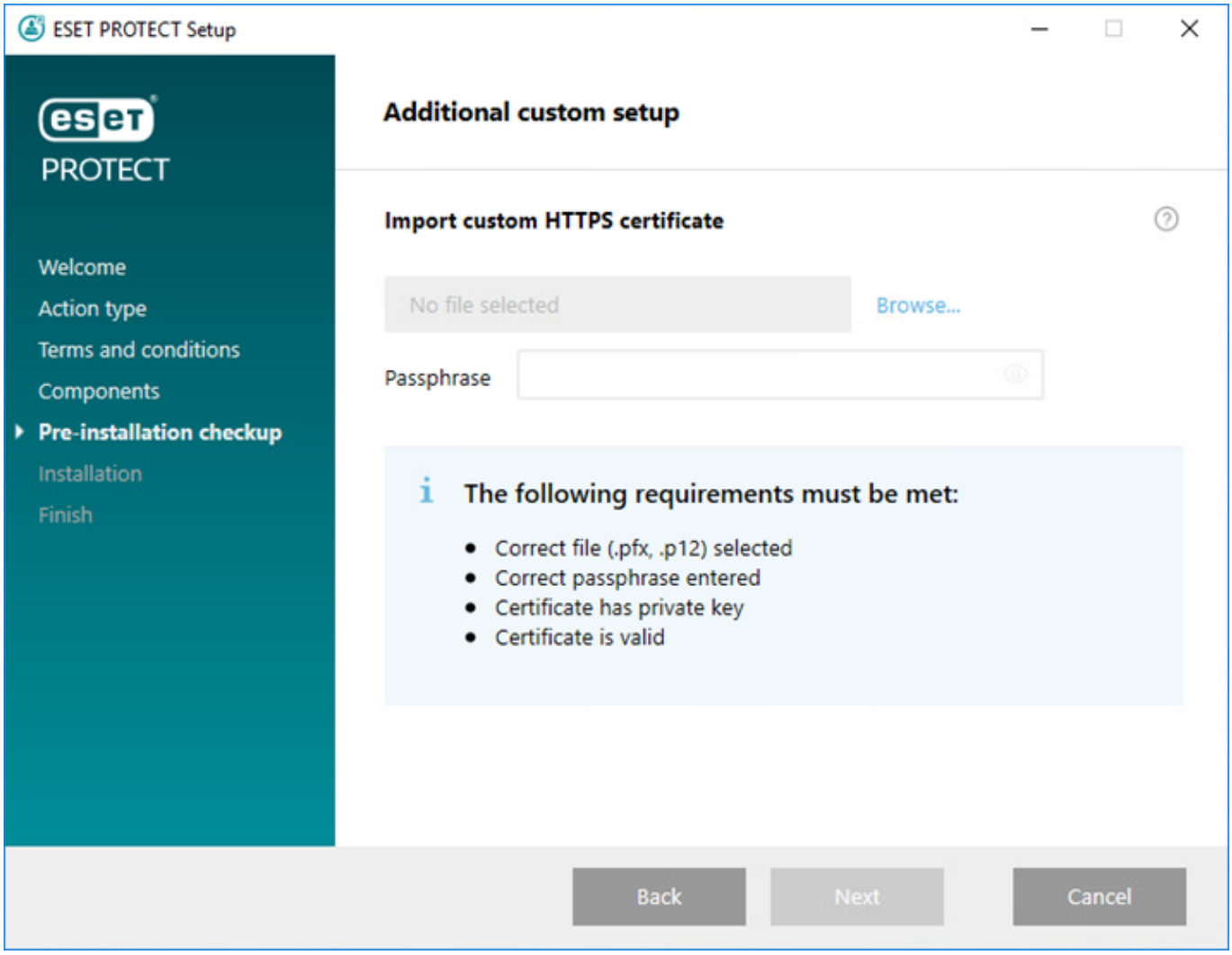
  - ESET Endpoint for Windows
  - ESET Endpoint for macOS (OS X) and Linux
  - ESET Management Agent
  - ESET File Security for Windows Server (6+)
  - ESET Server Security dla Windows (8+)

- ESET Shared Local Cache

Polityka ta włącza serwer proxy HTTP w wymienionych produktach. Host serwera proxy HTTP ma ten sam adres IP, co lokalny adres IP serwera ESET PROTECT i korzysta z portu 3128. Funkcja uwierzytelniania jest wyłączona. W przypadku konieczności skonfigurowania innych produktów można skopiować powyższe ustawienia do innej polityki.



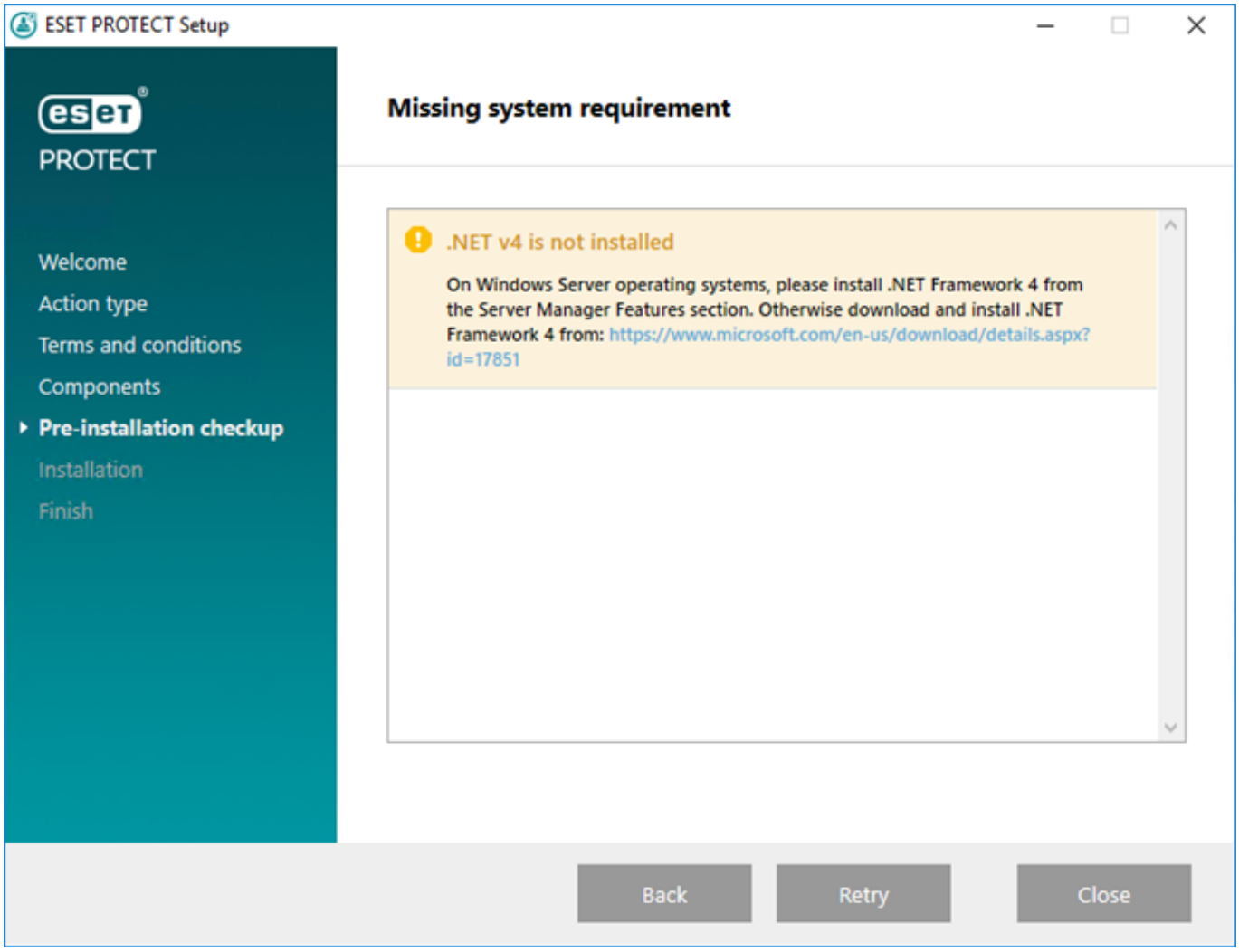
5. W przypadku wybrania opcji **Dodaj niestandardowy certyfikat HTTPS dla konsoli internetowej** kliknij **Przeglądaj** i wybierz ważny certyfikat (plik *.pfx* lub .p12 file), a w polu **Hasło** wpisz hasło do niego (lub pozostaw to pole puste, jeśli nie ustawiono hasła). Instalator zainstaluje certyfikat dostępu do konsoli internetowej na serwerze Tomcat. Kliknij przycisk **Dalej**, aby kontynuować.



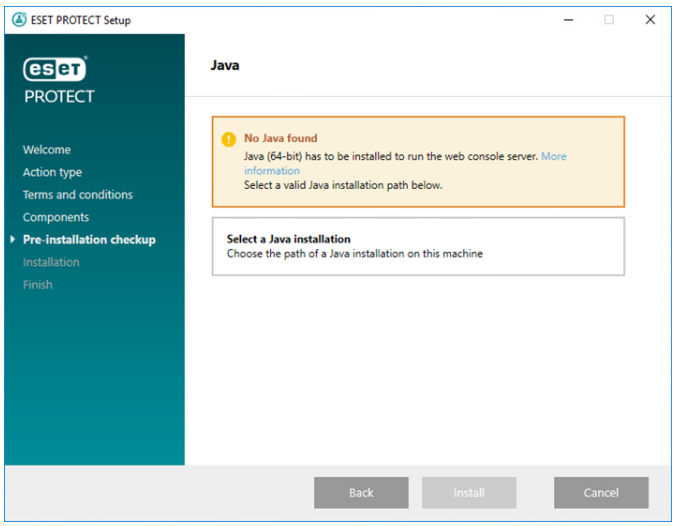
6. Jeśli podczas sprawdzania wymagań wstępnych wystąpią błędy, rozwiąż je. Sprawdź, czy system spełnia wszystkie wymagania wstępne.

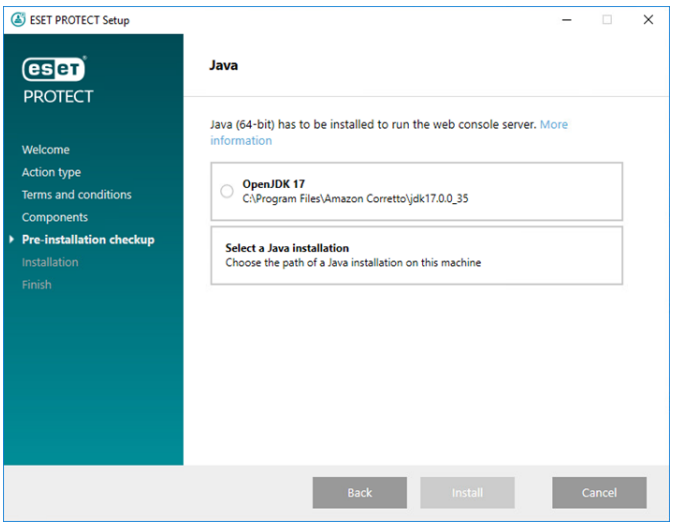
Nie zainstalowano platformy .NET 4

Zainstaluj oprogramowanie .NET Framework



Nie znaleziono środowiska Java/Java (wersja 64-bitowa)





Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

a)Aby wybrać już zainstalowane środowisko Java, kliknij opcję **Wybierz instalację środowiska Java**, wybierz folder, w którym jest zainstalowane środowisko Java (z podfolderem *bin*, np. *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) i kliknij przycisk **OK**. Pojawi się pytanie, czy została wybrana nieprawidłowa ścieżka.

b)Kliknij przycisk **Zainstaluj**, aby kontynuować, lub **Zmień**, aby zmienić ścieżkę instalacji środowiska Java.

Na dysku systemowym dostępnych jest tylko 32 MB wolnego miejsca.

- Jeśli w systemie nie ma wystarczająco dużo wolnego miejsca na instalację produktu ESET PROTECT, może zostać wyświetlone to powiadomienie.

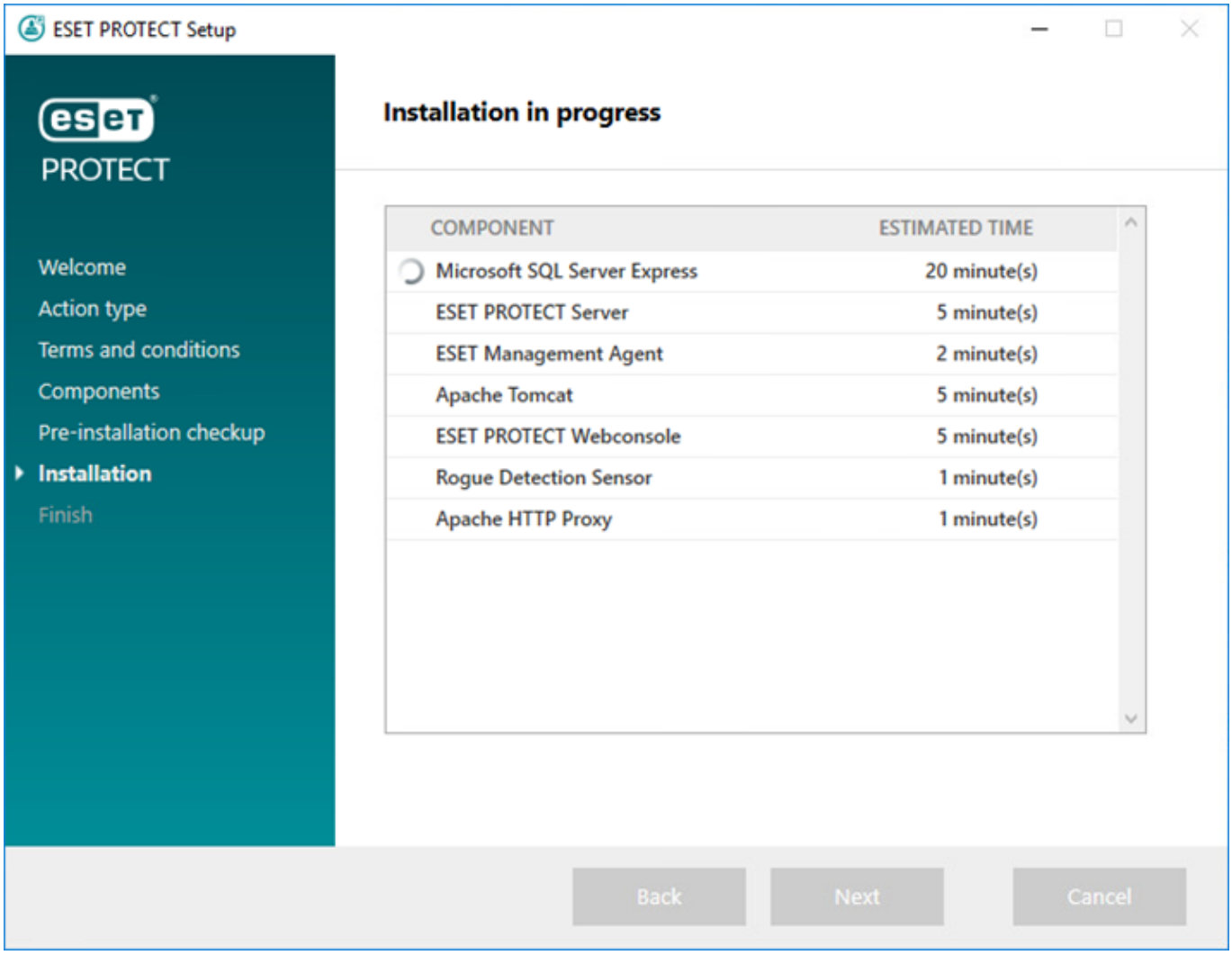
- Do zainstalowania programu ESET PROTECT i wszystkich jego komponentów niezbędne jest co najmniej 4400 MB wolnego miejsca na dysku.

Na komputerze jest zainstalowany program ESET Remote Administrator 5.x lub starszy.

Bezpośrednie uaktualnienie nie jest obsługiwane – zobacz Migracja z wersji ERA 5.x oraz Aktualizacja z wersji ERA 6.x.

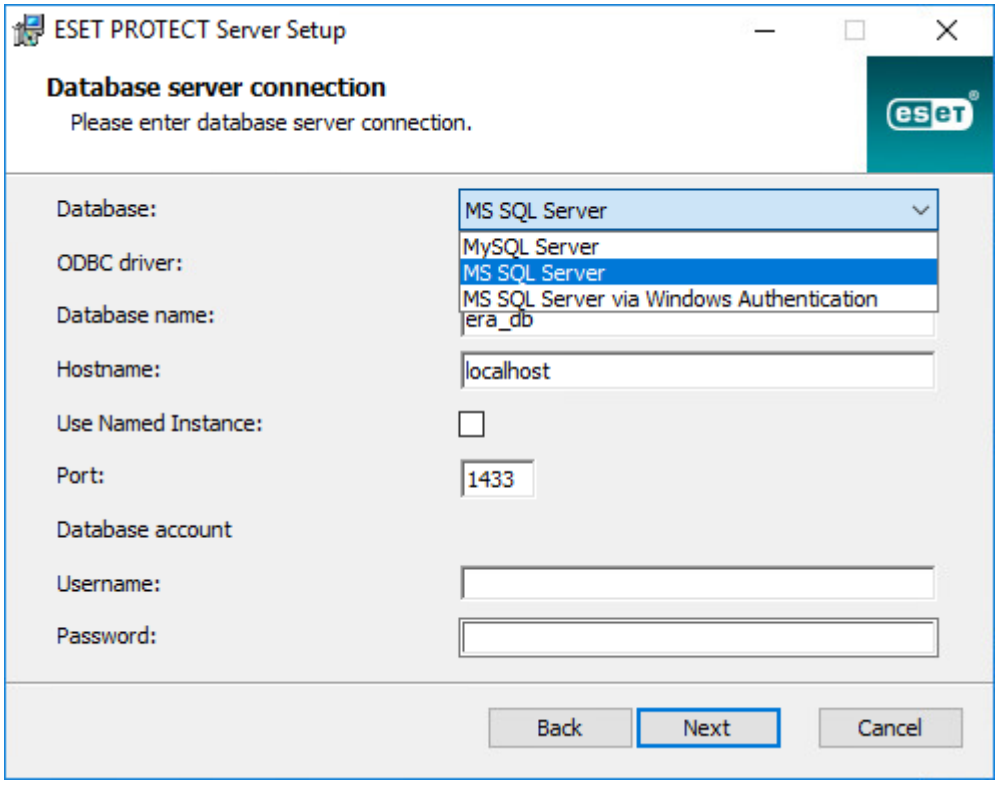
7. Jeśli po ukończeniu sprawdzania wymagań wstępnych okaże się, że środowisko spełnia wszystkie wymagania, rozpocznie się instalacja. Pamiętaj, że instalacja może potrwać ponad godzinę w zależności od konfiguracji systemu oraz sieci.

Podczas trwania instalacji Kreator instalacji ESET PROTECT nie będzie odpowiadać.



8. Jeśli w kroku 4 zostanie zainstalowany program **Microsoft SQL Server Express**, instalator przeprowadzi sprawdzenie połączenia z bazą danych. Jeśli masz istniejący serwer baz danych, instalator wyświetli monit o wprowadzenie szczegółów połączenia z bazą danych:

Konfigurowanie połączenia z serwerem SQL/MySQL

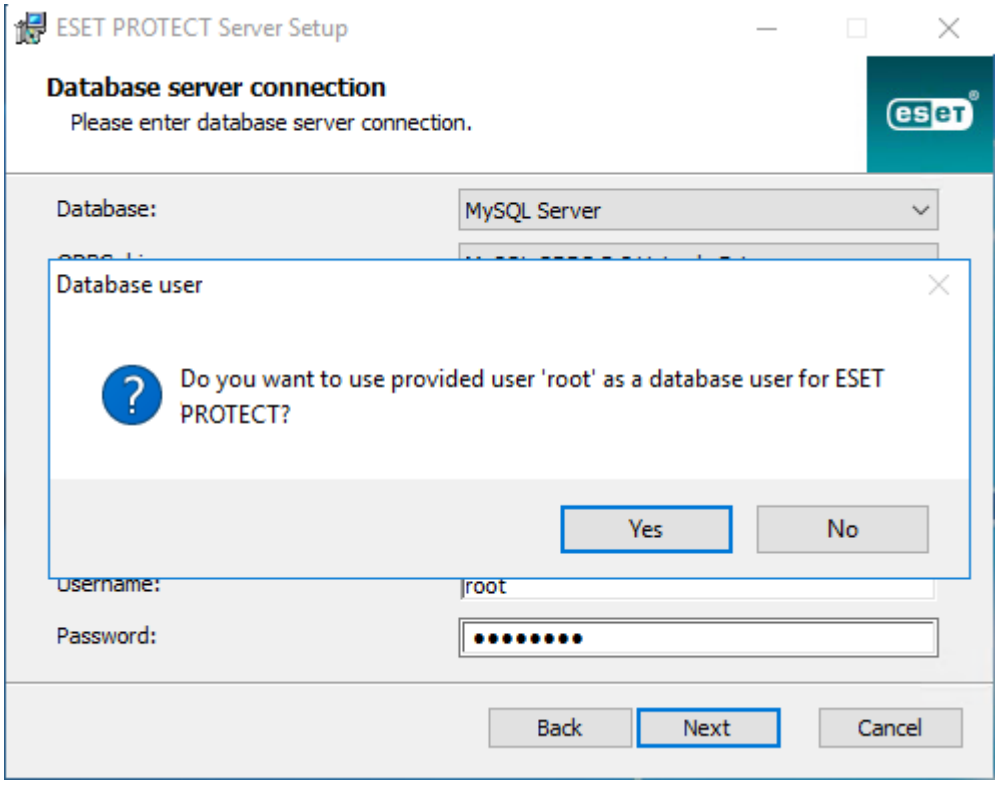


W odpowiednich polach wpisz **nazwę bazy danych**, **nazwę hosta** i **numer portu** (informacje te można znaleźć w narzędziu Microsoft SQL Server Configuration Manager) oraz **konto bazy danych** (**nazwę użytkownika** i **hasło**), a następnie kliknij przycisk **Dalej**. Instalator zweryfikuje połączenie z bazą danych. Jeśli na serwerze bazy danych istnieje baza danych (z wcześniejszej instalacji programu ESMC/ESET PROTECT), zostanie ona wykryta. Możesz wybrać pozycję **Użyj istniejącej bazy danych i zastosuj uaktualnienie** lub **Usuń istniejącą bazę danych i zainstaluj nową wersję**.

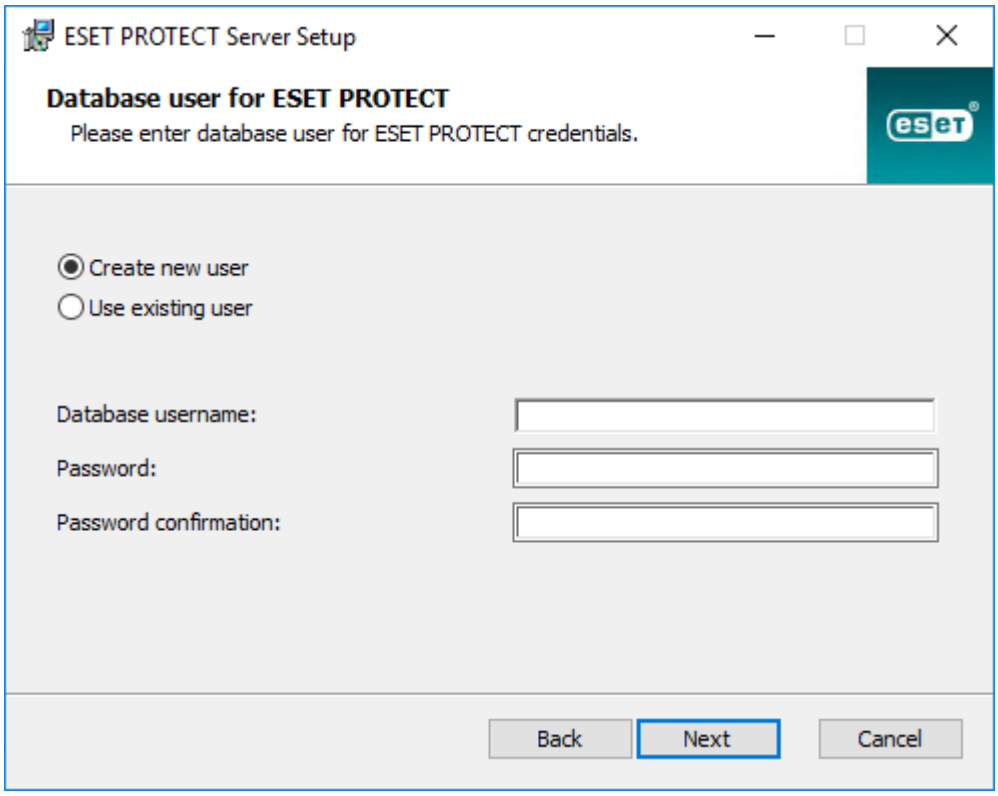
Użyj nazwanej instancji — w przypadku używania bazy danych MS SQL można też zaznaczyć pole wyboru **Użyj nazwanej instancji**, jeśli chcesz korzystać z własnej, niestandardowej instancji bazy danych. Niestandardową instancję bazy danych można ustawić w polu **Nazwa hosta** w postaci *NAZWA_HOSTA**INSTANCJA_BD* (na przykład *192.168.0.10**ESMC7SQL*). W przypadku bazy danych w klastrze należy użyć jedynie nazwy klastra. Po wybraniu tej opcji nie można zmienić używanego portu do łączenia się z bazą danych. System będzie korzystał z domyślnych portów określonych przez firmę Microsoft. Aby połączyć serwer ESET PROTECT z bazą danych MS SQL zainstalowaną w klastrze typu failover, wprowadź nazwę klastra w polu **Nazwa hosta**.

Podczas wprowadzania informacji o **koncie bazy danych** dostępne są dwie opcje. Można użyć **dedykowanego konta użytkownika bazy danych**, które będzie mieć dostęp tylko do bazy danych ESET PROTECT, albo **konta SA** (MS SQL) lub **konta użytkownika root** (MySQL). W przypadku zdecydowania o używaniu dedykowanego konta użytkownika konto to musi zostać utworzone z określonymi uprawnieniami. Szczegółowe informacje zawiera sekcja Dedykowane konto użytkownika bazy danych. Jeśli takie konto ma nie być używane, należy wprowadzić konto administratora (konto SA lub konto użytkownika root).

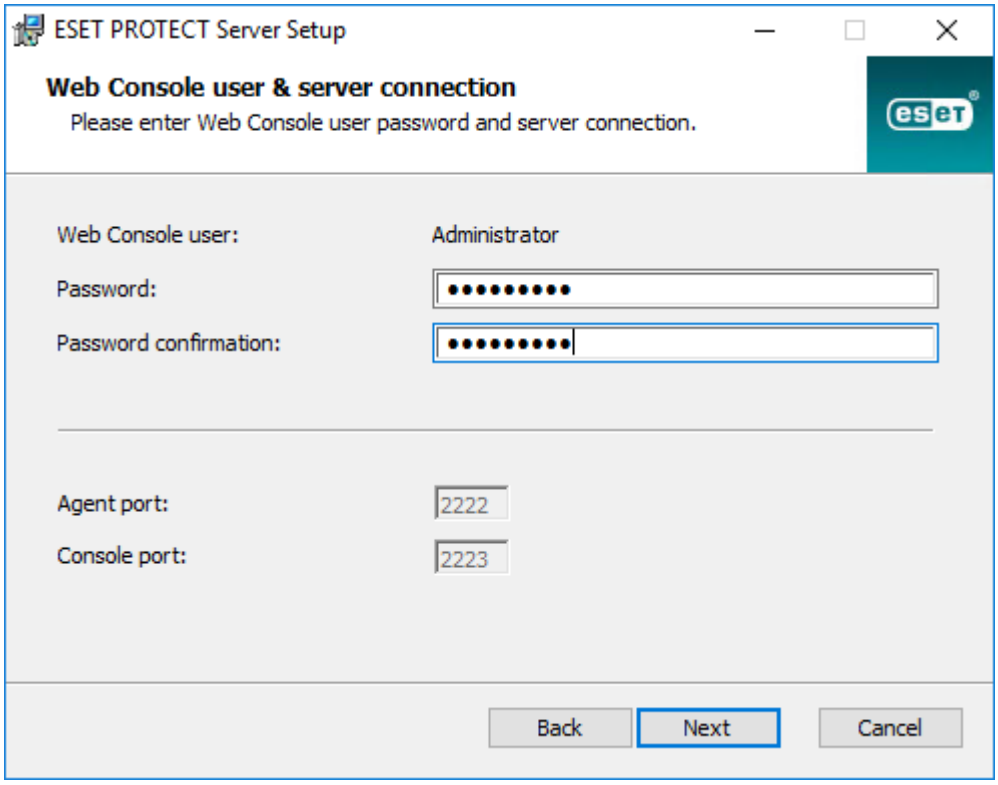
Jeśli w poprzednim oknie wprowadzono **konto SA** lub **konto użytkownika root**, kliknij pozycję **Tak**, aby kontynuować przy użyciu konta SA / konta użytkownika root jako użytkownika bazy danych programu ESET PROTECT.



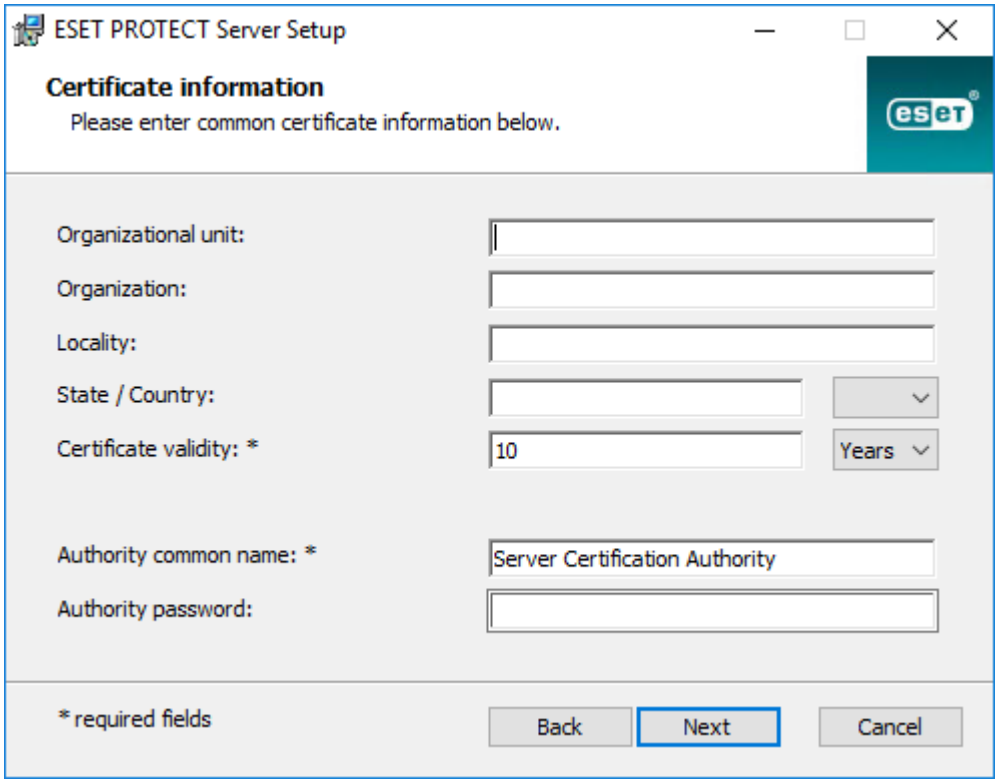
W przypadku kliknięcia pozycji **Nie** musisz wybrać pozycję **Utwórz nowego użytkownika** (jeśli nie został jeszcze utworzony) lub **Użyj istniejącego użytkownika** (w przypadku dedykowanego konta użytkownika bazy danych).



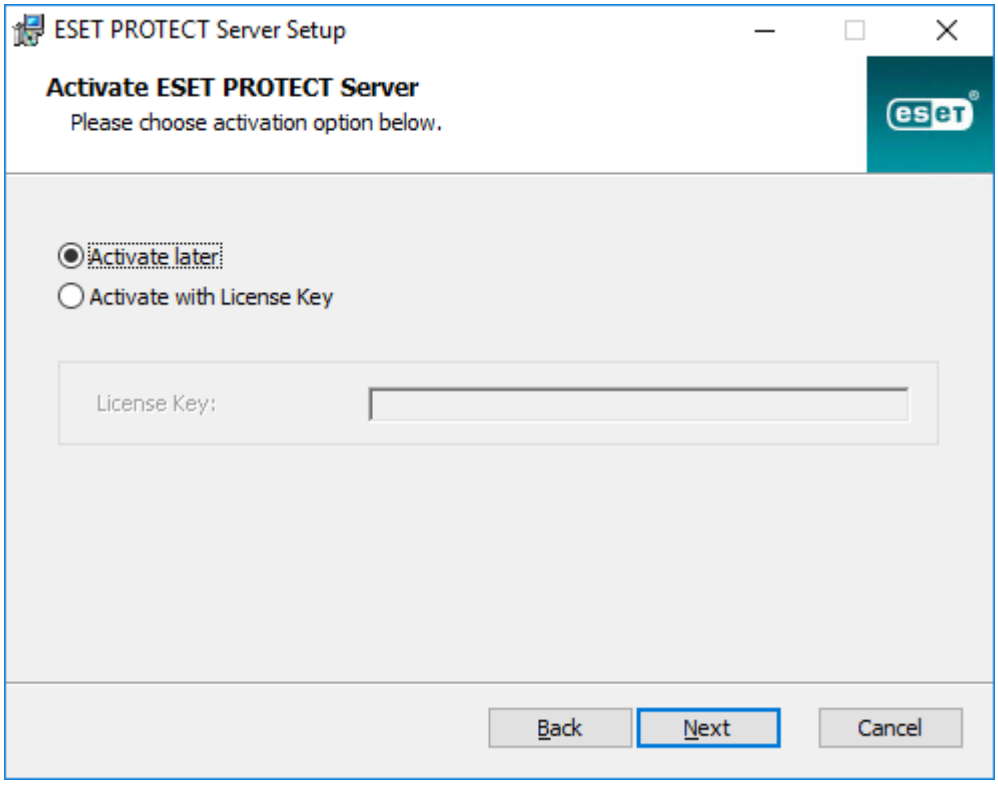
9. Instalator wyświetli monit o wprowadzenie hasła do konta administratora konsoli internetowej. To hasło jest ważne, ponieważ będzie służyć do logowania się w konsoli internetowej ESET PROTECT. Kliknij przycisk **Dalej**.



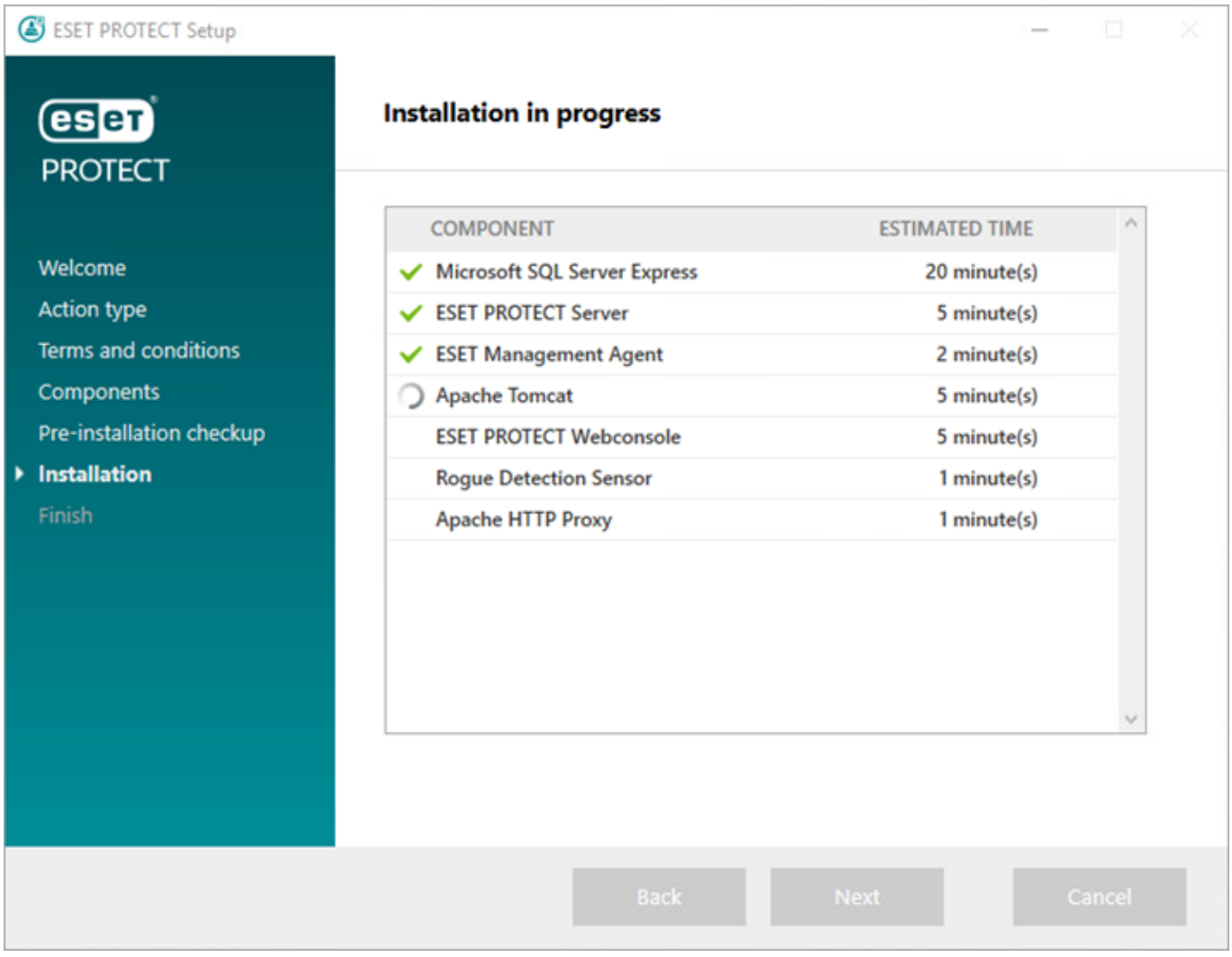
10. Możesz pozostawić puste pola lub wprowadzić informacje o firmie, które będą widoczne w szczegółach certyfikatów agenta ESET Management i serwera ESET PROTECT. Jeśli wprowadzisz hasło w polu **Hasło urzędu**, zapamiętaj je. Kliknij przycisk **Dalej**.



11. Wprowadź prawidłowy **Klucz licencyjny** (jest dołączony do wiadomości e-mail od firmy ESET z informacjami o nowym zakupie), a następnie kliknij przycisk **Dalej**. Jeśli korzystasz z poświadczeń licencyjnych starszej wersji (nazwy użytkownika i hasła), przekonwertuj te poświadczenia na klucz licencyjny. Alternatywnie można wybrać opcję **Aktywuj później** (dodatkowe instrukcje można znaleźć w rozdziale Aktywacja).



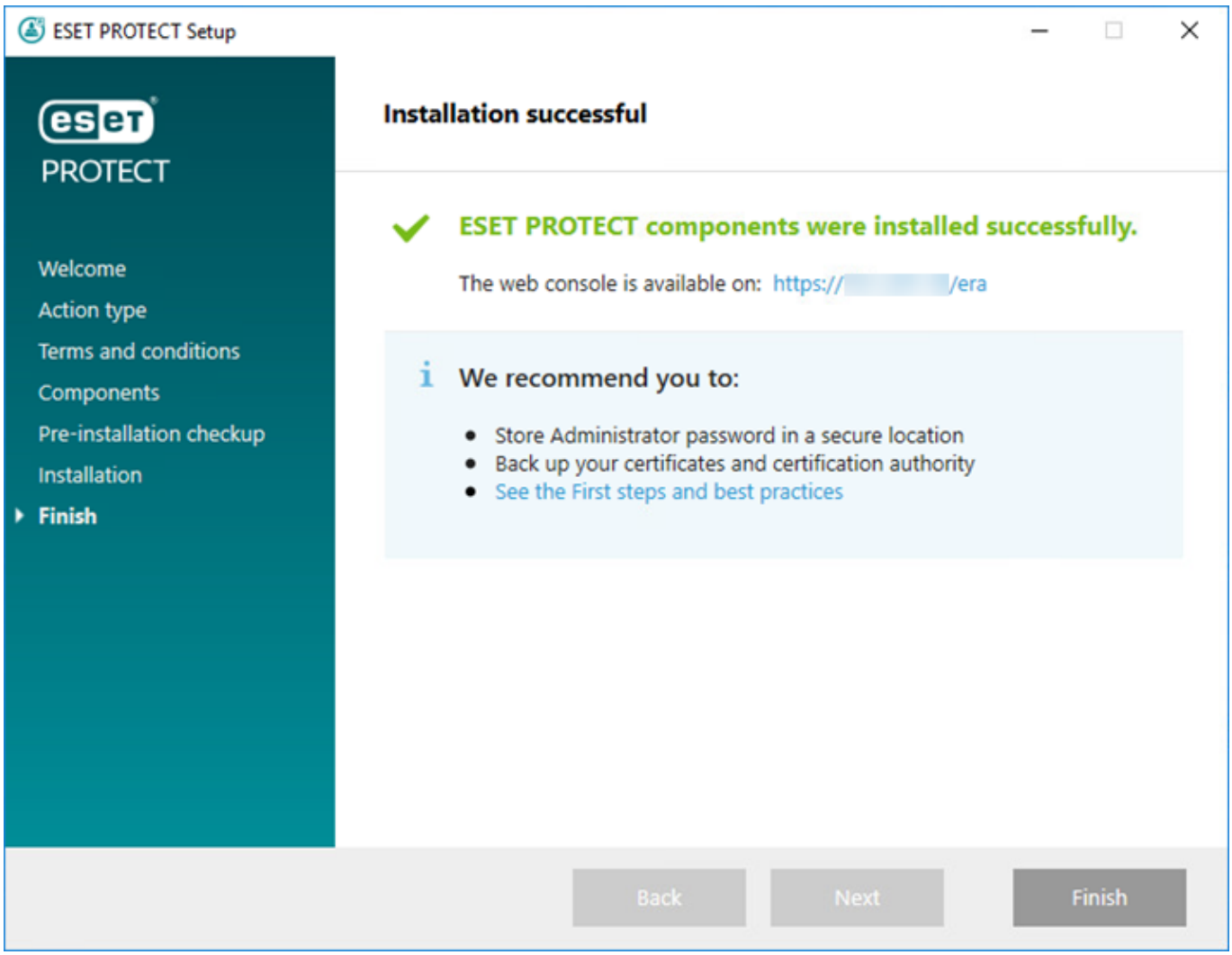
12. Zobaczysz postęp instalacji.



13. Jeśli wybrana została opcja instalacji narzędzia **Rogue Detection Sensor**, wyświetlą się okna instalacji

sterownika WinPcap. Należy się upewnić, że zaznaczone jest pole wyboru **Automatycznie uruchamiaj sterownik WinPcap przy rozruchu**.

14. Po ukończeniu instalacji zostanie wyświetlony komunikat „Zainstalowano komponenty rozwiązania ESET PROTECT" z adresem URL konsoli internetowej ESET PROTECT. Kliknij adres URL, aby otworzyć konsolę internetową lub kliknij przycisk **Zakończ**.



Jeśli instalacja nie powiedzie się:

• Zapoznaj się z plikami dziennika instalacji w pakiecie instalacji kompleksowej. Dzienniki znajdują się w tym samym katalogu co instalator kompleksowy, na przykład:
`C:\Users\Administrator\Downloads\x64\logs\`

• Dodatkowe informacje dotyczące rozwiązywania problemów można znaleźć w sekcji Rozwiązywanie problemów.

Instalowanie Modułu zarządzania urządzeniami mobilnymi ESET PROTECT (tryb autonomiczny)

Aby zainstalować narzędzie Moduł zarządzania urządzeniami mobilnymi jako narzędzie autonomiczne na komputerze innym niż serwer ESET PROTECT, należy postępować zgodnie z poniższymi instrukcjami.

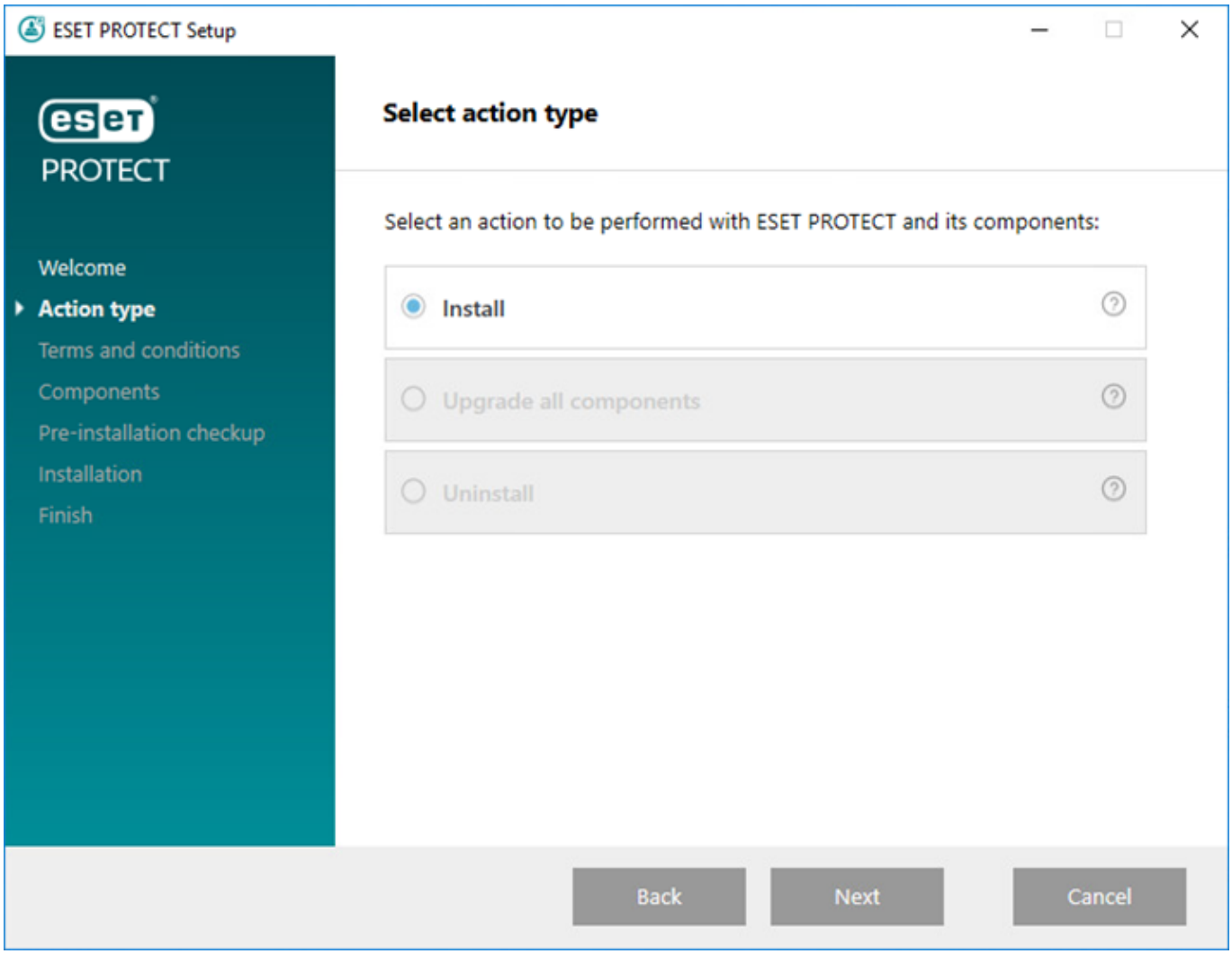
Moduł zarządzania urządzeniami mobilnymi musi być dostępny przez Internet, aby na stałe umożliwić zarządzanie urządzeniami mobilnymi bez względu na ich lokalizację.

Należy pamiętać, że urządzenie mobilne łączy się z narzędziem Moduł zarządzania urządzeniami mobilnymi, co wiąże się z przesyłaniem danych przez sieć komórkową. Jest to szczególnie istotne w przypadku roamingu.

W celu zainstalowania narzędzia Moduł zarządzania urządzeniami mobilnymi w systemie Windows wykonaj poniższe czynności:

1. Najpierw przeczytaj wymagania wstępne i upewnij się, czy zostały wszystkie spełnione.

2. Kliknij dwukrotnie pakiet instalacyjny, aby go uruchomić. Wybierz pozycję **Zainstaluj** i kliknij przycisk **Dalej**.

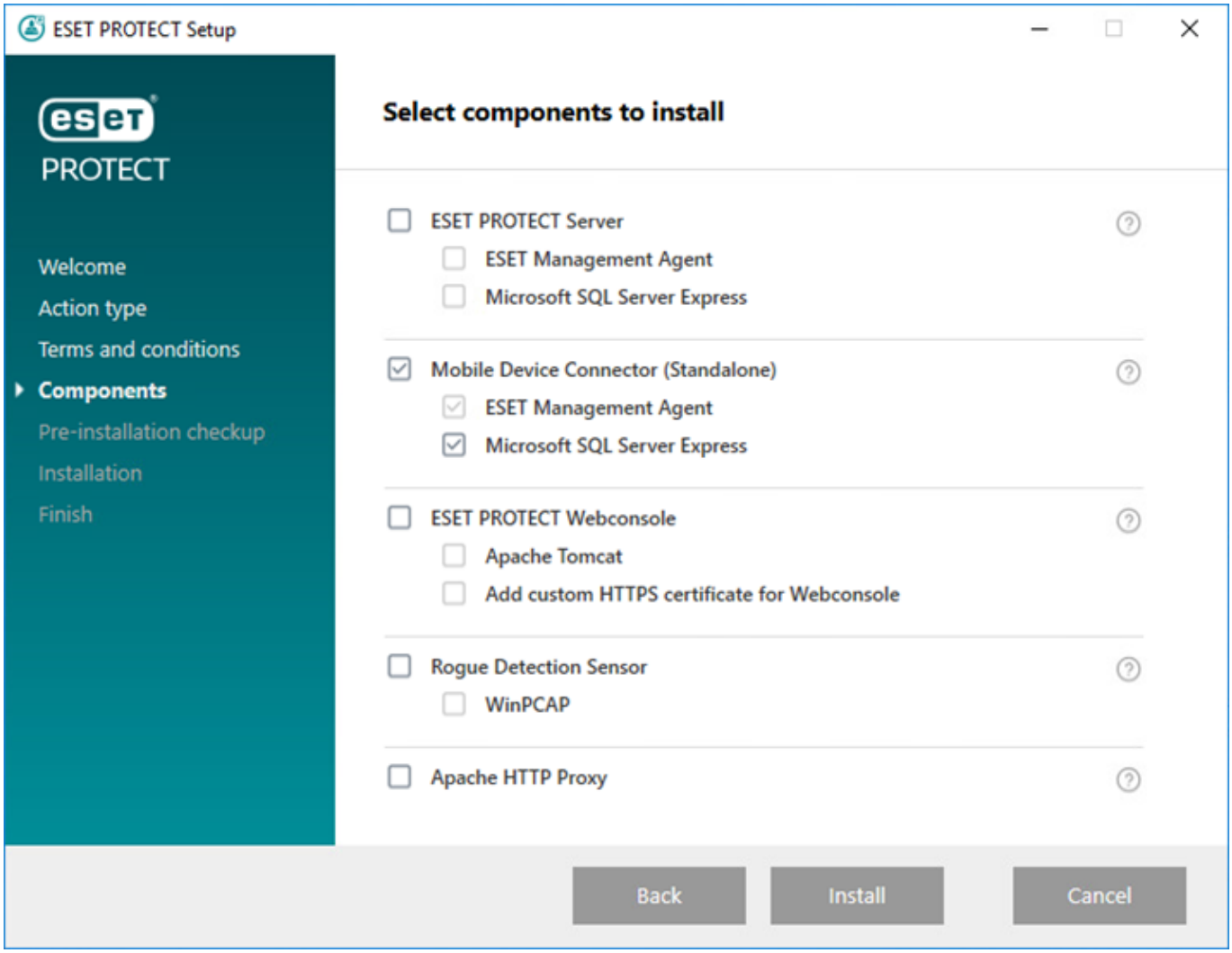


3. Jeśli nie zgadzasz się na przesyłanie firmie ESET raportów o awariach i anonimowych danych telemetrycznych (takich jak rodzaj i wersja systemu operacyjnego, wersja produktu ESET i inne informacje dotyczące konkretnego produktu), usuń zaznaczenie pola wyboru **Weź udział w programie ulepszania produktu**. W przypadku niezaznaczenia tego pola wyboru dane telemetryczne i raporty o awariach będą przesyłane firmie ESET.

4. Po zaakceptowaniu umowy EULA kliknij opcję **Dalej**.

5. Zaznacz tylko pole wyboru przy opcji **Mobile Device Connector (Samodzielne)**. Narzędzie Moduł zarządzania urządzeniami mobilnymi ESET PROTECT wymaga do działania **bazy danych**. Jeśli chcesz ją zainstalować,

zaznacz pole wyboru **Microsoft SQL Server Express**. W przeciwnym razie pozostaw je puste. Jeśli chcesz się połączyć z istniejącą bazą danych, będziesz mieć taką możliwość w trakcie procesu instalacji. Aby rozpocząć instalację, kliknij przycisk **Zainstaluj**.



6. Jeśli baza danych została zainstalowana w ramach procesu instalacji zgodnie z informacjami podanymi w kroku 5, zostanie ona teraz zainstalowana automatycznie. W związku z tym przejdź od razu do kroku 8. Jeśli opcja instalacji bazy danych nie została zaznaczona w kroku 5, wyświetli się teraz komunikat z prośbą o podłączenie komponentu MDM do istniejącej bazy danych.

> Istnieje możliwość korzystania z tego samego serwera bazy danych, który jest używany do obsługi bazy danych programu ESET PROTECT, zalecamy jednak korzystanie z innego, jeśli planowana liczba zarejestrowanych urządzeń mobilnych przekracza 80.

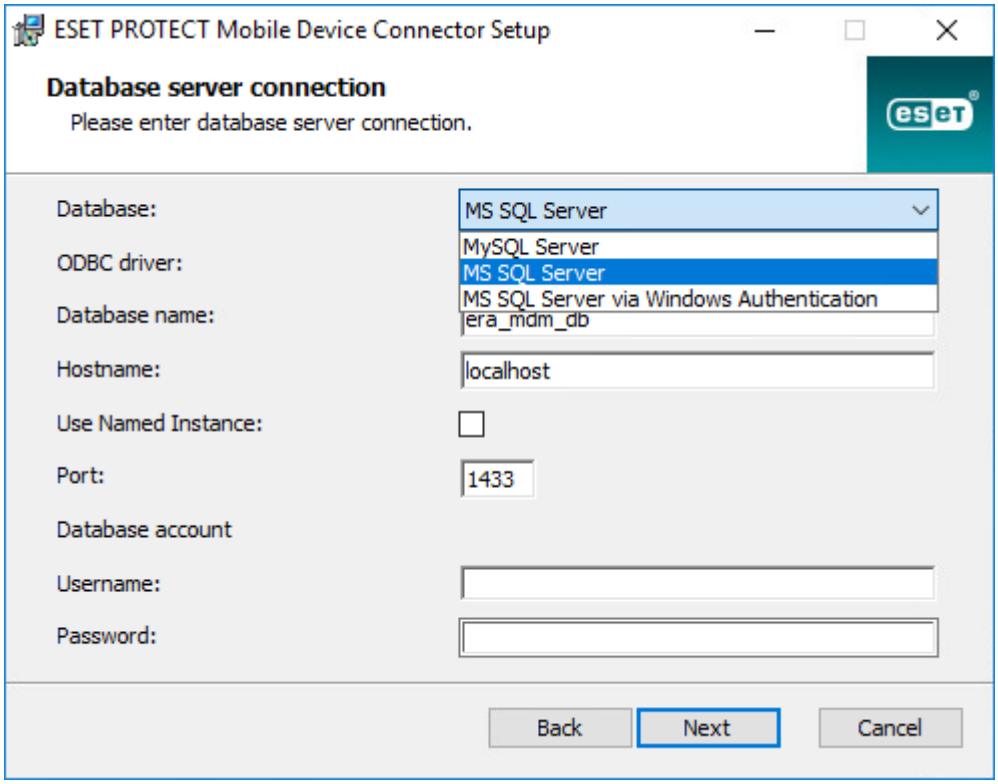
7. Instalator musi nawiązać połączenie z istniejącą bazą danych, która będzie używana przez narzędzie Moduł zarządzania urządzeniami mobilnymi. Należy podać następujące szczegóły połączenia:

- **Baza danych**: MySQL Server/MS SQL Server/MS SQL Server z uwierzytelnianiem systemu Windows

- **Sterownik ODBC**: sterownik MySQL ODBC 5.1/sterownik MySQL ODBC 5.2 Unicode/sterownik MySQL ODBC 5.3 Unicode/sterownik MySQL ODBC 8.0 Unicode/SQL Server/klient macierzysty SQL Server 10.0/sterownik ODBC 11 dla SQL Server/sterownik ODBC 13 dla SQL Server/sterownik ODBC 17 dla SQL Server/sterownik ODBC 18 dla SQL Server

- **Nazwa bazy danych**: Zalecamy użycie wstępnie zdefiniowanej nazwy lub jej zmianę w razie potrzeby.

- **Nazwa hosta**: nazwa hosta lub adres IP serwera bazy danych
- **Port**: port używany do łączenia się z serwerem bazy danych
- **Nazwa użytkownika / hasło** bazy danych.
- **Użyj nazwanej instancji** — w przypadku używania bazy danych MS SQL można też zaznaczyć pole wyboru **Użyj nazwanej instancji**, jeśli chcesz korzystać z własnej, niestandardowej instancji bazy danych. Niestandardową instancję bazy danych można ustawić w polu **Nazwa hosta** w postaci *NAZWA_HOSTA**INSTANCJA_BD* (na przykład *192.168.0.10**ESMC7SQL*). W przypadku bazy danych w klastrze należy użyć jedynie nazwy klastra. Po wybraniu tej opcji nie można zmienić używanego portu do łączenia się z bazą danych. System będzie korzystał z domyślnych portów określonych przez firmę Microsoft. Aby połączyć serwer ESET PROTECT z bazą danych MS SQL zainstalowaną w klastrze typu failover, wprowadź nazwę klastra w polu **Nazwa hosta**.

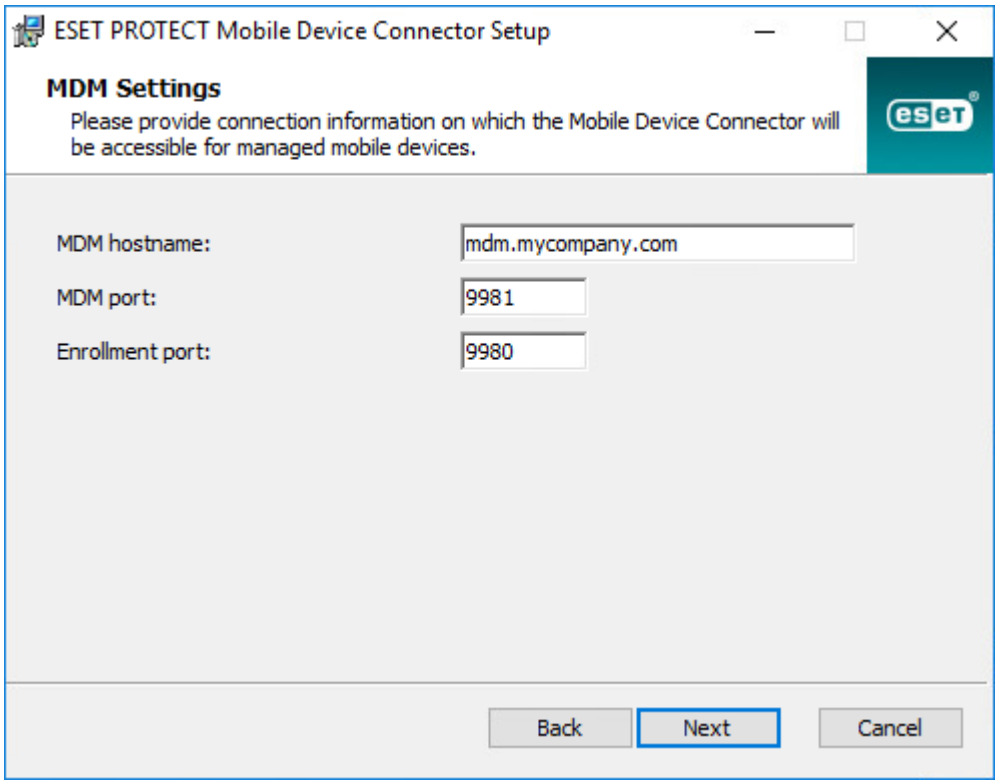


8. Jeśli połączenie zostało nawiązane pomyślnie, zostanie wyświetlony monit o zatwierdzenie danego użytkownika jako użytkownika bazy danych komponentu MDM ESET PROTECT.

9. Po pomyślnym zainstalowaniu bazy danych lub nawiązaniu przez instalator połączenia z istniejącą bazą danych możesz przejść do instalacji komponentu MDM. Podaj **nazwę hosta MDM**: to domena publiczna lub publiczny adres IP serwera MDM dostępny dla urządzeń mobilnych łączących się przez Internet.

wpisana nazwa hosta MDM musi mieć taką samą postać, jak w **certyfikacie serwera HTTPS**. W przeciwnym razie na urządzeniu mobilnym z systemem iOS nie będzie można zainstalować profilu MDM. Jeśli na przykład istnieje adres IP określony w certyfikacie HTTPS, wpisz ten adres IP w polu **Nazwa hosta MDM**. W przypadku określenia nazwy FQDN (np. `mdm.mycompany.com`) w certyfikacie HTTPS, wprowadź tę nazwę FQDN w polu **Nazwa hosta MDM**. W przypadku użycia symbolu wieloznacznego * (np. `*.mycompany.com`) w certyfikacie HTTPS możesz użyć wpisu `mdm.mycompany.com` w polu **Nazwa hosta MDM**.

Na tym etapie instalacji należy zwracać szczególną uwagę na informacje wprowadzane w polu **Nazwa hosta MDM**. Jeśli okażą się one błędne, łącznik MDM będzie działał w sposób nieprawidłowy, a jedynym sposobem rozwiązania tego problemu będzie ponowna instalacja komponentu.



10. W następnym kroku sprawdź połączenie z bazą danych, klikając przycisk **Dalej**.

11. Podłącz łącznik MDM do serwera ESET PROTECT. Wypełnij pola **Host serwera** i **Port serwera** wymagane do nawiązania połączenia z serwerem ESET PROTECT oraz wybierz opcję **Wspomagana instalacja serwerowa** lub **Instalacja offline**, aby przejść dalej:

- **Wspomagana instalacja serwerowa** — podaj poświadczenia administratora konsoli internetowej ESET PROTECT, a instalator automatycznie pobierze wymagane certyfikaty. Sprawdź również uprawnienia wymagane w przypadku wspomaganej instalacji serwerowej.

    1.Wprowadź dane w polach **Host serwera** (nazwa lub adres IP serwera ESET PROTECT) oraz **Port konsoli internetowej** (jeśli nie korzystasz z portu niestandardowego, pozostaw domyślny port 2223). Podaj również poświadczenia konta administratora konsoli internetowej — w polach **Nazwa użytkownika/Hasło**.

    2.Po wyświetleniu monitu o zaakceptowanie certyfikatu kliknij pozycję **Tak**. Przejdź do kroku 11.

- **Instalacja offline** — uzupełnij pola Certyfikat serwera proxy oraz Urząd certyfikacji, które można wyeksportować z programu ESET PROTECT. Możesz też użyć certyfikatu niestandardowego i właściwego urzędu certyfikacji.

    1.Kliknij przycisk **Przeglądaj** obok **certyfikatu równorzędnego** i przejdź do lokalizacji, w której się on znajduje (jest to certyfikat serwera proxy wyeksportowany z programu ESET PROTECT). Pole tekstowe **Hasło do certyfikatu** pozostaw puste, ponieważ ten certyfikat nie wymaga podawania hasła.

    2.Powtórz tę samą procedurę w przypadku urzędu certyfikacji i przejdź do kroku 11.

Jeśli w programie ESET PROTECT używane są certyfikaty niestandardowe (zamiast domyślnych generowanych automatycznie podczas instalowania produktu ESET PROTECT), należy z nich skorzystać po wyświetleniu monitu o podanie certyfikatu serwera proxy.

12. Określ folder docelowy dla narzędzia Moduł zarządzania urządzeniami mobilnymi (zalecamy użycie folderu domyślnego), kliknij przycisk **Dalej**, a następnie **Zainstaluj**.

Po zakończeniu instalacji komponentu MDM zostanie wyświetlony komunikat z informacją o potrzebie zainstalowania Agenta. Aby rozpocząć instalację, kliknij przycisk **Dalej**, zaakceptuj umowę EULA, jeśli zgadzasz się z jej treścią, i postępuj zgodnie z poniższymi instrukcjami:

1. Wprowadź dane w polach **Host serwera** (nazwę hosta lub adres IP serwera ESET PROTECT) i **Port serwera** (port domyślny to 2222 — jeśli używasz innego portu, zastąp go niestandardowym numerem portu).

Należy upewnić się, że **host serwera** odpowiada co najmniej jednej z wartości (najlepiej, aby to była wartość FQDN) zdefiniowanych w polu **Host certyfikatu serwera**. W przeciwnym razie zostanie wyświetlony błąd „Odebrany certyfikat serwera nie jest prawidłowy”. Jedynym wyjątkiem jest symbol wieloznaczny (*) znajdujący się w polu Host certyfikatu serwera. Symbol ten oznacza, że można użyć dowolnego **hosta serwera**.

2. W przypadku używania serwera proxy zaznacz pole wyboru **Użyj serwera proxy**. Po wybraniu tego pola instalator będzie kontynuował **instalację offline**.

To ustawienie serwera proxy jest używane wyłącznie w celu replikacji między agentem ESET Management a serwerem ESET PROTECT, a nie do buforowania aktualizacji.
- **Nazwa hosta serwera proxy**: nazwa hosta lub adres IP komputera z serwerem proxy HTTP.
- **Port serwera**: wartość domyślna to 3128.
- **Nazwa użytkownika**, **hasło**: należy wprowadzić poświadczenia powiązane z serwerem proxy, jeśli korzysta on z funkcji uwierzytelniania.

Ustawienia serwera proxy można zmienić na późniejszym etapie w polityce. Serwer proxy musi być zainstalowany przed konfiguracją połączenia między agentem a serwerem za pośrednictwem serwera proxy.

3. Wybierz jedną z następujących opcji instalacji i wykonaj działania opisane w odpowiedniej części poniżej:

Wspomagana instalacja serwerowa — podaj poświadczenia administratora konsoli internetowej ESET PROTECT (instalator automatycznie pobierze wymagane certyfikaty).

Instalacja offline— podaj certyfikat agenta i urząd certyfikacji, które można wyeksportować z programu ESET PROTECT. Można też użyć certyfikatu niestandardowego.

- Aby kontynuować **wspomaganą instalację serwerową agenta**, należy postępować zgodnie z poniższymi instrukcjami:

1. W polu **Host serwera** wpisz nazwę hosta lub adres IP konsoli internetowej ESET PROTECT (taki sam jak serwera ESET PROTECT). Jeśli nie jest używany niestandardowy port, w polu **Port konsoli internetowej** pozostaw port domyślny, czyli 2223. W polach **Nazwa użytkownika i Hasło wpisz poświadczenia konta konsoli internetowej**. Aby zalogować się jako użytkownik domeny, zaznacz pole wyboru obok pozycji **Zaloguj się do domeny**.

- należy się upewnić, że **host serwera** odpowiada co najmniej jednej z wartości (najlepiej, aby to była wartość FQDN) zdefiniowanych w polu **Host certyfikatu serwera**. W przeciwnym razie zostanie wyświetlony błąd „Odebrany certyfikat serwera nie jest prawidłowy”. Jedynym wyjątkiem jest symbol wieloznaczny (*) znajdujący się w polu Host certyfikatu serwera. Symbol ten oznacza, że można użyć dowolnego **hosta serwera**.
- Nie można używać użytkownika z uwierzytelnianiem dwuskładnikowym w instalacjach wspomaganych przez serwer.

2. Po wyświetleniu monitu o zaakceptowanie certyfikatu kliknij opcję **Tak**.

3. Wybierz opcję **Nie twórz komputera (komputer zostanie utworzony automatycznie przy pierwszym połączeniu)** lub **Wybierz niestandardową grupę statyczną**. Kliknięcie opcji **Wybierz niestandardową grupę statyczną** umożliwi wybranie pozycji z listy grup statycznych istniejących na serwerze ESET PROTECT. Komputer zostanie dodany do wybranej grupy.

4. Określ folder docelowy dla agenta ESET Management (zalecamy użycie domyślnej lokalizacji), kliknij przycisk **Dalej** i następnie przycisk **Zainstaluj**.

- Aby kontynuować **instalację offline agenta**, należy postępować zgodnie z poniższymi instrukcjami:

1. Jeśli w poprzednim kroku wybrano opcję **Użyj serwera proxy**, podaj **nazwę hosta serwera proxy**, **port serwera proxy** (port domyślny to 3128), **nazwę użytkownika** i **hasło**, a następnie kliknij przycisk **Dalej**.

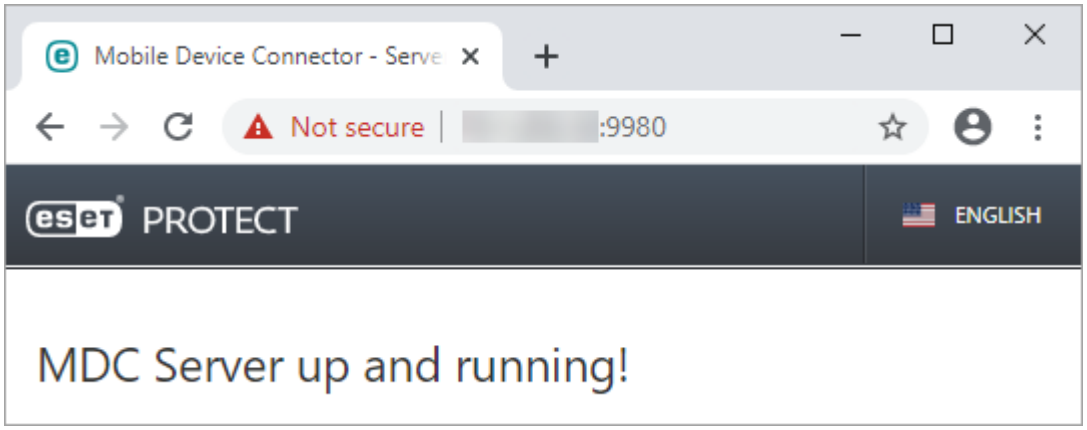
2. Kliknij przycisk **Przeglądaj** i przejdź do lokalizacji certyfikatu równorzędnego (jest to certyfikat agenta wyeksportowany z programu ESET PROTECT). Pole tekstowe **Hasło do certyfikatu** pozostaw puste, ponieważ ten certyfikat nie wymaga podawania hasła. Nie musisz wybierać wartości pola **Urząd certyfikacji** — pozostaw to pole puste.

Jeśli w programie ESET PROTECT jest używany certyfikat niestandardowy (zamiast certyfikatów domyślnych wygenerowanych automatycznie podczas instalacji programu ESET PROTECT), należy wskazać odpowiednie certyfikaty niestandardowe.

Hasło do certyfikatu nie może zawierać następujących znaków: " \ Znaki te powodują błąd krytyczny podczas inicjowania agenta.

3. Kliknij przycisk **Dalej**, aby zainstalować w folderze domyślnym, lub przycisk **Zmień**, aby wybrać inny folder (zalecamy użycie folderu domyślnego).

Po ukończeniu instalacji sprawdź, czy Moduł zarządzania urządzeniami mobilnymi działa poprawnie, otwierając stronę *https://nazwa-hosta-mdm:port-rejestracji* (na przykład *https://mdm.company.com:9980*) w przeglądarce internetowej lub na urządzeniu mobilnym. Jeśli instalacja przebiegła prawidłowo, wyświetlony zostanie następujący komunikat:



Po wykonaniu powyższych czynności można aktywować narzędzie MDM w programie ESET PROTECT.

Instalowanie na platformie Microsoft Azure

Użytkownicy, którzy preferują rozwiązanie zarządzane, zamiast programu ESET PROTECT w siedzibie firmy, mogą korzystać z programu ESET ESET PROTECT na platformie chmurowej Microsoft Azure.

Więcej informacji na ten temat zawiera następująca treść w bazie wiedzy:

- Rozpocznij pracę z programem ESET PROTECT — Azure
- Maszyna wirtualna programu ESET PROTECT dla platformy Microsoft Azure — najczęściej zadawane pytania
- Aby zainstalować program ESET PROTECT 9.1 na platformie Azure, wykonaj instrukcje podane w tym artykule z bazy wiedzy i skorzystaj z instalatora kompleksowego programu ESET PROTECT 9.1. Możesz też zainstalować program ESMC 7.2 na platformie Azure, a następnie uaktualnić go do wersji ESET PROTECT.

Instalacja komponentów w systemie Windows

Wiele scenariuszy instalacji wymaga zainstalowania różnych komponentów ESET PROTECT na różnych komputerach na potrzeby obsługi architektur sieci, w celu spełnienia wymagań dotyczących wydajności i z innych powodów. Poniższe pakiety instalacyjne są dostępne dla poszczególnych komponentów ESET PROTECT:

Instalacja komponentów podstawowych

- Serwer ESET PROTECT
- Konsola internetowa ESET PROTECT - Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT.
- Agent ESET Management (musi być zainstalowany na komputerach klienckich, może być zainstalowany na serwerze ESET PROTECT)

Instalacja komponentów opcjonalnych

- RD Sensor

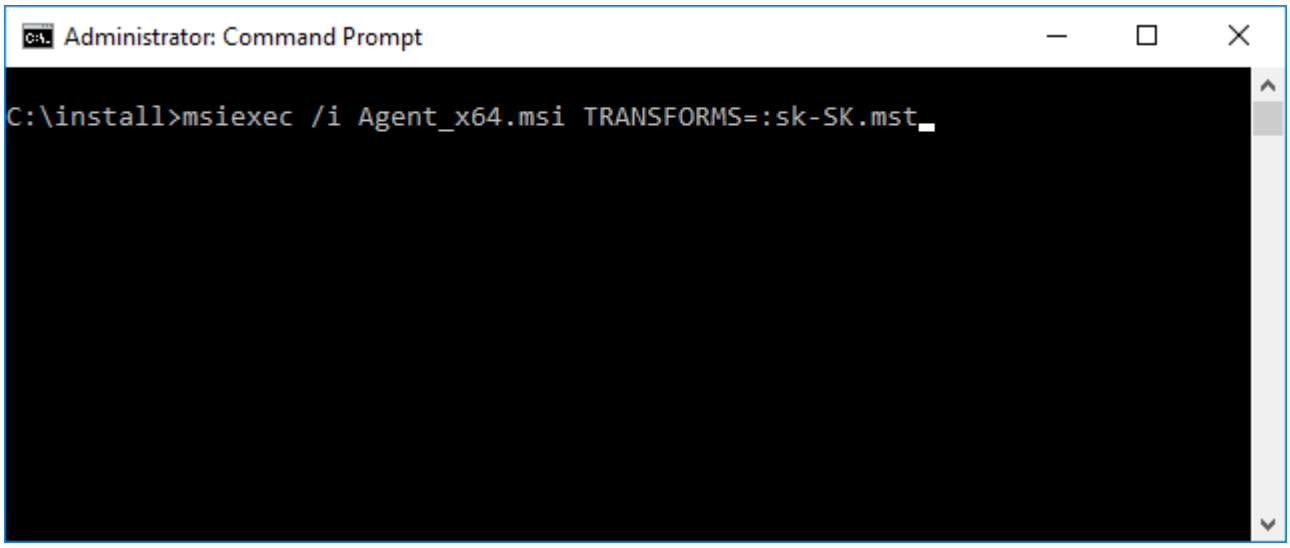
- Moduł zarządzania urządzeniami mobilnymi
- Serwer proxy Apache HTTP
- Narzędzie Mirror Tool

Zobacz także ESET PROTECT instalacja kompleksowa.

Dodatkowe instrukcje dotyczące uaktualniania programu ESMC do najnowszej wersji ESET PROTECT9.1 znajdziesz w procedurach aktualizacji.

Aby uruchomić instalację w języku lokalnym, należy uruchomić instalator MSI danego komponentu programu ESET PROTECT przy użyciu wiersza polecenia.

Poniżej przedstawiono przykład objaśniający sposób uruchomienia instalacji w języku słowackim:



W celu wskazania wybranego języka należy, w którym ma zostać uruchomiony instalator, należy podać odpowiedni parametr TRANSFORMS zgodnie z poniższą tabelą:

Język	Kod
Angielski (Stany Zjednoczone)	en-US
Arabski (Egipt)	ar-EG
Chiński uproszczony	zh-CN
Chiński tradycyjny	zh-TW
Chorwacki (Chorwacja)	hr-HR
Czeski (Czechy)	cs-CZ
Francuski (Francja)	fr-FR
Francuski (Kanada)	fr-CA
Niemiecki (Niemcy)	de-DE
Grecki (Grecja)	el-GR
Węgierski (Węgry)*	hu-HU
Indonezyjski (Indonezja)*	id-ID
Włoski (Włochy)	it-IT
Japoński (Japonia)	ja-JP

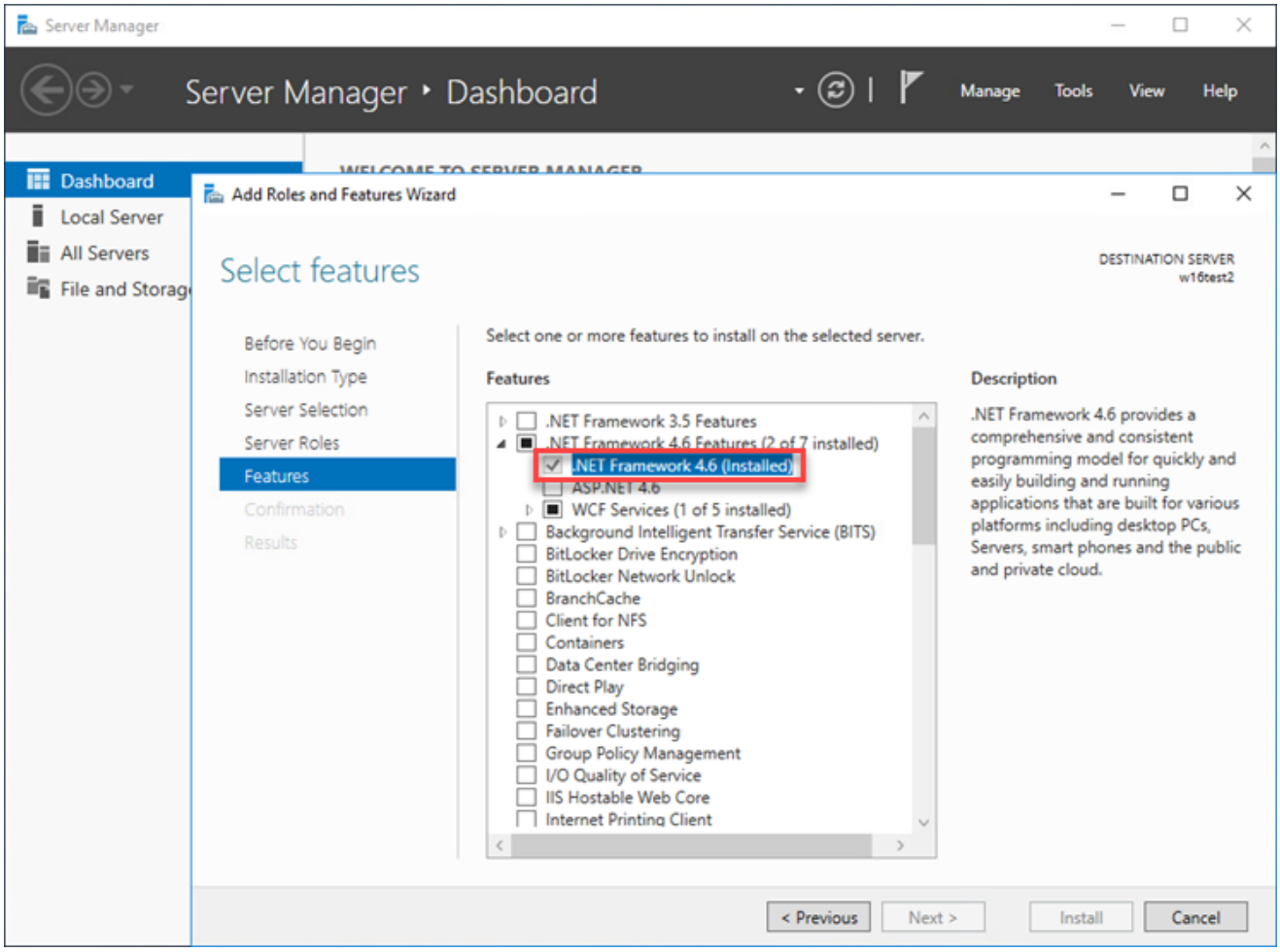
Język	Kod
Koreański (Korea)	ko-KR
Polski (Polska)	pl-PL
Portugalski (Brazylia)	pt-BR
Rosyjski (Rosja)	ru-RU
Hiszpański (Chile)	es-CL
Hiszpański (Hiszpania)	es-ES
Słowacki (Słowacja)	sk-SK
Turecki (Turcja)	tr-TR
Ukraiński (Ukraina)	uk-UA

* W tym języku jest dostępny jedynie produkt. Pomoc online jest niedostępna.

Instalacja serwera — Windows

Wymagania wstępne

- Wymagany jest ważny klucz licencyjny.
- Musisz mieć obsługiwaną wersję systemu Windows.
- Wymagane porty muszą być otwarte i dostępne — pełną listę portów można znaleźć tutaj.
- Zainstalowany i uruchomiony serwer oraz łącznik obsługiwanej bazy danych (Microsoft SQL Server lub MySQL). Zalecamy zapoznanie się ze szczegółami konfiguracji serwera bazy danych (Microsoft SQL Server lub MySQL) w celu prawidłowego skonfigurowania go pod kątem współpracy z programem ESET PROTECT. Informacje na temat konfiguracji bazy danych oraz użytkownika bazy danych MS SQL i MySQL znajdują się w naszym artykule bazy wiedzy.
- Zainstalowana konsola internetowa ESET PROTECT do zarządzania serwerem ESET PROTECT.
- Instalacja MS SQL Server Express wymaga programu Microsoft .NET Framework 4. Można go zainstalować przy użyciu **Kreatora dodawania ról i funkcji**:



Instalacja

Aby zainstalować komponent serwera ESET PROTECT w systemie Windows, należy wykonać poniższe czynności:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (*server_x64.msi*).

2. Uruchom instalator serwera ESET PROTECT i zaakceptuj umowę EULA, jeśli zgadzasz się z jej postanowieniami.

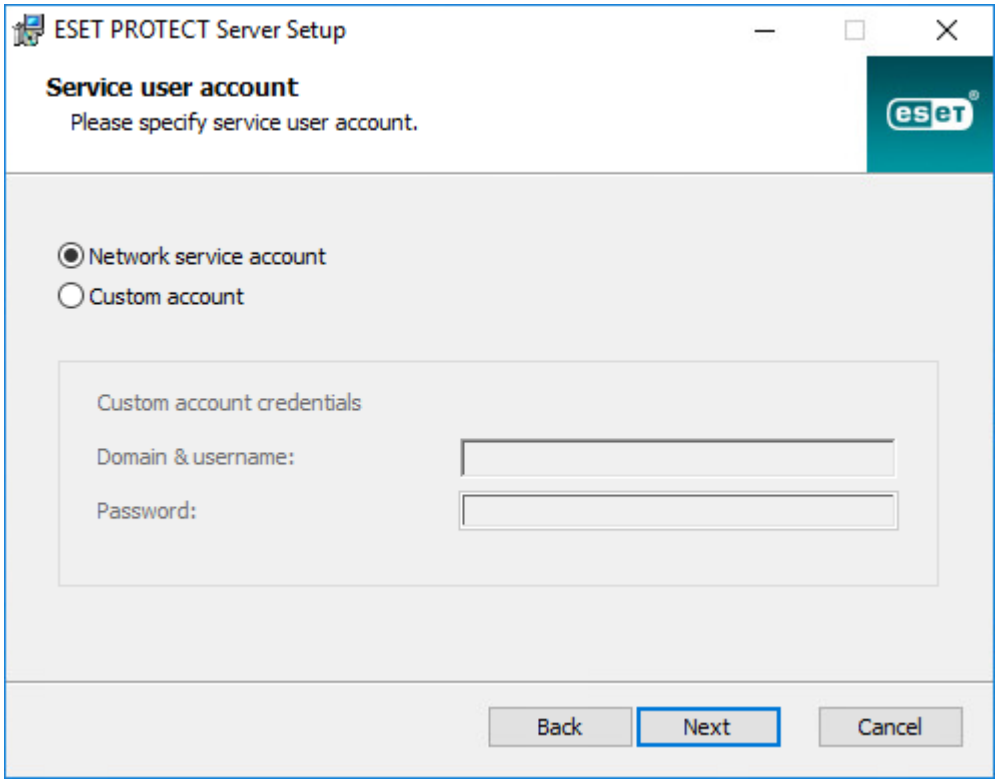
3. Jeśli nie zgadzasz się na przesyłanie firmie ESET raportów o awariach i anonimowych danych telemetrycznych (takich jak rodzaj i wersja systemu operacyjnego, wersja produktu ESET i inne informacje dotyczące konkretnego produktu), usuń zaznaczenie pola wyboru **Weź udział w programie ulepszania produktu**. W przypadku niezaznaczenia tego pola wyboru dane telemetryczne i raporty o awariach będą przesyłane firmie ESET.

4. Nie zaznaczaj pola wyboru **To jest instalacja klastra** i kliknij przycisk **Dalej**. Czy to instalacja w klastrze?

5. Wybierz **konto użytkownika usługi**. Konto to będzie używane do uruchamiania Usługi ESET PROTECT. Dostępne są następujące opcje:

• **Konto usługi sieciowej** — wybierz tę opcję, jeśli nie używasz domeny.

• **Konto niestandardowe**: wprowadź poświadczenia użytkownika domenowego: `DOMENA\NAZWA UŻYTKOWNIKA` oraz hasło.



6. Nawiąż połączenie z bazą danych. Tutaj przechowywane są wszystkie dane (hasło do konsoli internetowej ESET PROTECT, dzienniki komputerów klienckich itd.):

• **Baza danych**: MySQL Server/MS SQL Server/MS SQL Server z uwierzytelnianiem systemu Windows

• **Sterownik ODBC**: sterownik MySQL ODBC 5.1/sterownik MySQL ODBC 5.2 Unicode/sterownik MySQL ODBC 5.3 Unicode/sterownik MySQL ODBC 8.0 Unicode/SQL Server/klient macierzysty SQL Server 10.0/sterownik ODBC 11 dla SQL Server/sterownik ODBC 13 dla SQL Server/sterownik ODBC 17 dla SQL Server/sterownik ODBC 18 dla SQL Server

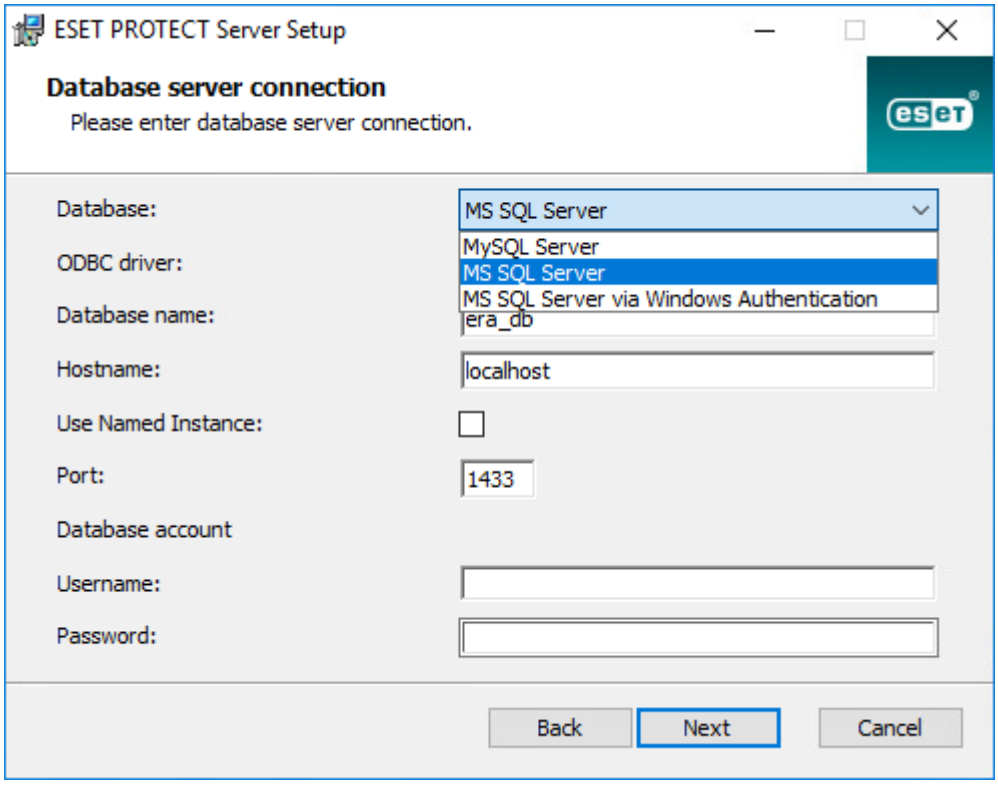
• **Nazwa bazy danych**: Zalecamy użycie wstępnie zdefiniowanej nazwy lub jej zmianę w razie potrzeby.

• **Nazwa hosta**: nazwa hosta lub adres IP serwera bazy danych

• **Port**: port używany do łączenia się z serwerem bazy danych

• **Nazwa użytkownika / hasło** bazy danych.

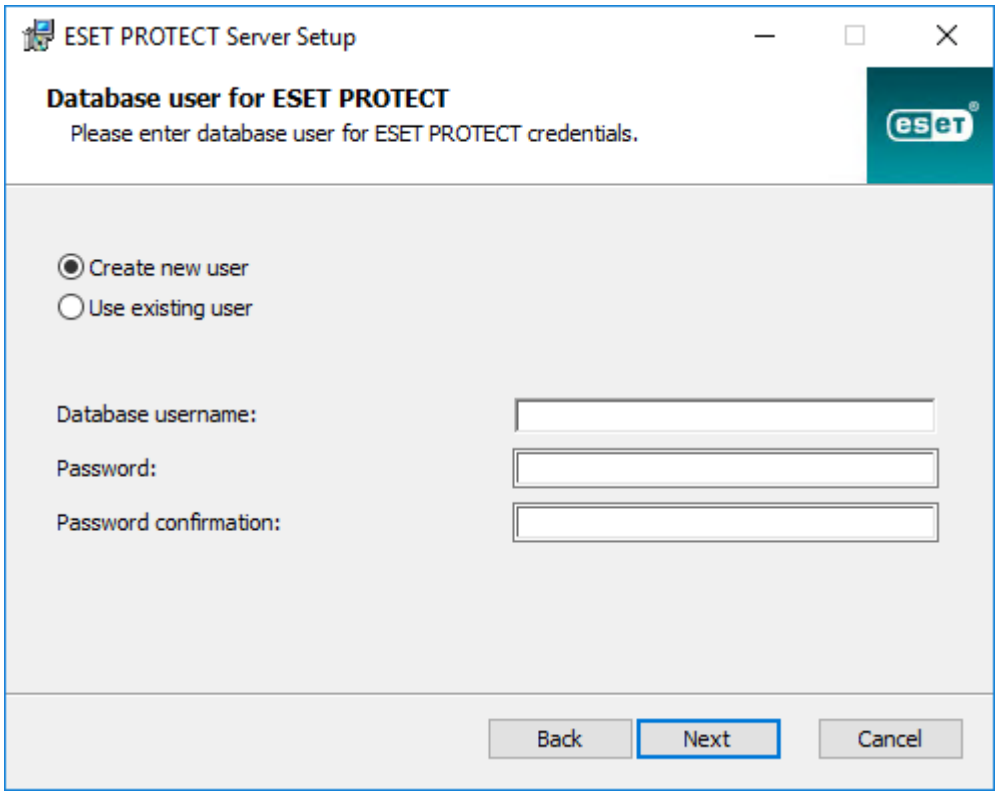
• **Użyj nazwanej instancji** — w przypadku używania bazy danych MS SQL można też zaznaczyć pole wyboru **Użyj nazwanej instancji**, jeśli chcesz korzystać z własnej, niestandardowej instancji bazy danych. Niestandardową instancję bazy danych można ustawić w polu **Nazwa hosta** w postaci *NAZWA_HOSTA\INSTANCJA_BD* (na przykład *192.168.0.10\ESMC7SQL*). W przypadku bazy danych w klastrze należy użyć jedynie nazwy klastra. Po wybraniu tej opcji nie można zmienić używanego portu do łączenia się z bazą danych. System będzie korzystał z domyślnych portów określonych przez firmę Microsoft. Aby połączyć serwer ESET PROTECT z bazą danych MS SQL zainstalowaną w klastrze typu failover, wprowadź nazwę klastra w polu **Nazwa hosta**.



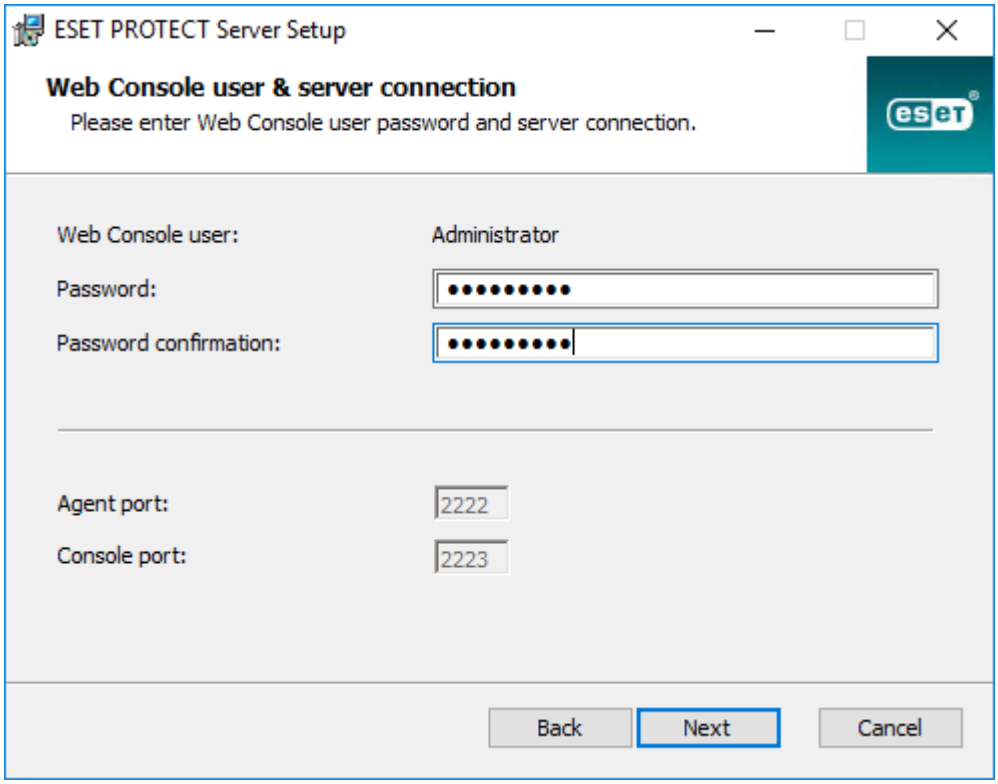
W bazie danych na serwerze ESET PROTECT zapisywane są duże obiekty blob danych. W związku z tym prawidłowe działanie ESET PROTECT wymaga skonfigurowania programu MySQL tak, by przyjmował duże pakiety.

W tym kroku weryfikowane jest połączenie z bazą danych. Jeśli połączenie jest prawidłowe, przejdź do następnego kroku.

7. Wybierz użytkownika programu ESET PROTECT, który ma dostęp do bazy danych. Można wybrać istniejącego użytkownika lub użytkownik może zostać skonfigurowany automatycznie.

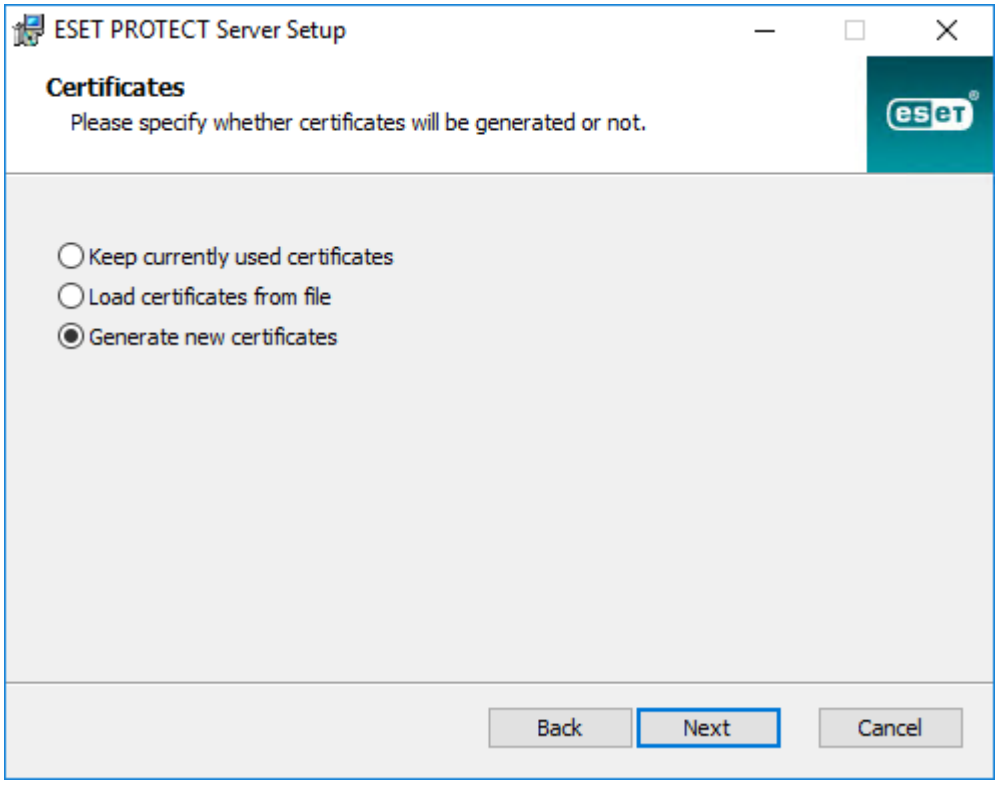


8. Wprowadź hasło dostępu do **konsoli internetowej**.



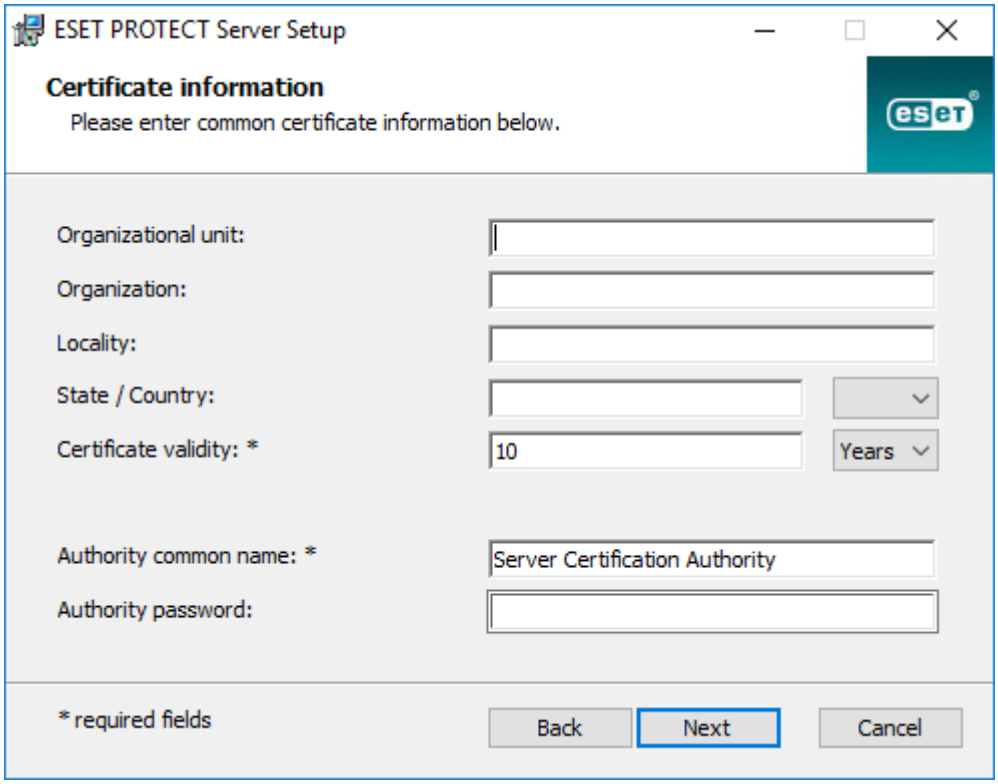
9. Program ESET PROTECT do komunikacji między klientem a serwerem wykorzystuje certyfikaty. Należy wybrać jedną z następujących opcji:

- **Zachowaj aktualnie używane certyfikaty** — ta opcja jest dostępna tylko wtedy, gdy baza danych była już wcześniej używana z innym serwerem ESET PROTECT.
- **Wczytaj certyfikaty z pliku** — wybierz istniejący certyfikat serwera i urząd certyfikacji.
- **Generuj nowe certyfikaty** — instalator generuje nowe certyfikaty.



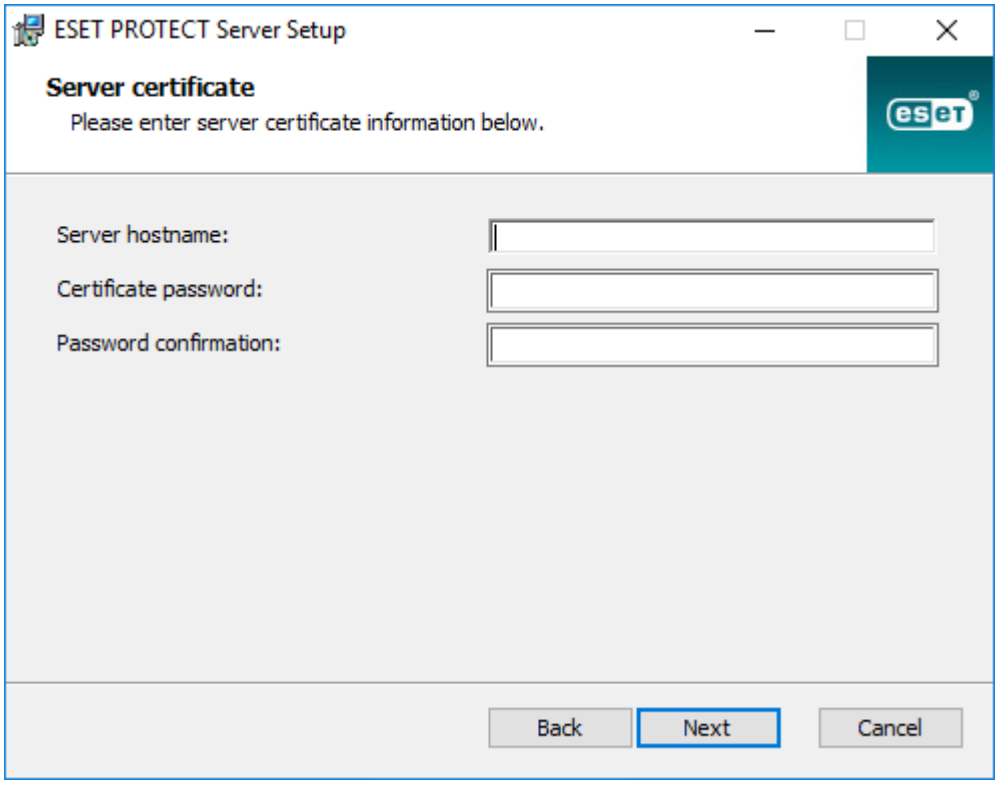
10. Wykonaj ten krok, jeśli w poprzednim kroku wybrano opcję **Generuj nowe certyfikaty**.

a)Określ dodatkowe informacje o certyfikatach (opcjonalnie). Jeśli wpiszesz **hasło urzędu**, upewnij się, że zostało ono zapamiętane.

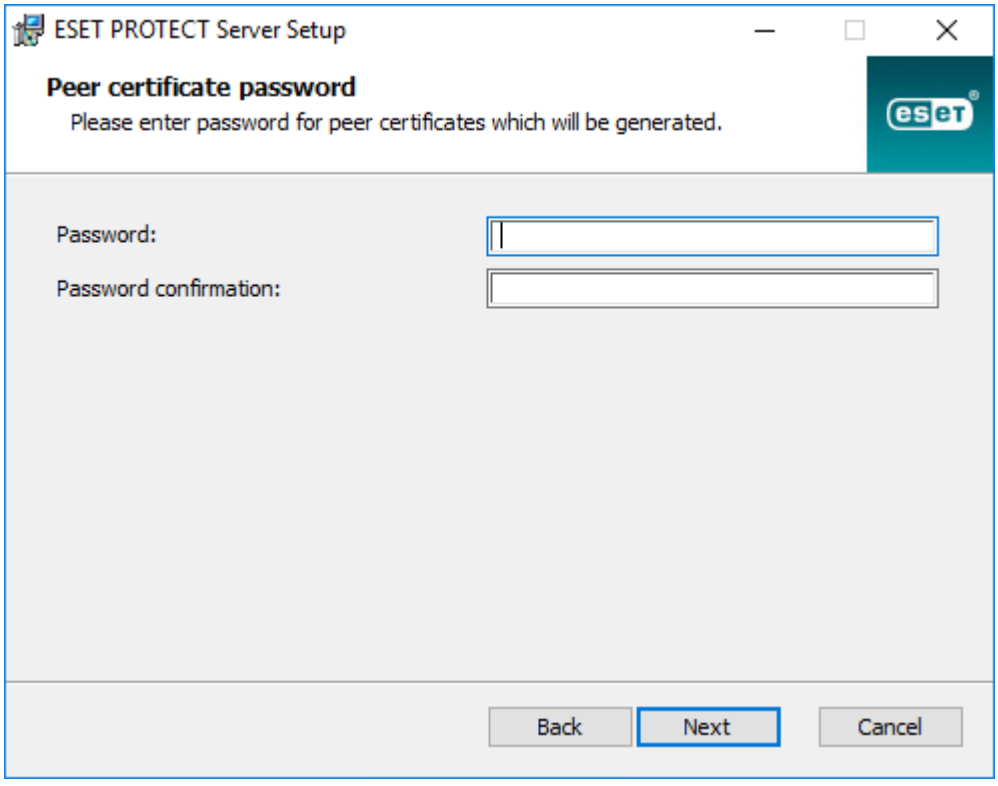


b)W polu **Certyfikat serwera** wpisz **nazwę hosta serwera** i **hasło do certyfikatu** (opcjonalnie).

Nazwa hosta serwera w certyfikacie serwera nie może zawierać żadnych z następujących słów kluczowych: `server`, `proxy` oraz `agent`.

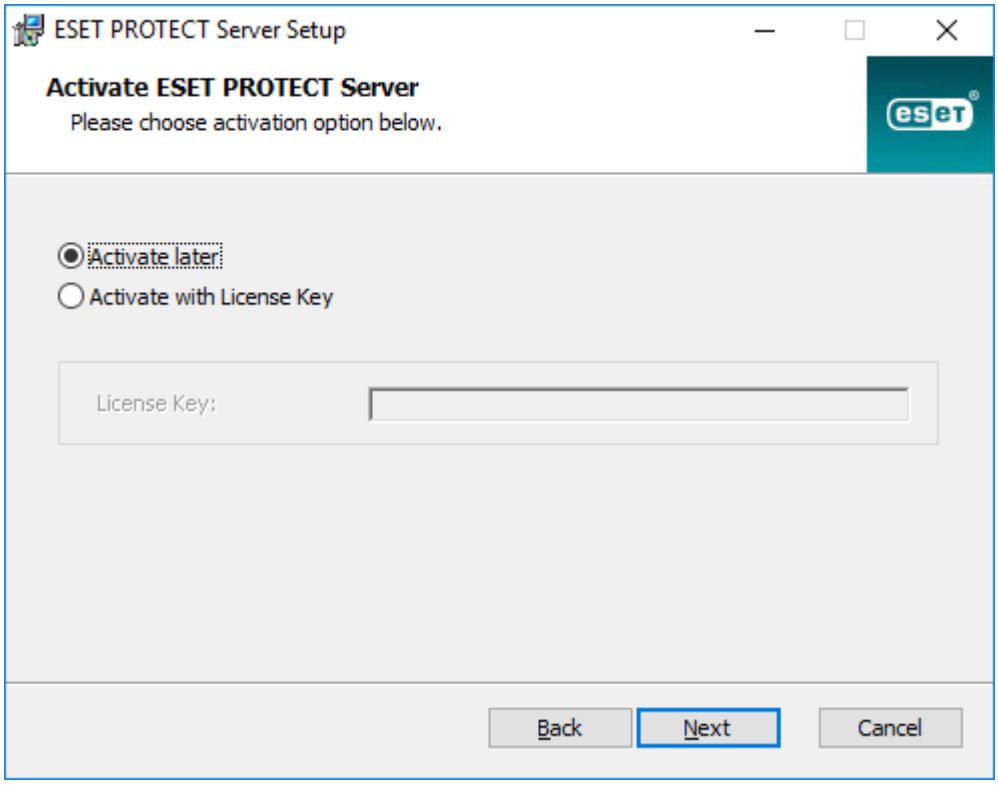


c)W polu **Hasło do certyfikatu równorzędnego** wpisz hasło dla certyfikatów równorzędnych agenta i serwera proxy.



11. W ramach konfiguracji może zostać wykonane wstępne zadanie Synchronizacja grupy statycznej. Wybierz metodę (**Nie synchronizuj**, **Synchronizuj z siecią Windows Network**, **Synchronizuj z usługą Active Directory**) i kliknij przycisk **Dalej**.

12. Wpisz prawidłowy klucz licencyjny lub wybierz opcję **Aktywuj później**.



13. Potwierdź lub zmień folder instalacji serwera i kliknij przycisk **Dalej**.

14. Aby zainstalować serwer ESET PROTECT, kliknij opcję **Zainstaluj**.

Po zakończeniu ESET PROTECT instalacji serwera można zainstalować agenta ESET Management na tym samym komputerze (opcjonalnie), aby włączyć zarządzanie serwerem w taki sam sposób, jak na komputerze klienta.

Wymagania dotyczące programu Microsoft SQL Server

Muszą być spełnione następujące wymagania związane z programem Microsoft SQL Server:

- Należy zainstalować obsługiwaną wersję programu Microsoft SQL Server. Podczas instalacji wybierz opcję uwierzytelniania **Tryb mieszany**.

- Jeśli program Microsoft SQL Server jest już zainstalowany, ustaw w opcji uwierzytelnienia **Tryb mieszany (Uwierzytelnianie programu SQL Server i Uwierzytelnianie Windows)**. Aby to zrobić, wykonaj działania opisane w tym artykule bazy wiedzy. Jeśli chcesz logować się do programu Microsoft SQL Server przy użyciu **uwierzytelniania systemu Windows**, wykonaj czynności opisane w tym artykule z bazy wiedzy.

- Zezwól na połączenia TCP/IP z programem SQL Server. Aby to zrobić, wykonaj działania opisane w tym artykule bazy wiedzy, rozpoczynając od części **II. Zezwalanie na połączenia TCP/IP z programem SQL Server**.

- Aby można było skonfigurować program Microsoft SQL Server (bazy danych i użytkowników), a także nim zarządzać i administrować, należy pobrać program SQL Server Management Studio (SSMS).
- Nie instaluj programu SQL Server na kontrolerze domeny (np. w przypadku korzystania z systemu Windows SBS/Essentials). Zalecamy zainstalowanie programu ESET PROTECT na innym serwerze lub niezaznaczanie komponentu SQL Server Express podczas instalacji (wymaga to uruchomienia bazy danych ESET PROTECT na istniejącym serwerze SQL lub MySQL).

Instalacja i konfiguracja programu MySQL Server

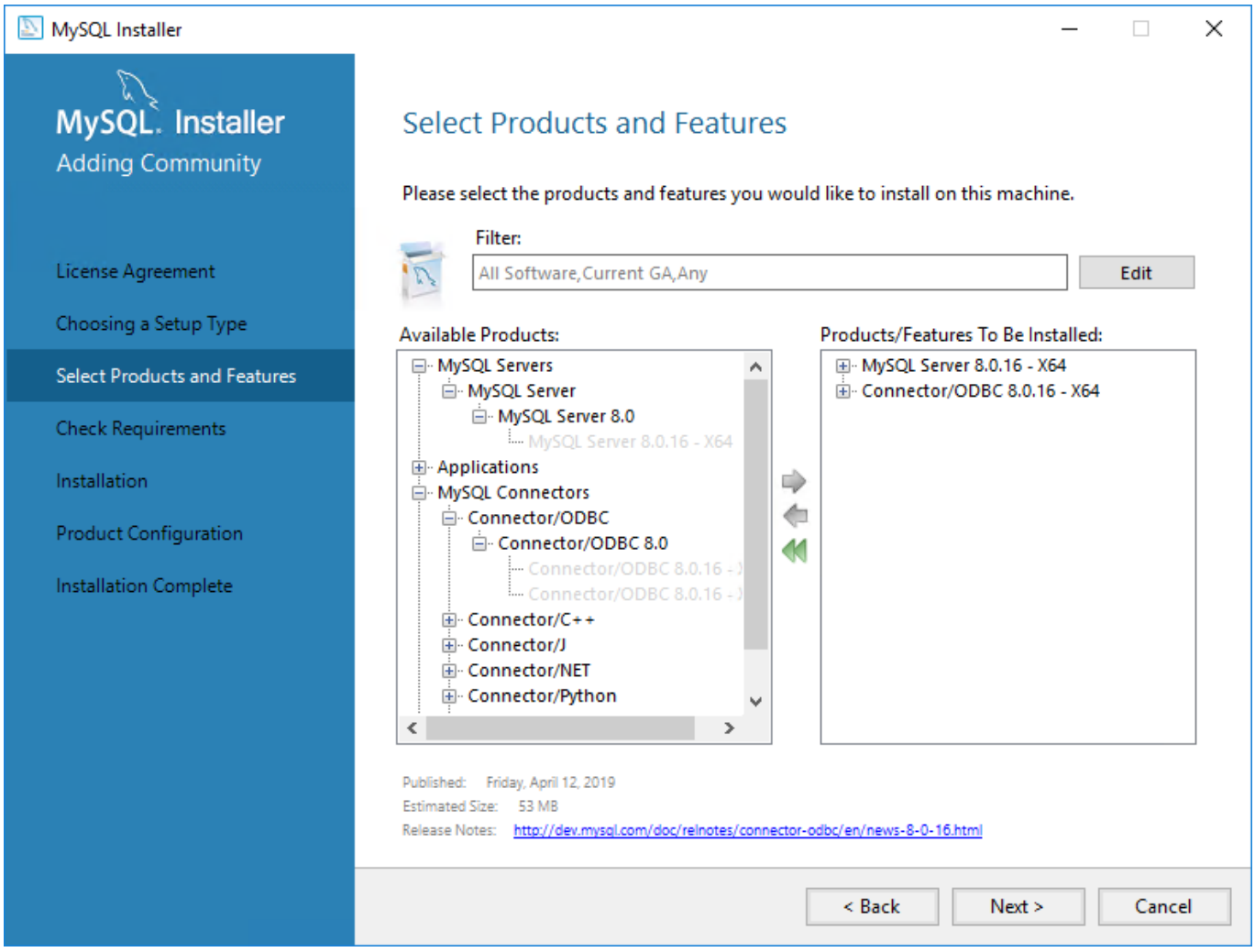
Instalacja

Pamiętaj o zainstalowaniu obsługiwanej wersji programu MySQL Server i łącznika ODBC.

1. Pobierz instalator programu MySQL 8 dla systemu Windows ze strony https://dev.mysql.com/downloads/installer/ i uruchom go.

2. Zaznacz pole wyboru **Akceptuję postanowienia licencyjne** i kliknij **Dalej**.

3. Podczas konfiguracji instalacji wybierz opcję **Niestandardowa**, a następnie wybierz pozycje **MySQL Server** i **Łącznik/ODBC**, aby przeprowadzić instalację. Upewnij się, że architektura łącznika ODBC odpowiada zainstalowanej wersji programu MySQL Server (x86 lub x64).



4. Kliknij przycisk **Dalej**, a następnie **Wykonaj**, aby zainstalować serwer MySQL i łącznik ODBC.

5. Kliknij przycisk **Dalej**. W obszarze **Wysoka dostępność** wybierz opcję **Samodzielny serwer MySQL / Klasyczna replikacja MySQL** i kliknij przycisk **Dalej**.

6. W obszarze **Typ i Sieć** wybierz pozycję **Komputer serwera** z menu rozwijanego **Typ konfiguracji** i kliknij przycisk **Dalej**.

7. W obszarze **Metoda uwierzytelniania** wybierz zalecaną opcję **Użyj silnego szyfrowania hasłem do uwierzytelniania** i kliknij przycisk **Dalej**.

8. W obszarze **Konta i role** wpisz dwukrotnie **hasło główne MySQL**. Zalecamy również utworzenie dedykowanego konta użytkownika bazy danych.

9. W obszarze **Usługa systemu Windows** zachowaj wstępnie wybrane wartości i kliknij przycisk **Dalej**.

10. Kliknij przycisk **Uruchom** i poczekaj, aż instalacja serwera MySQL zostanie zakończona. Kliknij kolejno **Zakończ**, **Dalej** i **Zakończ**, aby zamknąć okno instalacji.

Konfiguracja

1. Otwórz następujący plik w edytorze tekstowym:

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. Znajdź poniższą konfigurację w sekcji `[mysqld]` pliku *my.ini* lub dodaj ją do tego pliku:

- Utwórz sekcję `[mysqld]`, jeśli nie ma jej w pliku.
- Jeśli danych parametrów nie ma w pliku, dodaj je w części `[mysqld]`.
- Aby określić wersję MySQL, uruchom polecenie: `mysql --version`

Parametr	Komentarze i zalecane wartości	MySQL wersja
`max_allowed_packet=33M`		Wszystkie obsługiwane wersje.
`log_bin_trust_function_creators=1`	Inną opcją jest wyłączenie rejestrowania binarnego: `log_bin=0`	Obsługiwane wersje 8.x
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	Mnożnik wartości tych dwóch parametrów musi wynosić co najmniej **200**. Minimalna wartość elementu `innodb_log_files_in_group` to **2** a wartość maksymalna to **100**; przy czym musi to też być liczba całkowita).	Obsługiwane wersje 8x 5.7 5.6.22 (i późniejsze 5.6.x)
`innodb_log_file_size=200M`	Ustaw wartość na co najmniej **200M**, ale nie więcej niż **3000M**.	5.6.20 i 5.6.21

3. Zapisz i zamknij plik *my.ini*.

4. Otwórz wiersz polecenia i wprowadź następujące polecenia, aby uruchomić ponownie serwer MySQL i zastosować konfigurację (nazwa procesu zależy od wersji programu MySQL — wersja 8.0 to mysql80 itd.):

```
net stop mysql80
net start mysql80
```

5. Wpisz następujące polecenie w wierszu polecenia, aby sprawdzić, czy serwer MySQL działa:

```
sc query mysql80
```

Dedykowane konto użytkownika bazy danych

Jeśli ma nie być używane **konto SA** (MS SQL) lub **konto użytkownika root** (MySQL), można utworzyć **dedykowane konto użytkownika bazy danych**. Dedykowane konto użytkownika jest używane tylko do uzyskiwania dostępu do bazy danych ESET PROTECT. Zalecamy utworzenie dedykowanego konta użytkownika bazy danych na serwerze bazy danych przed rozpoczęciem instalacji programu ESET PROTECT. Przy użyciu tego konta konieczne jest też utworzenie pustej bazy danych programu ESET PROTECT.

Istnieje minimalny zestaw uprawnień, które należy przydzielić dedykowanemu kontu użytkownika bazy danych:

- MySQL — uprawnienia użytkownika: `ALTER`, `ALTER ROUTINE`, `CREATE`, `CREATE ROUTINE`, `CREATE TEMPORARY TABLES`, `CREATE VIEW`, `DELETE`, `DROP`, `EXECUTE`, `INDEX`, `INSERT`, `LOCK TABLES`, `SELECT`, `UPDATE`, `TRIGGER`. — więcej informacji na temat uprawnień MySQL można znaleźć pod adresem http://dev.mysql.com/doc/refman/8.0/en/grant.html.

- Microsoft SQL Server — role na poziomie bazy danych: Użytkownik bazy danych ESET PROTECT musi być członkiem roli bazy danych db_owner. Więcej informacji na temat ról na poziomie bazy danych programu Microsoft SQL Server zawiera artykuł https://msdn.microsoft.com/en-us/library/ms189121%28v=sql.100%29.aspx

Szczegółowy przewodnik dotyczący konfigurowania bazy danych i konta użytkownika serwerów MS SQL i MySQL znajduje się w naszym artykule bazy wiedzy.

Instalacja agenta — Windows

Dostępne metody

W przypadku instalacji agenta ESET Management na stacjach roboczych z systemem Windows dostępne są różne metody instalacji i wdrażania:

Metoda	Dokumentacja	Opis
Instalacja z użyciem graficznego interfejsu użytkownika (GUI) z instalatora *.msi*	• Ten rozdział • KB	• **Standardowa** metoda instalacji. • W ramach tej metody można wybrać opcję instalacji serwerowej lub offline. • Ta metoda pozwala zainstalować agenta na serwerze ESET PROTECT.
ESET Remote Deployment Tool	• Pomoc online	• Zalecana w przypadku masowych wdrożeń w sieci lokalnej. • Można jej użyć do wdrożenia instalatora kompleksowego (agent + produkt zabezpieczający ESET)
Kompleksowy instalator agenta	• Tworzenie kompleksowego instalatora agenta • KB	• Instalator może też obejmować produkt zabezpieczający i osadzoną politykę. • Rozmiar instalatora wynosi kilkaset MB.
Skrypt instalacyjny agenta	• Tworzenie instalatora skryptu agenta • KB	• Instalator to skrypt wykonywalny. Jest niewielki, ale wymaga dostępu do lokalizacji instalatora *.msi*. • Skrypt można zmodyfikować, tak aby wskazywał na instalator lokalny i serwer proxy HTTP.

Metoda	Dokumentacja	Opis
Wdrażanie za pomocą skryptu SCCM i GPO	• SCCM • GPO • KB	• Zaawansowana metoda do zdalnych wdrożeń masowych. • Korzysta z niewielkiego pliku *.ini*.
Zadanie serwera — Wdrażanie agenta	• Pomoc online • KB	• Metoda alternatywna względem skryptu SCCM i GPO. • Nie można z niej korzystać za pośrednictwem serwera proxy HTTP. • Wykonywana przez serwer ESET PROTECT z poziomu konsoli internetowej ESET PROTECT.

Protokół komunikacji między agentem a serwerem ESET PROTECT nie obsługuje uwierzytelniania. Żadne rozwiązanie proxy używane do przekazywania komunikacji agenta na serwer ESET PROTECT i wymagające uwierzytelniania nie będzie działać.
Jeśli port domyślny używany dla konsoli internetowej lub agenta zostanie zmieniony, może być konieczna korekta ustawień zapory. W przeciwnym razie instalacja może się nie powieść.

Instalacja z użyciem graficznego interfejsu użytkownika (GUI)

Należy wykonać poniższe czynności, aby zainstalować komponent agenta ESET Management lokalnie w systemie Windows:

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (*agent_x86.msi* lub *agent_x64.msi*lub *agent_arm64.msi*).

2. Uruchom instalatora agenta ESET Management i zaakceptuj umowę EULA, jeśli zgadzasz się z jej postanowieniami.

3. Jeśli nie zgadzasz się na przesyłanie firmie ESET raportów o awariach i anonimowych danych telemetrycznych (takich jak rodzaj i wersja systemu operacyjnego, wersja produktu ESET i inne informacje dotyczące konkretnego produktu), usuń zaznaczenie pola wyboru **Weź udział w programie ulepszania produktu**. W przypadku niezaznaczenia tego pola wyboru dane telemetryczne i raporty o awariach będą przesyłane firmie ESET.

4. Wprowadź dane w polach **Host serwera** (nazwę hosta lub adres IP serwera ESET PROTECT) i **Port serwera** (port domyślny to 2222 — jeśli używasz innego portu, zastąp go niestandardowym numerem portu).

Należy się upewnić, że **host serwera** odpowiada co najmniej jednej z wartości (najlepiej, by to była wartość FQDN) zdefiniowanych w polu **Host certyfikatu serwera**. W przeciwnym razie zostanie wyświetlony błąd „Odebrany certyfikat serwera nie jest prawidłowy”. Użycie symbolu wieloznacznego (*) w polu Host certyfikatu serwera sprawi, że certyfikat będzie działał z dowolnym **hostem serwera**.

5. Jeśli komunikacja między agentem a serwerem odbywa się za pośrednictwem serwera proxy, zaznacz pole wyboru obok pozycji **Użyj serwera proxy**. Po wybraniu tego pola instalator będzie kontynuował instalację offline.

To ustawienie serwera proxy jest używane wyłącznie w celu replikacji między agentem ESET Management a serwerem ESET PROTECT, a nie do buforowania aktualizacji.
- **Nazwa hosta serwera proxy**: nazwa hosta lub adres IP komputera z serwerem proxy HTTP.
- **Port serwera**: wartość domyślna to 3128.
- **Nazwa użytkownika**, **hasło**: należy wprowadzić poświadczenia powiązane z serwerem proxy, jeśli korzysta on z funkcji uwierzytelniania.

Ustawienia serwera proxy można zmienić na późniejszym etapie w polityce. Serwer proxy musi być zainstalowany przed konfiguracją połączenia między agentem a serwerem za pośrednictwem serwera proxy.

6. Wybierz jedną z następujących opcji instalacji i wykonaj działania opisane w odpowiedniej części poniżej:

- Wspomagana instalacja serwerowa — będzie wymagane wprowadzenie poświadczeń administratora konsoli internetowej ESET PROTECT. Instalator automatycznie pobierze wymagane certyfikaty.

Nie można używać użytkownika z uwierzytelnianiem dwuskładnikowym w instalacjach wspomaganych przez serwer.

- Instalacja offline— będzie wymagane wprowadzenie certyfikatu agenta i urzędu certyfikacji. Oba elementy można wyeksportować z programu ESET PROTECT. Można też użyć certyfikatu niestandardowego.

Instalacja z wiersza polecenia

Instalator *MSI* można uruchomić lokalnie lub zdalnie. Pobierz agenta ESET Management z witryny internetowej firmy ESET.

Parametr	Opis i dozwolone wartości
P_HOSTNAME=	Nazwa hosta lub adres IP serwera ESET PROTECT.
P_PORT=	Port serwera na potrzeby połączenia z agentem (opcjonalny; jeśli go nie podasz, domyślnie zostanie użyty port 2222).
P_CERT_PATH=	Ścieżka do certyfikatu agenta w formacie Base64 w pliku *.txt* (wyeksportowanym z konsoli internetowej ESET PROTECT).
P_CERT_AUTH_PATH=	Ścieżka do urzędu certyfikacji w formacie Base64 w pliku *.txt* (wyeksportowanym z konsoli internetowej ESET PROTECT).
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**. Tego parametru należy używać w przypadku odwołań do certyfikatu agenta i urzędu certyfikacji w plikach *.txt*.
P_CERT_PASSWORD=	Za pomocą tego parametru można przekazać hasło na potrzeby certyfikatu agenta.
P_CERT_CONTENT=	Ciąg certyfikatu agenta w formacie Base64 (wyeksportowany z konsoli internetowej ESET PROTECT).
P_CERT_AUTH_CONTENT=	Ciąg urzędu certyfikacji w formacie Base64 (wyeksportowany z konsoli internetowej ESET PROTECT).
PASSWORD=	Hasło do dezinstalacji agenta chronionego hasłem.
P_ENABLE_TELEMETRY=	**0** — wyłączone (opcja domyślna); **1** — włączone. Wysyłanie raportów o awariach i danych telemetrycznych do firmy ESET (parametr opcjonalny).

Parametr	Opis i dozwolone wartości
P_INSTALL_MODE_EULA_ONLY=	**1**. Ten parametr pozwala przeprowadzić częściowo cichą instalację agenta ESET Management. Pojawi się okno instalacji agenta i prośba o zaakceptowanie Umowy licencyjnej użytkownika końcowego oraz włączenie/wyłączenie telemetrii (jeśli podano parametr P_ENABLE_TELEMETRY, zostanie on zignorowany). Pozostałe ustawienia instalacji agenta zostaną pobrane z parametrów wiersza polecenia. Następnie pojawi się komunikat o ukończeniu procesu instalacji agenta.
P_USE_PROXY=	**1**. Ten parametr powoduje włączenie korzystania z serwera proxy HTTP (który jest już zainstalowany w sieci) na potrzeby replikacji między agentem ESET Management a serwerem ESET PROTECT (nie dotyczy buforowania aktualizacji).
P_PROXY_HTTP_HOSTNAME=	Nazwa hosta lub adres IP serwera proxy HTTP.
P_PROXY_HTTP_PORT=	Port serwera proxy HTTP do nawiązywania połączenia z agentem.

Przykłady instalacji z wiersza polecenia

Pomarańczowe fragmenty kodu należy zastąpić odpowiednimi wartościami.

- Instalacja cicha (parametr `/q`) z połączeniem z portem domyślnym, włączoną telemetrią i certyfikatem agenta oraz urzędem certyfikacji zapisanymi w plikach:

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Użytkownicy\Administrator\Pulpit\certyfikat.txt P_CERT_AUTH_PATH=C:\Użytkownicy\Administrator\Pulpit\uc.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- Instalacja cicha z podanymi ciągami certyfikatu agenta i urzędu certyfikacji oraz parametrami hasła do certyfikatu agenta i serwera proxy HTTP:

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvkpqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_HTTP_PORT=3128
```

- Instalacja częściowo cicha:

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Użytkownicy\Administrator\Pulpit\certyfikat.txt P_CERT_AUTH_PATH=C:\Użytkownicy\Administrator\Pulpit\uc.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

Wspomagana instalacja serwerowa agenta

Aby kontynuować **wspomaganą instalację serwerową agenta**, należy postępować zgodnie z poniższymi instrukcjami:

1. W polu **Host serwera** wpisz nazwę hosta lub adres IP konsoli internetowej ESET PROTECT (taki sam jak serwera ESET PROTECT). Jeśli nie jest używany niestandardowy port, w polu **Port konsoli internetowej** pozostaw port domyślny, czyli 2223. W polach **Nazwa użytkownika i Hasło wpisz poświadczenia konta konsoli internetowej**. Aby zalogować się jako użytkownik domeny, zaznacz pole wyboru obok pozycji **Zaloguj się do domeny**.

- należy się upewnić, że **host serwera** odpowiada co najmniej jednej z wartości (najlepiej, aby to była wartość FQDN) zdefiniowanych w polu **Host certyfikatu serwera**. W przeciwnym razie zostanie wyświetlony błąd „Odebrany certyfikat serwera nie jest prawidłowy”. Jedynym wyjątkiem jest symbol wieloznaczny (*) znajdujący się w polu Host certyfikatu serwera. Symbol ten oznacza, że można użyć dowolnego **hosta serwera**.
- Nie można używać użytkownika z uwierzytelnianiem dwuskładnikowym w instalacjach wspomaganych przez serwer.

2. Po wyświetleniu monitu o zaakceptowanie certyfikatu kliknij opcję **Tak**.

3. Wybierz opcję **Nie twórz komputera (komputer zostanie utworzony automatycznie przy pierwszym połączeniu)** lub **Wybierz niestandardową grupę statyczną**. Kliknięcie opcji **Wybierz niestandardową grupę statyczną** umożliwi wybranie pozycji z listy grup statycznych istniejących na serwerze ESET PROTECT. Komputer zostanie dodany do wybranej grupy.

4. Określ folder docelowy dla agenta ESET Management (zalecamy użycie domyślnej lokalizacji), kliknij przycisk **Dalej** i następnie przycisk **Zainstaluj**.

Instalacja offline agenta

Aby kontynuować **instalację offline agenta**, należy postępować zgodnie z poniższymi instrukcjami:

1. Jeśli w poprzednim kroku wybrano opcję **Użyj serwera proxy**, podaj **nazwę hosta serwera proxy**, **port serwera proxy** (port domyślny to 3128), **nazwę użytkownika** i **hasło**, a następnie kliknij przycisk **Dalej**.

2. Kliknij przycisk **Przeglądaj** i przejdź do lokalizacji certyfikatu równorzędnego (jest to certyfikat agenta wyeksportowany z programu ESET PROTECT). Pole tekstowe **Hasło do certyfikatu** pozostaw puste, ponieważ ten certyfikat nie wymaga podawania hasła. Nie musisz wybierać wartości pola **Urząd certyfikacji** — pozostaw to pole puste.

Jeśli w programie ESET PROTECT jest używany certyfikat niestandardowy (zamiast certyfikatów domyślnych wygenerowanych automatycznie podczas instalacji programu ESET PROTECT), należy wskazać odpowiednie certyfikaty niestandardowe.

Hasło do certyfikatu nie może zawierać następujących znaków: " \ Znaki te powodują błąd krytyczny podczas inicjowania agenta.

3. Kliknij przycisk **Dalej**, aby zainstalować w folderze domyślnym, lub przycisk **Zmień**, aby wybrać inny folder (zalecamy użycie folderu domyślnego).

ESET Remote Deployment Tool

Narzędzie do wdrażania ESET Remote Deployment Tool to wygodny sposób dystrybucji pakietu instalatora stworzone przez ESET PROTECT na potrzeby zdalnego wdrażania agenta ESET Management oraz produktów zabezpieczających firmy ESET na komputerach za pośrednictwem sieci.

Narzędzie Remote Deployment Tool firmy ESET można pobrać bezpłatnie z witryny internetowej firmy ESET jako autonomiczny komponent oprogramowania ESET PROTECT. Narzędzie do wdrażania jest przeznaczone do użycia w małych oraz średnich sieciach i jest uruchamiane przy użyciu uprawnień administratora.

Narzędzie do wdrażania zdalnego firmy ESET jest przeznaczone do wdrażania agentów ESET Management wyłącznie na komputerach klienckich z obsługiwanymi systemami operacyjnymi Microsoft Windows.

Aby uzyskać więcej informacji na temat wymagań wstępnych i użytkowania narzędzia, należy zapoznać się z rozdziałem Narzędzie do wdrażania ESET Remote Deployment Tool.

Instalacja konsoli internetowej — Windows

Konsolę internetową ESET PROTECT w systemie Windows można zainstalować na dwa sposoby:

- Zalecane jest użycie instalatora kompleksowego
- Zaawansowani użytkownicy mogą przeprowadzać instalację ręczną

Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT.

Instalacja konsoli internetowej przy użyciu instalatora kompleksowego

Wymagania wstępne

- Zainstalowany serwer ESET PROTECT.

Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT. Ta procedura wymaga podjęcia dodatkowych kroków.

- Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT.
- Apache Tomcat wymaga 64-bitowego Java/OpenJDK. Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

Instalacja

Aby zainstalować składnik konsoli internetowej ESET PROTECT w systemie Windows przy użyciu instalatora kompleksowego:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Pobierz Instalator kompleksowy ESET PROTECT ze strony internetowej firmy ESET i rozpakuj pobrany plik.

2. Jeśli chcesz zainstalować najnowszą wersję serwera Apache Tomcat, a instalator kompleksowy zawiera starszą wersję Apache Tomcat (ten krok jest opcjonalny – jeśli nie potrzebujesz najnowszej wersji Apache Tomcat, przejdź do kroku 4):

   a. Otwórz folder *x64* i przejdź do folderu *installers*.

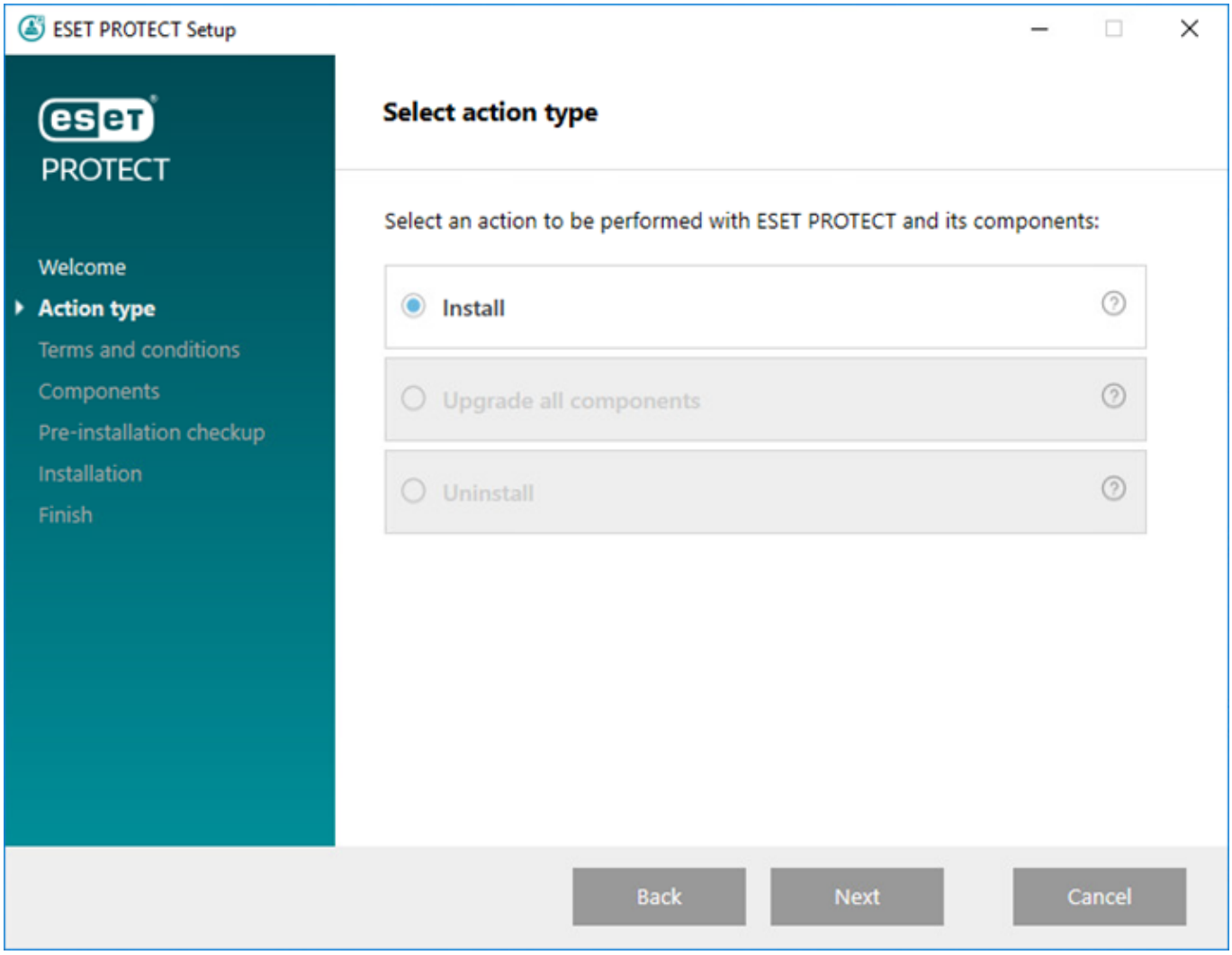
   b. Usuń plik *apache-tomcat-9.0.x-windows-x64.zip* znajdujący się w folderze *installers*.

   c. Pobierz pakiet zip Apache Tomcat 9 dla 64-bitowego systemu Windows.

   d. Przenieś pobrany pakiet zip do folderu *installers*.

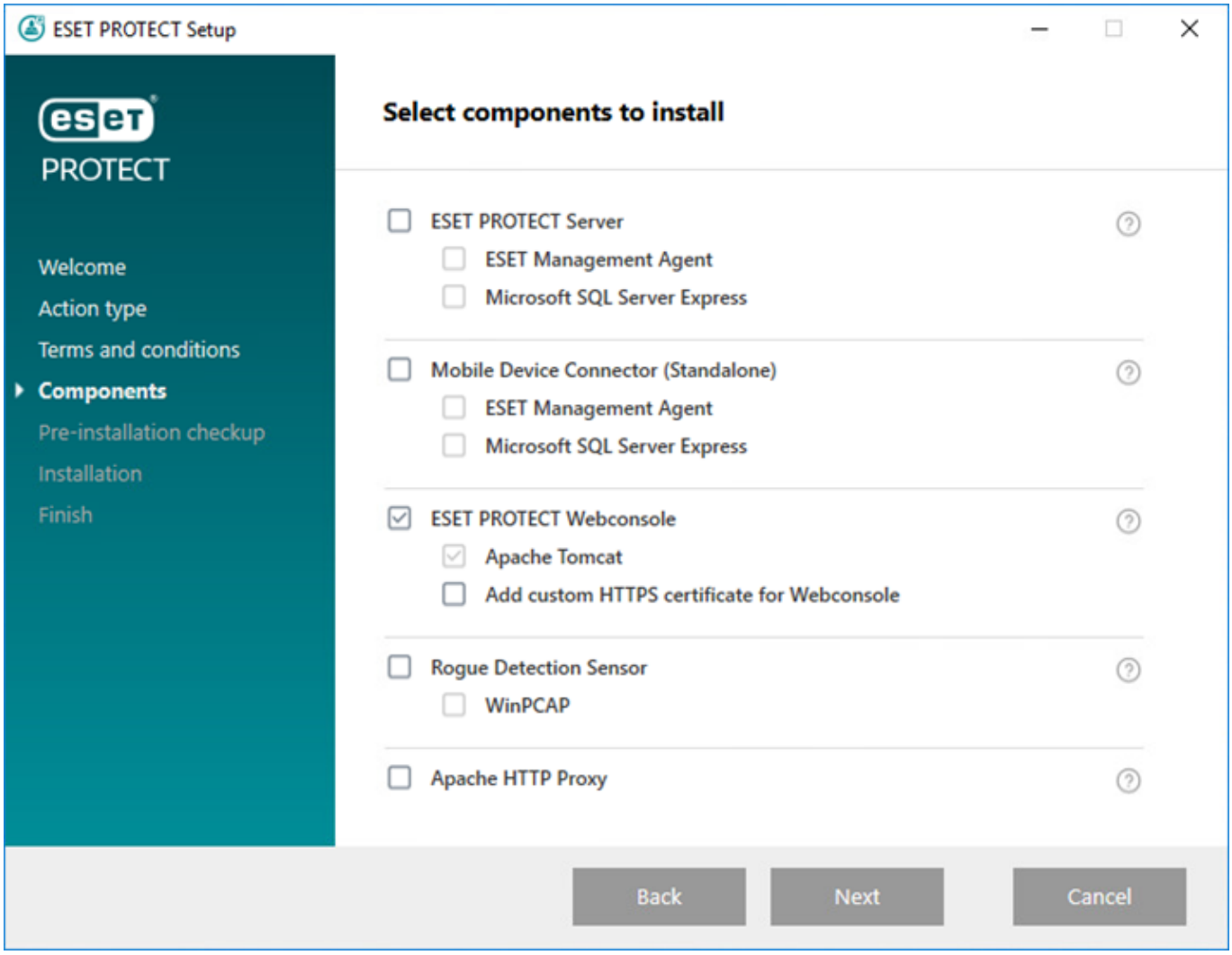
3. Uruchom kompleksowy instalator, klikając dwukrotnie plik *Setup.exe*. Kliknij przycisk **Dalej** na **ekranie powitalnym**.

4. Wybierz opcję **Zainstaluj** i kliknij przycisk **Dalej**.



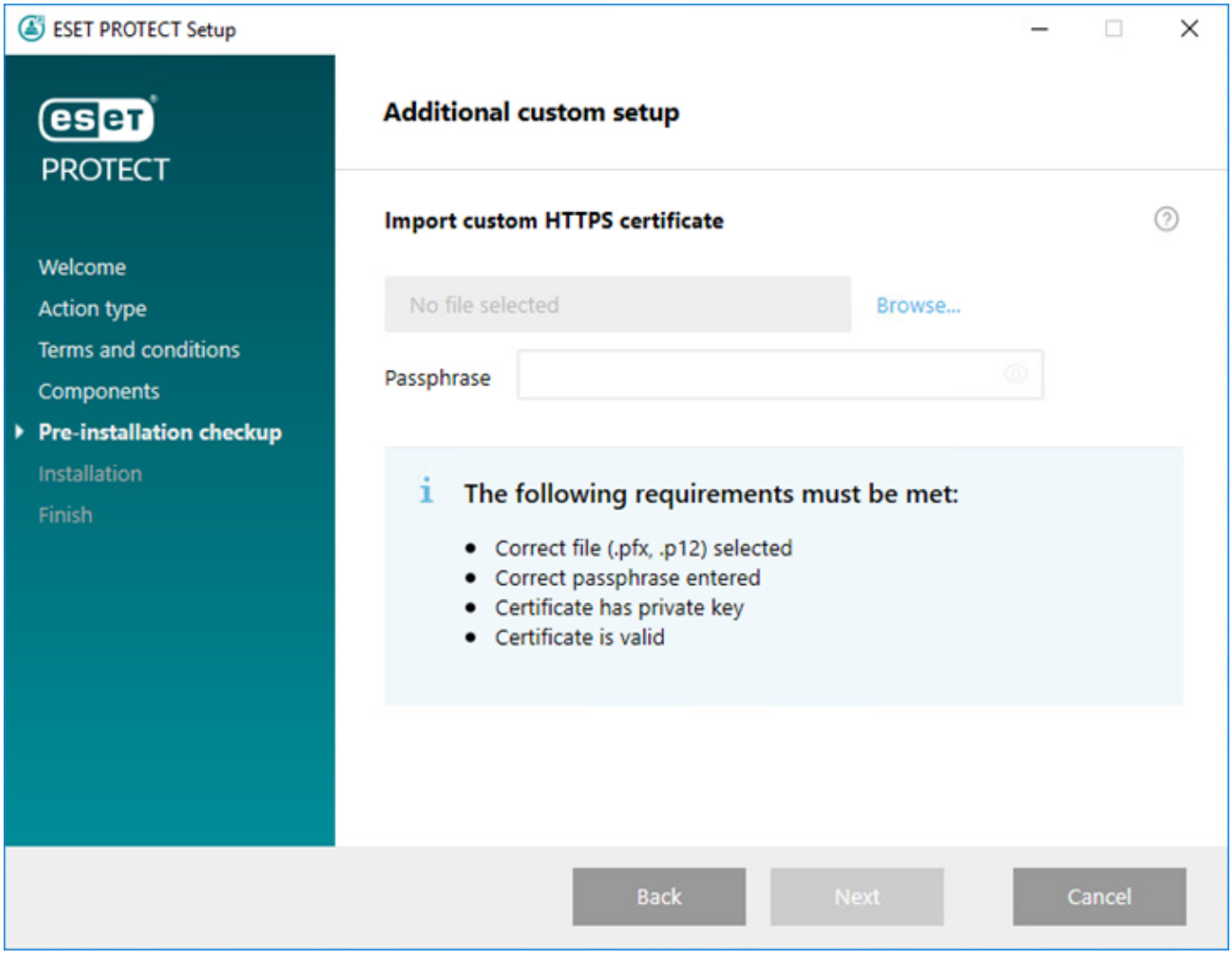
5. Po zaakceptowaniu umowy EULA kliknij opcję **Dalej**.

6. W polu **Wybierz komponenty do zainstalowania** zaznacz tylko pole wyboru **Konsola internetowa ESET PROTECT** i kliknij przycisk **Dalej**.



Opcjonalnie zaznacz pole wyboru **Dodaj niestandardowy certyfikat HTTPS dla konsoli internetowej**.

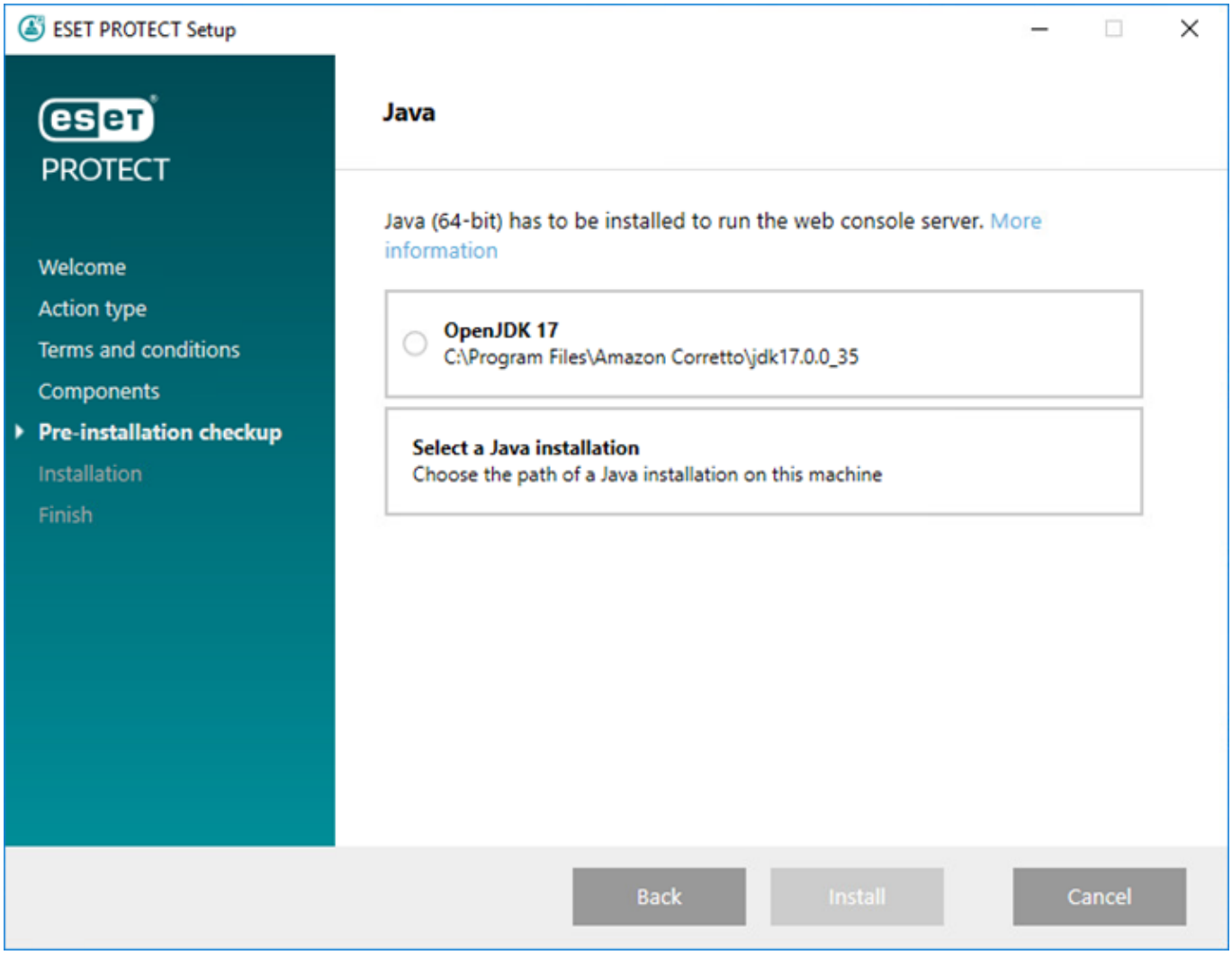
- Zaznacz tę opcję, jeśli chcesz użyć niestandardowego certyfikatu HTTPS dla konsoli internetowej ESET PROTECT.
- Jeśli ta opcja nie zostanie zaznaczona, instalator automatycznie wygeneruje nowy magazyn kluczy dla serwera Tomcat (samodzielnie podpisany certyfikat HTTPS).
- W przypadku wybrania opcji **Dodaj niestandardowy certyfikat HTTPS dla konsoli internetowej** kliknij **Przeglądaj** i wybierz ważny certyfikat (plik *.pfx* lub .p12 file), a w polu **Hasło** wpisz hasło do niego (lub pozostaw to pole puste, jeśli nie ustawiono hasła). Instalator zainstaluje certyfikat dostępu do konsoli internetowej na serwerze Tomcat. Kliknij przycisk **Dalej**, aby kontynuować.



7. Wybierz instalację środowiska Java na komputerze. Sprawdź, czy używasz najnowszej wersji programu Java/OpenJDK.

a)Aby wybrać już zainstalowane środowisko Java, kliknij opcję **Wybierz instalację środowiska Java**, wybierz folder, w którym jest zainstalowane środowisko Java (z podfolderem *bin*, np. *C:\Program Files\Amazon Corretto\jdk1.8.0_212*) i kliknij przycisk **OK**. Pojawi się pytanie, czy została wybrana nieprawidłowa ścieżka.

b)Kliknij przycisk **Zainstaluj**, aby kontynuować, lub **Zmień**, aby zmienić ścieżkę instalacji środowiska Java.



8. Po zakończeniu instalacji kliknij przycisk **Zakończ**.

Jeśli konsola internetowa ESET PROTECT została zainstalowana na innym komputerze niż ten, na którym znajduje się serwer ESET PROTECT, postępuj zgodnie z poniższymi dodatkowymi instrukcjami w celu włączenia komunikacji między konsolą internetową ESET PROTECT a serwerem ESET PROTECT:
a)Zatrzymaj usługę Apache Tomcat: Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Zatrzymaj**.
b)Uruchom aplikację Notatnik jako administrator i edytuj plik *C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Znajdź ciąg `server_address=localhost`.
d)Część `localhost` zastąp adresem IP serwera ESET PROTECT i zapisz plik.
e) Uruchom usługę Apache Tomcat. Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Uruchom**.

9. Otwórz konsolę internetową ESET PROTECT w obsługiwanej przeglądarce internetowej; zostanie wyświetlony ekran logowania.

- Z komputera obsługującego konsolę internetową ESET PROTECT: *https://localhost/era*

- Z dowolnego komputera z dostępem do internetu i konsoli internetowej ESET PROTECT (zastąp *IP_ADDRESS_OR_HOSTNAME* adresem IP lub nazwą hosta konsoli ESET PROTECT): *https://IP_ADDRESS_OR_HOSTNAME/era*

Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Ręczne instalowanie konsoli internetowej

Ręczna instalacja konsoli internetowej ESET PROTECT jest zaawansowaną procedurą. Zaleca się zainstalowanie konsoli internetowej ESET PROTECT przy użyciu instalatora kompleksowego.

Wymagania wstępne

- Zainstalowany serwer ESET PROTECT.

Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT. Ta procedura wymaga podjęcia dodatkowych kroków.

- Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT. Zainstaluj Apache Tomcat:

  a)Pobierz najnowszą obsługiwaną wersję pliku instalatora Apache Tomcat (32-bitowy/64-bitowy instalator usługi systemu Windows) *apache-tomcat-[wersja].exe* z witryny https://tomcat.apache.org.

  a)Uruchom instalator.

  b)Podczas instalacji wybierz ścieżkę do folderu Java (folder nadrzędny folderów Java *bin* i *lib*) i zaznacz pole wyboru **Run Apache Tomcat**.

  c)Po zakończeniu instalacji sprawdź, czy usługa Apache Tomcat jest uruchomiona, a jej typ uruchamiania jest ustawiony na **Automatyczny** (w narzędziu **services.msc**).

- Apache Tomcat wymaga 64-bitowego Java/OpenJDK. Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

Instalacja

Aby zainstalować komponent konsoli internetowej ESET PROTECT w systemie Windows, należy wykonać poniższe czynności:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (Konsola internetowa*era.war*).

2. Skopiuj plik *era.war* do folderu aplikacji sieciowych serwera Apache Tomcat:

C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps

3. Apache Tomcat automatycznie wyodrębnia plik *era.war* do folderu *era* i instaluje konsolę internetową ESET PROTECT. Poczekaj kilka minut na zakończenie wyodrębniania. Jeśli wyodrębnianie nie nastąpi, wykonaj działania zmierzające do rozwiązania problemu.

4. Jeśli na tym samym komputerze co serwer ESET PROTECT jest zainstalowana konsola internetowa ESET PROTECT, uruchom ponownie usługę Apache Tomcat. Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Zatrzymaj**. Kliknij pozycję Stop, poczekaj 30 sekund, a następnie kliknij pozycję **Start**.

Jeśli konsola internetowa ESET PROTECT została zainstalowana na innym komputerze niż ten, na którym znajduje się serwer ESET PROTECT, postępuj zgodnie z poniższymi dodatkowymi instrukcjami w celu włączenia komunikacji między konsolą internetową ESET PROTECT a serwerem ESET PROTECT:
a)Zatrzymaj usługę Apache Tomcat: Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Zatrzymaj**.
b)Uruchom aplikację Notatnik jako administrator i edytuj plik *C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)Znajdź ciąg `server_address=localhost`.
d)Część `localhost` zastąp adresem IP serwera ESET PROTECT i zapisz plik.
e) Uruchom usługę Apache Tomcat. Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Uruchom**.

5. Otwórz konsolę internetową ESET PROTECT w obsługiwanej przeglądarce internetowej, aby wyświetlić ekran logowania:

- Z komputera obsługującego konsolę internetową ESET PROTECT: *http://localhost:8080/era*
- Z dowolnego komputera z dostępem do internetu i konsoli internetowej ESET PROTECT (zastąp *IP_ADDRESS_OR_HOSTNAME* adresem IP lub nazwą hosta konsoli ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. Skonfiguruj konsolę internetową po instalacji:

- Domyślną wartością portu HTTP podczas ręcznej instalacji serwera Apache Tomcat jest 8080. Zalecamy skonfigurowanie połączenia HTTPS dla serwera Apache Tomcat.
- Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Instalacja serwera proxy HTTP

Serwer proxy HTTP — informacje

Serwer proxy HTTP przesyła dalej zaszyfrowaną komunikację między agentem ESET Management a serwerem ESET PROTECT. Domyślnie program ESET PROTECT jako serwera proxy HTTP używa serwera proxy Apache HTTP.

Serwera proxy HTTP należy używać tylko w przypadku braku widoczności sieciowej między agentami ESET Management a serwerem ESET PROTECT. Serwer proxy HTTP nie agreguje komunikacji ani nie zmniejsza ruchu sieciowego.

Zalecane jest zainstalowanie agenta ESET Management na komputerze z serwerem proxy HTTP, ale nie jest to wymagane. Agent ESET Management nie może zarządzać aplikacją Serwer proxy HTTP (czyli jej konfigurować).

- Architektura serwera proxy HTTP
- Architektura serwera proxy Apache HTTP
- Zaawansowane scenariusze dotyczące serwera proxy HTTP

Przed instalacją

Protokół komunikacji między agentem a serwerem ESET PROTECT nie obsługuje uwierzytelniania. Żadne rozwiązanie proxy używane do przekazywania komunikacji agenta na serwer ESET PROTECT i wymagające uwierzytelniania nie będzie działać.
Jeśli port domyślny używany dla konsoli internetowej lub agenta zostanie zmieniony, może być konieczna korekta ustawień zapory. W przeciwnym razie instalacja może się nie powieść.

Instalacja i konfiguracja

Serwer proxy Apache HTTP można zainstalować za pomocą osobnego instalatora lub instalatora kompleksowego ESET PROTECT.

- Instalacja za pomocą instalatora kompleksowego wymaga pobrania całego pakietu, ale jest prostsza. Należy uruchomić pobrany instalator i wybrać tylko opcję instalacji **Serwer proxy Apache HTTP**. Po zainstalowaniu serwera Apache należy go skonfigurować.

- Instalacja za pomocą instalatora autonomicznego jest bardziej złożona, ale wymaga pobrania tylko kilku MB danych. Zapoznaj się z instrukcjami dotyczącymi instalacji i konfiguracji.

Konfigurowanie serwera proxy HTTP dla dużej liczby klientów

Jeśli używasz 64-bitowego serwera proxy Apache HTTP, możesz zwiększyć limit wątków swojego serwera Apache HTTP Proxy. Edytuj plik konfiguracyjny *httpd.conf* w folderze Apache HTTP Proxy. Znajdź następujące ustawienia w pliku i zaktualizuj wartości, aby dopasować je do liczby klientów.

Zamień przykładową wartość `5000` potrzebną liczbą. Maksymalna wartość to `32000`.

```
ThreadLimit 5000

ThreadsPerChild 5000
```

Nie zmieniaj pozostałej części pliku.

Instalacja narzędzia RD Sensor — Windows

Wymagania wstępne

- WinPcap — należy użyć najnowszej wersji programu WinPcap (co najmniej wersji 4.1.0)
- Sieć powinna być poprawnie skonfigurowana (odpowiednie porty otwarte, komunikacja przychodząca nie

jest blokowana przez zaporę sieciową itp.)

- Serwer ESET PROTECT jest osiągalny
- Agent ESET Management musi być zainstalowany na komputerze lokalnym, aby wszystkie funkcje programu były w pełni obsługiwane.
- Plik dziennika Rogue Detection Sensor można znaleźć tutaj: *C:\ProgramData\ESET\Rouge Detection Sensor\Logs*

Instalacja

Aby zainstalować komponent narzędzia RD Sensor w systemie Windows, należy wykonać poniższe czynności:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (*rdsensor_x86.msi* lub *rdsensor_x64.msi*).

2. Aby rozpocząć instalację, dwukrotnie kliknij plik instalacyjny narzędzia RD Sensor.

3. Zaakceptuj umowę EULA i kliknij przycisk **Dalej**.

4. Jeśli nie zgadzasz się na przesyłanie firmie ESET raportów o awariach i anonimowych danych telemetrycznych (takich jak rodzaj i wersja systemu operacyjnego, wersja produktu ESET i inne informacje dotyczące konkretnego produktu), usuń zaznaczenie pola wyboru **Weź udział w programie ulepszania produktu**. W przypadku niezaznaczenia tego pola wyboru dane telemetryczne i raporty o awariach będą przesyłane firmie ESET.

5. Wybierz lokalizację instalacji narzędzia RD Sensor i kliknij przycisk **Dalej** > **Instaluj**.

Jeśli istnieje wiele segmentów sieci, Rogue Detection Sensor musi być zainstalowany osobno w każdym segmencie sieci, aby uzyskać pełną listę wszystkich urządzeń w całej sieci.

Narzędzie Mirror Tool — system Windows

Czy jesteś użytkownikiem systemu Linux?

Narzędzie Mirror Tool jest potrzebne w przypadku aktualizacji silnika detekcji. Jeśli komputery klienckie nie mają połączenia z Internetem, a trzeba na nich zainstalować aktualizacje silnika detekcji, przy użyciu narzędzia Mirror Tool można pobrać pliki aktualizacji z serwerów aktualizacji firmy ESET, aby przechowywać je lokalnie.

Narzędzie Mirror Tool pobiera tylko aktualizacje silnika detekcji i innych modułów programu. Nie pobiera aktualizacji komponentów programu ani danych systemu ESET LiveGrid®. Tworzy też pełne repozytorium offline. Można też zaktualizować poszczególne produkty.

Wymagania wstępne

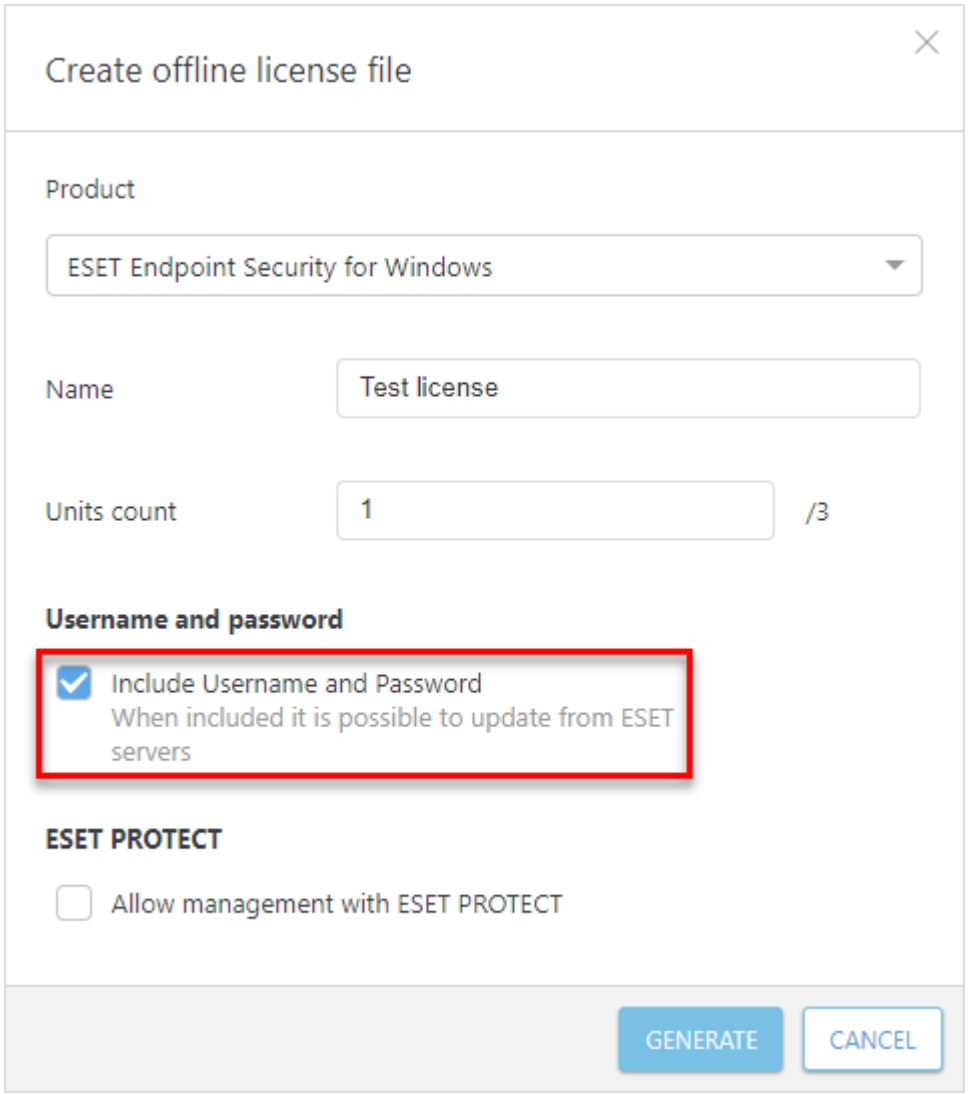
Narzędzie Mirror Tool nie obsługuje systemu Windows XP ani Windows Server 2003.

• Należy udostępnić folder docelowy przy użyciu usługi Samba/Windows lub HTTP/FTP — zależnie od tego jak mają zostać udostępnione aktualizacje.

  oProdukty zabezpieczające ESET dla systemu Windows — można je aktualizować zdalnie za pomocą protokołu HTTP lub folderu udostępnionego.

  oProdukty zabezpieczające ESET dla systemów Linux/macOS — można je aktualizować zdalnie tylko za pomocą protokołu HTTP. W przypadku używania folderu udostępnionego musi on znajdować się na tym samym komputerze co produkt zabezpieczający ESET.

• Potrzebny jest prawidłowy plik licencji offline zawierający nazwę i hasło użytkownika. Podczas generowania pliku licencji należy pamiętać o zaznaczeniu pola wyboru **Uwzględniaj nazwę użytkownika i hasło**. Należy również wprowadzić **nazwę licencji**. Plik licencji offline jest wymagany do aktywacji narzędzia Mirror Tool i wygenerowania kopii dystrybucyjnej aktualizacji.



• Przed uruchomieniem narzędzia Mirror Tool konieczne jest zainstalowanie następujących pakietów:

• Pakiet dystrybucyjny Visual C++ dla Visual Studio 2010

• Pakiet dystrybucyjny Visual C++ 2015 x86

Jak korzystać z narzędzia Mirror Tool

1.Pobierz narzędzie Mirror Tool ze strony pobierania firmy ESET (w sekcji z **instalatorami autonomicznymi**).

2.Rozpakuj pobrane archiwum.

3.Otwórz wiersz polecenia i przejdź do folderu zawierającego plik *MirrorTool.exe*.

4.Uruchom poniższe polecenie, aby wyświetlić wszystkie dostępne parametry narzędzia Mirror Tool i jego wersji:

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. 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. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --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.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Wszystkie filtry uwzględniają wielkość liter.

Parametr	Opis
`--updateServer`	W przypadku jego użycia należy też określić adres URL serwera aktualizacji.
`--offlineLicenseFilename`	Należy określić ścieżkę do pliku licencji offline (zgodnie z powyższymi informacjami).
`--mirrorOnlyLevelUpdates`	Nie wymaga argumentu. Po skonfigurowaniu pobierane będą tylko aktualizacje poziomowe (nanoaktualizacje nie zostaną pobrane). Więcej informacji o typach aktualizacji można przeczytać w naszym artykule bazy wiedzy.
`--mirrorFileFormat`	Przed użyciem parametru `--mirrorFileFormat` upewnij się, że środowisko nie zawiera zarówno starszych (6.5 i starszych), jak i nowszych (6.6. i nowszych) wersji produktów zabezpieczających firmy ESET. Nieprawidłowe użycie tego parametru może spowodować nieprawidłowe aktualizacje produktów zabezpieczających firmy ESET. Można określić, jaki typ plików aktualizacji zostanie pobrany. Możliwe wartości (z uwzględnieniem wielkości liter): • `dat` — użyj tej wartości, jeśli środowisko jest dostępne tylko w produkcie zabezpieczającym ESET w wersji 6.5 lub starszej. • `dll` — użyj tej wartości, jeśli środowisko jest dostępne tylko w produkcie zabezpieczającym ESET w wersji 6.6 lub starszej. Parametr jest ignorowany podczas tworzenia kopii dystrybucyjnych starszych produktów (`ep4` , `ep5`).
`--compatibilityVersion`	Ten opcjonalny parametr dotyczy narzędzia Mirror Tool dystrybuowanego z ESET PROTECT 8.1 i nowszymi wersjami. Narzędzie Mirror Tool pobierze pliki aktualizacji zgodne z wersją repozytorium ESET PROTECT określoną w argumencie parametru w formacie `x.x` lub `x.x.x.x`, na przykład: `--compatibilityVersion 9.1` lub `--compatibilityVersion 8.1.13.0`.

Aby zmniejszyć ilość danych ładowanych z repozytorium ESET, zalecamy użycie nowych parametrów w narzędziu Mirror Tool dystrybuowanym z ESET PROTECT 9: `--filterFilePath` i `--dryRun`:
1.Utwórz filtr w formacie *JSON* (patrz `--filterFilePath` poniżej).
2.Wykonaj próbne uruchomienie narzędzia Mirror Tool, używając parametru `--dryRun` (patrz poniżej) i dostosuj filtr w razie potrzeby.
3.Uruchom narzędzie Mirror Tool z parametrem `--filterFilePath` i zdefiniowanym filtrem pobierania wraz z parametrami `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`.
4.Regularnie uruchamiaj narzędzie Mirror Tool, aby zawsze korzystać z najnowszych instalatorów.

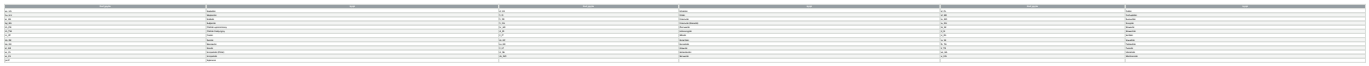
Parametr	Opis

`--filterFilePath`	Użyj tego opcjonalnego parametru, aby filtrować produkty zabezpieczające ESET na podstawie pliku tekstowego w formacie *JSON* umieszczonego w tym samym folderze co Mirror Tool, na przykład: `--filterFilePath filter.txt`)
	Opis konfiguracji filtra:
	Format pliku konfiguracyjnego do filtrowania produktów to *JSON* on następującej strukturze:
	• Obiekt główny *JSON*:
	o`use_legacy` (boolean, opcjonalnie) — jeśli ma wartość true, starsze produkty zostaną uwzględnione.
	o`defaults` (*JSON* obiekt, opcjonalnie) — definiuje właściwości filtra, które będą stosowane do wszystkich produktów.
	■`languages` (lista) — określa kody ISO języków, które mają być uwzględniane, na przykład dla francuskiego wpisz `"fr_FR"`. Pozostałe kody języków znajdują się w poniższej tabeli. Aby wybrać więcej języków, oddziel je przecinkami i spacjami. Na przykład: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista) — platformy do włączenia (`["x64", "x86", "arm64"]`).
	Używaj filta `platforms` ostrożnie. Jeśli na przykład narzędzie Mirror Tool pobierze tylko instalatory 64-bitowe, a w infrastrukturze znajdują się komputery 32-bitowe, 64-bitowe produkty zabezpieczające ESET nie zostaną zainstalowane na komputerach 32-bitowych.
	■`os_types` (lista) — rodzaje systemów operacyjnych do włączenia (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista obiektów JSON, opcjonalnie) — filtry do zastosowania do określonych produktów — nadpisanie wartości `defaults` dla określonych produktów. Obiekty mają następujące właściwości:
	■`app_id` (ciąg znaków) — wymagany, jeśli nie określono `name`.
	■`name` (ciąg znaków) — wymagany, jeśli nie określono `app_id`.
	■`version` (ciąg znaków) — określa wersję lub zakres wersji do uwzględnienia.
	■`languages` (lista) — kody ISO języków, które należy uwzględnić (patrz tabela poniżej).
	■`platforms` (lista) — platformy do włączenia (`["x64", "x86", "arm64"]`).
	■`os_types` (lista) — rodzaje systemów operacyjnych do włączenia (`["windows"]`, `["linux"]`, `["mac"]`).
	Aby określić odpowiednie wartości dla pól, uruchom narzędzie Mirror Tool w trybie suchego przebiegu i znajdź odpowiedni produkt w utworzonym pliku CSV.
	Opisy formatu ciągu znaków określającego wersję
	Wszystkie numery wersji składają się z czterech liczb oddzielonych kropkami (na przykład `7.1.0.0`). Możesz określić mniej liczb podczas wprowadzania filtrów wersji (na przykład `7.1`), a reszta liczb będzie równa zero (`7.1` to to samo, co `7.1.0.0`).
	Ciąg znaków określający wersję może mieć jeden z dwóch następujących formatów:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oWybiera wersje większe/mniejsze lub równe/mniejsze lub równe/równe w stosunku do wskazanej wersji.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oWybiera wersje, które są większe lub równe progowi dolnemu i mniejsze lub równe progowi górnemu.
	Porównania są wykonywane numerycznie na każdej części numeru wersji, od lewej do prawej.
	Przykład JSON
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Parametr `--filterFilePath` zastępuje parametry `--languageFilterForRepository` i `--productFilterForRepository` `--downloadLegacyForRepository` używane w starszych wersjach narzędzia Mirror Tool (wydanych z ESET PROTECT 8.x).

Parametr	Opis
`--dryRun`	Po użyciu tego opcjonalnego parametru narzędzie Mirror Tool nie pobierze żadnych plików, ale wygeneruje plik *.csv* z listą wszystkich pakietów, które zostaną pobrane. Możesz użyć tego parametru bez obowiązkowych parametrów `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`, na przykład: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. ℹ Niektóre instalatory ESET są niezależne od języka (mają kod języka `multilang`), a narzędzie Mirror Tool wyświetli je w pliku *.csv*, nawet jeśli określisz `języki` w parametrze `--filterFilePath`. Jeśli użyjesz parametru `--dryRun`, a także parametrów `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`, narzędzie Mirror Tool nie wyczyści repozytorium *outputRepositoryDirectory*.
`--listUpdatableProducts`	Wyświetla wszystkie produkty ESET, dla których narzędzie Mirror Tool może pobrać aktualizacje modułu (chyba że jest używany parametr `--excludedProducts`). Parametr jest dostępny w wersjach narzędzia Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Struktura folderów tworzona przez narzędzie Mirror Tool różni się od struktury tworzonej w kopii dystrybucyjnej oprogramowania Endpoint. W każdym folderze znajdują się pliki aktualizacji dla grupy produktów. W ustawieniach aktualizacji produktu za pomocą kopii dystrybucyjnej należy podać pełną ścieżkę do prawidłowego folderu.
Na przykład w celu przeprowadzenia aktualizacji oprogramowania ESET PROTECT 9. z kopii dystrybucyjnej jako Serwer aktualizacji (zgodnie z lokalizacją serwera głównego HTTP) należy ustawić:
`http://your_server_address/mirror/eset_upd/era6`
Uwaga: Folder lustrzany `era6` jest wspólny dla tych rozwiązań firmy ESET do zdalnego zarządzania: ERA 6, ESMC 7, ESET PROTECT.

Tabela kodów języków



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

Poniżej znajduje się przykład bardziej zaawansowanej konfiguracji repozytorium offline z wybranymi produktami, językami i włączonym pobieraniem starszych plików zdefiniowanymi w pliku *filter.txt* (przykład zawartości pliku znajduje się powyżej w opisie parametru `--filterFilePath`):

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

Narzędzie Mirror Tool i ustawienia aktualizacji

- Aby zautomatyzować pobieranie aktualizacji modułów, można utworzyć harmonogram uruchamiania narzędzia Mirror Tool. Aby to zrobić, otwórz konsolę internetową i wybierz kolejno opcje **Zadania klienta** > **System operacyjny** > **Uruchom polecenie. Wybierz opcję Wiersz polecenia do uruchomienia** (w tym ścieżkę do narzędzia *MirrorTool.exe*) i odpowiedni element wyzwalający (na przykład CRON co godzinę 0 0 * * * ? *). Można też użyć harmonogramu zadań systemu Windows lub narzędzia `Cron` w systemie Linux.

- Aby skonfigurować aktualizacje na komputerach klienckich, utwórz nową politykę i skonfiguruj **serwer aktualizacji**, aby wskazywał adres kopii dystrybucyjnej lub folder udostępniony.

Jeśli używasz serwera kopii dystrybucyjnych HTTPS, musisz zaimportować jego certyfikat do zaufanego magazynu głównego na komputerze klienckim. Zobacz Instalowanie zaufanego certyfikatu głównego w systemie Windows.

Zapoznaj się z tym artykułem z bazy wiedzy, aby skonfigurować tworzenie łańcucha przy użyciu narzędzia Mirror Tool (konieczne jest skonfigurowanie narzędzia Mirror Tool w taki sposób, aby pobierało aktualizacje z innego narzędzia Mirror Tool).

Instalacja narzędzia Moduł zarządzania urządzeniami mobilnymi – Windows

Moduł zarządzania urządzeniami mobilnymi musi być dostępny przez Internet, aby na stałe umożliwić zarządzanie urządzeniami mobilnymi bez względu na ich lokalizację.

Zalecamy wdrożenie komponentu MDM na innym urządzeniu hosta niż to, na którym jest hostowany serwer ESET PROTECT.

W celu zainstalowania komponentu Mobile Device Connector dla serwera ESET PROTECT w systemie Windows wykonaj następujące kroki:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczceinstalacji.

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (*mdmcore_x64.msi*).

2. Uruchom instalator narzędzia Moduł zarządzania urządzeniami mobilnymi i zaakceptuj umowę EULA, jeśli zgadzasz się na jej warunki.

3. Kliknij przycisk **Przeglądaj**, przejdź do lokalizacji certyfikatu SSL do obsługi komunikacji przy użyciu protokołu HTTPS i wpisz hasło do tego certyfikatu.

4. Podaj **nazwę hosta MDM**: to domena publiczna lub publiczny adres IP serwera MDM dostępny dla urządzeń mobilnych łączących się przez Internet.

Wpisana nazwa hosta MDM musi mieć taką samą postać, jak w przypadku **certyfikatu serwera HTTPS**. W przeciwnym razie na urządzeniu mobilnym z systemem iOS nie będzie można zainstalować profilu MDM. Jeśli na przykład istnieje adres IP określony w certyfikacie HTTPS, wpisz ten adres IP w polu **Nazwa hosta MDM**. W przypadku gdy w certyfikacie HTTPS podana jest nazwa FQDN (np. `mdm.mycompany.com`) wprowadź tę nazwę FQDN w polu **Nazwa hosta MDM**. W przypadku użycia symbolu wieloznacznego * (np. `*.mycompany.com`) w certyfikacie HTTPS możesz użyć wpisu `mdm.mycompany.com` w polu **Nazwa hosta MDM**.

5. Instalator musi teraz nawiązać połączenie z istniejącą bazą danych, która będzie wykorzystywana przez Moduł zarządzania urządzeniami mobilnymi. Należy podać następujące szczegóły połączenia:

- **Baza danych**: MySQL Server/MS SQL Server/MS SQL Server z uwierzytelnianiem systemu Windows

- **Sterownik ODBC**: sterownik MySQL ODBC 5.1/sterownik MySQL ODBC 5.2 Unicode/sterownik MySQL ODBC 5.3 Unicode/sterownik MySQL ODBC 8.0 Unicode/SQL Server/klient macierzysty SQL Server 10.0/sterownik ODBC 11 dla SQL Server/sterownik ODBC 13 dla SQL Server/sterownik ODBC 17 dla SQL Server/sterownik ODBC 18 dla SQL Server

- **Nazwa bazy danych**: Zalecamy użycie wstępnie zdefiniowanej nazwy lub jej zmianę w razie potrzeby.

- **Nazwa hosta**: nazwa hosta lub adres IP serwera bazy danych

- **Port**: port używany do łączenia się z serwerem bazy danych

- **Nazwa użytkownika / hasło** bazy danych.

- **Użyj nazwanej instancji** — w przypadku używania bazy danych MS SQL można też zaznaczyć pole wyboru **Użyj nazwanej instancji**, jeśli chcesz korzystać z własnej, niestandardowej instancji bazy danych. Niestandardową instancję bazy danych można ustawić w polu **Nazwa hosta** w postaci *NAZWA_HOSTA**INSTANCJA_BD* (na przykład *192.168.0.10**ESMC7SQL*). W przypadku bazy danych w klastrze należy użyć jedynie nazwy klastra. Po wybraniu tej opcji nie można zmienić używanego portu do łączenia się z bazą danych. System będzie korzystał z domyślnych portów określonych przez firmę Microsoft. Aby połączyć serwer ESET PROTECT z bazą danych MS SQL zainstalowaną w klastrze typu failover, wprowadź nazwę klastra w polu **Nazwa hosta**.

Istnieje możliwość korzystania z tego samego serwera bazy danych, który jest używany do obsługi bazy danych programu ESET PROTECT, zalecamy jednak korzystanie z innego, jeśli planowana liczba zarejestrowanych urządzeń mobilnych przekracza 80.

6. Określ użytkownika nowo utworzonej bazy danych narzędzia Moduł zarządzania urządzeniami mobilnymi. Możesz **utworzyć nowego użytkownika** lub **wybrać istniejącego użytkownika bazy danych**. Wpisz hasło użytkownika bazy danych.

7. Wprowadź dane w polach **Host serwera** (nazwa lub adres IP serwera ESET PROTECT) oraz **Port serwera** (port domyślny to 2222; jeśli korzystasz z innego portu, zastąp port domyślny własnym numerem portu).

8. Podłącz łącznik MDM do serwera ESET PROTECT. Wypełnij pola **Host serwera** i **Port serwera** wymagane do nawiązania połączenia z serwerem ESET PROTECT oraz wybierz opcję **Wspomagana instalacja serwerowa** lub **Instalacja offline**, aby przejść dalej:

- **Wspomagana instalacja serwerowa** — podaj poświadczenia administratora konsoli internetowej ESET PROTECT, a instalator automatycznie pobierze wymagane certyfikaty. Sprawdź również uprawnienia

wymagane w przypadku wspomaganej instalacji serwerowej.

1.Wprowadź dane w polach **Host serwera** (nazwa lub adres IP serwera ESET PROTECT) oraz **Port konsoli internetowej** (jeśli nie korzystasz z portu niestandardowego, pozostaw domyślny port 2223). Podaj również poświadczenia konta administratora konsoli internetowej — w polach **Nazwa użytkownika/Hasło**.

2.Po wyświetleniu monitu o zaakceptowanie certyfikatu kliknij pozycję **Tak**. Przejdź do kroku 10.

- **Instalacja offline** — uzupełnij pola **Certyfikat serwera proxy** oraz **Urząd certyfikacji**, które można wyeksportować z programu ESET PROTECT. Możesz też użyć certyfikatu niestandardowego i właściwego urzędu certyfikacji.

1.Kliknij przycisk **Przeglądaj** obok **certyfikatu równorzędnego** i przejdź do lokalizacji, w której się on znajduje (jest to certyfikat serwera proxy wyeksportowany z programu ESET PROTECT). Pole tekstowe **Hasło do certyfikatu** pozostaw puste, ponieważ ten certyfikat nie wymaga podawania hasła.

2.Powtórz tę samą procedurę w przypadku urzędu certyfikacji i przejdź do kroku 10.

Jeśli w programie ESET PROTECT używane są certyfikaty niestandardowe (zamiast domyślnych generowanych automatycznie podczas instalowania produktu ESET PROTECT), należy z nich skorzystać po wyświetleniu monitu o podanie certyfikatu serwera proxy.

9. Określ folder docelowy dla narzędzia Moduł zarządzania urządzeniami mobilnymi (zalecamy użycie folderu domyślnego), kliknij przycisk **Dalej**, a następnie **Zainstaluj**.

10. Po ukończeniu instalacji sprawdź, czy narzędzie Mobile Device Connector działa poprawnie, otwierając stronę *https://your-mdm-hostname:enrollment-port* (np. *https://mdm.company.com:9980*) w przeglądarce internetowej lub na urządzeniu mobilnym. Jeśli instalacja przebiegła prawidłowo, wyświetlony zostanie następujący komunikat: Serwer MDM jest uruchomiony i działa!

11. Po wykonaniu powyższych czynności można aktywować narzędzie MDM w programie ESET PROTECT.

Wymagania wstępne dotyczące komponentu Moduł zarządzania urządzeniami mobilnymi

W przypadku zmiany portu lub nazwy hosta serwera MDM konieczna jest ponowna rejestracja wszystkich urządzeń mobilnych.
W związku z tym zalecane jest skonfigurowanie dedykowanej nazwy hosta na potrzeby serwera MDM. Dzięki temu gdy będzie trzeba zmienić urządzenie hosta serwera MDM, wystarczy przypisać adres IP nowego urządzenia hosta do nazwy hosta MDM w ustawieniach DNS.

W celu zainstalowania komponentu Moduł zarządzania urządzeniami mobilnymi w systemie Windows niezbędne jest spełnienie następujących wymagań wstępnych:

- publiczny adres IP, nazwa hosta lub domena publiczna dostępna przez Internet.

Gdy zachodzi konieczność zmiany nazwy hosta serwera MDM, należy uruchomić instalację naprawczą komponentu MDC. Po zmianie nazwy hosta serwera MDM trzeba zaimportować nowy **certyfikat serwera HTTPS** z nową nazwą hosta w celu zapewnienia dalszego prawidłowego działania komponentu MDM.

- Otwarte i dostępne porty — pełną listę portów można znaleźć tutaj. Zalecamy używanie domyślnych numerów portów (9981 i 9980), jednak można je w razie potrzeby zmienić w pliku konfiguracyjnym serwera MDM. Należy się upewnić, że urządzenia mobilne mogą się łączyć przy użyciu określonych portów. Aby zapewnić taką możliwość, należy skonfigurować ustawienia zapory i/lub sieci (w razie potrzeby). Przeczytaj więcej o architekturze MDM.

- Ustawienia zapory — w przypadku instalowania Modułu zarządzania urządzeniami mobilnymi na nieserwerowych systemach operacyjnych, takich jak Windows 7 (wyłącznie do celów testowych) należy pamiętać, by udostępnić porty komunikacyjne, tworząc reguły zapory na potrzeby następujących plików:

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

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

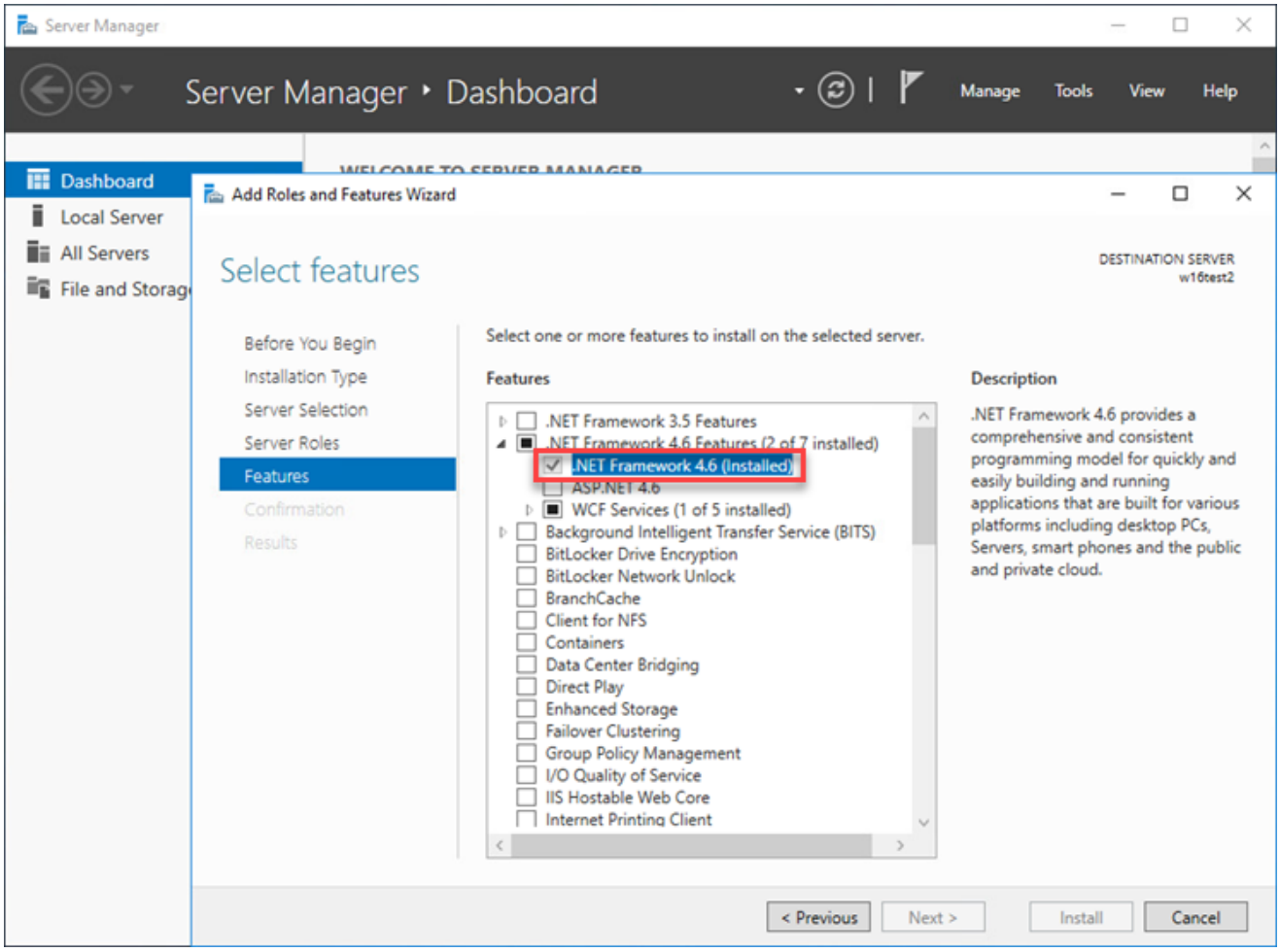
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, port TCP 2222

Rzeczywiste ścieżki do plików.*exe* mogą się różnić zależnie od miejsca instalacji poszczególnych komponentów ESET PROTECT w systemie operacyjnym klienta.

- Zainstalowany i skonfigurowany serwer bazy danych. Należy się upewnić, że zostały spełnione wymagania programu Microsoft SQL lub MySQL.

- Użycie pamięci RAM przez łącznik MDM jest zoptymalizowane, dlatego maksymalnie może działać współbieżnie 48 procesów „ESET PROTECT MDMCore Module”, a jeśli użytkownik podłączy więcej urządzeń, procesy będą okresowo zmieniane tak, aby spełniały wymagania każdego urządzenia, które aktualnie używa zasobów.

- Instalacja MS SQL Server Express wymaga programu Microsoft .NET Framework 4. Można go zainstalować przy użyciu **Kreatora dodawania ról i funkcji**:



Wymagania dotyczące certyfikatu

• Bezpieczna komunikacja przy użyciu protokołu HTTPS wymaga **certyfikatu SSL** w formacie *.pfx*. Zalecamy użycie certyfikatu dostarczonego przez niezależny urząd certyfikacji. Certyfikaty podpisane samodzielnie (w tym te podpisane przez urząd certyfikacji ESET PROTECT) nie są zalecane, ponieważ nie wszystkie urządzenia mobilne umożliwiają użytkownikom akceptowanie takich certyfikatów.

• Wymagane są: certyfikat podpisany przy użyciu urzędu certyfikacji, odpowiedni klucz prywatny oraz stosowanie standardowych procedur (zwykle z użyciem biblioteki OpenSSL), aby można było scalić oba elementy w jeden plik *.pfx*:

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```

To standardowa procedura w przypadku większości serwerów używających certyfikatów SSL.

• W przypadku instalacji offline potrzebny jest też certyfikat równorzędny (**certyfikat agenta** wyeksportowany z programu ESET PROTECT). W programie ESET PROTECT można również użyć certyfikatu niestandardowego.

Aktywacja Modułu zarządzania urządzeniami

mobilnymi

Po zainstalowaniu Modułu zarządzania urządzeniami mobilnymi należy aktywować go przy użyciu licencji punktu końcowego, licencji biznesowej lub licencji biurowej ESET:

1.Dodaj licencję punktu końcowego, licencję biznesową lub licencję biurową ESET w obszarze Zarządzanie licencjami programu ESET PROTECT.

2.Aktywuj moduł Mobile Device Connector, używając zadań klienta Aktywacja produktu. Ta procedura przebiega tak samo jak przy aktywacji dowolnego produktu firmy ESET na komputerze klienckim — w tym przypadku komputerem klienckim jest Moduł zarządzania urządzeniami mobilnymi.

Narzędzie MDM, funkcja licencjonowania urządzeń z systemem iOS

Firma ESET nie oferuje aplikacji do pobrania w sklepie Apple App Store, w związku z czym Moduł zarządzania urządzeniami mobilnymi przechowuje dane dotyczące licencji na potrzeby urządzeń z systemem iOS.

Licencje są przyznawanie na urządzenie i można je aktywować przy użyciu zadania Aktywacja produktu (tak samo jak w systemie Android).

Sposoby dezaktywacji licencji dla urządzeń z systemem iOS:

- Usunięcie urządzenia z zarządzanych elementów poprzez użycie zadania Zatrzymanie zarządzania
- Odinstalowanie Modułu zarządzania urządzeniami mobilnymi przy użyciu opcji **Usuń bazę danych**
- Inna metoda dezaktywacji (dezaktywacja programu ESET PROTECT lub portalu EBA)

W związku z tym, że narzędzie Moduł zarządzania urządzeniami mobilnymi komunikuje się z serwerami licencyjnymi firmy ESET w imieniu urządzeń z systemem iOS, w portalu EBA widoczny jest stan narzędzia Modułu zarządzania urządzeniami mobilnymi, a nie stany poszczególnych urządzeń. Aktualne informacje o urządzeniach są zawsze dostępne w konsoli internetowej ESET PROTECT.

Przy urządzeniach, które nie zostały aktywowane lub których licencje wygasły, wyświetlana jest czerwona ikona stanu ochrony i komunikat „Produkt nie został aktywowany”. Te urządzenia nie obsługują zadań, nie rejestrują zdarzeń innych niż krytyczne i nie można na nich ustawiać zasad.

Jeśli podczas odinstalowywania narzędzia MDM wybrano opcję **Nie usuwaj bazy danych**, używane licencje nie zostaną dezaktywowane. Można z nich korzystać po ponownym zainstalowaniu komponentu MDM w bazie danych albo usunąć za pośrednictwem programu ESET PROTECT lub dezaktywacji portalu EBA. W przypadku przenoszenia na inny serwer MDM należy ponownie wykonać zadanie Aktywacja produktu.

Wymagania dotyczące certyfikatu HTTPS

Aby zarejestrować urządzenie mobilne z systemem iOS w Module zarządzania urządzeniami mobilnymi ESET, należy zadbać o to, aby serwer HTTPS zwracał cały łańcuch certyfikatów.

W celu zapewnienia prawidłowego działania certyfikatu spełnione muszą być następujące wymagania:

- Certyfikat HTTPS (kontener pkcs#12/pfx) musi obejmować cały łańcuch certyfikatów, włącznie z głównym urzędem certyfikacji.
- Certyfikat musi być ważny w wymaganym okresie (ważność od/ważność do).
- Wartości **CommonName** lub **subjectAltName** muszą być zgodne z nazwą hosta serwera MDM.

Jeśli **nazwa hosta serwera MDM** to na przykład hostname.mdm.domain.com, certyfikat może obejmować nazwy takie jak:
- hostname.mdm.domain.com
- *.mdm.domain.com

Nie może jednak obejmować nazw typu:
- *
- *.com
- *.domain.com

Krótko mówiąc, część „ * ” nie może zastępować elementu „z kropką”. Jest to potwierdzony sposób działania w przypadku akceptowania certyfikatów serwera MDM przez system iOS.

Podczas sprawdzania ważności certyfikatu niektóre urządzenia uwzględniają swoją aktualną strefę czasową, a inne nie. Aby uniknąć możliwych problemów, warto ustawić ważność certyfikatu na dzień lub dwa przed bieżącą datą.

Instalacja i pamięć podręczna serwera proxy Apache HTTP

Serwer proxy Apache HTTP — informacje

Serwer proxy Apache HTTP może służyć do różnych celów:

Funkcja	Rozwiązanie proxy, które udostępnia tę funkcję
Buforowanie plików do pobrania i aktualizacji	Apache HTTP Proxy lub inne rozwiązanie proxy
Buforowanie wyników ESET LiveGuard Advanced	Tylko skonfigurowana usługa Apache HTTP Proxy
Komunikacja replikacji agenta ESET Management z serwerem ESET PROTECT	Apache HTTP Proxy lub inne rozwiązanie proxy

Jeśli w systemie Windows już zainstalowano serwer proxy Apache HTTP i jest potrzebne jego uaktualnienie do najnowszej wersji, należy przejść do sekcji Uaktualnianie serwera proxy Apache HTTP.

Funkcja buforowania serwera proxy Apache HTTP

Apache HTTP Proxypobieranie i zapisywanie w pamięci podręcznej:

- Aktualizacja modułów ESET
- Pakiety instalacyjne z serwerów repozytorium

- Aktualizacje komponentów produktów

Buforowane dane są dystrybuowane do klientów w punktach końcowych sieci. Buforowanie może znacznie zmniejszyć natężenie ruchu internetowego w sieci.

Można zainstalować oprogramowanie Squid jako alternatywę dla serwera proxy Apache HTTP.

Serwer proxy Apache HTTP można zainstalować w systemie Windows na dwa sposoby:

- Instalacja z użyciem instalatora kompleksowego
- Instalacja z użyciem instalatora autonomicznego

Instalacja z użyciem instalatora autonomicznego

1. Przejdź do sekcji pobierania programu ESET PROTECT w celu pobrania instalatora autonomicznego tego komponentu programu ESET PROTECT (*apachehttp.zip*).

2. Otwórz plik *ApacheHttp.zip* i wyodrębnij pliki do lokalizacji *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*.

Jeśli serwer proxy Apache HTTP ma zostać zainstalowany na innym dysku twardym, ścieżkę *C:\Program Files* należy zastąpić odpowiednią ścieżką zgodnie z poniższą instrukcją — w pliku *httpd.conf* znajdującym się w katalogu *Apache HTTP Proxy\conf*. Jeśli na przykład zawartość pliku *ApacheHttp.zip* rozpakowano do katalogu *D:\Apache Http Proxy*, ścieżkę *C:\Program Files* należy zastąpić ścieżką *D:\Apache Http Proxy*.

3. Otwórz administracyjny wiersz polecenia i zmień katalog na *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin*

4. Wykonaj następujące polecenie:

```
httpd.exe -k install -n ApacheHttpProxy
```

5. Uruchom usługę **ApacheHttpProxy** za pomocą następującego polecenia:

```
sc start ApacheHttpProxy
```

6. Przy użyciu wtyczki `services.msc` można sprawdzić, czy usługa serwera proxy Apache HTTP działa (należy szukać pozycji **ApacheHttpProxy**). Domyślnie usługa jest tak skonfigurowana, by uruchamiać się automatycznie.

Po ukończeniu instalacji skonfiguruj serwer proxy Apache HTTP pod kątem potrzebnych funkcji.

Konfiguracja serwera proxy Apache HTTP

Instalator serwera proxy Apache HTTP dostarczony przez firmę ESET jest wstępnie skonfigurowany. Jednak aby zapewnić prawidłowe działanie usługi, trzeba będzie wprowadzić dodatkowe zmiany konfiguracji.

Konfiguracja serwera proxy Apache HTTP pod kątem replikacji (agent-

serwer)

1. Zmodyfikuj plik konfiguracyjny programu *Apache HTTP Proxy httpd.conf* znajdujący się w lokalizacji *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*.

   a.Do komunikacji z agentem ESET Management jest używany domyślnie port 2222. W przypadku zmiany portu podczas instalacji należy podać zmieniony numer portu. Zmień ciąg 2222 w wierszu `AllowCONNECT 443 563 2222 8883 53535` na swój numer portu.

   b.Dodaj oddzielny segment `ProxyMatch`:

      I.Adres używany przez agenty do nawiązywania połączenia z serwerem ESET PROTECT.

      II.Wszystkie pozostałe adresy serwera ESET PROTECT (IP, FQDN)
      (Dodaj cały poniższy kod — adres IP 10.1.1.10 i nazwa hosta `hostname.example` to tylko przykłady, które należy zastąpić własnymi adresami. Możesz też wygenerować wyrażenie `ProxyMatch` zgodnie z tym artykułem w bazie wiedzy).

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>
Allow from all
</ProxyMatch>
```

   c.Uruchom ponownie usługę *Apache HTTP Proxy*.

2. Skonfiguruj odpowiednią politykę agentów, aby agenty używały serwera proxy do replikacji.

Konfiguracja serwera proxy Apache HTTP pod kątem buforowania

1. Zatrzymaj usługę **ApacheHttpProxy** za pomocą następującego polecenia:

```
sc stop ApacheHttpProxy
```

2. Otwórz plik *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* w prostym edytorze tekstu. Dodaj następujące wiersze na końcu pliku:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

3. Zapisz plik i uruchom usługę Apache.

```
sc start ApacheHttpProxy
```

> Jeśli katalog pamięci podręcznej ma się znajdować w innym miejscu, na przykład na innym dysku (takim jak `D:\Apache HTTP Proxy\cache`), w ostatnim wierszu powyższego kodu należy zmienić ciąg `"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"` na `"D:\Apache HTTP Proxy\cache"`.

Konfiguracja serwera proxy Apache HTTP pod kątem nazwy użytkownika i hasła

Z ustawienia nazwy użytkownika i hasła można korzystać tylko na potrzeby buforowania. W przypadku protokołu replikacji używanego w komunikacji agent-serwer uwierzytelnianie nie jest obsługiwane.

1. Zatrzymaj usługę **ApacheHttpProxy**, otwierając wiersz polecenia z podwyższonym poziomem uprawnień i wykonując następujące polecenie:

```
sc stop ApacheHttpProxy
```

2. Sprawdź, czy w pliku *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* znajdują się następujące moduły:

```
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. Dodaj następujące wiersze w pliku *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* w sekcji `<Proxy *>`:

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

4. Użyj polecenia `htpasswd`, aby utworzyć plik o nazwie `password.file` w folderze *Apache HTTP Proxy\bin* (zostanie wyświetlony monit o podanie hasła):

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

5. W folderze *Apache HTTP Proxy* ręcznie utwórz plik `group.file` o następującej zawartości:

```
usergroup:username
```

6. Uruchom usługę **ApacheHttpProxy** przez wykonanie następującego polecenia w wierszu polecenia z podwyższonym poziomem uprawnień:

```
sc start ApacheHttpProxy
```

7. Przetestuj połączenie z serwerem proxy HTTP, wpisując w przeglądarce następujący adres URL:

http:///[IP address]:3128/index.html

Po pomyślnym zainstalowaniu serwera proxy Apache HTTP można zezwolić na komunikację tylko z produktami ESET (zablokowanie całego pozostałego ruchu — opcja domyślna) lub zezwolić na cały ruch. Należy wprowadzić konieczne zmiany w konfiguracji zgodnie z poniższym opisem:

- Przekazywanie jedynie w ramach komunikacji z produktami ESET
- Tworzenie łańcucha na serwerze proxy (cały ruch)

Wyświetlanie listy aktualnie buforowanej zawartości

"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -a -p "C:\ProgramData\Apache HTTP Proxy\cache"

Użyj polecenia htcacheclean do wyczyszczenia pamięci podręcznej dysku. Zobacz zalecane polecenie poniżej (ustawienie rozmiaru pamięci podręcznej na 20 GB i ograniczenie liczby buforowanych plików do około 128 000):

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M -L128000
```

Aby zaplanować czyszczenie pamięci podręcznej co godzinę, uruchom polecenie:

```
schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\"^
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M -L128000"
```

Jeśli wybrano opcję zezwolenia na cały ruch, zalecane są następujące polecenia:

```
"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe" -n -t^
-p"C:\ProgramData\Apache HTTP Proxy\cache" -l20000M

schtasks /Create /F /RU "SYSTEM" /SC HOURLY /TN ESETApacheHttpProxyCleanTask^
/TR "\"C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\htcacheclean.exe\"^
-n -t -p \"C:\ProgramData\Apache HTTP Proxy\cache\" -l20000M"
```

Bardzo ważny jest znak ^ na końcu wiersza powyższych poleceń. W przypadku pominięcia go polecenie nie zostanie wykonane prawidłowo.

Więcej informacji zawiera ten artykuł w bazie wiedzy oraz dokumentacja dotycząca uwierzytelniania i autoryzacji w oprogramowaniu Apache.

Squid — instalowanie w systemie Windows i pamięć

podręczna serwera proxy HTTP

Oprogramowanie Squid to alternatywa dla serwera proxy Apache HTTP. Aby zainstalować oprogramowanie Squid w systemie Windows, należy wykonać poniższe czynności:

1. Pobierz instalator MSI oprogramowania Squid i zainstaluj oprogramowanie Squid.

2. Kliknij ikonę **Squid for Windows** w menu paska zadań i wybierz element **Stop Squid Service**.

3. Przejdź do folderu instalacyjnego oprogramowania Squid, na przykład C:\Squid\bin, i w wierszu polecenia uruchom następujące polecenie:

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

Spowoduje to utworzenie katalogów swap na potrzeby pamięci podręcznej.

4. Kliknij ikonę **Squid for Windows** w menu paska zadań i wybierz element **Open Squid Configuration**.

5. Zastąp element `http_access deny all` elementem `http_access allow all`.

6. Włącz pamięć podręczną na dysku, dodając ten wiersz:

```
cache_dir aufs /cygdrive/c/Squid/var/cache 3000 16 256
```

i
- Lokalizację tego katalogu można zmienić zgodnie z preferencjami. W powyższym przykładzie lokalizacja katalogu pamięci podręcznej to `C:\Squid\var\cache` (należy zachować format ścieżki w poleceniu).
- Można też zmienić łączny rozmiar pamięci podręcznej (w tym przykładzie jest to 3000 MB) oraz liczbę podkatalogów pierwszego poziomu (w tym przykładzie jest to 16) i podkatalogów drugiego poziomu (w tym przykładzie jest to 256) w katalogu pamięci podręcznej.

7. Zapisz i zamknij plik konfiguracyjny oprogramowania Squid o nazwie *squid.conf*.

8. Kliknij ikonę **Squid for Windows** w menu paska zadań i wybierz element **Start Squid Service**.

9. Możesz sprawdzić, czy usługa Squid działa w przystawce `services.msc` (poszukaj pozycji **Squid for Windows**).

Repozytorium offline — Windows

Za pomocą narzędzia Kopia dystrybucyjna można utworzyć repozytorium offline (w systemie Windows). Zazwyczaj jest to wymagane w przypadku zamkniętych sieci komputerowych lub sieci o ograniczonym dostępie do Internetu. Narzędzia Mirror Tool można użyć do utworzenia klonu repozytorium ESET w lokalnym folderze. Sklonowane repozytorium można następnie przenieść do lokalizacji w sieci zamkniętej (np. na dysku zewnętrznym). Repozytorium można skopiować do bezpiecznej lokalizacji w sieci lokalnej, a następnie udostępnić je za pośrednictwem serwera HTTP.

Aby zaktualizować repozytorium offline, należy uruchomić to samo polecenie z tymi samymi parametrami, które zostały użyte na potrzeby utworzenia repozytorium offline. Zostaną użyte istniejące dane w folderze pośredniczącym i zastąpione zostaną tylko nieaktualne pliki.

Należy pamiętać, że rozmiar repozytorium jest coraz większy, a rozmiar katalogu pośredniczącego będzie taki sam. Przed rozpoczęciem tej procedury należy się upewnić, że jest dostępne co najmniej **1,2 TB** wolnego miejsca.

Najlepsze praktyki

Zobacz też artykuł bazy wiedzy ESET Najważniejsze wskazówki dotyczące korzystania z ESET PROTECT w środowisku offline.

Przykładowy scenariusz dla systemu Windows

I. Utworzenie klonu repozytorium

1. Pobierz narzędzie Mirror Tool.

2. Wyodrębnij narzędzie Mirror Tool z pobranego pliku *.zip*.

3. Przygotuj (utwórz) foldery dla następujących elementów:

   - pliki pośredniczące
   - repozytorium końcowe

4. Otwórz wiersz polecenia i zmień katalog na folder, do którego wyodrębniono narzędzie Mirror Tool (użyj polecenia `cd`).

5. Uruchom następujące polecenie (zmieniając katalog pośredniczący i katalog wyjściowy repozytorium na foldery z kroku 3):

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

6. Po skopiowaniu repozytorium do folderu `outputRepositoryDirectory` przenieś folder wraz z zawartością na inny komputer, z którego dostępna jest sieć zamknięta.

II. Skonfigurowanie serwera HTTP

7. Na komputerze znajdującym się w sieci zamkniętej należy uruchomić serwer HTTP. W tym celu można użyć:

   - serwera Apache HTTP Proxy z witryny pobierania firmy ESET (niniejszy scenariusz),
   - innego serwera HTTP.

8. Otwórz plik *apachehttp.zip* i wyodrębnij pliki do lokalizacji *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*.

9. Otwórz administracyjny wiersz polecenia i zmień katalog na *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin* (polecenie `cd`).

10. Wykonaj następujące polecenie:

```
httpd.exe -k install -n ApacheHttpProxy
```

11. Za pomocą edytora tekstu otwórz plik *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf* i na końcu tego pliku dodaj następujące wiersze:

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

12. Uruchom usługę **ApacheHttpProxy** za pomocą następującego polecenia:

```
sc start ApacheHttpProxy
```

13. Sprawdź, czy usługa działa, przechodząc pod adres *http://YourIPaddress:80/index.html* w przeglądarce internetowej (zastąp ciąg *YourIPaddress* adresem IP komputera).

III. Uruchomienie repozytorium offline

14. Utwórz nowy folder dla repozytorium offline, na przykład *C:\Repository.*

15. W pliku *httpd.conf* zastąp poniższe wiersze:

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
```

adresem folderu repozytorium:

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

16. Skopiuj pobrane repozytorium do katalogu *C:\Repository* .

17. Uruchom ponownie usługę **ApacheHttpProxy** za pomocą następującego polecenia:

```
sc restart ApacheHttpProxy
```

18. Repozytorium offline działa teraz pod adresem *http://YourIPaddress* (np. *http://10.1.1.10*).

19. Ustaw nowy adres repozytorium za pomocą konsoli internetowej produktu ESET PROTECT:

a.Serwer ESET PROTECT — kliknij pozycję **Więcej** > **Serwera** > **Ustawienia zaawansowane** > **Repozytorium** i wprowadź adres repozytorium trybu offline w polu **Serwer**.

b.Agenty ESET Management — kliknij **Zasady**, a następnie zasadę agenta i wybierz **Edytuj** > **Ustawienia** > **Ustawienia zaawansowane** > **Repozytorium** > wprowadź adres repozytorium trybu offline w polu **Serwer**.

c.Produkty ESET dla punktów końcowych (dla systemu Windows) — kliknij **Zasady**, zasadę **Produkt firmy ESET do obsługi punktów końcowych** > **Edytuj** > **Ustawienia** > **Aktualizuj** > **Profile** > **Aktualizacje** >**Aktualizacje modułów** > Usuń zaznaczenie opcji **Wybierz automatycznie** i wprowadź adres repozytorium trybu offline w polu **Serwer niestandardowy**.

Klaster trybu failover — Windows

Poniżej przedstawiono zaawansowane czynności wymagane podczas instalacji programu ESET PROTECT w klastrze trybu failover:

> Więcej informacji na temat instalacji klastra zawiera artykuł w bazie wiedzy dotyczący serwera ESET PROTECT.

1. Utwórz klaster trybu failover z dyskiem udostępnionym:

   - Instrukcje dotyczące tworzenia klastra trybu failover w systemie Windows Server 2016 i 2019
   - Instrukcje dotyczące tworzenia klastra trybu failover w systemie Windows Server 2012 i 2012 R2

2. W **Kreatorze tworzenia klastra** wprowadź żądaną nazwę hosta (wymyśl nazwę) i adres IP.

3. Uzyskaj dostęp online do udostępnionego dysku klastrowego w węźle 1 i zainstaluj na nim serwer ESET PROTECT przy użyciu instalatora autonomicznego. Podczas instalacji pamiętaj o zaznaczeniu opcji **To jest instalacja klastra** oraz wybraniu dysku udostępnionego jako pamięci masowej do przechowywania danych aplikacji. Wymyśl nazwę hosta i wprowadź ją w polu Certyfikat serwera programu ESET PROTECT Server obok wstępnie podanych nazw hosta. Zapamiętaj tę nazwę hosta i użyj jej w kroku 6 podczas tworzenia roli serwera ESET PROTECT w Menedżerze klastra.

4. Zatrzymaj ESET PROTECT Server w węźle 1. Uzyskaj dostęp online do udostępnionego dysku klastrowego w węźle 2 i zainstaluj na nim serwer ESET PROTECT przy użyciu instalatora autonomicznego. Upewnij się, że podczas instalacji została zaznaczona opcja **To jest instalacja klastra**. Wybierz dysk udostępniony jako pamięć masową do przechowywania danych aplikacji. Nie zmieniaj informacji o połączeniu z bazą danych i certyfikacie. Zostały one skonfigurowane podczas instalacji programu ESET PROTECT Server w węźle 1.

5. Skonfiguruj zaporę, aby zezwolić na połączenia przychodzące we wszystkich portach używanych przez program ESET PROTECT Server.

6. W menedżerze konfiguracji klastra utwórz i uruchom rolę (**Konfiguruj rolę** > **Wybierz rolę** > **Usługa ogólna**) dla usługi serwera ESET PROTECT. Wybierz usługę **serwera ESET PROTECT** z listy dostępnych usług. Bardzo ważne jest użycie tej samej nazwy hosta dla roli co w kroku 3. dotyczącym certyfikatu serwera.

7. Zainstaluj agenta ESET Management we wszystkich węzłach klastra przy użyciu instalatora autonomicznego. Na ekranach **Konfiguracja agenta** i **Połączenie z serwerem ESET PROTECT** użyj nazwy hosta z kroku 6. Przechowuj dane agenta w węźle lokalnym (nie na dysku klastrowym).

8. Serwer internetowy (Apache Tomcat) nie jest obsługiwany w klastrze, dlatego trzeba go zainstalować na dysku nieklastrowym albo na innym komputerze:

a.Zainstaluj konsolę internetową na oddzielnym komputerze i skonfiguruj ją poprawnie, aby połączyć się z rolą klastra serwera ESET PROTECT.

b.Po zainstalowaniu konsoli internetowej znajdź jej plik konfiguracyjny pod adresem: *C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

c.Otwórz plik w aplikacji Notatnik lub w innym prostym edytorze tekstu. W wierszu `server_address=localhost` zastąp element „localhost” adresem IP lub nazwą hosta roli klastra serwera ESET PROTECT.

Instalacja komponentów w systemie Linux

W większości scenariuszy instalacji na poszczególnych komputerach należy zainstalować różne komponenty oprogramowania ESET PROTECT w celu dostosowania go do różnych architektur, spełnienia wymogów związanych z wydajnością lub z innych przyczyn.

Postępuj zgodnie z instrukcjami instalacji ESET PROTECT krok po kroku.

Instalacja komponentów podstawowych

- Serwer ESET PROTECT
- Konsola internetowa ESET PROTECT - Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT.
- Agent ESET Management
- Serwer bazy danych

Instalacja komponentów opcjonalnych

- RD Sensor
- Moduł zarządzania urządzeniami mobilnymi
- Serwer proxy Apache HTTP
- Narzędzie Mirror Tool

Informacje o uaktualnianiu programu ESET PROTECT w systemie Linux do najnowszej wersji zawiera rozdział Zadanie uaktualniania komponentów oraz ten artykuł w bazie wiedzy.

Szczegółowa instrukcja instalacji ESET PROTECT w

systemie Linux

W tej procedurze instalacji przedstawimy szczegółową symulację instalacji serwera ESET PROTECT i konsoli internetowej ESET PROTECT. Przeprowadzimy symulację instalacji z użyciem bazy danych MySQL.

> **Instrukcje instalacji dla wybranych dystrybucji Linuksa**
> Możesz postępować zgodnie z naszymi artykułami bazy wiedzy z instrukcjami dotyczącymi poszczególnych dystrybucji:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Przed instalacją

1. Sprawdź, czy serwer bazy danych istnieje w sieci i jest możliwy dostęp do niego na serwerze lokalnym/zdalnym. Jeśli serwer bazy danych nie jest zainstalowany, zainstaluj i skonfiguruj nowy.

2. Pobierz autonomiczne komponenty ESET PROTECT dla systemu Linux (Agent, Serwer, Konsola internetowa). Odpowiednie pliki instalacyjne znajdują się w kategorii Instalatory autonomiczne ESET PROTECT w witrynie firmy ESET.

Proces instalacji

Do ukończenia instalacji wymagana jest możliwość użycia polecenia `sudo` lub uprawnień `root`.

1. Zainstaluj wymagane pakiety serwera ESET PROTECT.

2. Skonfiguruj połączenie z serwerem MySQL zgodnie z tematem dotyczącym konfiguracji programu MySQL.

3. Weryfikacja konfiguracji sterownika MySQL ODBC. Aby uzyskać więcej informacji, zobacz sekcję Instalacja i konfiguracja sterownika ODBC.

4. Dostosuj parametry instalacji i uruchom instalację serwera ESET PROTECT. Więcej informacji można znaleźć w części Instalacja serwera — system Linux.

5. Zainstaluj wymagane pakiety Java i Tomcat oraz zainstaluj konsolę internetową ESET PROTECT. W przypadku problemów z połączeniem HTTPS z konsolą internetową ESET PROTECT zapoznaj się z informacjami dotyczącymi konfiguracji połączenia HTTPS/SSL.

6. Zainstaluj agenta ESET Management na komputerze serwera.

> Firma ESET zaleca usunięcie poleceń zawierających poufne dane (na przykład hasło) z historii wiersza poleceń:
> 1.Uruchom polecenie `history`, aby wyświetlić listę wszystkich poleceń w historii.
> 2.Uruchom polecenie `history -d line_number` (określ numer wiersza, w którym występuje interesujące Cię polecenie). Możesz też wywołać polecenie `history -c`, aby usunąć całą historię wiersza poleceń.

Instalacja i konfiguracja oprogramowania MySQL

Instalacja

> ⚠ Pamiętaj o zainstalowaniu obsługiwanej wersji programu MySQL Server i łącznika ODBC.

Jeśli już zainstalowano i skonfigurowano oprogramowanie MySQL, należy przejść do punktu Konfiguracja.

1. Dodaj repozytorium MySQL:

Debian, Ubuntu	Uruchom następujące polecenia w terminalu:
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	Można wybrać wersje składników, które mają zostać zainstalowane podczas instalacji pakietu. Zalecamy skorzystanie z opcji domyślnych. Zobacz też Dodawanie repozytorium MySQL APT.

CentOS, Red Hat	Dodawanie repozytorium MySQL Yum
OpenSuse, SUSE Linux Enterprise Server	Dodawanie repozytorium MySQL SLES

2. Zaktualizuj pamięć podręczną repozytorium lokalnego:

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
OpenSuse, SUSE Linux Enterprise Server	`sudo zypper update`

3. Instalacja oprogramowania MySQL różni się w zależności od używanej dystrybucji i wersji systemu Linux.

Linux dystrybucja:	MySQL Server — polecenie instalacji:	MySQL Server — instalacja zaawansowana:
Debian, Ubuntu	`sudo apt-get install mysql-server`	Instalowanie oprogramowania MySQL ze źródła za pomocą repozytorium MySQL APT
CentOS, Red Hat	`sudo yum install mysql-community-server`	Instalowanie oprogramowania MySQL w systemie Linux przy użyciu repozytorium MySQL Yum
OpenSuse, SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Etapy ponownej instalacji MySQL

Pobierz MySQL Community Server w celu ręcznej instalacji.

Konfiguracja

1. Otwórz plik konfiguracyjny *my.cnf* w edytorze tekstowym:

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

Jeśli nie ma pliku, sprawdź w lokalizacji `/etc/mysql/my.cnf` lub `/etc/my.cnf.d/community-mysql-server.cnf` lub `/etc/mysql/mysql.conf.d/mysqld.cnf`.

2. Znajdź następującą konfigurację w części `[mysqld]` pliku *my.cnf* i zmień wartości.

> i
> - Utwórz sekcję `[mysqld]`, jeśli nie ma jej w pliku.
> - Jeśli danych parametrów nie ma w pliku, dodaj je w części `[mysqld]`.
> - Aby określić wersję MySQL, uruchom polecenie: `mysql --version`

Parametr	Komentarze i zalecane wartości	MySQL wersja
`max_allowed_packet=33M`		Wszystkie obsługiwane wersje.
`log_bin_trust_function_creators=1`	Inną opcją jest wyłączenie rejestrowania binarnego: `log_bin=0`	Obsługiwane wersje 8.x
`innodb_log_file_size=100M`	Mnożnik wartości tych dwóch parametrów musi wynosić co najmniej **200**. Minimalna wartość elementu `innodb_log_files_in_group` to **2** a wartość maksymalna to **100**; przy czym musi to też być liczba całkowita).	Obsługiwane wersje 8x 5.7 5.6.22 (i późniejsze 5.6.x)
`innodb_log_files_in_group=2`		
`innodb_log_file_size=200M`	Ustaw wartość na co najmniej **200M**, ale nie więcej niż **3000M**.	5.6.20 i 5.6.21

3. Naciśnij **CTRL + X** i wpisz **Y**, aby zapisać zmiany i zamknąć plik.

4. Uruchom ponownie serwer MySQL i zastosuj konfigurację (w niektórych przypadkach usługa ma nazwę `mysqld`):

```
sudo systemctl restart mysql
```

5. Skonfiguruj uprawnienia MySQL i hasło do programu (to polecenie opcjonalne, które może nie działać w niektórych dystrybucjach systemu Linux):

a)Ujawnij tymczasowe hasło MySQL: `sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)Skopiuj i zapisz hasło.

c)Ustaw nowe hasło, korzystając z jednej z następujących opcji:

- Uruchom `/usr/bin/mysql_secure_installation` i wpisz hasło tymczasowe. Następnie zostaniesz poproszony o utworzenie nowego hasła.

- Uruchom `mysql -u root -p` i wpisz hasło tymczasowe. Uruchom `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';`, aby zmienić hasło użytkownika root (zastąp `strong_new_password` własnym hasłem) i wpisz `Quit`.

Zobacz także Popraw bezpieczeństwo instalacji MySQL w podręczniku referencyjnym MySQL.

6. Sprawdź, czy usługa serwera MySQL jest uruchomiona:

```
sudo systemctl status mysql
```

Instalacja i konfiguracja sterownika ODBC

Pamiętaj o zainstalowaniu obsługiwanej wersji programu MySQL Server i łącznika ODBC.

Po zainstalowaniu sterownika MS ODBC (w wersji 13 lub nowszej) można połączyć serwer ESET PROTECT w systemie Linux z programem MS SQL Server w systemie Windows. Więcej informacji można znaleźć w tym artykule bazy wiedzy.

Zainstaluj sterownik MySQL ODBC za pomocą polecenia Terminal. Postępuj zgodnie z instrukcjami dla swojej dystrybucji Linuksa:

- Debian, Ubuntu
- CentOS 7
- Inne obsługiwane dystrybucje Linuksa

Debian, Ubuntu

1. Instalowanie sterowników unixODBC

```
sudo apt-get install unixodbc
```

2. Pobierz łącznik ODBC:

Ubuntu 16	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
Ubuntu 18	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
Ubuntu 20	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
Debian 10	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz`

- Pamiętaj o wybraniu i pobraniu wersji zgodnej z dystrybucją i wersją używanego systemu Linux.
- Możesz pobrać łącznik ODBC dla oprogramowania MySQL z oficjalnej witryny MySQL.

3. Rozpakuj archiwum sterownika ODBC (nazwa pakietu zmienia się w zależności od użytego łącza):

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. Wyodrębnij sterownik ODBC (nazwa pakietu zmienia się w zależności od użytego łącza):

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. Przejdź do folderu sterownika ODBC (nazwa pakietu zmienia się w zależności od użytego łącza):

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. Skopiuj pliki sterownika ODBC:

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. Zarejestruj sterownik dla ODBC.

- W przypadku nowych wersji Linuksa, takich jak Ubuntu 20.x, zalecamy użycie sterownika Unicode:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

- W przypadku innych systemów lub gdy sterownik Unicode nie działa:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. Lista zainstalowanych sterowników:

```
sudo myodbc-installer -d -l
```

Aby uzyskać więcej informacji, odwiedź stronę:
https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html.

CentOS 7

1. Instalowanie sterowników unixODBC

```
sudo yum install unixODBC -y
```

2. Pobierz łącznik ODBC:

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.e
l7.x86_64.rpm
```

- Nie instaluj łącznika ODBC za pomocą YUM — spowoduje to zainstalowanie najnowszej, niekompatybilnej wersji.
- Pamiętaj o wybraniu i pobraniu wersji zgodnej z dystrybucją i wersją używanego systemu Linux.
- Możesz pobrać łącznik ODBC dla oprogramowania MySQL z oficjalnej witryny MySQL.

3. Instalowanie serwera ODBC:

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. Konfiguracja serwera ODBC:

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. Lista zainstalowanych sterowników:

```
sudo myodbc-installer -d -l
```

Inne obsługiwane dystrybucje Linuksa

- Pamiętaj o wybraniu i pobraniu wersji zgodnej z dystrybucją i wersją używanego systemu Linux.
- Możesz pobrać łącznik ODBC dla oprogramowania MySQL z oficjalnej witryny MySQL.

1. Postępuj zgodnie z poniższymi instrukcjami, aby zainstalować sterownik ODBC:

- **OpenSuse, SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. Dodatkowe informacje: https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-rpm.html

- Instalowanie łącznika/ODBC z binarnej dystrybucji Tarball

2. Uruchom poniższe polecenie, aby otworzyć plik *odbcinst.ini* w edytorze tekstowym:

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

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

3. Skopiuj następującą konfigurację do pliku *odbcinst.ini* (upewnij się, że ścieżki **Driver** i **Setup** są prawidłowe), a następnie zapisz i zamknij plik:

```
[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
```

W niektórych dystrybucjach sterownik może się znajdować w innej lokalizacji. Plik można znaleźć przy użyciu następującego polecenia:

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

4. Zaktualizuj pliki konfiguracyjne kontrolujące dostęp ODBC do serwerów bazy danych na bieżącym hoście, wykonując to polecenie:

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

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

Instalacja serwera — system Linux

> **Instrukcje instalacji dla wybranych dystrybucji Linuksa**
> Możesz postępować zgodnie z naszymi artykułami bazy wiedzy z instrukcjami dotyczącymi poszczególnych dystrybucji:
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

Instalacja

Wykonaj poniższe czynności, aby zainstalować komponent serwera ESET PROTECT w systemie Linux przy użyciu polecenia Terminal:

> Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczącеinstalacji.

1. Pobierz składnik serwera ESET PROTECT:

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. Spraw, aby pobrany plik był wykonywalny:

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

3. Można przygotować skrypt instalacyjny, a następnie wykonać go przy użyciu programu `sudo`.

Uruchom skrypt instalacji w oparciu o poniższy przykład (nowe wiersze są oddzielone znakiem „\”, co umożliwia skopiowanie całego polecenia do terminala):

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

Można modyfikować następujące atrybuty:

Atrybut	Opis	Wymagane
`--uninstall`	Odinstalowuje produkt.	-
`--keep-database`	Baza danych nie zostanie usunięta podczas dezinstalacji.	-
`--locale`	Identyfikator ustawień regionalnych (LCID) zainstalowanego serwera (wartość domyślna to `en_US`). Zobacz obsługiwane języki, aby sprawdzić dostępne opcje. **i** Jeśli nie określisz parametru `--locale`, serwer ESET PROTECT zostanie zainstalowany w języku angielskim. Po instalacji serwera ESET PROTECT język można ustawić dla każdej sesji konsoli internetowej ESET PROTECT. Zmiana języka nie ma wpływu na niektóre elementy konsoli internetowej. Niektóre elementy (domyślne panele kontrolne, zasady, zadania itp.) są tworzone podczas instalacji ESET PROTECT i nie można zmienić ich języka.	Tak
`--skip-license`	Podczas instalacji użytkownik nie będzie proszony o potwierdzenie umowy licencyjnej.	-
`--skip-cert`	Pomiń generowanie certyfikatów (użyj w połączeniu z parametrem `--server-cert-path`).	-
`--license-key`	Klucz licencyjny produktu ESET. Klucz licencyjny można wprowadzić później.	-
`--server-port`	Port serwera ESET PROTECT (wartość domyślna to `2222`).	-
`--console-port`	Port konsoli ESET PROTECT (wartość domyślna to `2223`).	-
`--server-root-password`	Hasło umożliwiające zalogowanie się do konsoli internetowej jako użytkownik „Administrator”. Musi składać się z co najmniej 8 znaków.	Tak

Atrybut	Opis	Wymagane
`--db-type`	Typ bazy danych, która będzie używana (możliwe wartości: `"MySQL Server"`, `"MS SQL Server"`). Program MS SQL Server dla systemu Linux nie jest obsługiwany. Można jednak połączyć serwer ESET PROTECT w systemie Linux z programem MS SQL Server w systemie Windows.	-
`--db-driver`	Sterownik ODBC używany w celu łączenia się z bazą danych wskazaną w pliku *odbcinst.ini* (polecenie `odbcinst -q -d` zwraca listę dostępnych sterowników. Można użyć na przykład jednego z tych sterowników: `--db-driver="MySQL ODBC 8.0 Driver"`, `--db-driver="MySQL ODBC 8.0 Unicode Driver"` lub `--db-driver="MySQL ODBC 8.0.17"`).	Tak
`--db-hostname`	Nazwa komputera lub adres IP serwera bazy danych. Nazwana instancja bazy danych nie jest obsługiwana.	Tak
`--db-port`	Port serwera bazy danych (wartość domyślna to `3306`).	Tak
`--db-name`	Nazwa bazy danych serwera ESET PROTECT (wartość domyślna to `era_db`)	-
`--db-admin-username`	Nazwa użytkownika będącego administratorem bazy danych (używana w instalatorze podczas tworzenia i modyfikowania bazy danych). Ten parametr można pominąć, jeśli istnieje wcześniej utworzony użytkownik bazy danych zdefiniowany parametrami `--db-user-username` oraz `--db-user-password`.	Tak
`--db-admin-password`	Hasło administratora bazy danych. Ten parametr można pominąć, jeśli istnieje wcześniej utworzony użytkownik bazy danych zdefiniowany parametrami `--db-user-username` oraz `--db-user-password`	Tak
`--db-user-username`	Nazwa użytkownika bazy danych serwera ESET PROTECT (używana na serwerze ESET PROTECT w celu nawiązywania połączenia z bazą danych). Jej długość nie powinna przekraczać 16 znaków.	Tak
`--db-user-password`	Hasło użytkownika bazy danych serwera ESET PROTECT	Tak
`--cert-hostname`	Zawiera wszystkie możliwe nazwy i/lub adres IP serwera ESET PROTECT na komputerze. Wartość musi być zgodna z nazwą serwera podaną w certyfikacie agenta, który próbuje nawiązać połączenie z serwerem.	Tak
`--server-cert-path`	Ścieżka do certyfikatu serwera równorzędnego (tej opcji należy użyć w przypadku określenia również parametru `--skip-cert`)	-
`--server-cert-password`	Hasło do certyfikatu serwera równorzędnego.	-
`--agent-cert-password`	Hasło do certyfikatu agenta równorzędnego.	-
`--cert-auth-password`	Hasło do urzędu certyfikacji.	-
`--cert-auth-path`	Ścieżka do pliku urzędu certyfikacji serwera	-
`--cert-auth-common-name`	Nazwa pospolita urzędu certyfikacji (należy użyć „”)	-
`--cert-organizational-unit`	-	-
`--cert-organization`	-	-
`--cert-locality`	-	-
`--cert-state`	-	-

Atrybut	Opis	Wymagane
`--cert-country`	-	-
`--cert-validity`	Ważność certyfikatu w dniach lub latach (należy to określić w argumencie `--cert-validity-unit`)	-
`--cert-validity-unit`	Jednostka, w jakiej podawana jest ważność certyfikatu; możliwe wartości to „Years” (Lata) lub „Days” (Dni) (wartość domyślna to `Years`)	-
`--ad-server`	Serwer Active Directory.	-
`--ad-user-name`	Nazwa użytkownika, który dysponuje prawami do wyszukiwania w sieci AD.	-
`--ad-user-password`	Hasło użytkownika usługi Active Directory.	-
`--ad-cdn-include`	Ścieżka drzewa Active Directory, które będzie synchronizowane. Aby synchronizować całe drzewo, należy nie wpisywać nic pomiędzy cudzysłowami ""	-
`--enable-imp-program`	Włącza program ulepszania produktu.	-
`--disable-imp-program`	Wyłącza program ulepszania produktu.	-

Firma ESET zaleca usunięcie poleceń zawierających poufne dane (na przykład hasło) z historii wiersza poleceń:
1.Uruchom polecenie `history`, aby wyświetlić listę wszystkich poleceń w historii.
2.Uruchom polecenie `history -d line_number` (określ numer wiersza, w którym występuje interesujące Cię polecenie). Możesz też wywołać polecenie `history -c`, aby usunąć całą historię wiersza poleceń.

4. Podczas instalacji pojawi się zapytanie o chęć dołączenia do programu ulepszania produktu. Naciśnij klawisz **T**, jeśli zgadzasz się na wysyłanie raportów o awariach i danych telemetrycznych do firmy ESET, lub **N**, aby nie wysyłać żadnych danych.

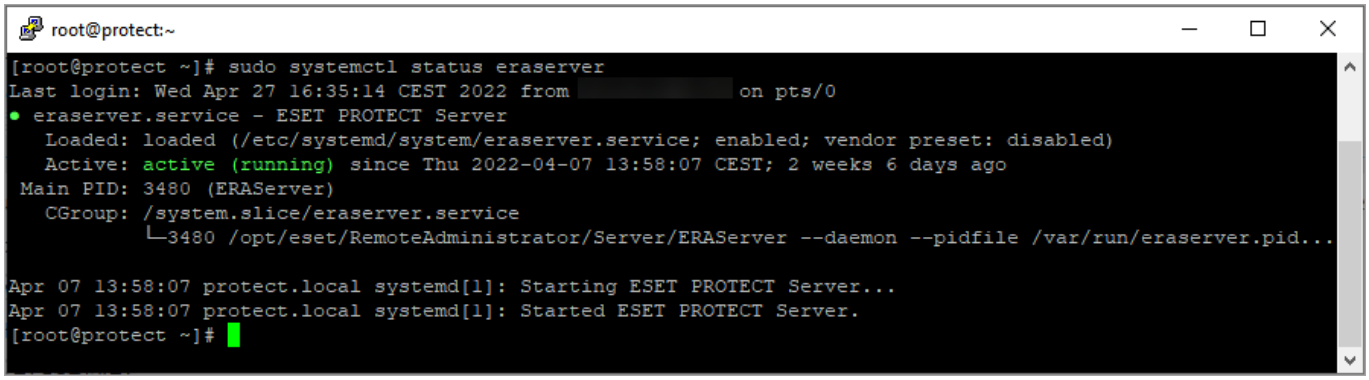
5. Serwer ESET PROTECT oraz usługa `eraserver` zostaną zainstalowane w następującej lokalizacji:

/opt/eset/RemoteAdministrator/Server

Instalacja może zakończyć się z **SELinux policy... failure** Można to zignorować, jeśli nie używasz systemu SELinux.

6. Po ukończeniu instalacji przy użyciu poniższego polecenia należy sprawdzić, czy usługa serwera ESET PROTECT działa:

```
sudo systemctl status eraserver
```



Dziennik instalatora

Dziennik instalatora może być przydatny do rozwiązywania problemów i można go znaleźć w plikach dziennika.

Wymagania wstępne dotyczące serwera — system Linux

Aby zainstalować serwer ESET PROTECT na systemie Linux, należy spełnić następujące warunki wstępne:

- Wymagana jest ważna licencja.
- Musisz mieć obsługiwaną wersję systemu Linux.
- Wymagane porty muszą być otwarte i dostępne — pełną listę portów można znaleźć tutaj.
- Serwer bazy danych zainstalowany i skonfigurowany przy użyciu konta użytkownika root. Nie ma konieczności utworzenia konta użytkownika przed rozpoczęciem instalacji. Instalator może je utworzyć. Program MS SQL Server dla systemu Linux nie jest obsługiwany. Można jednak połączyć serwer ESET PROTECT w systemie Linux z programem MS SQL Server w systemie Windows.

> W bazie danych na serwerze ESET PROTECT zapisywane są duże obiekty blob danych. Aby rozwiązanie ESET PROTECT działało prawidłowo, należy skonfigurować w programie MySQL przyjmowanie większych pakietów.

- **Sterownik ODBC** — sterownik służący do nawiązywania połączenia z serwerem bazy danych (MySQL).
- Ustawienie pliku instalacyjnego serwera jako pliku wykonywalnego za pomocą polecenia Terminal:

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

- Zalecamy **korzystanie z najnowszej wersji programu OpenSSL 1.1.1**. Wersja OpenSSL 3.x nie jest obsługiwana. Najniższa obsługiwana wersja biblioteki OpenSSL w systemie Linux to openssl-1.0.1e-30. Jednocześnie w systemie może być zainstalowanych więcej wersjiOpenSSL. Co najmniej jedna obsługiwana wersja musi być zainstalowana w systemie.
    - Aby pokazać bieżącą wersję domyślną, możesz użyć polecenia `openssl version`.
    - Możesz też wyświetlić wszystkie wersje biblioteki OpenSSL zainstalowane w systemie. W tym celu sprawdź końcówki nazw plików wyświetlonych przy użyciu polecenia `sudo find / -iname *libcrypto.so*`
    - Można sprawdzić zgodność klienta Linux przy pomocy następującego polecenia: `openssl s_client -connect google.com:443 -tls1_2`
- **Xvfb** — pakiet wymagany do drukowania raportów (Generowanie raportów) na serwerach z systemem Linux bez interfejsu graficznego.
- **Xauth** — pakiet zostanie zainstalowany razem z **xvfb**. Musisz zainstalować **xauth**, jeśli **xvfb** nie zostanie zainstalowany.
- **cifs-utils** — pakiet wymagany do prawidłowego wdrażania agenta w systemie operacyjnym Windows.

- **Qt4 WebKit** — biblioteki służące do drukowania raportów w formacie PDF i PS (wymagana jest wersja 4.8, nie 5). Wszystkie pozostałe zależności Qt4 zostaną zainstalowane automatycznie. Jeśli pakiet nie jest dostępny w repozytorium systemu operacyjnego, możesz skompilować go samodzielnie na komputerze docelowym lub zainstalować go z repozytorium innej firmy (na przykład z repozytoriów EPEL): Instrukcje dla CentOS 7, Instrukcje dla Ubuntu 20.04.

- **kinit + klist** — protokół Kerberos jest używany w celu uwierzytelnienia użytkownika domenowego podczas logowania oraz do zadań synchronizacji z usługą Active Directory. Upewnij się, że protokół Kerberos został poprawnie skonfigurowany (*/etc/krb5.conf*). Program ESET PROTECT 9.1 obsługuje synchronizację z wieloma domenami.

- **ldapsearch** — pakiet używany w zadaniu synchronizacji z usługą AD oraz do autoryzacji.

- **snmptrap** — opcjonalnie, używany do wysyłania komunikatów SNMP traps. Protokół SNMP również należy skonfigurować.

- **SELinux Development Package** — pakiet używany podczas instalacji produktu do tworzenia modułów polityk SELinux. Ten pakiet jest wymagany tylko w systemach z włączonym modułem SELinux (CentOS, RHEL). Moduł SELinux może powodować problemy z innymi aplikacjami. Nie jest on wymagany w przypadku serwera ESET PROTECT.

- **lshw** - Zainstaluj pakiet `lshw` na komputerze klienta/serwera z systemem Linux, aby agent ESET Management mógł poprawnie sporządzić spis sprzętu.

Poniższa tabela zawiera odpowiednie polecenia terminala dla każdego opisanego powyżej pakietu dla różnych dystrybucji systemu Linux (polecenia te należy wywoływać jako `sudo` lub `root`):

Pakiet	Dystrybucja Debian i Ubuntu	Dystrybucje CentOS i Red Hat	Dystrybucje OpenSUSE
Sterownik ODBC	Zapoznaj się z rozdziałem Instalacja i konfiguracja sterownika ODBC.		
OpenSSL	`apt-get install openssl`	`yum install openssl -y`	`zypper install openssl`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`	`zypper install xorg-x11-server-extra`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`	`zypper install cifs-utils`

Biblioteki Qt4 WebKit	`apt-get install libqtwebkit4`
	Zobacz instrukcje dla Ubuntu 20.04.
		Qt4 WebKit nie jest standardowym repozytorium CentOS. Zainstaluj następujące pakiety:
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		Ewentualnie można zainstalować pakiet z repozytoriów Fedora.
			`zypper install libqtwebkit4`

Pakiet	Dystrybucja Debian i Ubuntu	Dystrybucje CentOS i Red Hat	Dystrybucje OpenSUSE
kinit + klist — opcjonalnie (wymagany przez usługę Active Directory)	`apt-get install krb5-user`	`yum install krb5-workstation`	`zypper install krb5-client`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`	`zypper install openldap2-client cyrus-sasl-gssapi cyrus-sasl-ldap-auxprop`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`	`zypper install net-snmp`
Pakiet programistyczny SELinux (opcjonalny — nie jest niezbędny dla serwera ESET PROTECT; moduł SELinux może powodować problemy z innymi aplikacjami).	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`	`zypper install selinux-policy-devel`
samba (opcjonalny, niezbędny tylko w przypadku wdrożenia zdalnego)	`apt-get install samba`	`yum install samba samba-winbind-clients`	`zypper install samba samba-client`
lshw	`apt-get install -y lshw`	`yum install -y lshw`	`zypper install lshw`

Instalacja agenta — system Linux

Wymagania wstępne

- Zalecamy **korzystanie z najnowszej wersji programu OpenSSL 1.1.1**. Wersja OpenSSL 3.x nie jest obsługiwana. Najniższa obsługiwana wersja biblioteki OpenSSL w systemie Linux to openssl-1.0.1e-30. Jednocześnie w systemie może być zainstalowanych więcej wersjiOpenSSL. Co najmniej jedna obsługiwana wersja musi być zainstalowana w systemie.

  - Aby pokazać bieżącą wersję domyślną, możesz użyć polecenia `openssl version`.

  - Możesz też wyświetlić wszystkie wersje biblioteki OpenSSL zainstalowane w systemie. W tym celu sprawdź końcówki nazw plików wyświetlonych przy użyciu polecenia `sudo find / -iname *libcrypto.so*`

  - Można sprawdzić zgodność klienta Linux przy pomocy następującego polecenia: `openssl s_client -`

```
connect google.com:443 -tls1_2
```

- Zainstaluj pakiet `lshw` na komputerze klienta/serwera z systemem Linux, aby agent ESET Management mógł poprawnie sporządzić spis sprzętu.

Dystrybucja Linuksa	Polecenie terminala
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- W przypadku systemu Linux CentOS zalecamy zainstalowanie pakietu `policycoreutils-devel`. Aby zainstalować pakiet, należy uruchomić polecenie:

```
yum install policycoreutils-devel
```

- Wspomagana instalacja serwerowa agenta:
  - Dostępny w sieci komputer pełniący rolę serwera, na którym zainstalowano serwer ESET PROTECT i konsolę internetową ESET PROTECT.
- Instalacja offline agenta:
  - Dostępny w sieci komputer pełniący rolę serwera, na którym zainstalowano serwer ESET PROTECT.
  - Musi istnieć certyfikat dla agenta.
  - Musi istnieć klucz publiczny urzędu certyfikacji.

Instalacja

Wykonaj poniższe czynności, aby zainstalować komponent agenta ESET Management w systemie Linux przy użyciu polecenia Terminal:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Pobierz skrypt instalacji agenta:

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. Spraw, aby plik był wykonywalny:

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

3. Uruchom skrypt instalacji w oparciu o poniższy przykład (nowe wiersze są oddzielone znakiem „\”, co umożliwia skopiowanie całego polecenia do terminala):

Aby uzyskać więcej informacji, zapoznaj się z parametrami poniżej.

Wspomagana instalacja serwerowa

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

Instalacja offline

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

Firma ESET zaleca usunięcie poleceń zawierających poufne dane (na przykład hasło) z historii wiersza poleceń:
1.Uruchom polecenie `history`, aby wyświetlić listę wszystkich poleceń w historii.
2.Uruchom polecenie `history -d line_number` (określ numer wiersza, w którym występuje interesujące Cię polecenie). Możesz też wywołać polecenie `history -c`, aby usunąć całą historię wiersza poleceń.

4. Po wyświetleniu monitu naciśnij **y**, aby zaakceptować certyfikat. Możesz zignorować wszelkie błędy dotyczące SELinux zgłoszone przez instalator.

5. Po zakończeniu instalacji sprawdź, czy usługa agenta ESET Management jest aktywna:

```
sudo systemctl status eraagent
```

6. Ustaw usługę **eraagent** tak, by uruchamiała się podczas rozruchu: `sudo systemctl enable eraagent`

Dziennik instalatora

Dziennik instalatora może się przydać podczas rozwiązywania problemów. Można go znaleźć w plikach dziennika.

Parametry

Połączenie z serwerem ESET PROTECT jest nawiązywane przy użyciu parametrów --hostname oraz --port (port nie jest używany, gdy dostępny jest rekord SRV). Możliwe formaty połączenia.

- **Nazwa hosta** i **port**
- **Adres IPv4** i **port**
- **Adres IPv6** i **port**

• Rekord usługi (rekord SRV) — aby skonfigurować rekord zasobu DNS w systemie Linux, komputer musi należeć do domeny z działającym serwerem DNS. Patrz Rekord zasobu DNS. Rekord SRV musi rozpoczynać się od prefiksu „_NAME._tcp”, gdzie „NAME” odpowiada nazewnictwu niestandardowemu (na przykład „era”).

Atrybut	Opis	Wymagane
`--hostname`	Nazwa hosta lub adres IP serwera ESET PROTECT używana do nawiązania połączenia.	Tak
`--port`	Port serwera ESET PROTECT (wartość domyślna to `2222`).	Tak
`--cert-path`	Ścieżka lokalna do pliku certyfikatu agenta (więcej informacji na temat certyfikatu).	Tak (offline)
`--cert-auth-path`	Ścieżka do pliku urzędu certyfikacji serwera (więcej informacji na temat urzędu).	Tak (offline)
`--cert-password`	Hasło certyfikatu agenta.	Tak (offline)
`--cert-auth-password`	Hasło do urzędu certyfikacji.	Tak (jeśli jest używany)
`--skip-license`	Podczas instalacji użytkownik nie będzie proszony o potwierdzenie umowy licencyjnej.	Nie
`--cert-content`	— zakodowana w formacie Base64 treść zakodowanego w formacie PKCS12 certyfikatu klucza publicznego oraz klucza prywatnego, służącego do zabezpieczania kanałów komunikacyjnych na serwerze i agentach. Należy używać wyłącznie opcji `--cert-path` lub `--cert-content`.	Nie
`--cert-auth-content`	Zakodowana w formacie Base64 treść certyfikatu kodowanego DER klucza prywatnego urzędu certyfikacji, używanego do weryfikacji zdalnych elementów równorzędnych (serwerów lub serwerów proxy). Należy używać wyłącznie opcji `--cert-auth-path` lub `--cert-auth-content`.	Nie
`--webconsole-hostname`	Nazwa hosta lub adres IP używane w konsoli internetowej do łączenia się z serwerem (jeśli wartość ta pozostanie pusta, instalator skopiuje ją z „hostname”).	Nie
`--webconsole-port`	Port używany przez konsolę internetową do nawiązywania połączenia z serwerem (wartość domyślna to `2223`).	Nie
`--webconsole-user`	Nazwa użytkownika używana przez konsolę internetową do nawiązywania połączenia z serwerem (wartość domyślna to `Administrator`). Nie można używać użytkownika z uwierzytelnianiem dwuskładnikowym w instalacjach wspomaganych przez serwer.	Nie
`--webconsole-password`	Hasło używane przez konsolę internetową do łączenia się z serwerem.	Tak (wspomagane przez serwer)
`--proxy-hostname`	Nazwa hosta serwera proxy. Ten parametr powoduje włączenie korzystania z serwera proxy HTTP (który jest już zainstalowany w sieci) na potrzeby replikacji między agentem ESET Management a serwerem ESET PROTECT (nie dotyczy buforowania aktualizacji).	Jeśli używany jest serwer proxy
`--proxy-port`	Port serwera proxy HTTP służący do nawiązywania połączenia z serwerem.	Jeśli używany jest serwer proxy
`--enable-imp-program`	Włącza program ulepszania produktu.	Nie

Atrybut	Opis	Wymagane
`--disable-imp-program`	Wyłącza program ulepszania produktu.	Nie

Połączenie i certyfikaty

- Należy skonfigurować **połączenie z serwerem ESET PROTECT**: `--hostname`, `--port` (port nie jest potrzebny w przypadku podania rekordu usługi; wartość domyślna dla portu to `2222`)
- W przypadku **wspomaganej instalacji serwerowej** należy podać następujące informacje: `--webconsole-port, --webconsole-user, --webconsole-password`
- W przypadku **instalacji offline** należy podać informacje dotyczące certyfikatu: `--cert-path`, `--cert-password`. Parametry instalacji `--cert-path` i `--cert-auth-path` wymagają plików certyfikatów (*.pfx* i *.der*), które można wyeksportować z konsoli internetowej ESET PROTECT. (Zapoznaj się z informacjami o eksportowaniu pliku .pfx i pliku .der).

Parametry typu hasła

Parametry typu hasła można podać w postaci zmiennych środowiskowych, pliku, wartości odczytywanej ze strumienia `stdin` lub podawanej w formie zwykłego tekstu. czyli:

`--password=env:SECRET_PASSWORD`, gdzie`SECRET_PASSWORD` to zmienna środowiskowa zawierająca hasło

`--password=file:/opt/secret`, gdzie hasło zawiera pierwszy wiersz zwykłego pliku `/opt/secret`

`--password=stdin` to instrukcja umożliwiająca instalatorowi odczytanie hasła ze standardowego strumienia wejścia

Zapis `--password="pass:PASSWORD"` jest odpowiednikiem `--password="PASSWORD"` i jest obowiązkowy, jeśli hasło to faktycznie `"stdin"` (wejście standardowe) lub ciąg znaków zaczynający się od `"env:"`, `"file:"` lub `"pass:"`

> ⚠ Hasło do certyfikatu nie może zawierać następujących znaków: `"` `\` Znaki te powodują błąd krytyczny podczas inicjowania agenta.

Połączenie z serwerem proxy HTTP

Jeśli używasz serwera proxy HTTP do replikacji między agentem ESET Management a serwerem ESET PROTECT (nie do buforowania aktualizacji), możesz określić parametry połączenia w `--proxy-hostname` i `--proxy-port`.

PRZYKŁAD – instalacja offline agenta z połączeniem z serwerem proxy HTTP

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
```

```
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

Protokół komunikacji między agentem a serwerem ESET PROTECT nie obsługuje uwierzytelniania. Żadne rozwiązanie proxy używane do przekazywania komunikacji agenta na serwer ESET PROTECT i wymagające uwierzytelniania nie będzie działać.
Jeśli port domyślny używany dla konsoli internetowej lub agenta zostanie zmieniony, może być konieczna korekta ustawień zapory. W przeciwnym razie instalacja może się nie powieść.

Uaktualnianie i naprawianie instalacji agenta w systemie Linux

W przypadku ręcznej instalacji agenta w systemie, w którym agent jest już zainstalowany, mogą wystąpić poniższe sytuacje:

- **Zaktualizuj** — uruchom nowszą wersję instalatora.
  - Wspomagana instalacja serwerowa — aplikacja zostaje uaktualniona, ale nadal używa wcześniejszych certyfikatów.
  - Instalacja offline — aplikacja zostaje uaktualniona i używane są nowe certyfikaty.
- **Napraw** — uruchom tę samą wersję instalatora. Za pomocą tej opcji można przeprowadzić migrację agenta na inny serwer ESET PROTECT.
  - Wspomagana instalacja serwerowa — aplikacja zostaje ponownie zainstalowana, a następnie otrzymuje bieżące certyfikaty z serwera ESET PROTECT (zdefiniowanego przy użyciu parametru `hostname`).
  - Instalacja offline — aplikacja zostaje zainstalowana ponownie i używane są nowe certyfikaty.

Jeśli podczas ręcznego migrowania agenta ze starszego serwera na inny nowszy serwer ESET PROTECT używana jest wspomagana instalacja serwerowa, polecenie instalacji należy uruchomić dwukrotnie. Pierwsze uruchomienie spowoduje uaktualnienie agenta, a drugie uzyskanie nowych certyfikatów, aby agent mógł połączyć się ze serwerem ESET PROTECT.

Instalacja konsoli internetowej — system Linux

Aby zainstalować konsolę internetową ESET PROTECT, należy wykonać poniższe czynności:

Konsolę internetową ESET PROTECT można zainstalować na innym komputerze niż ten, na którym jest zainstalowany serwer ESET PROTECT. Ta procedura wymaga podjęcia dodatkowych kroków.

1. Zainstaluj pakiety Apache Tomcat i Java. Przykłady nazw pakietów podane poniżej mogą się różnić od pakietów w repozytorium używanej dystrybucji systemu Linux.

Dystrybucja Linuksa	Polecenia terminala
Debian i Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOS i Red Hat	`yum update` `yum install java-17-openjdk tomcat`
OpenSUSE	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. Pobierz plik konsoli internetowej (*era.war*):

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. Skopiuj plik *era.war* do folderu usługi Tomcat:

Debian, **Ubuntu**	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, **Red Hat**	`sudo cp era.war /var/lib/tomcat/webapps/`
OpenSUSE	`sudo cp era.war /usr/share/tomcat/webapps/`

4. Uruchom ponownie usługę Tomcat i przeprowadź wdrożenie pliku *era.war*:

Debian, **Ubuntu**	`sudo systemctl restart tomcat9`
CentOS, **Red Hat**	`sudo systemctl restart tomcat`
OpenSUSE	`sudo systemctl restart tomcat`

5. Sprawdź, czy folder *era* znajduje się w folderze Tomcat:

Debian, **Ubuntu**	`ls /var/lib/tomcat9/webapps`
CentOS, **Red Hat**	`ls /var/lib/tomcat/webapps`
OpenSUSE	`ls /usr/share/tomcat/webapps`

Dane wyjściowe powinny wyglądać następująco: `era era.war`

6. Ustaw usługę Tomcat, by uruchamiała się podczas rozruchu: `sudo systemctl enable tomcat` (lub `tomcat9` na podstawie nazwy usługi)

7. Jeśli konsola internetowa ESET PROTECT została zainstalowana na innym komputerze niż ten, na którym znajduje się serwer ESET PROTECT, postępuj zgodnie z poniższymi dodatkowymi instrukcjami w celu włączenia komunikacji między konsolą internetową ESET PROTECT a serwerem ESET PROTECT:

a)Zatrzymaj usługę Tomcat: `sudo systemctl stop tomcat`

b)Edytuj plik *EraWebServerConfig.properties*:

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

Jeśli plik *EraWebServerConfig.properties* nie znajduje się w powyższej lokalizacji, użyj poniższego polecenia, aby

go zlokalizować w swoim systemie:

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

c)Znajdź ciąg `server_address=localhost`

d)Część `localhost` zastąp adresem IP serwera ESET PROTECT i zapisz plik.

e)Uruchom ponownie usługę Tomcat: `sudo systemctl restart tomcat` (lub `tomcat9` na podstawie nazwy usługi)

f)Ustaw usługę Tomcat, by uruchamiała się podczas rozruchu: `sudo systemctl enable tomcat` (lub `tomcat9` na podstawie nazwy usługi)

8. Otwórz konsolę internetową ESET PROTECT w obsługiwanej przeglądarce internetowej, aby wyświetlić ekran logowania:

• Z komputera obsługującego konsolę internetową ESET PROTECT: *http://localhost:8080/era*

• Z dowolnego komputera z dostępem do internetu i konsoli internetowej ESET PROTECT (zastąp *IP_ADDRESS_OR_HOSTNAME* adresem IP lub nazwą hosta konsoli ESET PROTECT): *http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. Skonfiguruj konsolę internetową po instalacji:

• Domyślną wartością portu HTTP podczas ręcznej instalacji serwera Apache Tomcat jest 8080. Zalecamy skonfigurowanie połączenia HTTPS dla serwera Apache Tomcat.

• Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Instalacja narzędzia rogue detection sensor – Linux

Jeśli istnieje wiele segmentów sieci, Rogue Detection Sensor musi być zainstalowany osobno w każdym segmencie sieci, aby uzyskać pełną listę wszystkich urządzeń w całej sieci.

Wymagania wstępne

• Sieć z możliwością wyszukiwania (otwarte porty, komunikacja przychodząca nieblokowana przez zaporę itd.).

• Można nawiązać połączenie z komputerem będącym serwerem.

• Agent ESET Management musi być zainstalowany na komputerze lokalnym, aby wszystkie funkcje programu były w pełni obsługiwane.

• Otwarty terminal.

• Konfiguracja pliku instalacyjnego narzędzia RD Sensor jako pliku wykonywalnego:

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

Instalacja

Wykonaj poniższe czynności, aby zainstalować narzędzie RD Sensor w systemie Linux przy użyciu polecenia Terminal:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Wpisz poniższe polecenie, by uruchomić plik jako program sudo:

```
sudo ./rdsensor-linux-x86_64.sh
```

2. Zapoznaj się z Umową licencyjną użytkownika końcowego. Użyj **spacji**, aby przejść do następnej strony tej umowy.
Instalator wyświetli monit z pytaniem, czy akceptujesz umowę. Naciśnij klawisz **Y** na klawiaturze, jeśli ją akceptujesz. W przeciwnym razie naciśnij **N**.

3. Naciśnij klawisz **T**, jeśli zgadzasz się na uczestnictwo w programie ulepszania produktu. W przeciwnym razie naciśnij **N**.

4. Po zakończeniu instalacji zostanie uruchomiony komponent ESET Rogue Detection Sensor.

5. Aby sprawdzić poprawność instalacji, należy zweryfikować działanie usługi, wpisując następujące polecenie:

```
sudo systemctl status rdsensor
```

6. Plik dziennika Rogue Detection Sensor można znaleźć w plikach dziennika:

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

Instalacja narzędzia Moduł zarządzania urządzeniami mobilnymi — system Linux

Narzędzie Moduł zarządzania urządzeniami mobilnymi można zainstalować na serwerze innym niż serwer, na którym zainstalowane jest rozwiązanie ESET PROTECT. Na przykład można użyć tego scenariusza instalacji, aby Mobile Device Connector był dostępny przez Internet, aby na stałe umożliwić zarządzanie urządzeniami mobilnymi użytkowników.

Wykonaj poniższe czynności, aby zainstalować komponent Mobile Device Connector w systemie Linux przy użyciu polecenia Terminal:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczącеinstalacji.

1. Pobierz skrypt instalacyjny Mobile Device Connector:

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. Uruchom skrypt instalacji w oparciu o poniższy przykład (nowe wiersze są oddzielone znakiem „\”, co

umożliwia skopiowanie całego polecenia do terminala):

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--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
```

Aby uzyskać pełną listę dostępnych parametrów (wydrukować komunikat pomocy), użyj polecenia:

```
--help
```

> Firma ESET zaleca usunięcie poleceń zawierających poufne dane (na przykład hasło) z historii wiersza poleceń:
> 1.Uruchom polecenie `history`, aby wyświetlić listę wszystkich poleceń w historii.
> 2.Uruchom polecenie `history -d line_number` (określ numer wiersza, w którym występuje interesujące Cię polecenie). Możesz też wywołać polecenie `history -c`, aby usunąć całą historię wiersza poleceń.

Wymagane parametry polecenia instalacji

Wiele parametrów instalacji ma charakter opcjonalny, jednak niektóre z nich są wymagane:

- Certyfikat równorzędny — istnieją dwie metody, aby uzyskać certyfikat równorzędny dla produktu ESET PROTECT:

  - **Wspomagana instalacja serwerowa** — podaj poświadczenia administratora konsoli internetowej ESET PROTECT (instalator automatycznie pobierze wymagane certyfikaty).

  - **Instalacja offline**— należy podać certyfikat równorzędny (certyfikat serwera proxy wyeksportowany z programu ESET PROTECT). Można też użyć certyfikatu niestandardowego.

  oW przypadku **wspomaganej instalacji serwerowej** należy podać przynajmniej:

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

  oW przypadku **instalacji offline** należy podać:

  ```
  --cert-path=
  --cert-password=
  ```

(Domyślny certyfikat agenta utworzony podczas instalacji serwera ESET PROTECT nie wymaga hasła).

- Certyfikat HTTPS (proxy):

  - Jeśli masz już certyfikat HTTPS:

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

  - Aby wygenerować nowy certyfikat HTTPS:

```
--https-cert-generate
--mdm-hostname=
```

- Połączenie z serwerem ESET PROTECT (nazwa lub adres IP):

```
--hostname=
```

- Połączenie z bazą danych:

  - W przypadku bazy danych MySQL należy podać:

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

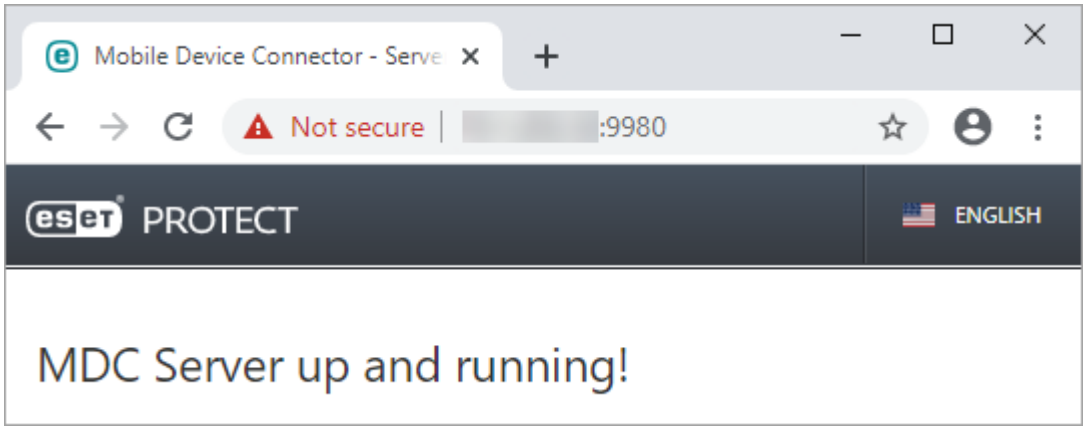
  - Dla bazy danych MS SQL należy podać:

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

Dziennik instalatora

Dziennik instalatora może być przydatny do rozwiązywania problemów i można go znaleźć w plikach dziennika.

Po ukończeniu instalacji sprawdź, czy narzędzie Moduł zarządzania urządzeniami mobilnymi działa prawidłowo, otwierając w przeglądarce internetowej łącze *https://nazwa-hosta-mdm:port-rejestracji* (np. *https://eramdm:9980*). Jeśli instalacja przebiegła prawidłowo, wyświetlony zostanie następujący komunikat:



Przy użyciu tego adresu URL można również sprawdzić dostępność serwera narzędzia Moduł zarządzania urządzeniami mobilnymi w Internecie (jeśli zastosowano taką konfigurację), przechodząc pod ten adres na urządzeniu mobilnym. Jeśli strona okaże się niedostępna, należy sprawdzić ustawienia zapory oraz inne elementy konfiguracji infrastruktury sieciowej.

Wymagania wstępne dotyczące komponentu Moduł zarządzania urządzeniami mobilnymi — system Linux

W celu zainstalowania komponentu Moduł zarządzania urządzeniami mobilnymi w systemie Linux niezbędne jest spełnienie następujących wymagań wstępnych:

- Zainstalowany i skonfigurowany serwer bazy danych z kontem użytkownika root (przed instalacją nie trzeba tworzyć konta użytkownika, ponieważ może je utworzyć instalator).
- Sterownik ODBC do obsługi połączenia z serwerem bazy danych (MySQL/MS SQL) zainstalowany na komputerze. Zapoznaj się z rozdziałem Instalacja i konfiguracja sterownika ODBC.

> Należy użyć pakietu `unixODBC_23` (nie domyślnego pakietu `unixODBC`) w celu połączenia komponentu MDC z bazą danych MySQL bez żadnych problemów. Dotyczy to w szczególności systemu SUSE Linux.

> Zalecamy wdrożenie komponentu MDM na innym urządzeniu hosta niż to, na którym jest hostowany serwer ESET PROTECT.

- Skonfigurowanie pliku instalacyjnego usługi MDMCore jako pliku wykonywalnego.

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

- Po instalacji należy sprawdzić, czy usługa MDMCore jest uruchomiona.

```
sudo systemctl status eramdmcore
```

- Zalecamy **korzystanie z najnowszej wersji programu OpenSSL 1.1.1**. Wersja OpenSSL 3.x nie jest obsługiwana. Najniższa obsługiwana wersja biblioteki OpenSSL w systemie Linux to openssl-1.0.1e-30. Jednocześnie w systemie może być zainstalowanych więcej wersjiOpenSSL. Co najmniej jedna obsługiwana wersja musi być zainstalowana w systemie.
  - Aby pokazać bieżącą wersję domyślną, możesz użyć polecenia `openssl version`.
  - Możesz też wyświetlić wszystkie wersje biblioteki OpenSSL zainstalowane w systemie. W tym celu

sprawdź końcówki nazw plików wyświetlonych przy użyciu polecenia `sudo find / -iname *libcrypto.so*`

oMożna sprawdzić zgodność klienta Linux przy pomocy następującego polecenia: `openssl s_client -connect google.com:443 -tls1_2`

Jeśli baza danych MDM w programie MySQL jest zbyt duża (tysiące urządzeń), domyślna wartość `innodb_buffer_pool_size` będzie za mała. Więcej informacji na temat optymalizacji bazy danych można znaleźć pod tym adresem: https://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

Wymagania dotyczące certyfikatu

• Bezpieczna komunikacja przy użyciu protokołu HTTPS wymaga **certyfikatu SSL** w formacie *.pfx*. Zalecamy użycie certyfikatu dostarczonego przez niezależny urząd certyfikacji. Certyfikaty podpisane samodzielnie (w tym te podpisane przez urząd certyfikacji ESET PROTECT) nie są zalecane, ponieważ nie wszystkie urządzenia mobilne umożliwiają użytkownikom akceptowanie takich certyfikatów.

• Wymagane są: certyfikat podpisany przy użyciu urzędu certyfikacji, odpowiedni klucz prywatny oraz stosowanie standardowych procedur (zwykle z użyciem biblioteki OpenSSL), aby można było scalić oba elementy w jeden plik *.pfx*:
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
To standardowa procedura w przypadku większości serwerów używających certyfikatów SSL.

• W przypadku instalacji offline potrzebny jest też certyfikat równorzędny (**certyfikat agenta** wyeksportowany z programu ESET PROTECT). W programie ESET PROTECT można również użyć certyfikatu niestandardowego.

Instalacja serwera proxy Apache HTTP — system Linux

Agenty ESET Management mogą łączyć się z serwerem ESET PROTECT przy użyciu rozwiązania Apache HTTP Proxy. Zapoznaj się z dodatkowymi informacjami na temat używania serwera proxy z agentami ESET Management.

Apache HTTP Proxy Jest powszechnie dystrybuowany jako pakiet `apache2` lub `httpd`.

Wybierz procedurę instalacji serwera proxy Apache HTTP na podstawie dystrybucji systemu Linux używanej na serwerze: Jeśli serwer Apache ma także buforować wyniki z ESET LiveGuard Advanced, zapoznaj się z odpowiednią dokumentacją.

Instalacja serwera proxy Apache HTTP w systemie Linux (dystrybucja ogólna)

1. Zainstaluj serwer Apache HTTP (co najmniej w wersji 2.4.10).

2. Sprawdź, czy załadowane są następujące moduły:

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

3. Dodaj konfigurację buforowania:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Jeśli katalog */var/cache/apache2/mod_cache_disk* nie istnieje, utwórz go i nadaj mu uprawnienia serwera Apache (r, w, x).

5. Dodaj konfigurację serwera proxy:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900


SetEnv proxy-initial-not-pooled 1


<VirtualHost *:3128>

ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

ServerName r.edtd.eset.com


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

Require all denied

</If>


ProxyRequests Off

CacheEnable disk /

SSLProxyEngine On


RequestHeader set Front-End-Https "On"
```

```
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0

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

</VirtualHost>


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

6. Do komunikacji z agentem ESET Management jest używany domyślnie port 2222. W przypadku zmiany portu podczas instalacji należy podać zmieniony numer portu. Zmień ciąg 2222 w wierszu `AllowCONNECT 443 563 2222 8883 53535` na swój numer portu.

7. Włącz dodaną konfigurację buforowania serwera proxy (jeśli konfiguracja jest zawarta w głównym pliku konfiguracyjnym serwera Apache, można pominąć ten krok).

8. W razie potrzeby zmień port nasłuchu (domyślnie ustawiony jest port 3128).

9. Opcjonalne uwierzytelnianie podstawowe:

- Dodaj konfigurację uwierzytelniania do dyrektywy serwera proxy:

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

- Utwórz plik hasła przy użyciu polecenia `/etc/httpd/.htpasswd -c`
- Ręcznie utwórz plik o nazwie group.file z elementem `usergroup:username`

10. Uruchom ponownie serwer Apache HTTP.

Instalacja serwera proxy Apache HTTP w systemie Ubuntu Server oraz w innych dystrybucjach systemu Linux opartych na systemie Debian

1. Zainstaluj najnowszą wersję serwera Apache HTTP z odpowiedniego repozytorium:

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

2. Wykonaj poniższe polecenie w celu załadowania wymaganych modułów serwera Apache:

```
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. Edytuj plik konfiguracji buforowania serwera Apache:

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

oraz skopiuj i wklej następującą konfigurację:

```
CacheEnable disk http://
CacheDirLevels 4
CacheDirLength 2
CacheDefaultExpire 3600
CacheMaxFileSize 500000000
CacheMaxExpire 604800
CacheQuickHandler Off
CacheRoot /var/cache/apache2/mod_cache_disk
```

4. Ten krok powinien być opcjonalny, jednak w razie braku katalogu buforowania uruchom następujące polecenia:

```
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. Edytuj plik konfiguracji serwera proxy Apache:

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

oraz skopiuj i wklej następującą konfigurację:

```
AllowCONNECT 443 563 2222 8883 53535


ProxyRequests On
ProxyVia On


CacheLock on

CacheLockMaxAge 10

ProxyTimeOut 900


SetEnv proxy-initial-not-pooled 1


<VirtualHost *:3128>

ProxyRequests On

</VirtualHost>


<VirtualHost *:3128>

        ServerName r.edtd.eset.com


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

```
Require all denied
</If>


ProxyRequests Off
CacheEnable disk /
SSLProxyEngine On


RequestHeader set Front-End-Https "On"
ProxyPass / https://r.edtd.eset.com/ timeout=300 keepalive=On ttl=100 max=100 smax=1
0
ProxyPassReverse / http://r.edtd.eset.com/ keepalive=On
</VirtualHost>


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

6. Do komunikacji z agentem ESET Management jest używany domyślnie port 2222. W przypadku zmiany portu podczas instalacji należy podać zmieniony numer portu. Zmień ciąg 2222 w wierszu `AllowCONNECT 443 563 2222 8883 53535` na swój numer portu.

7. Włącz pliki konfiguracyjne edytowane w poprzednich krokach:

```
sudo a2enconf cache_disk.conf proxy.conf
```

8. Zmień port nasłuchiwania serwera Apache HTTP na port 3128. Edytuj plik */etc/apache2/ports.conf* i zastąp element `Listen 80` elementem `Listen 3128`.

9. Opcjonalne uwierzytelnianie podstawowe:

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

- Skopiuj i wklej konfigurację uwierzytelniania przed elementem `</Proxy>`

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

- Zainstaluj element apache2-utils i utwórz nowy plik hasła (na przykład username: user, group: usergroup):

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

- Utwórz plik o nazwie group:

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

Skopiuj i wklej następujący wiersz:

usergroup:user
```

10. Uruchom ponownie serwer Apache HTTP przy użyciu następującego polecenia:

```
sudo systemctl restart apache2
```

Przekazywanie jedynie w ramach komunikacji z produktami ESETAby zezwolić tylko na przekazywanie w ramach komunikacji z produktami ESET, usuń następujący wpis:

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

I dodaj następujący wpis:

```
<Proxy *>

Deny from all

</Proxy>


#*.eset.com:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.eu:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#*.eset.systems:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-
Z0-9-
]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>

Allow from all
```

```
</ProxyMatch>


#Antispam module (ESET Mail Security only):

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-
rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-
uk11.mailshell.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#Services (activation)

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-
pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#ESET servers accessed directly via IP address:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.2
28.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>


#AV Cloud over port 53535

<ProxyMatch ^.*e5.sk.*$>

Allow from all

</ProxyMatch>
```

Przekazywanie całej komunikacji

Aby zezwolić na przekazywanie całej komunikacji, dodaj następujący wpis:

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

i usuń następujący wpis:

```
<Proxy *>

Deny from all

</Proxy>
```

```
#*.eset.com:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[c,C][o,O][m,M](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#*.eset.eu:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-]{0,63}\.[e,E][s,S][e,E][t,T]\.[e,E][u,U](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#*.eset.systems:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?([a-zA-Z0-9-]{0,63}\.)?[a-zA-Z0-9-
]{0,63}\.[e,E][s,S][e,E][t,T]\.[s,S][y,Y][s,S][t,T][e,E][m,M][s,S](:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#Antispam module (ESET Mail Security only):

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(ds1-uk-rules-1.mailshell.net|ds1-uk-rules-2.mailshell.net|ds1-uk-rules-3.mailshell.net|fh-uk11.mailshell.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#Services (activation)

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(edf-pcs.cloudapp.net|edf-pcs2.cloudapp.net|edfpcs.trafficmanager.net)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#ESET servers accessed directly via IP address:

<ProxyMatch ^([h,H][t,T][t,T][p,P][s,S]?://)?([^@/]*@)?(91.228.165.|91.228.166.|91.228.167.|38.90.226.)([0-9]+)(:[0-9]+)?(/.*)?$>

Allow from all

</ProxyMatch>



#AV Cloud over port 53535
```

```
<ProxyMatch ^.*e5.sk.*$>
Allow from all
</ProxyMatch>
```

Tworzenie łańcucha na serwerze proxy (cały ruch)

Program ESET PROTECT nie obsługuje łańcuchów serwerów proxy, w których serwery proxy wymagają uwierzytelnienia. Można użyć własnego rozwiązania do obsługi sieci przezroczystych serwerów proxy, jednak może ono wymagać dodatkowej konfiguracji, której nie omówiono w niniejszym dokumencie. Dodaj poniższy wiersz do konfiguracji serwera proxy (hasło działa wyłącznie w przypadku podrzędnego serwera proxy):

```
<VirtualHost *:3128>
ProxyRequests On
ProxyRemote * http://IP_ADDRESS:3128
</VirtualHost>
```

W przypadku korzystania z łańcucha na serwerze proxy na urządzeniu wirtualnym ESET PROTECT należy zmodyfikować politykę SELinux. Na urządzeniu wirtualnym ESET PROTECT należy otworzyć terminal i uruchomić następujące polecenie:

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

Konfigurowanie serwera proxy HTTP dla dużej liczby klientów

Jeśli używasz 64-bitowego serwera proxy Apache HTTP, możesz zwiększyć limit wątków swojego serwera Apache HTTP Proxy. Edytuj plik konfiguracyjny *httpd.conf* w folderze Apache HTTP Proxy. Znajdź następujące ustawienia w pliku i zaktualizuj wartości, aby dopasować je do liczby klientów.

Zamień przykładową wartość `5000` potrzebną liczbą. Maksymalna wartość to `32000`.

```
ThreadLimit 5000
ThreadsPerChild 5000
```

Nie zmieniaj pozostałej części pliku.

Skonfiguruj serwer proxy Apache HTTP na potrzeby przekazywania połączeń między agentem a serwerem

1. Na komputerze z serwerem proxy otwórz plik

   i. Dystrybucje Debian
   `/etc/apache2/mods-available/proxy.conf`

   ii. Dystrybucje Red Hat
   `/etc/httpd/conf/httpd.conf`

2. Dodaj następujące wiersze na końcu pliku:

```
AllowCONNECT 443 563 2222 8883 53535
```

3.Na komputerze z serwerem proxy otwórz plik

i.Dystrybucje Debian
`/etc/apache2/apache2.conf`

ii.Dystrybucje Red Hat
`/etc/httpd/conf/httpd.conf`

4.Znajdź wiersz:
`Listen 80`
i zmień go na wiersz
`Listen 3128`

5.Jeśli dodano ograniczenia dotyczące adresów IP w konfiguracji serwera proxy (krok 1), musisz zezwolić na dostęp do serwera ESET PROTECT:

Dodaj oddzielny segment `ProxyMatch`:
I.Adres używany przez agenty do nawiązywania połączenia z serwerem ESET PROTECT.

II.Wszystkie pozostałe adresy serwera ESET PROTECT (IP, FQDN)
(Dodaj cały poniższy kod — adres IP 10.1.1.10 i nazwa hosta `hostname.example` to tylko przykłady, które należy zastąpić własnymi adresami. Możesz też wygenerować wyrażenie `ProxyMatch` zgodnie z tym artykułem w bazie wiedzy).

```
<ProxyMatch ^(hostname\.example(:[0-9]+)?(\/.*)?|10\.1\.1\.10(:[0-9]+)?(\/.*)?)$>

Allow from all

</ProxyMatch>
```

6.Uruchom ponownie usługę *Apache HTTP Proxy*.

Konfiguruj buforowanie

Za pomocą htcachceclean można skonfigurować rozmiar i czyszczenie pamięci podręcznej Apache HTTP Proxy. Zobacz instrukcje konfiguracji pamięci podręcznej dla urządzenia wirtualnego ESET PROTECT.

Ustawienie SELinux

W przypadku korzystania z serwera proxy na urządzeniu wirtualnym ESET PROTECT należy zmodyfikować politykę SELinux (inne dystrybucje systemu Linux mogą mieć to samo wymaganie). Na urządzeniu wirtualnym ESET PROTECT należy otworzyć terminal i uruchomić następujące polecenie:

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

sudo semanage port -a -t http_port_t -p tcp 2222
```

Instalowanie serwera proxy Squid HTTP w systemie Ubuntu Server

W systemie Ubuntu Server można użyć oprogramowania Squid serwera proxy zamiast serwera Apache. W celu zainstalowania oprogramowania Squid w systemie Ubuntu Server (oraz podobnych dystrybucjach systemu Linux opartych na systemie Debian) należy wykonać poniższe czynności:

1. Zainstaluj pakiet Squid3:

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

2. W pliku konfiguracyjnym oprogramowania Squid */etc/squid3/squid.conf* zamień wpis:

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

na wpis:

```
cache_dir ufs /var/spool/squid3 3000 16 256 max-size=200000000
```

i
- Można też zmienić łączny rozmiar pamięci podręcznej (w tym przykładzie jest to 3000 MB) oraz liczbę podkatalogów pierwszego poziomu (w tym przykładzie jest to 16) i podkatalogów drugiego poziomu (w tym przykładzie jest to 256) w katalogu pamięci podręcznej.
- Parametr `max-size` definiuje maksymalny rozmiar pliku w pamięci podręcznej (w bajtach).

3. Zatrzymaj usługę squid3.

```
sudo systemctl stop squid3
sudo squid3 –z
```

4. Ponownie edytuj plik konfiguracyjny oprogramowania Squid i dodaj element `http_access allow all` przed elementem `http_access deny all`, aby zezwolić wszystkim klientom na dostęp do serwera proxy.

5. Uruchom ponownie usługę squid3:

```
sudo systemctl restart squid3
```

Narzędzie Mirror Tool — system Linux

Czy jesteś użytkownikiem systemu Windows?

Narzędzie Mirror Tool jest potrzebne w przypadku aktualizacji silnika detekcji. Jeśli komputery klienckie nie mają połączenia z Internetem, a trzeba na nich zainstalować aktualizacje silnika detekcji, przy użyciu narzędzia Mirror Tool można pobrać pliki aktualizacji z serwerów aktualizacji firmy ESET, aby przechowywać je lokalnie.

i
Narzędzie Mirror Tool pobiera tylko aktualizacje silnika detekcji i innych modułów programu. Nie pobiera aktualizacji komponentów programu ani danych systemu ESET LiveGrid®. Tworzy też pełne repozytorium offline. Można też zaktualizować poszczególne produkty.

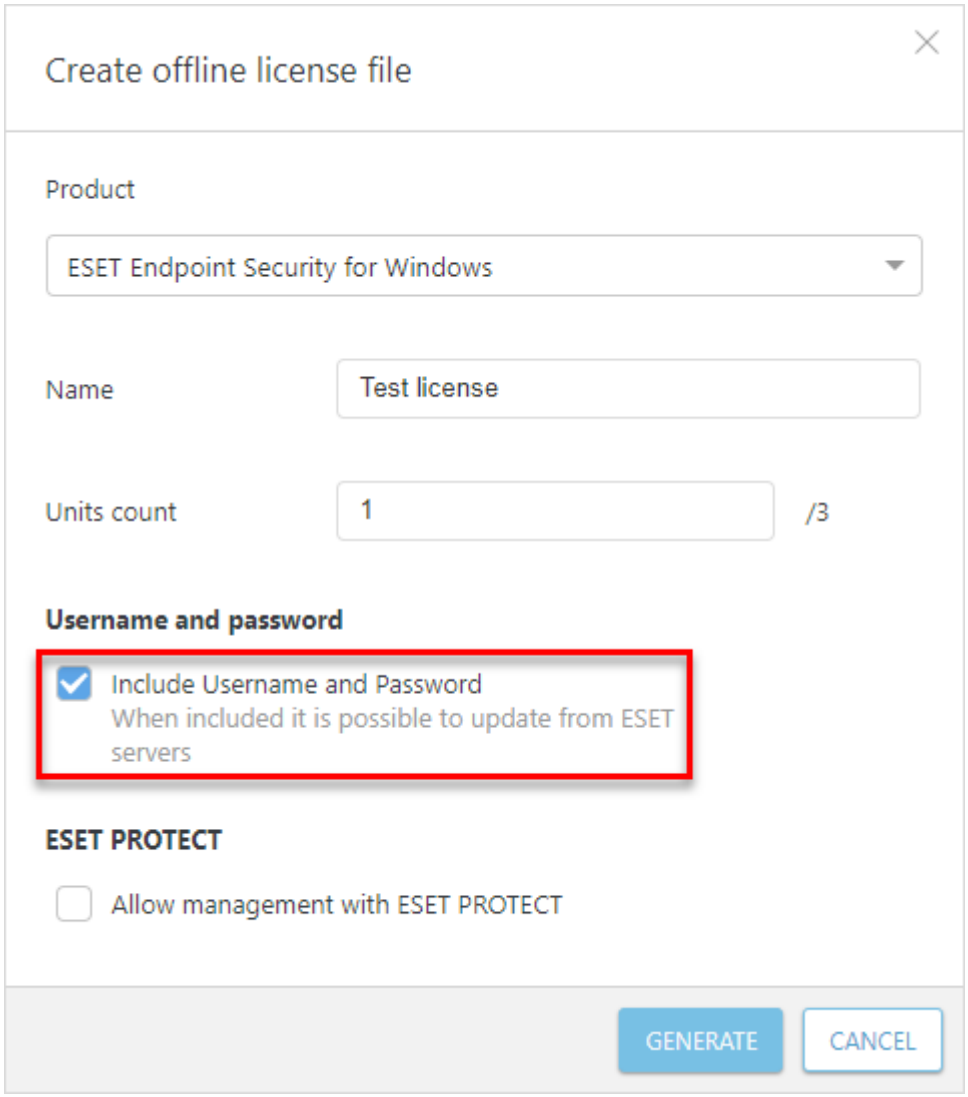
Wymagania wstępne

• Należy udostępnić folder docelowy przy użyciu usługi Samba/Windows lub HTTP/FTP — zależnie od tego jak mają zostać udostępnione aktualizacje.

oProdukty zabezpieczające ESET dla systemu Windows — można je aktualizować zdalnie za pomocą protokołu HTTP lub folderu udostępnionego.

oProdukty zabezpieczające ESET dla systemów Linux/macOS — można je aktualizować zdalnie tylko za pomocą protokołu HTTP. W przypadku używania folderu udostępnionego musi on znajdować się na tym samym komputerze co produkt zabezpieczający ESET.

• Potrzebny jest prawidłowy plik licencji offline zawierający nazwę i hasło użytkownika. Podczas generowania pliku licencji należy pamiętać o zaznaczeniu pola wyboru **Uwzględniaj nazwę użytkownika i hasło**. Należy również wprowadzić **nazwę licencji**. Plik licencji offline jest wymagany do aktywacji narzędzia Mirror Tool i wygenerowania kopii dystrybucyjnej aktualizacji.



Jak korzystać z narzędzia Mirror Tool

1.Pobierz narzędzie Mirror Tool ze strony pobierania firmy ESET (w sekcji z **instalatorami autonomicznymi**).

2.Rozpakuj pobrane archiwum.

3.Otwórz terminal w folderze zawierającym plik *MirrorTool* i spraw, aby plik był wykonywalny:

```
chmod +x MirrorTool
```

4.Uruchom poniższe polecenie, aby wyświetlić wszystkie dostępne parametry narzędzia Mirror Tool i jego wersji:

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. 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. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --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.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

Wszystkie filtry uwzględniają wielkość liter.

Parametr	Opis
`--updateServer`	W przypadku jego użycia należy też określić adres URL serwera aktualizacji.
`--offlineLicenseFilename`	Należy określić ścieżkę do pliku licencji offline (zgodnie z powyższymi informacjami).
`--mirrorOnlyLevelUpdates`	Nie wymaga argumentu. Po skonfigurowaniu pobierane będą tylko aktualizacje poziomowe (nanoaktualizacje nie zostaną pobrane). Więcej informacji o typach aktualizacji można przeczytać w naszym artykule bazy wiedzy.
`--mirrorFileFormat`	⚠ Przed użyciem parametru `--mirrorFileFormat` upewnij się, że środowisko nie zawiera zarówno starszych (6.5 i starszych), jak i nowszych (6.6. i nowszych) wersji produktów zabezpieczających firmy ESET. Nieprawidłowe użycie tego parametru może spowodować nieprawidłowe aktualizacje produktów zabezpieczających firmy ESET. Można określić, jaki typ plików aktualizacji zostanie pobrany. Możliwe wartości (z uwzględnieniem wielkości liter): • `dat` — użyj tej wartości, jeśli środowisko jest dostępne tylko w produkcie zabezpieczającym ESET w wersji 6.5 lub starszej. • `dll` — użyj tej wartości, jeśli środowisko jest dostępne tylko w produkcie zabezpieczającym ESET w wersji 6.6 lub starszej. Parametr jest ignorowany podczas tworzenia kopii dystrybucyjnych starszych produktów (`ep4` , `ep5`).
`--compatibilityVersion`	Ten opcjonalny parametr dotyczy narzędzia Mirror Tool dystrybuowanego z ESET PROTECT 8.1 i nowszymi wersjami. Narzędzie Mirror Tool pobierze pliki aktualizacji zgodne z wersją repozytorium ESET PROTECT określoną w argumencie parametru w formacie `x.x` lub `x.x.x.x`, na przykład: `--compatibilityVersion 9.1` lub `--compatibilityVersion 8.1.13.0`.

ℹ Aby zmniejszyć ilość danych ładowanych z repozytorium ESET, zalecamy użycie nowych parametrów w narzędziu Mirror Tool dystrybuowanym z ESET PROTECT 9: `--filterFilePath` i `--dryRun`:
1.Utwórz filtr w formacie *JSON* (patrz `--filterFilePath` poniżej).
2.Wykonaj próbne uruchomienie narzędzia Mirror Tool, używając parametru `--dryRun` (patrz poniżej) i dostosuj filtr w razie potrzeby.
3.Uruchom narzędzie Mirror Tool z parametrem `--filterFilePath` i zdefiniowanym filtrem pobierania wraz z parametrami `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`.
4.Regularnie uruchamiaj narzędzie Mirror Tool, aby zawsze korzystać z najnowszych instalatorów.

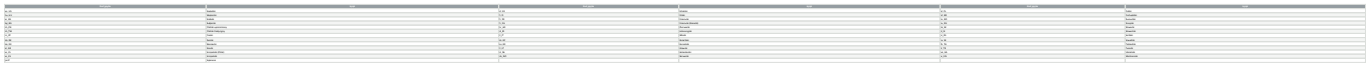
Parametr	Opis

`--filterFilePath`	Użyj tego opcjonalnego parametru, aby filtrować produkty zabezpieczające ESET na podstawie pliku tekstowego w formacie *JSON* umieszczonego w tym samym folderze co Mirror Tool, na przykład: `--filterFilePath filter.txt`)
	Opis konfiguracji filtra:
	Format pliku konfiguracyjnego do filtrowania produktów to *JSON* on następującej strukturze:
	• Obiekt główny *JSON*:
	o`use_legacy` (boolean, opcjonalnie) — jeśli ma wartość true, starsze produkty zostaną uwzględnione.
	o`defaults` (*JSON* obiekt, opcjonalnie) — definiuje właściwości filtra, które będą stosowane do wszystkich produktów.
	■`languages` (lista) — określa kody ISO języków, które mają być uwzględniane, na przykład dla francuskiego wpisz `"fr_FR"`. Pozostałe kody języków znajdują się w poniższej tabeli. Aby wybrać więcej języków, oddziel je przecinkami i spacjami. Na przykład: (`["en_US", "zh_TW", "de_DE"]`)
	■`platforms` (lista) — platformy do włączenia (`["x64", "x86", "arm64"]`).
	Używaj filta `platforms` ostrożnie. Jeśli na przykład narzędzie Mirror Tool pobierze tylko instalatory 64-bitowe, a w infrastrukturze znajdują się komputery 32-bitowe, 64-bitowe produkty zabezpieczające ESET nie zostaną zainstalowane na komputerach 32-bitowych.
	■`os_types` (lista) — rodzaje systemów operacyjnych do włączenia (`["windows"]`, `["linux"]`, `["mac"]`).
	o`products` (lista obiektów JSON, opcjonalnie) — filtry do zastosowania do określonych produktów — nadpisanie wartości `defaults` dla określonych produktów. Obiekty mają następujące właściwości:
	■`app_id` (ciąg znaków) — wymagany, jeśli nie określono `name`.
	■`name` (ciąg znaków) — wymagany, jeśli nie określono `app_id`.
	■`version` (ciąg znaków) — określa wersję lub zakres wersji do uwzględnienia.
	■`languages` (lista) — kody ISO języków, które należy uwzględnić (patrz tabela poniżej).
	■`platforms` (lista) — platformy do włączenia (`["x64", "x86", "arm64"]`).
	■`os_types` (lista) — rodzaje systemów operacyjnych do włączenia (`["windows"]`, `["linux"]`, `["mac"]`).
	Aby określić odpowiednie wartości dla pól, uruchom narzędzie Mirror Tool w trybie suchego przebiegu i znajdź odpowiedni produkt w utworzonym pliku CSV.
	Opisy formatu ciągu znaków określającego wersję
	Wszystkie numery wersji składają się z czterech liczb oddzielonych kropkami (na przykład `7.1.0.0`). Możesz określić mniej liczb podczas wprowadzania filtrów wersji (na przykład `7.1`), a reszta liczb będzie równa zero (`7.1` to to samo, co `7.1.0.0`).
	Ciąg znaków określający wersję może mieć jeden z dwóch następujących formatów:
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	oWybiera wersje większe/mniejsze lub równe/mniejsze lub równe/równe w stosunku do wskazanej wersji.
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	oWybiera wersje, które są większe lub równe progowi dolnemu i mniejsze lub równe progowi górnemu.
	Porównania są wykonywane numerycznie na każdej części numeru wersji, od lewej do prawej.
	Przykład JSON
	`{`
	`"use_legacy": true,`
	`"defaults": {`
	`"languages": [ "en_US" ],`
	`"platforms": [ "x64", "x86" ]`
	`},`
	`"products": [`
	`{`
	`"app_id": "com.eset.apps.business.ees.windows",`
	`"version": "7.1.0.0 - 8.0.0.0"`
	`},`
	`{`
	`"app_id": "com.eset.apps.business.eea.windows",`
	`"version": ">7.1.0.0"`
	`}`
	`]`
	`}`
	Parametr `--filterFilePath` zastępuje parametry `--languageFilterForRepository` i `--productFilterForRepository` `--downloadLegacyForRepository` używane w starszych wersjach narzędzia Mirror Tool (wydanych z ESET PROTECT 8.x).

Parametr	Opis
`--dryRun`	Po użyciu tego opcjonalnego parametru narzędzie Mirror Tool nie pobierze żadnych plików, ale wygeneruje plik *.csv* z listą wszystkich pakietów, które zostaną pobrane. Możesz użyć tego parametru bez obowiązkowych parametrów `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`, na przykład: `MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv`. ℹ Niektóre instalatory ESET są niezależne od języka (mają kod języka `multilang`), a narzędzie Mirror Tool wyświetli je w pliku *.csv*, nawet jeśli określisz `języki` w parametrze `--filterFilePath`. Jeśli użyjesz parametru `--dryRun`, a także parametrów `--intermediateRepositoryDirectory` i `--outputRepositoryDirectory`, narzędzie Mirror Tool nie wyczyści repozytorium *outputRepositoryDirectory*.
`--listUpdatableProducts`	Wyświetla wszystkie produkty ESET, dla których narzędzie Mirror Tool może pobrać aktualizacje modułu (chyba że jest używany parametr `--excludedProducts`). Parametr jest dostępny w wersjach narzędzia Mirror Tool: 1.0.1294.0 (Windows), 1.0.2226.0 (Linux).

Struktura folderów tworzona przez narzędzie Mirror Tool różni się od struktury tworzonej w kopii dystrybucyjnej oprogramowania Endpoint. W każdym folderze znajdują się pliki aktualizacji dla grupy produktów. W ustawieniach aktualizacji produktu za pomocą kopii dystrybucyjnej należy podać pełną ścieżkę do prawidłowego folderu.
Na przykład w celu przeprowadzenia aktualizacji oprogramowania ESET PROTECT 9. z kopii dystrybucyjnej jako Serwer aktualizacji (zgodnie z lokalizacją serwera głównego HTTP) należy ustawić:
`http://your_server_address/mirror/eset_upd/era6`
Uwaga: Folder lustrzany `era6` jest wspólny dla tych rozwiązań firmy ESET do zdalnego zarządzania: ERA 6, ESMC 7, ESET PROTECT.

Tabela kodów języków



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

Poniżej znajduje się przykład bardziej zaawansowanej konfiguracji repozytorium offline z wybranymi produktami, językami i włączonym pobieraniem starszych plików zdefiniowanymi w pliku *filter.txt* (przykład zawartości pliku znajduje się powyżej w opisie parametru `--filterFilePath`):

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

Firma ESET zaleca usunięcie poleceń zawierających poufne dane (na przykład hasło) z historii wiersza poleceń:
1.Uruchom polecenie `history`, aby wyświetlić listę wszystkich poleceń w historii.
2.Uruchom polecenie `history -d line_number` (określ numer wiersza, w którym występuje interesujące Cię polecenie). Możesz też wywołać polecenie `history -c`, aby usunąć całą historię wiersza poleceń.

Narzędzie Mirror Tool i ustawienia aktualizacji

- Aby zautomatyzować pobieranie aktualizacji modułów, można utworzyć harmonogram uruchamiania narzędzia Mirror Tool. Aby to zrobić, otwórz konsolę internetową i wybierz kolejno opcje **Zadania klienta** > **System operacyjny** > **Uruchom polecenie. Wybierz opcję Wiersz polecenia do uruchomienia** (w tym ścieżkę do narzędzia *MirrorTool.exe*) i odpowiedni element wyzwalający (na przykład CRON co godzinę 0 0 * * * ? *). Można też użyć harmonogramu zadań systemu Windows lub narzędzia `Cron` w systemie Linux.

- Aby skonfigurować aktualizacje na komputerach klienckich, utwórz nową politykę i skonfiguruj **serwer aktualizacji**, aby wskazywał adres kopii dystrybucyjnej lub folder udostępniony.

Instalacja komponentów w systemie macOS

W większości scenariuszy instalacji na poszczególnych komputerach należy zainstalować różne komponenty oprogramowania ESET PROTECT w celu dostosowania go do różnych architektur, spełnienia wymogów związanych z wydajnością lub z innych przyczyn.

System macOS jest obsługiwany wyłącznie w charakterze klienta. Agenta ESET Management i produkty ESET dla systemu macOS można zainstalować w systemie macOS. Jednak w systemie tym nie można zainstalować serwera ESET PROTECT.

Instalacja agenta — system macOS

Agenta ESET Management w systemie macOS można zainstalować na dwa sposoby:

- Zdalnie — korzystając z zadania serwera **Wdrażanie agenta**. Jeśli napotkasz jakiekolwiek problemy podczas zdalnego wdrażania agenta ESET Management (zadanie serwera **Wdrażanie agenta** zakończy się niepowodzeniem), zapoznaj się z artykułem Rozwiązywanie problemów z wdrażaniem agenta.

- Lokalnie — zgodnie z poniższym instrukcjami.

Wymagania wstępne

- ESET PROTECTSerwer i ESET PROTECTkonsola internetowa zainstalowane na komputerze pełniącym rolę serwera.

- Certyfikat agenta utworzony i przygotowany na dysku lokalnym.

- Urząd certyfikacji przygotowany na dysku lokalnym (wymagane tylko w przypadku certyfikatów niepodpisanych).

Instalacja

Należy wykonać poniższe czynności, aby zainstalować komponent agenta ESET Management lokalnie w systemie macOS:

Upewnij się, że spełnione są wszystkie wymagania wstępne dotyczące instalacji wskazane powyżej.

1. Pobierz plik instalacyjny (autonomiczny instalator agenta *.dmg*) z witryny pobierania firmy ESET lub uzyskaj go od administratora systemu.

2. Kliknij dwukrotnie plik *Agent-MacOSX-x86_64.dmg*, a następnie rozpocznij instalację, klikając dwukrotnie plik *.pkg*.

3. Kontynuuj instalację. Gdy pojawi się pytanie, wpisz dane **połączenia z serwerem**:

- **Nazwa hosta serwera**: nazwa hosta lub adres IP serwera ESET PROTECT
- **Port serwera**: port na potrzeby komunikacji między agentem a serwerem — domyślnie jest to 2222.
- **Użyj serwera proxy:** kliknij, aby komunikacja między agentem a serwerem odbywała się za pośrednictwem serwera proxy HTTP.

To ustawienie serwera proxy jest używane wyłącznie w celu replikacji między agentem ESET Management a serwerem ESET PROTECT, a nie do buforowania aktualizacji.
- **Nazwa hosta serwera proxy**: nazwa hosta lub adres IP komputera z serwerem proxy HTTP.
- **Port serwera**: wartość domyślna to 3128.
- **Nazwa użytkownika**, **hasło**: należy wprowadzić poświadczenia powiązane z serwerem proxy, jeśli korzysta on z funkcji uwierzytelniania.

Ustawienia serwera proxy można zmienić na późniejszym etapie w polityce. Serwer proxy musi być zainstalowany przed konfiguracją połączenia między agentem a serwerem za pośrednictwem serwera proxy.

4. Wybierz pozycję Certyfikat równorzędny i podaj hasło dla certyfikatu. Opcjonalnie możesz dodać urząd certyfikacji.

Hasło do certyfikatu nie może zawierać następujących znaków: " \ Znaki te powodują błąd krytyczny podczas inicjowania agenta.

5. Sprawdź miejsce instalacji i kliknij opcję **Zainstaluj**. Agent zostanie zainstalowany na komputerze.

6. Plik dziennika agenta ESET Management można znaleźć w tych lokalizacjach:

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

Protokół komunikacji między agentem a serwerem ESET PROTECT nie obsługuje uwierzytelniania. Żadne rozwiązanie proxy używane do przekazywania komunikacji agenta na serwer ESET PROTECT i wymagające uwierzytelniania nie będzie działać.
Jeśli port domyślny używany dla konsoli internetowej lub agenta zostanie zmieniony, może być konieczna korekta ustawień zapory. W przeciwnym razie instalacja może się nie powieść.

Obraz ISO

Plik obrazu ISO to jeden z formatów, w których można pobrać instalatory programu ESET PROTECT (kategoria instalatorów kompleksowych). Obraz ISO zawiera następujące elementy:

- Pakiet instalatora ESET PROTECT
- Odrębne instalatory dla każdego z komponentów

Obraz ISO jest przydatny, gdy użytkownik chce przechowywać wszystkie programy instalacyjne programu ESET PROTECT w jednym miejscu. Korzystanie z niego eliminuje również potrzebę pobierania programów instalacyjnych ze strony internetowej firmy ESET za każdym razem, gdy trzeba przeprowadzić instalację. Obraz ISO jest również przydatny podczas instalowania programu ESET PROTECT na maszynie wirtualnej.

Rekord usługi DNS

Aby skonfigurować rekord zasobu DNS:

1.Na serwerze DNS (serwerze DNS obsługiwanym przez kontroler domeny) wybierz kolejno opcje **Panel sterowania** > **Narzędzia administracyjne**.

2.Wybierz wartość DNS.

3.W Menedżerze DNS wybierz w strukturze drzewa pozycję _tcp i utwórz nowy rekord **Lokalizacja usługi (SRV**).

4.W polu **Usługa** wprowadź nazwę usługi w sposób zgodny ze standardowymi regułami DNS, wpisz symbol podkreślenia (_) przed nazwą usługi (użyj własnej nazwy usługi, na przykład **_era**).

5.W polu **Protokół** wprowadź protokół TCP w następującym formacie:_tcp.

6.W polu **Numer portu** wpisz port 2222.

7.W polu **Host oferujący tę usługę** wprowadź w pełni kwalifikowaną nazwę domeny (nazwę FQDN) serwera ESET PROTECT.

8.Kliknij **OK** > **Gotowe**, aby zapisać rekord. Rekord będzie wyświetlany na liście.

W celu zweryfikowania rekordu DNS:

1.Zaloguj się na dowolnym komputerze w swojej domenie i otwórz wiersz polecenia (cmd.exe).

2.Wpisz `nslookup` w wierszu polecenia i naciśnij klawisz **Enter**.

3.Wpisz`set querytype=srv` i naciśnij klawisz **Enter**.

4.Wpisz `_era._tcp.domain.name` i naciśnij klawisz **Enter**. Lokalizacja usługi zostanie poprawnie wyświetlona.

Należy pamiętać o zmianie wartości w polu „Host oferujący tę usługę:” na nazwę FQDN nowego serwera po zainstalowaniu serwera ESET PROTECT na innym komputerze.

Scenariusz instalacji offline programu ESET PROTECT

Aby zainstalować ESET PROTECT i jego składniki w środowiskach bez dostępu do Internetu, postępuj zgodnie z instrukcjami instalacji wysokiego poziomu (z zainstalowanym programem ESET PROTECT w systemie Windows).

Na komputerze z połączeniem internetowym

1. Utwórz udostępniony folder sieciowy.

2. Pobierz następujące instalatory do folderu udostępnionego:

   - Instalator kompleksowy ESET PROTECT
   - Obsługiwany pakiet JDK (wymagany dla konsoli internetowej).
   - Instalator agenta ESET Management
   - Instalatory produktów zabezpieczających ESET (na przykład ESET Endpoint Security)

Na komputerze z systemem Windows w trybie offline w tej samej sieci lokalnej

1. Skopiuj instalatory z udostępnionego folderu sieciowego na komputer z systemem Windows w trybie offline, na którym chcesz zainstalować program ESET PROTECT.

2. Zainstaluj pakiet JDK.

3. Instalacja ESET PROTECT w systemie Windows przy użyciu instalatora kompleksowego. Podczas instalacji wybierz opcję **Aktywuj później**.

4. Aktywuj ESET PROTECT za pomocą licencji offline.

5. Wdróż agenta ESET Management na komputerach w środowisku offline za pośrednictwem Skrypt instalacyjny agenta. Zmodyfikuj skrypt instalacyjny, aby użyć nowego adresu URL do uzyskania dostępu do pakietu instalacyjnego agenta z udostępnionego folderu sieciowego.

6. Wdróż produkty zabezpieczające ESET na stacjach roboczych przy użyciu zadania Instalacja oprogramowania. Wybierz **<Choose package>** i wprowadź własny adres URL pakietu instalacyjnego z repozytorium lokalnego.

7. Aktywuj zarządzane punkty końcowe za pomocą licencji offline.

8. Wyłącz ESET LiveGrid®.

Zdecydowanie zaleca się aktualizowanie infrastruktury ESET w trybie offline przy użyciu lokalnego repozytorium aktualizacji. Regularnie aktualizuj moduły produktów zabezpieczających ESET. Jeśli moduły nie zostaną zaktualizowane, konsola internetowa programu ESET PROTECT oznacza komputery jako **nie zaktualizowane**. Aby wyciszyć to ostrzeżenie konsoli internetowej, kliknij komputer na liście i wybierz polecenie **Wycisz** z menu kontekstowego.

Instrukcje dotyczące uaktualniania programu ESET PROTECT zawiera rozdział Uaktualnianie komponentów ESET PROTECT w środowisku offline.

Procedury uaktualniania

Istnieją różne sposoby uaktualniania serwera ESET PROTECT oraz innych komponentów programu ESET PROTECT. Zobacz również procedury migracji i ponownej instalacji.

Upewnij się, że masz obsługiwaną wersję systemu operacyjnego, zanim rozpoczniesz uaktualnienie do wersji ESET PROTECT 9.1.
Jeśli zainstalowana jest starsza, nieobsługiwana baza danych (MySQL 5.5 lub MS SQL 2008/2012), uaktualnij bazę danych do zgodnej wersji przed przystąpieniem do uaktualniania serwera ESET PROTECT.

Uaktualnianie programu ERA 5 lub 6.5

Bezpośrednie uaktualnienie nie jest obsługiwane – zobacz Migracja z wersji ERA 5.x oraz Aktualizacja z wersji ERA 6.x.

Uaktualnienie programu ESMC 7.2 do wersji ESET PROTECT 9.1

Wybierz jedną z procedur uaktualniania:

Procedura uaktualniania	System operacyjny	Komentarz
Zadanie uaktualnienia składników w konsoli internetowej	Windows/Linux	
Instalator kompleksowy ESET PROTECT 9.1	System Windows	W przypadku, gdy istniejąca kopia serwera została zainstalowana za pomocą instalatora kompleksowego, zalecaną opcją aktualizacji jest również skorzystanie z instalatora kompleksowego (zakładając, że masz domyślną instalację bazy danych MS SQL i serwera Apache Tomcat).
Ręczne uaktualnianie oparte na składnikach	Linux	Instrukcje dla zaawansowanych użytkowników Linuksa.
Aktualizacja urządzenia wirtualnego ESET PROTECT	(Urządzenie wirtualne) Linux	

Aby poznać wersję poszczególnych uruchomionych komponentów programu ESET PROTECT, należy sprawdzić wersję serwera ESET PROTECT. W konsoli internetowej ESET PROTECT przejdź na stronę Informacje, a następnie wyświetl listę wersji wszystkich składników ESET PROTECT.

Zadanie Uaktualnianie komponentów ESET PROTECT

Zalecenia przed uaktualnieniem

Zalecanym sposobem uaktualniania infrastruktury ESET PROTECT jest użycie zadania ESET PROTECTUaktualnianie komponentów dostępnego w konsoli internetowej ESET PROTECT. Przed uaktualnieniem należy dokładnie zapoznać się z instrukcjami.

Jeśli uaktualnianie komponentów nie powiedzie się na komputerze, na którym działa serwer lub konsola internetowa ESET PROTECT, zdalne logowanie do konsoli internetowej może być niemożliwe. Przed przystąpieniem do uaktualniania zalecamy skonfigurowanie fizycznego dostępu do komputera serwera. Jeśli fizyczny dostęp do komputera nie jest możliwy, należy zadbać o możliwość logowania się na nim przy użyciu uprawnień administratora za pośrednictwem pulpitu zdalnego. Przed przystąpieniem do tej operacji zalecamy wykonanie kopii zapasowej baz danych serwera ESET PROTECT i Modułu zarządzania urządzeniami mobilnymi. Aby utworzyć kopię zapasową urządzenia wirtualnego, należy utworzyć jego migawkę lub sklonować maszynę wirtualną.

Czy uaktualniasz z ESMC urządzenia wirtualnego ?

Instancja serwera ESET PROTECT jest zainstalowana w klastrze trybu failover?

Jeśli instancja serwera ESET PROTECT jest zainstalowana w klastrze trybu failover, komponent serwera ESET PROTECT należy uaktualnić ręcznie w poszczególnych węzłach klastra. Po uaktualnieniu serwera ESET PROTECT należy uruchomić zadanie Uaktualnianie komponentów w celu uaktualnienia pozostałych elementów infrastruktury (np. agentów ESET Management na komputerach klienckich).

Ważna instrukcja przed uaktualnianiem serwera proxy Apache HTTP w systemie Microsoft Windows

W przypadku używania serwera proxy Apache HTTP i skonfigurowania w pliku *httpd.conf* ustawień niestandardowych (takich jak nazwa użytkownika i hasło) należy utworzyć kopię zapasową oryginalnego pliku *httpd.conf* (znajdującego się w folderze *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*). Jeśli używane są ustawienia standardowe, utworzenie kopii zapasowej pliku *httpd.conf* nie jest konieczne. Uaktualnienie do najnowszej wersji serwera proxy Apache HTTP można przeprowadzić przy użyciu dowolnej z metod wskazanych w sekcji Uaktualnianie serwera proxy Apache HTTP.

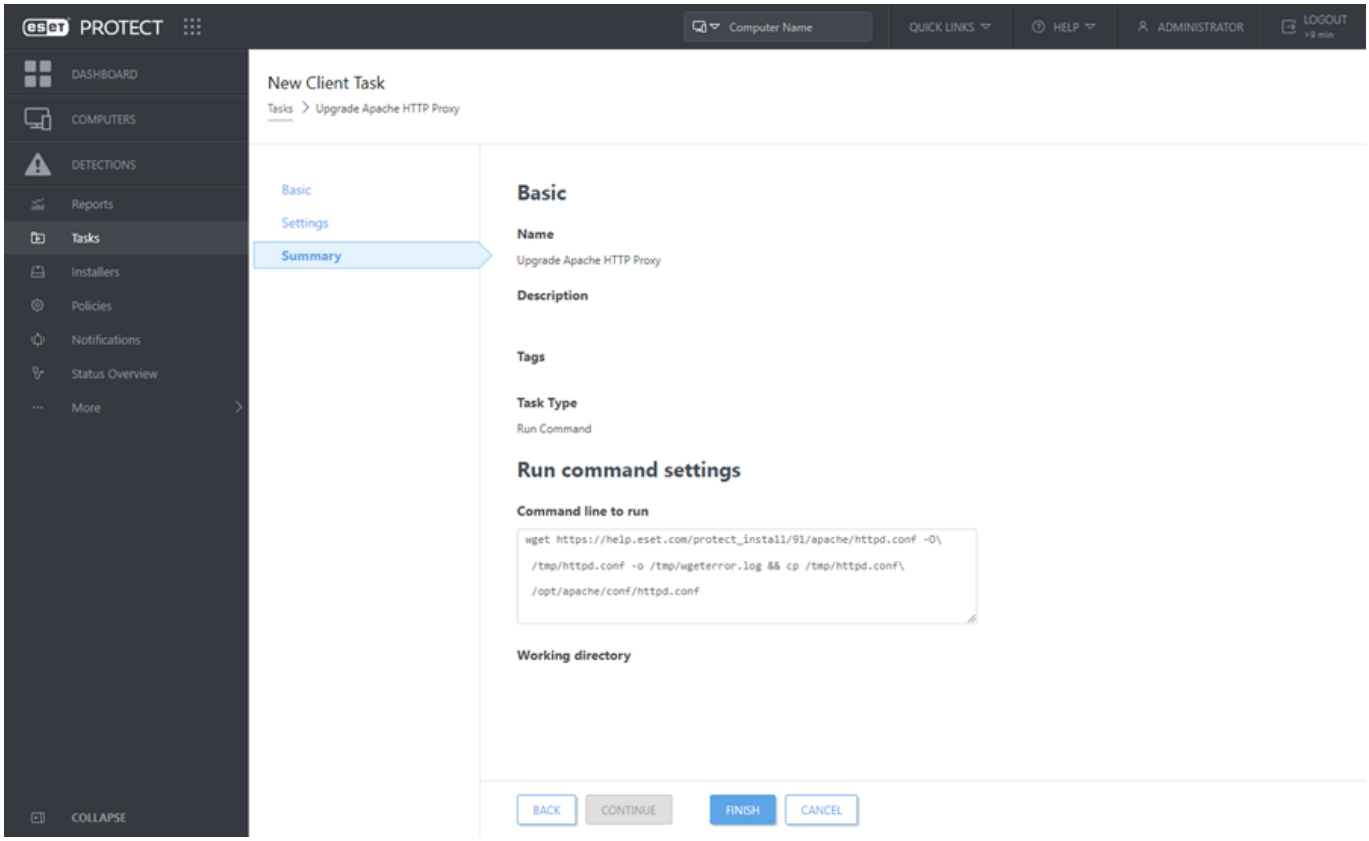
Jeśli uaktualniono serwer Apache HTTP Proxy w systemie Windows i w oryginalnym pliku *httpd.conf* znajdują się ustawienia niestandardowe (takie jak nazwa użytkownika i hasło), należy skopiować ustawienia z kopii zapasowej pliku *httpd.conf* i wstawić do nowego pliku *httpd.conf* tylko te ustawienia niestandardowe. Nie należy używać oryginalnego pliku *httpd.conf* z nową, uaktualnioną wersją serwera Apache HTTP Proxy, ponieważ nie będzie działać prawidłowo. Należy skopiować tylko ustawienia niestandardowe i użyć nowego pliku *httpd.conf*. Ewentualnie można ręcznie dostosować nowy plik *httpd.conf* — ustawienia opisano w sekcji Instalacja serwera proxy Apache HTTP — system Windows.

Ważna instrukcja przed uaktualnianiem serwera proxy Apache HTTP na urządzeniu wirtualnym

W przypadku używania **serwera proxy Apache HTTP** i skonfigurowania ustawień niestandardowych w pliku *httpd.conf* (takich jak nazwa użytkownika i hasło) należy utworzyć kopię zapasową oryginalnego pliku *httpd.conf* (znajdującego się w folderze */opt/apache/conf/*), a następnie uruchomić zadanie **Uaktualnianie komponentów programu ESET PROTECT** w celu uaktualnienia **serwera proxy Apache HTTP**. Jeśli nie są używane ustawienia niestandardowe, nie trzeba tworzyć kopii zapasowej pliku *httpd.conf*.

Po pomyślnym wykonaniu zadania Uaktualnianie komponentów należy uruchomić poniższe polecenie. Należy przypisać je do komputera z zainstalowanym serwerem proxy Apache HTTP. Należy użyć zadania klienta Uruchamianie polecenia. Spowoduje to aktualizację pliku *httpd.conf* (jest to wymagane do prawidłowego działania uaktualnionej wersji serwera proxy Apache HTTP):

```
wget https://help.eset.com/protect_install/91/apache/httpd.conf -O\
 /tmp/httpd.conf -o /tmp/wgeterror.log && cp /tmp/httpd.conf\
 /opt/apache/conf/httpd.conf
```



Jeśli serwer proxy Apache HTTP działa na komputerze z maszyną wirtualną, to samo polecenie można też uruchomić bezpośrednio z poziomu konsoli urządzenia wirtualnego ESET PROTECT. Innym sposobem jest ręczne zastąpienie pliku konfiguracyjnego serwera proxy Apache HTTP httpd.conf.

Jeśli w oryginalnym pliku *httpd.conf* znajdują się ustawienia niestandardowe (takie jak nazwa użytkownika i hasło), należy skopiować ustawienia z kopii zapasowej pliku *httpd.conf* i dodać do nowego pliku *httpd.conf* tylko te ustawienia niestandardowe. Nie należy używać oryginalnego pliku *httpd.conf* z nową, uaktualnioną wersją serwera proxy Apache HTTP, ponieważ nie będzie działać prawidłowo. Należy skopiować tylko ustawienia niestandardowe i użyć nowego pliku *httpd.conf*. Ewentualnie można ręcznie dostosować nowy plik *httpd.conf*. Zobacz szczegółowe ustawienia w sekcji Instalacja serwera proxy Apache HTTP — system Linux.

Możesz uaktualnić program do wersji ESET PROTECT 9.1 tylko z wersji ESMC 7.2 lub nowszej.
Program ESET PROTECT 9 automatycznie powiadamia użytkownika o dostępności nowej wersji serwera ESET PROTECT.
Przed uruchomieniem uaktualnienia należy wykonać kopię zapasową następujących danych:
• Wszystkie certyfikaty (urzędu certyfikacji, serwera i agenta).
• Wyeksportuj certyfikaty urzędu certyfikacji ze starego serwera ESET PROTECT do pliku *.der* i zapisz je w zewnętrznej pamięci masowej.
• Wyeksportuj certyfikaty równorzędne (dla agenta ESET Management i serwera ESET PROTECT) oraz plik klucza prywatnego *.pfx* ze starego serwera ESET PROTECT i zapisz je w zewnętrznej pamięci masowej.
• Baza danych ESMC/ESET PROTECT. Jeśli zainstalowana jest starsza, nieobsługiwana baza danych (MySQL 5.5 lub MS SQL 2008/2012), uaktualnij bazę danych do zgodnej wersji przed przystąpieniem do uaktualniania serwera ESET PROTECT.

Upewnij się, że masz obsługiwaną wersję systemu operacyjnego, zanim rozpoczniesz uaktualnienie do wersji ESET PROTECT 9.1.
Aby zainstalować produkty zabezpieczające ESET, uruchom zadanie instalacji oprogramowania przy użyciu najnowszego pakietu instalatora, aby zastąpić istniejące rozwiązanie najnowszą wersją.

Zalecana procedura uaktualniania

1.Uaktualnij serwer ESET PROTECT — wybierz tylko komputer z serwerem ESET PROTECT jako obiekt docelowy zadania **Uaktualniania składników ESET PROTECT.**

2.Wybierz kilka komputerów klienckich (jako przykład testowy — co najmniej jednego klienta z każdej kategorii systemu/wersji bitowej) i uruchom na nich zadanie **Uaktualnienia składników ESET PROTECT.**

Zalecamy używanie Apache HTTP Proxy (lub innego transparentnego serwera proxy WWW z włączonym buforowaniem) w celu ograniczenia obciążenia sieciowego. Testowe komputery klienckie uruchomią pobieranie/buforowanie instalatorów. Przy następnym uruchomieniu zadania nastąpi dystrybucja instalatorów na komputerach klienckich bezpośrednio z pamięci podręcznej.

3. Po pomyślnym nawiązaniu połączenia komputerów z uaktualnionym agentem ESET Management z serwerem ESET PROTECT należy kontynuować uaktualnianie pozostałych klientów.

Aby uaktualnić agenty ESET Management na wszystkich zarządzanych komputerach w sieci, wybierz grupę statyczną **Wszystkie** jako miejsce docelowe zadania **Uaktualniania składników ESET PROTECT.** Zadanie pominie komputery, na których jest już uruchomiony najnowszy agent ESET Management.
ESET PROTECT 9.1 obsługuje automatyczną aktualizację agenta ESET Management na zarządzanych komputerach.

Komponenty uaktualniane automatycznie:

• ESET PROTECTSerwer

• Agent ESET Management

• Konsola internetowa ESET PROTECT — tylko gdy serwer Apache Tomcat zainstalowano w domyślnym folderze instalacji zarówno w systemie Windows jak i w dystrybucjach systemu Linux, w tym również na urządzeniu wirtualnym ESET PROTECT (przykład: */var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*).

Ograniczenia dotyczące uaktualniania konsoli internetowej

- Serwer Apache Tomcat nie jest uaktualniany podczas uaktualniania konsoli internetowej ESET PROTECT za pomocą zadania Uaktualnianie komponentów.
- Uaktualnianie konsoli internetowej ESET PROTECT nie działa, jeśli serwer Apache Tomcat zainstalowano w lokalizacji niestandardowej.
- Jeśli zainstalowana jest niestandardowa wersja serwera Apache Tomcat (ręczna instalacja usługi Tomcat), kolejne uaktualnienie konsoli internetowej ESET PROTECT za pośrednictwem instalatora kompleksowego lub zadania uaktualnienia składników nie jest obsługiwane.

- ESET PROTECT Moduł zarządzania urządzeniami mobilnymi

Składniki wymagające ręcznego uaktualnienia:

Komponenty ESET

- ESET Rogue Detection Sensor – użyj zadania instalacji oprogramowania do przeprowadzenia uaktualnienia. Ewentualnie można zainstalować najnowszą wersję w celu zastąpienia wersji starszej (w tym celu należy postępować zgodnie z instrukcjami instalacji dla systemu Windows lub Linux). W przypadku zainstalowania narzędzia RD Sensor ze produktu ESMC 7.2 i późniejsze nie jest konieczne uaktualnianie go, ponieważ nie ma nowszych wersji narzędzia RD Sensor.

Składniki stron trzecich

Oprócz składników ESET ESET PROTECT używa składników innych firm, które mogą stać się nieaktualne i wymagać ręcznej aktualizacji.

W konsoli internetowej ESET PROTECT kliknij pozycję **Szybkie łącza** > **Nieaktualne składniki**, aby wyświetlić nieaktualne składniki innych firm.

Urządzenie wirtualne ESET PROTECT nie zgłasza nieaktualnych składników innych firm.

ESET PROTECT zgłasza wersje starsze niż wymienione poniżej jako nieaktualne:

Komponent stron trzecich:	Wersja:
Microsoft SQL Server	2019 (wersja 15.0.4223.0)1
MySQL	8.0.0.0
System operacyjny2	Windows Server 2016
Apache Tomcat	9.0.62
Java	17.0

1 Określ swoją wersję i edycję programu SQL Server Database Engine i zainstaluj najnowszą aktualizację zbiorczą.

2 ESET PROTECT nie zgłasza nieaktualnego systemu operacyjnego Linux.

Postępuj zgodnie z instrukcjami aktualizacji składników innych firm:

- Serwer bazy danych
- System operacyjny
- Serwer Apache Tomcat

- Java Runtime Environment
- Serwer proxy Apache HTTP

Rozwiązywanie problemów

- Należy sprawdzić, czy repozytorium ESET PROTECT jest dostępne z uaktualnionego komputera.
- Ponowne uruchomienie zadania Uaktualnianie komponentów ESET PROTECT nie przyniesie żądanego efektu, jeśli co najmniej jeden z komponentów uaktualniono już wcześniej do nowszej wersji.
- Jeśli nie można ustalić przyczyny niepowodzenia, można uaktualnić poszczególne komponenty ręcznie. Należy zapoznać się z instrukcjami dotyczącymi systemu Windows lub Linux.
- Więcej sugestii dotyczących rozwiązywania problemów z uaktualnianiem można znaleźć w ogólnych informacjach o rozwiązywaniu problemów.

Uaktualnianie za pomocą instalatora kompleksowego ESET PROTECT 9.1

Użyj instalatora kompleksowego ESET PROTECT 9.1, aby uaktualnić ESMC 7.2 lub starszą wersję ESET PROTECT do najnowszej wersji ESET PROTECT 9.1.

W przypadku, gdy istniejąca kopia serwera została zainstalowana za pomocą instalatora kompleksowego, zalecaną opcją aktualizacji jest również skorzystanie z instalatora kompleksowego (zakładając, że masz domyślną instalację bazy danych MS SQL i serwera Apache Tomcat).

W wersji ESET PROTECT 9.1 Instalator kompleksowy domyślnie instaluje produkt Microsoft SQL Server Express 2019.

- Jeśli używasz starszej wersji systemu Windows (Server 2012 lub SBS 2011), domyślnie zainstalowany zostanie produktMicrosoft SQL Server Express 2014.
- Instalator automatycznie generuje losowe hasło do uwierzytelniania bazy danych (przechowywane w pliku *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

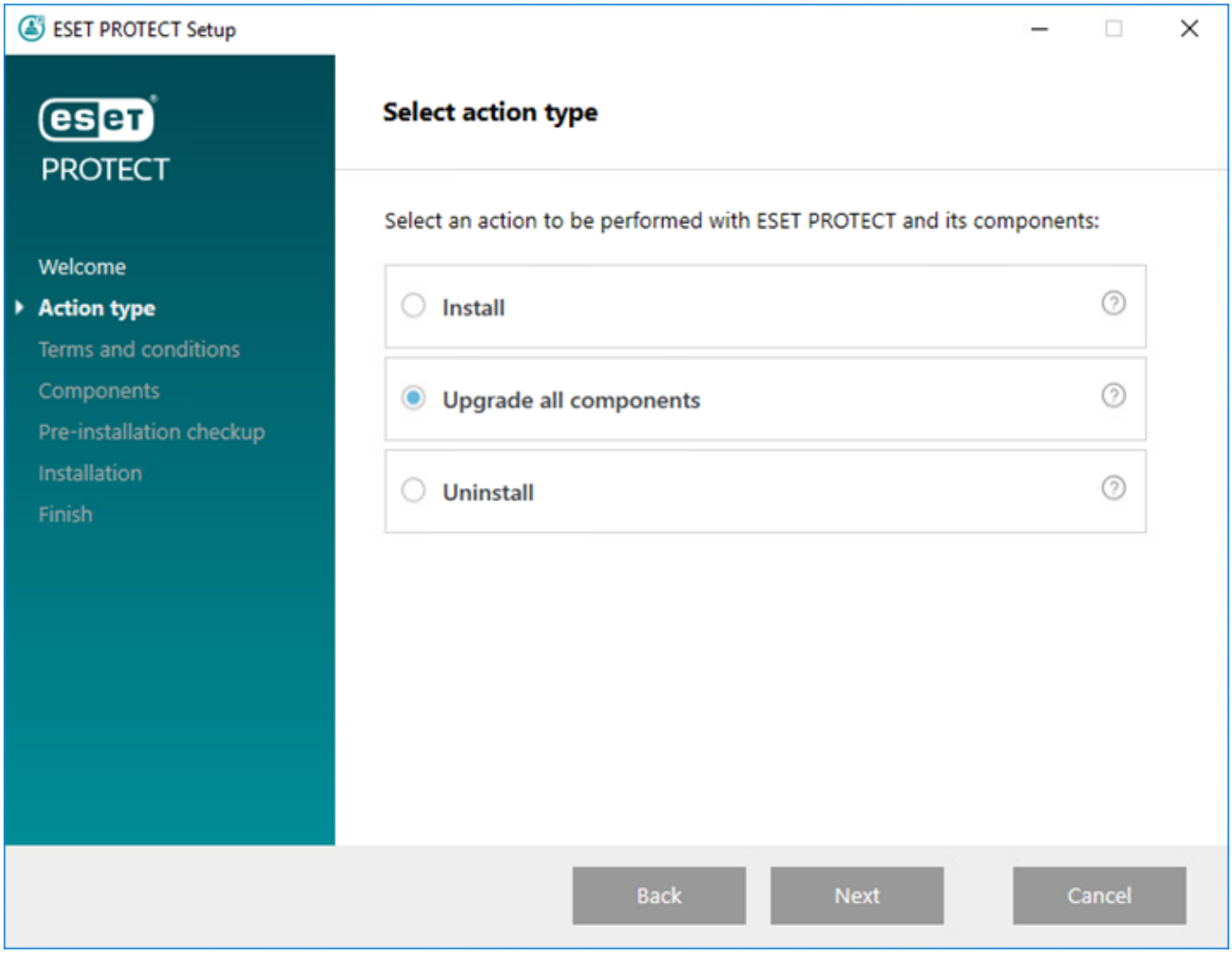
⚠ Program Microsoft SQL Server Express ma limit rozmiaru wynoszący 10 GB dla każdej relacyjnej bazy danych. Nie zalecamy korzystania z programu Microsoft SQL Server Express:
- w środowiskach firmowych lub dużych sieciach,
- Jeśli produkt ESET PROTECT ma być używany z ESET Inspect.

Możesz uaktualnić program do wersji ESET PROTECT 9.1 tylko z wersji ESMC 7.2 lub nowszej.
Przed uruchomieniem uaktualnienia należy wykonać kopię zapasową następujących danych:
• Wszystkie certyfikaty (urzędu certyfikacji, serwera i agenta).
• Wyeksportuj certyfikaty urzędu certyfikacji ze starego serwera ESET PROTECT do pliku *.der* i zapisz je w zewnętrznej pamięci masowej.
• Wyeksportuj certyfikaty równorzędne (dla agenta ESET Management i serwera ESET PROTECT) oraz plik klucza prywatnego *.pfx* ze starego serwera ESET PROTECT i zapisz je w zewnętrznej pamięci masowej.
• Baza danych ESMC/ESET PROTECT. Jeśli zainstalowana jest starsza, nieobsługiwana baza danych (MySQL 5.5 lub MS SQL 2008/2012), uaktualnij bazę danych do zgodnej wersji przed przystąpieniem do uaktualniania serwera ESET PROTECT.
Upewnij się, że masz obsługiwaną wersję systemu operacyjnego, zanim rozpoczniesz uaktualnienie do wersji ESET PROTECT 9.1.

1.Uruchom plik *Setup.exe*.

2.Wybierz język i kliknij przycisk **Dalej**.

3.Wybierz opcję **Uaktualnij wszystkie komponenty** i kliknij przycisk **Dalej**.



4.Przeczytaj **umowę licencyjną użytkownika końcowego oprogramowania**, zaakceptuj ją i kliknij przycisk **Dalej**.

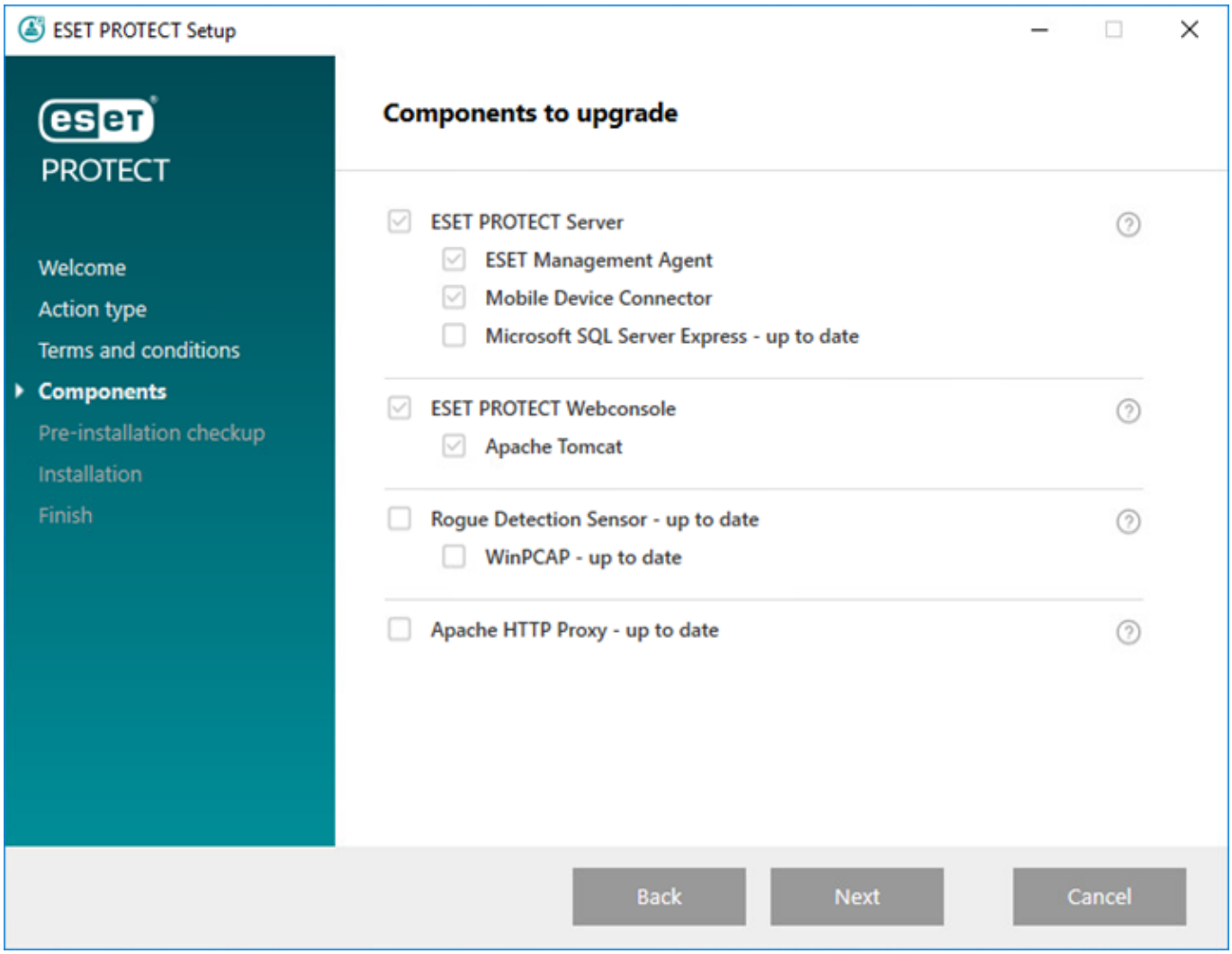
5.W sekcji **Komponenty** sprawdź komponenty programu ESET PROTECT, które można uaktualnić, i kliknij przycisk **Dalej**.

Apache Tomcat i ograniczenia aktualizacji konsoli internetowej

- Jeśli zainstalowana jest niestandardowa wersja serwera Apache Tomcat (ręczna instalacja usługi Tomcat), kolejne uaktualnienie konsoli internetowej ESET PROTECT za pośrednictwem instalatora kompleksowego lub zadania uaktualnienia składników nie jest obsługiwane.
- Uaktualnienie serwera Apache Tomcat spowoduje usunięcie folderu *era* z lokalizacji *C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps*. Jeśli używasz folderu *era* do przechowywania danych dodatkowych, pamiętaj o wykonaniu kopii zapasowej tych danych przed uaktualnieniem.
- W przypadku użycia użytkownika *C:\Program Files\Apache Software Foundation\[Tomcat folder]*w lokalizacji *webapps* znajdują się dane dodatkowe (inne niż foldery *era* i *ROOT*), uaktualnienie serwera Apache Tomcat nie zostanie przeprowadzone i uaktualniona zostanie wyłącznie konsola internetowa.
- Aktualizacja konsoli internetowej i Apache Tomcat usuwa pliki pomocy offline. Jeśli korzystałeś z pomocy offline w rozwiązaniu ESMC lub starszej wersji programu ESET PROTECT, po aktualizacji konieczne jest jej ponowne utworzenie dla ESET PROTECT 9.1, aby mieć pewność, że Twoja wersja pomocy offline odpowiada wersji ESET PROTECT.

Ograniczenia uaktualniania serwera proxy Apache HTTP

Instalator kompleksowy zastępuje *httpd.conf* i zapisuje oryginalną konfigurację w *httpd.conf.old*. Aby zachować niestandardową konfigurację serwera proxy Apache HTTP, należy wykonać kopię zapasową konfiguracji i użyć jej ponownie.



6.Wykonaj **Przegląd przed instalacją**, aby upewnić się, że system spełnia wszystkie wymagania wstępne.

7.Kliknij przycisk **Uaktualnij**, aby rozpocząć uaktualnianie produktu ESET PROTECT. Uaktualnienie może

zająć trochę czasu, w zależności od konfiguracji systemu i sieci.

8.Po zakończeniu uaktualniania kliknij przycisk **Zakończ**.

9.Po uaktualnieniu ESET PROTECT zaktualizuj agenta ESET Management na zarządzanych komputerach za pomocą zadania Uaktualnianie komponentów. ESET PROTECT 9.1 obsługuje automatyczną aktualizację agenta ESET Management na zarządzanych komputerach.

Uaktualnienie z wersji ERA 6.5

Nie można bezpośrednio uaktualnić do wersji ESET PROTECT 9.1.

Jeśli masz zainstalowaną wersję ERA 6,5, wykonaj następujące czynności:

1.Uaktualnienie wersji ERA 6.5 do wersji ESET PROTECT 8.1.

2.Uaktualnienie wersji ESET PROTECT 8.1 do wersji ESET PROTECT 9.1.

Kopa zapasowa / aktualizacja serwera bazy danych

Program ESET PROTECT używa bazy danych do przechowywania danych klientów. Poniższe sekcje zawierają szczegółowe informacje o tworzeniu kopii zapasowych oraz aktualizacji bazy danych serwera ESET PROTECT (lub serwera ESMC) lub bazy danych komponentu MDM:

- Jeśli nie ma bazy danych skonfigurowanej na potrzeby używania z serwerem ESET PROTECT, można użyć programu **Microsoft SQL Server Express** dołączonego do instalatora. W wersji ESET PROTECT 9.1 Instalator kompleksowy domyślnie instaluje produkt Microsoft SQL Server Express 2019.

  - Jeśli używasz starszej wersji systemu Windows (Server 2012 lub SBS 2011), domyślnie zainstalowany zostanie produktMicrosoft SQL Server Express 2014.

  - Instalator automatycznie generuje losowe hasło do uwierzytelniania bazy danych (przechowywane w pliku *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

> ⚠ Program Microsoft SQL Server Express ma limit rozmiaru wynoszący 10 GB dla każdej relacyjnej bazy danych. Nie zalecamy korzystania z programu Microsoft SQL Server Express:
> - w środowiskach firmowych lub dużych sieciach,
> - Jeśli produkt ESET PROTECT ma być używany z ESET Inspect.

- Jeśli zainstalowana jest starsza, nieobsługiwana baza danych (MySQL 5.5 lub MS SQL 2008/2012), uaktualnij bazę danych do zgodnej wersji przed przystąpieniem do uaktualniania serwera ESET PROTECT.

Zobacz też ESET PROTECT migrację bazy danych.

Muszą być spełnione następujące wymagania związane z programem Microsoft SQL Server:

- Należy zainstalować obsługiwaną wersję programu Microsoft SQL Server. Podczas instalacji wybierz opcję uwierzytelniania **Tryb mieszany**.

• Jeśli program Microsoft SQL Server jest już zainstalowany, ustaw w opcji uwierzytelnienia **Tryb mieszany (Uwierzytelnianie programu SQL Server i Uwierzytelnianie Windows)**. Aby to zrobić, wykonaj działania opisane w tym artykule bazy wiedzy. Jeśli chcesz logować się do programu Microsoft SQL Server przy użyciu **uwierzytelniania systemu Windows**, wykonaj czynności opisane w tym artykule z bazy wiedzy.

• Zezwól na połączenia TCP/IP z programem SQL Server. Aby to zrobić, wykonaj działania opisane w tym artykule bazy wiedzy, rozpoczynając od części **II. Zezwalanie na połączenia TCP/IP z programem SQL Server**.

• Aby można było skonfigurować program Microsoft SQL Server (bazy danych i użytkowników), a także nim zarządzać i administrować, należy pobrać program SQL Server Management Studio (SSMS).
• Nie instaluj programu SQL Server na kontrolerze domeny (np. w przypadku korzystania z systemu Windows SBS/Essentials). Zalecamy zainstalowanie programu ESET PROTECT na innym serwerze lub niezaznaczanie komponentu SQL Server Express podczas instalacji (wymaga to uruchomienia bazy danych ESET PROTECT na istniejącym serwerze SQL lub MySQL).

Tworzenie i przywracanie kopii zapasowej serwera bazy danych

Wszystkie informacje i ustawienia dotyczące programu ESET PROTECT przechowywane są w bazie danych. Aby uniknąć utraty danych, zalecamy regularne tworzenie kopii zapasowych bazy danych. Kopii zapasowej można użyć później podczas migracji programu ESET PROTECT na nowy serwer. Spośród sekcji znajdujących się poniżej należy skorzystać z tej, która odpowiada używanej bazie danych:

• Nazwy baz danych i plików dziennika nie zmieniają się nawet po zmianie nazwy produktu z ESET Security Management Center na ESET PROTECT.
• Jeśli używasz urządzenia wirtualnego ESET PROTECT, postępuj zgodnie z instrukcjami dotyczącymi tworzenia kopii zapasowej bazy danych urządzenia wirtualnego.

Przykłady tworzenia kopii zapasowej bazy danych MS SQL

Aby utworzyć kopię zapasową bazy danych MS SQL w pliku, prześledź poniższe przykłady:

W tych przykładach zastosowano ustawienia domyślne (np. domyślną nazwę bazy danych oraz domyślne ustawienia połączenia z bazą danych). Konieczne jest zmodyfikowanie skryptu kopii zapasowej w celu uwzględnienia zmian wprowadzonych w ustawieniach domyślnych.
Do uruchomienia podanych niżej poleceń niezbędne są odpowiednie uprawnienia. Jeśli nie korzystasz z lokalnego konta administratora, musisz zmienić ścieżkę kopii zapasowej, na przykład na następującą: *'C:\USERS\PUBLIC\BACKUPFILE'*.

Jednorazowa kopia zapasowa bazy danych

W celu utworzenia kopii zapasowej w pliku o nazwie **BACKUPFILE** wykonaj poniższe polecenie w wierszu polecenia w systemie Windows:

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

W tym przykładzie **HOST** oznacza adres IP lub nazwę hosta, a **ERASQL** nazwę instancji serwera MS SQL. Serwer ESET PROTECT można zainstalować w instancji SQL o niestandardowej nazwie (jeśli jest używana baza danych MS SQL). W takim przypadku należy odpowiednio zmodyfikować skrypty tworzenia kopii zapasowych.

Regularne kopie zapasowe bazy danych przy użyciu skryptu SQL

Wybierz jeden z poniższych skryptów SQL:

a)Utwórz regularne kopie zapasowe i przechowuj je z uwzględnieniem daty utworzenia:

```
1.@ECHO OFF

2.SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"

3.REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)Dołączaj kopie zapasowe do jednego pliku:

```
1. @ECHO OFF

2. SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Przywracanie bazy danych MS SQL

Aby przywrócić bazę danych MS SQL z pliku, prześledź poniższy przykład:

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

Tworzenie kopii zapasowej bazy danych MySQL

Aby utworzyć kopię zapasową bazy danych MySQL w pliku, prześledź poniższy przykład:

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

W tym przykładzie **HOST** oznacza adres IP lub nazwę hosta serwera MySQL, **ROOTLOGIN** oznacza konto główne na serwerze MySQL, a **DBNAME** oznacza nazwę bazy danych ESET PROTECT.

Przywracanie bazy danych MySQL

Aby przywrócić bazę danych MySQL z pliku, prześledź poniższy przykład:

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

> Więcej informacji na temat tworzenia kopii zapasowych na serwerze Microsoft SQL można znaleźć w witrynie internetowej Microsoft TechNet. Więcej informacji na temat tworzenia kopii zapasowych na serwerze MySQL można znaleźć w witrynie internetowej z dokumentacją rozwiązania MySQL.

Uaktualnianie serwera baz danych

Aby uaktualnić do nowszej wersji istniejącą instancję programu Microsoft SQL Server obsługującego bazę danych serwera ESET PROTECT, wykonaj poniższe instrukcje:

1. Zatrzymaj wszystkie uruchomione usługi serwera ESMC / ESET PROTECT lub serwera proxy wymagające połączenia z serwerem baz danych, który zamierzasz uaktualnić. Ponadto zatrzymaj wszystkie inne aplikacje, które mogą łączyć się z używaną instancją programu Microsoft SQL Server.

2. Wykonaj kopie zapasowe wszystkich niezbędnych baz danych przed rozpoczęciem następnych czynności.

3. Uaktualnij serwer baz danych:

Aktualizacja programu SQL Server (Windows):

- Postępuj zgodnie z artykułem bazy wiedzy dotyczącym aktualizacji bazy danych MS SQL Express do najnowszej wersji.
- Można to również zrobić, wykonując instrukcje dostawcy bazy danych: https://msdn.microsoft.com/en-us/library/bb677622.aspx.
- Program MS SQL Server dla systemu Linux nie jest obsługiwany. Można jednak połączyć serwer ESET PROTECT w systemie Linux z programem MS SQL Server w systemie Windows.

Aktualizacja serwera MySQL (Windows i Linux):

- Uaktualnienie z MySQL 5.6 do wersji 5.7
- Uaktualnienie z MySQL 5.7 do wersji 8

4. Uruchom usługę serwera ESET PROTECT i sprawdź dzienniki śledzenia w celu zweryfikowania, czy połączenie z bazą danych działa prawidłowo.

Uaktualnianie programu ESMC/ESET PROTECT zainstalowanego w klastrze trybu failover w systemie

Windows

Jeśli serwer ESMC/ESET PROTECT zainstalowano w środowisku klastra trybu failover w systemie Windows, wykonaj poniższe czynności, aby przeprowadzić aktualizację ESET PROTECT do najnowszej wersji.

Upewnij się, że masz obsługiwany system operacyjny.

1. Zatrzymaj rolę klastra serwera ESMC/ESET PROTECT w Menedżerze klastra. Upewnij się, że usługa **ESET Security Management Center Server** lub **ESET PROTECT Server** została zatrzymana we wszystkich węzłach klastra.

2. Uzyskaj dostęp online do udostępnionego dysku klastrowego w węźle 1 i uaktualnij komponent serwera ręcznie, uruchamiając najnowszy plik *.msi* instalatora — jak w przypadku instalacji komponentu.

3. Po zakończeniu instalacji (uaktualniania) upewnij się, że usługa **ESET PROTECT Server** została zatrzymana.

4. Uzyskaj dostęp online do udostępnionego dysku klastrowego w węźle 2 i uaktualnij komponent serwera tak, jak w kroku 2.

5. Po uaktualnieniu serwera ESET PROTECT we wszystkich węzłach klastra uruchom **rolę serwera ESET PROTECT** w Menedżerze klastra.

6. Uaktualnij agenta ESET Management ręcznie, uruchamiając najnowszy instalator *.msi* we wszystkich węzłach klastra.

7. W konsoli internetowej ESET PROTECT sprawdź, czy we wszystkich węzłach są najnowsze wersje agenta i serwera (te, do których przeprowadzono uaktualnienie).

Uaktualnianie serwera proxy Apache HTTP

Apache HTTP Proxy to usługa, z której można korzystać w połączeniu z programem ESET PROTECT w celu dystrybuowania aktualizacji wśród komputerów klienckich oraz przesyłania pakietów instalacyjnych do agentów ESET Management.

Jeśli wcześniej w systemie Windows zainstalowano serwer proxy Apache HTTP i jest konieczne jego uaktualnienie do najnowszej wersji, operację uaktualniania można przeprowadzić na dwa sposoby — ręcznie lub przy użyciu instalatora kompleksowego.

Uaktualnianie serwera proxy Apache HTTP przy użyciu instalatora kompleksowego (system Windows)

Jeśli pobrano najnowszy instalator kompleksowy ESET PROTECT, można użyć tej metody, aby szybko uaktualnić serwer proxy Apache HTTP do najnowszej wersji. Jeśli nie masz pobranego najnowszego instalatora, użyj ręcznej metody uaktualniania serwera proxy Apache HTTP.

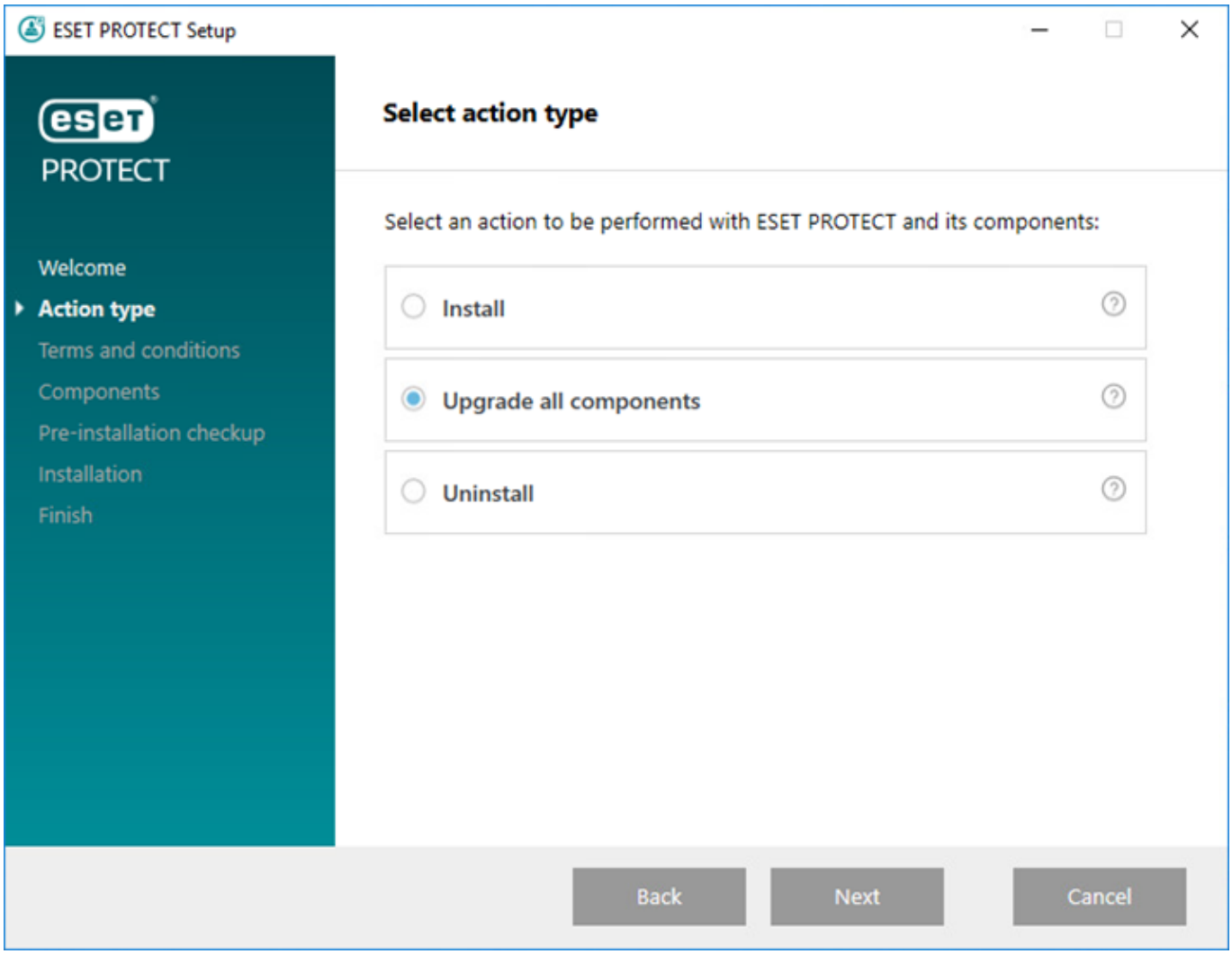
1. Utwórz kopie zapasowe następujących plików:

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*

- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*
- *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\group.file*

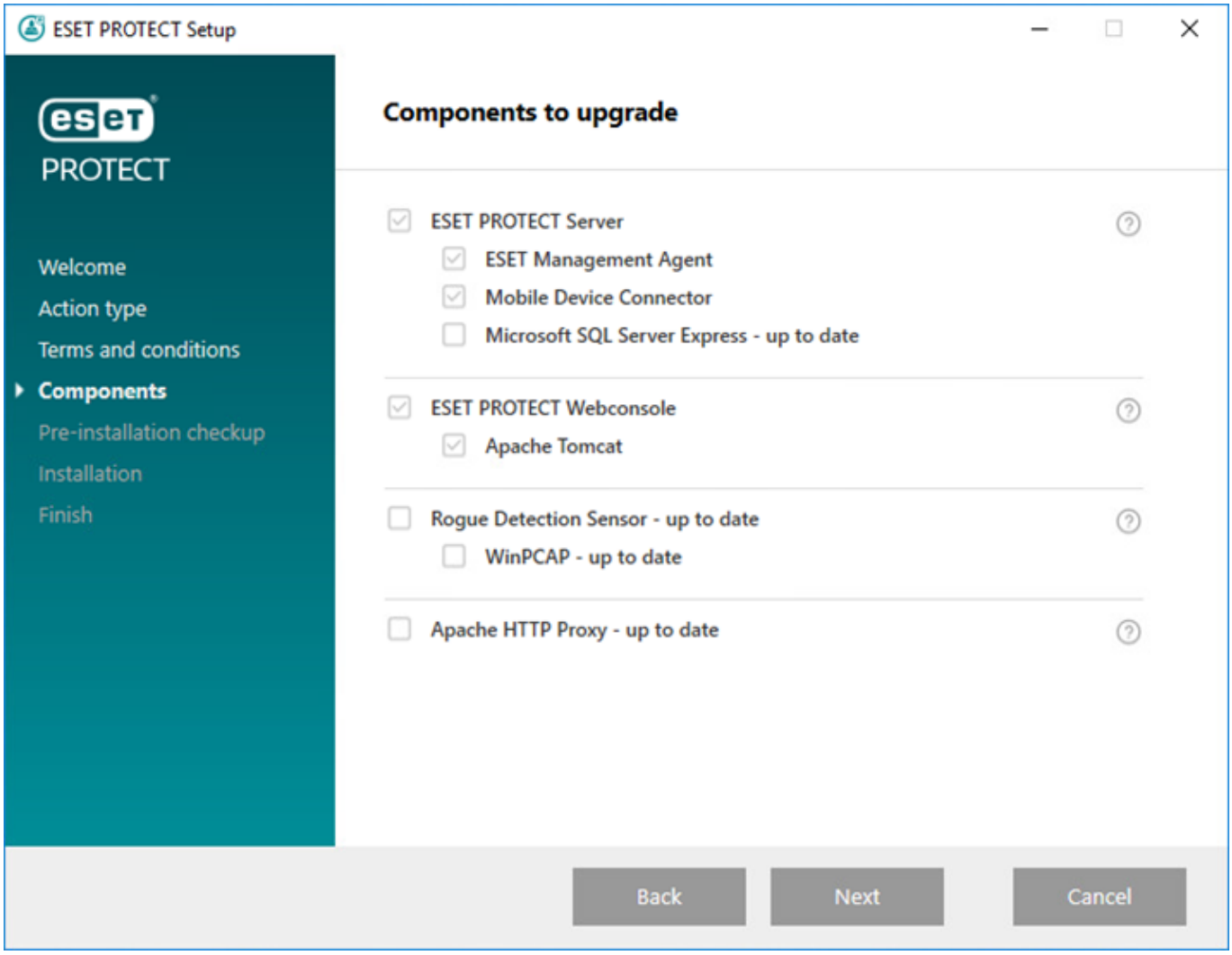
2. Uruchom instalator kompleksowy, klikając dwukrotnie plik *setup.exe*. Następnie kliknij przycisk **Dalej** na ekranie powitalnym.

3. Wybierz opcję **Uaktualnij wszystkie komponenty** i kliknij przycisk **Dalej**.



4. Przeczytaj **umowę licencyjną użytkownika końcowego oprogramowania**, zaakceptuj ją i kliknij przycisk **Dalej**.

5. W sekcji **Komponenty** sprawdź komponenty programu ESET PROTECT, które można uaktualnić, i kliknij przycisk **Dalej**.



6. Wykonaj **Przegląd przed instalacją**, aby upewnić się, że system spełnia wszystkie wymagania wstępne.

7. Kliknij przycisk **Uaktualnij**, aby rozpocząć uaktualnianie produktu ESET PROTECT. Uaktualnienie może zająć trochę czasu, w zależności od konfiguracji systemu i sieci.

8. Po zakończeniu uaktualniania kliknij przycisk **Zakończ**.

Instalator kompleksowy zastępuje *httpd.conf* i zapisuje oryginalną konfigurację w *httpd.conf.old*. Aby zachować niestandardową konfigurację serwera proxy Apache HTTP, należy wykonać kopię zapasową konfiguracji i użyć jej ponownie.

9. Przetestuj połączenie z serwerem proxy Apache HTTP, wpisując w przeglądarce następujący adres URL:

http://[IP address]:3128/index.html

Rozwiązywanie problemów

Informacje potrzebne do rozwiązania problemu można znaleźć w plikach dziennika serwera proxy Apache HTTP.

Jeśli przy poprzedniej instalacji serwera proxy Apache HTTP dokonano niestandardowej konfiguracji pliku *httpd.conf*, wykonaj następujące czynności:

1.Zatrzymaj usługę **ApacheHttpProxy**, otwierając administracyjny wiersz polecenia i uruchamiając następujące polecenie:

```
sc stop ApacheHttpProxy
```

2.Jeśli używana jest nazwa użytkownika/hasło dostępu do serwera proxy Apache HTTP (temat Instalacja serwera proxy Apache HTTP), zastąp następujący blok kodu:

```
<Proxy *>
 Deny from all
</Proxy>
```

poniższym kodem (znajdującym się w kopii zapasowej pliku *httpd.conf*):

```
<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>
```

3.Jeśli w poprzedniej instalacji serwera proxy Apache HTTP wprowadzono inne modyfikacje w pliku *httpd.conf*, można je ręcznie skopiować z pliku *httpd.conf.old* (lub kopii zapasowej *httpd.conf* wykonanej w kroku 1) do nowego (uaktualnionego) pliku *httpd.conf*.

4.Zapisz zmiany i uruchom usługę **ApacheHttpProxy** przez wykonanie następującego polecenia w wierszu polecenia z podwyższonym poziomem uprawnień:

```
sc start ApacheHttpProxy
```

Ręczne uaktualnianie serwera proxy Apache HTTP (system Windows)

Aby uaktualnić Apache HTTP Proxy do najnowszej wersji, należy postępować zgodnie z poniższymi instrukcjami.

1. Utwórz kopie zapasowe następujących plików:

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf\httpd.conf*

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\password.file*

   • *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\bin\group.file*

2. Zatrzymaj usługę **ApacheHttpProxy**, otwierając administracyjny wiersz polecenia i uruchamiając następujące polecenie:

```
sc stop ApacheHttpProxy
```

3. Pobierz plik instalatora Apache HTTP Proxy z witryny pobierania firmy ESET i wyodrębnij jego zawartość do folderu *C:\Program Files\Apache HTTP Proxy 2.[x.xx]*. Proces wyodrębniania spowoduje zastąpienie istniejących plików.

4. Przejdź do folderu *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\conf*, kliknij prawym przyciskiem myszy plik *httpd.conf* i z menu kontekstowego wybierz polecenia **Otwórz za pomocą** > **Notatnik**.

5. Dodaj następujący kod na końcu pliku *httpd.conf*:

```
ServerRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]"
DocumentRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\htdocs">
 Options Indexes FollowSymLinks
 AllowOverride None
 Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy 2.[x.xx]\cache"
```

6. Jeśli ustawiono nazwę użytkownika/hasło dostępu do serwera proxy Apache HTTP (temat Instalacja serwera proxy Apache HTTP), zastąp następujący blok kodu:

```
<Proxy *>
 Deny from all
</Proxy>
```

poniższym kodem (znajdującym się w kopii zapasowej pliku *httpd.conf* utworzonej w kroku 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>
```

> Jeśli w poprzedniej instalacji serwera proxy Apache HTTP wprowadzono inne modyfikacje w pliku *httpd.conf*, skopiuj modyfikacje konfiguracji z kopii zapasowej pliku *httpd.conf* do nowego (uaktualniony) pliku *httpd.conf*.

7. Zapisz zmiany i uruchom usługę **ApacheHttpProxy** przez wykonanie następującego polecenia w administracyjnym wierszu polecenia:

```
sc start ApacheHttpProxy
```

8. Zaktualizuj wersję w opisie usługi.

```
sc description ApacheHttpProxy "Apache/2.4.43"
```

9. Przetestuj połączenie z serwerem proxy Apache HTTP, wpisując w przeglądarce następujący adres URL:

http://[IP address]:3128/index.html

Informacje potrzebne do rozwiązania problemu można znaleźć w plikach dziennika serwera proxy Apache HTTP.

Uaktualnianie serwera Apache Tomcat

Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT.

W przypadku uaktualniania do najnowszej wersji programu ESET PROTECT lub uaktualniania serwera Apache Tomcat po raz pierwszy od długiego czasu należy rozważyć uaktualnienie serwera Apache Tomcat do najnowszej wersji. Aktualne publicznie dostępne usługi, w tym serwer Apache Tomcat i jego zależności, zmniejszają zagrożenia dla bezpieczeństwa środowiska.

Aby uaktualnić serwer Apache Tomcat, postępuj zgodnie z instrukcjami:

- Instrukcje dotyczące systemu Windows (najnowszy instalator kompleksowy ESET PROTECT) - Zalecamy tę opcję uaktualnienia w przypadku, gdy istniejąca kopia serwera Apache Tomcat została zainstalowana za pomocą instalatora kompleksowego.

- Instrukcje dotyczące systemu Windows (uaktualnienie ręczne) - Zaktualizuj serwer Apache Tomcat ręcznie, jeśli instalacja aktualnej kopii Apache Tomcat też była przeprowadzona ręcznie lub jeśli nie masz najnowszego instalatora kompleksowego ESET PROTECT.

- Instrukcje dotyczące systemu Linux

Uaktualnianie serwera Apache Tomcat przy użyciu instalatora kompleksowego (system Windows)

Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT. Ta metoda służy do uaktualniania serwera Apache Tomcat przy użyciu najnowszego instalatora kompleksowego ESET PROTECT 9.1. Zalecamy tę opcję uaktualnienia w przypadku, gdy istniejąca kopia serwera Apache Tomcat została zainstalowana za pomocą instalatora kompleksowego. Można też uaktualnić serwer Apache Tomcat ręcznie.

Przed uaktualnianiem

Utwórz kopie zapasowe następujących plików:

C:\Program Files\Apache Software Foundation\[Tomcat folder]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat folder]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Jeśli używasz niestandardowego magazynu certyfikatów SSL w folderze *Tomcat*, utwórz też kopię zapasową tego certyfikatu.

Apache Tomcat i ograniczenia aktualizacji konsoli internetowej

- Jeśli zainstalowana jest niestandardowa wersja serwera Apache Tomcat (ręczna instalacja usługi Tomcat), kolejne uaktualnienie konsoli internetowej ESET PROTECT za pośrednictwem instalatora kompleksowego lub zadania uaktualnienia składników nie jest obsługiwane.
- Uaktualnienie serwera Apache Tomcat spowoduje usunięcie folderu *era* z lokalizacji *C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps*. Jeśli używasz folderu *era* do przechowywania danych dodatkowych, pamiętaj o wykonaniu kopii zapasowej tych danych przed uaktualnieniem.
- W przypadku użycia użytkownika *C:\Program Files\Apache Software Foundation\[Tomcat folder]*w lokalizacji *webapps* znajdują się dane dodatkowe (inne niż foldery *era* i *ROOT*), uaktualnienie serwera Apache Tomcat nie zostanie przeprowadzone i uaktualniona zostanie wyłącznie konsola internetowa.
- Aktualizacja konsoli internetowej i Apache Tomcat usuwa pliki pomocy offline. Jeśli korzystałeś z pomocy offline w rozwiązaniu ESMC lub starszej wersji programu ESET PROTECT, po aktualizacji konieczne jest jej ponowne utworzenie dla ESET PROTECT 9.1, aby mieć pewność, że Twoja wersja pomocy offline odpowiada wersji ESET PROTECT.

Procedura uaktualniania

1. Pobierz Instalator kompleksowy ESET PROTECT ze strony internetowej firmy ESET i rozpakuj pobrany plik.

2. Jeśli chcesz zainstalować najnowszą wersję serwera Apache Tomcat, a instalator kompleksowy zawiera starszą wersję Apache Tomcat (ten krok jest opcjonalny – jeśli nie potrzebujesz najnowszej wersji Apache Tomcat, przejdź do kroku 4):

   a. Otwórz folder *x64* i przejdź do folderu *installers*.

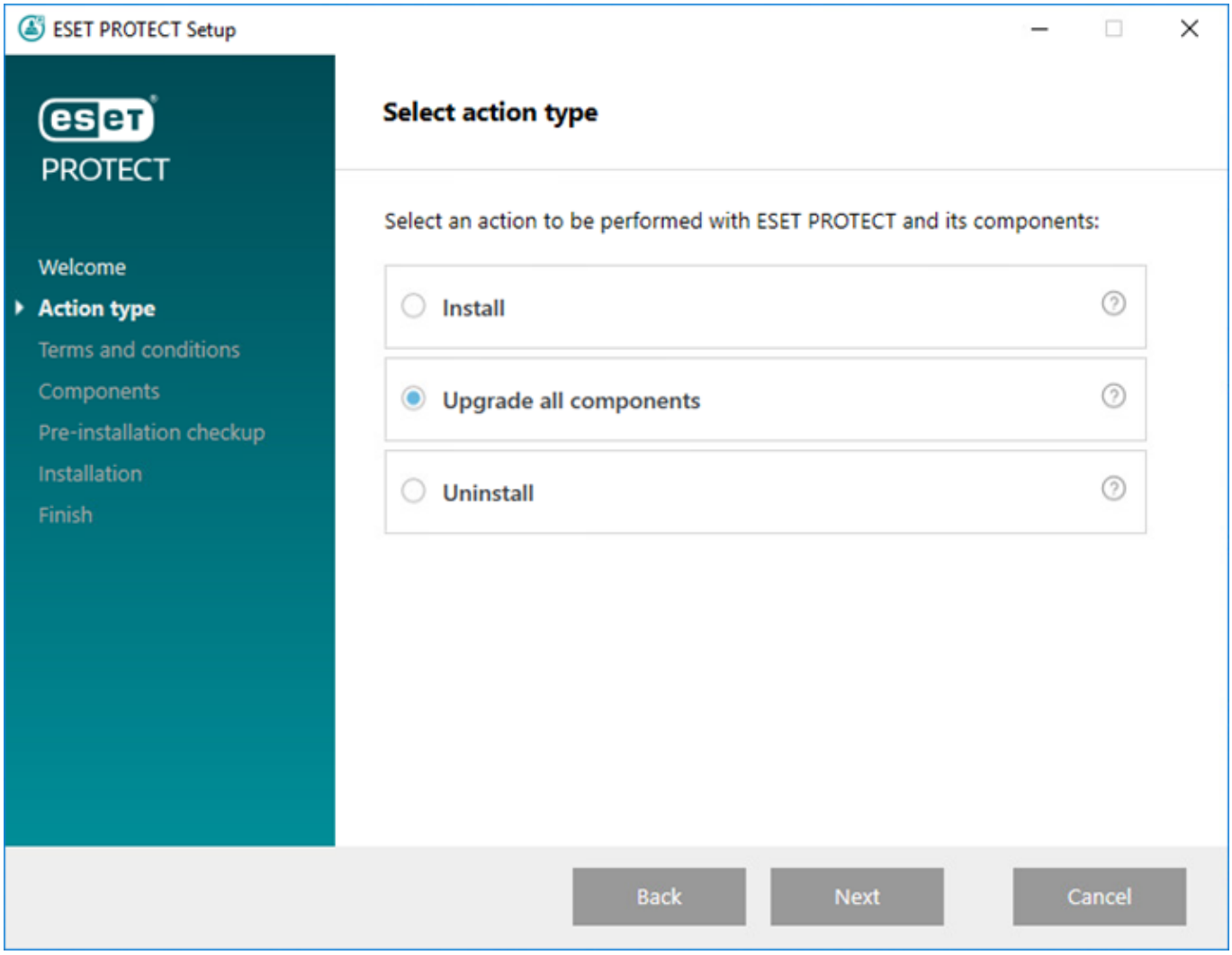
   b. Usuń plik *apache-tomcat-9.0.x-windows-x64.zip* znajdujący się w folderze *installers*.

   c. Pobierz pakiet zip Apache Tomcat 9 dla 64-bitowego systemu Windows.

   d. Przenieś pobrany pakiet zip do folderu *installers*.

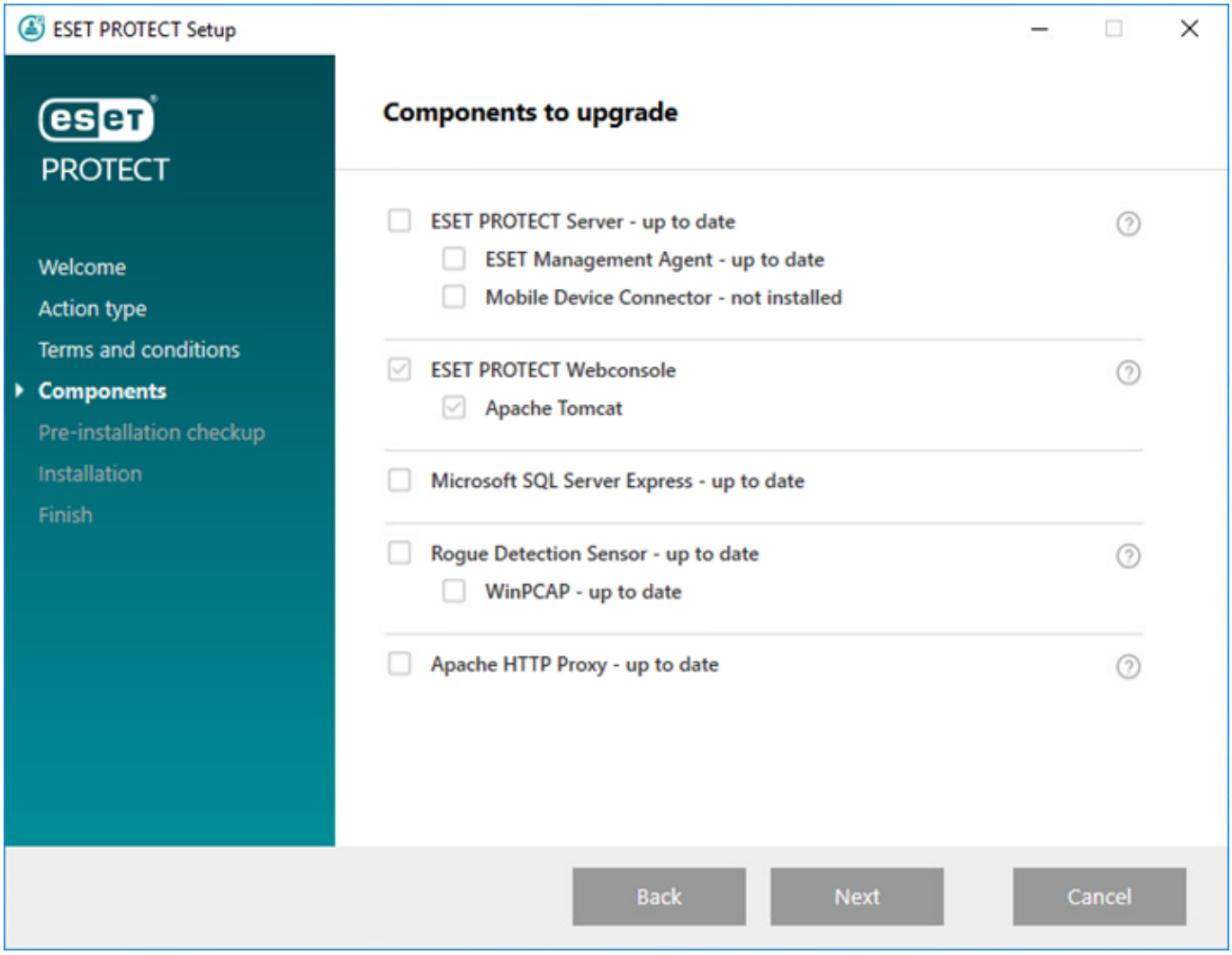
3. Uruchom kompleksowy instalator, klikając dwukrotnie plik *Setup.exe*. Kliknij przycisk **Dalej** na **ekranie powitalnym**.

5. Wybierz opcję **Uaktualnij wszystkie komponenty** i kliknij przycisk **Dalej**.



6. Po zaakceptowaniu umowy EULA kliknij opcję **Dalej**.

7. Instalator kompleksowy automatycznie wykrywa dostępność uaktualnienia: obok komponentów programu ESET PROTECT, które można uaktualnić, widoczne są pola wyboru. Kliknij przycisk **Dalej**.



8. Wybierz instalację środowiska Java na komputerze. Apache Tomcat wymaga 64-bitowego Java/OpenJDK. Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

9. Kliknij przycisk **Uaktualnij**, aby ukończyć uaktualnianie, a następnie kliknij przycisk **Zakończ**.

10. Jeśli konsola internetowa została zainstalowana na innym komputerze niż serwer ESET PROTECT:

a. Zatrzymaj usługę Apache Tomcat: Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Zatrzymaj**.

b.Przywróć plik *EraWebServerConfig.properties* (z kroku 1) do pierwotnej lokalizacji.

c. Uruchom usługę Apache Tomcat. Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Uruchom**.

11. Nawiąż połączenie z konsolą internetową ESET PROTECT i sprawdź, czy wczytuje się ona prawidłowo.

Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Rozwiązywanie problemów

Jeśli uaktualnienie serwera Apache Tomcat się nie powiedzie, zainstaluj poprzednią wersję i zastosuj konfigurację z kroku 1.

Ręczne uaktualnianie serwera Apache Tomcat (system Windows)

Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT. Zaktualizuj serwer Apache Tomcat ręcznie, jeśli instalacja aktualnej kopii Apache Tomcat też była przeprowadzona ręcznie lub jeśli nie masz najnowszego instalatora kompleksowego ESET PROTECT.

Jeśli zainstalowana jest niestandardowa wersja serwera Apache Tomcat (ręczna instalacja usługi Tomcat), kolejne uaktualnienie konsoli internetowej ESET PROTECT za pośrednictwem instalatora kompleksowego lub zadania uaktualnienia składników nie jest obsługiwane.

Przed uaktualnianiem

- Apache Tomcat wymaga 64-bitowego Java/OpenJDK. Jeśli w systemie zainstalowanych jest wiele wersji środowiska Java, zalecamy odinstalowanie starszych wersji środowiska Java i pozostawienie tylko najnowszej wersji obsługiwanego środowiska Java***.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

- Sprawdź aktualnie używaną wersję serwera Apache Tomcat.

  a.Przejdź do folderu instalacji komponentu Apache Tomcat:
  C:\Program Files\Apache Software Foundation\[Tomcat folder]

  b.Otwórz plik RELEASE-NOTES w edytorze tekstu i sprawdź numer wersji (np. 9.0.34).

  c.Jeśli dostępna jest nowsza obsługiwana wersja, przeprowadź uaktualnianie.

Procedura uaktualniania

1. Zatrzymaj usługę Apache Tomcat: Wybierz kolejno **Start** > **Usługi** > kliknij prawym przyciskiem myszy usługę Apache Tomcat i wybierz opcję **Zatrzymaj**.

Zamknij program *Tomcat7w.exe* (jeśli jest uruchomiony) na pasku zadań.

2. Utwórz kopie zapasowe następujących plików:

   C:\Program Files\Apache Software Foundation\[Tomcat folder]\.keystore
   C:\Program Files\Apache Software Foundation\[Tomcat folder]\conf\server.xml
   C:\Program Files\Apache Software Foundation\[Tomcat folder]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

Jeśli używasz niestandardowego magazynu certyfikatów SSL w folderze *Tomcat*, utwórz też kopię zapasową tego certyfikatu.

3. Odinstaluj bieżącą wersję serwera Apache Tomcat.

4. Usuń następujący folder, jeśli nadal znajduje się w systemie:

C:\Program Files\Apache Software Foundation\[Tomcat folder]

5. Pobierz najnowszą obsługiwaną wersję pliku instalatora Apache Tomcat (32-bitowy/64-bitowy instalator usługi systemu Windows) `apache-tomcat-[wersja].exe` z witryny https://tomcat.apache.org.

6. Zainstaluj pobraną nowszą wersję serwera Apache Tomcat:

- Jeśli masz zainstalowanych więcej wersji oprogramowania Java, podczas instalacji wybierz ścieżkę do najnowszej wersji.
- Po zakończeniu instalacji usuń zaznaczenie pola wyboru obok pozycji **Uruchom Apache Tomcat**.

7. Przywróć pliki *.keystore* i *server.xml* oraz certyfikaty niestandardowe do ich pierwotnej lokalizacji.

8. Otwórz plik *server.xml* i upewnij się, że ścieżka *keystoreFile* jest poprawna (zaktualizuj ścieżkę, jeśli serwer Apache Tomcat został zaktualizowany do nowszej wersji z innym numerem na początku):

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat folder]\.keystore"

9. Upewnij się, że konfiguracja połączenia HTTPS serwera Apache Tomcat dla konsoli internetowej ESET PROTECT jest prawidłowa.

10. Wdróż konsolę internetową ESET PROTECT (więcej informacji zawiera sekcja dotycząca instalacji konsoli internetowej w systemie Windows).

11. Przywróć plik *EraWebServerConfig.properties* w jego pierwotnej lokalizacji.

12. Uruchom serwer Apache Tomcat i ustaw prawidłową maszynę wirtualną Java:

a.Przejdź do folderu *C:\Program Files\Apache Software Foundation\[Tomcat folder]\bin* i uruchom program *Tomcat9w.exe*.

b.Na karcie **Ogólne** ustaw **Typ uruchamiania** na **Automatycznie** i naciśnij przycisk **Uruchom**.

c.Kliknij kartę **Java**, usuń zaznaczenie opcji **Użyj wartości domyślnych** i upewnij się, że **Java Virtual Machine** zawiera ścieżkę do pliku *jvm.dll* (zobacz ilustrowane instrukcje w bazie wiedzy), a następnie kliknij **OK**.

13. Nawiąż połączenie z konsolą internetową ESET PROTECT i sprawdź, czy wczytuje się ona prawidłowo.

> Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Rozwiązywanie problemów

- W przypadku niepowodzenia konfiguracji połączenia HTTPS na potrzeby serwera Apache Tomcat możesz pominąć ten krok i użyć tymczasowego połączenia HTTP.
- Jeśli uaktualnienie serwera Apache Tomcat się nie powiedzie, zainstaluj oryginalną wersję i zastosuj konfigurację z kroku 2.
- Aktualizacja konsoli internetowej i Apache Tomcat usuwa pliki pomocy offline. Jeśli korzystałeś z pomocy offline w rozwiązaniu ESMC lub starszej wersji programu ESET PROTECT, po aktualizacji konieczne jest jej ponowne utworzenie dla ESET PROTECT 9.1, aby mieć pewność, że Twoja wersja pomocy offline odpowiada wersji ESET PROTECT.

Uaktualnianie serwera Apache Tomcat (system Linux)

Serwer Apache Tomcat to komponent wymagany do uruchomienia konsoli internetowej ESET PROTECT.

Przed uaktualnianiem

1. Wykonaj następujące polecenie, aby zobaczyć zainstalowaną wersję Apache Tomcat (w niektórych przypadkach nazwa folderu to `tomcat7` lub `tomcat8`):

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. Jeśli jest dostępna nowsza wersja:

   a.Upewnij się, że nowsza wersja jest obsługiwana.

   b.Wykonaj kopię zapasową pliku konfiguracyjnego serwera Tomcat */etc/tomcat7/server.xml*.

Procedura uaktualniania

1. Uruchom następujące polecenie, aby zatrzymać usługę Apache Tomcat (w niektórych przypadkach nazwa usługi to `tomcat7`):

```
sudo systemctl stop tomcat
```

2. Uaktualnij serwer Apache Tomcat i środowisko Java. Przykłady nazw pakietów podane poniżej mogą się różnić od pakietów w repozytorium używanej dystrybucji systemu Linux.

Dystrybucja Linuksa	Polecenia terminala
Debian i Ubuntu	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOS i Red Hat	`yum update` `yum install java-17-openjdk tomcat`
OpenSUSE	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. Zastąp plik */etc/tomcat9/server.xml* plikiem *server.xml* z kopii zapasowej.

4. Otwórz plik *server.xml* i upewnij się, że ścieżka *keystoreFile* jest poprawna.

5. Upewnij się, że połączenie HTTPS dla Apache Tomcat jest poprawnie skonfigurowane.

Zobacz też dodatkowy zasób Konfiguracja konsoli internetowej na potrzeby rozwiązań firmowych lub systemów o niskiej wydajności.

Po uaktualnieniu serwera Apache Tomcat do nowszej głównej wersji (na przykład po uaktualnieniu serwera Apache Tomcat 7.x do wersji 9.x) należy wykonać te czynności:
1.Wdróż ponownie konsolę internetową ESET PROTECT. Więcej informacji zawiera sekcja dotycząca instalacji konsoli internetowej ESET PROTECT w systemie Linux.
2.Użyj ponownie pliku *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* w celu zachowania ustawień niestandardowych w konsoli internetowej ESET PROTECT.
Aktualizacja konsoli internetowej i Apache Tomcat usuwa pliki pomocy offline. Jeśli korzystałeś z pomocy offline w rozwiązaniu ESMC lub starszej wersji programu ESET PROTECT, po aktualizacji konieczne jest jej ponowne utworzenie dla ESET PROTECT 9.1, aby mieć pewność, że Twoja wersja pomocy offline odpowiada wersji ESET PROTECT.

Procedury migracji i ponownej instalacji

Istnieją różne sposoby uaktualniania, migrowania i ponownego instalowania serwera ESET PROTECT oraz innych komponentów programu ESET PROTECT:

- Ponowne instalowanie lub migrowanie programu ESET PROTECT 9 pomiędzy serwerami.

Aby dokonać migracji z jednego serwera ESET PROTECT na drugi, należy wyeksportować wszystkie urzędy certyfikacji i certyfikaty serwera ESET PROTECT lub utworzyć ich kopie zapasowe. W przeciwnym razie żaden z komponentów programu ESET PROTECT nie będzie mógł się komunikować z nowym serwerem ESET PROTECT.

- migracja bazy danych ESET PROTECT
- Migracja komponentu MDM
- Zmiana adresu IP lub nazwy hosta na serwerze ESET PROTECT.
- Migracja z programu ERA 5.x

Zobacz Procedury uaktualniania.

Migracja między serwerami

Istnieje wiele sposobów migracji programu ESET PROTECT między serwerami (mogą one być używane podczas ponownego instalowania serwera ESET PROTECT):

- Czysta instalacja — ten sam adres IP — nowa instalacja nie używa bazy danych ze starego serwera ESET PROTECT i zachowuje pierwotny adres IP.

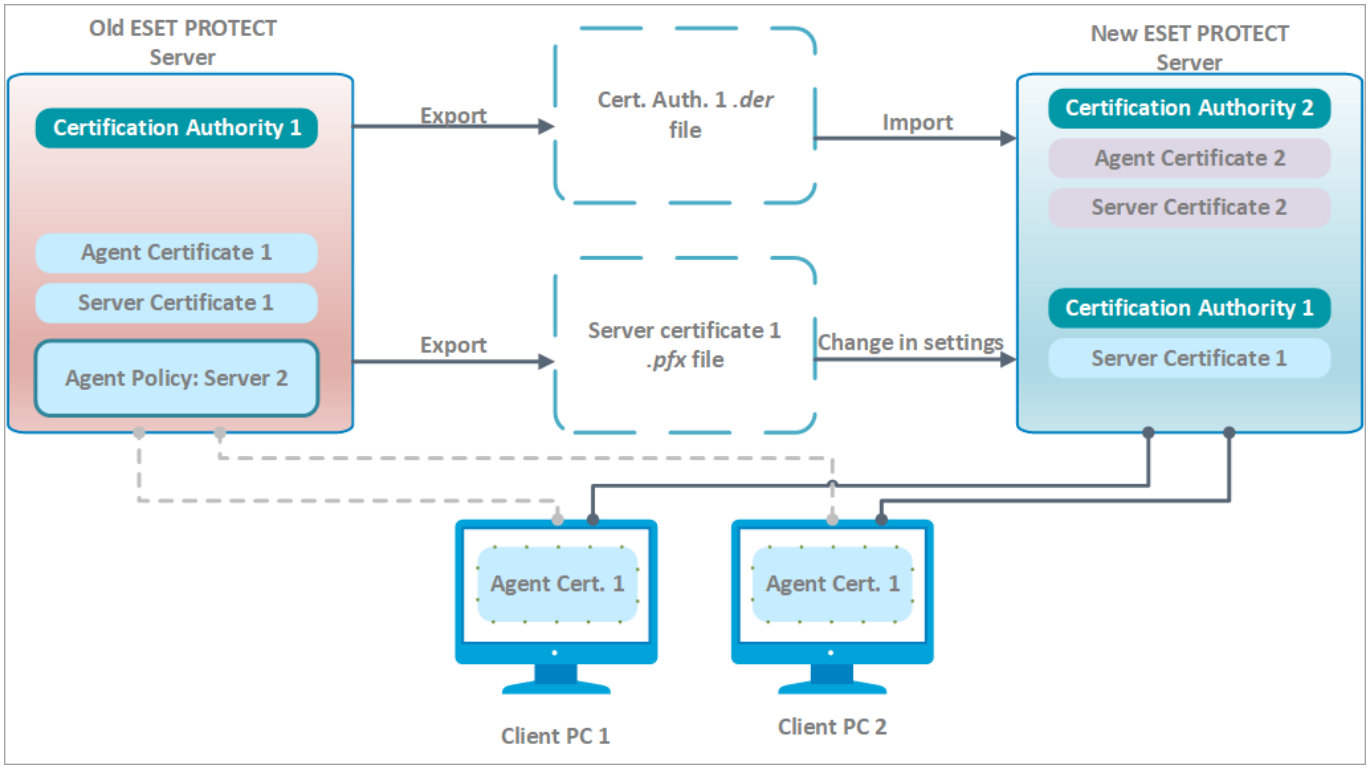
- Czysta instalacja — inny adres IP (artykuł bazy wiedzy) — nowa instalacja nie używa bazy danych ze starego serwera ESET PROTECT i używa innego adresu IP.

- Baza danych poddana migracji — ten sam/inny adres IP — migracja bazy danych może się odbywać tylko między dwoma tymi samymi typami bazy danych (z MySQL do MySQL albo z MS SQL do MS SQL) i tymi samymi wersjami programu ESET PROTECT.

Czysta instalacja, ten sam adres IP

Celem tej procedury jest zainstalowanie zupełnie nowej instancji serwera ESET PROTECT, który nie korzysta z poprzedniej bazy danych. Nowy serwer ESET PROTECT będzie mieć **ten sam adres IP** co poprzedni serwer, ale nie będzie używać bazy danych ze starego serwera ESET PROTECT.

Poniższe instrukcje wymagają, aby stary serwer ESET PROTECT działał z dostępną konsolą internetową. Jeśli stary serwer ESET PROTECT jest niedostępny:
1. Zainstaluj serwer ESET PROTECT lub komponent MDM przy użyciu instalatora kompleksowego (w systemie Windows) lub wybierz inną metodę instalacji (instalacja ręczna w systemie Windows, w systemie Linux lub przy użyciu urządzenia wirtualnego).
2. Nawiąż połączenie z konsolą internetową ESET PROTECT.
3. Dodaj komputery klienckie do infrastruktury ESET PROTECT i wdróż agenta ESET Management lokalnie lub zdalnie.



Powiększyć obraz

❑ **Na bieżącym (starym) serwerze ESET PROTECT:**

Jeśli zarządzasz urządzeniami zaszyfrowanymi za pomocą ESET Full Disk Encryption, wykonaj następujące kroki, aby uniknąć utraty danych odzyskiwania.
1.Przed migracją — Przejdź do **Przegląd stanu** > **Szyfrowanie**. Tutaj możesz **wyeksportować** bieżące **Dane odzyskiwania ESET Full Disk Encryption**.
2.Po migracji należy **Zaimportować Dane odzyskiwaniaESET Full Disk Encryption** do nowej konsoli zarządzania.
Jeśli nie możesz wykonać tych kroków, musisz odszyfrować zarządzane urządzenia przed migracją. Po migracji można szyfrować zarządzane urządzenia za pomocą konsoli internetowej ESET PROTECT.

1. Wyeksportuj certyfikat serwera z obecnego serwera ESET PROTECT i zapisz go w zewnętrznej pamięci masowej.

   • Wyeksportuj wszystkie certyfikaty urzędu certyfikacji z serwera ESET PROTECT i zapisz każdy z nich jako plik *.der*.

   • Wyeksportuj certyfikat serwera z serwera ESET PROTECT do pliku *.pfx*. Wyeksportowany plik *.pfx* będzie zawierał również klucz prywatny.

2. Zatrzymaj usługę serwera ESET PROTECT.

3. Wyłącz komputer pełniący rolę serwera ESET PROTECT.

Nie należy jeszcze odinstalowywać/usuwać starego serwera ESET PROTECT.

❑ **Na nowym serwerze ESET PROTECT:**

Aby używać serwera ESET PROTECT z tym samym adresem IP, należy upewnić się, że konfiguracja sieci na nowym serwerze ESET PROTECT (**adres IP, nazwa FQDN, nazwa komputera, rekord SRV usługi DNS**) odpowiada konfiguracji starego serwera ESET PROTECT.

1. Zainstaluj serwer ESET PROTECT lub komponent MDM przy użyciu instalatora kompleksowego (w systemie Windows) lub wybierz inną metodę instalacji (instalacja ręczna w systemie Windows, w systemie Linux lub przy użyciu urządzenia wirtualnego).

2. Nawiąż połączenie z konsolą internetową ESET PROTECT.

3. Zaimportuj wszystkie urzędy certyfikacji wyeksportowane ze starego serwera ESET PROTECT. W tym celu wykonaj instrukcję dotyczącą importowania klucza publicznego.

4. Zmień certyfikat serwera ESET PROTECT w obszarze **Więcej** > Ustawienia serwera, aby użyć certyfikatu serwera ze starego serwera ESET PROTECT.

5. Zaimportuj wszystkie wymagane licencje firmy ESET do programu ESET PROTECT.

6. Uruchom ponownie usługę serwera ESET PROTECT (szczegóły można znaleźć w naszym artykule bazy wiedzy).

Po jednej lub dwóch interwałach połączenia agenta komputery klienckie powinny łączyć się z nowym serwerem ESET PROTECT przy użyciu oryginalnego certyfikatu agenta ESET Management, który jest uwierzytelniany przez urząd certyfikacji zaimportowany ze starego serwera ESET PROTECT. Jeśli klienty nie nawiązują połączenia, należy zapoznać się z sekcją Problemy po uaktualnieniu/migracji serwera ESET PROTECT.

Podczas dodawania nowych komputerów klienckich certyfikaty agenta należy podpisać przy użyciu nowego agenta certyfikacji. Jest to wymagane, ponieważ zaimportowany urząd certyfikacji nie może być używany do podpisywania nowych certyfikatów równorzędnych — może tylko uwierzytelniać agenty ESET Management komputerów klienckich poddanych migracji.

❑ **Dezinstalacja starego serwera ESET PROTECT lub komponentu MDM:**

Po prawidłowym skonfigurowaniu nowego serwera ESET PROTECT można ostrożnie wycofać z użytku stary serwer ESET PROTECT lub komponent MDM, postępując zgodnie z naszymi szczegółowymi instrukcjami.

Migrowana baza danych — ten sam/inny adres IP

Celem tej procedury jest zainstalowanie zupełnie nowej instancji serwera ESET PROTECT i **zachowanie istniejącej bazy danych ESET PROTECT**, w tym istniejących komputerów klienckich. Nowy serwer ESET PROTECT będzie mieć **ten sam lub inny adres IP**, a baza danych ze starego serwera ESET PROTECT zostanie zaimportowana na nowy serwer przed instalacją.

- Migrowanie baz danych jest obsługiwane tylko między tymi samymi typami baz danych (z MySQL do MySQL lub z MS SQL do MS SQL).
- Migrację bazy danych należy przeprowadzić między instancjami programu ESET PROTECT w tej samej wersji. Instrukcje określania wersji komponentów programu ESET PROTECT zawiera ten artykuł bazy wiedzy. Po zakończeniu migracji bazy danych w razie potrzeby można przeprowadzić uaktualnienie, aby uzyskać najnowszą wersję programu ESET PROTECT.

❑ **Na bieżącym (starym) serwerze ESET PROTECT:**

Zalecamy migrację na inny adres IP tylko dla zaawansowanych użytkowników. Jeśli nowy serwer ESET PROTECT ma **inny adres IP**, wykonaj następujące dodatkowe kroki na bieżącym (starym) serwerze ESET PROTECT:
a)Wygeneruj nowy certyfikat serwera ESET PROTECT (z informacjami o połączeniu dla nowego serwera ESET PROTECT). W przypadku pozostawienia wartości domyślnej (gwiazdka) w polu **Host** następuje dystrybucja certyfikatu bez uwzględnienia konkretnej nazwy DNS i adresu IP.
b)Utwórz politykę, aby ustawić nowy adres IP serwera ESET PROTECT, i przypisz ją do wszystkich komputerów. Poczekaj do zakończenia dystrybucji zasady na wszystkie komputery klienckie (komputery przestaną wysyłać raporty, gdy otrzymają informacje o nowym serwerze).

1. Zatrzymaj usługę serwera ESET PROTECT.

2. Wyeksportuj bazę danych ESET PROTECT lub utwórz jej kopię zapasową.

3. Wyłącz komputer pełniący rolę bieżącego serwera ESET PROTECT (opcjonalnie, jeśli nowy serwer ma inny adres IP).

Nie należy jeszcze odinstalowywać/usuwać starego serwera ESET PROTECT.

❑ **Na nowym serwerze ESET PROTECT:**

Aby używać serwera ESET PROTECT z tym samym adresem IP, należy upewnić się, że konfiguracja sieci na nowym serwerze ESET PROTECT (**adres IP, nazwa FQDN, nazwa komputera, rekord SRV usługi DNS**) odpowiada konfiguracji starego serwera ESET PROTECT.

1. Zainstaluj/uruchom obsługiwaną bazę danych ESET PROTECT.

2. Zaimportuj/przywróć bazę danych ESET PROTECT ze starego serwera ESET PROTECT.

3. Zainstaluj serwer ESET PROTECT lub komponent MDM przy użyciu instalatora kompleksowego (w systemie Windows) lub wybierz inną metodę instalacji (instalacja ręczna w systemie Windows, w systemie Linux lub przy użyciu urządzenia wirtualnego). Podczas instalowania serwera ESET PROTECT zdefiniuj ustawienia połączenia z bazą danych.

4. Nawiąż połączenie z konsolą internetową ESET PROTECT.

5. Przejdź do sekcji **Więcej** > **Ustawienia** > **Połączenie**. Kliknij **Zmień certyfikat** > **Otwórz listę certyfikatów** i wybierz **certyfikat serwera** starego serwera ESET PROTECT, a następnie dwukrotnie kliknij przycisk **OK**.

6. Uruchom ponownie usługę serwera ESET PROTECT.

7. Zaloguj się w konsoli internetowej ESET PROTECT i kliknij pozycję **Komputery**.

Po upływie jednego lub dwóch interwałów między połączeniami agenta komputery klienckie powinny połączyć się z nowym ESET PROTECT serwerem przy użyciu oryginalnego certyfikatu agenta ESET Management. Jeśli klienty nie nawiązują połączenia, należy zapoznać się z sekcją Problemy po uaktualnieniu/migracji serwera ESET PROTECT.

❑ **Dezinstalacja starego serwera ESET PROTECT lub komponentu MDM:**

Po prawidłowym skonfigurowaniu nowego serwera ESET PROTECT można ostrożnie wycofać z użytku stary serwer ESET PROTECT lub komponent MDM, postępując zgodnie z naszymi szczegółowymi instrukcjami.

migracja bazy danych ESET PROTECT

Poniższe instrukcje dotycząc migracji bazy danych ESET PROTECT między różnymi instancjami programu SQL Server (dotyczy to również migracji do innych wersji programu SQL Server lub migracji do programu SQL Server zainstalowanego na innym komputerze):

- Procedura migracji programu MS SQL Server
- Procedura migracji programu MySQL Server

Procedura migracji programu MS SQL Server

Procedura migracji jest taka sama w przypadku programów **Microsoft SQL Server** oraz **Microsoft SQL Server Express**.

Dodatkowe informacje można znaleźć w następującym artykule bazy wiedzy firmy Microsoft: https://msdn.microsoft.com/en-us/library/ms189624.aspx.

Wymagania wstępne

- Zainstalowana źródłowa i docelowa instancja programu SQL Server. Mogą być hostowane na różnych komputerach.

• Docelowa instancja programu SQL Server musi być co najmniej w tej samej wersji co instancja źródłowa. **Migracja do starszej wersji nie jest obsługiwana!**

• Zainstalowane musi być narzędzie **SQL Server Management Studio**. Jeśli instancje programu SQL Server znajdują się na różnych komputerach, narzędzie to musi być zainstalowane na obu komputerach.

Migracja przy użyciu narzędzia SQL Server Management Studio.

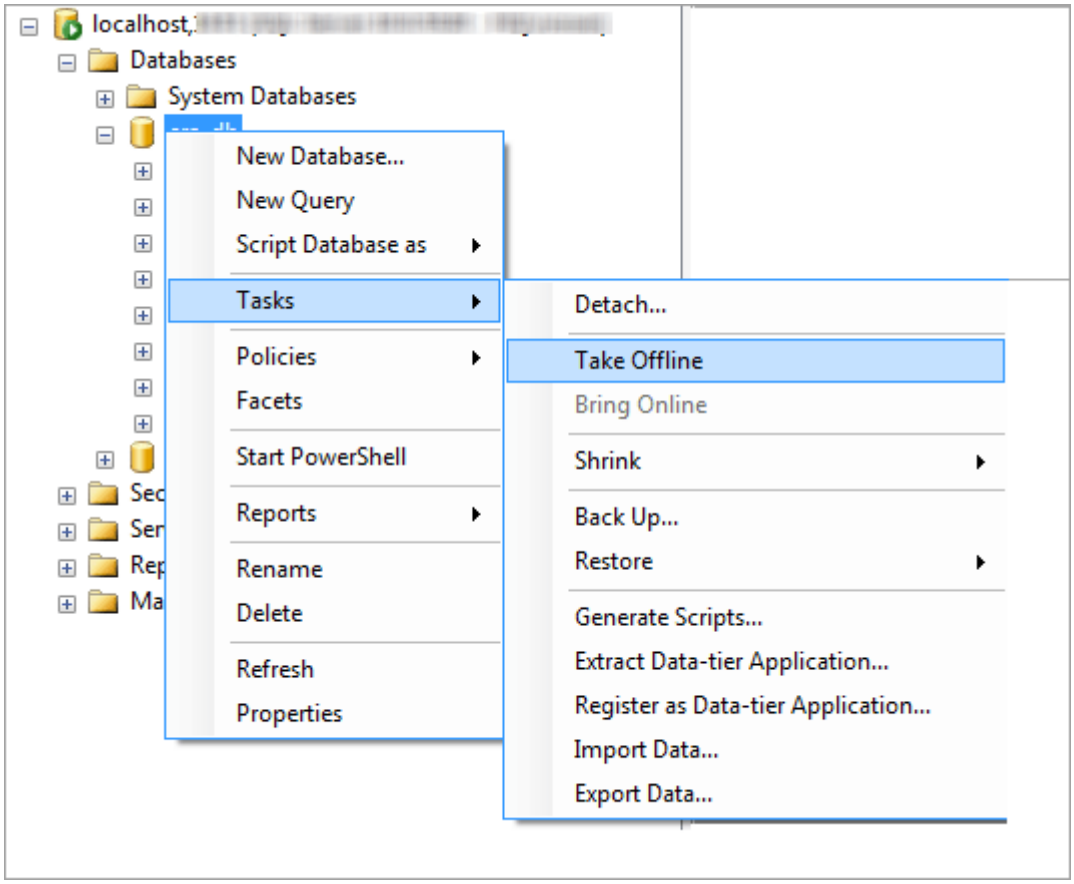
1. Zatrzymaj usługę serwera ESET PROTECT (lub usługę serwera ESMC) lub usługę MDM ESET PROTECT.

Nie należy uruchamiać serwera ESET PROTECT ani komponentu MDM ESET PROTECT przed ukończeniem wszystkich poniższych kroków.

2. Zaloguj się do źródłowej instancji programu SQL Server przy użyciu narzędzia SQL Server Management Studio.

3. Utwórz pełną kopię zapasową bazy danych, która ma zostać podana migracji. Zalecamy podanie nowej nazwy zestawu kopii zapasowych. W przeciwnym razie, jeśli zestaw kopii zapasowych był już wcześniej używany, nowa kopia zapasowa zostanie do niego dołączona, co spowoduje niepotrzebne zwiększenie objętości pliku kopii zapasowej.

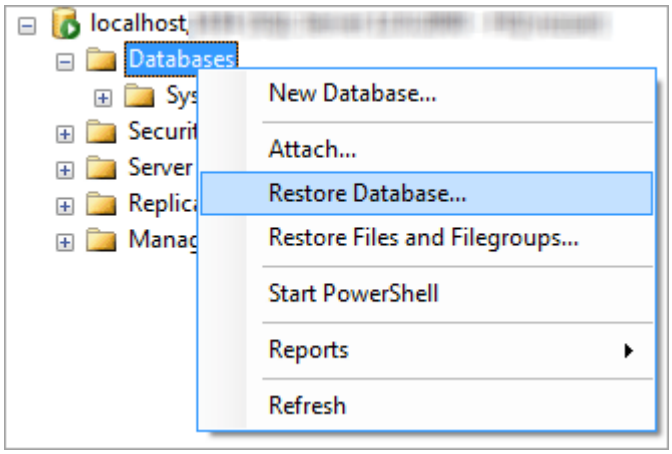
4. Przełącz źródłową bazę danych do trybu offline, wybierając opcje **Zadania** > **Przełącz do trybu offline**.



5. Skopiuj plik kopii zapasowej (*.bak*) utworzony w kroku 3 do lokalizacji dostępnej dla docelowej instancji programu SQL Server. Konieczna może być edycja uprawnień dostępu do pliku kopii zapasowej bazy danych.

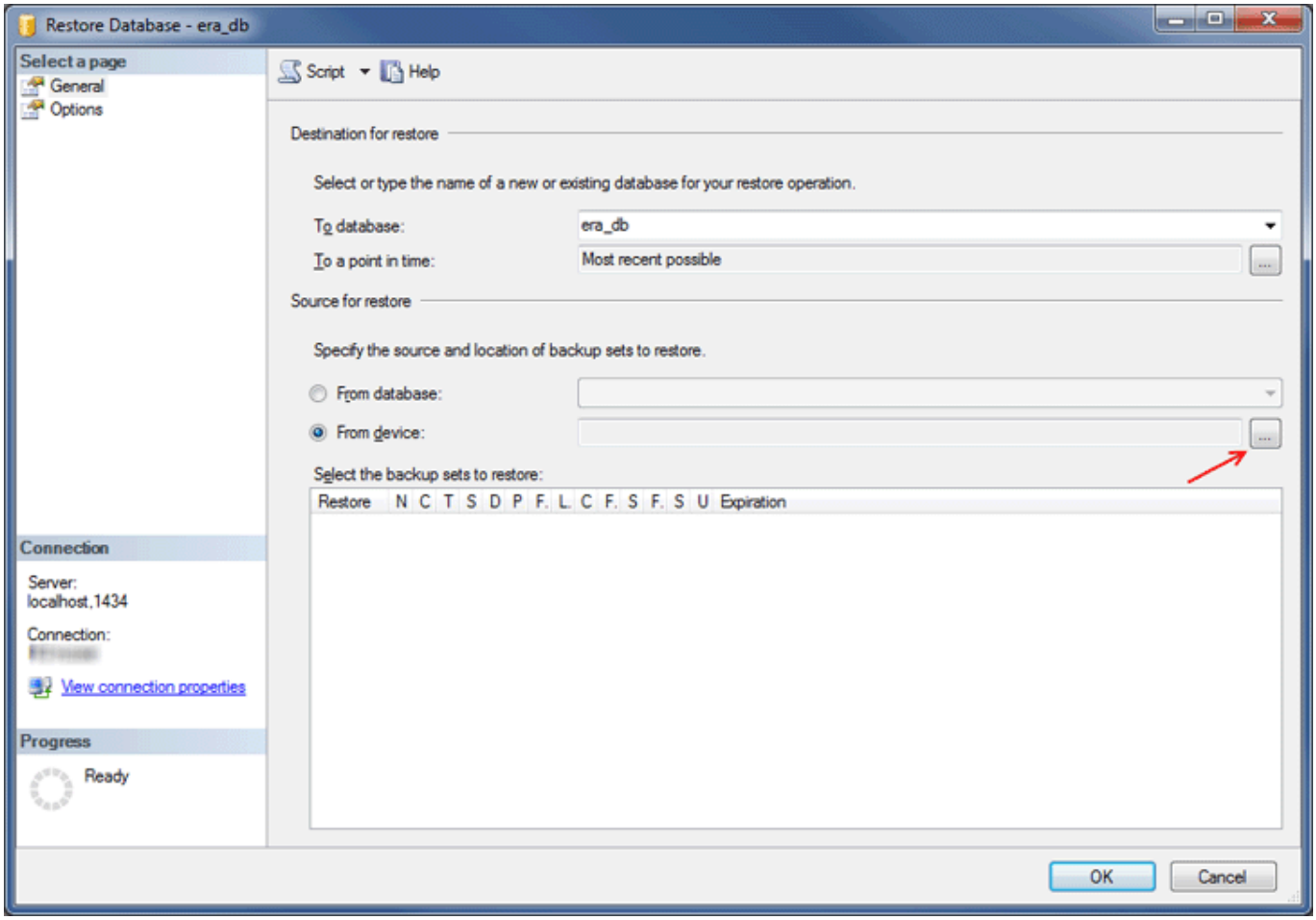
6. Zaloguj się do docelowej instancji programu SQL Server przy użyciu narzędzia SQL Server Management Studio.

7. Przywróć bazę danych w docelowej instancji programu SQL Server.



8. Wpisz nazwę nowej bazy danych w polu **Do bazy danych**. Możesz nazwać ją tak samo jak starą bazę danych.

9. Wybierz opcję Z urządzenia w obszarze **Określ źródło i lokalizację zestawów kopii zapasowych do przywrócenia**, a następnie kliknij przycisk … .

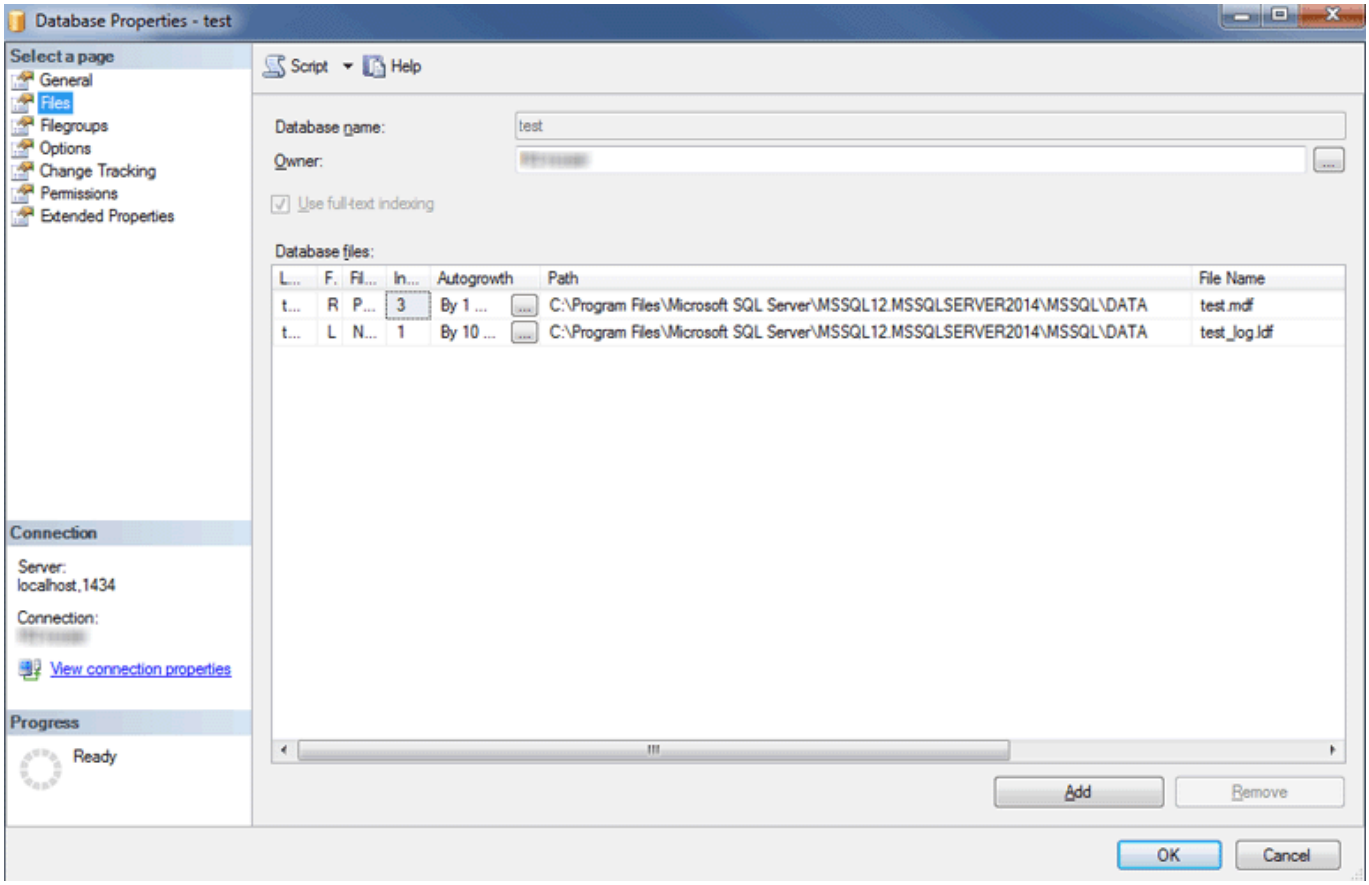


10. Kliknij opcję **Dodaj, przejdź do pliku kopii zapasowej i otwórz go**.

11. Wybierz najnowszą z dostępnych kopii zapasowych do przywrócenia (w zestawie kopii zapasowych może się znajdować większa liczba kopii zapasowych).

12. Kliknij stronę **Opcje** w kreatorze przywracania. Można też wybrać opcję **Zastąp istniejącą bazę danych** i sprawdzić, czy lokalizacje przywracania bazy danych (*.mdf*) oraz dziennika (*.ldf*) są poprawne. Pozostawienie wartości domyślnych bez zmian spowoduje użycie ścieżek ze źródłowej instancji programu SQL Server, dlatego należy sprawdzić te wartości.

- Jeśli nie wiesz, gdzie w docelowej instancji programu SQL Server zapisywane są pliki bazy danych, kliknij prawym przyciskiem myszy istniejącą bazę danych, wybierz pozycję **Właściwości** i kliknij kartę **Pliki**. Katalog, w którym zapisana jest baza danych, jest widoczny w kolumnie **Ścieżka** w tabeli przedstawionej poniżej.

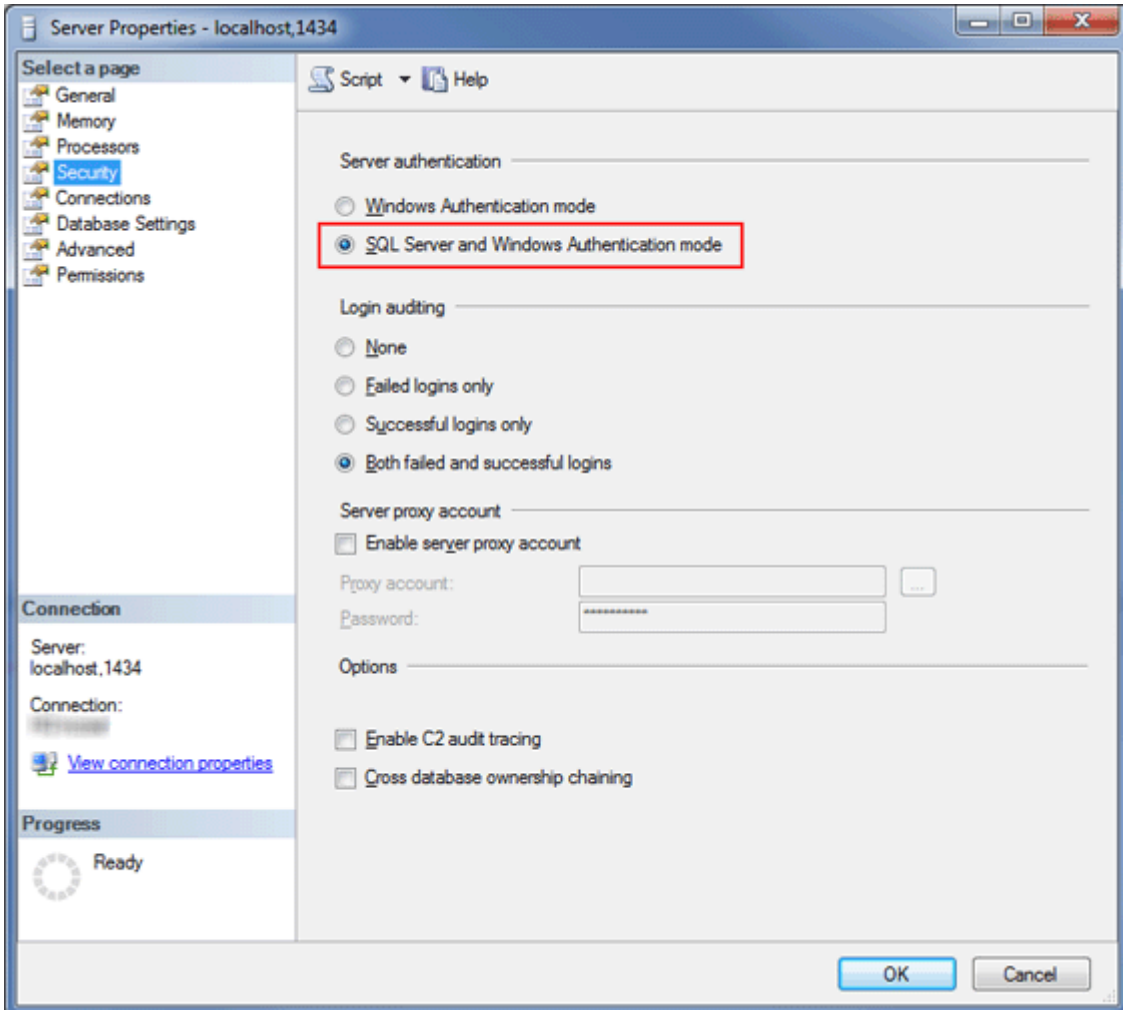


13. Kliknij przycisk **OK** w oknie kreatora przywracania.

14. Kliknij prawym przyciskiem myszy bazę danych **era_db**, wybierz opcję **Nowe zapytanie** i uruchom poniższe zapytanie, aby usunąć zawartość tabeli **tbl_authentication_certificate** (w przeciwnym razie agenty mogą nie być w stanie połączyć się z nowym serwerem):

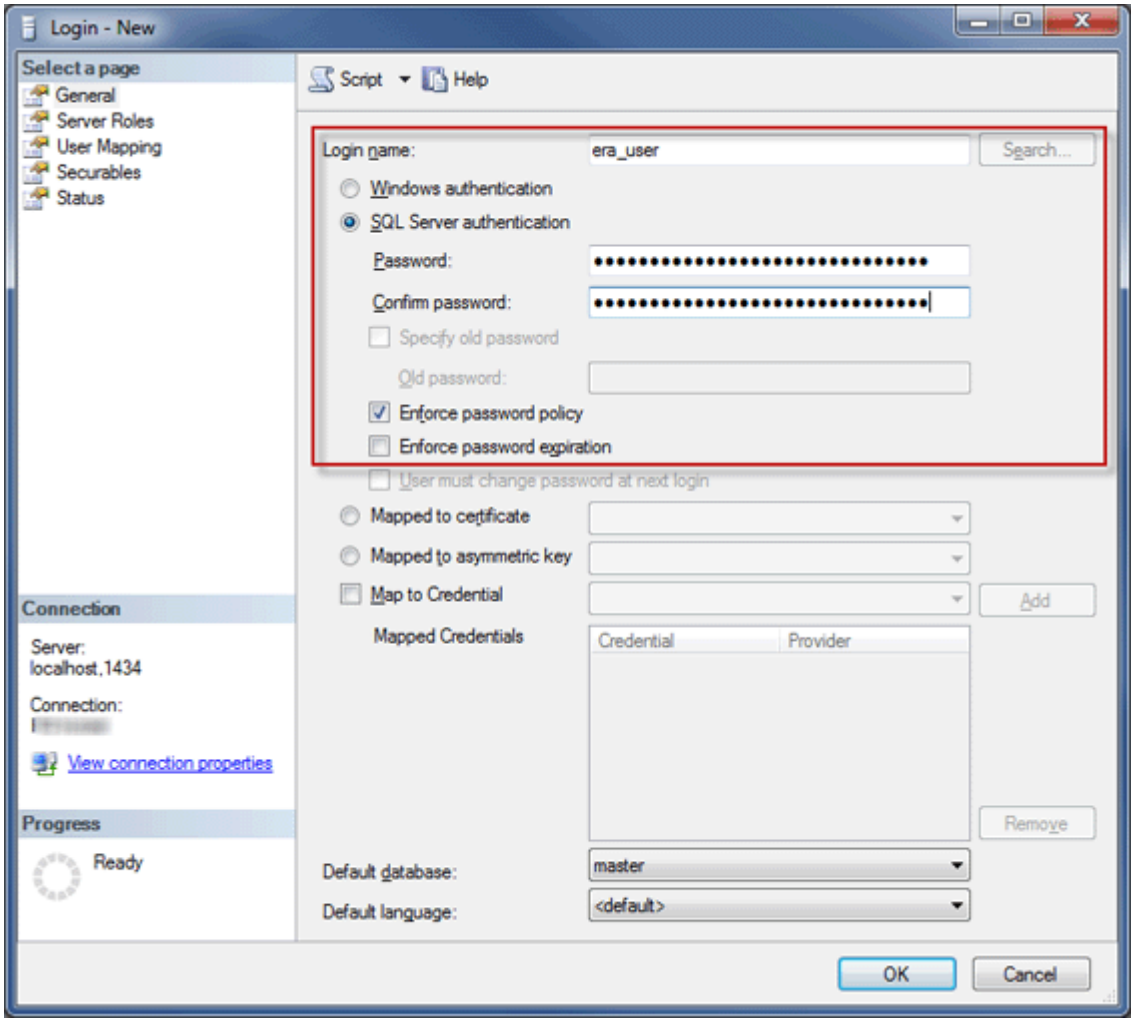
```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. Sprawdź, czy na nowym serwerze bazy danych **włączone jest uwierzytelnianie programu SQL Server**. Kliknij serwer prawym przyciskiem myszy i kliknij pozycję **Właściwości**. Przejdź do obszaru **Zabezpieczenia** i sprawdź, czy wybrano **Tryb uwierzytelniania programu SQL Server oraz Tryb uwierzytelniania Windows**.

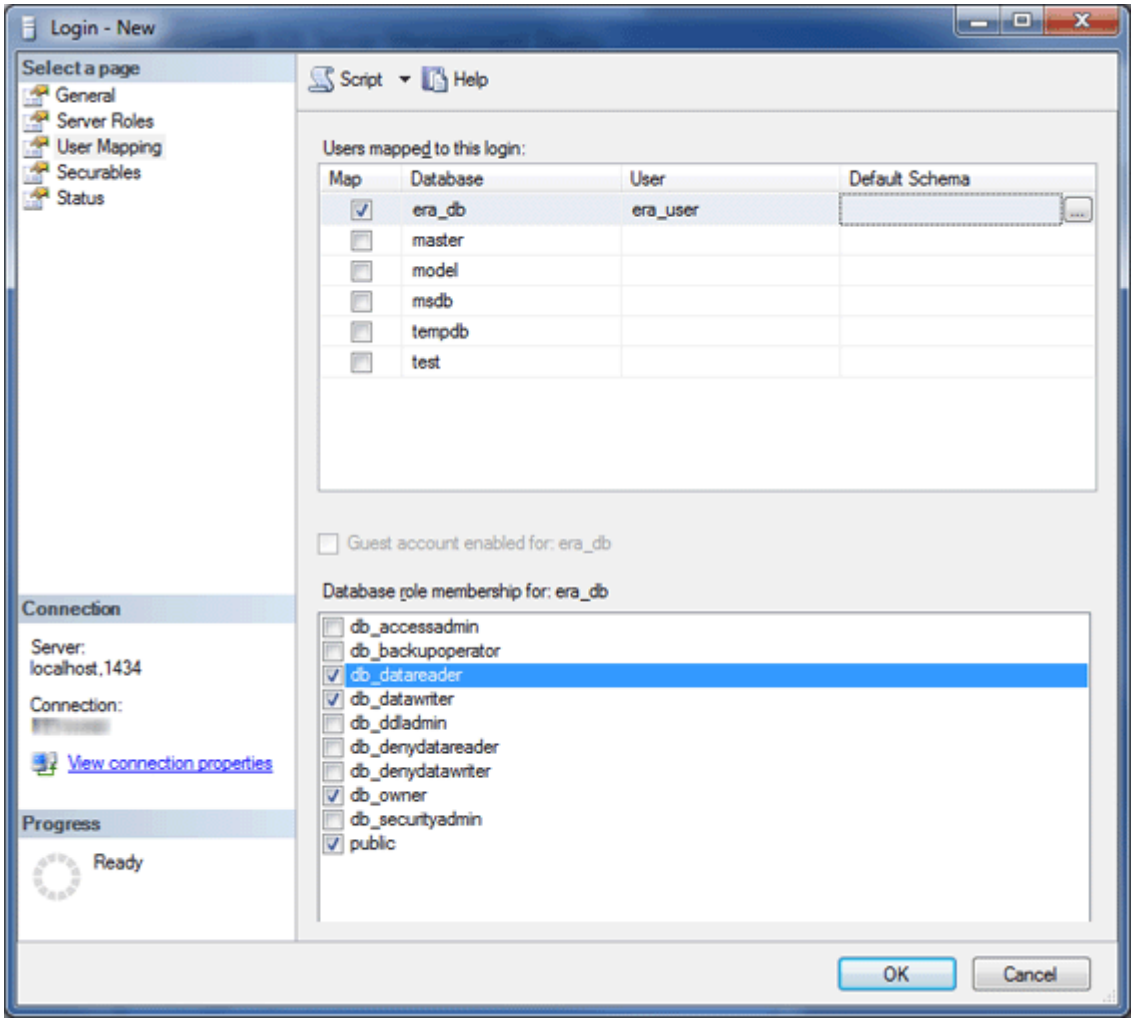


16. Utwórz nową nazwę użytkownika programu SQL Server (na potrzeby serwera ESET PROTECT/komponentu MDM ESET PROTECT) w docelowej instancji programu SQL Server z **uwierzytelnianiem programu SQL Server**, przypisując ją do użytkownika w przywróconej bazie danych.

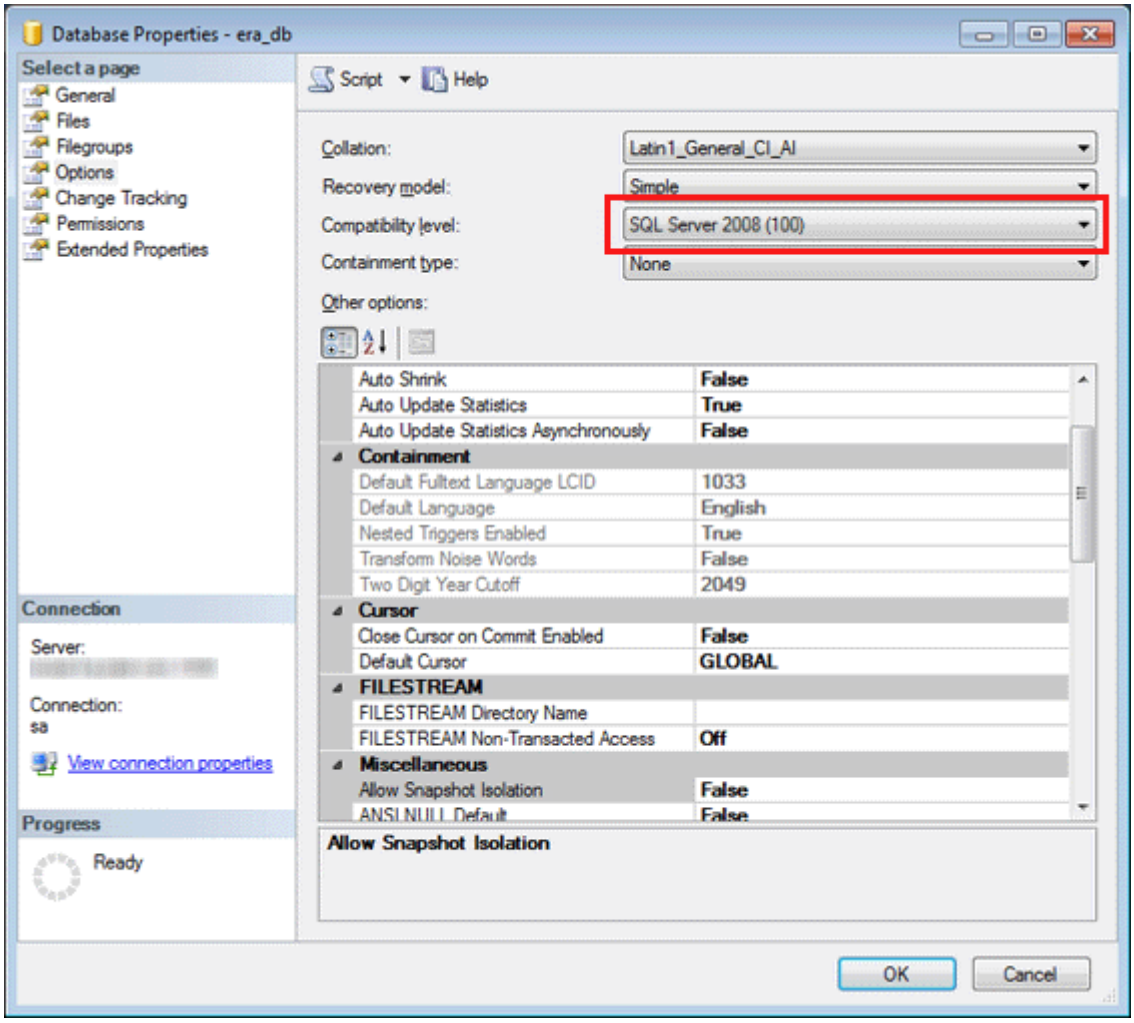
- Nie wymuszaj wygasania hasła!
- Znaki zalecane w przypadku nazw użytkowników:
  - Małe litery z zestawu znaków ASCII, cyfry oraz znak podkreślenia „_”
- Znaki zalecane w przypadku haseł:
  - TYLKO znaki z zestawu znaków ASCII, w tym małe i wielkie litery z zestawu znaków ASCII, cyfry, spacje i znaki specjalne
- Nie należy używać znaków spoza zestawu znaków ASCII, nawiasów klamrowych {} ani znaku @
- Uwaga: W razie niezastosowania się do powyższych zaleceń dotyczących znaków możliwe są problemy z komunikacją z bazą danych lub konieczne może być anulowanie znaków specjalnych na późniejszych etapach, podczas modyfikacji ciągu połączenia bazy danych. Reguły anulowania znaków nie zostały opisane w niniejszym dokumencie.



17. Zmapuj nazwę użytkownika, przypisując ją do użytkownika w docelowej bazie danych. Na **karcie mapowań** użytkowników sprawdź, czy do użytkownika bazy danych przypisane są następujące role: **db_datareader**, **db_datawriter**, **db_owner**.

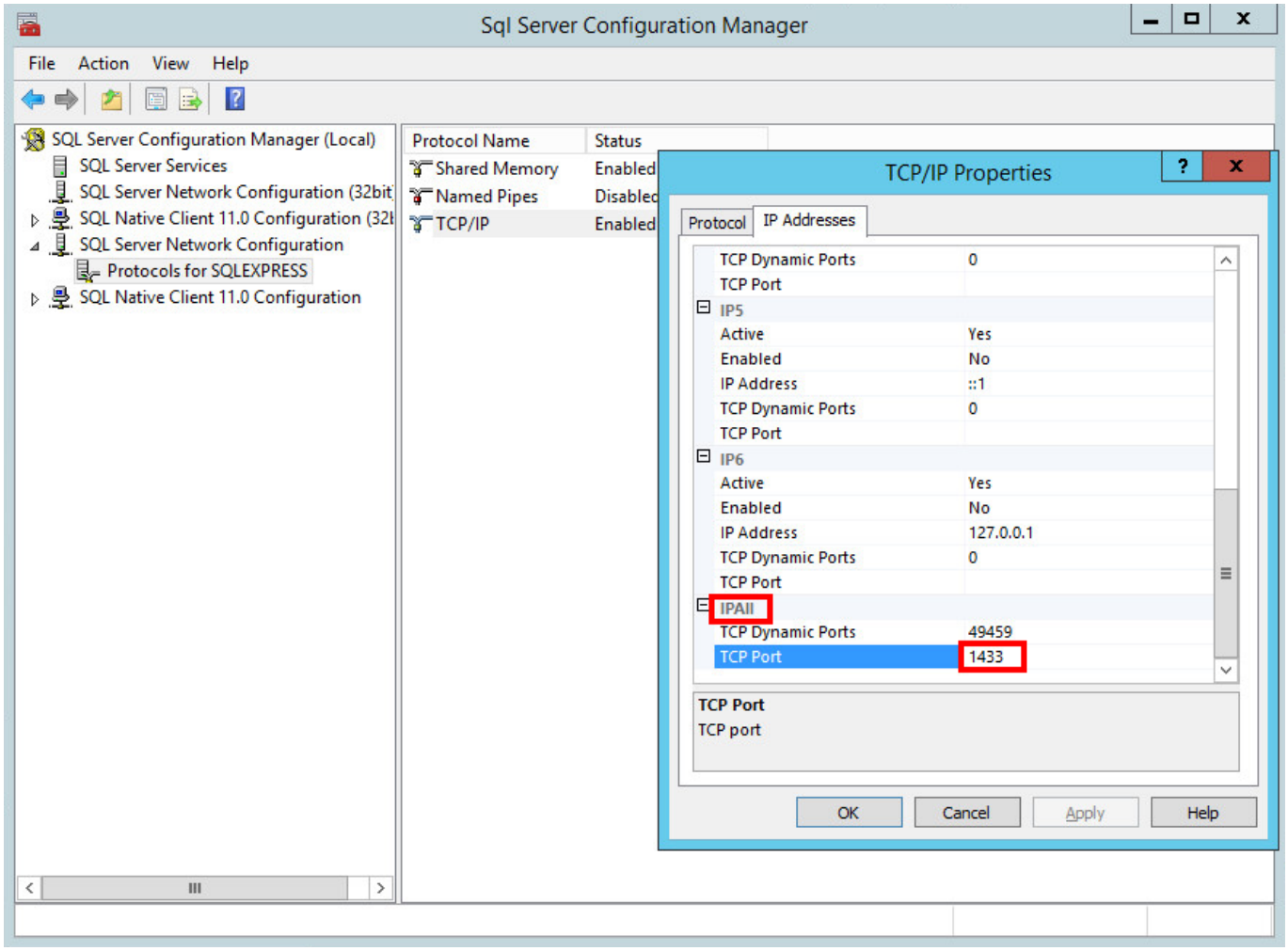


18. Aby włączyć najnowsze funkcje serwera bazy danych, zmień **poziom zgodności** w przywróconej bazie danych na najnowszy. Kliknij nową bazę danych prawym przyciskiem myszy i otwórz obszar **Właściwości** bazy danych.



> W narzędziu SQL Server Management Studio nie można określać poziomów zgodności nowszych od wersji, która jest w użyciu. Na przykład w narzędziu SQL Server Management Studio 2014 nie można ustawić poziomu zgodności z programem SQL Server 2019.

19. Upewnij się, że protokół połączenia **TCP/IP** jest **włączony** na potrzeby programu „db_instance_name” (na przykład SQLEXPRESS lub MSSQLSERVER), a **port** TCP/IP to **1433**. Aby to zrobić, otwórz narzędzie **Sql Server Configuration Manager**, przejdź do pozycji **SQL Server Network Configuration** > **Protocols for db_instance_name** (Konfiguracja sieci serwera SQL > Protokoły dla db_instance_name), kliknij prawym przyciskiem myszy pozycję **TCP/IP** i wybierz opcję **Enabled** (Włączony). Kliknij dwukrotnie pozycję **TCP/IP**, przejdź na kartę **Protokoły**, przewiń w dół do pozycji **IPAll** i w polu **TCP Port** (Port TCP) wprowadź wartość 1433. Kliknij przycisk **OK** i uruchom ponownie usługę **SQL Server**.



20. Łączenie serwera ESET PROTECT lub komponentu MDM z bazą danych.

Procedura migracji programu MySQL Server

Wymagania wstępne

• Zainstalowana źródłowa i docelowa instancja programu SQL Server. Mogą być hostowane na różnych komputerach.

• Narzędzia MySQL muszą być dostępne na co najmniej jednym z komputerów (`mysqldump` i kliencie mysql).

Przydatne łącza

- 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

Procedura migracji

W przedstawionych dalej poleceniach, plikach konfiguracyjnych oraz instrukcjach SQL należy zawsze zastępować zmienne według poniższych instrukcji:
- **SRCHOST** zastąp adresem serwera źródłowej bazy danych
- **SRCROOTLOGIN** zastąp nazwą użytkownika źródłowego serwera głównego MySQL
- **SRCDBNAME** zastąp nazwą źródłowej bazy danych ESET PROTECT, której kopię zapasową chcesz utworzyć
- **BACKUPFILE** zastąp ścieżką do pliku, w którym zostanie zapisana kopia zapasowa
- **TARGETROOTLOGIN** zastąp nazwą użytkownika docelowego serwera głównego MySQL
- **TARGETHOST** zastąp adresem serwera docelowej bazy danych
- **TARGETDBNAME** zastąp nazwą docelowej bazy danych ESET PROTECT (po migracji)
- **TARGETLOGIN** zastąp nazwą użytkownika nowej bazy danych ESET PROTECT na docelowym serwerze bazy danych
- **TARGETPASSWD** zastąp hasłem nowego użytkownika bazy danych ESET PROTECT na docelowym serwerze bazy danych

Poniższych instrukcji SQL nie trzeba wykonywać przy użyciu wiersza polecenia. Jeśli dostępne jest narzędzie z graficznym interfejsem użytkownika, można skorzystać ze znanej aplikacji.

1. Zatrzymaj usługę serwera ESET PROTECT/MDM.

2. Utwórz pełną kopię zapasową źródłowej bazy danych ESET PROTECT (bazy danych, która ma zostać poddana migracji):

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. Przygotuj pustą bazę danych na docelowym serwerze MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

W systemie Linux zamiast znaku cudzysłowu (") należy używać znaku apostrofu (').

4. Na docelowym serwerze MySQL przywróć bazę danych do przygotowanej wcześniej pustej bazy danych:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. Utwórz użytkownika bazy danych ESET PROTECT na docelowym serwerze MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

Znaki zalecane w przypadku elementu **TARGETLOGIN:**

- Małe litery z zestawu znaków ASCII, cyfry oraz znak podkreślenia „_”

Znaki zalecane w przypadku elementu **TARGETPASSWD:**

- Tylko znaki z zestawu znaków ASCII, w tym małe i wielkie litery z zestawu znaków ASCII, cyfry, spacje i znaki specjalne
- Nie należy używać znaków spoza zestawu znaków ASCII, nawiasów klamrowych {} ani znaku @

Uwaga: W razie niezastosowania się do powyższych zaleceń dotyczących znaków możliwe są problemy z komunikacją z bazą danych lub konieczne może być anulowanie znaków specjalnych na późniejszych etapach, podczas modyfikacji ciągu połączenia bazy danych. Reguły anulowania znaków nie zostały opisane w niniejszym dokumencie.

6. Nadaj odpowiednie uprawnienia dostępu użytkownikowi bazy danych ESET PROTECT na docelowym serwerze MySQL:

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

W systemie Linux zamiast znaku cudzysłowu (") należy używać znaku apostrofu (').

7. Usuń zawartość tabeli **tbl_authentication_certificate** (w przeciwnym razie agenty mogą nie być w stanie połączyć się z nowym serwerem):

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. Łączenie serwera ESET PROTECT lub komponentu MDM z bazą danych.

Łączenie serwera ESET PROTECT lub komponentu MDM z bazą danych

Wykonaj poniższe czynności na komputerze z zainstalowanym serwerem ESET PROTECT lub komponentem ESET PROTECT MDM, aby połączyć go z bazą danych.

1. Zatrzymaj usługę serwera ESET PROTECT/komponentu MDM.
2. Znajdź plik *startupconfiguration.ini*
   - Windows:

Serwer:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore:

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

- System Linux :

Serwer:

/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini

MDMCore:

/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini

3. Zmień ciąg połączenia z bazą danych w pliku *startupconfiguration.ini* serwera ESET PROTECT/komponentu MDM

- Skonfiguruj adres i port nowego serwera bazy danych.
- Ustaw nową nazwę użytkownika i hasło ESET PROTECT w ciągu połączenia.

Efekt końcowy powinien wyglądać następująco:

- MS SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL:

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

W powyższej konfiguracji należy zawsze zmieniać:
- **TARGETHOST** zastąp adresem serwera docelowej bazy danych
- **TARGETDBNAME** zastąp nazwą docelowej bazy danych ESET PROTECT (po migracji)
- **TARGETLOGIN** zastąp nazwą użytkownika nowej bazy danych ESET PROTECT na docelowym serwerze bazy danych
- **TARGETPASSWD** zastąp hasłem nowego użytkownika bazy danych ESET PROTECT na docelowym serwerze bazy danych

4. Uruchom serwer ESET PROTECT lub komponent MDM ESET PROTECT i sprawdź, czy usługa działa prawidłowo.

Migracja komponentu MDM

Celem tej procedury jest przeprowadzenie procesu migracji obecnej instancji komponentu MDM ESET PROTECT i **zachowanie istniejącej bazy danych MDM ESET PROTECT**, w tym zarejestrowanych urządzeń mobilnych. Komponent MDM ESET PROTECT objęty migracją będzie miał **ten sam adres IP/nazwę hosta** co stary komponent MDM ESET PROTECT, a baza danych ze starego komponentu MDM ESET PROTECT zostanie zaimportowana na nowy host MDM przed instalacją.

- Migrowanie baz danych jest obsługiwane tylko między tymi samymi typami baz danych (z MySQL do MySQL lub z MS SQL do MS SQL).
- Migrację bazy danych należy przeprowadzić między instancjami programu ESET PROTECT w tej samej wersji. Instrukcje określania wersji komponentów programu ESET PROTECT zawiera ten artykuł bazy wiedzy. Po zakończeniu migracji bazy danych w razie potrzeby można przeprowadzić uaktualnienie, aby uzyskać najnowszą wersję programu ESET PROTECT.

❑ **Na obecnym (starym) serwerze MDM ESET PROTECT:**

1. Utwórz kopię zapasową konfiguracji MDM.

   a)W obszarze **Komputery** kliknij serwer MDM i wybierz pozycję **Szczegóły**.

   b)Kliknij pozycję **Konfiguracja** > **Konfiguracja żądania**. Może być konieczne odczekanie chwilę (w zależności od interwału połączenia agenta) do momentu utworzenia żądanej konfiguracji.

   c)Kliknij Mobile Device Connector **ESET PROTECT** i wybierz pozycję **Otwórz konfigurację**.

   d)Wyeksportuj następujące elementy z konfiguracji do zewnętrznej pamięci masowej:

   - Dokładna nazwa hosta serwera MDM.
   - Certyfikaty równorzędne – wyeksportowany plik *.pfx* będzie zawierał klucz prywatny.

   Jeśli używasz serwera MDM produktu ESET PROTECT w systemie Linux, musisz wyeksportować certyfikat HTTPS z zasad konfiguracji MDM:
   I.Kliknij pozycję **Wyświetl** obok pozycji **Certyfikat HTTPS**.
   II.Kliknij pozycję **Pobierz** i pobierz certyfikat HTTPS w formacie PFX.

   e)Wyeksportuj także następujące certyfikaty i tokeny (o ile istnieją):

   - Certyfikat podpisywania profilu rejestracji.
   - certyfikat APNS (wyeksportuj zarówno certyfikat APNS, jak i klucz prywatny APNS).
   - Token autoryzacji programu rejestracji urządzeń firmy Apple (Device Enrollment Program — DEP).

2. Zatrzymaj usługę MDM ESET PROTECT.

3. Wyeksportuj bazę danych MDM ESET PROTECT lub wykonaj jej kopię zapasową.

4. Wyłącz komputer z obecnym komponentem MDM ESET PROTECT.

Nie należy jeszcze odinstalowywać ani usuwać starego komponentu MDM ESET PROTECT.

❑ **Na nowym serwerze MDM ESET PROTECT:**

Należy się upewnić, że konfiguracja sieci na nowym serwerze MDM ESET PROTECT (nazwa hosta wyeksportowana z konfiguracji starego serwera MDM) odpowiada konfiguracji starego serwera MDM ESET PROTECT.

1. Zainstaluj/uruchom obsługiwaną ESET PROTECT bazę danych MDM.

2. Zaimportuj/przywróć bazę danych MDM ESET PROTECT ze starego serwera MDM ESET PROTECT.

3. Zainstaluj serwer ESET PROTECT lub komponent MDM przy użyciu instalatora kompleksowego (w systemie Windows) lub wybierz inną metodę instalacji (instalacja ręczna w systemie Windows, w systemie Linux lub przy użyciu urządzenia wirtualnego). Na etapie instalacji komponentu MDM ESET PROTECT określ ustawienia połączenia z bazą danych.

Podczas instalowania serwera MDM produktu ESET PROTECT na Linuksie użyj certyfikatu HTTPS z kopii zapasowej.

4. Połącz się z konsolą internetową ESET PROTECT.

5. Uruchom ponownie usługę MDM ESET PROTECT.

Zarządzane urządzenia mobilne powinny teraz łączyć się z nowym serwerem MDM ESET PROTECT przy użyciu oryginalnego certyfikatu.

❑ **Dezinstalacja starego serwera ESET PROTECT lub komponentu MDM:**

Po prawidłowym skonfigurowaniu nowego serwera ESET PROTECT można ostrożnie wycofać z użytku stary serwer ESET PROTECT lub komponent MDM, postępując zgodnie z naszymi szczegółowymi instrukcjami.

Zmienianie adresu IP lub nazwy hosta serwera ESET PROTECT po migracji

Aby zmienić adres IP lub nazwę hosta serwera ESET PROTECT, należy wykonać poniższe kroki:

1. Jeśli certyfikat serwera ESET PROTECT zawiera określony adres IP i/lub nazwę hosta, utwórz nowy certyfikat serwera zawierający nowy adres IP i nową nazwę hosta, z którym nawiązujesz połączenie. Jeśli jednak pole hosta certyfikatu Serwera zawiera symbol wieloznaczny *, **przejdź do kroku 2**. Jeśli to pole nie zawiera symbolu wieloznacznego, utwórz nowy certyfikat Serwera, dodając nowy adres IP i nową nazwę hosta oddzielone przecinkiem oraz dodaj poprzedni adres IP oraz poprzednią nazwę hosta.

2. Podpisz nowy certyfikat serwera przy użyciu urzędu certyfikacji serwera ESET PROTECT.

3. Utwórz politykę przekierowującą połączenia z klientem na nowy adres IP lub pod nową nazwę hosta (preferowany jest adres IP). Dodaj też informacje o drugim (alternatywnym) połączeniu ze starym adresem IP lub starą nazwą hosta, aby umożliwić agentowi ESET Management łączenie się z obydwoma serwerami. Więcej

informacji zawiera artykuł Tworzenie polityki dla agenta ESET Management na potrzeby połączenia z nowym serwerem ESET PROTECT.

4. Zastosuj tę politykę na komputerach klienckich i zezwól na replikację przez agenty ESET Management. Chociaż polityka może przekierowywać klienty na nowy serwer (który nie jest uruchomiony), agenty ESET Management będą używać alternatywnych informacji o serwerze, aby łączyć się z pierwotnym adresem IP.

5. Ustaw nowy certyfikat serwera w sekcji Więcej > Ustawienia.

6. Uruchom ponownie usługę serwera ESET PROTECT i zmień adres IP lub nazwę hosta.

Ilustrowane instrukcje dotyczące zmiany adresu serwera ESET PROTECT można znaleźć w tym artykule bazy wiedzy.

Migracja z programu ERA 5.x

Nie można bezpośrednio uaktualnić ani przeprowadzić migracji ERA 5.x do wersji ESET PROTECT 9.1.

Jeśli masz zainstalowaną wersję ERA 5.x, wykonaj następujące czynności:

1. Migracja z wersji ERA 5.x do wersji ESMC 7.2
2. Uaktualnienie wersji ESMC 7.2 do wersji ESET PROTECT 9.1

Odinstalowywanie serwera ESET PROTECT i jego składników

Wybierz jeden z poniższych rozdziałów, aby odinstalować serwer ESET PROTECT i jego składniki:

- Odinstaluj agenta ESET Management
- Windows — odinstalowywanie serwera ESET PROTECT i jego składników
- Linux — uaktualnianie, ponowne instalowanie lub odinstalowywanie składników ESET PROTECT
- macOS — odinstalowywanie agenta ESET Management i produktu punktu końcowego firmy ESET
- Likwidacja starego serwera ESMC / ESET PROTECT / MDM po migracji na inny serwer

Odinstaluj agenta ESET Management

Agent ESET Management może zostać odinstalowany na kilka sposobów.

Zdalna dezinstalacja przy użyciu konsoli internetowej ESET PROTECT

1. Zaloguj się w konsoli internetowej ESET PROTECT.

2. W okienku **Komputery** wybierz komputer, z którego chcesz usunąć agenta ESET Management, i kliknij

pozycję **Nowe zadanie**.

Możesz też wybrać wiele komputerów, zaznaczając odpowiednie pola wyboru i klikając kolejno pozycje **Komputer** > **Zadania** > **Nowe zadanie**.

3. Wpisz **nazwę** zadania.

4. Z menu rozwijanego **Kategoria zadania** wybierz pozycję **ESET PROTECT**.

5. Z menu rozwijanego **Zadanie** wybierz pozycję Zatrzymanie zarządzania (odinstalowanie agenta ESET Management).

Po odinstalowaniu agenta ESET Management z komputera klienckiego urządzenie przestaje być zarządzane przez produkt ESET PROTECT:
- Produkt zabezpieczający firmy ESET może zachować pewne ustawienia po odinstalowaniu agenta ESET Management.
- Jeśli agent jest chroniony hasłem, nie będzie można go odinstalować. Przed usunięciem urządzenia z grupy urządzeń zarządzanych zalecane jest przywrócenie niektórych ustawień, które nie mają być zachowane (np. ochrony hasłem) do ustawień domyślnych przy użyciu polityki.
- Ponadto wszystkie zadania uruchomione na agencie zostaną porzucone. W zależności od replikacji następujący stan tego zadania w konsoli internetowej ESET PROTECT może nie być precyzyjnie wyświetlany: **Uruchomiono**, **Zakończono** lub **Niepowodzenie**.
- Po odinstalowaniu agenta możesz zarządzać produktem zabezpieczającym za pośrednictwem zintegrowanego interfejsu EGUI lub eShell.

6. Zapoznaj się z **podsumowaniem** zadania i kliknij przycisk **Zakończ**.

7. Kliknięcie pozycji Utwórz element wyzwalający w celu określenia czasu wykonania oraz **obiektów docelowych** zadania klienta.

Dezinstalacja lokalna – Windows

Zobacz także instrukcje lokalnej dezinstalacji agenta ESET Management w systemie Linux lub macOS.
Aby zapoznać się z instrukcjami rozwiązywania problemów z dezinstalacją agenta, zobacz Rozwiązywanie problemów z dezinstalacją agenta ESET Management.

1. Połącz się z komputerem pełniącym rolę punktu końcowego, z którego chcesz usunąć agenta ESET Management (na przykład przy użyciu protokołu RDP).

2. Wybierz kolejno pozycje **Panel sterowania** > **Programy i funkcje**, a następnie kliknij dwukrotnie pozycję **Agent ESET Management**.

3. Kliknij kolejno pozycje **Dalej** > **Usuń** i postępuj zgodnie z instrukcją dezinstalacji.

Jeśli przy użyciu zasad agentów ESET Management zostało skonfigurowane hasło, dostępne są następujące opcje:
- Podczas dezinstalacji należy wpisać hasło.
- Można wyłączyć zasady przed rozpoczęciem dezinstalacji agenta ESET Management.
- Ponowne wdrożenie agenta ESET Management na istniejącym agencie chronionym hasłem (artykuł bazy wiedzy).

Windows — odinstalowywanie serwera ESET PROTECT i jego składników

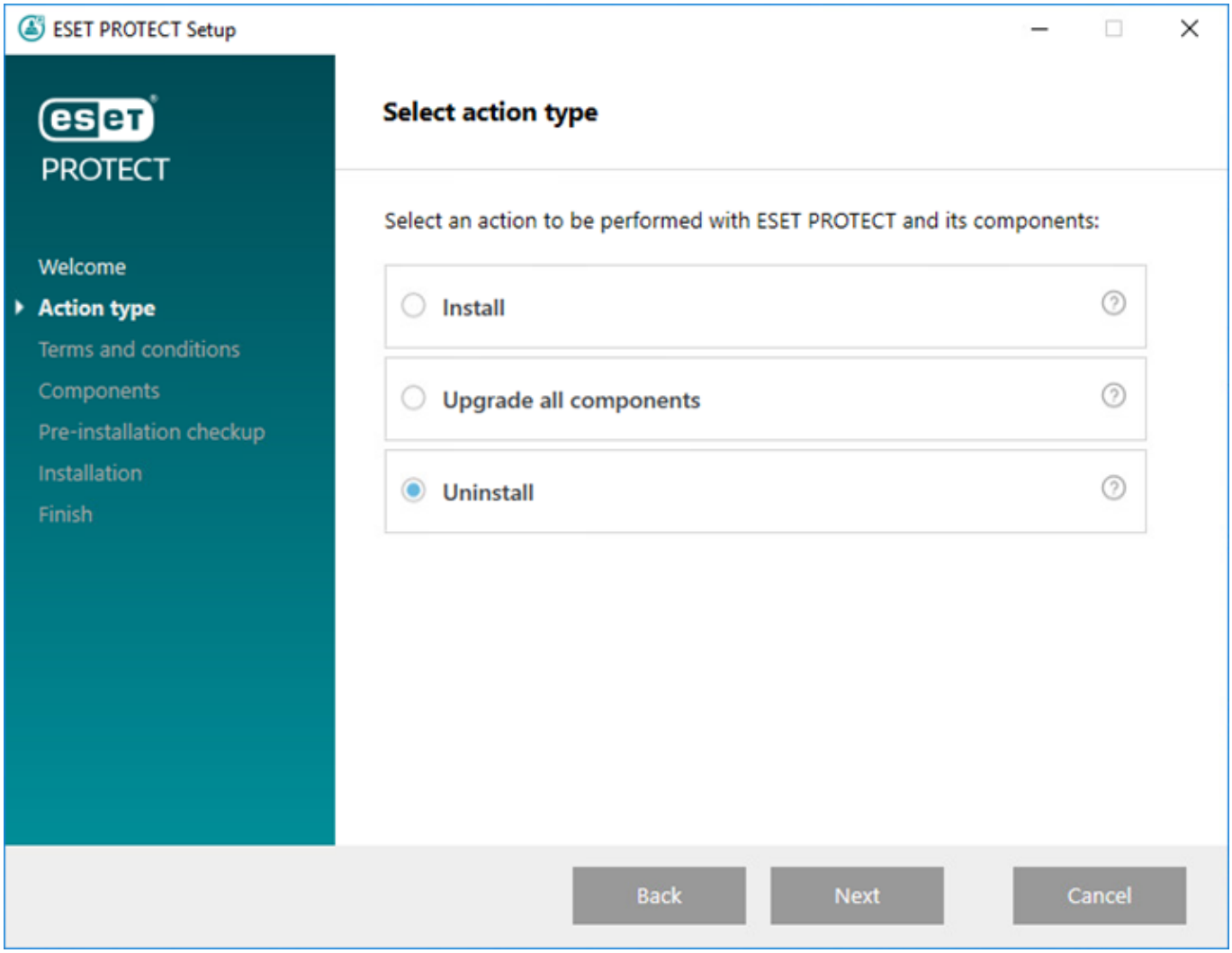
Przed odinstalowaniem ESET PROTECT odinstaluj agentów na zarządzanych komputerach.
Przed zainstalowanie Modułu zarządzania urządzeniami mobilnymi przeczytaj informacje w sekcji Narzędzie MDM, funkcja licencjonowania urządzeń z systemem iOS.

Wykonaj następujące kroki, aby odinstalować serwer ESET PROTECT i jego składniki w systemie Windows:

1. Pobierz instalator kompleksowy ESET PROTECT i rozpakuj pakiet.

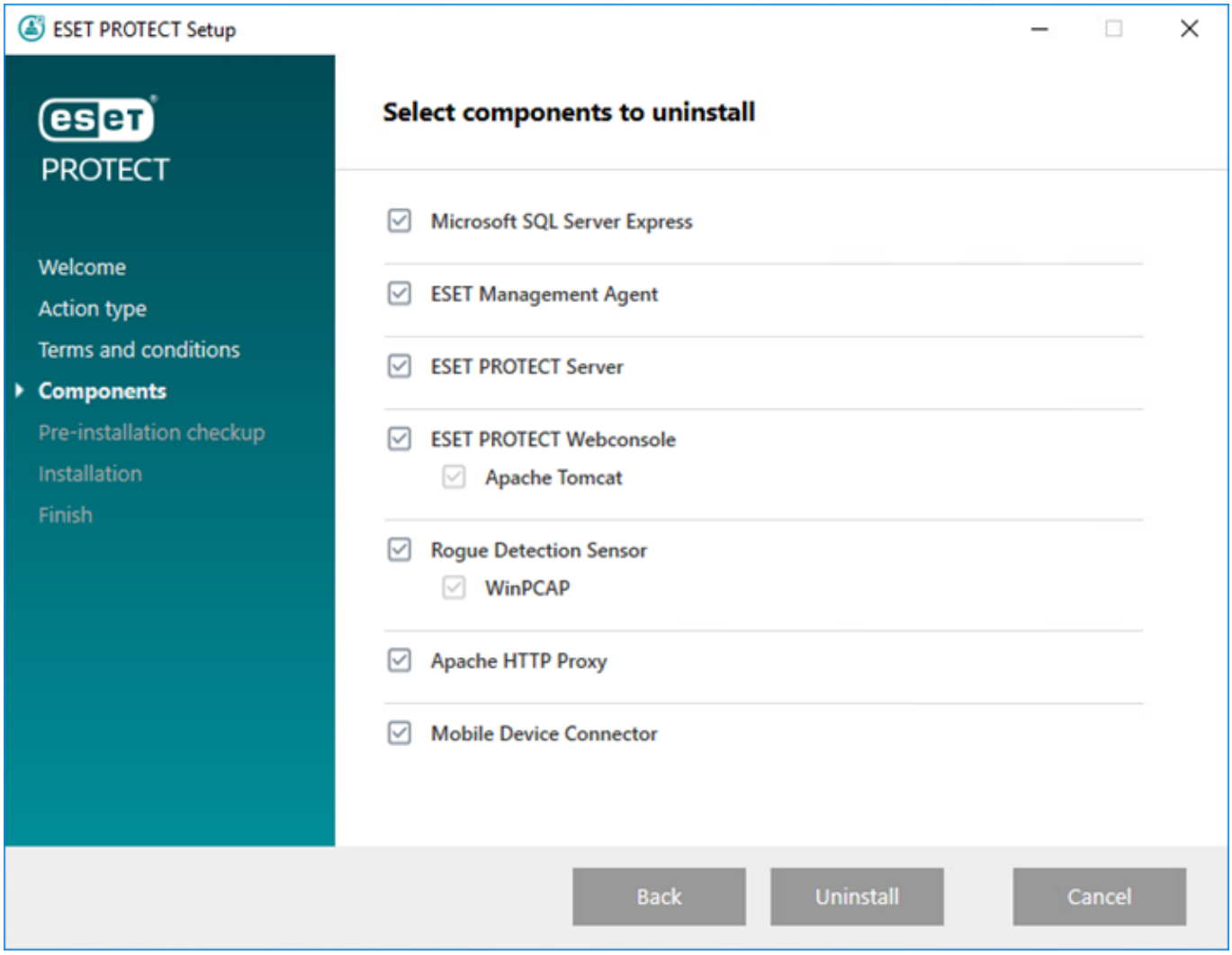
2. Uruchom plik *Setup.exe*. Możesz wybrać **Język** z menu rozwijanego. Kliknij przycisk **Dalej**.

3. Wybierz opcję **Odinstaluj** i kliknij przycisk **Dalej**.



4. Zaakceptuj umowę EULA i kliknij przycisk **Dalej**.

5. Wybierz komponenty, które chcesz odinstalować, i kliknij **Odinstaluj**.



6. Ukończenie usuwania poszczególnych komponentów może wymagać ponownego uruchomienia komputera.

Zobacz też Likwidacja starego serwera ESMC / ESET PROTECT / MDM po migracji na inny serwer.

Linux — uaktualnianie, ponowne instalowanie lub odinstalowywanie składników ESET PROTECT

Jeśli chcesz ponownie zainstalować lub uaktualnić komponent do nowszej wersji, uruchom ponownie skrypt instalacyjny.

Aby odinstalować komponent (w tym przypadku serwer ESET PROTECT), uruchom program instalacyjny z parametrem `--uninstall`, jak w poniższym przykładzie:

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

W celu odinstalowania innych komponentów w poleceniu należy użyć nazw odpowiednich pakietów. Przykład dla agenta ESET Management:

```
sudo ./agent-linux-x86_64.sh --uninstall
```

Podczas procesu dezinstalacji dane konfiguracji i bazy danych zostaną usunięte. Aby zachować pliki bazy danych, można utworzyć zrzut SQL bazy danych lub użyć parametru `--keep-database`.

Po dezinstalacji należy sprawdzić:

- czy usługa `eraserver` została usunięta.
- czy folder `/etc/opt/eset/RemoteAdministrator/Server/` został usunięty.

Zalecamy utworzenie kopii zapasowej bazy danych przed przeprowadzeniem dezinstalacji, na wypadek, gdyby zaistniała potrzeba odzyskania danych.
Więcej informacji na temat ponownego instalowania agenta zawiera pokrewny rozdział.
Aby zapoznać się z instrukcjami rozwiązywania problemów z dezinstalacją agenta, zobacz Rozwiązywanie problemów z dezinstalacją agenta ESET Management.

macOS — odinstalowywanie agenta ESET Management i produktu punktu końcowego firmy ESET

Odinstalowywanie agenta ESET Management i produktu punktu końcowego firmy ESET lokalnie lub zdalnie za pośrednictwem produktu ESET PROTECT.

Bardziej szczegółowe instrukcje dotyczące lokalnej dezinstalacji produktu agenta ESET Management i produktu firmy ESET dla punktu końcowego można znaleźć w naszym artykule bazy wiedzy.

Jeśli chcesz zdalnie odinstalować produkt ESET dla punktu końcowego, upewnij się, żeby zrobić to przed odinstalowaniem agenta ESET Management.

Lokalna dezinstalacja agenta ESET Management

1. Kliknij pozycję **Finder**, aby otworzyć nowe okno programu **Finder**.
2. Kliknij **Aplikacje** > przytrzymaj klawisz **CTRL** i kliknij pozycję **Agnet ESET Management** > wybierz pozycję **Pokaż zawartość pakietu** z menu kontekstowego.
3. Przejdź do sekcji **Zawartość** > **Skrypty zawartości** i kliknij dwukrotnie polecenie **Uninstaller.command**, aby uruchomić deinstalator.
4. Wpisz hasło administratora i naciśnij klawisz **Enter**, jeśli zostanie wyświetlony monit o wprowadzenie hasła.
5. Po odinstalowaniu agenta ESET Management zostanie wyświetlony komunikat **Proces zakończony**.

Lokalna dezinstalacja agenta ESET Management za pośrednictwem terminala

1. Otwórz **Finder** > **Aplikacje** > **Narzędzia** > **Terminal**.
2. Wpisz następujący kod i naciśnij klawisz **Enter**:

```
sudo /Applications/ESET\ Management\ Agent.app/Contents/Scripts/Uninstall.command ;
 exit;
```

3. Wpisz hasło administratora i naciśnij klawisz **Enter**, jeśli zostanie wyświetlony monit o wprowadzenie hasła.

4. Po odinstalowaniu agenta ESET Management zostanie wyświetlony komunikat **Proces zakończony**.

Zdalna dezinstalacja agenta ESET Management za pomocą programu ESET PROTECT

W obszarze **Komputery** kliknij komputer kliencki z systemem macOS i wybierz pozycję **Usuń**, aby odinstalować agenta ESET Management i usunąć komputer z zarządzania.

Aby zapoznać się z instrukcjami rozwiązywania problemów z dezinstalacją agenta, zobacz Rozwiązywanie problemów z dezinstalacją agenta ESET Management.

Lokalna dezinstalacja produktu punktu końcowego firmy ESET

1. Kliknij pozycję **Finder**, aby otworzyć nowe okno programu **Finder**.

2. Kliknij pozycję **Aplikacje** > przytrzymaj klawisz **CTRL** > kliknij pozycję **ESET Endpoint Security** lub **ESET Endpoint Antivirus** > wybierz pozycję **Pokaż zawartość pakietu** z menu kontekstowego.

3. Przejdź do pozycji **Zawartość** > **Pomocnicy** i kliknij dwukrotnie pozycję > **Uninstaller.app**, aby uruchomić deinstalator.

4. Kliknij pozycję **Odinstaluj**.

5. Wpisz hasło administratora i kliknij przycisk **OK**, jeśli zostanie wyświetlony monit o wprowadzenie hasła.

6. Po pomyślnym odinstalowaniu programu ESET Endpoint Security lub programu antywirusowego ESET Endpoint Antivirus zostanie wyświetlony komunikat **Pomyślnie odinstalowano**. Kliknij opcję **Zamknij**.

Lokalna dezinstalacja produktu punktu końcowego firmy ESET za pośrednictwem terminala

1. Otwórz **Finder** > **Aplikacje** > **Narzędzia** > **Terminal**.

2. Wpisz następujący kod i naciśnij klawisz **Enter**:

- Odinstaluj ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

- Odinstaluj ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
```

```
Contents/Scripts/uninstall.sh
```

3. Wpisz hasło administratora i naciśnij klawisz **Enter**, jeśli zostanie wyświetlony monit o wprowadzenie hasła.

4. Po odinstalowaniu produktu punktu końcowego firmy ESET zostanie wyświetlony komunikat **Proces zakończony**.

Zdalna dezinstalacja produktu punktu końcowego firmy ESET za pomocą programu ESET PROTECT

Aby zdalnie odinstalować agenta ESET Management za pomocą programu ESET PROTECT, można użyć jednej z następujących opcji:

- W obszarze **Komputery** kliknij komputer kliencki z systemem macOS, wybierz pozycję **Szczegóły** > **Zainstalowane aplikacje**, wybierz pozycję **ESET Endpoint Security** lub **ESET Endpoint Antivirus** i kliknij przycisk **Odinstaluj**.

- Użyj zadania Dezinstalacja oprogramowania***.

Likwidacja starego serwera ESMC / ESET PROTECT / MDM po migracji na inny serwer

⚠ Należy się upewnić, że nowy serwer ESET PROTECT lub komponent MDM działa, a komputery klienckie i urządzenia mobilne poprawnie nawiązują połączenie z nowym programem ESET PROTECT.

Podczas wycofywania z użycia starego serwera lub komponentu MDM ESMC/ESET PROTECT dostępnych jest kilka opcji po migracji na inny serwer:

I.**Zachowaj system operacyjny serwera i wykorzystaj go ponownie**

1. Zatrzymaj usługę starego serwera ESMC/ESET PROTECT.

2. Usuń (`DROP DATABASE`) z serwera stare wystąpienie bazy danych ESMC/ESET PROTECT (MS SQL lub MySQL).

⚠ Jeśli zmigrowano bazę danych do nowego serwera ESET PROTECT, przed jej odinstalowaniem upewnij się, że usunięto ją na starym serwerze ESMC/ESET PROTECT, aby zapobiec rozłączeniu (usunięciu) licencji z bazy danych na nowym serwerze ESET PROTECT.

3. Odinstaluj stary serwer ESMC / ESET PROTECT / MDM i wszystkie jego składniki (w tym agenta ESET Management, Rogue Detection Sensor, MDM itp.):

   - Odinstaluj ESMC 7.2 — Windows
   - Odinstaluj ESET PROTECT 8.x – system Windows
   - Odinstaluj ESET PROTECT 9.x – system Windows
   - Odinstaluj ESET PROTECT — Linux

Nie wykonuj dezinstalacji bazy danych, jeśli istnieje inne oprogramowanie zależne od bazy danych.

4. Po zakończeniu dezinstalacji zaplanuj ponowne uruchomienie systemu operacyjnego

II.**Zachowaj serwer**

Najprostszym sposobem na usunięcie produktu ESMC/ESET PROTECT/MDM jest sformatowanie dysku, na którym jest on zainstalowany.

Spowoduje to usunięcie z dysku wszystkich danych, w tym również systemu operacyjnego.

Rozwiązywanie problemów

Ponieważ program ESET PROTECT to złożony produkt wykorzystujący kilka narzędzi innych firm i obsługujący wiele platform systemów operacyjnych, mogą wystąpić problemy, które należy rozwiązać.

Dokumentacja firmy ESET zawiera kilka metod rozwiązywania problemów z ESET PROTECT. Rozwiązania częstych problemów z programem ESET PROTECT znajdziesz w sekcji Odpowiedzi dotyczące częstych problemów z instalacją. Zobacz także znane problemy dotyczące produktów biznesowych ESET.

Czy nie można rozwiązać problemu?

- Każdy składnik programu ESET PROTECT ma plik dziennika, którego szczegółowość można skonfigurować. Należy zapoznać się z dziennikami w celu zidentyfikowania błędów, które mogą wyjaśnić występujący problem.

- Szczegółowość wpisów w dzienniku każdego komponentu jest określana przy użyciu jego polityki > **Ustawienia zaawansowane** > **Zapisywanie w dzienniku** > **Szczegółowość dziennika śledzenia** — istnieje możliwość skonfigurowania szczegółowości dziennika i wybrania poziomu informacji gromadzonych i zapisywanych w dzienniku — od poziomu **Śledzenie** (informacyjne) do poziomu **Krytyczny** (najważniejsze informacje o decydującym znaczeniu).

  - Polityka agenta ESET Management – aby polityka obowiązywała, musi wcześniej zostać zastosowana do urządzenia. W celu włączenia pełnego rejestrowania danych przez agenta ESET Management w pliku *trace.log* należy utworzyć fikcyjny plik o nazwie *traceAll* bez rozszerzenia i umieścić go w tym samym folderze, w którym znajduje się plik *trace.log*, a następnie ponownie uruchomić komputer (aby tym samym ponownie uruchomić usługę agenta ESET Management).

  - ESET PROTECT Ustawienia serwera

  - Polityka rozwiązania ESET Mobile Device Connector – aby polityka obowiązywała, musi wcześniej zostać zastosowana do urządzenia. Zobacz też Rozwiązywanie problemów z MDM.

- Jeśli nie można rozwiązać tego problemu, należy odwiedzić Forum zabezpieczeń ESET i poprosić społeczność firmy ESET o informacje o występujących problemach.

- Podczas kontaktowania się z pomocą techniczną firmy ESET możesz zostać poproszony o zbieranie plików dziennika za pomocą ESET Log Collector lub narzędzia diagnostycznego. Zdecydowanie zalecamy dołączenie dzienników podczas kontaktowania się z działem obsługi. Przyśpieszy to obsługę.

Uaktualnianie komponentów ESET PROTECT w środowisku offline

Aby uaktualnić komponenty ESET PROTECT oraz produkty ESET do obsługi punktów końcowych bez dostępu do Internetu, należy wykonać poniższe czynności:

Aby można było użyć zadania Uaktualnianie komponentów w środowisku offline, muszą zostać spełnione następujące warunki:
- Musi być dostępne repozytorium offline.
- Dostępna lokalizacja repozytorium agenta ESET Management musi być skonfigurowana przy użyciu polityki

Uaktualnij serwer i konsolę internetową ESET PROTECT

1. Sprawdź wersję programu konsola zarządzania ESET działającego na serwerze.

2. Pobierz najnowszą wersję instalatora kompleksowego dla Windows lub najnowsze wersje instalatorów składników ESET PROTECT dla Linuksa z witryny pobierania firmy ESET.

3. Uaktualnij serwer ESET PROTECT i konsolę internetową ESET PROTECT

   - Windows — uaktualnianie przy użyciu instalatora kompleksowego

   - Linux — ręczna aktualizacja oparta na składnikach

Aktualizacja konsoli internetowej i Apache Tomcat usuwa pliki pomocy offline. Jeśli korzystałeś z pomocy offline w rozwiązaniu ESMC lub starszej wersji programu ESET PROTECT, po aktualizacji konieczne jest jej ponowne utworzenie dla ESET PROTECT 9.1, aby mieć pewność, że Twoja wersja pomocy offline odpowiada wersji ESET PROTECT.

Kontynuuj uaktualnianie offline produktów firmy ESET do obsługi punktów końcowych

1. Sprawdź, które produkty firmy ESET są zainstalowane na klientach: Otwórz konsolę internetową ESET PROTECT i wybierz kolejno pozycje **Panel kontrolny** > **Aplikacje ESET**.

2. Upewnij się, że masz najnowsze wersje produktów firmy ESET do obsługi punktów końcowych.

3. Pobierz instalatory ze strony pobierania firmy ESET do lokalnego repozytorium skonfigurowanego podczas instalacji offline.

4. Uruchom zadanie instalacji oprogramowania w konsoli internetowej ESET PROTECT.

Rozwiązania częstych problemów z instalacją

Rozwiń sekcję komunikatu o błędzie, który chcesz usunąć:

ESET PROTECTSerwer

Usługa serwera ESET PROTECT nie uruchamia się:

Uszkodzona instalacja

- Przyczyną tego problemu mogą być brakujące klucze rejestru, brakujące pliki lub niewłaściwe uprawnienia do plików.
- Instalator kompleksowy ESET ma własny plik dziennika. W przypadku ręcznego instalowania komponentu użyj metody zapisywania w dzienniku MSI.

Port nasłuchiwania jest już używany (najczęściej jest to port 2222 i 2223)

Użyj polecenia odpowiedniego w przypadku danego systemu operacyjnego:

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- System Linux :

```
netstat | grep 2222
netstat | grep 2223
```

Baza danych nie działa / jest nieosiągalna

- MS SQL Server: Sprawdź, czy port 1433 jest dostępny na serwerze bazy danych / dla serwera bazy danych, albo spróbuj się zalogować w programie SQL Server Management Studio
- MySQL: Sprawdź, czy port 3306 jest dostępny na serwerze bazy danych/dla serwera bazy danych, albo spróbuj się zalogować w interfejsie bazy danych (na przykład przy użyciu interfejsu wiersza polecenia programu MySQL lub programu `phpmyadmin`)

Uszkodzona baza danych

Plik dziennika serwera ESET PROTECT zawiera wiele błędów SQL. Zalecamy przywrócenie bazy danych z kopii zapasowej. Jeśli kopia zapasowa nie istnieje, zainstaluj ponownie ESET PROTECT.

Niewystarczające zasoby systemu (pamięć RAM, miejsce na dysku)

Zapoznaj się z uruchomionymi procesami i wydajnością systemu:

- Użytkownicy systemu Windows: Uruchom Menedżera zadań lub Podgląd zdarzeń i przejrzyj informacje
- Użytkownicy Linuksa: Uruchom jedno z następujących poleceń:
`df -h` (powoduje wyświetlenie informacji o miejscu na dysku)
`cat /proc/meminfo` (powoduje wyświetlenie informacji o miejscu w pamięci)
`dmesg` (powoduje wyświetlenie informacji o stanie systemu Linux)

Błąd łącznika ODBC podczas instalacji serwera ESET PROTECT

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

Ponownie zainstaluj wersję sterownika ODBC obsługującego wielowątkowość lub ponownie skonfiguruj plik

odbcinst.ini zgodnie z sekcją dotyczącą konfiguracji sterownika ODBC.

Błąd połączenia z bazą danych podczas instalacji serwera ESET PROTECT

Instalacja serwera ESET PROTECT kończy się ogólnym komunikatem o błędzie:

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

Komunikat o błędzie w dzienniku instalacji:

```
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.
```

Sprawdź, czy konfiguracja sterownika bazy danych odpowiada konfiguracji znajdującej się w sekcji dotyczącej konfiguracji sterownika ODBC.

Agent ESET Management

Dezinstalacja ESET Management i rozwiązywanie problemów dotyczących Agenta

- Pliki dziennika zawierają informacje dotyczące agenta ESET Management.

- Agenta ESET Management można odinstalować, używając dezinstalatora firmy ESET lub przeprowadzając tę operację w sposób niestandardowy (np. usuwając pliki, usługę agenta ESET Management i wpisy w rejestrze). Jeśli na tym samym komputerze znajduje się punkt końcowy produktu ESET, nie będzie można wykonać tego działania ze względu na włączoną technologię Self-Defense.

- Podczas odinstalowywania agenta jest wyświetlany komunikat: „Nie można uaktualnić bazy danych. Najpierw usuń produkt” – napraw agenta ESET Management:

    1. Kliknij kolejno pozycje **Panel sterowania** > **Programy i funkcje**, a następnie kliknij dwukrotnie pozycję **Agent ESET Management**.

    2. Kliknij kolejno pozycje **Dalej** > **Napraw** i postępuj zgodnie z instrukcjami.

Wszystkie możliwe sposoby odinstalowania agenta ESET Management zostały opisane w sekcji dotyczącej odinstalowywania.

Podczas instalacji agenta wystąpił kod błędu 1603

Ten błąd może występować, gdy pliki instalatora nie znajdują się na dysku lokalnym. Aby go rozwiązać, należy skopiować pliki instalatora do katalogu lokalnego i uruchomić instalację ponownie. Jeśli pliki już istnieją lub nadal występuje błąd, należy zapoznać się z instrukcjami w bazie wiedzy.

Podczas instalacji agenta w systemie Linux zostaje wyświetlony błąd

Komunikat o błędzie:

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

Możliwą przyczyną tego błędu jest nieprawidłowa nazwa pliku w poleceniu instalacji. W konsoli rozróżniana jest wielkość liter. Na przykład `Agent.pfx` różni się od `agent.pfx`.

Niepowodzenie wdrożenia zdalnego z systemu Linux w systemie Windows 8.1 (32-bitowym)

Jest to problem z uwierzytelnianiem spowodowany przez kb3161949 firmy Microsoft. Można go rozwiązać tylko przez usunięcie tej aktualizacji z hostów, na których wdrożenie się nie powiodło.

Agent ESET Management nie może połączyć się z serwerem ESET PROTECT

Zobacz Rozwiązywanie problemów — połączenie agenta i artykuł w bazie wiedzy.

Instalator skryptu agenta zakończył pracę z kodem 30

Użyto instalatora skryptu agenta oraz niestandardowej lokalizacji instalatora, jednak skrypt nie został prawidłowo edytowany. Zapoznaj się z treścią strony pomocy i spróbuj ponownie.

Konsola internetowa

Serwer proxy Apache HTTP

Pamięć podręczna serwera proxy Apache HTTP wynosi kilka GB i wciąż rośnie

Jeśli serwer proxy Apache HTTP został zainstalowany przy użyciu instalatora kompleksowego, czyszczenie jest włączane automatycznie. Jeśli czyszczenie automatyczne nie działa poprawnie, wykonaj je ręcznie lub zaplanuj zadanie czyszczenia.

Aktualizacje silnika detekcji nie działają po zainstalowaniu serwera proxy Apache HTTP

Jeśli nie można zaktualizować klienckich stacji roboczych, zapoznaj się z instrukcjami w bazie wiedzy, aby tymczasowo wyłączyć serwer proxy Apache HTTP na końcowych stacjach roboczych. Po rozwiązaniu problemów z połączeniem ponownie włącz serwer proxy Apache HTTP.

Zdalna aktualizacja agenta ESET Management kończy się niepowodzeniem

i wyświetleniem kodu błędu 20008

Jeśli zdalna aktualizacja agenta ESET Management zakończy się niepowodzeniem i wyświetleniem następującego komunikatu:
GetFile: Nie udało się przetworzyć żądania HTTP (kod błędu 20008, url: 'http://repository.eset.com/v1//info.meta')

Wykonaj kroki od I do III opisane w tym artykule, aby rozwiązać problem z połączeniem. Gdy komputer, na którym ma zostać zaktualizowany agent ESET Management, znajduje się poza siecią korporacyjną, należy skonfigurować dla agenta ESET Management politykę uniemożliwiającą korzystanie z serwera proxy do łączenia się z repozytorium, jeśli komputer znajduje się poza siecią firmową.

Usługa ESET Rogue Detector Sensor

Dlaczego w dzienniku trace.log narzędzia ESET Rogue Detector stale jest zapisywany poniższy komunikat o błędzie?

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_

{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:

The system cannot find the device specified. (20)
```

Ten problem dotyczy programu WinPcap. Zatrzymaj usługę ESET Rogue Detector Sensor, ponownie zainstaluj najnowszą wersję programu WinPcap (co najmniej wersję 4.1.0) i uruchom ponownie usługę ESET Rogue Detector Sensor.

Linux

Wymagany pakiet libQtWebKit nie jest zainstalowany w systemie CentOS Linux

Występuje następujący błąd:

```
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]
```

Wykonaj instrukcje opisane w tym artykule bazy wiedzy.

Niepowodzenie instalacji serwera ESET PROTECT w systemie CentOS 7

Występuje następujący błąd:

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

Przyczyną tego problemu są prawdopodobnie ustawienia środowiska / ustawienia regionalne. W rozwiązaniu tego problemu powinno pomóc uruchomienie następującego polecenia przed uruchomieniem skryptu instalatora serwera:

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

Podczas instalacji programu Microsoft SQL Server występuje kod błędu 2068052081

Uruchom komputer ponownie i jeszcze raz przeprowadź instalację. Jeśli problem nie ustąpi, odinstaluj macierzystego klienta serwera SQL i ponownie uruchom program instalacyjny. Jeśli to nie rozwiąże problemu, odinstaluj wszystkie programy Microsoft SQL Server, uruchom ponownie komputer i ponownie przeprowadź instalację.

Podczas instalacji programu Microsoft SQL Server występuje kod błędu 2067922943

Sprawdź, czy system spełnia wymagania dotyczące bazy danych programu ESET PROTECT.

Podczas instalacji programu Microsoft SQL Server występuje kod błędu 2067922934

Upewnij się, że masz prawidłowe uprawnienia konta użytkownika.

Konsola internetowa wyświetla komunikat „Ładowanie danych zakończyło się niepowodzeniem”.

Program MS SQL Server podejmuje próbę użycia jak największej ilości miejsca na dysku na potrzeby zapisywania dzienników transakcji. Aby rozwiązać ten problem, odwiedź stronę internetową firmy Microsoft.

Podczas instalacji programu Microsoft SQL Server występuje kod błędu 2067919934

Sprawdź, czy wszystkie poprzednie czynności zostały pomyślnie ukończone. Przyczyną tego błędu jest błąd w konfiguracji plików systemowych. Uruchom komputer ponownie i jeszcze raz przeprowadź instalację.

Pliki dziennika

Każdy komponent programu ESET PROTECT zapisuje informacje w dzienniku. Komponenty programu ESET PROTECT zapisują informacje o określonych zdarzeniach w plikach dziennika. Lokalizacja plików dziennika różni się zależnie od komponentu. Poniżej znajdują się lokalizacje plików dziennika:

System Windows

ESET PROTECT komponent	Lokalizacja plików dziennika
ESET PROTECTSerwer	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
Agent ESET Management	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* Zobacz też Rozwiązywanie problemów z połączeniem agenta.
ESET PROTECTKonsola internetowa i Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* Dodatkowe informacje: https://tomcat.apache.org/tomcat-9.0-doc/logging.html
Moduł zarządzania urządzeniami mobilnymi	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* Zobacz też Rozwiązywanie problemów z MDM.
Moduł Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*
Serwer proxy Apache HTTP	*C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs* *C:\Program Files\Apache HTTP Proxy 2.[x.xx]\logs\errorlog*

C:\ProgramData jest domyślnie ukryty. Aby wyświetlić folder:
1. Wybierz kolejno pozycje **Start** > **Panel sterowania** > **Opcje folderów** > **Widok**.
2. Wybierz pozycję **Pokaż ukryte pliki, foldery i dyski** i kliknij przycisk **OK**.

Linux

ESET PROTECT komponent	Lokalizacja plików dziennika
ESET PROTECTSerwer	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Agent ESET Management	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
Moduł zarządzania urządzeniami mobilnymi	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* Zobacz też Rozwiązywanie problemów z MDM.
Serwer proxy Apache HTTP	*/var/log/httpd/*
ESET PROTECTKonsola internetowa i Apache Tomcat	*/var/log/tomcat/* Dodatkowe informacje: https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

Urządzenie wirtualne ESET PROTECT

ESET PROTECT komponent	Lokalizacja plików dziennika
Konfiguracja urządzenia wirtualnego ESET PROTECT	*/root/appliance-configuration-log.txt*
ESET PROTECTSerwer	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Serwer proxy Apache HTTP	*/var/log/httpd*

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

Narzędzie diagnostyczne

Narzędzie diagnostyczne jest jednym z komponentów programu ESET PROTECT. Służy do gromadzenia i kompresowania dzienników używanych przez pracowników działu obsługi przy rozwiązywaniu problemów związanych z komponentami produktu.

Lokalizacja narzędzia diagnostycznego

System Windows

Folder *C:\Program Files\ESET\RemoteAdministrator\<product>***Diagnostic.exe**.

Linux

W następującym katalogu na serwerze: */opt/eset/RemoteAdministrator/<product>/* znajduje się plik wykonywalny o nazwie **Diagnostic<product>** (jedno słowo, np. **DiagnosticServer**, **DiagnosticAgent**).

Użycie (Linux)

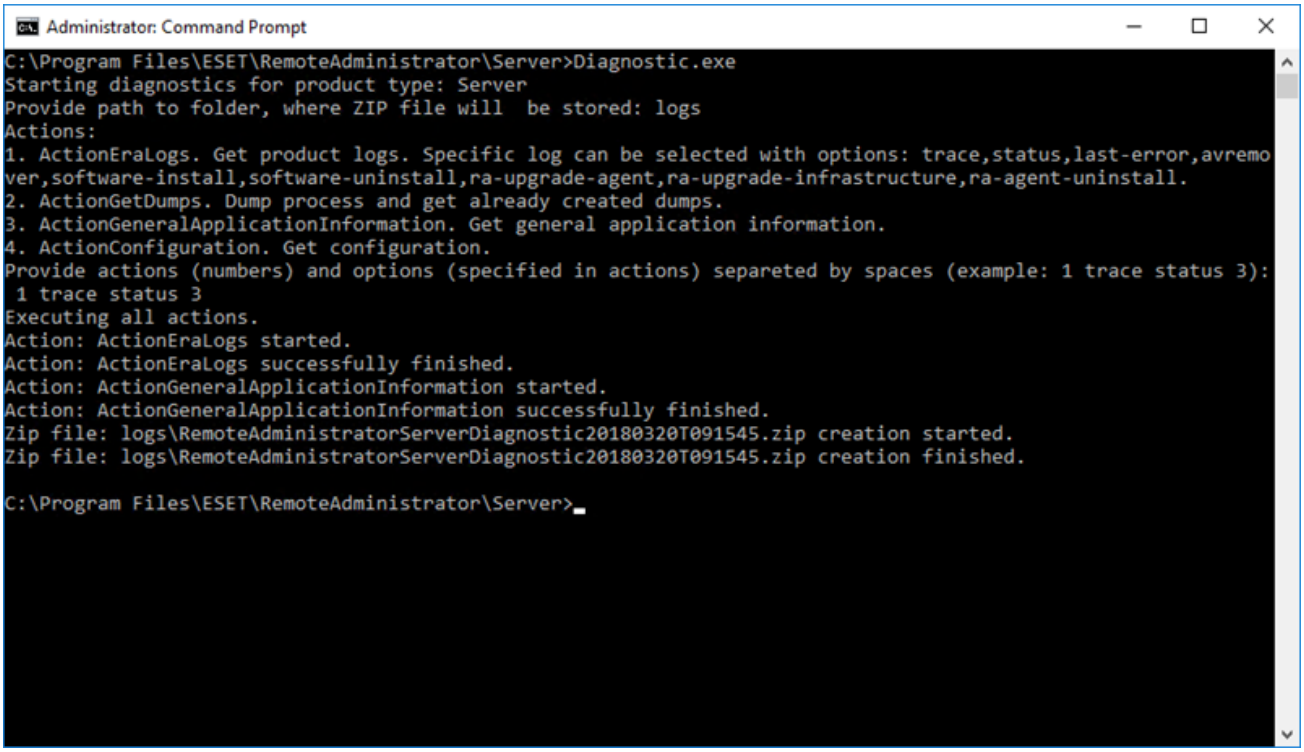
Uruchom plik wykonywalny narzędzia diagnostycznego jako użytkownik root i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Użycie (Windows)

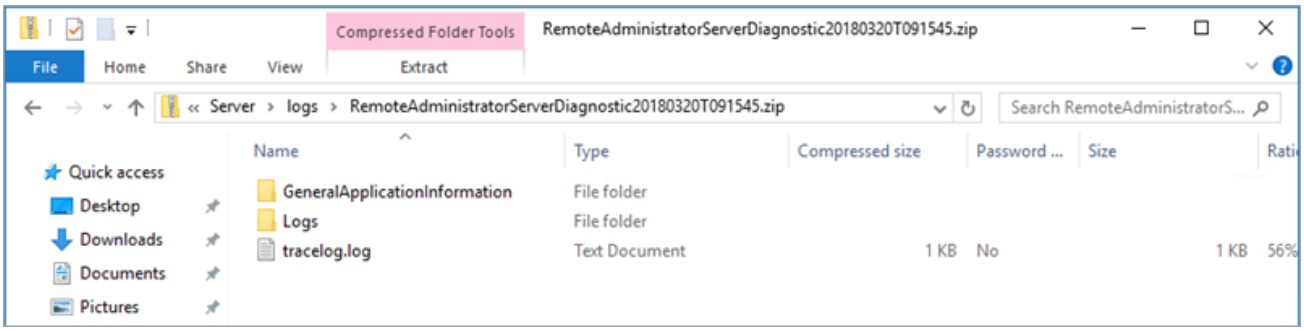
1. Uruchom narzędzie przy użyciu wiersza polecenia.

2. Wprowadź lokalizację przechowywania plików dziennika (w tym przykładzie to „logs”) i naciśnij klawisz **Enter**.

3. Wprowadź informacje, które chcesz zebrać (w tym przykładzie to `1 trace status 3`). Więcej informacji zawiera sekcja **Czynności** poniżej.



4. Po wykonaniu powyższych czynności skompresowane pliki dziennika w pliku *.zip* będą dostępne w katalogu „**logs**” w lokalizacji narzędzia diagnostycznego.



Czynności

• **ActionEraLogs** — Tworzony jest folder, w którym zapisywane są wszystkie dzienniki. Aby określić zapisywanie tylko niektórych dzienników, przy użyciu spacji należy oddzielić każdy dziennik.

• **ActionGetDumps** — Utworzony zostaje nowy folder. Plik zrzutu procesów jest tworzony w razie wykrycia problemów. W przypadku wykrycia poważnego problemu system tworzy plik zrzutu. Aby wykonać to działanie ręcznie, należy przejść do folderu %temp% (w systemie Windows) lub folderu /tmp/ (w systemie Linux) i wstawić plik dmp.

Usługa komponentu (Agent, , Server, RD Sensor,) musi być uruchomiona.

• **ActionGeneralApplicationInformation** — Tworzony jest folder GeneralApplicationInformation, w którym znajduje się plik *GeneralApplicationInformation.txt*. Ten plik zawiera informacje tekstowe, wśród których jest nazwa i wersja aktualnie zainstalowanego produktu.

• **ActionConfiguration** — w miejscu zapisu pliku storage.lua tworzony jest folder konfiguracji.

Problemy po uaktualnieniu/migracji serwera ESET PROTECT

Jeśli nie można uruchomić usługi serwera ESET PROTECT i są wyświetlane komunikaty o błędach dotyczące uszkodzonej instalacji oraz nieznanego pliku dziennika, należy przeprowadzić operację naprawy, postępując zgodnie z poniższymi instrukcjami:

⚠ Przed rozpoczęciem operacji naprawy zalecamy utworzenie kopii zapasowej serwera bazy danych.

1. Przejdź do menu **Start** > **Panel sterowania** > **Program i funkcje** i kliknij dwukrotnie pozycję **Serwer ESET PROTECT**.

2. Wybierz opcję **Napraw** i kliknij przycisk **Dalej**.

3. Ponownie użyj istniejących ustawień połączenia z bazą danych i kliknij przycisk **Dalej**. **Po wyświetleniu monitu o potwierdzenie kliknij przycisk Tak**. Informacje potrzebne do nawiązania połączenia z bazą danych można znaleźć tutaj: *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. Wybierz opcję **Użyj hasła, które jest już zapisane w bazie danych** i kliknij przycisk **Dalej**.

5. Wybierz opcję **Zachowaj obecnie używane certyfikaty** i kliknij przycisk **Dalej**.

6. Aktywuj serwer ESET PROTECT za pomocą ważnego klucza licencyjnego lub wybierz opcję **Aktywuj później** (dodatkowe instrukcje znajdują się w sekcji Zarządzanie licencjami) i kliknij przycisk **Dalej**.

7. Kliknij przycisk **Napraw**.

8. Ponownie połącz się z konsolą internetową i sprawdź, czy wszystko działa.

Inne scenariusze rozwiązywania problemów:

Serwer ESET PROTECT nie jest uruchomiony, ale istnieje kopia zapasowa bazy danych:

1. Przywróć kopię zapasową bazy danych.

2. Sprawdź, czy na nowym komputerze są używane taki sam adres IP lub nazwa hosta co w poprzedniej instalacji, aby mieć pewność, że agenty nawiążą połączenie.

3. Napraw serwer ESET PROTECT i użyj przywróconej bazy danych.

Serwer ESET PROTECT nie działa, ale są dostępne wyeksportowane z niego

certyfikat serwera i urząd certyfikacji:

1. Sprawdź, czy na nowym komputerze są używane taki sam adres IP lub nazwa hosta co w poprzedniej instalacji, aby mieć pewność, że agenty nawiążą połączenie.

2. Napraw serwer ESET PROTECT Server przy użyciu kopii zapasowych certyfikatów (podczas naprawy wybierz opcję **Wczytaj certyfikaty z pliku** i postępuj zgodnie z instrukcjami).

Serwer ESET PROTECT nie działa i nie ma kopii zapasowych bazy danych lub certyfikatu serwera ESET PROTECT i urzędu certyfikacji:

1. Napraw serwer ESET PROTECT.

2. Napraw agenty ESET Management, korzystając z jednej z następujących metod:

   - Skrypt instalacyjny agenta
   - wdrożenie zdalne (wymaga wyłączenia zapory na komputerach docelowych)
   - ręczny instalator komponentu agenta

Zapisywanie w dzienniku MSI

Ta funkcja jest przydatna, gdy nie można poprawnie zainstalować komponentu ESET PROTECT w systemie Windows, na przykład agenta ESET Management:

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

ServerApi programu ESET PROTECT (*ServerApi.dll*) to interfejs programowania aplikacji — zestaw funkcji i narzędzi służących do tworzenia niestandardowych aplikacji spełniających konkretne potrzeby. Dzięki temu interfejsowi aplikacja może mieć niestandardowy interfejs użytkownika oraz zapewniać niestandardowe możliwości (funkcje, działanie), które zwykle wykonuje się w konsoli internetowej ESET PROTECT, na przykład zarządzanie programem ESET PROTECT, generowanie i odbieranie raportów itp.

Więcej informacji oraz przykłady w języku C, a także listę dostępnych komunikatów JSON zawiera ta pomoc online:

INTERFEJS API PROGRAMU ESET PROTECT 9

Często zadawane pytania

Dlaczego środowisko Java jest instalowane na serwerze? Czy nie

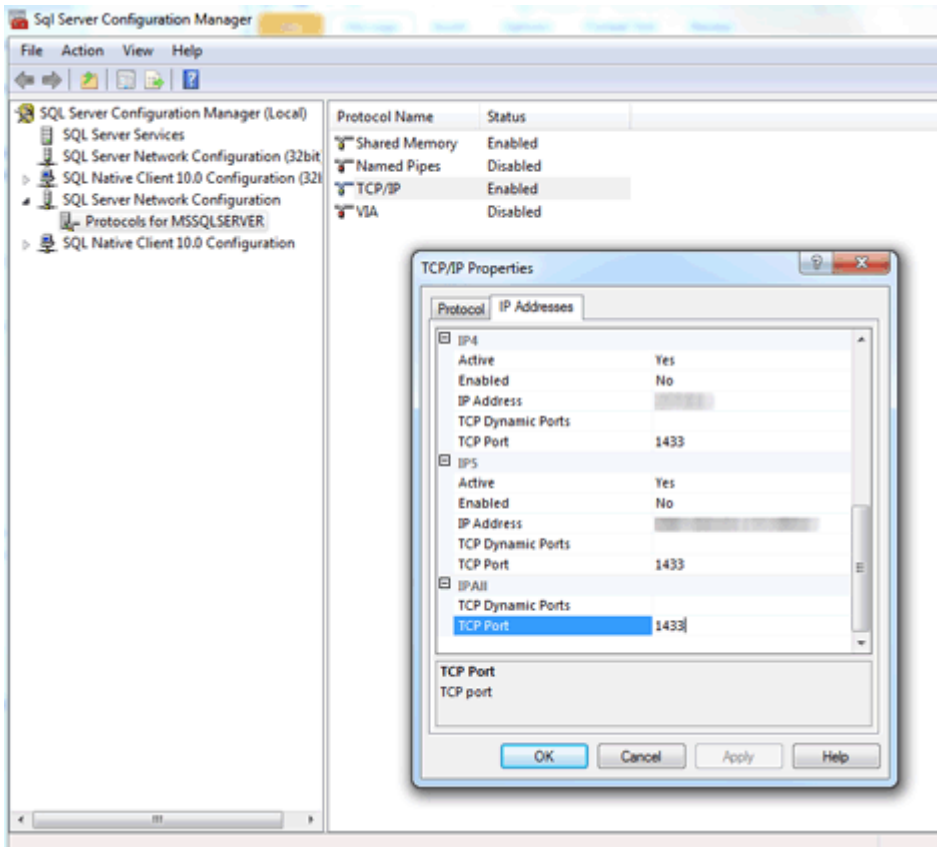
powoduje to zagrożenia bezpieczeństwa? Większość firm zajmujących się bezpieczeństwem i twórców struktur zabezpieczeń zaleca odinstalowanie środowiska Java z komputerów, a w szczególności z serwerów.

Konsola internetowa ESET PROTECT wymaga do działania oprogramowania Java/OpenJDK. Java to standard branżowy związany z obsługą konsol internetowych — wszystkie popularne konsole internetowe wymagają do działania środowiska Java i serwera internetowego (Apache Tomcat). Środowisko Java jest potrzebne do udostępnienia serwera internetowego obsługującego wiele platform. Ze względów bezpieczeństwa serwer internetowy można zainstalować na osobnym komputerze.

Począwszy od stycznia 2019 r., publiczne aktualizacje środowiska Oracle JAVA SE 8 do użytku biznesowego, komercyjnego lub produkcyjnego będą wymagać licencji komercyjnej. Jeśli nie chcesz kupować subskrypcji środowiska JAVA SE, możesz przejść na bezpłatną alternatywę. Zobacz obsługiwane wersje JDK.

Jak określić, którego portu używa program SQL Server?

Jest kilka sposobów na ustalenie, którego portu używa program SQL Server. Najlepszy rezultat można uzyskać przy użyciu Menedżera konfiguracji programu SQL Server. Na poniższym rysunku przedstawiono, gdzie można znaleźć te informacje w oknie Menedżera konfiguracji programu SQL Server:



Po zainstalowaniu programu SQL Server Express (dołączonego do pakietu ESET PROTECT) w systemie Windows Server 2012 informacje o nasłuchiwaniu przy użyciu standardowego portu SQL mogą być niedostępne. Jest tak, ponieważ nasłuch najprawdopodobniej odbywa się na porcie innym niż domyślny port 1433.

Jak skonfigurować program MySQL, by przyjmował większe pakiety?

Należy zapoznać się z sekcją dotyczącą instalacji i konfiguracji programu MySQL w systemie Windows lub Linux.

Jak w przypadku samodzielnej instalacji programu SQL utworzyć bazę danych programu ESET PROTECT?

Taka czynność nie jest wymagana. Baza danych jest tworzona przez instalator *Server.msi*, a nie przez instalator ESET PROTECT. W celu uproszczenia procedury do pakietu dołączono instalator programu ESET PROTECT. Instaluje on program SQL Server, po czym instalator *Server.msi* tworzy bazę danych.

Umożliwia utworzenie nowej bazy danych ESET PROTECT w ramach istniejącej instalacji oprogramowania MS SQL Server w przypadku podania prawidłowych danych połączenia z serwerem MS SQL oraz poświadczeń? Możliwość obsługi różnych wersji oprogramowania SQL Server (2014, 2019 itd.) byłaby udogodnieniem.

Baza danych jest tworzona przez instalator *Server.msi*. Tak, utworzenie bazy danych ESET PROTECT w osobno zainstalowanych instancjach oprogramowania SQL Server jest możliwe. Obsługiwane wersje oprogramowania MS SQL Server to wersja 2014 i nowsze.

W wersji ESET PROTECT 9.1 Instalator kompleksowy domyślnie instaluje produkt Microsoft SQL Server Express 2019.

- Jeśli używasz starszej wersji systemu Windows (Server 2012 lub SBS 2011), domyślnie zainstalowany zostanie produktMicrosoft SQL Server Express 2014.
- Instalator automatycznie generuje losowe hasło do uwierzytelniania bazy danych (przechowywane w pliku *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*).

⚠ Program Microsoft SQL Server Express ma limit rozmiaru wynoszący 10 GB dla każdej relacyjnej bazy danych. Nie zalecamy korzystania z programu Microsoft SQL Server Express:
- w środowiskach firmowych lub dużych sieciach,
- Jeśli produkt ESET PROTECT ma być używany z ESET Inspect.

Czy w przypadku instalacji na istniejącym serwerze SQL na tym serwerze powinien być domyślnie używany wbudowany tryb uwierzytelniania systemu Windows?

Nie, ponieważ tryb uwierzytelniania systemu Windows może być wyłączony na serwerze SQL. Należy logować się tylko przy użyciu uwierzytelniania programu SQL Server (wprowadzając nazwę użytkownika i hasło). Podczas instalacji serwera ESET PROTECT wymagane jest uwierzytelnianie w trybie mieszanym (uwierzytelnianie serwera SQL i systemu Windows). W przypadku ręcznego instalowania programu SQL Server zalecane jest utworzenie hasła głównego (nazwa użytkownika głównego, „sa", to skrót od słów „security admin", czyli administrator zabezpieczeń) i zapisanie go w bezpiecznym miejscu. Hasło główne może być potrzebne przy uaktualnianiu serwera ESET PROTECT. Po zainstalowaniu serwera ESET PROTECT można ustawić uwierzytelnianie systemu Windows.

Czy można użyć bazy danych MariaDB zamiast programu MySQL?

Nie, baza danych MariaDB nie jest obsługiwana. Pamiętaj o zainstalowaniu obsługiwanej wersji programu MySQL Server i łącznika ODBC. Patrz sekcja Instalacja i konfiguracja oprogramowania MySQL.

Musiałem zainstalować Microsoft .NET Framework 4, jak wskazał mi Instalator ESET PROTECT (http://www.microsoft.com/en-us/download/details.aspx?id=17851), ale to nie działało w nowej instalacji systemu Windows Server 2012 R2 z dodatkiem SP1.

W systemie Windows Server 2012 ze względu na jego zasady zabezpieczeń nie można tego instalatora użyć. Oprogramowanie Microsoft .NET Framework należy zainstalować przy użyciu **Kreatora dodawania ról i funkcji**.

Trudno ustalić, czy trwa instalacja programu SQL Server. Jak sprawdzić, co się dzieje, jeśli instalacja trwa dłużej niż 10 minut?

Instalacja programu SQL Server może w rzadkich przypadkach zająć nawet 1 godzinę. Czas instalacji zależy od wydajności systemu.

Jak zresetować hasło administratora konsoli internetowej (wprowadzone podczas konfiguracji)?

Hasło można zresetować, uruchamiając instalator serwera i wybierając pozycję **Napraw**. Jeśli podczas tworzenia bazy danych nie użyto uwierzytelniania systemu Windows, dostęp do bazy danych serwera ESET PROTECT może wymagać podania hasła.

- Należy zachować ostrożność, ponieważ niektóre opcje naprawy mogą spowodować usunięcie zapisanych danych.
- Zresetowanie hasła powoduje wyłączenie uwierzytelniania dwuskładnikowego.

Jaki format powinien mieć importowany plik z listą komputerów do dodania do serwera ESET PROTECT?

Format przedstawiono w poniższych wierszach:

*Wszystkie**Grupa_1**Grupa_N**Komputer_1*
*Wszystkie**Grupa_1**Grupa_M**Komputer_X*
Wszystkie to wymagana nazwa grupy głównej.

Czy zamiast produktu IIS można użyć oprogramowania Apache? Czy można użyć innego serwera HTTP?

Produkt IIS to serwer HTTP. Konsola internetowa wymaga do działania kontenera serwletu Java (na przykład Tomcat). Nie wystarczy serwer HTTP. Istnieją instrukcje zmieniania produktu IIS w kontener serwletu Java. Jednak nie zalecamy ich wykonywania.

Nie należy używać serwera Apache HTTP. Firma ESET stosuje inny produkt — serwer Apache Tomcat.

Ma ESET PROTECT interfejs wiersza polecenia?

Tak, jest to ESET PROTECT ServerApi.

Czy program ESET PROTECT można zainstalować na kontrolerze domeny?

Nie instaluj programu SQL Server na kontrolerze domeny (np. w przypadku korzystania z systemu Windows SBS/Essentials). Zalecamy zainstalowanie programu ESET PROTECT na innym serwerze lub niezaznaczanie komponentu SQL Server Express podczas instalacji (wymaga to uruchomienia bazy danych ESET PROTECT na istniejącym serwerze SQL lub MySQL).

Czy instalator serwera ESET PROTECT wykrywa oprogramowanie SQL zainstalowane w systemie? Co się, jeśli wykryje takie oprogramowanie? Jak to jest w przypadku oprogramowania MySQL?

Program ESET PROTECT sprawdza, czy w systemie działa oprogramowanie SQL, gdy używany jest kreator i wybrana została opcja zainstalowania oprogramowania SQL Express. Jeśli w systemie działa już oprogramowanie SQL, kreator wyświetla monit o odinstalowanie istniejącego oprogramowania SQL i ponownego uruchomienia instalacji lub o zainstalowanie programu ESET PROTECT bez oprogramowania SQL Express. Więcej informacji zawiera sekcja poświęcona wymaganiom bazy danych dotycząca programu ESET PROTECT.

Gdzie znajdują się informacje o komponentach ESET PROTECT w poszczególnych wersjach programu?

Szczegółowe informacje zawiera następujący artykuł bazy wiedzy.

Jak uaktualnić program ESET PROTECT do najnowszej wersji?

Zobacz Procedury uaktualniania.

Jak zaktualizować system bez połączenia z Internetem?

Należy użyć serwera proxy HTTP zainstalowanego na komputerze, który może połączyć się z serwerami aktualizacji firmy ESET (przechowującymi pliki aktualizacji), i wskazać punkty końcowe do tego serwera proxy

HTTP w sieci lokalnej. Jeśli serwer nie ma połączenia z Internetem, można włączyć funkcję kopii dystrybucyjnej produktu Endpoint na jednym z komputerów, przy użyciu dysku USB umieścić pliki aktualizacji na tym komputerze i skonfigurować wszystkie pozostałe komputery bez połączenia z Internetem tak, aby używały tego komputera jako serwera aktualizacji.

Szczegółowe instrukcje przeprowadzania instalacji offline znajdują się tutaj.

Jak odinstalować i ponownie zainstalować serwer ESET PROTECT i połączyć go z istniejącym serwerem SQL, jeśli serwer SQL został skonfigurowany automatycznie podczas początkowej instalacji programu ESET PROTECT?

W przypadku instalowania nowej instancji serwera ESET PROTECT za pomocą tego samego konta użytkownika (na przykład konta administratora domeny), którego użyto do instalacji oryginalnego serwera ESET PROTECT, można użyć opcji **MS SQL Server z uwierzytelnianiem systemu Windows**.

Jak rozwiązać problemy dotyczące synchronizacji z usługą Active Directory w systemie Linux?

Należy zweryfikować, czy wprowadzona nazwa domeny została napisana przy użyciu samych wielkich liter (`administrator@TEST.LOCAL` zamiast `administrator@test.local`).

Czy zamiast repozytorium można użyć własnych zasobów sieciowych (na przykład udziału SMB)?

Można wprowadzić bezpośredni adres URL do miejsca, w którym znajduje się pakiet. W przypadku używania udziału plików należy określić go w tym formacie: file://, a dalej pełna ścieżka sieciowa do pliku, na przykład:

file://\\serwer_era\instalator\ees_nt64_ENU.msi

Jak zresetować lub zmienić hasło?

Idealnym rozwiązaniem jest używanie konta administratora wyłącznie do tworzenia kont dla dodatkowych administratorów. Po utworzeniu kont administratorów należy zapisać hasło administratora i nie używać konta administratora. Dzięki temu konto administratora może być używane tylko na potrzeby resetowania hasła / szczegółów konta.

Resetowanie hasła wbudowanego konta administratora ESET PROTECT:

1. Otwórz aplet **Programy i funkcje** (uruchom polecenie appwiz.cpl), znajdź serwer ESET PROTECT i kliknij go prawym przyciskiem myszy.
2. Z menu kontekstowego wybierz opcję **Zmień**.
3. Wybierz opcję **Napraw**.
4. Podaj szczegóły połączenia z bazą danych.
5. Wybierz opcję **Użyj istniejącej bazy danych i zastosuj uaktualnienie**.
6. Wyczyść opcję **Użyj hasła, które jest już zapisane w bazie danych** i wprowadź nowe hasło.
7. Zaloguj się w konsoli internetowej ESET PROTECT przy użyciu nowego hasła.

> Zdecydowanie zalecamy utworzenie dodatkowych kont o określonych uprawnieniach dostępu w oparciu o wymagane kompetencje użytkownika konta.

Jak zmienić porty serwera ESET PROTECT i porty konsoli internetowej ESET PROTECT?

Aby umożliwić połączenia z serwerem internetowym przy użyciu nowego portu, należy zmienić port w konfiguracji serwera internetowego. W tym celu należy wykonać poniższe działania:

1. Wyłącz serwer internetowy.
2. Zmień port w konfiguracji serwera internetowego.
   a) Otwórz plik *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
   b) Ustaw nowy numer portu (na przykład `server_port=44591`))
3. Uruchom ponownie serwer internetowy.

Czy można uaktualnić program ERA w wersji 5 lub 6 do programu ESET PROTECT9 bezpośrednio przy użyciu instalatora kompleksowego?

Bezpośrednie uaktualnienie nie jest obsługiwane – zobacz Migracja z wersji ERA 5.x oraz Aktualizacja z wersji ERA 6.x.

Występują komunikaty o błędach lub problemy dotyczące produktu ESET PROTECT. Co należy zrobić?

Należy zapoznać się z odpowiedziami na często zadawane pytania dotyczące rozwiązywania problemów.

Umowa licencyjna użytkownika końcowego

Obowiązuje od 19 października 2021 r..

WAŻNE: Przed pobraniem, zainstalowaniem, skopiowaniem lub użyciem Oprogramowania należy się dokładnie zapoznać z poniższymi warunkami korzystania z produktu. **POBRANIE, ZAINSTALOWANIE, SKOPIOWANIE LUB UŻYCIE OPROGRAMOWANIA OZNACZA WYRAŻENIE ZGODY NA NINIEJSZE WARUNKI I AKCEPTACJĘ POLITYKI PRYWATNOŚCI.**

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego („Umową”), zawierana między spółką ESET, spol. s r. o., z siedzibą w Słowacji pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym Sądu Rejonowego dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („firmą ESET” lub „Dostawcą”), a licencjobiorcą, który jest osobą fizyczną lub prawną („Licencjobiorcą” lub „Użytkownikiem końcowym”), uprawnia Licencjobiorcę do korzystania z Oprogramowania określonego w punkcie 1 niniejszej Umowy. Oprogramowanie określone w punkcie 1 niniejszej Umowy może znajdować się na nośniku danych albo zostać przesłane pocztą elektroniczną, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł na warunkach wyszczególnionych poniżej.

NINIEJSZA UMOWA DOTYCZY WYŁĄCZNIE OKREŚLENIA PRAW UŻYTKOWNIKA KOŃCOWEGO I NIE STANOWI UMOWY SPRZEDAŻY. Dostawca pozostaje właścicielem kopii Oprogramowania i nośnika fizycznego zawartego w opakowaniu z produktem, a także wszystkich innych kopii Oprogramowania, które Użytkownik końcowy może wykonać zgodnie z niniejszą Umową.

Kliknięcie opcji „Akceptuję” lub „Akceptuję...” w trakcie instalowania, pobierania, kopiowania lub używania Oprogramowania oznacza, że Licencjobiorca wyraża zgodę na warunki określone w niniejszej Umowie oraz akceptuje Politykę prywatności. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie i/lub Polityce prywatności, powinien niezwłocznie kliknąć opcję anulowania i przerwać instalację lub pobieranie albo zniszczyć Oprogramowanie, nośnik instalacyjny, dokumentację towarzyszącą Oprogramowaniu i dowód sprzedaży Oprogramowania bądź zwrócić je Dostawcy lub w miejscu zakupu Oprogramowania.

LICENCJOBIORCA PRZYJMUJE DO WIADOMOŚCI, ŻE KORZYSTANIE Z OPROGRAMOWANIA OZNACZA ZAPOZNANIE

SIĘ Z NINIEJSZĄ UMOWĄ, ZROZUMIENIE WARUNKÓW W NIEJ OKREŚLONYCH ORAZ ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA.

1. **Oprogramowanie.** W niniejszej Umowie termin „Oprogramowanie" oznacza: (i) program komputerowy, do którego dołączono niniejszą Umowę, i wszystkie jego składniki; (ii) całą zawartość dysków, płyt CD-ROM i płyt DVD, wiadomości e-mail wraz z ich załącznikami oraz innych nośników, do których jest dołączona niniejsza Umowa, w tym Oprogramowanie w formie kodu obiektowego dostarczone na nośniku danych albo za pośrednictwem poczty elektronicznej lub Internetu; (iii) wszelkie powiązane drukowane materiały instruktażowe oraz wszelką inną dokumentację powiązaną z Oprogramowaniem, w tym przede wszystkim wszelkie opisy Oprogramowania, jego dane techniczne, wszelkie opisy jego właściwości lub działania, wszelkie opisy środowiska operacyjnego, w którym Oprogramowanie jest używane, instrukcje obsługi lub instalacji Oprogramowania oraz wszelkie opisy sposobu korzystania z Oprogramowania („Dokumentacją"); (iv) wszelkie ewentualne kopie Oprogramowania, poprawki możliwych błędów Oprogramowania, dodatki do Oprogramowania, rozszerzenia Oprogramowania, zmodyfikowane wersje Oprogramowania oraz aktualizacje składników Oprogramowania, na które Dostawca udziela Licencjobiorcy licencji zgodnie z zapisami w punkcie 3 niniejszej Umowy. Oprogramowanie będzie dostarczane wyłącznie w postaci wykonywalnego kodu obiektowego.

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

3. **Licencja**. Dostawca udziela Licencjobiorcy praw określonych poniżej (w dalszej części nazywanych zbiorczo „Licencją"), jeśli Licencjobiorca zobowiązał się przestrzegać i przestrzega wszelkich warunków określonych w niniejszej Umowie:

a) **Instalacja i użycie.** Licencjobiorcy przysługują niewyłączne, nieprzenoszalne prawa do zainstalowania Oprogramowania na dysku twardym komputera lub na innym nośniku do trwałego przechowywania danych, do zainstalowania i przechowywania Oprogramowania w pamięci systemu komputerowego oraz do zaimplementowania, przechowywania i wyświetlania Oprogramowania.

b) **Postanowienia w sprawie liczby Licencji.** Prawo do korzystania z Oprogramowania w ramach jednej Licencji jest ograniczone do jednego Użytkownika końcowego. Jeden Użytkownik końcowy oznacza: (i) instalację Oprogramowania na jednym komputerze lub, jeśli liczba Licencji zależy od liczby skrzynek pocztowych, (ii) użytkownika komputera, który odbiera pocztę elektroniczną za pośrednictwem klienta poczty elektronicznej. Jeśli do klienta poczty elektronicznej dociera poczta elektroniczna, która jest następnie automatycznie dystrybuowana do innych użytkowników, liczbę Użytkowników końcowych stanowi liczba wszystkich użytkowników, do których jest dostarczana poczta. Jeśli serwer poczty pełni funkcję bramy pocztowej, liczba Użytkowników końcowych jest równa liczbie użytkowników serwera poczty, którzy są obsługiwani przez tę bramę. Jeśli jeden użytkownik odbiera pocztę przesyłaną na różne adresy e-mail (np. za pośrednictwem usługi aliasów), a liczba tych adresów jest nieokreślona i wiadomości nie są automatycznie dystrybuowane przez klienta poczty elektronicznej do większej liczby użytkowników, wymagana jest Licencja na jednego użytkownika komputera. Z jednej Licencji można korzystać każdorazowo tylko na jednym komputerze. Użytkownik końcowy może wprowadzić klucz licencyjny do Oprogramowania tylko w zakresie, w jakim przysługuje mu prawo do korzystania z Oprogramowania zgodnie z

ograniczeniami wynikającymi z liczby Licencji przyznanych przez Dostawcę. Klucz licencyjny ma charakter poufny, Licencjobiorca nie może udostępniać Licencji stronom trzecim ani pozwalać im na używanie klucza licencyjnego, o ile nie dopuszcza tego niniejsza Umowa lub Dostawca. W przypadku naruszenia klucza licencyjnego należy bezzwłocznie powiadomić Dostawcę.

c) **Wersja Home/Business Edition.** Wersja Home Oprogramowania jest przeznaczona wyłącznie do używania w środowiskach prywatnych i/lub niekomercyjnych tylko na użytek domowy i rodzinny. W przypadku zamiaru zainstalowania i użycia Oprogramowania w środowisku komercyjnym, na serwerze poczty, w systemie przekazywania wiadomości e-mail lub w połączeniu z bramą pocztową bądź internetową wymagane jest nabycie wersji Business Edition Oprogramowania.

d) **Okres obowiązywania Licencji.** Prawo do korzystania z Oprogramowania jest ograniczone w czasie.

e) **Oprogramowanie dostarczone przez producenta urządzenia (OEM).** Prawo do korzystania z Oprogramowania, które zostało dostarczone przez producenta zakupionego urządzenia (OEM, Original Equipment Manufacturer), jest ograniczone do tego urządzenia. Prawa tego nie można przenosić na inne urządzenia.

f) **Oprogramowanie w wersji próbnej lub nieprzeznaczonej do obrotu handlowego.** Nie można pobierać opłat za korzystanie z Oprogramowania, które jest oznaczone napisem „Not for resale" lub „NFR" (Nie do sprzedaży) albo „TRIAL" (Wersja próbna). Oprogramowanie takie jest przeznaczone wyłącznie do prezentacji lub testowania jego funkcji.

g) **Wygaśnięcie Licencji.** Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

4. **Wymagania dotyczące funkcji gromadzących dane i połączenia z Internetem.** Aby Oprogramowanie działało poprawnie, wymagane jest stałe połączenie z Internetem oraz regularne połączenia z serwerami Dostawcy lub z serwerami innych firm, a gromadzenie potrzebnych danych powinno odbywać się zgodnie z obowiązującą Polityką prywatności. Połączenie z Internetem oraz gromadzenie potrzebnych danych są wymagane do funkcjonowania oraz aktualizowania Oprogramowania. Dostawca jest uprawniony do wprowadzania aktualizacji w Oprogramowaniu (w dalszej części nazywanych „Aktualizacjami"), przy czym nie jest zobowiązany do ich wprowadzania. Funkcja Aktualizacji jest domyślnie włączona w ustawieniach standardowych Oprogramowania, dlatego Aktualizacje są instalowane automatycznie, o ile Użytkownik końcowy nie zmienił ustawienia automatycznego instalowania Aktualizacji. W celu przeprowadzania aktualizacji wymagana jest weryfikacja autentyczności Licencji, w tym informacji dotyczących komputera i/lub platformy, na której zostało zainstalowane Oprogramowanie, zgodnie z Polityką Prywatności.

Dostarczanie wszelkich Aktualizacji może podlegać Polityce końca okresu użytkowania ("Polityka EOL"), która jest dostępna na stronie stronie https://go.eset.com/eol_business. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą dostarczane żadne aktualizacje.

Na potrzeby niniejszej Umowy konieczne jest gromadzenie, przetwarzanie i przechowywanie danych umożliwiających Dostawcy identyfikację Licencjobiorcy zgodnie z Polityką prywatności. Licencjobiorca niniejszym zgadza się, aby Dostawca, korzystając z własnych środków, mógł sprawdzić, czy Licencjobiorca używa Oprogramowania zgodnie z postanowieniami niniejszej Umowy. Licencjobiorca zgadza się, że na potrzeby niniejszej Umowy konieczne jest przekazywanie jego danych podczas komunikacji pomiędzy Oprogramowaniem a

systemami komputerowymi Dostawcy lub jego partnerów handlowych w ramach sieci dystrybucyjnej i wsparcia Dostawcy w celu zapewnienia funkcjonalności Oprogramowania i upoważnienia do używania Oprogramowania oraz ochrony praw Dostawcy.

Po zawarciu niniejszej Umowy Dostawca i każdy z jego partnerów handlowych, w ramach sieci dystrybucyjnej i wsparcia Dostawcy, będzie uprawniony do przekazywania, przetwarzania i przechowywania istotnych danych identyfikujących Licencjobiorcę w celach związanych z rozliczaniem opłat, wykonywaniem niniejszej Umowy i przekazywaniem powiadomień na komputerze Licencjobiorcy.

Szczegółowe informacje na temat ochrony prywatności, danych osobowych i praw Licencjobiorcy jako podmiotu danych dostępne są w Polityce prywatności w witrynie Dostawcy, bezpośrednio podczas procesu instalacji. Można do niej przejść także z poziomu sekcji pomocy w Oprogramowaniu.

5. **Wykonywanie praw Użytkownika końcowego**. Licencjobiorca może wykonywać swoje prawa wyłącznie osobiście lub za pośrednictwem swoich pracowników. Licencjobiorca może korzystać z Oprogramowania wyłącznie w celu zapewnienia ciągłości swojej działalności gospodarczej i w celu zabezpieczenia komputerów lub systemów komputerowych, na które uzyskał Licencję.

6. **Ograniczenie praw.** Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników Oprogramowania, jak również nie może tworzyć produktów na podstawie Oprogramowania (nie może wykonywać dzieł pochodnych). Korzystając z Oprogramowania, Licencjobiorca musi przestrzegać następujących ograniczeń:

a) Licencjobiorca może wykonać jedną kopię Oprogramowania na nośniku przeznaczonym do trwałego przechowywania danych i przechowywać tę kopię w charakterze archiwalnej kopii zapasowej, tj. nie może zainstalować ani użyć takiej kopii na żadnym komputerze. Wszelkie inne kopie Oprogramowania wykonane przez Licencjobiorcę stanowią naruszenie warunków określonych w niniejszej Umowie.

b) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Oprogramowania ani jego kopii w sposób inny niż wyszczególniony w niniejszej Umowie.

c) Licencjobiorca nie może sprzedawać Oprogramowania, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Oprogramowania w celu świadczenia usług o charakterze dochodowym.

d) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

f) Licencjobiorca zgadza się korzystać z Oprogramowania i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym Użytkownikom końcowym. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym Użytkownikom końcowym w celu zapewnienia możliwości korzystania z nich jak największej liczbie Użytkowników końcowych. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Oprogramowania oraz usunięcie Danych i informacji przechowywanych na serwerach Dostawcy lub zewnętrznego podmiotu związanych z wybranymi funkcjami Oprogramowania.

g) Licencjobiorca zobowiązuje się nie podejmować działań obejmujących korzystanie z klucza licencyjnego, niezgodnych z postanowieniami niniejszej Umowy lub prowadzących do przekazania klucza licencyjnego osobie nieuprawnionej do korzystania z Oprogramowania, takich jak przekazanie wykorzystanego lub niewykorzystanego

klucza licencyjnego w dowolnej formie, a także nieautoryzowana reprodukcja lub dystrybucja zduplikowanych lub wygenerowanych kluczy licencyjnych albo korzystanie z Oprogramowania w wyniku wykorzystania klucza licencyjnego uzyskanego z innego źródła niż Dostawca.

7. **Prawo autorskie**. Oprogramowanie i wszystkie prawa z nim związane, w tym między innymi prawa własności i prawa własności intelektualnej do Oprogramowania, należą do firmy ESET i/lub jej licencjodawców. Prawa te gwarantują zapisy traktatów międzynarodowych oraz wszelkie właściwe przepisy ustawowe obowiązujące w kraju, w którym jest używane Oprogramowanie. Struktura Oprogramowania, sposób jego zorganizowania i kod w nim zawarty są cennymi tajemnicami handlowymi oraz informacjami poufnymi firmy ESET i/lub jej licencjodawców. Licencjobiorca nie może kopiować Oprogramowania poza okolicznościami opisanymi w punkcie 6(a). Wszelkie kopie utworzone przez Licencjobiorcę zgodnie z niniejszą Umową muszą zawierać te same informacje o prawie autorskim i innych prawach własności, które znajdują się w Oprogramowaniu. Licencjobiorca niniejszym przyjmuje do wiadomości, że w razie naruszenia postanowień niniejszej Umowy przez podjęcie próby odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji albo w inny sposób prawa do wszelkich informacji uzyskanych przez Licencjobiorcę w wyniku podjęcia takiej próby zostaną uznane za automatycznie i nieodwołalnie przeniesione w całości na Dostawcę już w momencie powstania takich informacji i to niezależnie od praw przysługujących Dostawcy w związku z naruszeniem przez Licencjobiorcę warunków określonych w niniejszej Umowie.

8. **Zastrzeżenie praw**. Dostawca niniejszym zastrzega sobie wszelkie prawa do Oprogramowania, z wyjątkiem praw wyraźnie udzielonych Licencjobiorcy, występującemu w charakterze Użytkownika końcowego, na podstawie niniejszej Umowy.

9. **Różne wersje językowe, Oprogramowanie obsługujące wiele urządzeń i wiele kopii Oprogramowania**. Jeśli Oprogramowanie może obsługiwać wiele platform lub języków bądź jeśli Licencjobiorca uzyskał wiele kopii Oprogramowania, Oprogramowania można używać tylko na tych systemach komputerowych i w tych wersjach, na które Licencjobiorca uzyskał Licencje. Licencjobiorca nie może sprzedawać wersji ani kopii Oprogramowania, których nie używa, jak również nie może ich oddawać w użytkowanie, udzielać na nie podlicencji, wypożyczać ich ani przenosić do nich praw na inne osoby.

10. **Rozpoczęcie i zakończenie obowiązywania Umowy.** Niniejsza Umowa wchodzi w życie z datą wyrażenia przez Licencjobiorcę zgody na warunki określone w tej Umowie. Licencjobiorca może rozwiązać niniejszą Umowę w dowolnej chwili przez trwałe odinstalowanie i zniszczenie Oprogramowania, wszystkich jego kopii zapasowych i wszelkich powiązanych materiałów dostarczonych przez Dostawcę lub jego partnerów handlowych bądź przez zwrócenie tych produktów na własny koszt. Prawo Licencjobiorcy do korzystania z Oprogramowania i wszelkich jego funkcji może podlegać Polityce EOL. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, prawo Licencjobiorcy do korzystania z Oprogramowania wygaśnie. Bez względu na powód rozwiązania niniejszej Umowy po zakończeniu jej obowiązywania nadal obowiązują postanowienia zawarte w punktach 7, 8, 11, 13, 19 i 21.

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

12. **Brak innych zobowiązań**. W niniejszej Umowie określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

13. **OGRANICZENIE ODPOWIEDZIALNOŚCI**. O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA, ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY LICENCJODAWCY NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z INSTALACJĄ, UŻYCIEM CZY Z NIEMOŻNOŚCIĄ UŻYCIA OPROGRAMOWANIA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO LICENCJODAWCY BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, LICENCJODAWCÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

14. Jeśli którekolwiek postanowienie niniejszej Umowy jest sprzeczne z ustawowymi prawami konsumenckimi jakiejkolwiek osoby, postanowienie to nie może być interpretowane w sposób naruszający te prawa.

15. **Pomoc techniczna**. Usługi pomocy technicznej świadczą wedle własnego uznania i bez udzielania jakichkolwiek gwarancji firma ESET lub inne firmy, którym firma ESET zleca świadczenie takich usług. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą świadczone żadne usługi pomocy technicznej. Przed skorzystaniem z usługi pomocy technicznej Użytkownik końcowy musi utworzyć kopię zapasową wszystkich istniejących danych, programów i aplikacji. Ani firma ESET, ani inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, nie mogą wziąć na siebie odpowiedzialności za uszkodzenie lub utratę danych, własności, oprogramowania lub urządzeń, jak również nie mogą odpowiadać za utratę zysków spowodowaną świadczeniem usług pomocy technicznej. Firma ESET i/lub inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, zastrzegają sobie prawo do odmowy wykonania usługi, jeśli uznają, że nie mieści się ona w zakresie oferowanych usług pomocy technicznej. Firma ESET zastrzega sobie prawo do odmowy, wstrzymania lub zaprzestania świadczenia usług pomocy technicznej, jeśli uzna to za stosowne. Informacje dotyczące licencji, Informacje i inne dane zgodne z Polityką prywatności mogą być wymagane na potrzeby świadczenia pomocy technicznej.

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają, Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

17. **Weryfikowanie oryginalności Oprogramowania.** Użytkownik końcowy może wykazać swoje uprawnienia do korzystania z Oprogramowania w jeden z poniższych sposobów: (i) na podstawie certyfikatu licencyjnego wystawionego przez Dostawcę lub inną firmę wskazaną przez Dostawcę; (ii) na podstawie pisemnej umowy

licencyjnej, jeśli została ona zawarta; (iii) na podstawie wiadomości e-mail od Dostawcy z danymi dotyczącymi licencji (nazwą użytkownika i hasłem). Informacje dotyczące licencji oraz dane identyfikujące Użytkownika końcowego zgodne z Polityką prywatności mogą być wymagane w celu weryfikacji oryginalności Oprogramowania.

18. **Udzielanie Licencji organom władzy publicznej i rządowi USA**. Organy władzy publicznej, w tym rząd Stanów Zjednoczonych Ameryki Północnej, otrzymują Licencje na Oprogramowanie zgodnie z postanowieniami niniejszej Umowy, tj. z uwzględnieniem wszystkich praw i obowiązków określonych w niniejszej Umowie.

19. **Zgodność z przepisami o kontroli handlu**.

a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe („Podmiotami stowarzyszonymi"), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność.

(Akty prawne, o których mowa w pkt i i ii powyżej, łącznie nazywane są „Przepisami dotyczącymi kontroli handlu").

b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć postanowienia punktu 19 a) Umowy.

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z Umowy mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

20. **Zawiadomienia**. Wszystkie zawiadomienia oraz zwroty Oprogramowania i Dokumentacji należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez uszczerbku dla praw firmy ESET do

komunikowania użytkownikowi wszelkich zmian w niniejszej Umowie, Polityce Prywatności, Polityce EOL oraz Dokumentacji zgodnie z punktem 22 niniejszej Umowy. Firma ESET może wysyłać wiadomości e-mail, powiadomienia w aplikacji za pośrednictwem Oprogramowania lub poprzez publikację komunikatów na naszej stronie internetowej. Użytkownik wyraża zgodę na otrzymywanie od firmy ESET informacji prawnych w formie elektronicznej, w tym wszelkich komunikatów dotyczących zmian Warunków, Warunków szczególnych lub Polityki Prywatności, wszelkich propozycji/akceptacji umowy lub zaproszeń do pertraktacji, powiadomień lub innych komunikatów prawnych. Taką komunikację elektroniczną uznaje się za otrzymaną na piśmie, chyba że obowiązujące przepisy prawa wyraźnie wymagają innej formy komunikacji.

21. **Prawo właściwe**. Niniejsza Umowa podlega przepisom prawnym obowiązującym w Słowacji i powinna być interpretowana zgodnie z tymi przepisami. Użytkownik końcowy i Dostawca niniejszym stwierdzają, że do niniejszej Umowy nie mają zastosowania przepisy dotyczące konfliktu praw ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z zawarcia niniejszej Umowy, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu.

22. **Postanowienia ogólne**. Uznanie któregokolwiek z postanowień niniejszej Umowy za nieważne lub niewykonalne nie wpływa na ważność innych postanowień niniejszej Umowy, które pozostają wówczas w mocy zgodnie z warunkami określonymi w niniejszej Umowie. Niniejsza Umowa została zawarta w języku angielskim. W przypadku sporządzenia tłumaczenia niniejszej Umowy dla wygody lub do innych celów oraz w przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska.

Firma ESET zastrzega sobie prawo do wprowadzania zmian w Oprogramowaniu oraz modyfikowania warunków niniejszej Umowy, Aneksów, Załączników, Polityki Prywatności, Polityki EOL oraz Dokumentacji lub dowolnej ich części w dowolnym czasie poprzez aktualizowanie odpowiednich dokumentów (i) w celu odzwierciedlenia zmian wprowadzonych w zakresie Oprogramowania oraz w sposobie prowadzenia działalności przez firmę ESET, (ii) ze względów prawnych, regulacyjnych lub bezpieczeństwa lub (iii) w celu zapobiegania nadużyciom lub szkodom. Licencjobiorca zostanie powiadomiony o wszelkich zmianach w niniejszej Umowie za pośrednictwem poczty e-mail, powiadomienia w aplikacji lub innych kanałów komunikacji elektronicznej. Jeśli Licencjobiorca nie zgadza się z proponowanymi zmianami w Umowie, może ją rozwiązać zgodnie z punktem 10 w ciągu 30 dni od otrzymania powiadomienia o zmianie. O ile Licencjobiorca nie wypowie Umowy w tym terminie, proponowane zmiany zostaną uznane za zaakceptowane i wejdą w życie wobec Licencjobiorcy od dnia otrzymania powiadomienia o zmianie.

Niniejsza Umowa stanowi całość porozumienia między Dostawcą a Licencjobiorcą w sprawie Oprogramowania i zastępuje wszelkie wcześniejsze oświadczenia, negocjacje, zobowiązania, wymiany zdań lub reklamy związane z Oprogramowaniem.

ANEKS DO UMOWY

Przekazywanie informacji Dostawcy. Dodatkowe zapisy dotyczące przekazywania informacji Dostawcy brzmią następująco:

Oprogramowanie obejmuje funkcje, które gromadzą dane o procesie instalacji, komputerze i/lub platformie, na której zainstalowano Oprogramowanie, o działaniu i funkcjonalności Oprogramowania oraz o zarządzanych urządzeniach (odtąd ogólnie „Informacje"), a następnie wysyłają te dane Dostawcy. Informacje mogą obejmować dane dotyczące zarządzanych urządzeń (w tym losowo lub przypadkowo uzyskane dane osobowe). Włączenie tej funkcji Oprogramowania oznacza, że Dostawca może gromadzić i przetwarzać Informacje zgodnie z Polityką prywatności i obowiązującymi przepisami prawa.

Oprogramowanie wymaga zainstalowania na zarządzanym komputerze składnika, który umożliwia przesyłanie informacji między zarządzanym komputerem i oprogramowaniem do zdalnego zarządzania. Przesyłane informacje

obejmują dane z zakresu zarządzania, takie jak informacje o sprzęcie i oprogramowaniu zarządzanego komputera, a także instrukcje dotyczące zarządzania pochodzące ze zdalnego oprogramowania do zarządzania. Pozostała zawartość danych przesyłanych z zarządzanego komputera zostanie określona przez ustawienia oprogramowania zainstalowanego na zarządzanym komputerze. Zawartość instrukcji pochodzących z oprogramowania do zarządzania zostanie określona przez ustawienia zdalnego oprogramowania do zarządzania.

EULAID: EULA-PRODUCT-PROTECT; 3537.0

Zasady ochrony prywatności

Firma ESET, spol. s r. o. z siedzibą pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla Bratysławy I w sekcji Sro, pozycja nr 3586/B, numer w rejestrze gospodarczym: 31333532 jako administrator danych (dalej "ESET" lub "my") pragnie zachować przejrzystość w odniesieniu do danych osobowych oraz poufności informacji swoich klientów. W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej "Użytkownik" lub "Ty") informacji na następujące tematy: W związku z tym publikujemy niniejsze Zasady ochrony prywatności wyłącznie w celu przekazania klientowi (dalej „Użytkownik końcowy” lub „Ty”) informacji na następujące tematy:

- przetwarzanie danych osobowych,
- poufność danych,
- prawa osób, których dane dotyczą.

Przetwarzanie danych osobowych

Usługi zaimplementowane w produkcie firmy ESET są przez nas świadczone zgodnie z postanowieniami Umowy licencyjnej użytkownika końcowego („Umowa EULA”), ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat gromadzenia danych związanych ze świadczonymi przez nas usługami. Oferujemy szereg usług przedstawionych w umowie EULA i dokumentacji produktu, takich jak aktualizacja/uaktualnianie, ESET LiveGrid®, ochrona przed niewłaściwym użyciem danych, pomoc techniczna itp. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

- Zarządzanie produktami zabezpieczającymi firmy ESET wymaga m.in. następujących danych i ich lokalnego przechowywania: identyfikator i nazwa stanowiska, nazwa produktu, informacje dotyczące licencji, informacje dotyczące aktywacji i wygaśnięcia, informacje dotyczące sprzętu i oprogramowania powiązane z zarządzanym komputerem, na którym zainstalowano produkt zabezpieczający firmy ESET. Dzienniki dotyczące działań zarządzanych produktów zabezpieczających firmy ESET oraz urządzeń są gromadzone w celu umożliwienia zarządzania funkcjami oraz usługami i nadzorowania ich bez automatycznego przesyłania do firmy ESET.
- Informacje dotyczące procesu instalacji, w tym platformy, na której nasz produkt jest instalowany, a także informacje dotyczące działań i funkcjonalności naszych produktów, na przykład sprzętowy odcisk palca, identyfikator instalacji, zrzuty awaryjne, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracyjne produktu, które mogą obejmować również zarządzane urządzenia.
- Informacje dotyczące licencji, takie jak identyfikator licencji oraz dane osobowe, takie jak imię, nazwisko, adres oraz adres e-mail, są wymagane do celów związanych z rozliczeniami, weryfikacją autentyczności licencji oraz świadczeniem przez nas usług.
- Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju mogą być wymagane informacje kontaktowe i dane zawarte w zgłoszeniach do działu pomocy. W zależności od kanału komunikacji wybranego do kontaktu z nami możemy gromadzić: adres e-mail, numer telefonu, informacje dotyczące licencji, szczegółowe informacje o produkcie lub opis zgłoszenia do pomocy technicznej. W celu usprawnienia

świadczenia pomocy możemy poprosić Użytkownika o dodatkowe informacje, takie jak wygenerowane pliki dziennika lub zrzuty pamięci.

- Dane dotyczące korzystania z naszej usługi są całkowicie anonimowe po zakończeniu sesji. Po zakończeniu sesji nie będą przechowywane żadne informacje umożliwiające identyfikację użytkownika.

Poufność danych

ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci dystrybucji, usług i pomocy technicznej. Przetwarzane przez nas informacje mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy EULA, na przykład świadczenia usług lub udzielania pomocy technicznej albo w celach rozliczeniowych. W zależności od lokalizacji Użytkownika końcowego i wybranych przez niego usług możemy być zmuszeni do wysyłania jego danych do kraju, który nie uzyskał decyzji Komisji Europejskiej stwierdzającej odpowiedni poziom ochrony. Każdorazowo proces ten przebiega zgodnie z przepisami o ochronie danych i odbywa się wyłącznie w razie konieczności. W każdym przypadku, bez wyjątków, muszą być ustanowione standardowe klauzule umowne, wiążące reguły korporacyjne lub inne odpowiednie zabezpieczenia.

Dokładamy wszelkich starań, aby nie dopuścić do przechowywania danych dłużej, niż jest to konieczne w związku ze sprzedażą usług na mocy umowy EULA. Okres przechowywania przez nas danych może być dłuższy niż okres ważność licencji użytkownika. Ma to umożliwić użytkownikowi łatwe i wygodne odnowienie licencji. Statystyki i inne dane zgromadzone przez usługę ESET LiveGrid® (w postaci zminimalizowanej i pseudonimizowanej) mogą być nadal przetwarzane w celach statystycznych.

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić ciągłą poufność, integralność, dostępność i odporność przetwarzanych systemów i usług. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie organów nadzorczych oraz właścicieli danych. Jako osoba, której dane dotyczą, użytkownik ma prawo do wniesienia skargi do organu nadzorczego.

Prawa osób, których dane dotyczą

Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Zgodnie z warunkami zapisanymi w obowiązujących przepisach dotyczących ochrony danych osobowych, każdemu właścicielowi danych przysługują następujące prawa:

- prawo do uzyskania wglądu w swoje dane osobowe gromadzone przez firmę ESET;
- prawo do wprowadzenia zmian w swoich danych osobowych, jeśli są nieprawidłowe (Użytkownik końcowy ma także prawo do uzupełnienia niekompletnych danych osobowych);
- prawo do usunięcia swoich danych osobowych;
- prawo do ograniczenia zakresu przetwarzania swoich danych osobowych;
- prawo do niewyrażenia zgody na przetwarzanie danych;
- prawo do wniesienia skargi;
- prawo do przeniesienia danych.

Jeżeli użytkownik chce skorzystać z prawa przysługującego mu jako osobie, której dane dotyczą, a także w przypadku pytań lub wątpliwości, użytkownik może przesłać do nas wiadomość na adres:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk