ESET PROTECT

Przewodnik dla małych i średnich firm

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 Wprowadzenie 2
2.1 Produkty firmy ESET do obsługi punktów końcowych, którymi można zarządzać 2
2.2 Nowe funkcje produktu ESET PROTECT 9.1 2
3 Komponenty i architektura rozwiązania ESET PROTECT 4
4 Wymagania systemowe 5
4.1 Sprzęt 5
4.2 System operacyjny 7
4.3 Sieć 9
4.4 Oprogramowanie 9
5 Instalowanie serwera ESET PROTECT 10
5.1 Instalacja kompleksowa serwera ESET PROTECT 11
6 Kroki po instalacji 24
7 Wdrażanie agenta ESET Management i produktów ESET do obsługi punktów końcowych 25
7.1 Tworzenie pakietu wdrożeniowego 26
7.2 Instalowanie pakietu wdrożeniowego 30
7.3 Inne metody wdrażania 33
7.4 ESET Remote Deployment Tool 34
8 Konsola internetowa ESET PROTECT 37
8.1 Przewodnik ESET PROTECT 39
8.2 Panel kontrolny 40
8.3 Komputery 42
8.4 Grupy 43
8.5 Wykrycia 45
8.6 Raporty 47
8.7 Zadania 47
8.8 Polityki 48
8.9 Powiadomienia 49
8.10 Przegląd stanu 51
8.11 Kwarantanna 52
8.12 Zarządzanie licencjami 53
8.13 Użytkownicy i zestawy uprawnień 54
8.14 Certyfikaty 55
9 Pomoc i obsługa 56
10 Umowa licencyjna użytkownika końcowego 56
11 Zasady ochrony prywatności 64

Informacje o pomocy

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.

Wprowadzenie

Niniejszy podręcznik jest przeznaczony dla małych i średnich firm zarządzających sieciami złożonymi z maksymalnie 250 komputerów z systemem Windows i produktami firmy ESET służącymi do obsługi punktów końcowych przy użyciu rozwiązania ESET PROTECT 9.
Objaśniono w nim podstawowe pojęcia związane z wdrażaniem produktów zabezpieczających firmy ESET i korzystaniem z nich.

ESET PROTECT 9

ESET PROTECT 9 (wcześniej ESMC) 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 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. Bezpieczeństwo środowiska jest uzależnione od obecności na stacjach roboczych rozwiązań zabezpieczających firmy ESET, takich jak ESET Endpoint Security.

Produkty firmy ESET do obsługi punktów końcowych, którymi można zarządzać

Produkty firmy ESET do obsługi punktów końcowych są przeznaczone do użytku na stacjach roboczych w środowiskach małych firm lub środowiskach korporacyjnych w połączeniu z rozwiązaniem ESET PROTECT.

w ramach rozwiązania ESET PROTECT 9 można wdrażać i aktywować następujące produkty ESET do obsługi punktów końcowych oraz nimi zarządzać:

Możliwość zarządzania przy użyciu rozwiązania ESET PROTECT 9	Wersja produktu
ESET Endpoint Security dla systemu Windows	6.5+, 7.x, 8.x, 9.x
ESET Endpoint Antivirus dla systemu Windows	6.5+, 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

Zobacz także pełną listę produktów zabezpieczających firmy ESET, którymi można zarządzać.

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.

Komponenty i architektura rozwiązania ESET PROTECT

Aby przeprowadzić całkowite wdrożenie pakietu rozwiązań zabezpieczających firmy ESET, należy zainstalować następujące komponenty:

- Serwer ESET PROTECT (służy do kontrolowania komunikacji z komputerami klienckimi)
- Konsola internetowa ESET PROTECT (dostępny w przeglądarce internetowej interfejs użytkownika do obsługi serwera ESET PROTECT)
- Agent ESET Management (komponent wdrażany na komputerach klienckich służący do komunikacji z serwerem ESET PROTECT)

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

- Serwer proxy Apache HTTP
- Narzędzie RD Sensor (umożliwia wykrywanie niezarządzanych komputerów w sieci)

Zobacz też Certyfikaty i struktura komponentów ESET PROTECT.

Serwer

Serwer ESET PROTECT to aplikacja przetwarzająca wszystkie dane odbierane z klientów łączących się z serwerem (za pośrednictwem agenta ESET Management).

Agent

Agent ESET Management to kluczowa część programu ESET PROTECT. Komputery klienckie nie komunikują się bezpośrednio z serwerem. 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 produktu końcowego ESET działającego na komputerze klienckim.

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. Jeśli zdecydujesz się, by serwer sieciowy był dostępny przez Internet, możesz używać programu ESET PROTECT z praktycznie dowolnego miejsca, za pomocą dowolnego urządzenia.

Serwer proxy Apache HTTP

Apache HTTP Proxy to usługa, z której można korzystać w połączeniu z programem ESET PROTECT 9 w celu dystrybuowania pakietów instalacyjnych i aktualizacji na komputerach klienckich. Komponent ten działa jak przezroczysty serwer proxy, co oznacza, że zapisuje w pamięci podręcznej pliki, które zostały już pobrane, w celu ograniczenia do minimum wykorzystania połączenia z Internetem w ramach sieci.

Korzystanie z serwera proxy Apache HTTP wiąże się z następującymi korzyściami:

- Pobieranie i buforowanie następujących elementów:
  - Aktualizacje silnika detekcji
  - Zadania aktywacji — komunikacja z serwerami aktywacji i buforowanie żądań licencji
  - Dane repozytorium ESET PROTECT
  - Aktualizacje komponentów produktu — serwer proxy Apache pozwala na buforowanie i dystrybuowanie tych elementów wśród klientów będących punktami końcowymi w sieci.
- Ograniczenie natężenia ruchu internetowego w danej sieci.

Moduł Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) przeszukuje sieć w poszukiwaniu komputerów niezarejestrowanych w ESET PROTECT. Ten komponent umożliwia lokalizowanie nowych komputerów i ich automatyczne dodawanie w ramach rozwiązania ESET PROTECT.

> Zlokalizowanie nowych komputerów w sieci przy użyciu narzędzia Rogue Detection Sensor może potrwać do 24 godzin.

Nowo wykryte komputery są wyszczególnione we wstępnie zdefiniowanym raporcie, co ułatwia wdrażanie agenta ESET Management, przypisywanie ich do określonych grup statycznych oraz zarządzanie nimi za pomocą zadań i zasad.

Wymagania systemowe

Przed przystąpieniem do instalacji produktu ESET PROTECT należy sprawdzić, czy sprzęt, system operacyjny, sieć oraz oprogramowanie spełniają wymagania wstępne.

Sprzęt

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
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

System operacyjny

W poniższej tabeli wymieniono systemy operacyjne Windows obsługiwane przez poszczególne komponenty programu ESET PROTECT. Zobacz też pełną listę obsługiwanych systemów operacyjnych.

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		✔	✔	
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
Windows Server 2012 x64	✔	✔	✔	✔
Windows Server 2012 CORE x64	✔	✔	✔	✔

System operacyjny	Serwer	Agent	RD Sensor	MDM
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.

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), aby umożliwić komunikację z siecią i Internetem.

Komputery zarządzane przy użyciu serwera 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.

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.

Oprogramowanie

Aby można było zainstalować serwer ESET PROTECT w systemie Windows, muszą zostać spełnione następujące wymagania wstępne:

- Wymagana jest ważna licencja.

- Konieczne jest zainstalowanie oprogramowania Microsoft .NET Framework 4. Można to zrobić przy użyciu **Kreatora dodawania ról i funkcji**.

- Konsola internetowa ESET PROTECT wymaga oprogramowania Java/OpenJDK (wersja 64-bitowa).

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.

- Program ESET PROTECT obsługuje dwa typy serwerów baz danych: MS SQL i MySQL. Zalecamy użycie serwera Microsoft SQL Server Express 2019 dostępnego w instalatorze kompleksowym ESET PROTECT dla systemu Windows. Jeśli masz już serwer bazy danych i chcesz go używać na potrzeby ESET PROTECT, upewnij się, że spełnia wymagania dotyczące bazy danych.

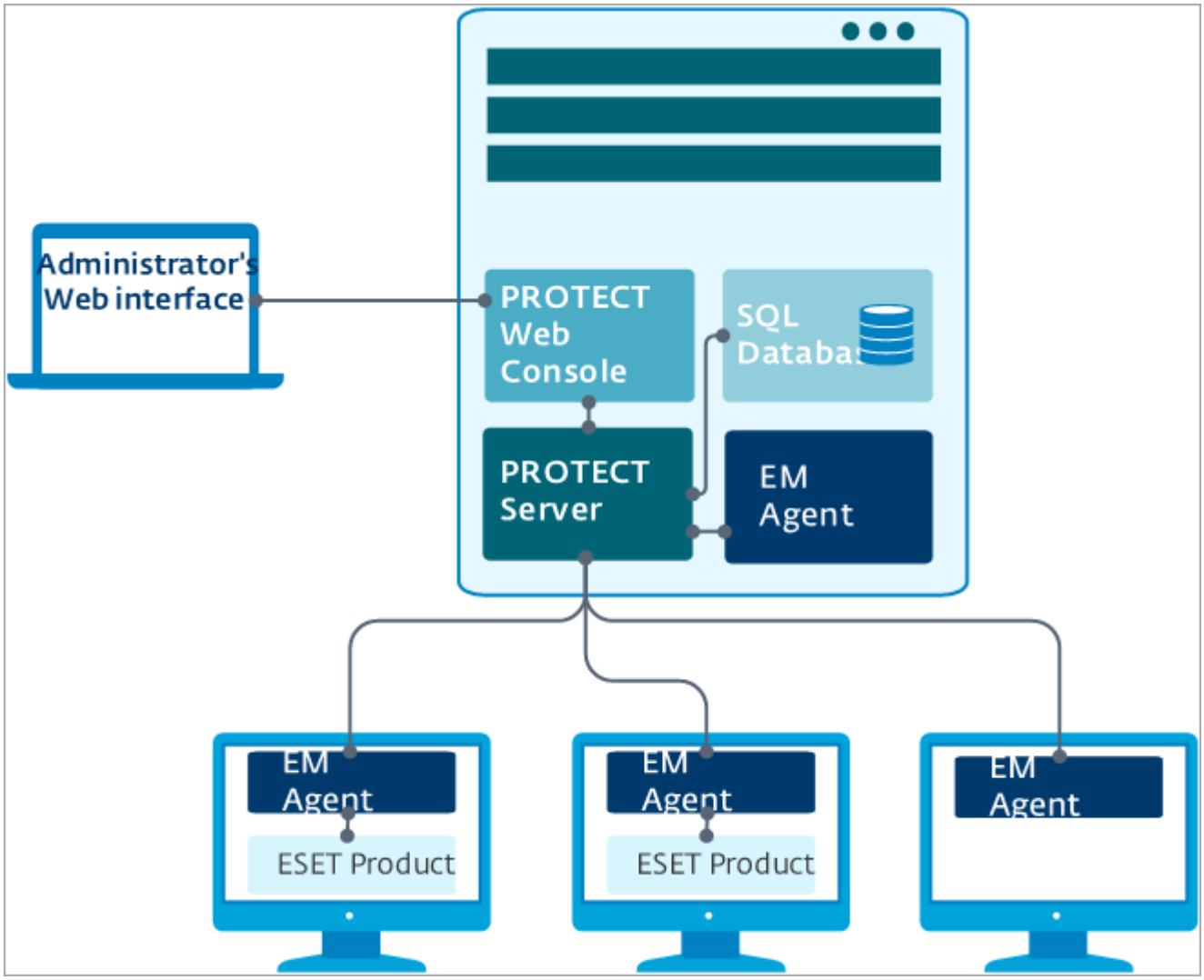
- Konsola internetowa ESET PROTECT działa w następujących przeglądarkach internetowych:
  - Mozilla Firefox
  - Microsoft Edge
  - Google Chrome
  - Safari
  - Opera

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.

Instalowanie serwera ESET PROTECT

Struktura komponentów serwera ESET PROTECT

Do zarządzania niewielkimi i średnimi sieciami (liczącymi nie więcej niż 1000 klientów) wystarczającym rozwiązaniem jest zwykle jeden komputer z zainstalowanym serwerem ESET PROTECT oraz wszystkimi komponentami serwera (dostarczonym serwerem internetowym, bazą danych itd.). Można postrzegać to rozwiązanie jako pojedynczy serwer lub samodzielną instalację. Wszystkie zarządzane klienty łączą się bezpośrednio z serwerem ESET PROTECT przy użyciu agenta ESET Management. Administrator może łączyć się z konsolą internetową ESET PROTECT przy użyciu przeglądarki internetowej z dowolnego komputera w sieci lub może uruchamiać konsolę internetową bezpośrednio na serwerze ESET PROTECT.



Instalacja

Instalatory serwera ESET PROTECT są dostępne w różnych formatach na potrzeby różnych metod instalacji:

- W przypadku niewielkich wdrożeń w systemie Windows firma ESET zaleca zastosowanie instalatora kompleksowego.

- Firma ESET zaleca wdrożenie wstępnie skonfigurowanego urządzenia wirtualnego ESET PROTECT (działającego na CentOS Linux), jeśli używasz hiperwizora. Jego wdrożenie jest szybkie i prostsze niż instalacja w systemie Windows.

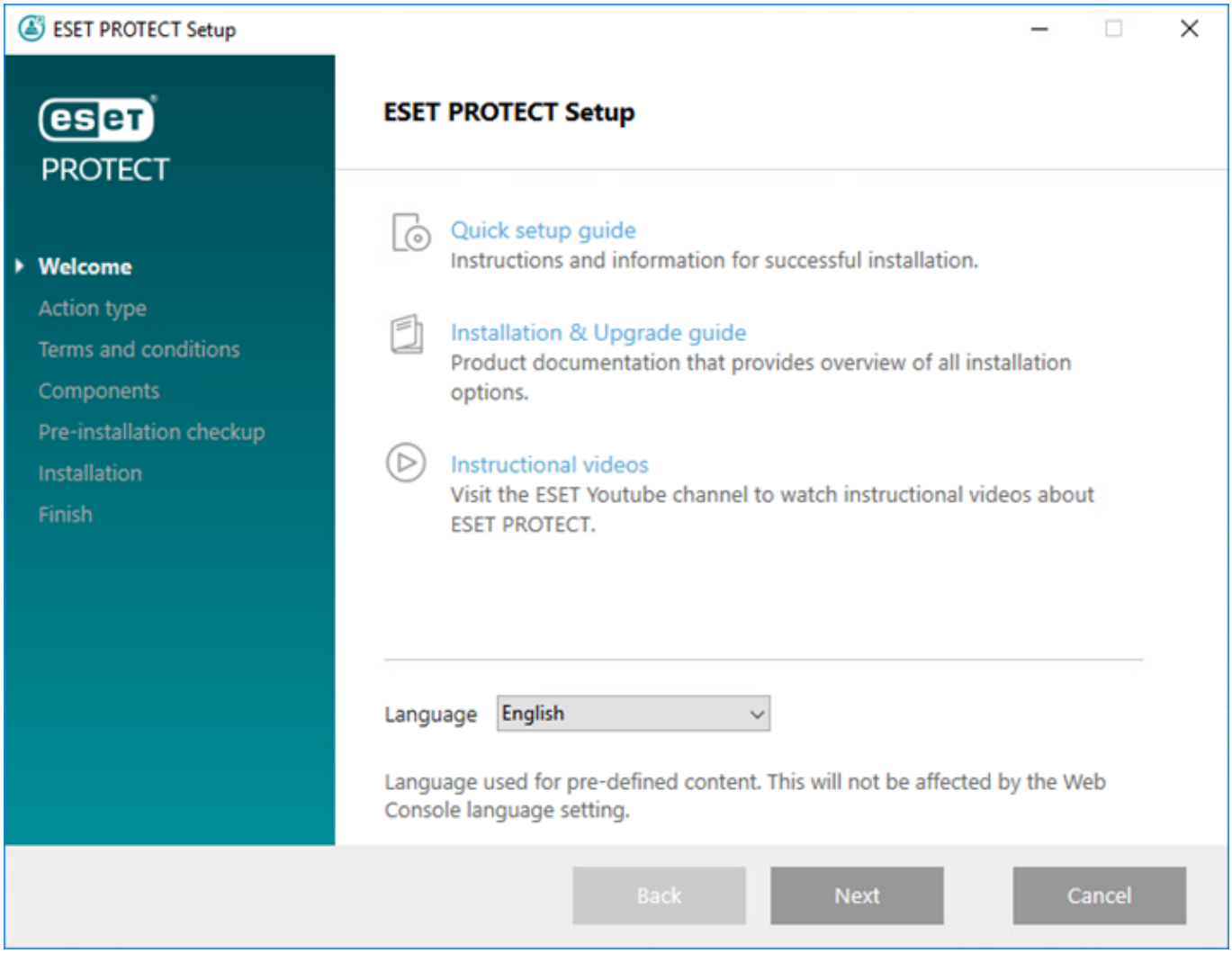
W przypadku uaktualniania z poprzedniej wersji ESET PROTECT lub ESMC 7.x należy postępować zgodnie z tymi instrukcjami.

Instalacja kompleksowa serwera ESET PROTECT

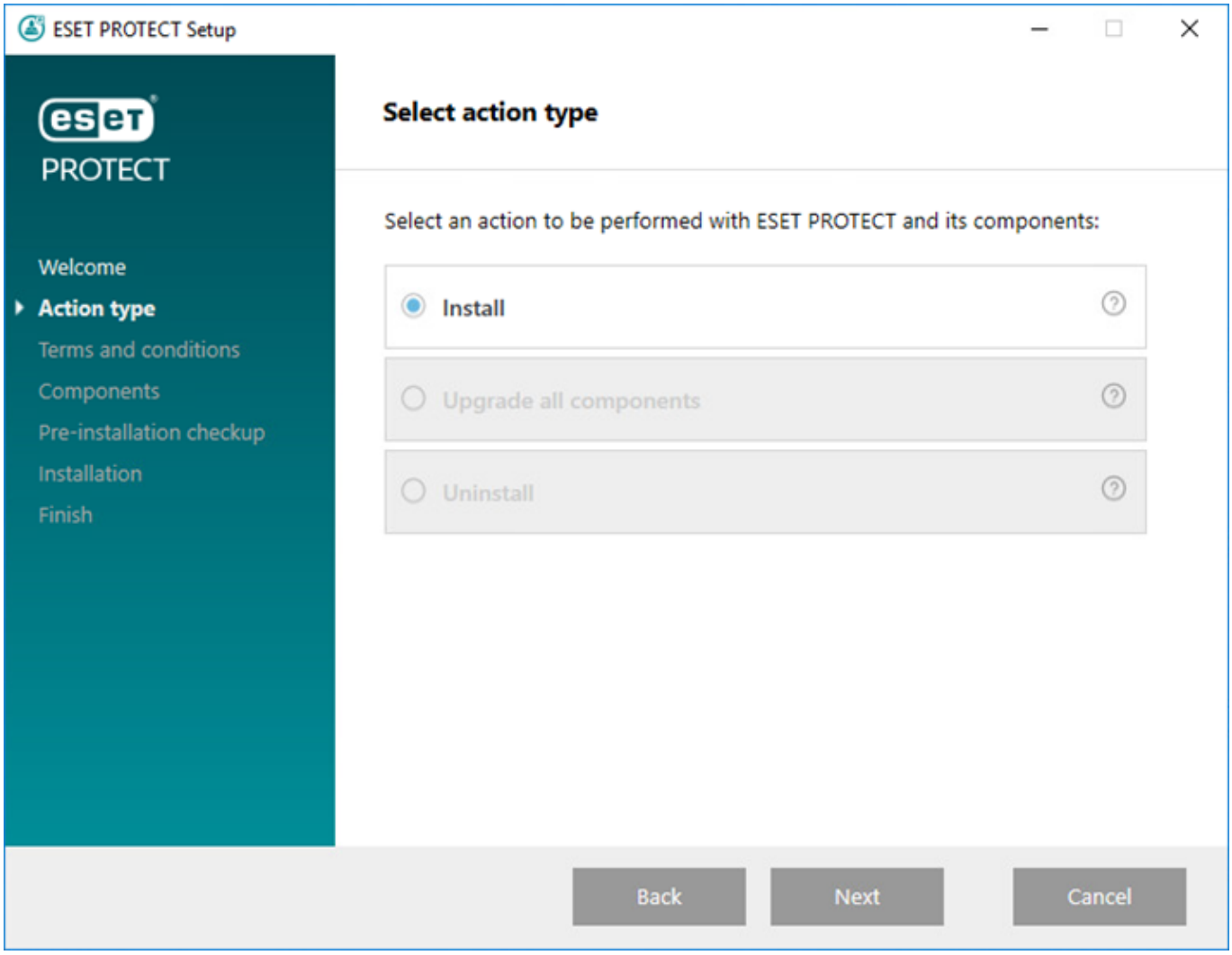
- Inną alternatywą jest wdrożenie wstępnie skonfigurowanego urządzenia wirtualnego ESET PROTECT (jeśli używasz funkcji hypervisor).
- W przypadku uaktualniania z poprzedniej wersji ESET PROTECT lub ESMC 7.x należy postępować zgodnie z tymi instrukcjami.

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.

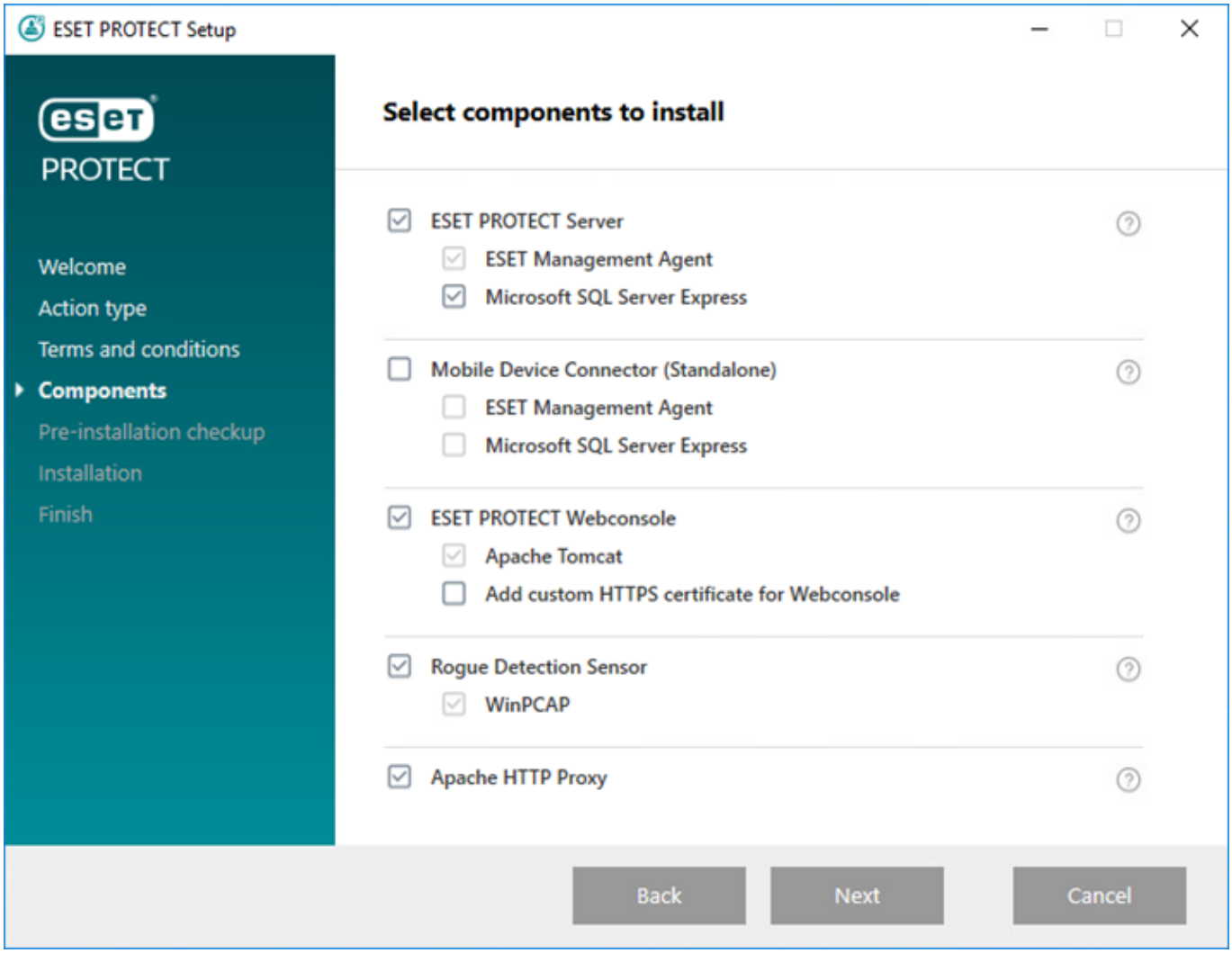
- Więcej informacji można znaleźć w sekcjach Co to jest serwer proxy Apache HTTP? oraz Różnice pomiędzy serwerem proxy Apache HTTP, narzędziem Mirror Tool a połączeniem bezpośrednim.

- 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:

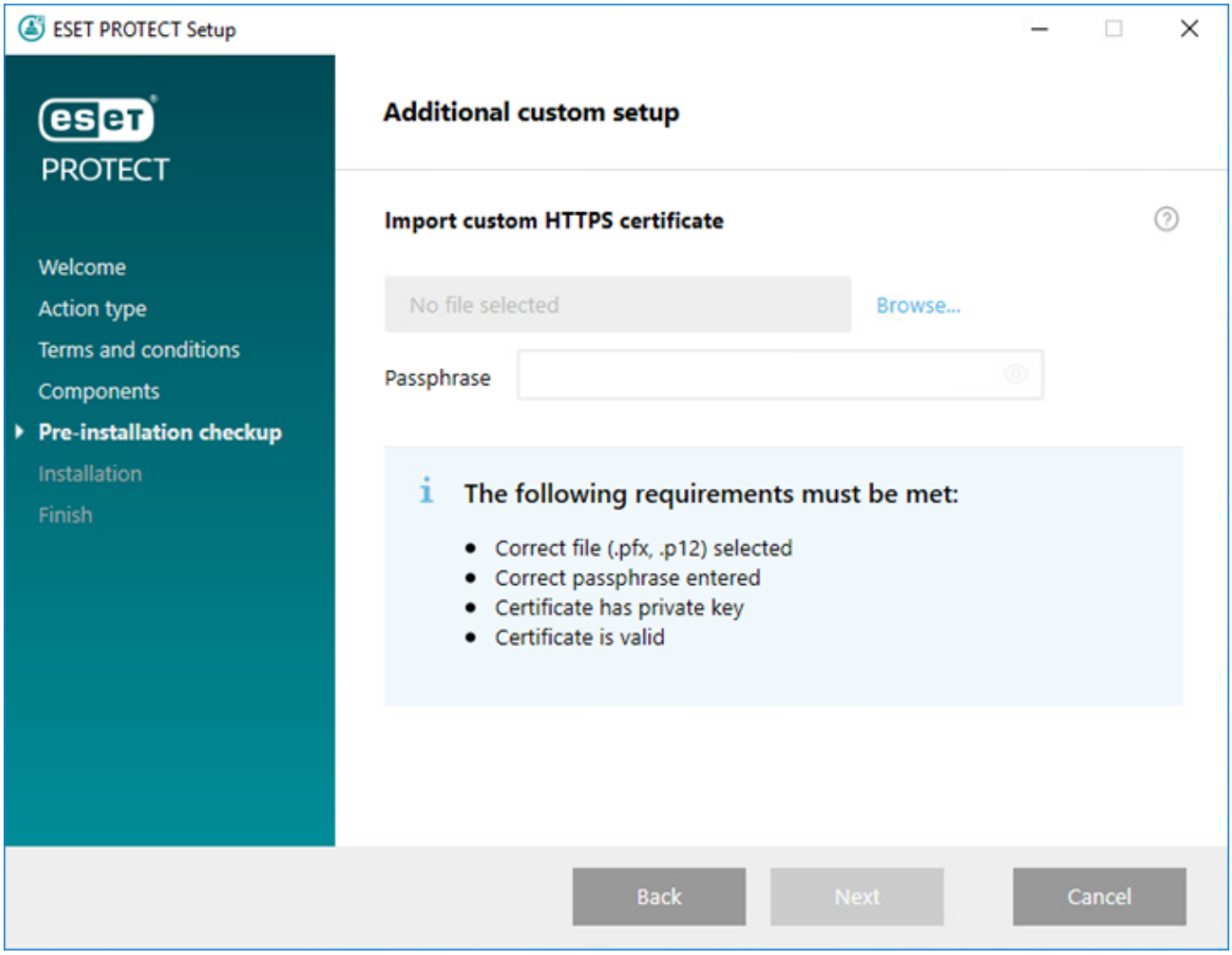
  - ESET Endpoint for Windows
  - ESET Endpoint for macOS (OS X) and Linux
  - ESET Management Agent
  - ESET File Security for Windows Server (6+)
  - ESET Server Security dla Windows (8+)

- 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.



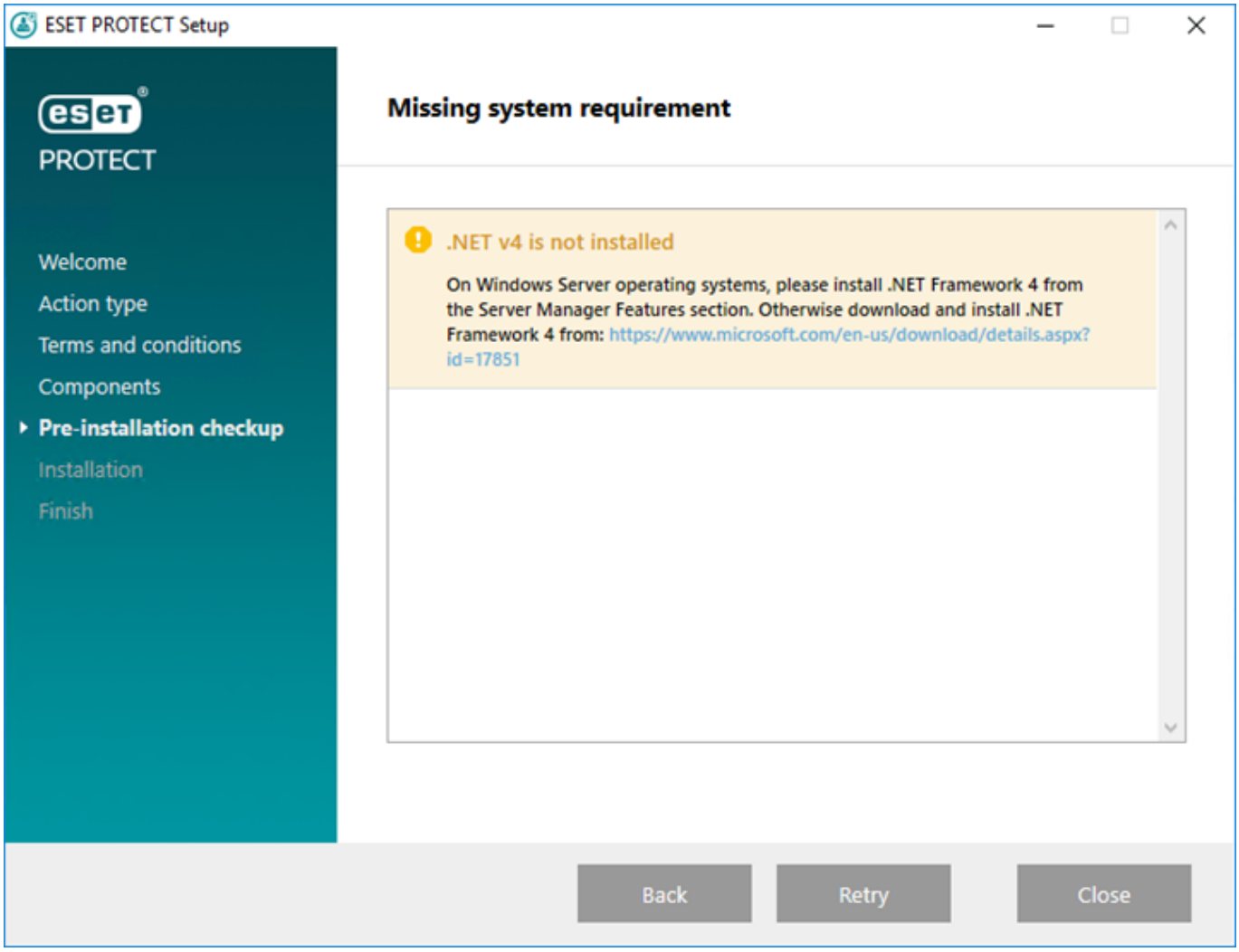
5. W przypadku wybrania opcji **Dodaj niestandardowy certyfikat HTTPS dla konsoli internetowej** kliknij **Przeglądaj** i wybierz ważny certyfikat (plik *.pfx* lub .p12 file), a w polu **Hasło** wpisz hasło do niego (lub pozostaw to pole puste, jeśli nie ustawiono hasła). Instalator zainstaluje certyfikat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



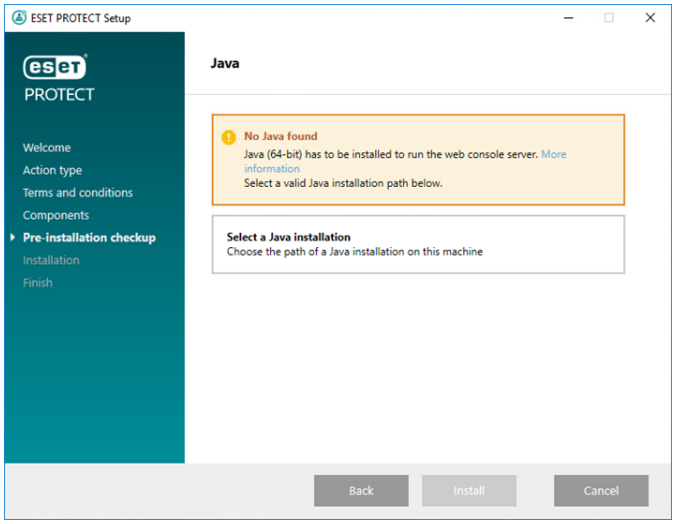
6. Jeśli podczas sprawdzania wymagań wstępnych wystąpią błędy, rozwiąż je. Sprawdź, czy system spełnia wszystkie wymagania wstępne.

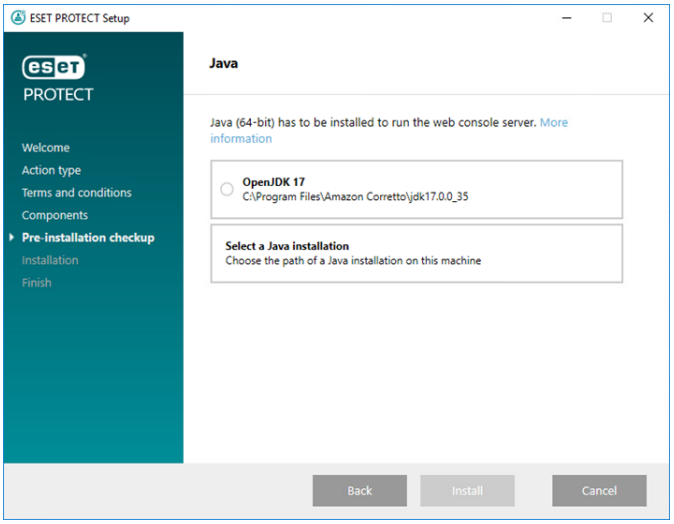
Nie zainstalowano platformy .NET 4

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.

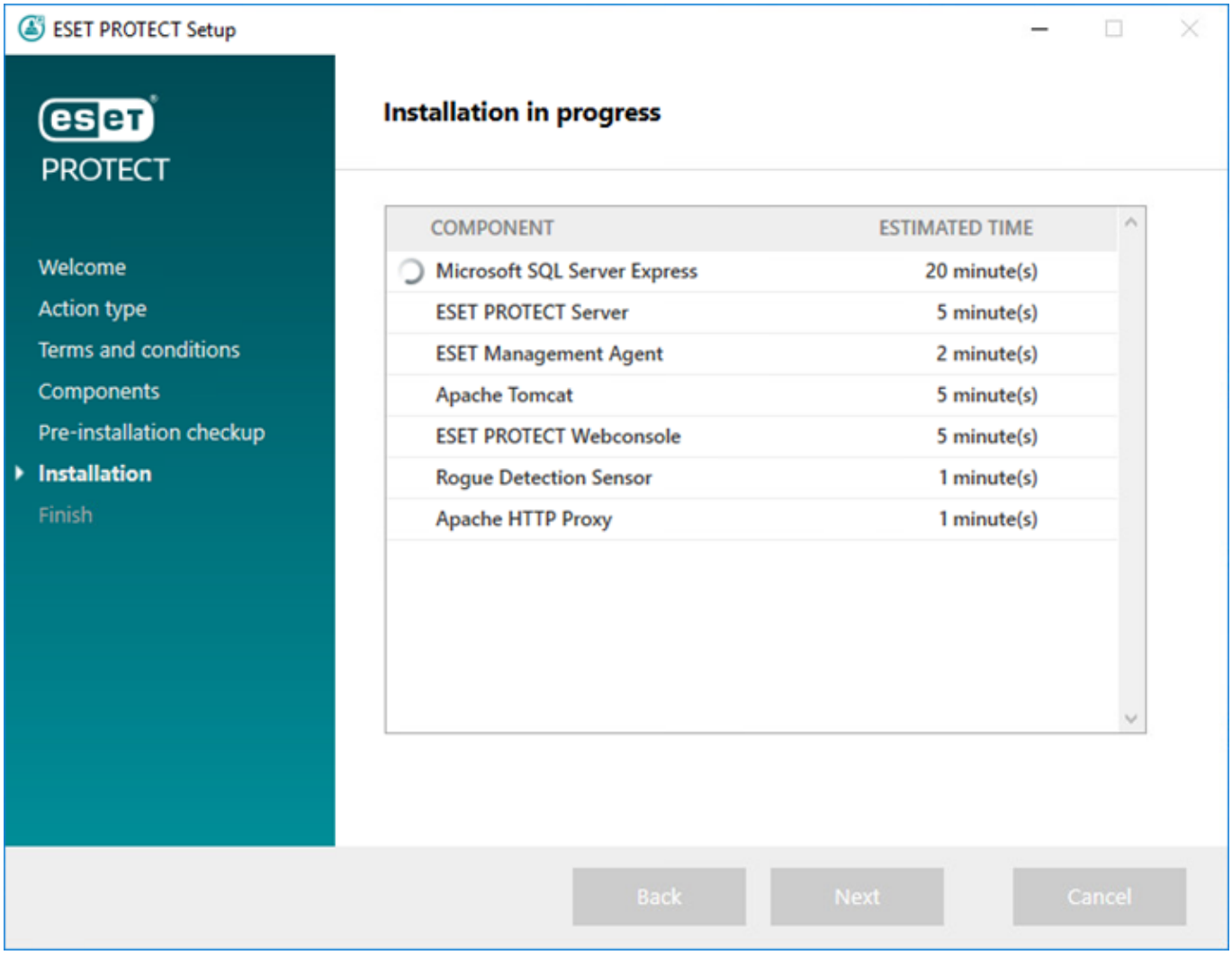
- Do zainstalowania programu ESET PROTECT i wszystkich jego komponentów niezbędne jest co najmniej 4400 MB wolnego miejsca na dysku.

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.

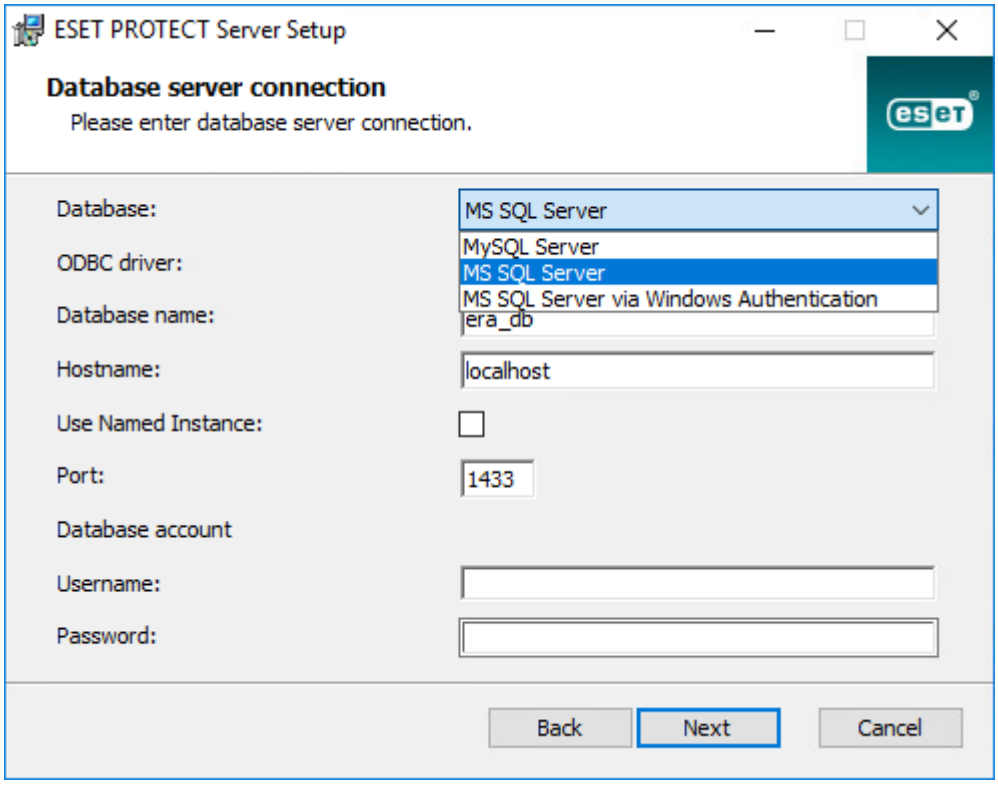
7. Jeśli po ukończeniu sprawdzania wymagań wstępnych okaże się, że środowisko spełnia wszystkie wymagania, rozpocznie się instalacja. Pamiętaj, że instalacja może potrwać ponad godzinę w zależności od konfiguracji systemu oraz sieci.

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

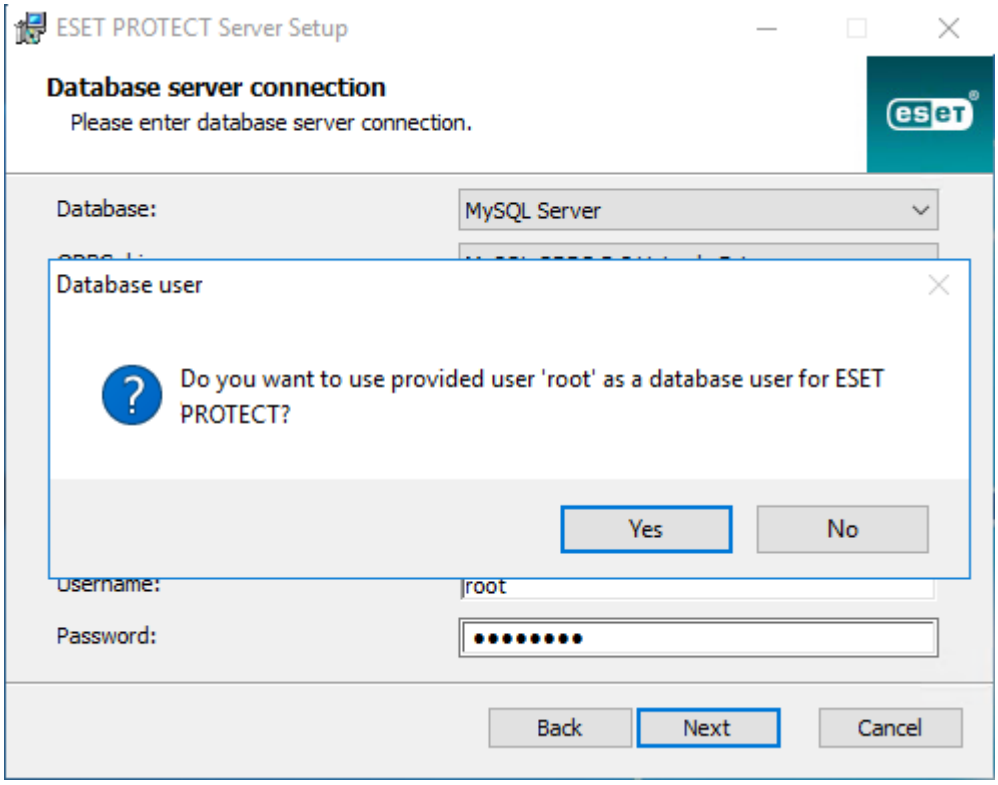


W odpowiednich polach wpisz **nazwę bazy danych**, **nazwę hosta** i **numer portu** (informacje te można znaleźć w narzędziu Microsoft SQL Server Configuration Manager) oraz **konto bazy danych** (**nazwę użytkownika** i **hasło**), a następnie kliknij przycisk **Dalej**. Instalator zweryfikuje połączenie 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**.

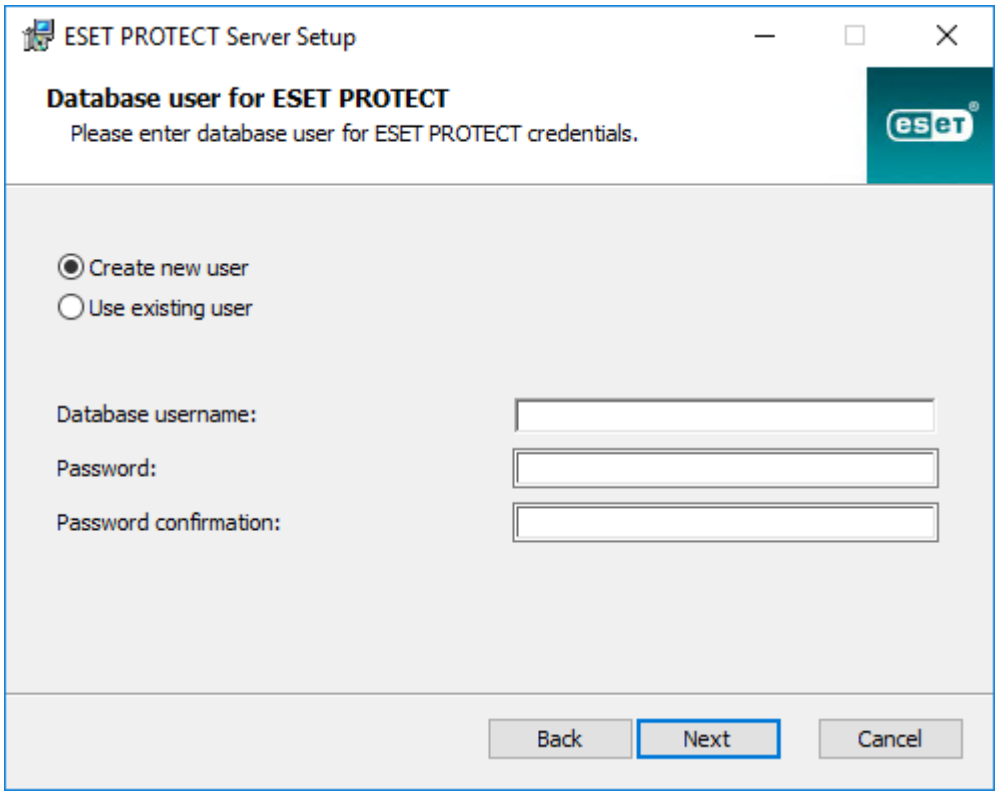
Użyj nazwanej instancji — w przypadku używania bazy danych MS SQL można też zaznaczyć pole wyboru **Użyj nazwanej instancji**, jeśli chcesz korzystać z własnej, niestandardowej instancji bazy danych. Niestandardową instancję bazy danych można ustawić w polu **Nazwa hosta** w postaci *NAZWA_HOSTA**INSTANCJA_BD* (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).

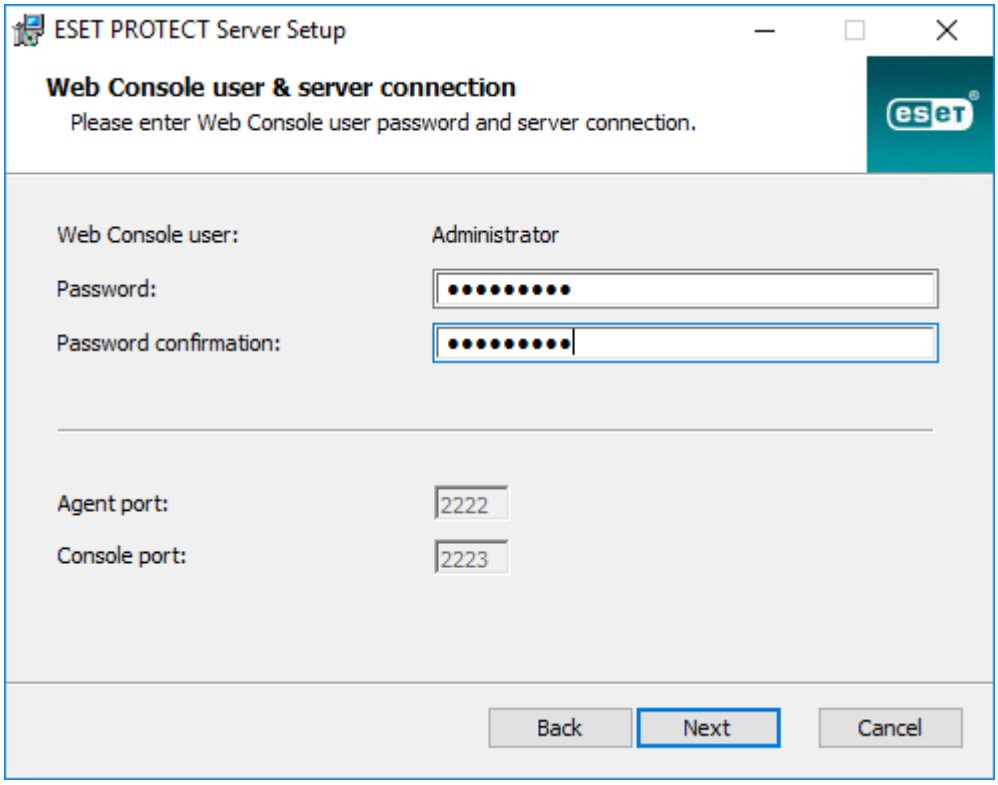
Jeśli w poprzednim oknie wprowadzono **konto SA** lub **konto użytkownika root**, kliknij pozycję **Tak**, aby kontynuować przy użyciu konta SA / konta użytkownika root jako użytkownika bazy danych programu ESET PROTECT.



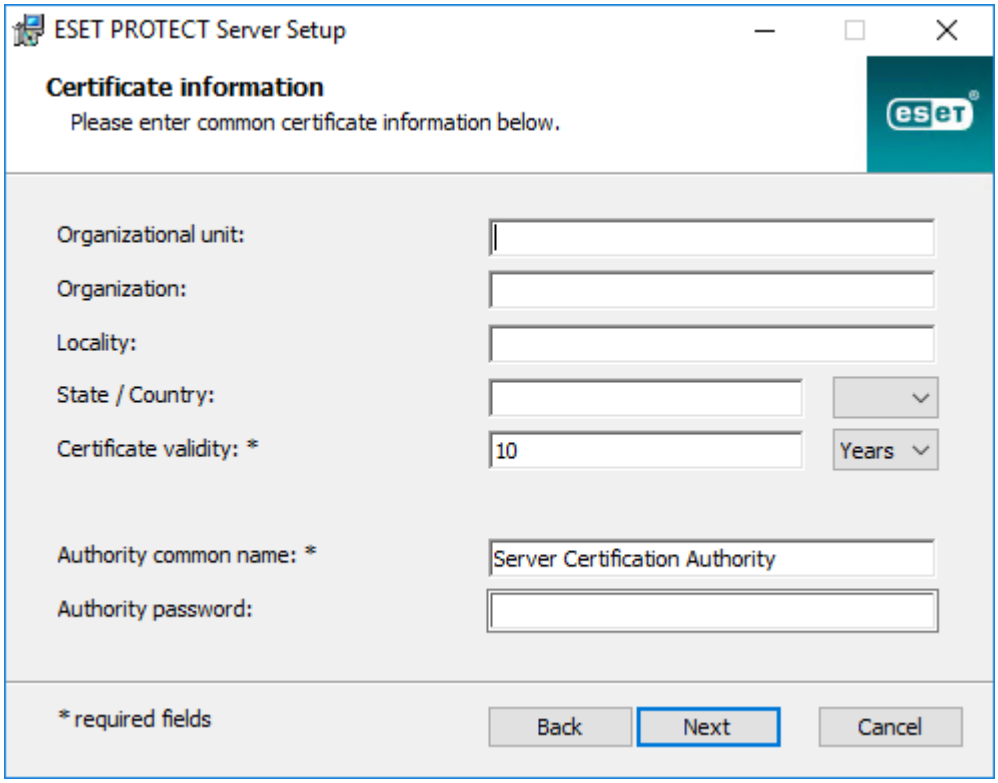
W przypadku kliknięcia pozycji **Nie** musisz wybrać pozycję **Utwórz nowego użytkownika** (jeśli nie został jeszcze utworzony) lub **Użyj istniejącego użytkownika** (w przypadku dedykowanego konta użytkownika bazy danych).



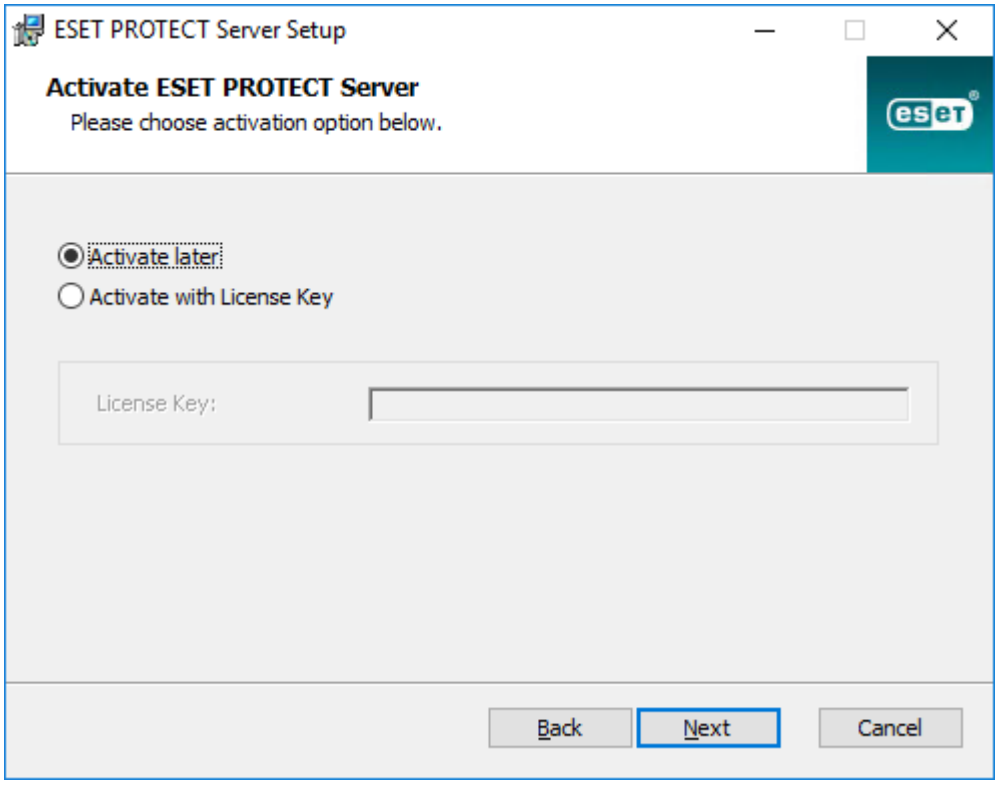
9. Instalator wyświetli monit o wprowadzenie hasła do konta administratora konsoli internetowej. To hasło jest ważne, ponieważ będzie służyć do logowania się w konsoli internetowej ESET PROTECT. Kliknij przycisk **Dalej**.



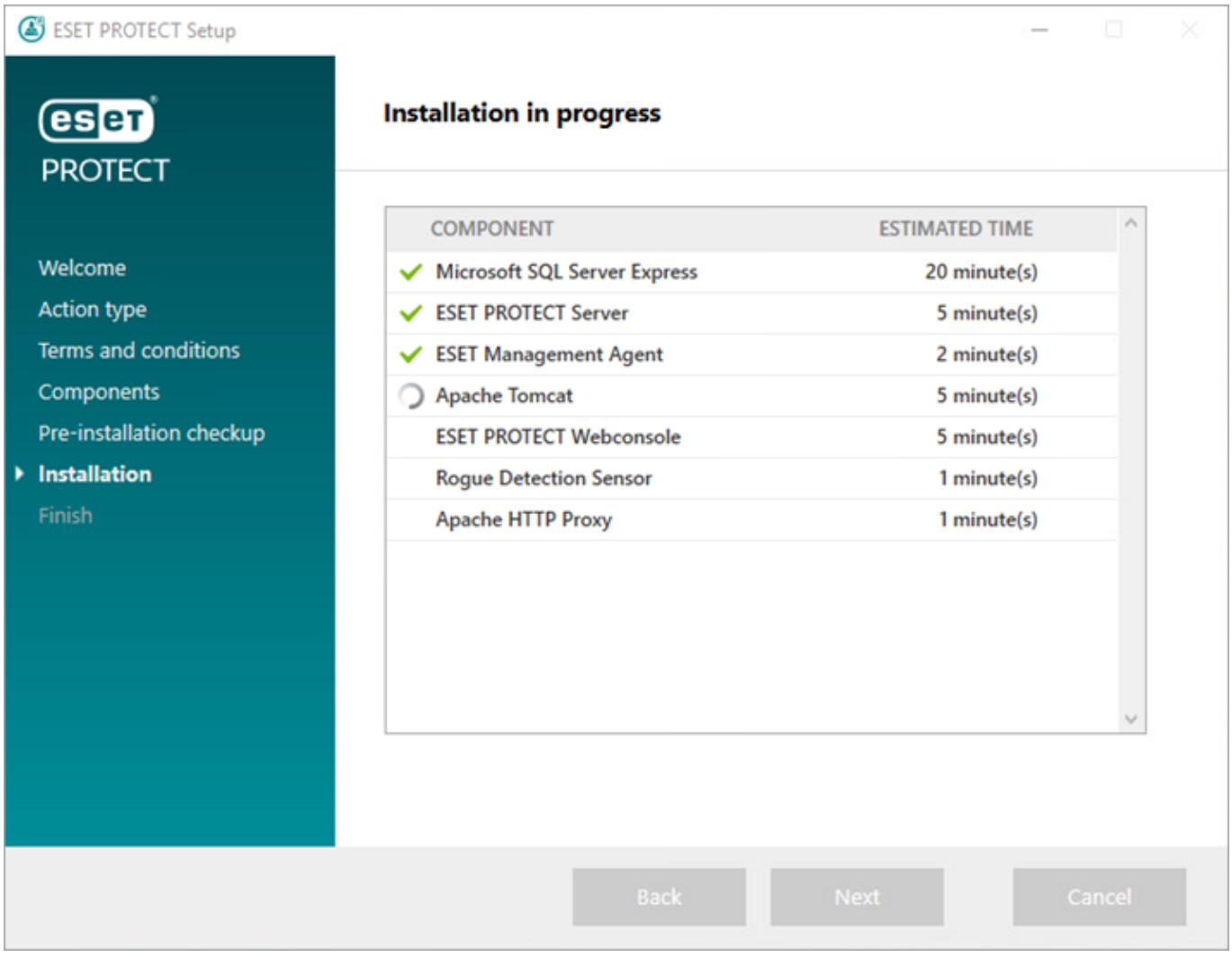
10. Możesz pozostawić puste pola lub wprowadzić informacje o firmie, które będą widoczne w szczegółach certyfikatów agenta ESET Management i serwera ESET PROTECT. Jeśli wprowadzisz hasło w polu **Hasło urzędu**, zapamiętaj je. Kliknij przycisk **Dalej**.



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).



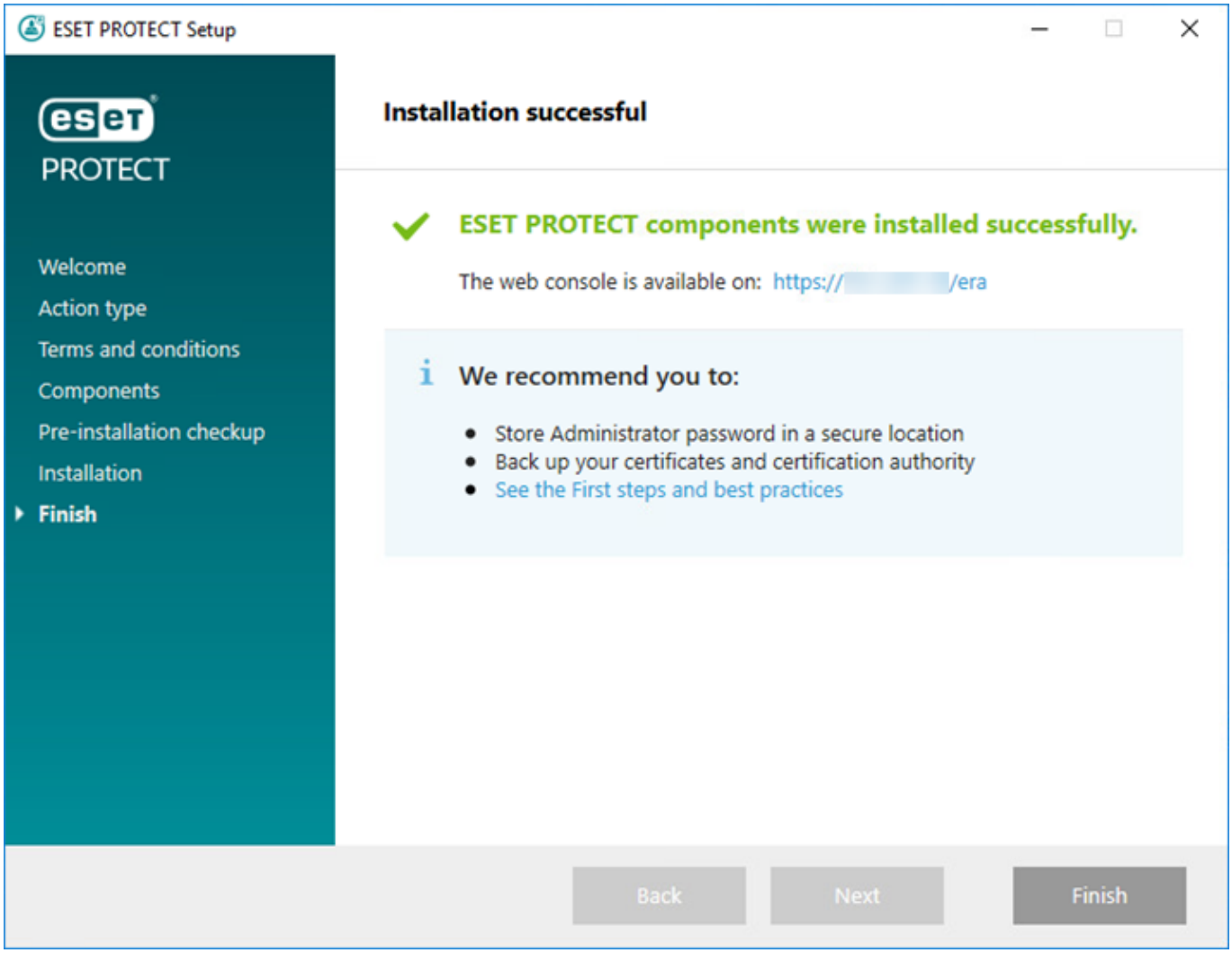
12. Zobaczysz postęp instalacji.



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.

Kroki po instalacji

Po zainstalowaniu ESET PROTECT można rozpocząć konfigurację.

Pierwsze kroki po wdrożeniu serwera ESET PROTECT

1.Połącz się z konsolą internetową ESET PROTECT.

2.Przeczytaj instrukcje w Przewodniku ESET PROTECT.

3.Dodanie licencji.

4.Wdróż agenta ESET Management i produkty firmy ESET do obsługi punktów końcowych na komputerach w swojej sieci.

Przegląd stanu może pomóc w początkowej konfiguracji programu ESET PROTECT.

Po zainstalowaniu na serwerze oprogramowania serwerowego ESET PROTECT oraz zainstalowaniu na klientach rozwiązań firmy ESET do obsługi punktów końcowych można rozpocząć zarządzanie siecią. Więcej informacji na temat zarządzania produktami do obsługi punktów końcowych firmy ESET można znaleźć w Przewodniku dla administratorów.

Dodatkowe zalecane kroki

- Powiadomienia i raporty umożliwiają monitorowanie stanu komputerów klienckich w danym środowisku.

- Konfigurowanie połączenia z serwerem SMTP. Ta konfiguracja jest opcjonalna, jeśli chcesz otrzymywać powiadomienia lub raporty pocztą e-mail. Można skonfigurować serwer ESET PROTECT tak, aby wysyłał powiadomienia do serwera programu Syslog.

- Utwórz nowego użytkownika konsoli internetowej ESET PROTECT.

Wdrażanie agenta ESET Management i produktów ESET do obsługi punktów końcowych

Po pomyślnym zainstalowaniu programu ESET PROTECT na komputerach klienckich w sieci należy wdrożyć agenta ESET Management i produkty firmy ESET do obsługi punktów końcowych.

Wdrożenie obejmuje następujące etapy:

1. Utworzenie pakietu wdrożeniowego

2. Zainstalowanie pakietu wdrożeniowego

Zobacz też inne opcje wdrożenia. W przypadku większych sieci zalecamy skorzystanie z narzędzia ESET Remote Deployment Tool.

Tworzenie pakietu wdrożeniowego

Instalator agenta i produktu zabezpieczającego ESET w systemie Windows można utworzyć na kilka sposobów:

- **Szybkie łącza** > **Wdrażanie agenta** > **Windows**
- **Instalatory** > **Utwórz instalator**

Kliknij **Windows** > **Pobierz instalator lub użyj narzędzia ESET Remote Deployment Tool**

Pakiet instalatora to plik *.exe*, który nadaje się do użytku wyłącznie w systemach operacyjnych Windows.

1. **Dystrybucja** – Wybierz **Pobierz instalator lub użyj narzędzia ESET Remote Deployment Tool**

Jeśli wybrano inny typ instalatora, postępuj zgodnie z odpowiednimi instrukcjami:
- Najpierw wdróż agenta (instalator skryptu agenta)
- Użyj GPO lub SCCM na potrzeby wdrażania

2. **Komponenty** — należy wybrać jedną z następujących opcji przy użyciu pól wyboru:

- **Management Agent** — jeśli nie wybierzesz innych elementów **pakietu**, instalator będzie zawierał tylko agenta ESET Management. Wybierz tę opcję, jeśli chcesz zainstalować produkt zabezpieczający ESET na komputerze klienckim później, lub jeśli komputer kliencki już ma zainstalowany produkt zabezpieczający ESET.
- **Produkt zabezpieczający** — dołącz produkt zabezpieczający firmy ESET do agenta ESET Management. Wybierz tę opcję, jeśli komputer kliencki nie ma zainstalowanego żadnego produktu zabezpieczającego ESET i chcesz zainstalować go wraz z agentem ESET Management.
- **Szyfrowanie całego dysku** — opcja szyfrowania jest widoczna tylko w przypadku aktywnej licencji ESET Full Disk Encryption.
- **Łącznik ESET Inspect** — dołączanie łącznika ESET Inspect do instalatora.

3. Zaznacz pole wyboru **Weź udział w programie udoskonalania produktu**, aby wysyłać anonimowe dane telemetryczne i raport o awariach do firmy ESET (wersja i typ systemu operacyjnego, wersja produktu ESET i inne informacje specyficzne dla produktu).

4. **Grupa nadrzędna (opcjonalnie)** — wybierz grupę nadrzędną, w której konsola internetowa ESET PROTECT umieści komputer po zainstalowaniu agenta. Możesz wybrać istniejącą lub utworzyć nową grupę statyczną, do której urządzenie zostanie przypisane po wdrożeniu instalatora. Wybranie grupy nadrzędnej spowoduje dodanie do instalatora wszystkich polityk zastosowanych do grupy.

5. **Nazwa hosta serwera (opcjonalnie)** — wpisz nazwę hosta lub adres IP serwera produktu ESET PROTECT. W razie potrzeby możesz określić numeru **Portu** (domyślnie jest to 2222).

6. **Certyfikat równorzędny**:

- **ESET PROTECT certyfikat** — certyfikat równorzędny dla instalacji agenta i urzędu certyfikacji ESET PROTECT są wybierane automatycznie. Aby użyć innego certyfikatu, kliknij **Opis certyfikatu ESET PROTECT**, aby wybrać z menu rozwijanego dostępne certyfikaty.

- **Certyfikat niestandardowy** — jeśli do uwierzytelniania używasz certyfikatu niestandardowego, kliknij **Niestandardowy certyfikat** > **Wybierz** i prześlij certyfikat .pfx i wybierz go podczas instalacji agenta. Aby uzyskać więcej informacji, kliknij Certyfikaty.

Hasło certyfikatu — w razie potrzeby wpisz hasło certyfikatu — jeśli hasło zostało określone podczas instalacji serwera ESET PROTECT (w kroku, w którym utworzono urząd certyfikacji) lub jeśli używasz certyfikatu niestandardowego z hasłem. W przeciwnym razie pozostaw pole **Hasło do certyfikatu** puste.

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

Warto pamiętać, że **hasło do certyfikatu** można wyodrębnić, ponieważ jest ono osadzone w instalatorze.

7. Dostosuj więcej ustawień

- Wpisz **nazwę instalatora** i **opis** (opcjonalnie).

- Kliknij opcję **Wybierz tagi**, aby przypisać tagi.

- **Konfiguracja wstępna (opcjonalnie)** – Użyj tej opcji, aby zastosować zasady konfiguracji do agenta ESET Management. Kliknij opcję **Wybierz** w obszarze **Konfiguracja agenta** i wybierz pozycję z listy dostępnych polityk. Jeśli żadna ze wstępnie zdefiniowanych polityk nie jest odpowiednia, możesz utworzyć nową politykę lub dostosować istniejące.

- Jeśli używasz serwera proxy HTTP, zaznacz pole wyboru **Włącz ustawienia serwera proxy HTTP** i określ ustawienia serwera proxy (**Host**, **Port**, **Nazwa użytkownika** i **Hasło**) w celu pobrania instalatora poprzez serwer proxy i ustawienia połączenia agenta ESET Management z serwerem proxy, aby włączyć przekazywanie komunikacji między agentem ESET Management a serwerem ESET PROTECT. Pole **Host** to adres urządzenia, na którym działa serwer proxy HTTP. Serwer proxy HTTP wykorzystuje domyślnie port 3128. W razie potrzeby można ustawić inny port. Ten sam port należy ustawić również w konfiguracji serwera proxy HTTP.

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.

Włącz **Użyj połączenia bezpośredniego, gdy serwer proxy HTTP jest niedostępny**, jeśli chcesz umożliwić tę opcję awaryjną.

8. Kliknij przycisk **Zakończ** lub **Konfiguracja produktu**.

9. Program zabezpieczający

a. Kliknij wstępnie zaznaczony produkt zabezpieczający ESET i zmień jego szczegóły:

oWybierz inny zgodny produkt zabezpieczający firmy ESET.

o Wybierz język z menu rozwijanego **Język**.

oZaznacz pole wyboru **Zaawansowane**. Domyślnie wstępnie zaznaczona jest najnowsza wersja produktu (zalecane). Możesz wybrać wcześniejszą wersję.

> Jeśli nie widzisz żadnych plików instalacyjnych produktu, upewnij się, że repozytorium zostało ustawione na **AUTOSELECT**. Aby uzyskać więcej informacji, zapoznaj się z sekcją **Ustawienia zaawansowane** w rozdziale Ustawienia.

b. Zaznacz pole wyboru obok ustawienia, aby je włączyć dla instalatora:

oWłącz system informacji zwrotnych ESET LiveGrid® (zalecane)

oWłącz wykrywanie potencjalnie niepożądanych aplikacji — więcej informacji zawiera artykuł w bazie wiedzy.

o**Zezwalaj na zmianę ustawień ochrony podczas instalacji** — zalecamy, aby nie zaznaczać tego pola wyboru.

c.Zaznacz pole wyboru **Akceptuję warunki Umowy licencyjnej użytkownika końcowego aplikacji i potwierdzam politykę prywatności**. Więcej informacji umowy licencyjnej użytkownika końcowego (EULA), Warunkach korzystania i Polityce prywatności dotyczących produktów firmy ESET.

d.**Dostosuj więcej ustawień**:

o**Licencja** — wybierz licencję z listy dostępnych licencji odpowiednich dla wybranego instalatora produktu zabezpieczającego. Licencja aktywuje produkt zabezpieczający ESET podczas instalacji. Możesz dodać licencję, korzystając z jednej z metod opisanych w sekcji Zarządzanie licencjami. Dodawanie/usuwanie licencji jest ograniczone do Administratora, którego grupą domową jest grupa **Wszystkie** i który ma uprawnienie **Zapis** na licencjach.

o**Konfiguracja** Można opcjonalnie wybrać **politykę**, która zostanie zastosowana do produktu zabezpieczającego firmy ESET podczas jego instalacji.

o**Uruchom narzędzie ESET AV Remover** — zaznacz pole wyboru, aby odinstalować lub całkowicie usunąć inne oprogramowanie antywirusowe na urządzeniu docelowym.

Jeśli w kroku 2 wybrano Full Disk Encryption lub łącznik ESET Inspect, można również zmienić ich ustawienia.

Pełne szyfrowanie dysku

a.Kliknij wstępnie wybrany **ESET Full Disk Encryption** i zmień jego szczegóły:

o Wybierz język z menu rozwijanego **Język**.

oZaznacz pole wyboru **Zaawansowane**. Domyślnie wstępnie zaznaczona jest najnowsza wersja produktu

(zalecane). Możesz wybrać wcześniejszą wersję.

b.Zaznacz pole wyboru **Akceptuję warunki Umowy licencyjnej użytkownika końcowego aplikacji i potwierdzam politykę prywatności**. Więcej informacji umowy licencyjnej użytkownika końcowego (EULA), Warunkach korzystania i Polityce prywatności dotyczących produktów firmy ESET.

c.**Konfiguracja** — wybierz zasadę, która zostanie zastosowana do ESET Full Disk Encryption podczas instalacji.

d.**Dostosuj więcej ustawień**:

o**Licencja** — wybierz licencję z listy dostępnych licencji odpowiednich dla wybranego instalatora produktu zabezpieczającego. Licencja aktywuje produkt zabezpieczający ESET podczas instalacji. Możesz dodać licencję, korzystając z jednej z metod opisanych w sekcji Zarządzanie licencjami. Dodawanie/usuwanie licencji jest ograniczone do Administratora, którego grupą domową jest grupa **Wszystkie** i który ma uprawnienie **Zapis** na licencjach.

ESET Inspect Connector

Wymagania dotyczące łącznika ESET Inspect:
- Aby aktywować łącznik ESET Inspect, musisz mieć licencję ESET Inspect.
- Zgodny produkt zabezpieczający firmy ESET zainstalowany na zarządzanym komputerze.

a.Kliknij wstępnie wybrany **ESET Inspect łącznik** i zmień jego szczegóły:

o Wybierz język z menu rozwijanego **Język**.

oZaznacz pole wyboru **Zaawansowane**. Domyślnie wstępnie zaznaczona jest najnowsza wersja produktu (zalecane). Możesz wybrać wcześniejszą wersję.

b.Zaznacz pole wyboru **Akceptuję warunki Umowy licencyjnej użytkownika końcowego aplikacji i potwierdzam politykę prywatności**. Więcej informacji umowy licencyjnej użytkownika końcowego (EULA), Warunkach korzystania i Polityce prywatności dotyczących produktów firmy ESET.

c.**Dostosuj więcej ustawień**:

o**Licencja** — wybierz licencję z listy dostępnych licencji odpowiednich dla wybranego instalatora produktu zabezpieczającego. Licencja aktywuje produkt zabezpieczający ESET podczas instalacji. Możesz dodać licencję, korzystając z jednej z metod opisanych w sekcji Zarządzanie licencjami. Dodawanie/usuwanie licencji jest ograniczone do Administratora, którego grupą domową jest grupa **Wszystkie** i który ma uprawnienie **Zapis** na licencjach.

o**Konfiguracja** — kliknij przycisk **Wybierz**, aby wybrać istniejącą ESET Inspectpolitykę łącznika lub **Utwórz**, aby utworzyć nową ESET Inspect politykę łącznika. Instalator zastosuje ustawienia polityki podczas instalacji łącznika ESET Inspect.

oWpisz **nazwę hosta serwera ESET Inspect** i **port** połączenia wskazany podczas instalacji serwera ESET Inspect (portem domyślnym jest 8093).

oWybierz **urząd certyfikacji** dla połączenia z serwerem ESET Inspect.

10. Kliknij opcję **Zakończ**.

11. Pobierz wygenerowany pakiet instalatora kompleksowego. Wybierz wersję, którą chcesz wdrożyć:

- **32-bitowa** (na przykład *PROTECT_Installer_x86_en_US.exe*)
- **64-bitowa** (na przykład *PROTECT_Installer_x64_en_US.exe*)
- **ARM64** (na przykład *PROTECT_Installer_arm64.exe*) — nie można zainstalować wersji x86 ani x64 agenta lub produktu zabezpieczającego ESET Management na systemie Windows ARM64.

> Wszystkie dane pobrane z repozytorium (ESET Repository lub kopii dystrybucyjnej repozytorium niestandardowego) są podpisywane cyfrowo przez firmę ESET, a serwer ESET PROTECT weryfikuje skróty plików i podpisy PGP. Serwer ESET PROTECT generuje instalator kompleksowy lokalnie. Dlatego instalator kompleksowy nie jest podpisany cyfrowo, co może generować ostrzeżenie przeglądarki internetowej podczas pobierania instalatora lub ostrzeżenie systemu operacyjnego i uniemożliwić instalację w systemach, w których niepodpisane instalatory są blokowane.

12. Po utworzeniu i pobraniu pakietu instalatora kompleksowego są dostępne dwie opcje wdrożenia agenta ESET Management:

- Lokalnie na komputerze klienckim Uruchom plik pakietu instalacyjnego na komputerze klienckim. Program zainstaluje agenta ESET Management i produkt zabezpieczający firmy ESET na urządzeniu i połączy urządzenie z programem ESET PROTECT. Instalator ESET Endpoint Antivirus/Security utworzony w ESET PROTECT 8.1 i późniejsze obsługuje Windows 10 Enterprise pulpity wirtualne i tryb wielosesyjny Windows 10. Szczegółowe instrukcje zawiera kreator instalacji. Można uruchomić pakiet instalacyjny w trybie cichym, aby ukryć okno kreatora instalacji.
- Za pomocą narzędzia do wdrażania zdalnego firmy ESET umożliwiającego wdrożenie agentów ESET Management na wielu komputerach klienckich równocześnie.

Instalowanie pakietu wdrożeniowego

Możesz utworzyć ten pakiet instalatora w ESET PROTECT.

Pakiet instalatora instaluje Agenta ESET Management. Może on również instalować następujące składniki (jeśli zostały wybrane podczas tworzenia pakietu instalatora):

- Produkt zabezpieczający ESET (dla punktu końcowego lub serwera)
- ESET Full Disk Encryption
- ESET Inspect Connector

- Pakiet instalatora jest dostępny poprzez plik *.exe* i jest przeznaczony wyłącznie do systemu operacyjnego Windows.
- Jeśli instalator zostanie uruchomiony na komputerze klienckim, na którym jest już zainstalowany produkt zabezpieczający lub agent ESET Management firmy ESET, instalator uaktualni go do wersji z instalatora.
- Instalator trzeba uruchomić przy użyciu wbudowanego konta administratora lub konta administratora domeny (jeżeli wbudowane konto administratora zostało wyłączone). Inni użytkownicy, nawet jeśli należą do grupy Administratorzy, nie mają wystarczających uprawnień dostępu. Z tego powodu należy użyć wbudowanego konta administratora — pomyślne ukończenie instalacji nie będzie możliwe przy użyciu konta innego niż konto administratora lokalnego lub administratora domeny.
- Wszystkie dane pobrane z repozytorium (ESET Repository lub kopii dystrybucyjnej repozytorium niestandardowego) są podpisywane cyfrowo przez firmę ESET, a serwer ESET PROTECT weryfikuje skróty plików i podpisy PGP. Serwer ESET PROTECT generuje instalator kompleksowy lokalnie. Dlatego instalator kompleksowy nie jest podpisany cyfrowo, co może generować ostrzeżenie przeglądarki internetowej podczas pobierania instalatora lub ostrzeżenie systemu operacyjnego i uniemożliwić instalację w systemach, w których niepodpisane instalatory są blokowane.
- Warto pamiętać, że można wyodrębnić dane wrażliwe (np. hasło do certyfikatu), ponieważ są one osadzone w instalatorze.
- Instalator ESET Endpoint Antivirus/Security utworzony w ESET PROTECT 8.1 i późniejszej wersji obsługuje tryb wielosesyjny Windows 10 Enterprise for Virtual Desktops i Windows 10.

Proces instalacji

- Jeśli chcesz uruchomić instalator bez wyświetlania okna dialogowego, postępuj zgodnie z instrukcjami dotyczącymi cichej instalacji.
- W przypadku wystąpienia błędu podczas instalacji zapoznaj się z sekcją dotyczącą rozwiązywania problemów, w której opisano najczęściej spotykane błędy instalacji.

1. Uruchom pakiet instalatora.

Przed zainstalowaniem produktu zabezpieczającego ESET należy odinstalować z komputera wszelkie produkty zabezpieczające innych firm.

- Jeśli podczas tworzenia pakietu instalacyjnego wybrano opcję **ESET AV Remover**, **ESET AV Remover** pomoże odinstalować lub całkowicie usunąć oprogramowanie zabezpieczające innych firm:

a)Zaznacz pole wyboru **Chcę odinstalować niezgodne produkty zabezpieczające**, aby usunąć/odinstalować oprogramowanie zabezpieczające innych firm uruchomione lub zainstalowane na komputerze. Sprawdź listę obsługiwanego oprogramowania.

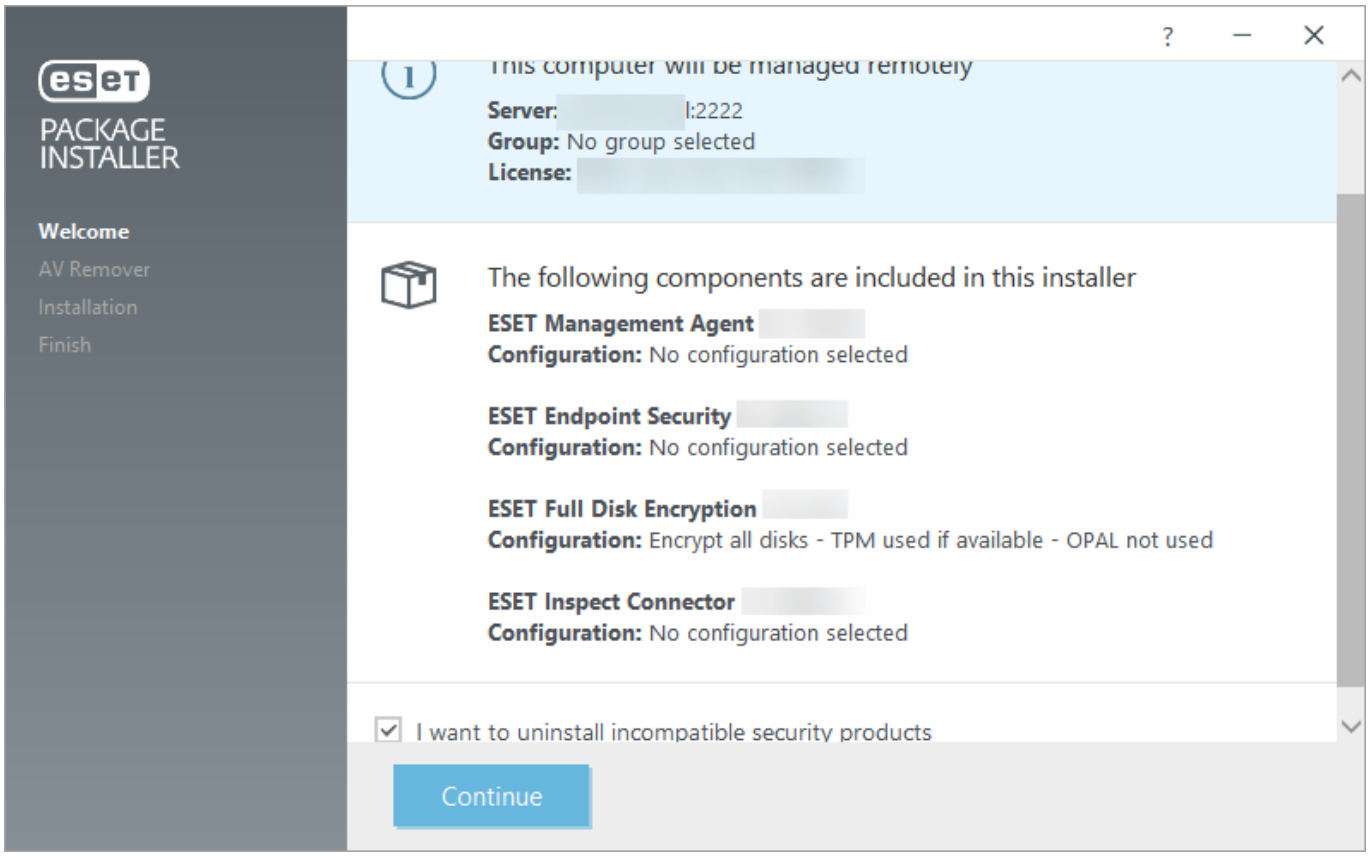
b)Kliknij przycisk **Kontynuuj**.

c)Po ukończeniu skanowania zainstalowanych aplikacji zaznacz pole wyboru obok aplikacji, które chcesz usunąć, a następnie kliknij przycisk **Usuń**. Więcej informacji można znaleźć w artykule bazy wiedzy na temat programu ESET AV Remover.

d)Po odinstalowaniu oprogramowania zabezpieczającego ESET AV Remover lub jeśli nie została usunięta żadna aplikacja, kliknij **Kontynuuj instalację**.

- Jeśli na komputerze lokalnym nie jest używany żaden produkt zabezpieczający innej firmy, kliknij

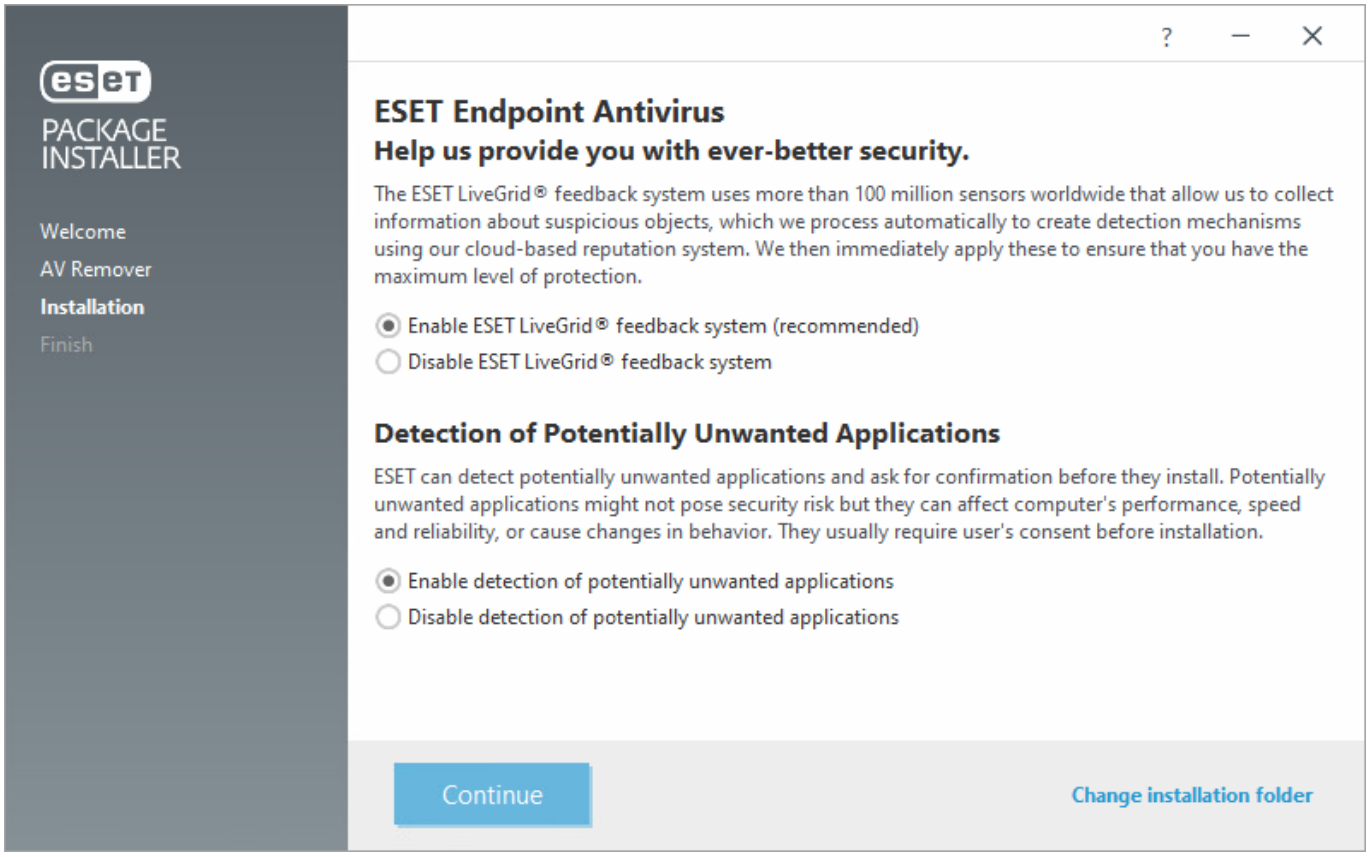
Kontynuuj.



2.

oWłącz system informacji zwrotnych ESET LiveGrid® (zalecane)

oWłącz wykrywanie potencjalnie niepożądanych aplikacji — więcej informacji zawiera artykuł w bazie wiedzy.



3. Po zakończeniu instalacji kliknij przycisk **Gotowe**. Produkt ESET Security otworzy się automatycznie. Możesz sprawdzić dziennik stanu (*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs\status.html* - ta lokalizacja jest domyślnie ukryta) na maszynie klienta, aby upewnić się, że aplikacja ESET Management Agent działa prawidłowo. W przypadku problemów z zainstalowanym agentem ESET Management (np. gdy nie łączy się on z serwerem ESET PROTECT) patrz sekcja Rozwiązywanie problemów z połączeniem agenta.

Rozwiązywanie problemów

W przypadku wystąpienia błędu podczas instalacji zapoznaj się z sekcją dotyczącą rozwiązywania problemów, w której opisano najczęściej spotykane błędy instalacji.

Inne metody wdrażania

Agenta ESET Management oraz produkty ESET Endpoint można wdrażać oddzielnie na wiele sposobów.

Wdrażanie agenta ESET Management

Wdrażanie lokalne:

- Instalator kompleksowy — pakiet zawiera agenta ESET Management i produkt zabezpieczający firmy ESET.
- Skrypt instalacyjny agenta
- Pobierz agenta z witryny firmy ESET i wybierz wspomaganą instalację serwerową lub instalację w trybie offline.

Zdalne wdrażanie (zalecane w przypadku większych sieci):

- Narzędzie ESET Remote Deployment Tool — zdalne wdrażanie instalatora kompleksowego.
- Obiekt GPO (obiekt zasad grupy)
- Wdrażanie agenta — zadanie serwera

Wdróż produkty firmy ESET do obsługi punktów końcowych

Po wdrożeniu agenta ESET Management można zainstalować produkt firmy ESET do obsługi punktów końcowych bezpośrednio z poziomu rozwiązania ESET PROTECT w jeden z następujących sposobów:

- Przy użyciu zadania instalacji oprogramowania.
- Lokalnie, w ramach standardowej instalacji produktu firmy ESET

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.

Wymagania wstępne dotyczące Narzędzia do wdrażania ESET

W przypadku wdrażania zdalnego należy upewnić się, że wszystkie komputery klienckie mają połączenie z internetem.

Aby można było używać narzędzia do wdrażania zdalnego opracowanego przez firmę ESET w systemie Windows, muszą zostać spełnione następujące wymagania wstępne:

- Serwer ESET PROTECT i konsola internetowa ESET PROTECT muszą być zainstalowane (na komputerze serwera).
- Muszą być otwarte odpowiednie porty. Sprawdź porty używane do zdalnego wdrożenie agenta ESET Management na komputerze docelowym z systemem operacyjnym Windows.
- Nazwy pakietów instalacyjnych muszą zawierać ciąg "x86" lub "x64". W przeciwnym razie wdrożenie nie powiedzie się.
- Pakiet instalatora (instalacja kompleksowa) musi zostać utworzony i pobrany na dysk lokalny.
- Wymagane są uprawnienia do tworzenia instalatora kompleksowego.

Wdrażanie może zakończyć się niepowodzeniem z wielu powodów. W przypadku problemów z wdrożeniem należy zapoznać się z rozdziałem Rozwiązywanie problemów lub sprawdzonymi przykładowymi scenariuszami wdrażania agenta ESET Management.

W celu wdrożenia agentów ESET Management na komputerach klienckich należy wykonać następujące czynności:

1. Pobierz narzędzie ESET Remote Deployment Tool z witryny internetowej firmy ESET.

2. Sprawdź, czy spełnione są wszystkie wymagania wstępne.

3. Na komputerze klienckim uruchom narzędzie do wdrażania zdalnego opracowane przez firmę ESET.

4. Wybierz **Ręczne dodawanie komputerów**. Należy ręcznie wprowadzić listę nazw hostów lub adresów IP.

5. Wprowadź nazwy hostów lub adresy IP i kliknij przycisk **Dalej**. Każdy adres IP oraz każda nazwa hosta musi się znajdować w nowym wierszu.

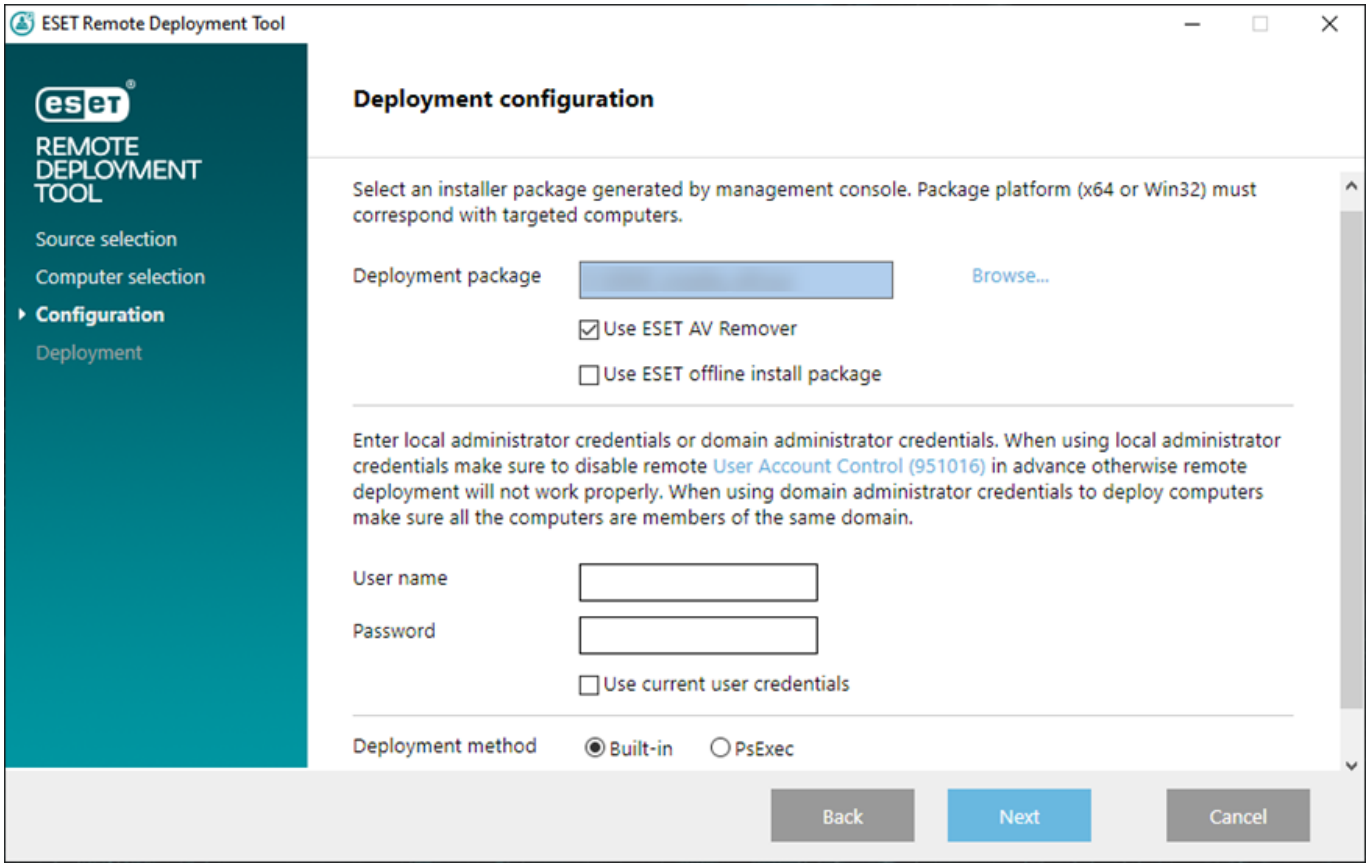
Należy upewnić się, że wszystkie wybrane komputery mają tę samą platformę (64- lub 32-bitowy system operacyjny).

6. Zostaną wyświetlone wybrane komputery przeznaczone do wdrażania zdalnego. Upewnij się, że zostały dodane wszystkie komputery, a następnie kliknij przycisk **Dalej**.

7. Kliknij przycisk **Przeglądaj** i wybierz pakiet instalatora utworzony w rozwiązaniu ESET PROTECT lub konsoli internetowej ESET PROTECT Cloud. Możesz także wybrać opcję **Użyj pakietu instalacyjnego ESET offline**. Pakiet ten ma postać pliku *.dat* i jest tworzony z poziomu programu ESET PROTECT Live Installer (tylko ESET PROTECT Cloud). Jeśli na komputerze lokalnym nie są zainstalowane dodatkowe aplikacje zabezpieczające, anuluj zaznaczenie pola wyboru **Użyj narzędzia ESET AV Remover**. Narzędzie ESET AV Remover może usunąć niektóre aplikacje.

8. Wprowadź poświadczenia logowania dla komputerów docelowych. Jeśli komputery należą do domeny, wprowadź **poświadczenia administratora domeny**. W przypadku logowania przy użyciu **lokalnych poświadczeń administracyjnych** niezbędne jest wyłączenie zdalnej kontroli konta użytkownika na komputerach docelowych. Opcjonalnie możesz zaznaczyć pole wyboru **Użyj poświadczeń bieżącego użytkownika**, aby poświadczenia logowania zostały automatycznie wprowadzone.

9. Wybierz **metodę wdrażania** służącą do uruchamiania programów na komputerach zdalnych. Metoda **Wbudowana** to ustawienie domyślne obsługujące komunikaty o błędach systemu Windows. **PsExec** to narzędzie zewnętrzne stanowiące alternatywę dla metody wbudowanej. Wybierz jedną z tych opcji i kliknij przycisk **Dalej**.



Jeśli wybrano **PsExec**, wdrożenie zakończy się niepowodzeniem, ponieważ narzędzie nie może zaakceptować Umowy Licencyjnej Użytkownika Końcowego **PsExec**. Aby przeprowadzić pomyślne wdrożenie, otwórz wiersz polecenia i uruchom ręcznie polecenie **PsExec**.

10. Po rozpoczęciu instalacji zostanie wyświetlony komunikat „Powodzenie”. Kliknij przycisk **Zakończ**, aby ukończyć wdrażanie. Jeśli wdrażanie nie powiedzie się, możesz wyeksportować listę komputerów, w przypadku których wystąpiło niepowodzenie. Kliknij przycisk **Przeglądaj** obok pola **Eksportuj komputery zakończone niepowodzeniem**, wybierz plik *.txt*, w którym chcesz zapisać listę, a następnie kliknij opcję **Eksportuj komputery zakończone niepowodzeniem**.



Na komputerze klienckim można zapoznać się z dziennikiem stanu (jego lokalizacja to *C:\ProgramData\ESET\RemoteAdministrator\Agent\Logs\status.html*), aby sprawdzić, czy agent ESET Management działa prawidłowo.

Inne metody wdrażania agentów ESET Management za pomocą narzędzia

ESET Remote Deployment Tool

- Usługa Active Directory — podaj poświadczenia usługi Active Directory. Ta opcja obejmuje eksportowanie struktury usługi Active Directory w celu jej późniejszego zaimportowania do programu ESET PROTECT.
- Skanowanie sieci — podaj zakresy adresów IP na potrzeby skanowania komputerów w sieci.
- Importowanie listy — podaj listę nazw hostów lub adresów IP.

Rozwiązywanie problemów

Wdrażanie może zakończyć się niepowodzeniem z wielu powodów. W przypadku problemów z wdrożeniem należy zapoznać się z rozdziałem Rozwiązywanie problemów lub sprawdzonymi przykładowymi scenariuszami wdrażania agenta ESET Management.

Konsola internetowa ESET PROTECT

Zaloguj się w konsoli internetowej centrum ESET PROTECT.

- Na serwerze lokalnym Windows (komputerze będącym hostem dla konsoli internetowej):

Kliknij **Start** > **Wszystkie programy** > **ESET** > **Konsola internetowa ESET PROTECT**.

- Na dowolnym urządzeniu z dostępem do używanego serwera internetowego wpisz adres URL w następującym formacie (część „nazwa_serwera” zastąp prawdziwą nazwą lub adresem IP używanego serwera internetowego): https://yourservername/era/

W domyślnej przeglądarce internetowej zostanie otwarty ekran logowania. Jeśli zostanie wyświetlone ostrzeżenie o certyfikacie SSL, dodaj wyjątek certyfikatu do przeglądarki internetowej.

Połączenia z konsolą internetową ESET PROTECT należy nawiązywać przy użyciu obsługiwanej przeglądarki internetowej.

Przy pierwszym logowaniu do konsoli internetowej wyświetlany jest Przewodnik ESET PROTECT. Za jego pomocą można wdrożyć agentów ESET Management na komputerach w sieci.

Interfejs użytkownika konsoli internetowej programu ESET PROTECT

Interfejs użytkownika konsoli internetowej programu ESET PROTECT składa się z kilku części:

- W górnej części konsoli internetowej ESET PROTECT dostępne jest narzędzie **Wyszukiwanie**.
- Kliknij **Szybkie łącza**, aby wykonać niektóre z najczęściej używanych czynności w konsoli internetowej.
- W celu uzyskania pomocy podczas pracy z programem ESET PROTECT należy kliknąć ikonę **Pomoc**, a następnie kliknąć pozycję **<Current topic> — Pomoc**. Zostanie wyświetlone odpowiednie okno pomocy

dotyczące bieżącej strony.

• W prawym górnym rogu wyświetlany jest bieżący użytkownik z odliczaniem limitu czasu sesji użytkownika. W dowolnym momencie można się wylogować, klikając opcję **Wyloguj**. Po upłynięciu limitu czasu sesji (z powodu braku aktywności użytkownika) użytkownik musi się ponownie zalogować.

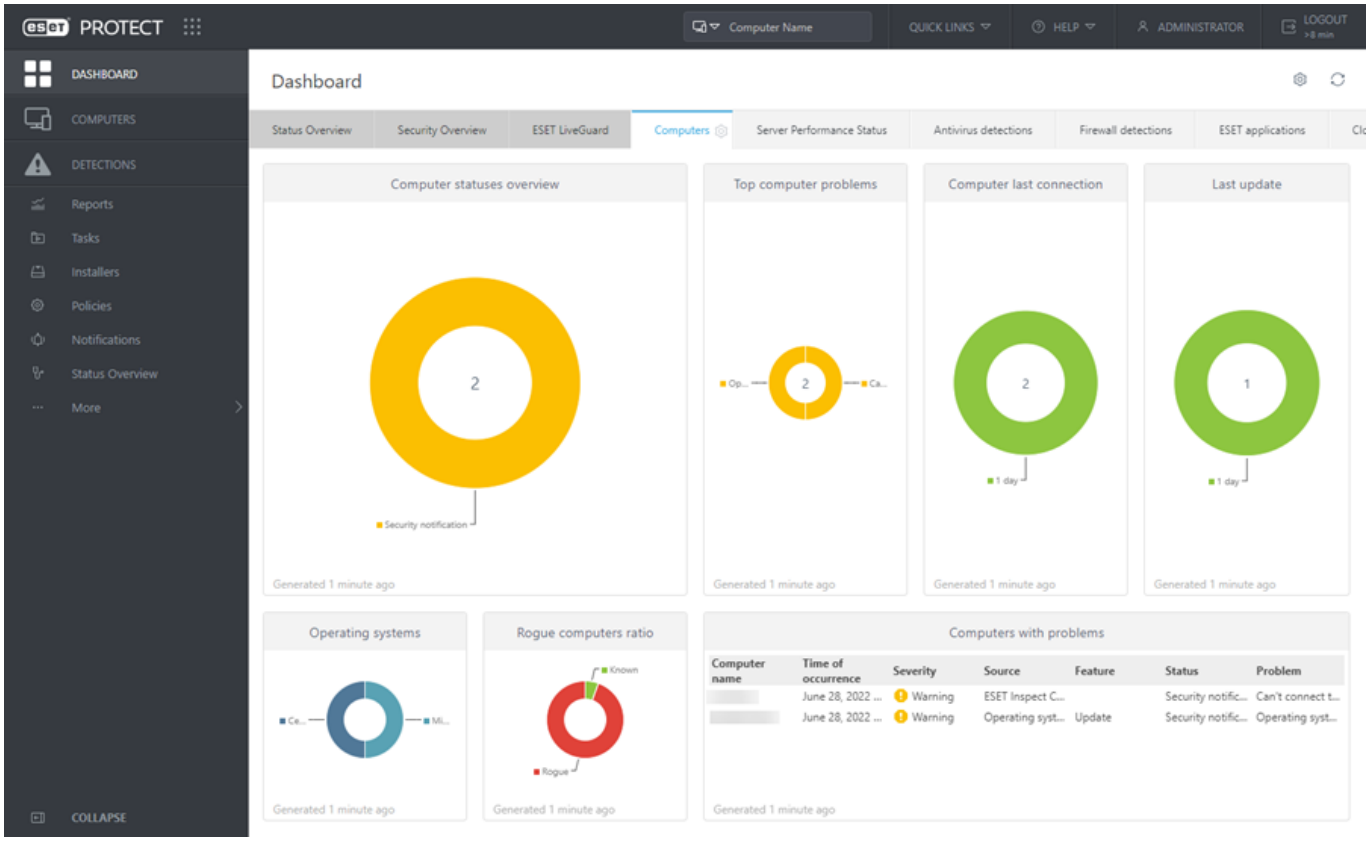
• Menu główne po lewej stronie konsoli internetowej zawiera narzędzia, za pomocą których administratorzy mogą zarządzać klienckimi rozwiązaniami zabezpieczającymi oraz ustawienia serwera ESET PROTECT. Za pomocą narzędzi w obszarze **Więcej** można skonfigurować środowisko sieciowe i zminimalizować potrzeby konserwacyjne. Można również skonfigurować powiadomienia i panele kontrolne, aby monitorować stan sieci. Kliknij umożliwia rozwinięcie menu z lewej strony ekranu. Menu można zwinąć, klikając ikonę **Zwiń**.

• W lewej górnej części ekranu obok nazwy ESET PROTECT znajduje się ikona nawigacji po produktach , która ułatwia nawigację między ESET PROTECT i pozostałymi produktami: ESET Inspect, ESET Business Account i ESET MSP Administrator.

• zawsze oznacza menu kontekstowe.

• **Należy kliknąć opcję Odśwież**, aby załadować ponownie/odświeżyć wyświetlane informacje.

• Przyciski u dołu strony są różne w poszczególnych sekcjach i funkcjach, a ich szczegółowe opisy można znaleźć w odpowiednich rozdziałach.



Poniższe tematy opisują główne pozycje menu:

Panel kontrolny
Komputery i grupy

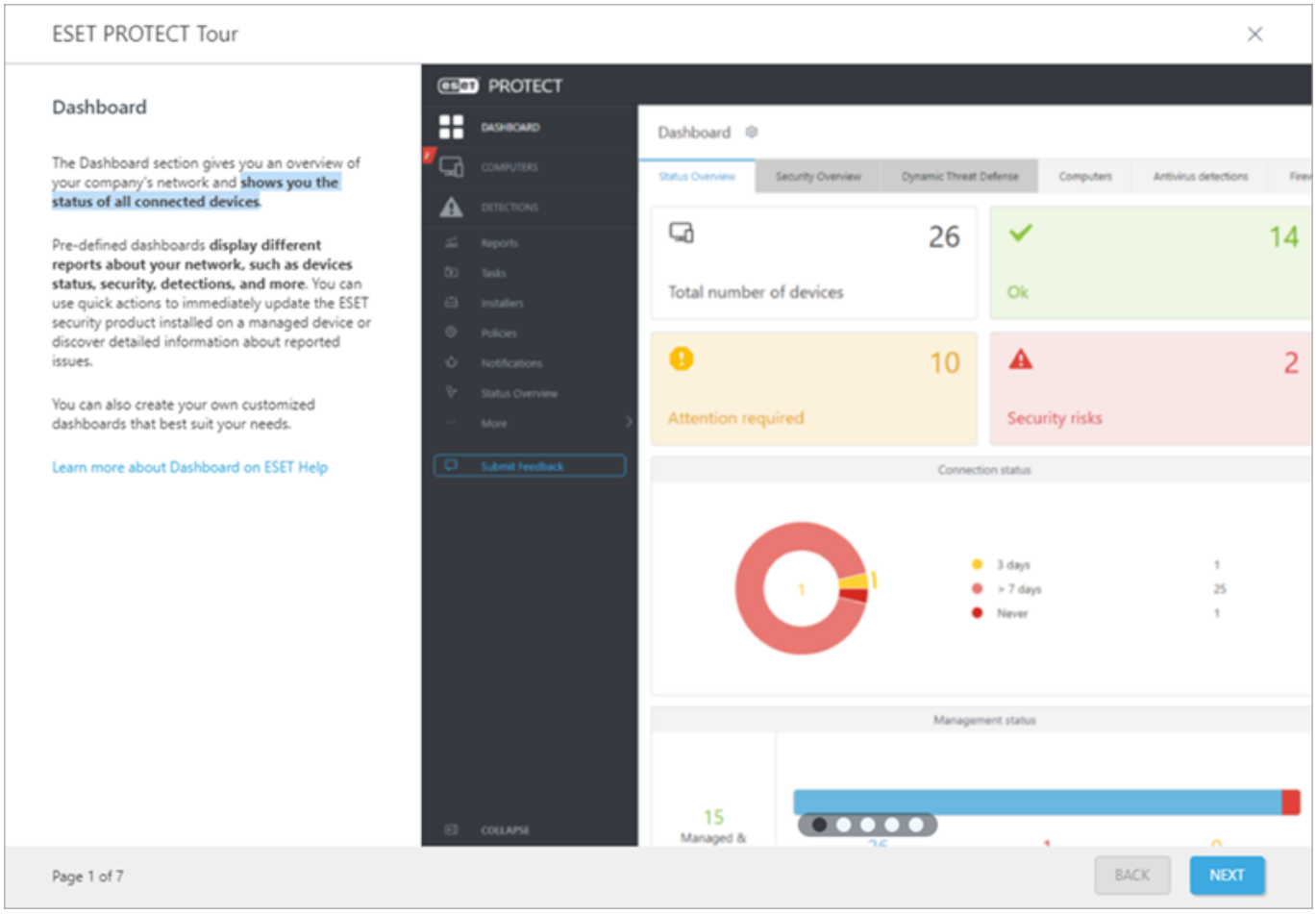
Wykrycia
Raporty
Zadania
Polityki
Powiadomienia
Przegląd stanu
··· **Więcej** > Wykluczenia
··· **Więcej** > Kwarantanna
··· **Więcej** > Użytkownicy i zestawy uprawnień
··· **Więcej** > Zarządzanie licencjami
··· **Więcej** > Certyfikaty

Przewodnik ESET PROTECT

Gdy zalogujesz się do konsoli internetowej po raz pierwszy, **pojawi się Przewodnik ESET PROTECT**.

Zawiera on podstawowe objaśnienia ważnych elementów konsoli internetowej ESET PROTECT, agenta ESET Management oraz produktów zabezpieczających firmy ESET. Przeczytasz o Panelach kontrolnych, Komputerach, Wykrywaniach, Zadaniach, Politykach, Powiadomieniach i Automatycznych aktualizacjach produktu.

Kliknij opcję **Chroń urządzenia** w ostatnim kroku **Przewodnika ESET PROTECT**, aby wdrożyć Agentów ESET Management na komputerach w sieci. Instalator agenta można również utworzyć bez użycia kreatora, klikając przycisk **Instalatory** > **Utwórz instalator**.



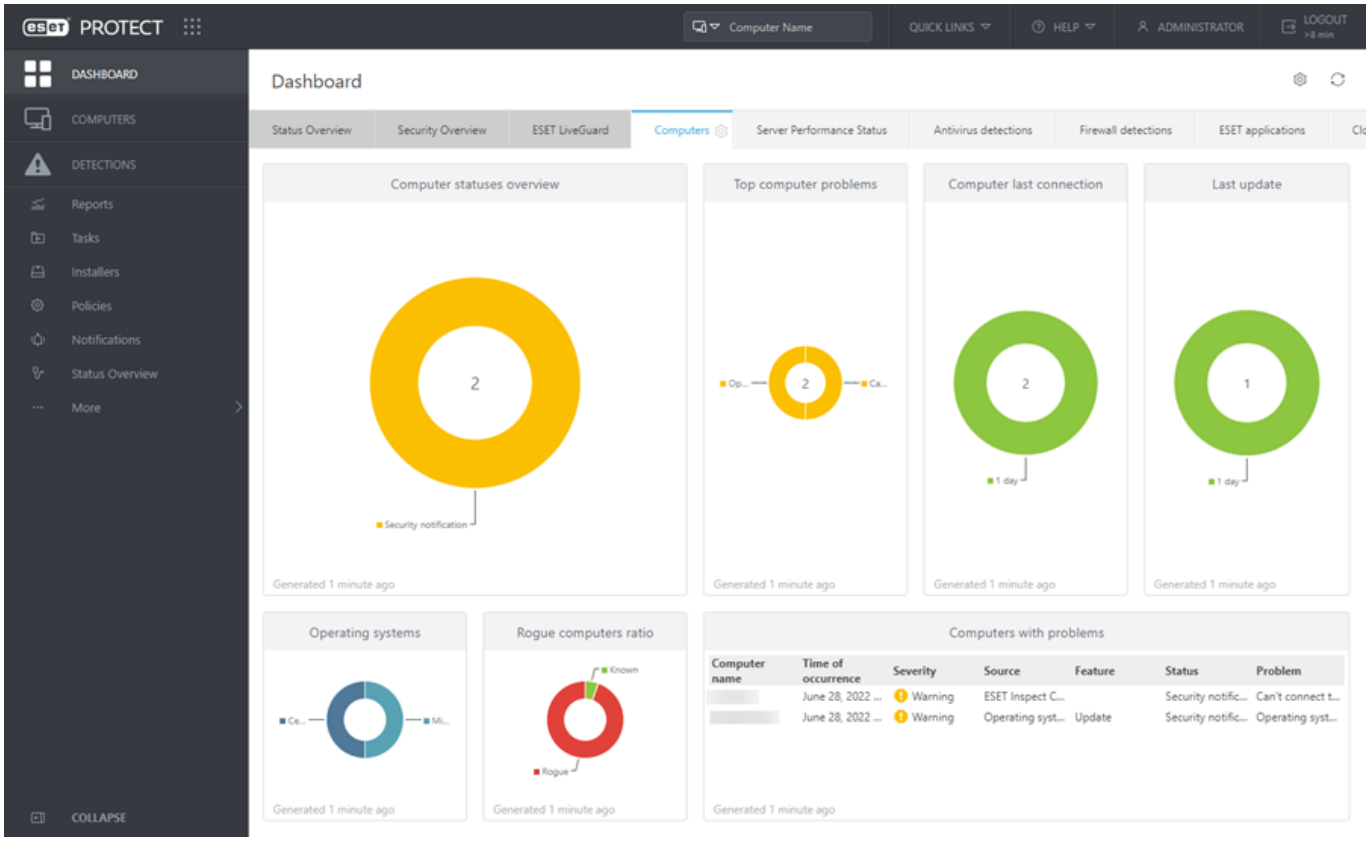
Jeśli nie chcesz korzystać z **Przewodnika ESET PROTECT**, kliknij **X**. Spowoduje to otwarcie konsoli internetowej ESET PROTECT. **Przewodnik ESET PROTECT** nie zostanie wyświetlony przy następnym logowaniu do konsoli internetowej ESET PROTECT.

Aby ponownie uruchomić **Przewodnik ESET PROTECT**, należy kliknąć kolejno **Pomoc** > **ESET PROTECT Prezentacja**.

Po pierwszym zalogowaniu się do konsoli internetowej ESET PROTECT zaleca się uruchomienie zadania klienta Aktualizacja systemu operacyjnego na komputerze, na którym zainstalowano ESET PROTECT.

Panel kontrolny

Panel kontrolny to ekran wyświetlany domyślnie po pierwszym zalogowaniu się użytkownika do konsoli internetowej ESET PROTECT. Wyświetlane są tam wstępnie zdefiniowane raporty dotyczące sieci. Przy użyciu kart widocznych na górnym pasku menu można przełączać poszczególne panele kontrolne. Na każdym panelu kontrolnym znajduje się kilka raportów.



Panele kontrolne można dostosowywać (z wyjątkiem paneli **Przegląd stanu**, **Przegląd incydentów** i **ESET LiveGuard**), dodając nowe raporty i modyfikując istniejące, zmieniając ich rozmiary oraz przesuwając i zmieniając ich rozmieszczenie. Umożliwia to uzyskanie wszechstronnego wglądu w funkcje produktu ESET PROTECT i jego elementy (komputery, grupy, zadania, polityki, użytkowników itd.).

W programie ESET PROTECT dostępne są następujące wstępnie zdefiniowane panele kontrolne:

- **Przegląd stanu** — podstawowy panel kontrolny zawierający najważniejsze informacje na temat sieci ESET PROTECT. Tego panelu kontrolnego nie można zmodyfikować.

- **Przegląd incydentów** — ten panel kontrolny udostępnia przegląd nierozwiązanych wykryć zgłoszonych w ciągu ostatnich 7 dni, włącznie z ich poziomem, metodą wykrycia, stanem rozwiązania oraz listą 10 komputerów/użytkowników z największą liczbą wykryć. Tego panelu kontrolnego nie można zmodyfikować.

- **ESET LiveGuard** — Jeśli używasz produktu ESET LiveGuard Advanced, znajdziesz tutaj przegląd przydatnych raportów ESET LiveGuard Advanced.

- **Komputery** — na tym panelu kontrolnym widoczne jest zestawienie komputerów klienckich, przedstawiające stan ich ochrony, systemy operacyjne, stan aktualizacji itd.

- **Stan wydajności serwera** — na tym panelu kontrolnym można wyświetlać informacje dotyczące samego serwera ESET PROTECT: obciążenie serwera, klienty, na których występują problemy, obciążenie procesora, połączenia z bazą danych itd.

- **Wykrycia antywirusowe**— tutaj wyświetlane są raporty z modułu antywirusowego działającego w ramach produktów zabezpieczających klienty — aktywne wykrycia, zagrożenia w ciągu ostatnich 7/30 dni itd.

- **Zagrożenia** dla zapory — zdarzenia zapory dotyczące połączonych klientów uszeregowane według stopnia ważności, czasu zgłoszenia itd.

• **Aplikacje firmy ESET** — ten panel kontrolny umożliwia wyświetlanie informacji na temat zainstalowanych aplikacji firmy ESET.

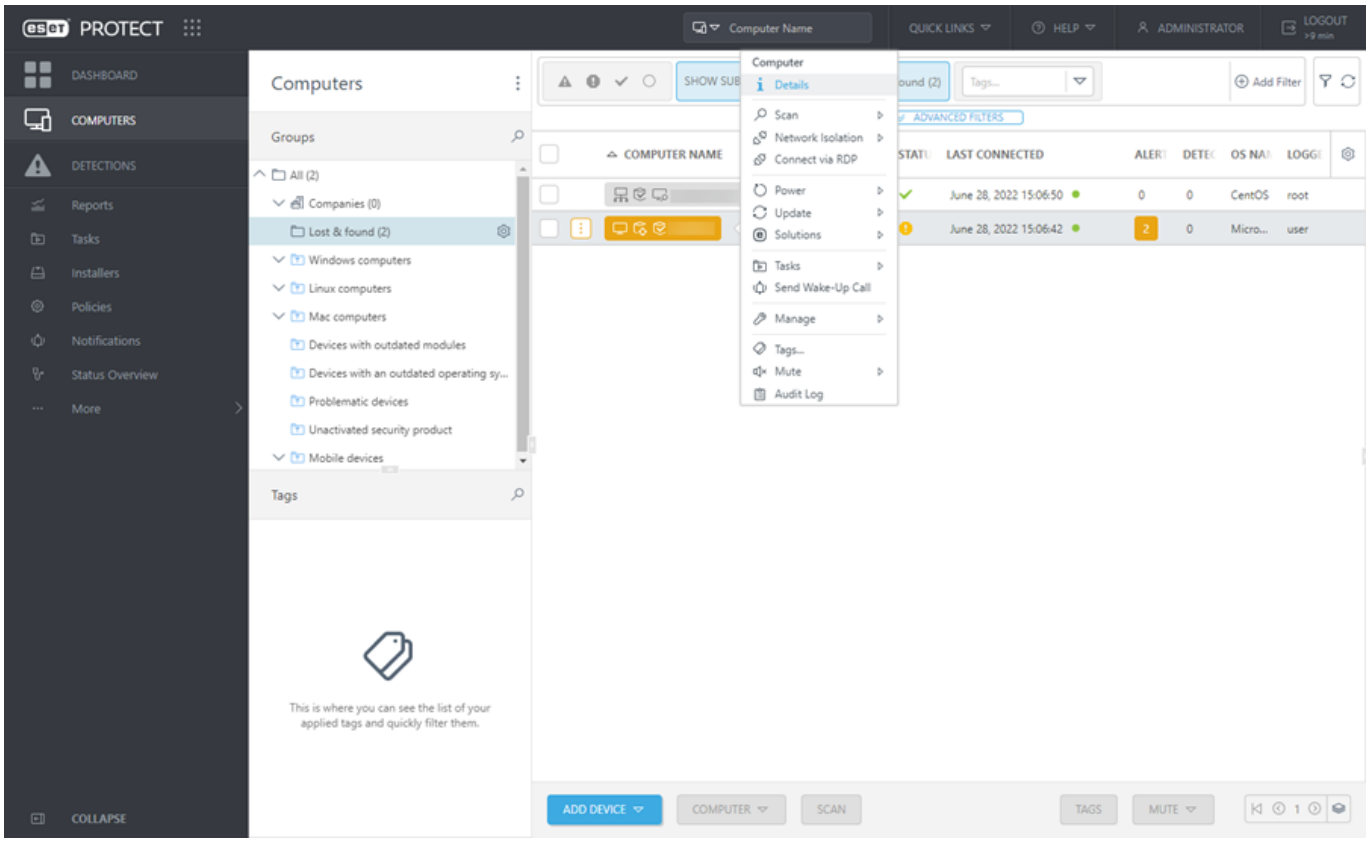
• **Ochrona oparta na chmurze** — ten panel kontrolny zawiera przegląd raportów ochrony opartej na chmurze (ESET LiveGrid®, a jeśli masz kwalifikującą się licencję, również ESET LiveGuard Advanced).

Komputery

Wszystkie komputery klienckie, które są osiągalne dla ESET PROTECT, są wyświetlane w sekcji **Komputery** i zorganizowane według grup. Kliknięcie którejś z grup dostępnych na liście (okno po lewej) powoduje wyświetlenie członków tej grupy (klientów) w prawym okienku. Można przeciągać i upuszczać klienty, aby przenosić ich między grupami.

Zarządzaj komputerami

Kliknij urządzenie, aby otworzyć nowe menu z czynnościami dostępnymi w przypadku tego urządzenia. Możesz także zaznaczyć pole wyboru obok urządzenia i kliknąć menu **Komputer** na dolnym pasku. Menu **Komputer** wyświetla różne opcje w zależności od typu urządzenia.



Filtrowanie komputerów

Jeśli nie możesz znaleźć określonego komputera na liście i wiesz, że znajduje się w Twojej infrastrukturze ESET PROTECT, wyłącz wszystkie filtry.

Klienty (komputery) można filtrować za pomocą filtrów u góry strony:

- Wybierz pole **Pokaż podgrupy**, aby wyświetlić podgrupy w ramach wybranej grupy.

- Kliknięcie przycisku **Dodaj filtr** pokazuje dostępne kryteria filtrowania. Dostępnych jest kilka wygodnych w użyciu wstępnie zdefiniowanych filtrów.

- Możesz kliknąć pozycję **Dodaj filtr** > **Kategoria produktu** i wybrać jedną z dostępnych kategorii:

  - **Wszystkie urządzenia** — wyświetlane są wszystkie komputery klienckie bez filtrowania. Wszystkich powyższych opcji filtrowania można używać łącznie w celu ograniczenia liczby pozycji wyświetlanych w widoku.

  - **Ochrona ESET** — wyświetlane są klienty chronione przez produkt ESET.

  - **ESET PROTECT —** Wyświetlane są poszczególne komponenty ESET PROTECT, takie jak agent, sensor RD czy serwer proxy.

  - **Inne** — wyświetla tylko komputery klienckie z uruchomionym wybranym produktem (Shared Local Cache, wirtualne urządzenie zabezpieczające lub ESET Inspect).

- Ikony stanu służą do filtrowania klientów według ważności wykrytych problemów (czerwony kolor dla błędów, żółty dla ostrzeżeń, zielony dla powiadomień i szary dla komputerów niezarządzanych). Ikona stanu przedstawia bieżący stan określonego komputera klienckiego i zainstalowanego na nim rozwiązania ESET. Można ukryć lub wyświetlić ikony stanu o różnej ważności, aby ocenić klienty w sieci według stanu. Na przykład w celu wyświetlenia tylko komputerów z ostrzeżeniami należy zaznaczyć wyłącznie żółtą ikonę (pozostałe ikony nie powinny być zaznaczone). Aby wyświetlić ostrzeżenia i błędy, należy zaznaczyć czerwoną i żółtą ikonę stanu. Komputery niezarządzane (klienty w sieci bez zainstalowanego agenta ESET Management oraz bez produktu zabezpieczającego ESET) wyświetlane są zwykle w grupie statycznej **Zgubione i znalezione**.

- **Filtry zaawansowane** można zobaczyć jako rozwijany panel filtrów na ekranie **Komputery**. Podczas filtrowania dużych zestawów komputerów zaawansowane filtry pokazują, które wartości filtrów zwrócą możliwą do opanowania liczbę wyników, co pozwoli na znacznie szybsze znalezienie odpowiednich urządzeń.

- Można również kliknąć nagłówek kolumny w celu posortowania komputerów według danego atrybutu.

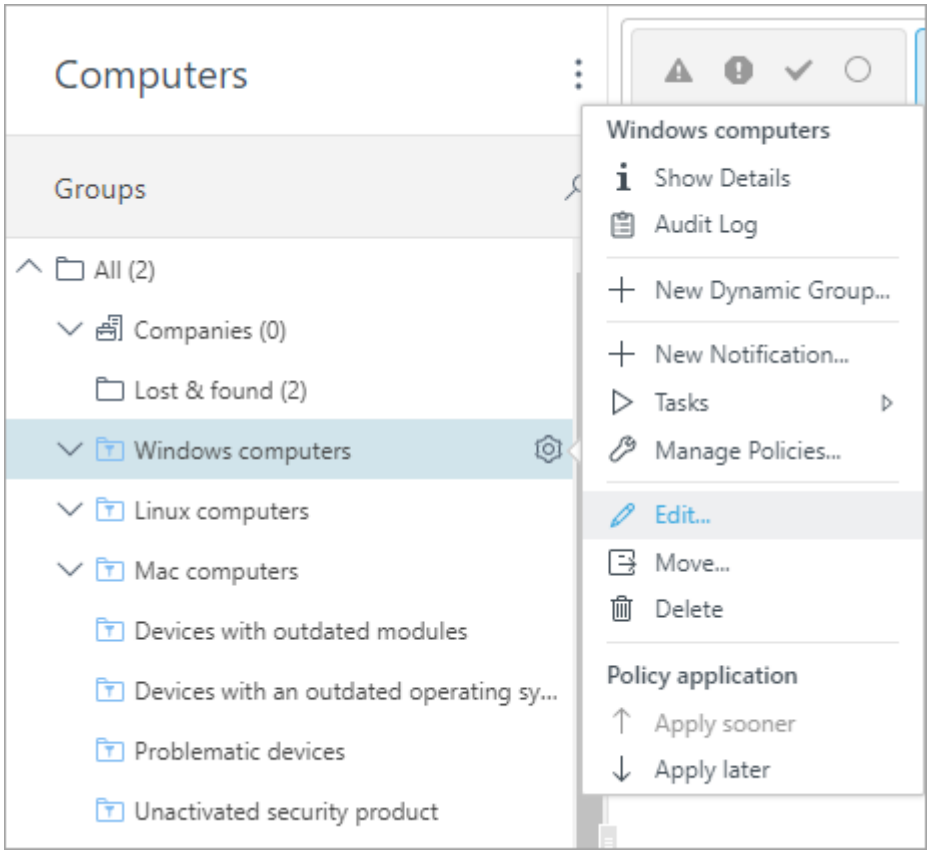
Ostatnie połączenie wyświetla datę i godzinę ostatniego połączenia zarządzanego urządzenia. Zielona kropka wskazuje, że komputer łączył się mniej niż 10 minut temu. Informacje **Ostatnie połączenie** zostają wyróżnione w celu wskazania braku połączenia komputera:

- Żółty (błąd) — komputer nie połączył się przez 2–14 dni.

- Czerwony (ostrzeżenie) — komputer nie połączył się od ponad 14 dni.

Grupy

Grupami można zarządzać w sekcji Komputery. Grupy umożliwiają organizowanie punktów końcowych w sieci, dzięki czemu można je systematycznie przypisywać zasady i zadania. To ustawienie dotyczy wszystkich członków grupy. Komputery należące do danej grupy są wyświetlane w prawym okienku. Kliknij ikonę koła zębatego obok nazwy grupy, aby wyświetlić dostępne czynności dotyczące grupy i szczegóły grupy.



Istnieją dwa typy grup: grupy statyczne i grupy dynamiczne.

Grupy statyczne

- Grupy statyczne to grupy wybranych komputerów klienckich i innych obiektów.
- Wszystkie urządzenia mobilne i komputery znajdują się w grupie statycznej.
- Można ręcznie wybrać, które punkty końcowe należą do dowolnej grupy statycznej.
- Obiekt może należeć tylko do jednej grupy statycznej.
- Grupy statyczne odgrywają ważną rolę w modelu zabezpieczeń produktu ESET PROTECT.
- Jeśli importujesz licencje z ESET Business Account lub ESET MSP Administrator, struktura firmy w ESET Business Account (w tym witryny) lub struktura ESET MSP Administrator pojawi się w drzewie grupy statycznej.

Grupy dynamiczne

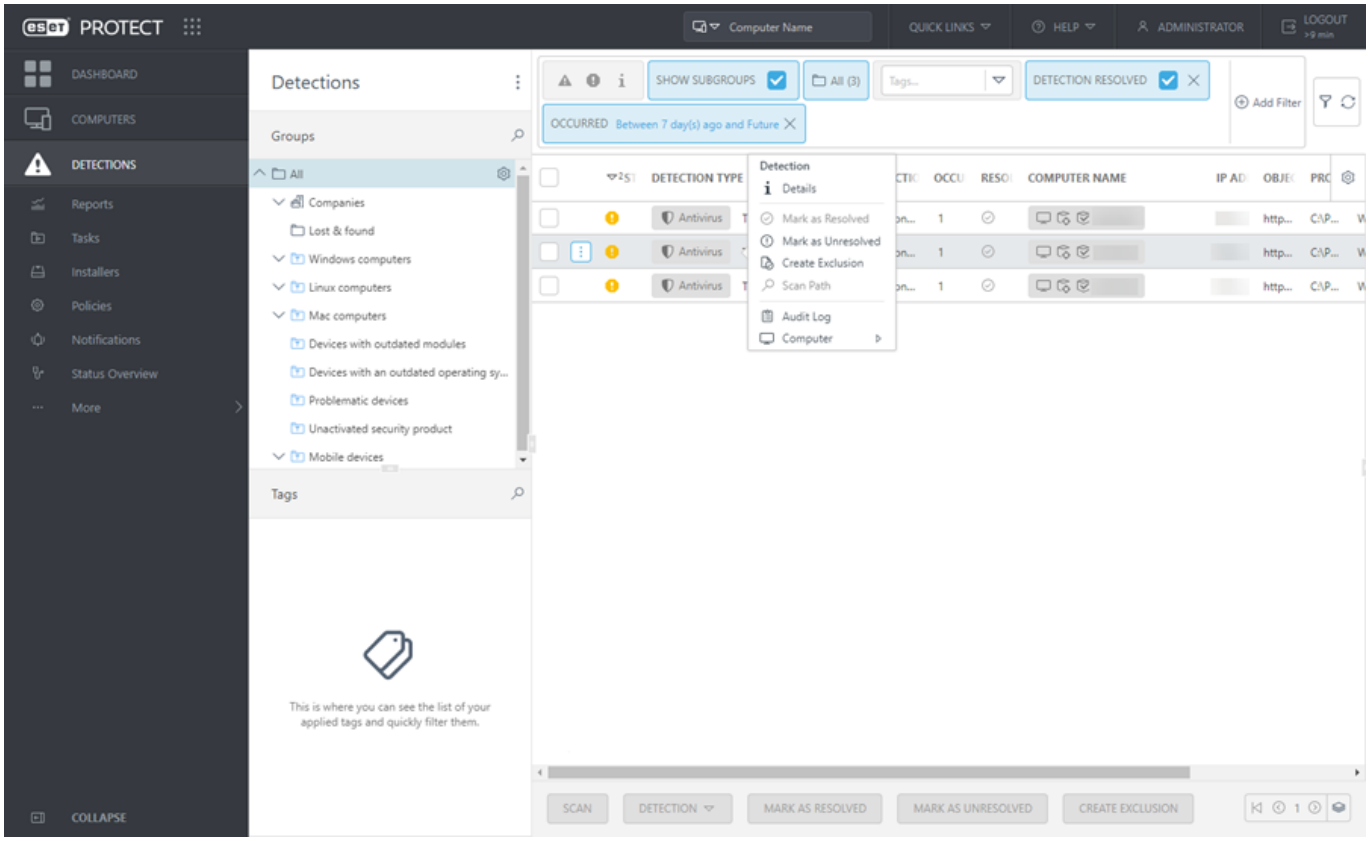
- Grupy dynamiczne można zrozumieć jako filtry niestandardowe, w których można ustawić reguły odpowiedniego filtrowania komputerów.
- Grupy dynamiczne opierają się na szablonach, w związku z czym punkty końcowe spełniające kryteria ustalone w szablonie są do nich dołączane automatycznie.
- Jeśli urządzenie klienckie nie spełnia kryteriów, zostanie automatycznie usunięte z grupy dynamicznej.
- Komputer może jednocześnie należeć do wielu grup dynamicznych. Może też nie należeć do żadnej takiej grupy.

W bazie wiedzy dostępne są informacje ułatwiające dodawanie komputerów do grup statycznych, tworzenie nowych szablonów grup dynamicznych oraz przypisywanie polityk do grup.

Dodatkowe informacje na temat grup można znaleźć w sekcji Grupy.

Wykrycia

Aby uzyskać dostęp do raportów wykrywania, kliknij opcję **Wykrywanie** w menu Konsoli internetowej po lewej stronie. Panel **Wykrywanie** zawiera przegląd wszystkich wykryć znalezionych na komputerach w sieci.



Można przeglądać grupy oraz wyświetlać wykrycia związane z członkami danej grupy. Można filtrować widok; wszystkie typy wykryć z ostatnich siedmiu dni są domyślnie widoczne. Wykrycia można teraz **oznaczać jako rozwiązane** w sekcji **Wykrycia** lub w obszarze szczegółów określonego klienta.

Wykrycia są grupowane według czasu i innych kryteriów, aby uprościć ich rozwiązywanie. Wykrycia starsze niż 24 godziny są automatycznie agregowane każdego dnia o północy. Zgrupowane wykrycia można zidentyfikować na podstawie wartości X/Y (rozwiązane elementy/łączna liczba elementów) w kolumnie **Rozwiązane**. Listę zgrupowanych wykryć można wyświetlić na karcie **Wystąpienia** w szczegółach wykrycia.

Wykrycia poddane kwarantannie można znaleźć w polu ··· **Więcej** > **Kwarantanna**.

Wyłączenia

Istnieje możliwość wykluczenia wybranych elementów z **wykrywania** w przyszłości. Kliknij wykrycie i wybierz pozycję **Utwórz wyłączenie**. Można wyłączyć tylko wykrycia **programów antywirusowych** oraz wykrycia **zapory** — reguły IDS. Można utworzyć wyłączenie i zastosować je do kilku komputerów bądź grup.

Wyłączenia należy stosować z dużą ostrożnością. Ich nieuważne stosowanie może spowodować zainfekowanie komputera.

Sekcja ··· **Więcej** > **Wyłączenia** zawiera wszystkie utworzone wyłączenia, zwiększając ich widoczność i ułatwiając zarządzanie nimi.

Wykrycia w archiwach

Jeśli w archiwum zostanie znalezione co najmniej jedno wykrycie, to archiwum oraz każde wykrycie wewnątrz tego archiwum są zgłaszane w obszarze **Wykrycia**.

Wyłączenie pliku archiwum zawierającego wykrycie nie wyłącza wykrycia. Musisz wyłączyć poszczególne wykrycia wewnątrz archiwum. Maksymalny rozmiar pojedynczego pliku w archiwum to 3 GB.

Wyłączone wykrycia nie zostaną już wykryte, nawet jeśli występują w innym archiwum lub nie są zarchiwizowane.

Ochrona przed oprogramowaniem wymuszającym okup

Produkty biznesowe ESET (wersja 7 i nowsze) zawierają rozwiązanie **Ochrona przed oprogramowaniem wymuszającym okup**. Ta nowa funkcja zabezpieczająca to część systemu HIPS, który chroni komputery przed oprogramowaniem wymuszającym okup. Gdy oprogramowanie wymuszające okup zostanie wykryte na komputerze klienckim, można wyświetlić szczegóły wykrycia w obszarze **Wykrycia** konsoli internetowej ESET PROTECT. Aby filtrować tylko wykrycia oprogramowania wymuszającego okup, kliknij pozycję **Dodaj filtr** > **Skaner** > **Skaner oprogramowania wymuszającego okup**. Więcej informacji na temat ochrony przed oprogramowaniem wymuszającym okup można znaleźć w glosariuszu firmy ESET.

Można zdalnie skonfigurować funkcję **Ochrona przed oprogramowaniem wymuszającym okup** z konsoli internetowej ESET PROTECT przy użyciu ustawień **Polityka** dotyczących danego produktu biznesowego ESET:

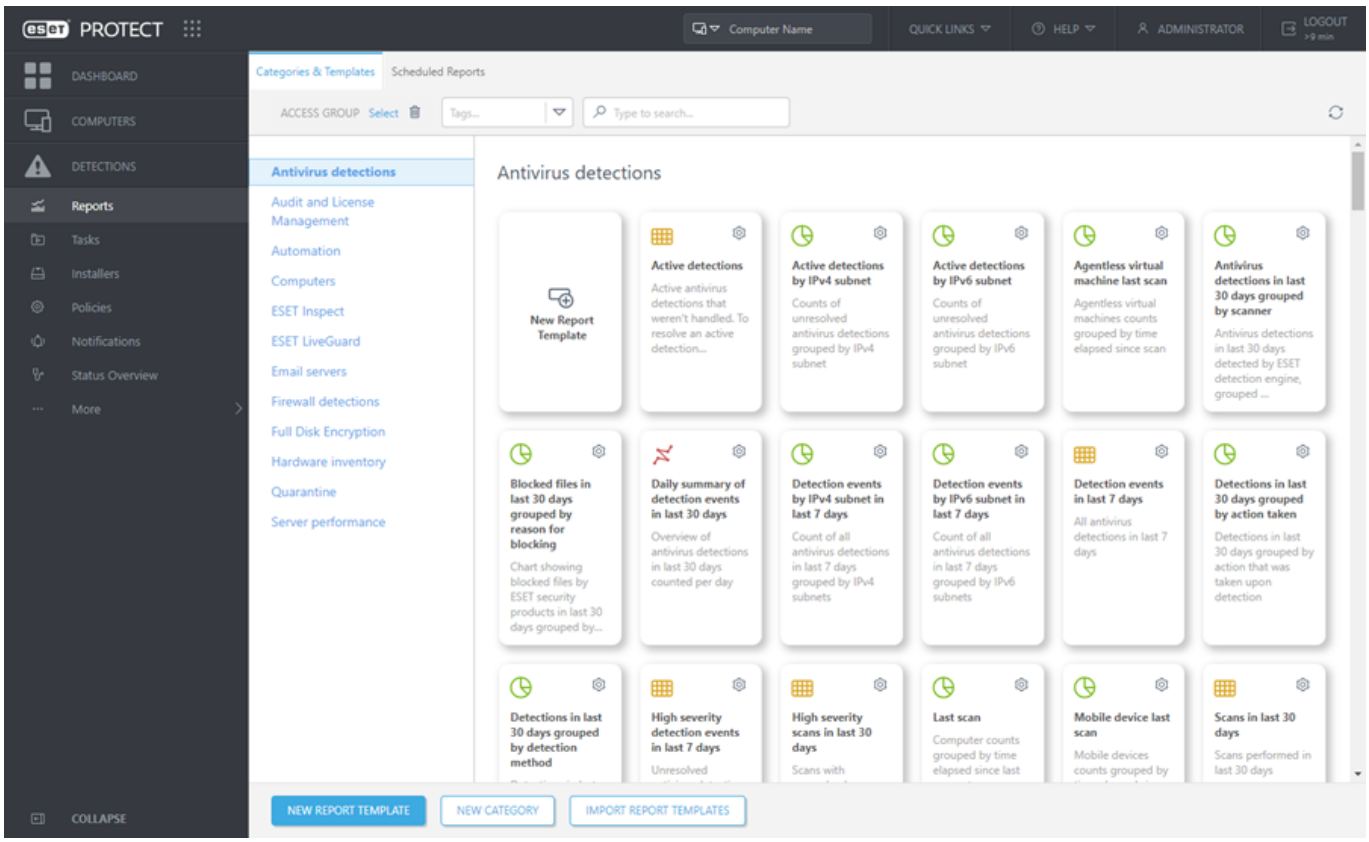
- **Włącz ochronę przed oprogramowaniem wymuszającym okup** — produkt biznesowy ESET automatycznie blokuje wszystkie podejrzane aplikacje, które zachowują się jak oprogramowanie wymuszające okup.
- **Włącz tryb audytu** — po włączeniu trybu audytu potencjalne wykrycia zidentyfikowane przez ochronę przed oprogramowaniem wymuszającym okup są zgłaszane w konsoli internetowej ESET PROTECT, ale produkt zabezpieczający ESET ich nie blokuje. Administrator może zdecydować o zablokowaniu zgłoszonego wykrycia lub wyłączeniu go przez wybranie opcji **Utwórz wyłączenie**. To ustawienie polityki jest dostępne tylko z poziomu konsoli internetowej ESET PROTECT.

Domyślnie ochrona przed oprogramowaniem wymuszającym okup blokuje wszystkie aplikacje, których zachowanie przypomina działanie oprogramowania wymuszającego okup. Dotyczy to także wiarygodnych aplikacji. Zalecamy **włączenie trybu audytu** na krótki czas na nowo zarządzanym komputerze, aby można było wyłączyć wiarygodne aplikacje, które — na podstawie ich zachowania — zostały błędnie zidentyfikowane jako oprogramowanie wymuszające okup (wynik fałszywie dodatni). Nie zalecamy trwałego używania trybu audytu, ponieważ nie umożliwia on automatycznego blokowania oprogramowania wymuszającego okup na komputerach zarządzanych.

Raporty

Raporty umożliwiają wygodny dostęp do danych w bazie danych oraz ich filtrowanie. Raporty są podzielone na kategorie. Każda kategoria zawiera krótki opis.

Aby uzyskać dostęp do raportów, kliknij pozycję **Raporty** w menu konsoli internetowej widocznym po lewej stronie, wybierz żądany szablon raportu (kafelek z opisem, czynnością), dla którego chcesz wyświetlić raport, i kliknij ikonę koła zębatego > **Generuj teraz**.



> Domyślnie wszystkie szablony raportów są dostępne tylko dla administratora. Inni użytkownicy nie mogą zobaczyć ani używać tych szablonów, chyba że przypisano im odpowiednie uprawnienia (lub jeśli szablony znajdują się w innej lokalizacji).

Aby otrzymywać raporty za pośrednictwem poczty e-mail, należy poprawnie skonfigurować połączenie z serwerem SMTP.

Szczegółowe instrukcje na temat konfiguracji automatycznych raportów w rozwiązaniu ESET PROTECT zawiera ten artykuł w bazie wiedzy firmy ESET.

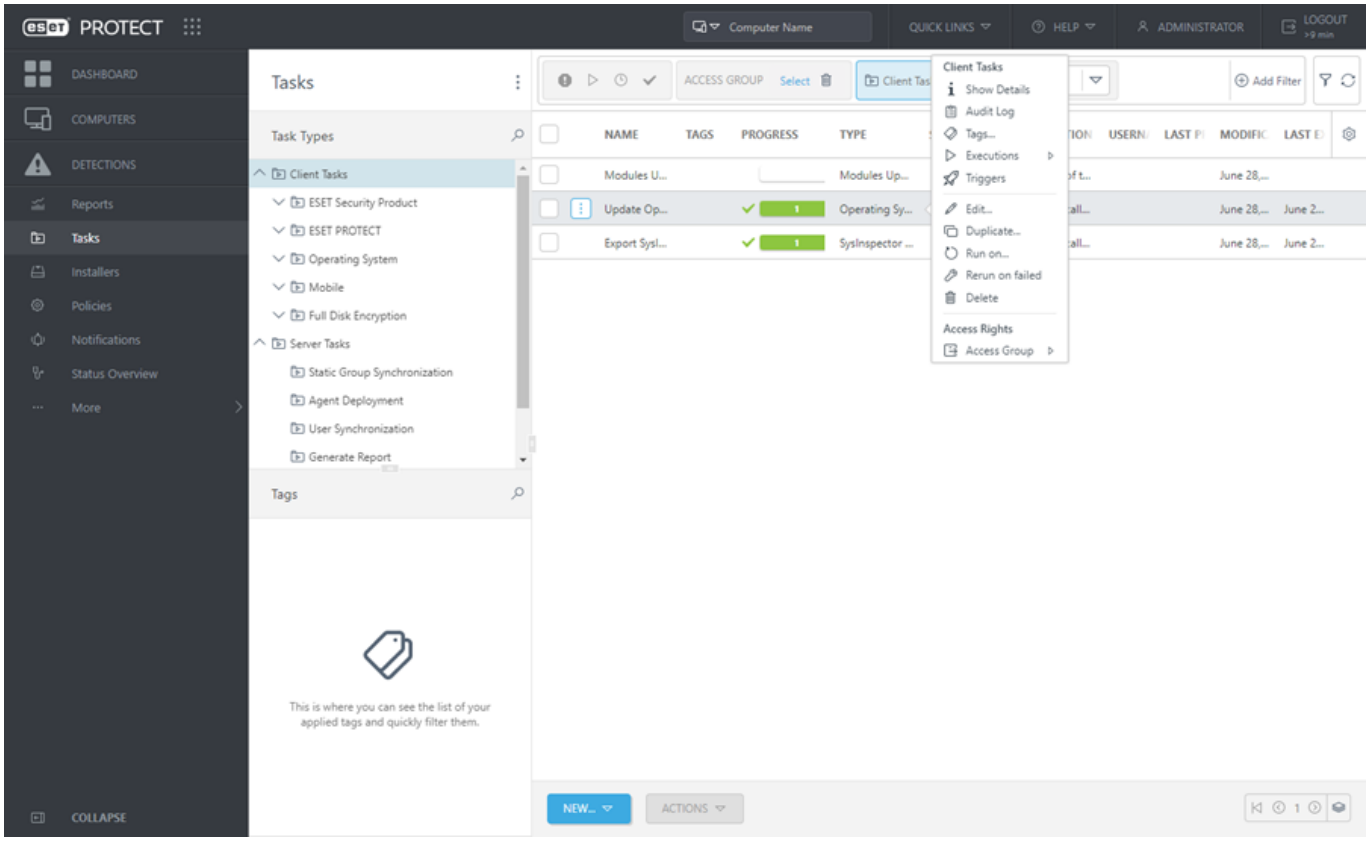
Zadania

Zadania służą do zarządzania serwerem ESET PROTECT, komputerami klienckimi i produktami firmy ESET. Zadania służą do automatyzacji rutynowych działań. Celem zadań mogą być pojedyncze komputery lub grupy.

Zadania umożliwiają przypisywanie określonych procedur do poszczególnych klientów lub grup klientów.

Oprócz okna **Zadania** można tworzyć zadania z menu kontekstowych w obszarze Komputery. Aby

wyświetlić stan wykonanych zadań, kliknij **Zadania** i obserwuj, czy zadania zakończyły się pomyślnie.



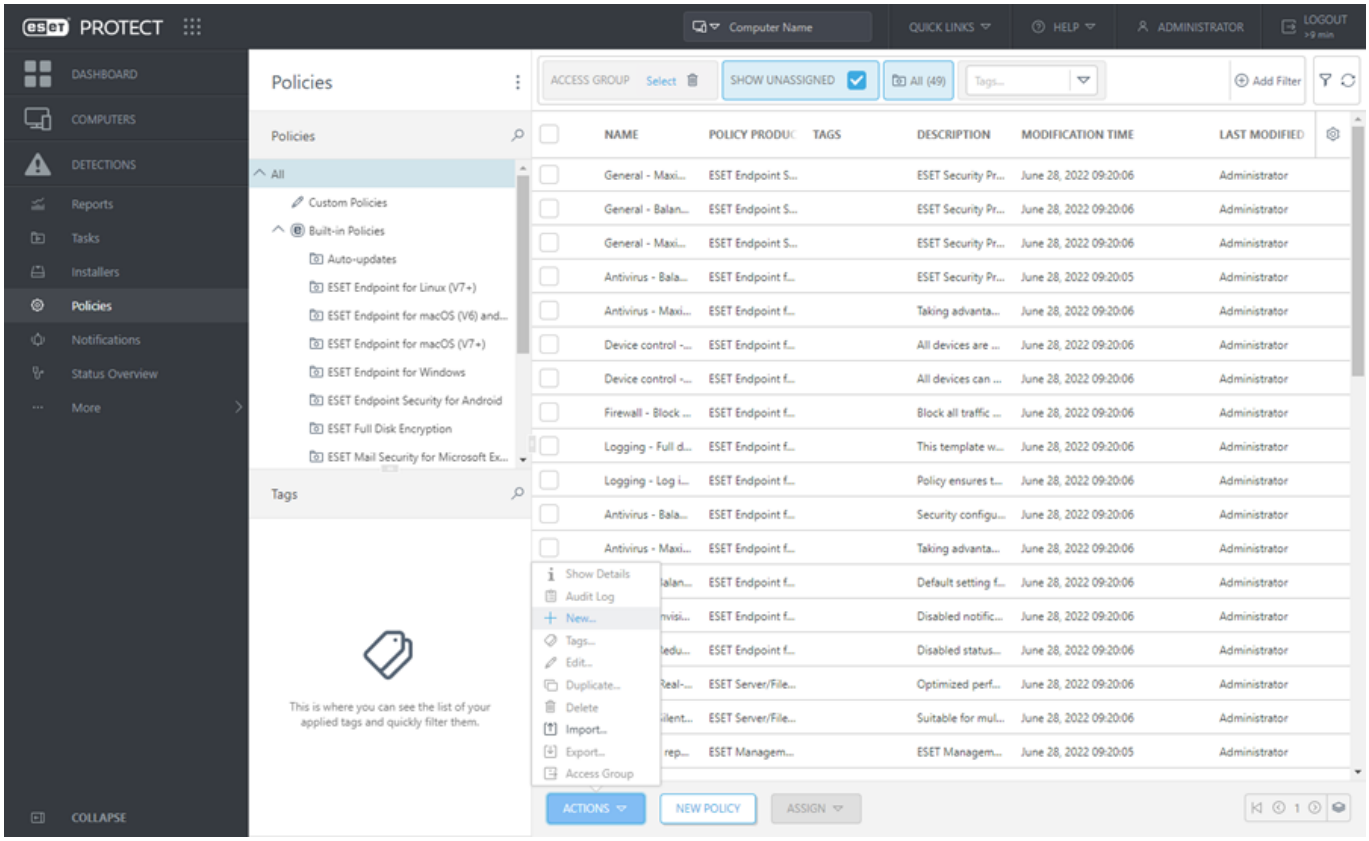
Sekcja Zadania przewodnika administratora produktu ESET PROTECT zawiera informacje dotyczące tworzenia, przypisywania i planowania nowych zadań.

Baza wiedzy firmy ESET obejmuje przykłady procedur konfigurowania określonych zadań, takich jak:

- Wysyłanie sygnału wznowienia do komputerów klienckich w celu natychmiastowego wykonania zadania w produkcie ESET PROTECT.
- Zmiana interwału połączenia agenta dla komputerów klienckich w ESET PROTECT.
- Używanie zadania instalacji oprogramowania klienta, aby wdrożyć lub uaktualnić produkty firmy ESET dla punktów końcowych.
- Synchronizuj ESET PROTECT z usługą Active Directory.

Polityki

Polityki służą do zarządzania komputerami klienckimi. Polityki to zestawy reguł konfiguracji, które można zastosować do produktów firmy ESET uruchomionych na komputerach klienckich, dzięki czemu można uniknąć ręcznego konfigurowania produktu ESET dla każdego klienta. Polityki można zastosować bezpośrednio do poszczególnych komputerów i grup. Do danego komputera lub grupy można ponadto przypisać wiele polityk.



W celu utworzenia nowej polityki i przypisania jej do grupy należy wykonać działania opisane w tym artykule bazy wiedzy.

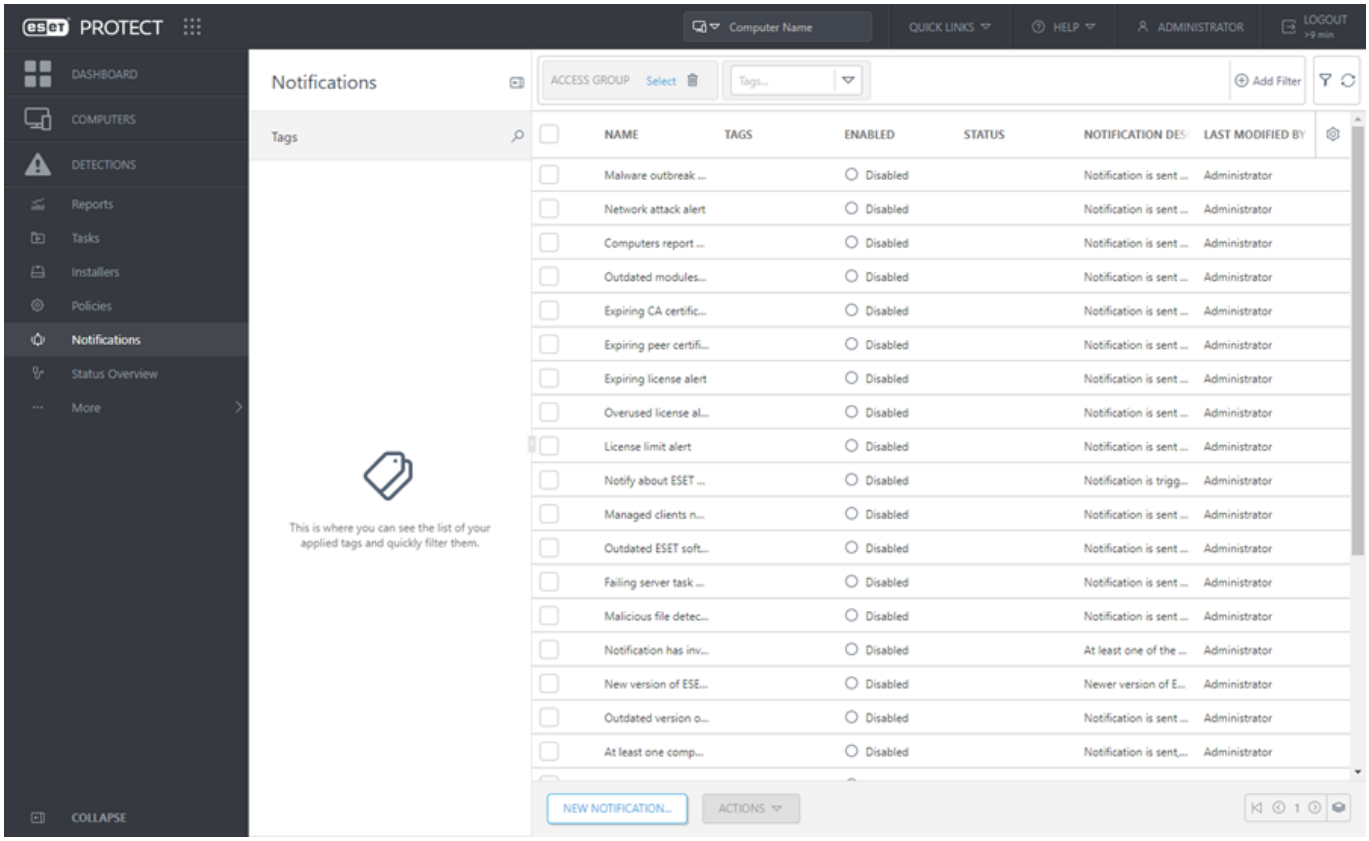
Polityki są stosowane w kolejności, w której uszeregowane są grupy statyczne. Ta reguła nie jest prawidłowa dla grup dynamicznych, w których najpierw uwzględniane są podrzędne grupy dynamiczne, dzięki czemu polityki o większym wpływie mogą znajdować się na szczycie drzewa grup, natomiast bardziej szczegółowe polityki stosowane są w odniesieniu do podgrup.

> Firma ESET zaleca przypisywanie polityk bardziej ogólnych (na przykład ustawień serwera aktualizacji) do grup znajdujących się wyżej w hierarchii drzewa grup. Polityki bardziej szczegółowe (na przykład ustawienia kontroli dostępu do urządzeń) należy stosować głębiej w hierarchii drzewa grup.

Zapoznaj się z sekcją Polityki przewodnika dla administratorów ESET PROTECT, aby dowiedzieć się więcej na temat zarządzania politykami i ich stosowania oraz reguł usuwania polityk.

Powiadomienia

Istnieje możliwość skonfigurowania automatycznych powiadomień generowanych w przypadku określonych zdarzeń, takich jak zgłoszone wykrycia, nieaktualne punkty końcowe itp. Zobacz sekcję Powiadomienia przewodnika dla administratorów ESET PROTECT lub przeczytaj nasz artykuł bazy wiedzy, aby uzyskać więcej informacji na temat konfigurowania powiadomień i zarządzania nimi.



Aby otrzymywać powiadomienia za pośrednictwem poczty e-mail, należy poprawnie skonfigurować połączenie z serwerem SMTP.

W programie ESET PROTECT dostępna jest funkcja automatycznego wysyłania wiadomości e-mail z raportami i powiadomieniami. Włącz opcję **Użyj serwera SMTP**, kliknij **Więcej** > **Ustawienia** > **Ustawienia zaawansowane** > **Serwer SMTP** i skonfiguruj następujące ustawienia:

- **Hosta** — nazwa hosta lub adres IP serwera SMTP.

- **Port** — dla serwera SMTP domyślnie używany jest port 25, jednak to ustawienie można zmienić, gdy serwer SMTP korzysta z innego portu.

- **Nazwa użytkownika** — jeśli serwer SMTP wymaga uwierzytelnienia, podaj nazwę konta użytkownika serwera SMTP (bez nazwy domeny).

- **Hasło** — hasło powiązane z kontem użytkownika serwera SMTP.

- **Typ zabezpieczenia połączenia** — podaj typ połączenia. Wartość domyślna to **Niezabezpieczony**, jednak w przypadku gdy na serwerze SMTP dozwolone są połączenia zabezpieczone, wybierz ustawienie TLS lub STARTTLS. Jeśli chcesz, aby połączenie było bezpieczniejsze, użyj rozszerzenia STARTTLS lub SSL/TLS, w którym do komunikacji szyfrowanej używany jest osobny port.

- **Typ uwierzytelniania** — ustawienie domyślne to **Brak uwierzytelniania**. Jednak z listy rozwijanej można wybrać odpowiedni typ uwierzytelniania (np. Logowanie, CRAM-MD5, CRAM-SHA1, SCRAM-SHA1, NTLM lub Automatyczny).

- **Adres nadawcy** — w tym polu można wpisać adres nadawcy, który będzie wyświetlany w nagłówkach wiadomości e-mail z powiadomieniami (w polu Od:)

- **Testuj serwer SMTP** — ta opcja umożliwia sprawdzenie poprawności ustawień serwera SMTP. Kliknij pozycję

Wyślij testową wiadomość e-mail, aby otworzyć wyskakujące okno. Wprowadź adres e-mail odbiorcy, po czym wiadomość testowa zostanie wysłana na ten adres za pośrednictwem serwera SMTP. Sprawdź, czy testowa wiadomość e-mail trafiła do skrzynki pocztowej odbiorcy.

Jako serwera SMTP można użyć usługi Gmail, jeśli masz konto Gmail. Użyj poniższych ustawień:

Ustawienie	Wartość
Użyj serwera SMTP	*Prawda*
Host	`smtp.gmail.com`
Port	**465** (**TLS**) lub **587** (**STARTTLS**)
Nazwa użytkownika	*Twój adres Gmail*
Hasło	*Twoje hasło Gmail*
Typ zabezpieczenia połączenia	**TLS** lub **STARTTLS**
Typ uwierzytelniania	**Automatic**
Adres nadawcy	*Twój adres Gmail*

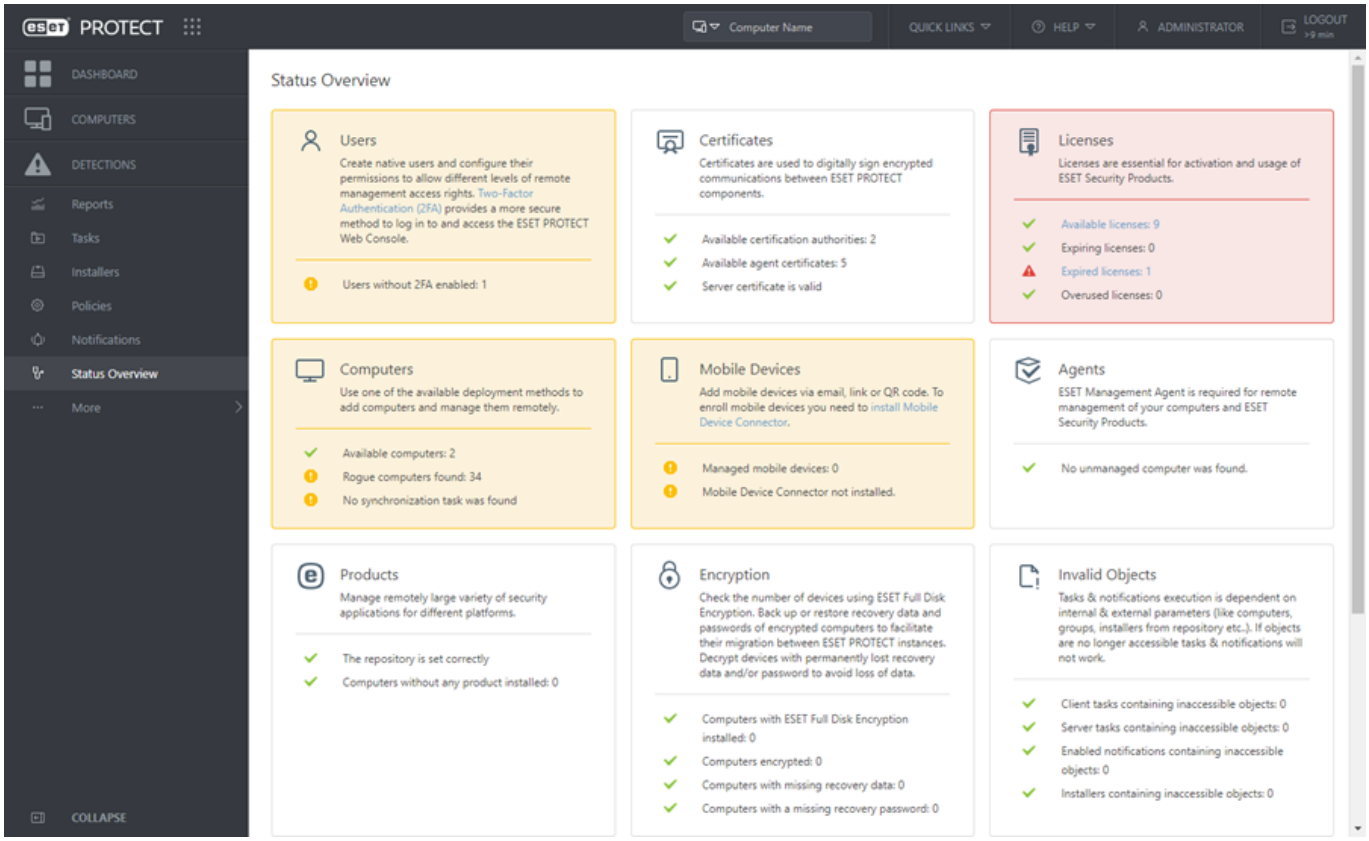
Jeśli wysyłanie wiadomości e-mail nie powiedzie się, może być konieczne zezwolenie na mniej bezpieczne aplikacje na koncie Gmail lub odblokowanie konta Gmail.

Przegląd stanu

Serwer ESET PROTECT wykonuje okresowe kontrole diagnostyczne.

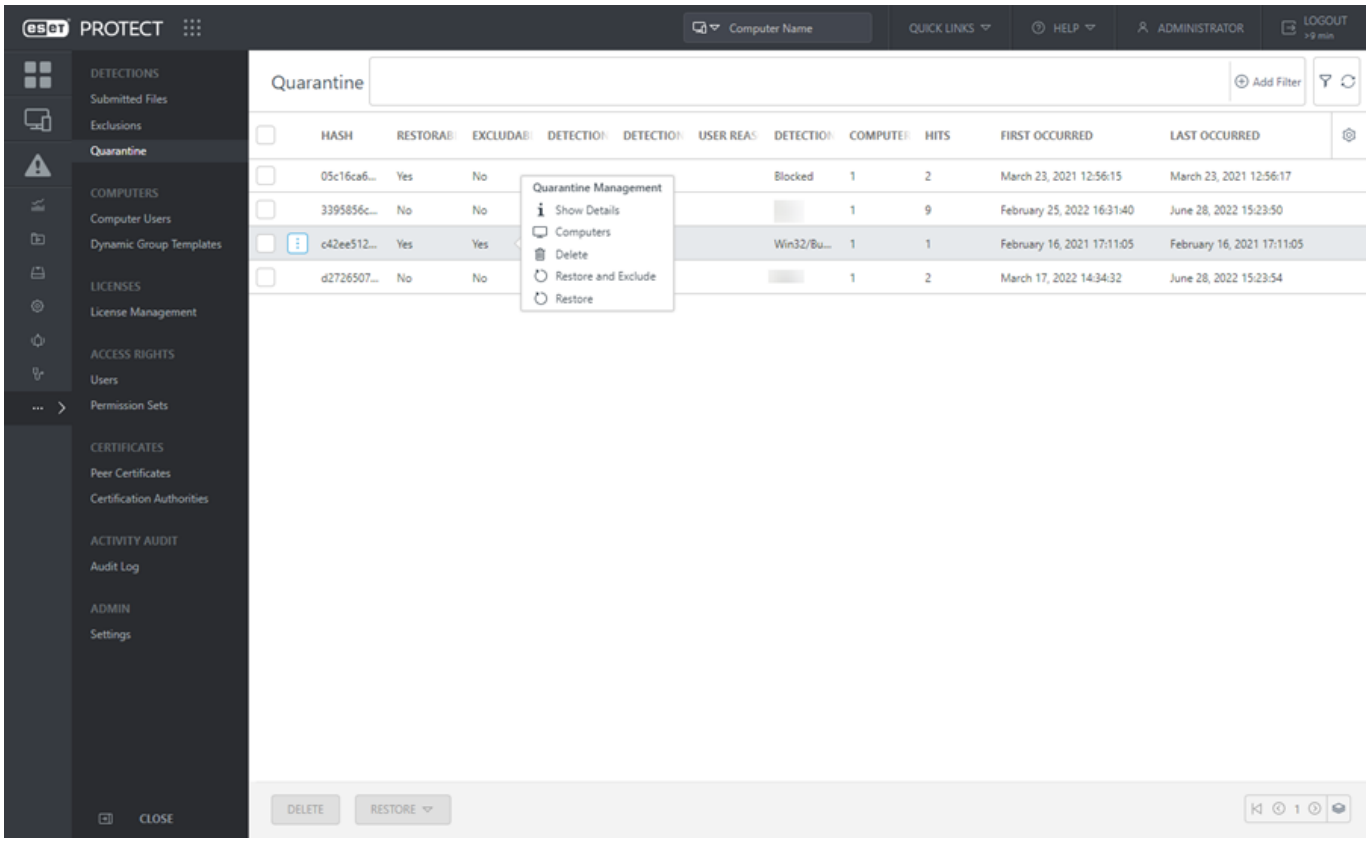
1.Kliknij **Przegląd stanu**, aby wyświetlić szczegółowe informacje na temat stanu produktu ESET PROTECT. **Przegląd stanu** umożliwia wyświetlanie statystyk użytkowania oraz ogólnego stanu produktu ESET PROTECT. Może również ułatwić początkową konfigurację produktu ESET PROTECT.

2.Kliknij kafelek sekcji, aby wyświetlić z prawej pasek zadań z czynnościami.



Kwarantanna

Sekcja Kwarantanna znajduje się w konsoli internetowej w obszarze ⋯ **Więcej** > **Kwarantanna**. Ta sekcja zawiera wszystkie pliki poddane kwarantannie na urządzeniach klienckich.



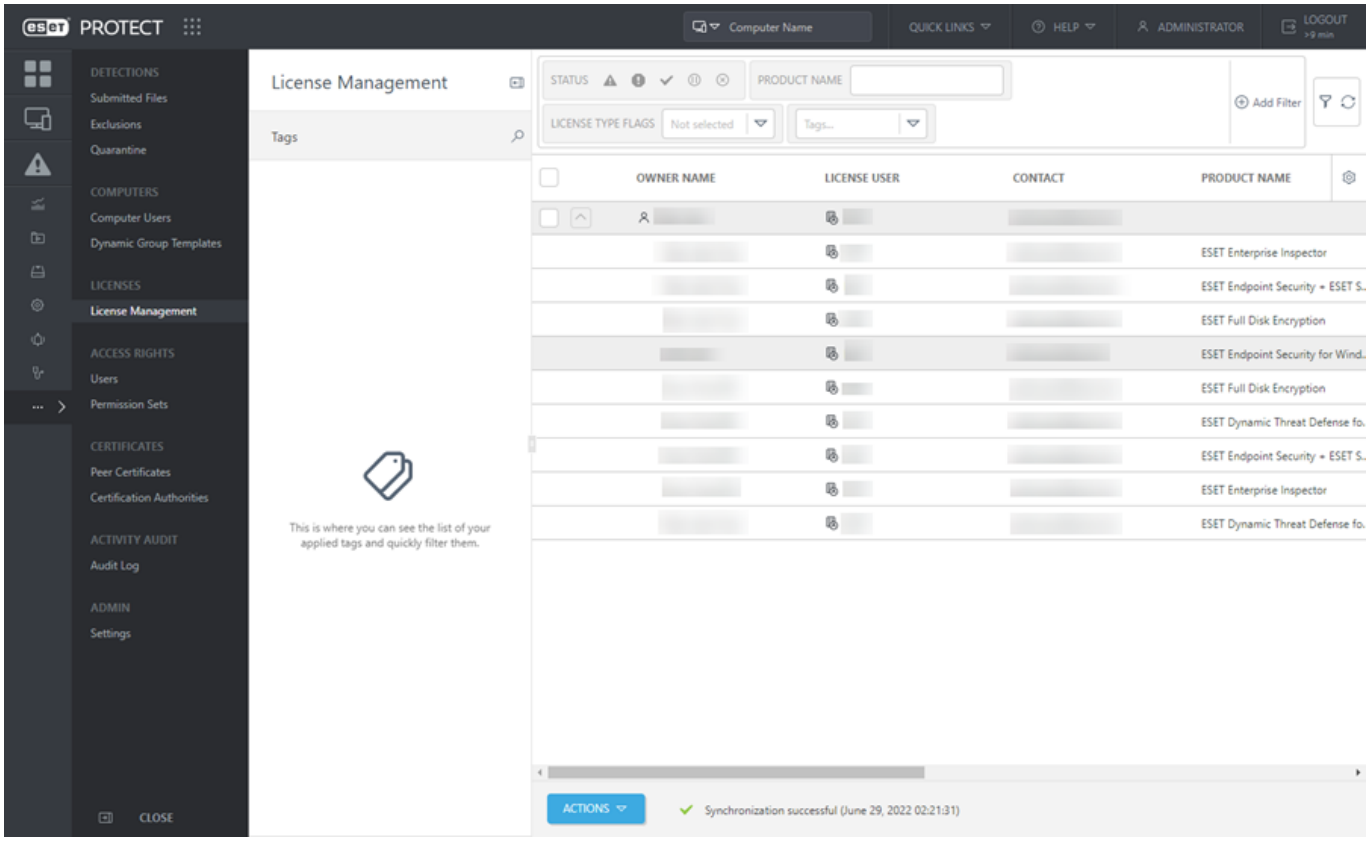
Pliki należy poddawać kwarantannie, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane albo gdy są one nieprawidłowo wykrywane przez program ESET.

Nie wszystkie wykrycia znalezione na urządzeniach klienckich są przenoszone do kwarantanny. Wykrycia, które nie są poddawane kwarantannie, obejmują:
- Wykrycia, których nie można usunąć
- Wykrycia, które są podejrzane ze względu na ich zachowanie, ale nie są identyfikowane jako szkodliwe oprogramowanie, np. potencjalnie niepożądane aplikacje.

Zobacz też artykuł bazy wiedzy ESET dotyczący zarządzania kwarantanną.

Zarządzanie licencjami

Wybierz pozycję **Więcej** > **Zarządzanie licencjami**, aby zarządzać licencjami.



Aby dodać nową licencję w rozwiązaniu ESET PROTECT:

1. Kliknij **Więcej** > **Zarządzanie licencjami**, a następnie kliknij kolejno **Czynności** > **Dodaj licencje**.

2. Wybierz metodę, która ma zostać użyta w celu dodania nowych licencji:

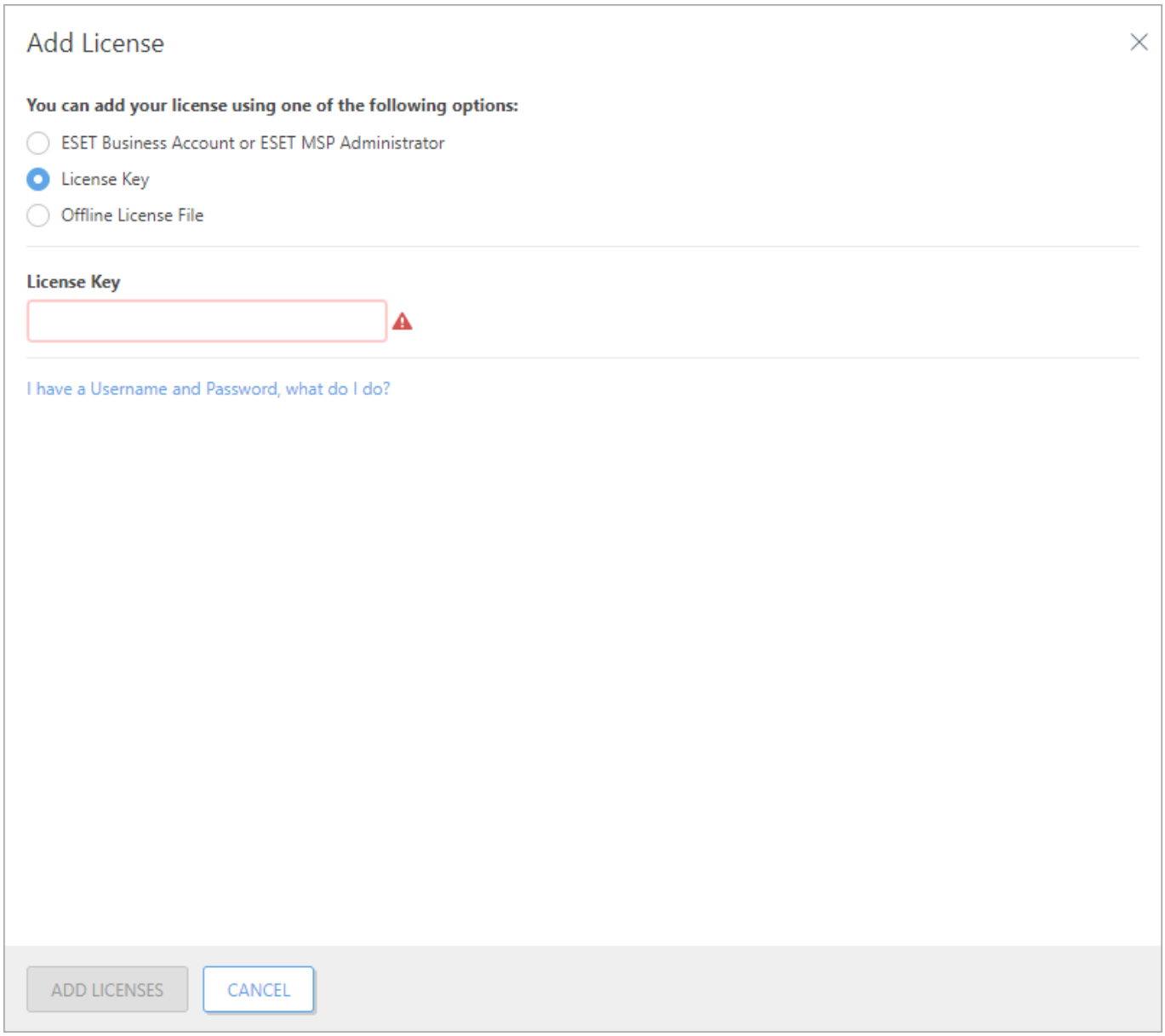
   a. **ESET Business Account lub ESET MSP Administrator** — synchronizuj licencje z konta ESET Business Account lub z konta ESET MSP Administrator z konsolą internetową ESET PROTECT. Teraz można zaimportować pełną strukturę ESET Business Account, w tym dystrybucję stanowisk licencji pomiędzy lokalizacje.

   b. **Klucz licencyjny** — w polu **Klucz licencyjny** wpisz lub wklej klucz licencyjny otrzymany przy zakupie

oprogramowania zabezpieczającego ESET.

c.**Plik licencji offline**.

3.Kliknij przycisk **Dodaj licencje**.



ESET PROTECT obsługuje zarządzanie licencjami subskrypcyjnymi. Możesz dodać taką licencję przy użyciu konta ESET Business Account, konta ESET MSP Administrator lub klucza licencyjnego. Możesz sprawdzić ważność swojej subskrypcji w obszarze **Zarządzanie licencjami** w kolumnie **Ważność** lub klikając **Komputery** > Szczegóły.

Użytkownicy i zestawy uprawnień

ESET PROTECT model zabezpieczeń

Oto główne terminy stosowane w modelu zabezpieczeń:

Termin	Objaśnienie
Grupa domowa	Grupa domowa to miejsce, w którym automatycznie zapisywane są wszystkie obiekty (urządzenia, zadania, szablony itd.) tworzone przez użytkownika. Każdy użytkownik musi mieć dokładnie jedną grupę domową.
Obiekt	Każdy obiekt (komputer, zadanie, polityka, raport lub powiadomienie) znajduje się w grupie statycznej. a dostęp do obiektów jest zawsze skojarzony z grupami, a nie użytkownikami (ułatwia to dodawanie wielu użytkowników, np. na wypadek jeśli jeden z nich jest na urlopie).
Dostęp do grup	Grupa dostępu jest grupą statyczną, która umożliwia użytkownikom filtrowanie lokalizacji obiektu według uprawnień dostępu.
Administrator	Administrator jest użytkownikiem z grupą domową **Wszystko** i pełnym zestawem uprawnień nad grupą.
Uprawnienia dostępu	Uprawnienia dostępu do obiektu lub do wykonania zadania są przyznawane w ramach zestawu uprawnień.
Zestaw uprawnień	Zestaw uprawnień odzwierciedla uprawnienia użytkowników uzyskujących dostęp do konsoli internetowej ESET PROTECT. Zestaw uprawnień określa, co użytkownik może zobaczyć lub zrobić w konsoli internetowej ESET PROTECT. Użytkownikowi można przypisać wiele zestawów uprawnień. Zestawy uprawnień są stosowane wyłącznie do obiektów w zdefiniowanych grupach statycznych.
Funkcjonalność	Funkcjonalność to typ obiektu lub działania. Zwykle funkcjonalność przyjmuje następujące wartości: **Odczyt**, **Zapis** lub **Użyj**. Połączenie funkcjonalności w ramach grupy dostępu nazywa się zestawem uprawnień.

Aby uzyskać bardziej szczegółowe informacje, zobacz sekcję Prawa dostępu w podręczniku administracji ESET PROTECT.

Tworzenie nowego użytkownika konsoli internetowej ESET PROTECT

Nowa konfiguracja produktu ESET PROTECT początkowo ma domyślnego **administratora** (użytkownika z grupą domową **Wszystko** i dostępem do wszystkiego) jako jedynego użytkownika.

Firma ESET nie zaleca używania domyślnego konta użytkownika administratora. Należy utworzyć inne konto administratora. Możesz również utworzyć dodatkowe konta użytkowników z ograniczonym dostępem, bazując na niezbędnych kompetencjach.

Certyfikaty

Certyfikaty

Certyfikaty są istotną częścią produktu ESET PROTECT. Służą one do bezpiecznej komunikacji między składnikami ESET PROTECT a serwerem ESET PROTECT oraz do ustanawiania bezpiecznego połączenia z konsolą internetową ESET PROTECT. Certyfikatami ESET PROTECT można zarządzać w sekcji ··· **Więcej** > **Certyfikaty równorzędne**.

Można użyć certyfikatów, które są generowane automatycznie podczas instalacji ESET PROTECT.

Urzędy certyfikacji

Urząd certyfikacji legitymizuje certyfikaty dystrybuowane z sieci. W środowisku przedsiębiorstwa klucz publiczny służy automatycznemu skojarzeniu oprogramowania klienckiego z serwerem ESET PROTECT w celu umożliwienia zdalnej instalacji produktów firmy ESET. Urzędami certyfikacji ESET PROTECT można zarządzać w sekcji **Więcej** > **Urzędy certyfikacji**.

Wszystkie certyfikaty równorzędne muszą być ważne i podpisane przez ten sam urząd certyfikacji, aby umożliwić komponentom poprawną komunikację.

Aby uzyskać więcej informacji o certyfikatach i urzędzie certyfikacji, przeczytaj artykuł bazy wiedzy ESET lub skorzystaj z Pomocy online.

Pomoc i obsługa

Firma ESET nieustannie pracuje nad uaktualnianiem i usprawnianiem rozwiązania ESET PROTECT oraz produktów ESET do obsługi punktów końcowych.

- Baza wiedzy firmy ESET to zbiór pomocnych artykułów ułatwiających rozwiązywanie problemów z możliwością wyszukiwania odpowiedzi na pytania
- Forum użytkowników rozwiązań firmy ESET to monitorowane przez pracowników firmy ESET forum, na którym użytkownicy produktów firmy ESET mogą omawiać napotkane problemy oraz wyszukiwać rozwiązania.
- Kanał wideo bazy wiedzy firmy ESET to zbiór filmów z objaśnieniem standardowych procedur związanych z produktami firmy ESET.
- Na stronie z informacjami dotyczącymi wsparcia produktów firmy ESET oraz poradami dla klientów można znaleźć najnowsze powiadomienia dotyczące funkcji i uaktualnień produktów firmy ESET.
- W razie trudności z rozwiązaniem problemu lub znalezieniem odpowiedzi na pytanie w dowolnym momencie można skontaktować się z działem obsługi klienta firmy ESET.

Więcej szczegółowych informacji można także znaleźć w Przewodniku po instalacji rozwiązania ESET PROTECT (omówiono tam również uaktualnianie, migrację oraz rozwiązywanie problemów), Podręczniku administratora (zarządzanie rozwiązaniem ESET PROTECT przy użyciu konsoli internetowej ESET PROTECT) oraz Instrukcji wdrażania urządzenia wirtualnego (rozwiązanie ESET PROTECT w hiperwizorze itp.).

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