ESET ENDPOINT SECURITY 6

Podręcznik użytkownika

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2
Kliknij tutaj, aby pobrać najnowszą wersję tego dokumentu

ESET **ENDPOINT SECURITY 6**

Pomoc techniczna dla klientów z całego świata: www.eset.com/support

WER. 1/18/2016

Spis treści

Spis treści

1. ESET Endpoint Security

Program ESET Endpoint Security 6 jest nowym rozwiązaniem zapewniającym w pełni zintegrowaną ochronę komputera przed zagrożeniami. Bezpieczeństwo komputera zapewnia najnowsza wersja aparatu skanowania ThreatSense® o szybkim i precyzyjnym działaniu, w połączeniu z naszymi niestandardowymi modułami zapory osobistej i ochrony przed spamem. W wyniku tego połączenia powstał „inteligentny" system, który w porę ostrzega przed atakami i szkodliwymi aplikacjami zagrażającymi komputerowi.

Program ESET Endpoint Security 6 to kompletne rozwiązanie, które zapewnia wysoki poziom bezpieczeństwa; efekt naszych długotrwałych prac nad uzyskaniem maksymalnej ochrony przy jednoczesnym minimalnym obciążeniu systemu. Zaawansowane techniki oparte na sztucznej inteligencji potrafią z wyprzedzeniem eliminować przenikające do systemu wirusy, aplikacje szpiegujące, konie trojańskie, robaki, oprogramowanie reklamowe i programy typu rootkit oraz inne formy ataków z Internetu, unikając przy tym obniżania wydajności komputera czy zakłócania jego pracy.

Program ESET Endpoint Security 6 jest przeznaczony głównie do użytku na stacjach roboczych w małym środowisku firmowym. Można z niego korzystać w połączeniu z programem ESET Remote Administrator, co pozwala na łatwe zarządzanie dowolną liczbą klienckich stacji roboczych, stosowanie zasad i reguł, monitorowanie procesu wykrywania oraz zdalne konfigurowanie z dowolnego komputera podłączonego do sieci.

1.1 Nowości

Graficzny interfejs użytkownika w programie ESET Endpoint Security został gruntownie zmodyfikowany, by zapewnić większą przejrzystość oraz intuicyjność obsługi. Oto przykłady usprawnień wprowadzonych w wersji 6 programu ESET Endpoint Security:

Usprawnienia funkcjonalności i łatwości obsługi

- Kontrola dostępu do stron internetowych — możliwość ustalenia jednej reguły dla wielu adresów URL oraz różnych zasad w odniesieniu do różnych lokalizacji sieciowych. „Miękkie" zasady blokowania to nowość w wersji 6, podobnie jak możliwość częściowego dostosowania strony blokowania i ostrzeżeń.
- Zapora osobista — reguły zapory można teraz tworzyć bezpośrednio z poziomu dziennika lub okna powiadomień o wykryciu IDS, a ponadto można przypisywać profile do interfejsów sieciowych.
- Nowa funkcja ochrony przed botnetami — ułatwia wykrywanie szkodliwego oprogramowania poprzez analizowanie wzorców komunikacji sieciowej i protokołów.
- Kontrola dostępu do urządzeń — dostępna jest tu obecnie możliwość określenia typu i numeru seryjnego urządzenia oraz zdefiniowania pojedynczych reguł w odniesieniu do wielu urządzeń.
- Nowy tryb inteligentny systemu HIPS — jest to tryb dodatkowy, pośredni między automatycznym a interaktywnym. Umożliwia identyfikowanie podejrzanych działań i szkodliwych procesów w systemie.
- Usprawnienia w programie aktualizacyjnym i kopii dystrybucyjnej — obecnie można wznowić nieudane pobieranie bazy sygnatur wirusów oraz modułów produktu.
- Nowe podejście do obsługi zdalnej komputerów z programem ESET Remote Administrator — ponowne wysyłanie dzienników w przypadku ponownej instalacji serwera ERA lub do celów testowych, zdalne instalowanie oprogramowania zabezpieczającego ESET, pozyskiwanie przeglądu stanu zabezpieczeń środowiska sieciowego oraz sortowanie różnego rodzaju danych w celu ich wykorzystania w przyszłości.
- Usprawnienia w interfejsie użytkownika — dodano opcję uruchamiania ręcznej aktualizacji bazy sygnatur wirusów oraz modułów za pomocą jednego kliknięcia pozycji dostępnej na pasku zadań systemu Windows. Obsługa ekranów dotykowych oraz wyświetlaczy o wysokiej rozdzielczości.
- Usprawnione wykrywanie i usuwanie oprogramowania zabezpieczającego innych firm.

Nowe funkcje

- Ochrona przed atakami typu „phishing" — ochrona użytkownika przed próbami wyłudzenia haseł oraz innych informacji poufnych poprzez ograniczenie dostępu do szkodliwych stron internetowych, które podszywają się pod legalne strony.
- Zwiększenie szybkości skanowania — wykorzystanie lokalnej pamięci podręcznej w środowiskach zwirtualizowanych.

Technologie wykrywania i ochrony

- Zwiększenie szybkości i niezawodności instalacji.
- Zaawansowany skaner pamięci — monitorowanie działania procesów i skanowanie procesów szkodliwych w momencie ich ujawnienia się w pamięci.
- Usprawnienie blokady programów typu Exploit — jej zadaniem jest wzmacnianie ochrony używanych zazwyczaj typów aplikacji, takich jak przeglądarki internetowe, przeglądarki plików PDF, programy poczty e-mail oraz składniki pakietu MS Office. W blokadzie programów typu Exploit dostępna jest teraz obsługa środowiska Java, a ponadto usprawniono wykrywanie tego rodzaju luk w zabezpieczeniach i ochronę przed nimi.
- Usprawnione wykrywanie i usuwanie programów typu rootkit.
- Ochrona przed lukami w systemie zabezpieczeń — bardziej zaawansowane opcje filtrowania, umożliwiające wykrywanie różnego typu ataków i luk w zabezpieczeniach.
- Skaner stanu bezczynności — skanowanie w trybie cichym wszystkich dysków lokalnych, gdy komputer znajduje się w stanie bezczynności.

1.2 Wymagania systemowe

Aby zapewnić płynne działanie programu ESET Endpoint Security, komputer powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

Obsługiwane procesory: Intel® lub AMD x86-x64

Systemy operacyjne: Microsoft® Windows® 10/8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit

1.3 Zapobieganie

Podczas użytkowania komputera — a zwłaszcza w trakcie przeglądania witryn internetowych — należy pamiętać, że żaden program antywirusowy na świecie nie może całkowicie wyeliminować zagrożenia powodowanego przez infekcje i ataki. Aby zapewnić maksymalną ochronę i wygodę, należy korzystać z programu antywirusowego w odpowiedni sposób i przestrzegać kilku użytecznych reguł:

Regularne aktualizowanie

Zgodnie z danymi statystycznymi uzyskanymi dzięki systemowi ESET Live Grid każdego dnia powstają tysiące nowych, unikatowych infekcji mających na celu pokonanie istniejących zabezpieczeń i przyniesienie korzyści ich autorom — wszystko kosztem innych użytkowników. Specjaliści z laboratorium firmy ESET codziennie analizują takie zagrożenia oraz przygotowują i publikują aktualizacje w celu stałego zwiększania poziomu ochrony użytkowników. Aby zapewnić maksymalną efektywność tych aktualizacji, ważna jest ich prawidłowa konfiguracja w systemie. Więcej informacji na temat konfigurowania aktualizacji można znaleźć w rozdziale Ustawienia aktualizacji.

Pobieranie poprawek zabezpieczeń

Twórcy złośliwego oprogramowania często korzystają z rozmaitych luk w zabezpieczeniach komputera, aby zwiększyć skuteczność rozprzestrzeniania się złośliwego kodu. Dlatego producenci oprogramowania starannie wyszukują nowe luki w zabezpieczeniach swoich aplikacji i regularnie publikują aktualizacje zabezpieczeń eliminujące potencjalne zagrożenia. Bardzo ważne jest pobieranie i instalowanie tych aktualizacji zabezpieczeń jak najszybciej po ich opublikowaniu. System Microsoft Windows i przeglądarki internetowe takie, jak Internet Explorer to dwa przykłady programów, dla których aktualizacje zabezpieczeń są wydawane regularnie.

Wykonywanie zapasowych kopii ważnych danych

Autorzy szkodliwego oprogramowania zazwyczaj nie dbają o potrzeby użytkowników, a działanie ich szkodliwych aplikacji często prowadzi do całkowitego zablokowania systemu operacyjnego i utraty ważnych danych. Dlatego ważne jest regularne wykonywanie zapasowych kopii ważnych i poufnych informacji na nośniku zewnętrznym, np. na płycie DVD czy zewnętrznym dysku twardym. To znacznie ułatwia i przyspiesza odzyskanie danych w razie awarii komputera.

Regularne skanowanie komputera w celu wykrycia wirusów

Wykrywanie znanych i nieznanych wirusów, robaków, koni trojańskich oraz programów typu rootkit jest

wykonywane przez moduł ochrony w czasie rzeczywistym. Oznacza to, że każda operacja dostępu do pliku lub jego otwarcia powoduje skanowanie go pod kątem aktywności szkodliwego oprogramowania. Zalecamy jednak wykonywanie skanowania komputera przynajmniej raz w miesiącu, ponieważ sygnatury wirusów mogą się zmieniać a bazy danych sygnatur wirusów są aktualizowane codziennie.

Przestrzeganie podstawowych zasad bezpieczeństwa

To najpożyteczniejsza i najskuteczniejsza reguła ze wszystkich: należy zawsze zachowywać ostrożność. Obecnie wiele infekcji wymaga interwencji użytkownika w celu wykonania kodu i rozpowszechnienia zagrożenia. Jeśli użytkownik będzie ostrożny podczas otwierania nowych plików, zaoszczędzi sporo czasu i wysiłku, które w innym wypadku musiałby poświęcić na leczenie infekcji. Oto kilka przydatnych wskazówek:

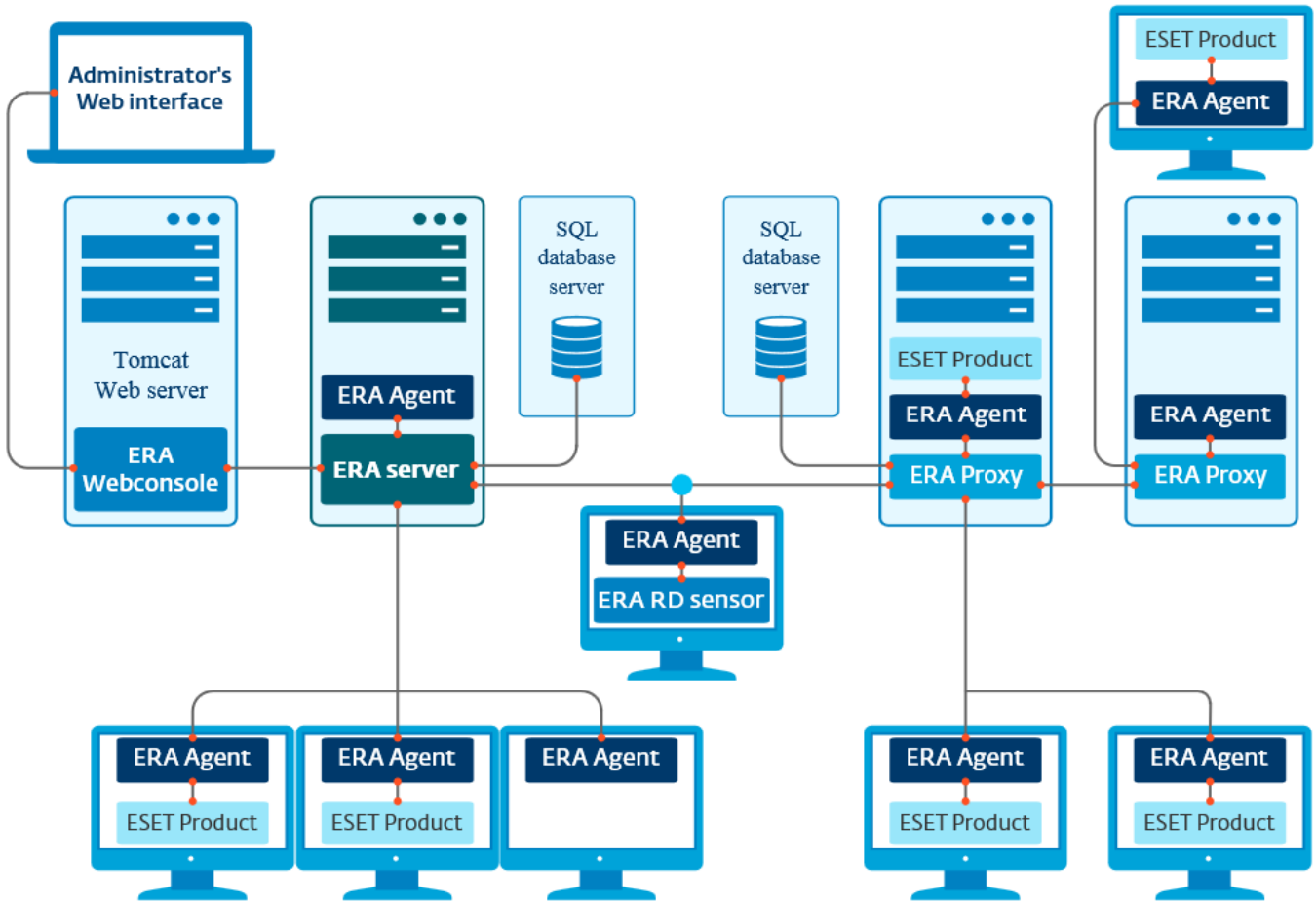
- nie należy odwiedzać podejrzanych witryn internetowych o wielu wyskakujących oknach i napastliwych reklamach;
- należy zachowywać ostrożność przy instalowaniu bezpłatnych programów, zestawów koderów-dekoderów itp. — trzeba korzystać tylko z bezpiecznych programów i odwiedzać jedynie bezpieczne witryny internetowe;
- należy uważać przy otwieraniu załączników do wiadomości e-mail, zwłaszcza w przypadku wiadomości kierowanych do wielu adresatów i pochodzących od nieznanych nadawców;
- Przy codziennym użytkowaniu komputera nie należy korzystać z konta administratora.

2. Dokumentacja dla użytkowników połączonych przy użyciu rozwiązania ESET Remote Administrator

ESET Remote Administrator (ERA) to aplikacja umożliwiająca zarządzanie produktami firmy ESET w środowisku sieciowym z jednej lokalizacji centralnej. System zarządzania zadaniami ESET Remote Administrator umożliwia instalowanie oprogramowania zabezpieczającego ESET na komputerach zdalnych oraz szybkie reagowanie na nowe problemy i zagrożenia. ESET Remote Administrator samodzielnie nie zapewnia ochrony przed szkodliwym kodem. Do tego niezbędne jest zainstalowanie oprogramowania zabezpieczającego ESET na każdym z klientów.

Oprogramowanie zabezpieczające ESET obsługuje sieci obejmujące platformy różnego typu. Sieć może stanowić połączenie aktualnych systemów operacyjnych firmy Microsoft, systemów operacyjnych Linux i Mac OS oraz systemów wykorzystywanych w urządzeniach mobilnych (telefony komórkowe i tablety).

Poniższa ilustracja przedstawia przykładową architekturę sieci chronionej przez oprogramowanie zabezpieczające ESET zarządzane przy pomocy narzędzia ERA:



UWAGA: Więcej informacji zawiera Podręcznik użytkownika programu ESET Remote Administrator.

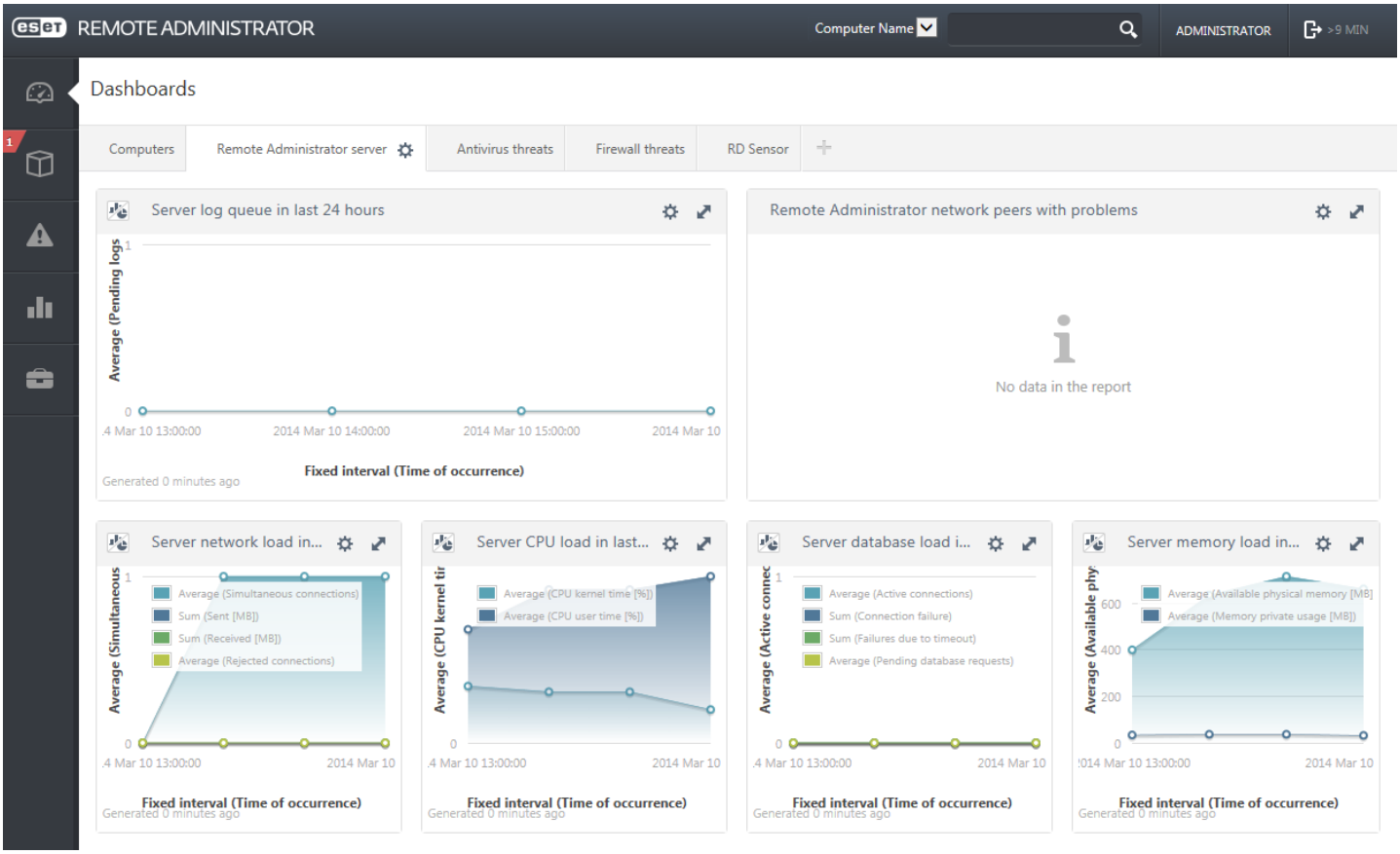
2.1 Serwer ESET Remote Administrator

Serwer administracji zdalnej ESET jest głównym komponentem programu ESET Remote Administrator. To aplikacja wykonawcza przetwarzająca wszystkie dane otrzymywane od klientów nawiązujących połączenia z serwerem (za pośrednictwem agenta ERA). Agent ERA usprawnia komunikację pomiędzy klientem a serwerem. Dane (dzienniki klienta, konfiguracja, replikacja agenta itp.) są przechowywane w bazie danych. Do prawidłowego przetworzenia danych przez serwer ERA wymagane jest stabilne połączenie z serwerem bazy danych. W celu zoptymalizowania wydajności zalecane jest zainstalowanie serwera ERA i bazy danych na oddzielnych serwerach. Komputer, na którym zainstalowany jest serwer ERA, musi być tak skonfigurowany, by akceptować wszystkie połączenia Agent/Proxy/RD Sensor, które są weryfikowane przy użyciu certyfikatów. Po jego zainstalowaniu można otwierać konsolę internetową ERA, która łączy się z serwerem ERA (co widać na ilustracji). Za pomocą konsoli internetowej przeprowadzane są wszystkie operacje serwera ERA dotyczące zarządzania programami zabezpieczającymi ESET.

2.2 Konsola internetowa

Konsola internetowa ERA to sieciowy interfejs użytkownika, który prezentuje dane z serwera ERA i umożliwia zarządzanie oprogramowaniem zabezpieczającym ESET z poziomu sieci użytkownika. Do konsoli internetowej można uzyskać dostęp za pomocą przeglądarki internetowej. Umożliwia wyświetlanie podsumowania stanu klientów w danej sieci i może być używana do zdalnego wdrażania rozwiązań ESET na niezarządzanych komputerach. Jeśli użytkownik zdecyduje się, by serwer internetowy był dostępny przez Internet, może używać programu ESET Remote Administrator z praktycznie dowolnego miejsca, za pomocą dowolnego urządzenia.

To jest panel kontrolny konsoli internetowej:



Narzędzie **Szybkie wyszukiwanie** znajduje się w górnej części konsoli internetowej. Z menu rozwijanego należy wybrać opcję **Nazwa komputera**, **Adres IPv4/IPv6** lub **Nazwa zagrożenia**, wpisać wyszukiwany ciąg w polu tekstowym i kliknąć symbol szkła powiększającego lub nacisnąć klawisz **Enter**, by rozpocząć wyszukiwanie. Spowoduje to przekierowanie do sekcji **Grupy**, gdzie zostanie wyświetlony wynik wyszukiwania.

UWAGA: Więcej informacji zawiera Podręcznik użytkownika programu ESET Remote Administrator.

2.3 Serwer proxy

Serwer proxy ERA to jeden z komponentów programu ESET Remote Administrator, który służy do realizacji dwóch celów. W przypadku sieci średniej wielkości lub sieci firmowej z wieloma klientami (na przykład od 10 000 klientów wzwyż) można korzystać z serwera proxy ERA w celu dystrybuowania obciążeń pomiędzy wieloma serwerami proxy ERA, co umożliwia usprawnienie działania głównego serwera ERA. Kolejną zaletą serwera proxy ERA jest to, że można go użyć w celu nawiązania połączenia ze zdalnym biurem oddziału, w którym dostępne jest słabe łącze. Oznacza to, że agent ERA na każdym z klientów nie łączy się z głównym serwerem ERA bezpośrednio, lecz przez serwer proxy ERA znajdujący się w tej samej lokalnej sieci oddziału. Taka konfiguracja uwalnia łącze do oddziału. Serwer proxy ERA przyjmuje połączenia ze wszystkich lokalnych agentów ERA, kompiluje pobrane od nich dane i przesyła je do głównego serwera ERA (lub do innego serwera proxy ERA). Umożliwia to umieszczenie w sieci większej liczby klientów bez obniżenia sprawności działania sieci oraz jakości kwerend bazy danych.

W zależności od konfiguracji sieci serwer proxy ERA może łączyć się z innym serwerem proxy ERA, a następnie z serwerem głównym ERA.

Aby serwer proxy ERA funkcjonował poprawnie, komputer, na którym zainstalowany jest serwer proxy ERA, musi mieć zainstalowanego agenta ESET i być połączony z wyższym poziomem sieci (serwerem ERA lub wyższym w hierarchii serwerem proxy ERA, jeśli taki istnieje).

2.4 Agent

Agent ERA to podstawowy element produktu ESET Remote Administrator. Oprogramowanie zabezpieczające ESET na komputerach klienckich (na przykład ESET Endpoint Security) komunikuje się z serwerem ERA za pośrednictwem agenta. Taka komunikacja umożliwia zarządzanie oprogramowaniem zabezpieczającym ESET na wszystkich klientach zdalnych z jednej centralnej lokalizacji. Agent gromadzi informacje pozyskiwane od klienta i wysyła je do serwera. Gdy serwer wysyła zadanie do klienta, przesyła je do agenta, który następnie nawiązuje komunikację z klientem. Całość komunikacji w sieci odbywa się pomiędzy agentem oraz górną warstwą sieci ERA, którą stanowi serwer oraz serwer proxy.

Agent ESET łączy się z serwerem przy użyciu jednej spośród trzech metod opisanych poniżej:

1. Agent klienta jest bezpośrednio połączony z serwerem.
2. Agent klienta jest połączony przy użyciu serwera proxy, który jest połączony z serwerem.
3. Agent klienta jest połączony z serwerem za pośrednictwem wielu serwerów proxy.

Agent ESET komunikuje się z rozwiązaniami ESET zainstalowanymi na kliencie, gromadzi informacje pozyskiwane z programów na tym kliencie, a także przekazuje do klienta informacje uzyskane od serwera.

UWAGA: Serwer proxy ESET jest wyposażony we własnego agenta, który obsługuje wszystkie zadania związane z komunikacją pomiędzy klientami, innymi serwerami proxy oraz serwerem.

2.5 RD Sensor

RD (Rogue Detection) Sensor jest elementem programu ESET Remote Administrator, który służy do wyszukiwania komputerów w sieci. W wygodny sposób umożliwia dodawania nowych komputerów w programie ESET Remote Administrator bez konieczności ich ręcznego wyszukiwania i dodawania. Każdy z komputerów znalezionych w sieci zostaje wyświetlony w konsoli internetowej oraz dodany do domyślnej grupy **Wszystkie**. W tym miejscu można podjąć dalsze działania związane z poszczególnymi komputerami klienckimi.

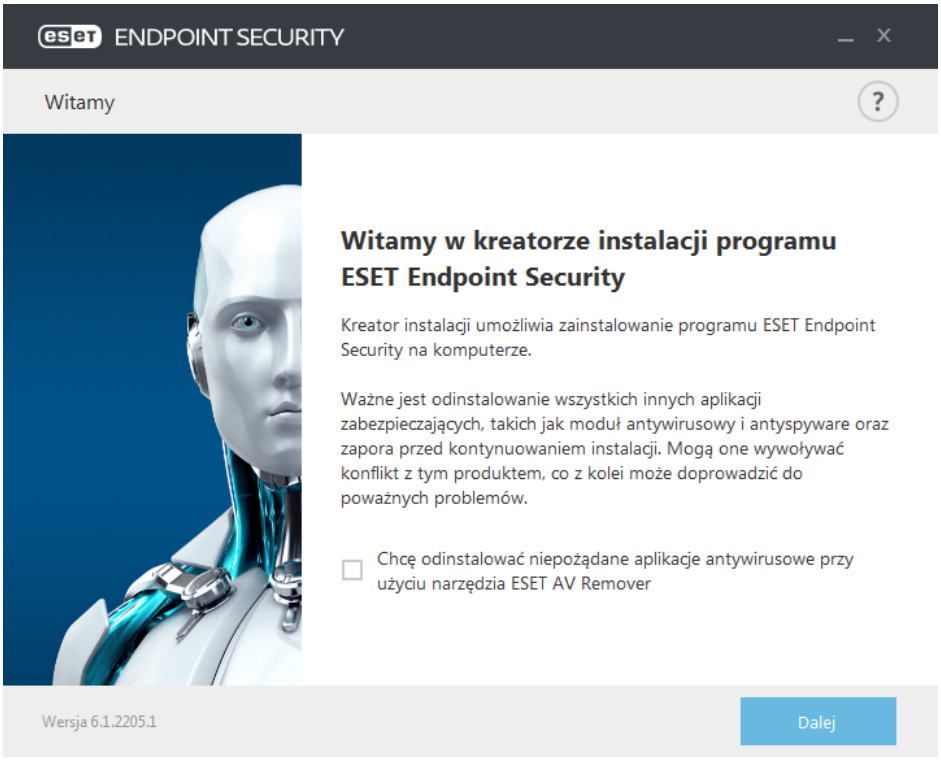
Działanie narzędzia RD Sensor opiera się na nasłuchu pasywnym, co umożliwia wykrywanie komputerów znajdujących się w sieci oraz wysyłanie informacji o nich do serwera ERA. Serwer ERA ocenia, czy komputery znalezione w sieci są nieznane, czy może są już obsługiwane.

3. Korzystanie z samego programu ESET Endpoint Security

Ta część podręcznika użytkownika przeznaczona jest dla użytkowników korzystających z programu ESET Endpoint Security bez programu ESET Remote Administrator. W zależności od uprawnień konta użytkownik może mieć dostęp do wszystkich funkcji programu ESET Endpoint Security.

3.1 Instalacja z użyciem narzędzia ESET AV Remover

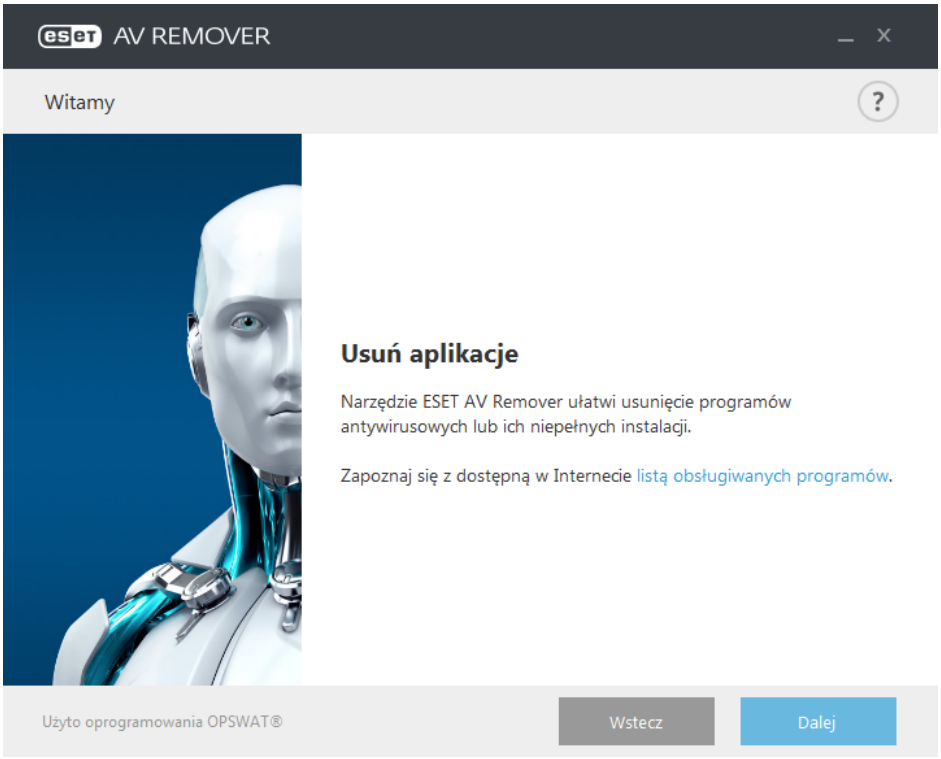
Ważne jest, aby przed przystąpieniem do instalacji odinstalować wszystkie inne aplikacje zabezpieczające zainstalowane aktualnie na komputerze. Zaznacz pole wyboru obok pozycji **Chcę odinstalować niepożądane aplikacje antywirusowe przy użyciu narzędzia ESET AV Remover**, aby umożliwić przeskanowanie systemu przy użyciu narzędzia ESET AV Remover i usunięcie obsługiwanych aplikacji zabezpieczających. Pozostaw pole wyboru bez zaznaczenia i kliknij opcję **Dalej**, aby zainstalować produkt ESET Endpoint Security bez uruchamiania narzędzia ESET AV Remover.



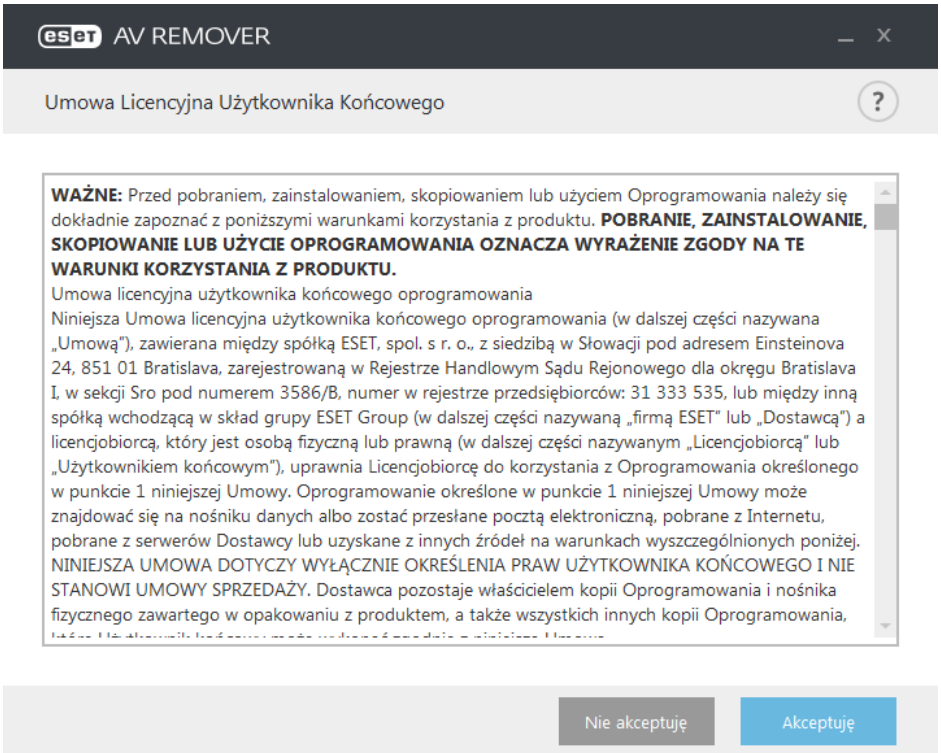
3.1.1 ESET AV Remover

Narzędzie ESET AV Remover ułatwia usuwanie niemal wszystkich programów antywirusowych, które były wcześniej zainstalowane w systemie. W celu usunięcia istniejącego programu antywirusowego przy użyciu narzędzia ESET AV Remover należy wykonać poniższe instrukcje:

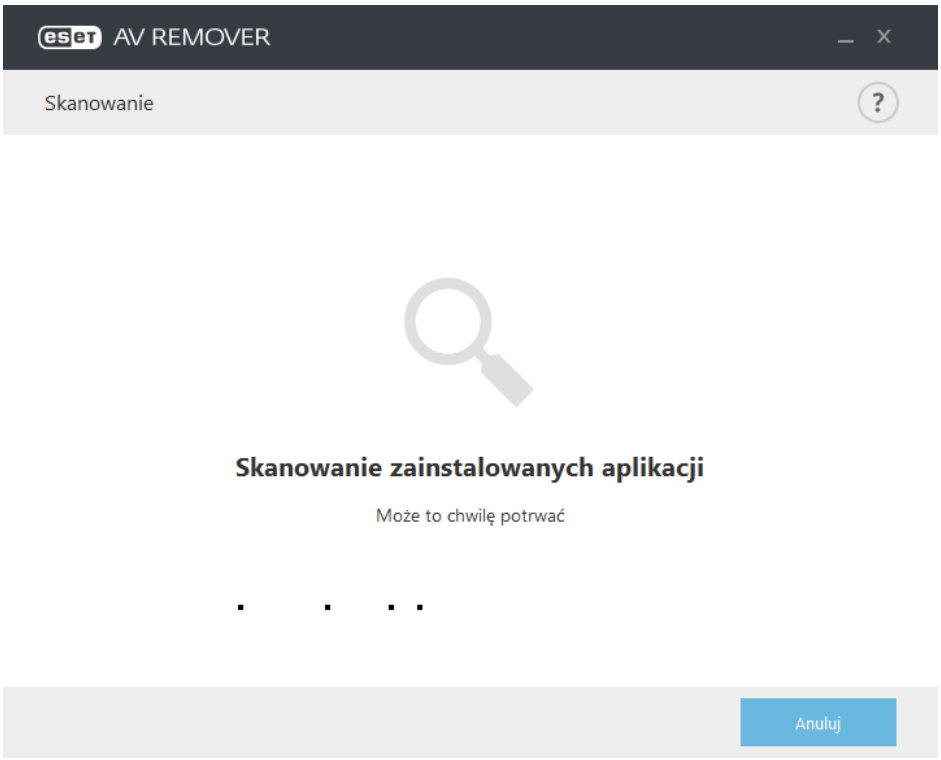
1. Aby wyświetlić listę programów antywirusowych, które można usunąć przy użyciu narzędzia ESET AV Remover, przejdź do odpowiedniego artykułu bazy wiedzy ESET.



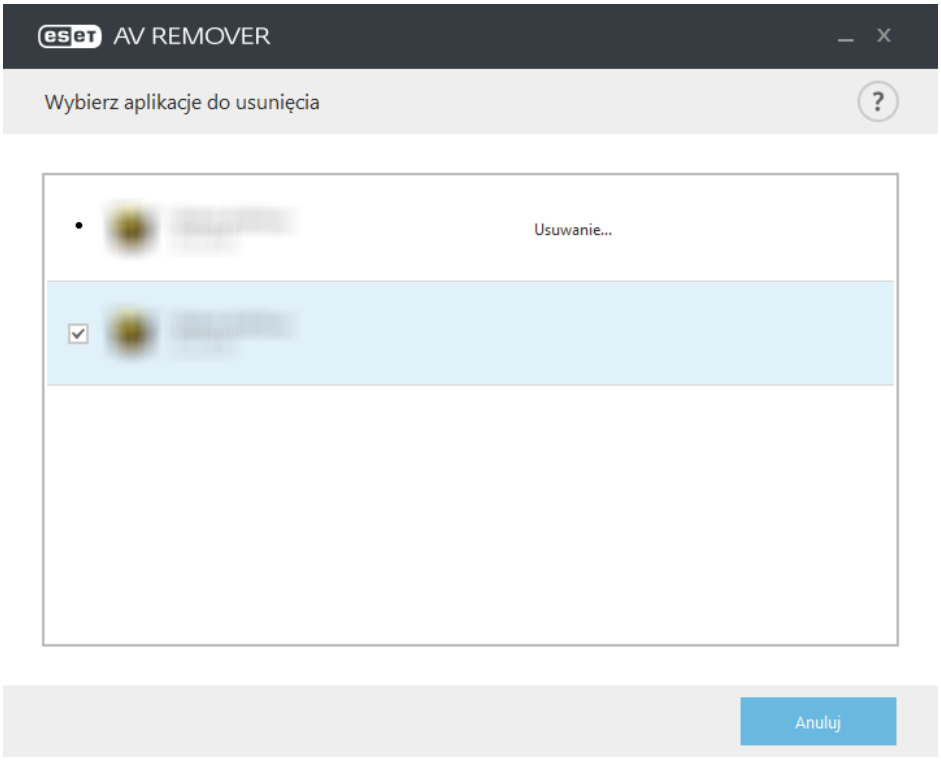
2. Przeczytaj Umowę Licencyjną Użytkownika Końcowego i kliknij przycisk **Akceptuj**, aby potwierdzić jej akceptację. Kliknięcie przycisku **Nie akceptuję** spowoduje przejście do dalszej instalacji produktu ESET Endpoint Security bez usuwania istniejącego oprogramowania zabezpieczającego zainstalowanego na komputerze.



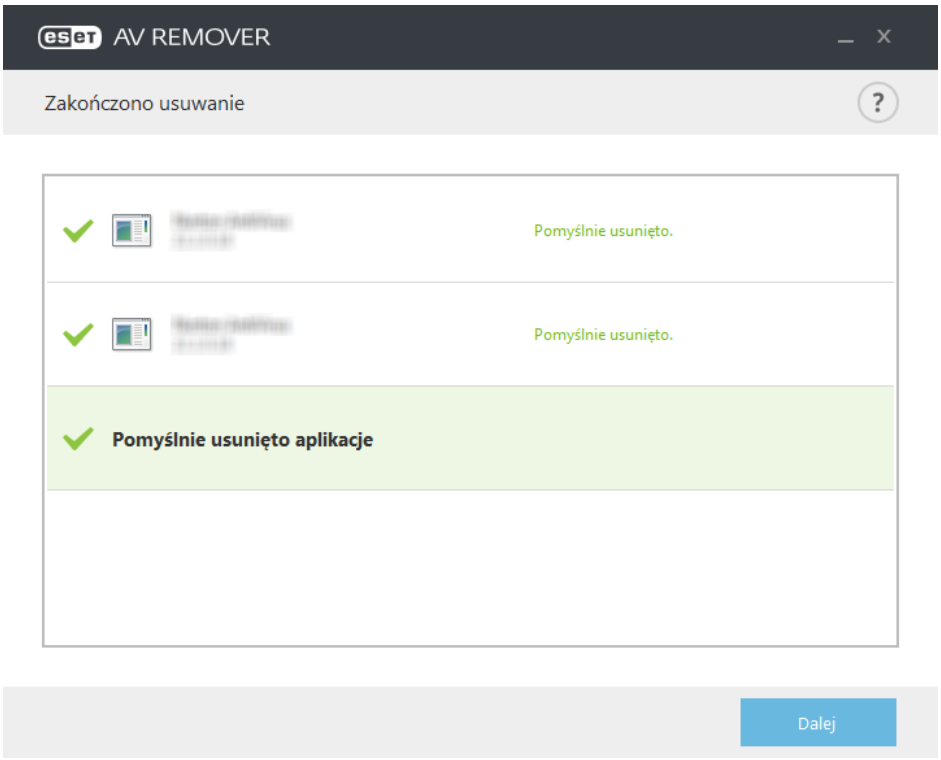
3. Narzędzie ESET AV Remover rozpocznie przeszukiwanie systemu pod kątem oprogramowania antywirusowego.



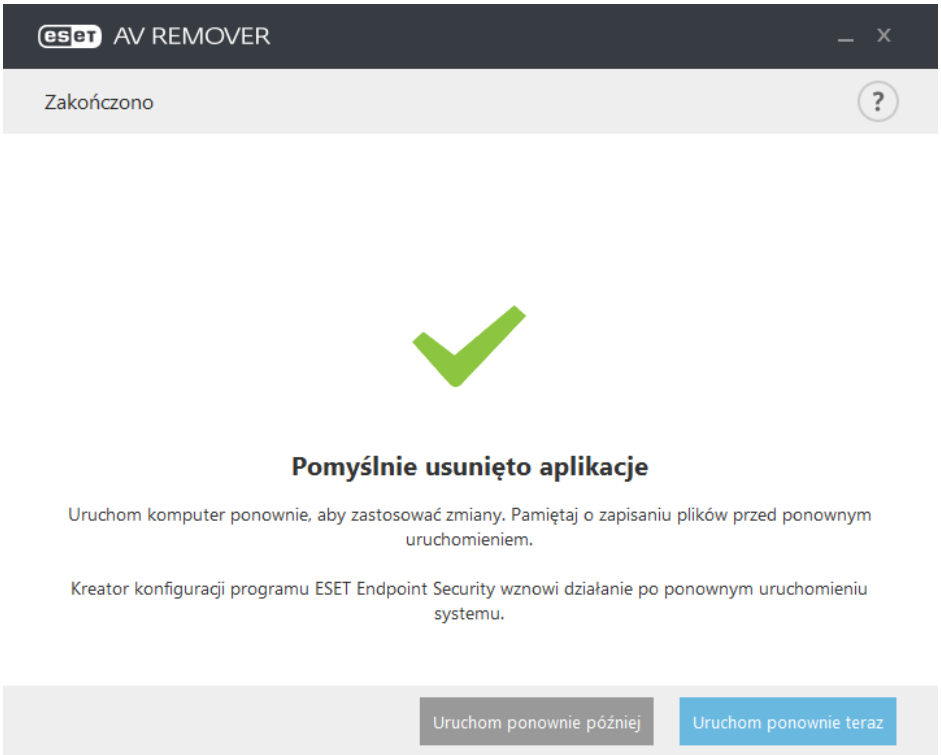
4. Wybierz dowolną z wymienionych na liście aplikacji antywirusowych i kliknij opcję Usuń. Usuwanie może chwilę potrwać.



5. Po pomyślnym usunięciu kliknij przycisk **Dalej**.



6. Uruchom komputer ponownie, aby zastosować zmiany i kontynuuj instalowanie programu ESET Endpoint Security. Jeśli odinstalowywanie zakończy się niepowodzeniem, zapoznaj się z częścią Proces odinstalowania przy użyciu narzędzia ESET AV Remover zakończył się błędem w niniejszej instrukcji.



3.1.2 Proces odinstalowania przy użyciu narzędzia ESET AV Remover zakończył się błędem

Jeśli usunięcie programu antywirusowego przy użyciu narzędzia ESET AV Remover okaże się niemożliwe, zostanie wyświetlone powiadomienie z informacją, że odinstalowywana aplikacja może nie być obsługiwana przez narzędzie ESET AV Remover. Informacje na temat możliwości usunięcia danego programu można znaleźć na liście obsługiwanych produktów lub w artykule dotyczącym narzędzi do odinstalowywania programów antywirusowych dla systemu Windows w bazie wiedzy firmy ESET.

Gdy odinstalowanie produktu zabezpieczającego zakończy się niepowodzeniem lub część komponentów produktu zostanie odinstalowanych częściowo, zostanie wyświetlony monit o **ponowne uruchomienie i ponowne przeprowadzenie skanowania**. Po uruchomieniu należy potwierdzić dane kontroli konta użytkownika i przystąpić do procedury skanowania i odinstalowania.

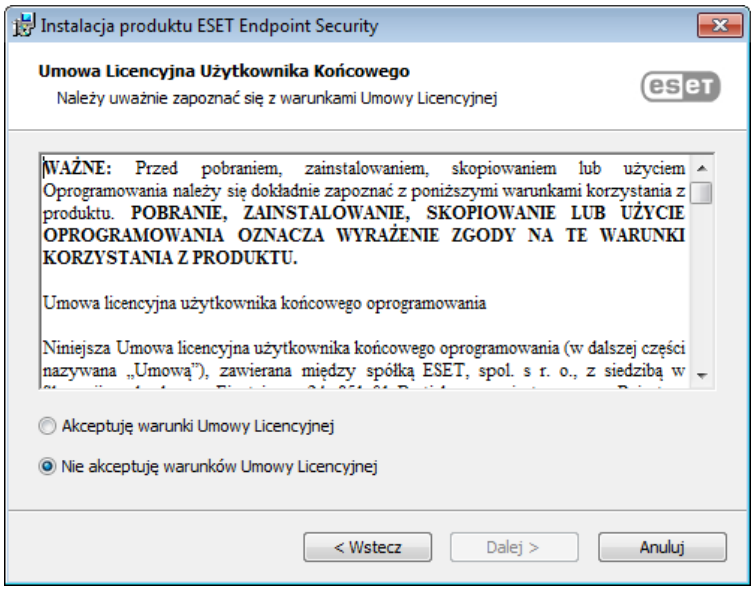
W razie konieczności należy skontaktować się z działem obsługi klienta firmy ESET w celu przesłania zgłoszenia oraz udostępnić plik **AppRemover.log** technikom firmy ESET. Plik **AppRemover.log** znajduje się w folderze **eset**. Aby uzyskać dostęp do tego folderu, w Eksploratorze Windows należy przejść do obszaru *%TEMP%*. Pracownicy działu obsługi klienta firmy ESET odpowiedzą jak najszybciej, by pomóc w rozwiązaniu problemu.

3.2 Instalacja

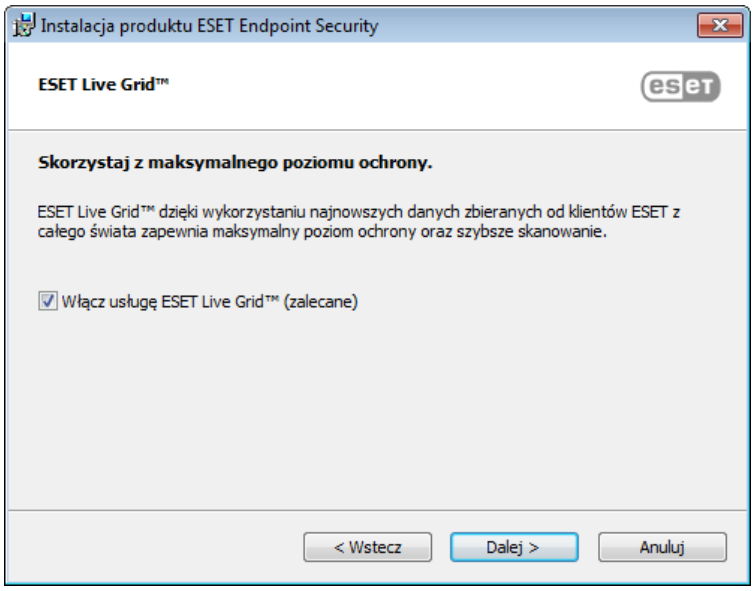
Po uruchomieniu programu instalacyjnego kreator instalacji poprowadzi użytkownika przez procedurę instalacji.

Ważne: Należy się upewnić, że na komputerze nie ma zainstalowanych innych programów antywirusowych. Zainstalowanie na pojedynczym komputerze dwóch lub więcej rozwiązań antywirusowych może powodować wystąpienie konfliktów. Zaleca się odinstalowanie innych programów antywirusowych znajdujących się w systemie. Listę narzędzi do odinstalowywania popularnych programów antywirusowych (dostępną w języku angielskim i w kilku innych językach) można znaleźć w artykule w naszej bazie wiedzy.

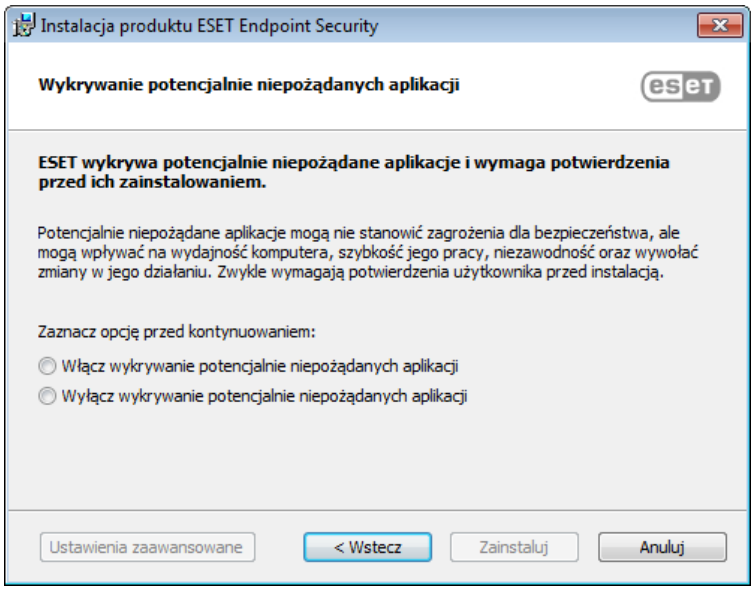
W następnym kroku zostanie wyświetlona Umowa Licencyjna Użytkownika Końcowego. Aby potwierdzić akceptację Umowy Licencyjnej Użytkownika Końcowego, należy ją przeczytać i kliknąć przycisk **Akceptuj**. Po zaakceptowaniu warunków umowy należy kliknąć przycisk **Dalej**, aby kontynuować instalację.



Po wybraniu pozycji „Akceptuję..." i kliknięciu przycisku **Dalej** zostanie wyświetlony monit o skonfigurowanie usługi ESET Live Grid. Usługa ESET Live Grid ułatwia natychmiastowe i ciągłe informowanie firmy ESET o nowych zagrożeniach, co usprawnia ochronę klientów. System umożliwia zgłaszanie nowych zagrożeń do laboratorium firmy ESET, gdzie są one analizowane, przetwarzane i dodawane do bazy sygnatur wirusów.



Kolejnym krokiem w procedurze instalacji jest skonfigurowanie wykrywania potencjalnie niepożądanych aplikacji, które niekoniecznie są szkodliwe, ale często mogą negatywnie wpływać na działanie systemu operacyjnego. Więcej informacji można znaleźć w rozdziale Potencjalnie niepożądane aplikacje. Dostęp do ustawień dodatkowych można uzyskać, klikając pozycję **Ustawienia zaawansowane** (np. w celu zainstalowania produktu ESET w określonym folderze lub w celu włączenia automatycznego skanowania po zainstalowaniu).



Ostatnią czynnością jest potwierdzenie instalacji poprzez kliknięcie przycisku **Zainstaluj**.

3.2.1 Instalacja zaawansowana

Instalacja zaawansowana umożliwia dostosowanie różnych parametrów instalacji niedostępnych podczas typowej instalacji.

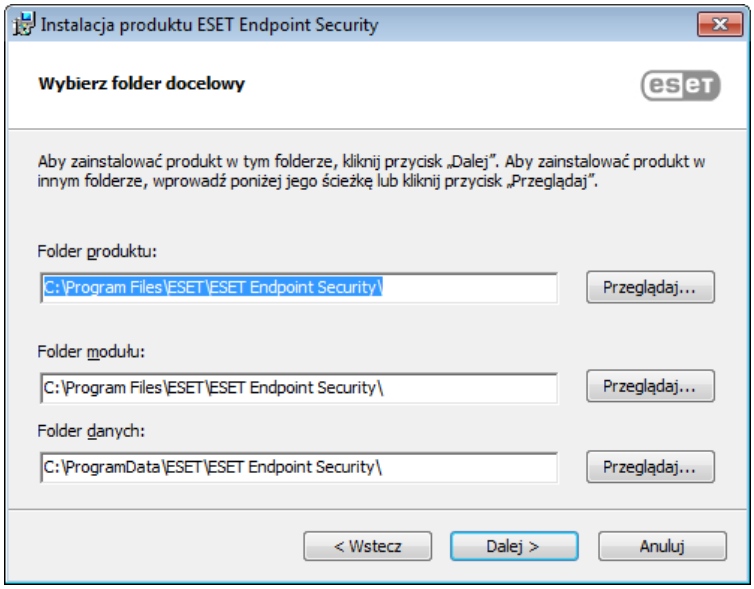
Po wybraniu preferencji wykrywania potencjalnie niepożądanych aplikacji i kliknięciu opcji **Ustawienia zaawansowane** zostanie wyświetlony monit o wybranie miejsca na folder instalacyjny produktu. Domyślnie program instaluje się w następującym katalogu:

C:\Program Files\ESET\ESET Endpoint Security

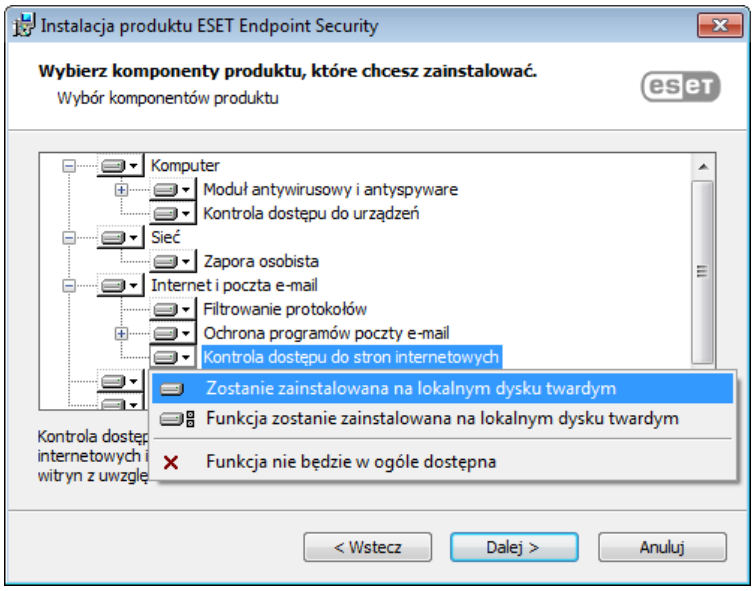
Można wybrać lokalizację modułów i danych programu. Domyślnie są instalowane w następujących katalogach:

C:\Program Files\ESET\ESET Endpoint Security
C:\ProgramData\ESET\ESET Endpoint Security

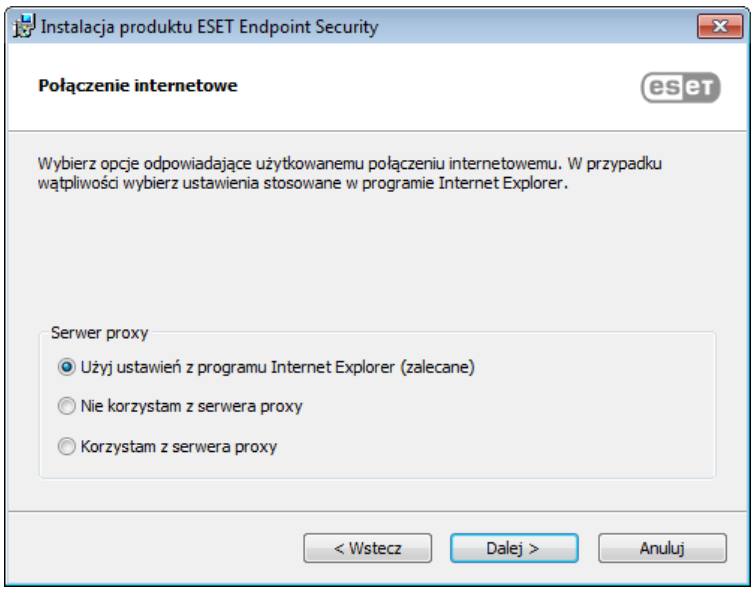
Aby zmienić te lokalizacje, należy kliknąć przycisk **Przeglądaj...** (niezalecane).



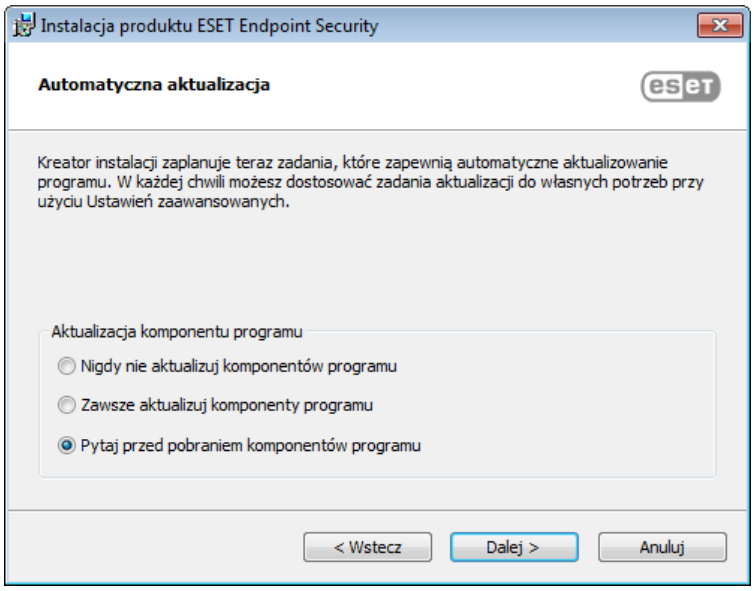
W następnym oknie można wybrać, które komponenty produktu mają zostać zainstalowane. Komponenty produktu w sekcji Komputer to Ochrona systemu plików w czasie rzeczywistym, Skanowanie komputera, Ochrona dokumentów oraz Kontrola dostępu do urządzeń. Należy pamiętać, że pierwsze dwa komponenty są niezbędne do działania programu zabezpieczającego. W sekcji Sieć dostępna jest opcja instalacji Zapory osobistej, która umożliwia monitorowanie całości przychodzącego i wychodzącego ruchu sieciowego oraz stosowanie reguł w odniesieniu do poszczególnych połączeń sieciowych. Zapora osobista zapewnia również ochronę przed atakami z komputerów zdalnych. Komponenty z sekcji Strony internetowe i poczta e-mail odpowiadają za ochronę użytkownika podczas przeglądania Internetu oraz komunikowania się za pośrednictwem poczty e-mail. Komponent Kopia dystrybucyjna aktualizacji może posłużyć do aktualizowania innych komputerów w sieci użytkownika. Sekcja obsługi technologii Microsoft NAP umożliwia agentowi ESET zapewnienie pełnej zgodności z architekturą NAP.



Aby skonfigurować ustawienia serwera proxy, wybierz ustawienie **Korzystam z serwera proxy** i kliknij przycisk **Dalej**. W polu **Adres** wprowadź adres IP lub URL serwera proxy. Jeśli nie masz pewności, czy w celu uzyskania połączenia z Internetem jest używany serwer proxy, wybierz opcję **Użyj ustawień z programu Internet Explorer (zalecane)** i kliknij przycisk **Dalej**. Jeśli serwer proxy nie jest używany, wybierz opcję **Nie korzystam z serwera proxy**. Więcej informacji można znaleźć w sekcji Serwer proxy.

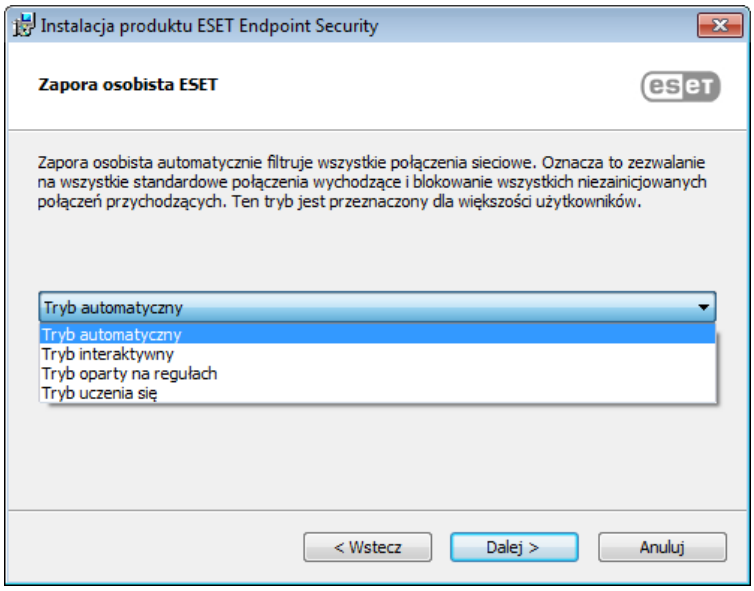


Instalacja niestandardowa pozwala na określenie sposobu przeprowadzenia automatycznych aktualizacji programu na komputerze. Kliknij przycisk **Zmień...**, aby uzyskać dostęp do ustawień zaawansowanych.

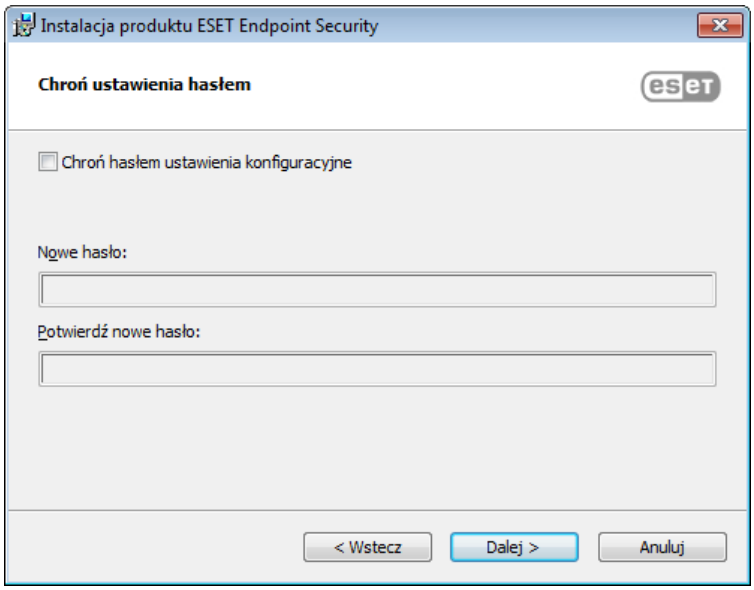


Jeśli komponenty programu nie mają być aktualizowane, należy wybrać opcję **Nigdy nie aktualizuj komponentów programu**. Aby przy każdej próbie pobrania komponentów programu pojawiało się okno potwierdzenia, wybierz opcję **Pytaj przed pobraniem aktualizacji komponentów programu**. Aby pobieranie uaktualnień komponentów programu odbywało się automatycznie, należy wybrać ustawienie **Zawsze aktualizuj komponenty programu**.

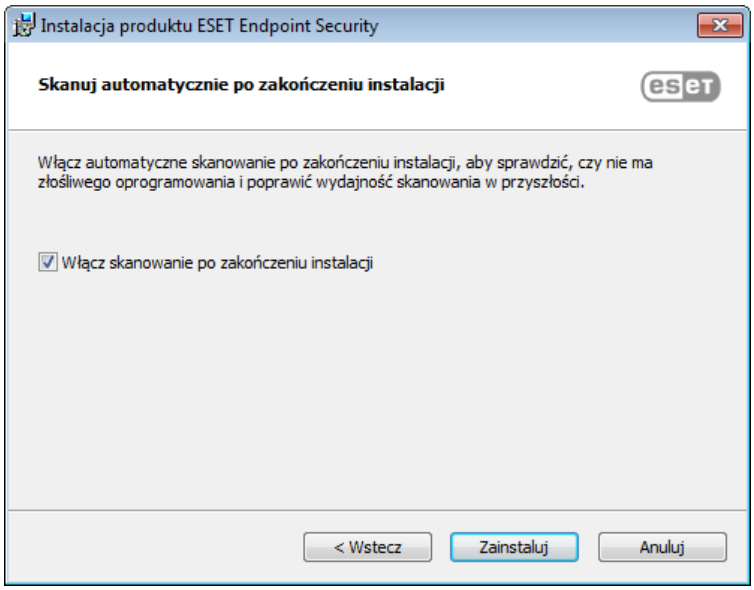
Następnie wybierz tryb filtrowania zapory osobistej ESET. Zapora osobista w programie ESET Endpoint Security udostępnia cztery tryby filtrowania. Zachowanie zapory zmienia się w zależności od wybranego trybu. Tryby filtrowania mają również wpływ na wymagany poziom interakcji użytkownika.



W następnym oknie instalacji można ustawić hasło służące do ochrony ustawień programu. Wybierz opcję **Chroń hasłem ustawienia konfiguracyjne** i wprowadź hasło w polach **Nowe hasło** i **Potwierdź nowe hasło**. Podanie tego hasła będzie wymagane w celu uzyskania dostępu do ustawień programu ESET Endpoint Security lub ich zmiany. Gdy hasła podane w obu polach są zgodne, kliknij przycisk **Dalej**, aby kontynuować.



Aby wyłączyć pierwsze skanowanie po zakończeniu instalacji, które jest zazwyczaj wykonywane po zakończeniu instalacji, należy usunąć zaznaczenie pola wyboru **Włącz skanowanie po zakończeniu instalacji**.



Kliknij **Zainstaluj**, aby rozpocząć instalację.

3.3 Instalacja produktu za pośrednictwem programu ERA (wiersza polecenia)

Poniższe ustawienia są przeznaczone do użytku w interfejsie użytkownika **wyłącznie na poziomie ograniczonym**, **podstawowym i przy ustawieniu brak**. Informacje o wersji programu **msiexec** używanego w odniesieniu do odpowiednich przełączników wiersza polecenia można znaleźć w dokumentacji.

Obsługiwane parametry:

APPDIR=<ścieżka>

- Ścieżka — prawidłowa ścieżka do katalogu
- Katalog instalacji aplikacji
- Przykład: `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<ścieżka>

- Ścieżka — prawidłowa ścieżka do katalogu
- Katalog instalacji danych aplikacji

MODULEDIR=<ścieżka>

- Ścieżka — prawidłowa ścieżka do katalogu
- Katalog instalacji modułu

ADDLOCAL=<lista>

- Instalacja komponentów — lista funkcji nieobowiązkowych do instalacji lokalnej
- Zastosowanie z pakietami ESET .msi: `ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Więcej informacji na temat właściwości ADDLOCAL można znaleźć tutaj: http://msdn.microsoft.com/en-us/library/aa367536%28v=vs.85%29.aspx

Reguły

- **Lista ADDLOCAL** to lista wartości oddzielanych przecinkami zawierająca nazwy wszystkich funkcji do zainstalowania.
- Przy wybieraniu funkcji do zainstalowania na liście należy wyraźnie podać pełną ścieżkę (z uwzględnieniem wszystkich funkcji nadrzędnych).
- Informacje na temat prawidłowego użytkowania podano w części Reguły dodatkowe.

Obecność funkcji

- **Obowiązkowa** — funkcja zawsze będzie instalowana
- **Opcjonalna** — można usunąć zaznaczenie funkcji przy instalacji
- **Niewidoczna** — funkcja logiczna niezbędna do prawidłowego działania innych funkcji
- **Wypełniacz** — funkcja, która nie wpływa na produkt, ale musi być wymieniona wśród funkcji podrzędnych

Drzewo funkcji programu Endpoint 6.1 wygląda następująco:

Drzewo funkcji	Nazwa funkcji	Obecność funkcji
Komputer	Komputer	Obowiązkowa
Komputer/Moduł antywirusowy i antyspyware	Ochrona antywirusowa	Obowiązkowa
Komputer/Moduł antywirusowy i antyspyware > Ochrona systemu plików w czasie rzeczywistym	RealtimeProtection	Obowiązkowa
Komputer/Moduł antywirusowy i antyspyware > Skanowanie komputera	Skanuj	Obowiązkowa
Komputer/Moduł antywirusowy i antyspyware > Ochrona dokumentów	Ochrona dokumentów	Opcjonalna
Komputer/Kontrola dostępu do urządzeń	DeviceControl	Opcjonalna
Sieć	Sieć	Wypełniacz
Sieć/Zapora osobista	Zapora	Opcjonalna
Strony internetowe i poczta e-mail	WebAndEmail	Wypełniacz
Strony internetowe i poczta e-mail/Filtrowanie protokołów	ProtocolFiltering	Niewidoczna
Strony internetowe i poczta e-mail/Ochrona dostępu do stron internetowych	WebAccessProtection	Opcjonalna
Strony internetowe i poczta e-mail/Ochrona programów poczty e-mail	EmailClientProtection	Opcjonalna
Strony internetowe i poczta e-mail/Ochrona programów poczty e-mail/Wtyczki do programów pocztowych	MailPlugins	Niewidoczna
Strony internetowe i poczta e-mail/Ochrona programów poczty e-mail/Ochrona przed spamem	Ochrona przed spamem	Opcjonalna
Strony internetowe i poczta e-mail/Kontrola dostępu do stron internetowych	WebControl	Opcjonalna
Kopia dystrybucyjna aktualizacji	UpdateMirror	Opcjonalna
Obsługa technologii Microsoft NAP	MicrosoftNAP	Opcjonalna

Reguły dodatkowe

- W przypadku wybrania do zainstalowania dowolnych spośród funkcji **WebAndEmail** niewidoczna funkcja **ProtocolFiltering** musi zostać wyraźnie uwzględniona na liście.
- W przypadku wybrania do zainstalowania dowolnych spośród funkcji podrzędnych funkcji **EmailClientProtection** niewidoczna funkcja **MailPlugins** musi zostać wyraźnie uwzględniona na liście.

Przykłady:

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

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

Lista właściwości CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0 — wyłączone, 1 — włączone
• PUA

CFG_LIVEGRID_ENABLED=1/0
• 0 — wyłączone, 1 — włączone
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0 — wyłącz, 1 — włącz
• Zaplanowanie nowego pierwszego skanowania po instalacji

CFG_EPFW_MODE=0/1/2/3
• 0 — automatyczny, 1 — interaktywny, 2 — oparty na regułach, 3 — tryb uczenia się

CFG_PROXY_ENABLED=0/1
• 0 — wyłączone, 1 — włączone

CFG_PROXY_ADDRESS=<ip>
• Adres IP serwera proxy

CFG_PROXY_PORT=<port>
• Numer portu serwera proxy

CFG_PROXY_USERNAME=<użytkownik>
• Nazwa użytkownika do celów uwierzytelniania

CFG_PROXY_PASSWORD=<hasło>
• Hasło do celów uwierzytelniania

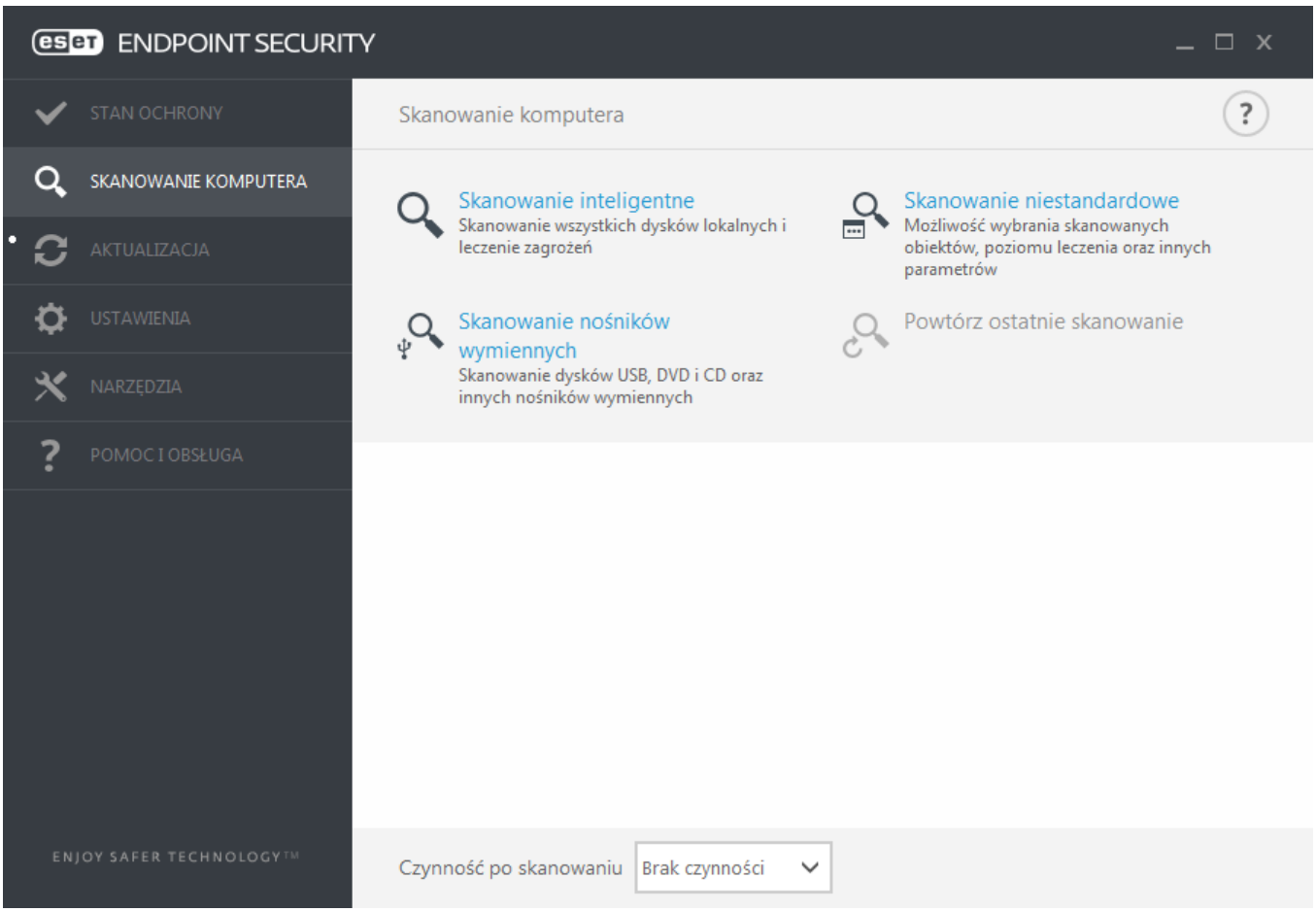
3.4 Aktywacja produktu

Po zakończeniu instalacji zostanie wyświetlony monit o aktywowanie produktu.

Wybierz jedną z dostępnych metod aktywacji programu ESET Endpoint Security. Więcej informacji na ten temat znajduje się w dziale Aktywowanie programu ESET Endpoint Security.

3.5 Skanowanie komputera

Najpóźniej po 15 minutach od zakończenia instalacji (może być konieczne ponowne uruchomienie komputera), program ESET Endpoint Security automatycznie rozpocznie skanowanie komputera. Oprócz początkowego skanowania zalecane jest regularne przeprowadzanie skanowania komputera lub zaplanowanie regularnego skanowania mającego na celu wykrywanie zagrożeń. W głównym oknie programu należy kliknąć opcję **Skanowanie komputera**, a następnie opcję **Skanowanie inteligentne**. Więcej informacji o skanowaniu komputera można znaleźć w sekcji Skanowanie komputera.



3.6 Uaktualnianie do nowszej wersji

Nowsze wersje programu ESET Endpoint Security publikuje się w celu wprowadzania w nim poprawek lub udoskonaleń, których nie można wdrożyć w ramach automatycznych aktualizacji poszczególnych modułów. Uaktualnienie do nowszej wersji można przeprowadzić na kilka sposobów:

1. Automatycznie za pomocą aktualizacji programu.
   W związku z tym, że uaktualnienie programu jest rozsyłane do wszystkich użytkowników i może wpływać na niektóre konfiguracje systemowe, jego publikacja odbywa się po długim okresie testów w celu zapewnienia sprawnego działania we wszystkich możliwych konfiguracjach. Jeśli zachodzi potrzeba uaktualnienia programu do nowszej wersji natychmiast po jej udostępnieniu, należy posłużyć się jedną z poniższych metod.
2. Ręcznie przez pobranie i zainstalowanie nowszej wersji już zainstalowanego programu.
3. Ręcznie z automatycznym wdrożeniem w środowisku sieciowym za pośrednictwem programu ESET Remote Administrator.

3.7 Przewodnik dla początkujących

Niniejszy rozdział zawiera ogólny opis programu ESET Endpoint Security i jego podstawowych ustawień.

3.7.1 Interfejs użytkownika

Główne okno programu ESET Endpoint Security jest podzielone na dwie główne części. W okienku z prawej strony są wyświetlane informacje dotyczące opcji wybranej w menu głównym z lewej strony.

Poniżej opisano opcje dostępne w menu głównym:

Stan ochrony — przedstawia informacje o stanie ochrony zapewnianej przez program ESET Endpoint Security.

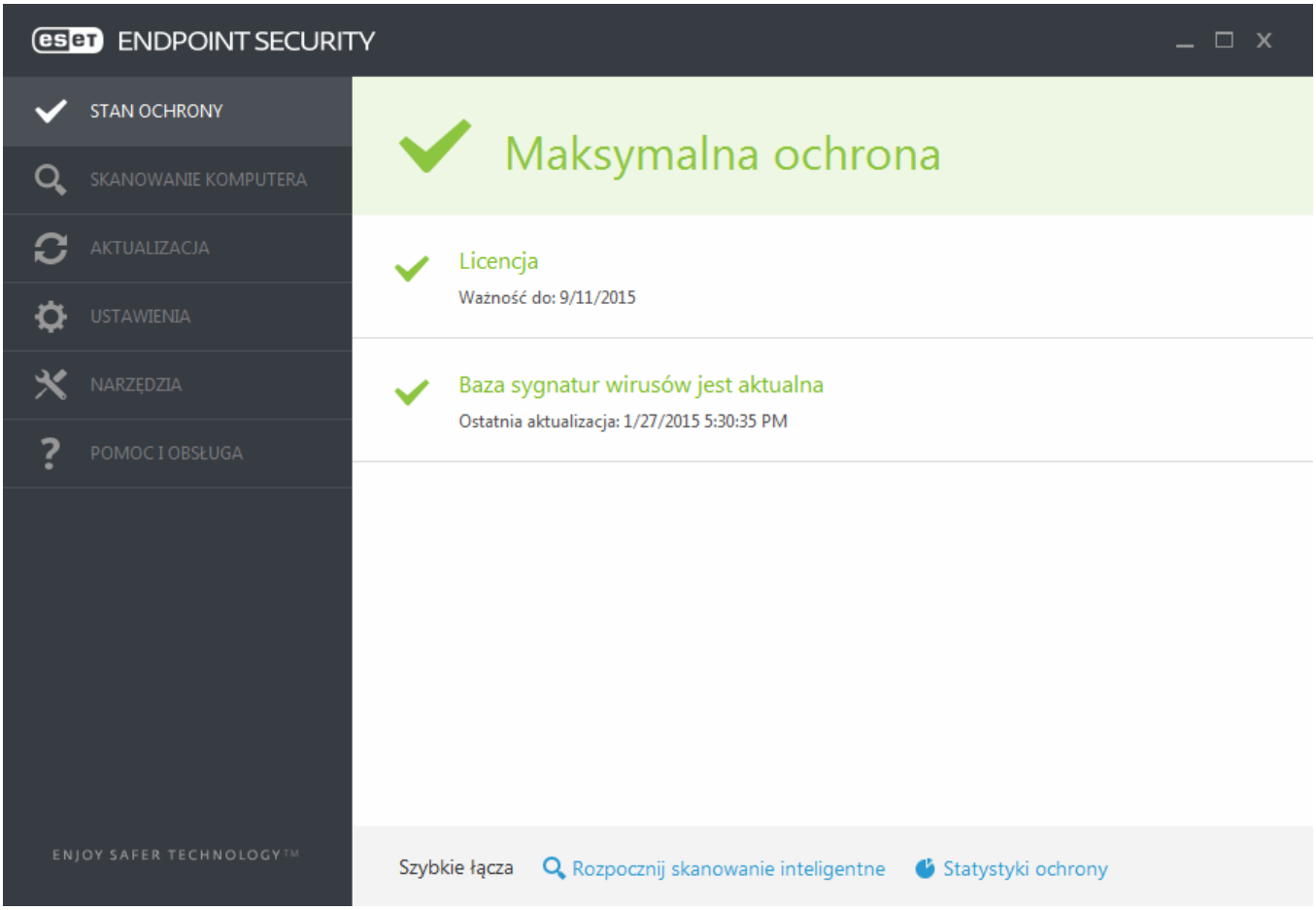
Skanowanie komputera — pozwala skonfigurować i uruchomić skanowanie inteligentne, skanowanie niestandardowe lub skanowanie nośników wymiennych. Umożliwia również powtórzenie ostatnio uruchamianego skanowania.

Aktualizacja — prezentuje informacje dotyczące bazy sygnatur wirusów.

Ustawienia — wybranie tej opcji umożliwia skonfigurowanie ustawień zabezpieczeń komputera, sieci lub stron internetowych i poczty e-mail.

Narzędzia — ta opcja zapewnia dostęp do plików dziennika, statystyk ochrony, Monitora aktywności, uruchomionych procesów, harmonogramu, kwarantanny, połączeń sieciowych, oraz narzędzi ESET SysInspector i ESET SysRescue w celu utworzenia ratunkowej płyty CD. Możliwe jest również przesłanie próbki do analizy.

Pomoc i obsługa — dostęp do plików pomocy, bazy wiedzy firmy ESET oraz strony internetowej firmy ESET. Dostępne są również łącza umożliwiające otwarcie formularza zgłoszenia do działu obsługi klienta oraz narzędzi pomocy technicznej, a także wyświetlenie informacji dotyczących aktywacji produktu.

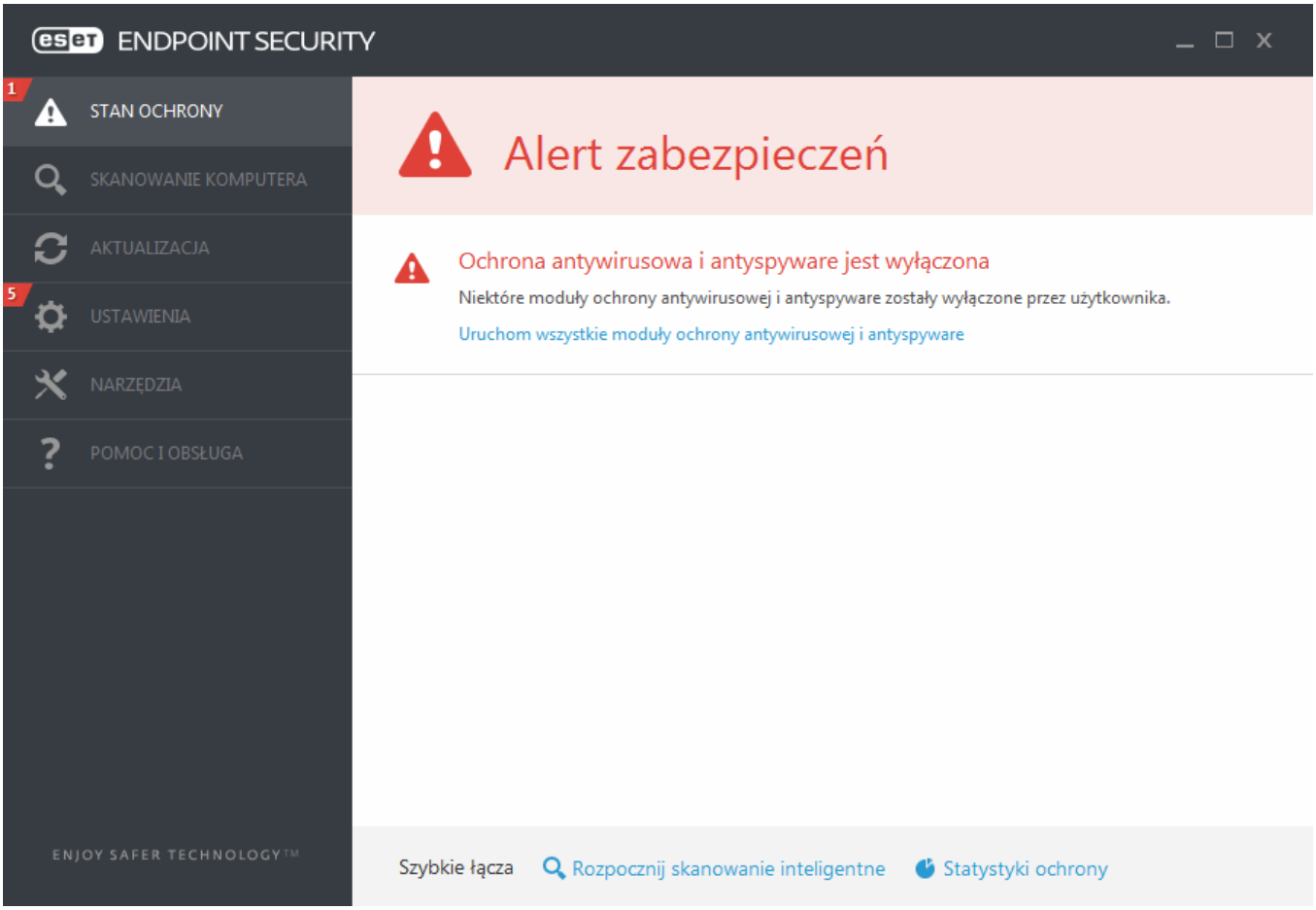


Ekran **Stan ochrony** zawiera informacje o zabezpieczeniach i bieżącym poziomie ochrony komputera. Zielona ikona stanu **Maksymalna ochrona** oznacza maksymalny poziom bezpieczeństwa.

W oknie stanu widoczne są również szybkie łącza do często używanych funkcji programu ESET Endpoint Security oraz informacje dotyczące ostatniej aktualizacji.

Postępowanie w przypadku, gdy program nie działa poprawnie?

Jeśli włączone moduły działają prawidłowo, są oznaczone zielonym znacznikiem wyboru. W przeciwnym razie jest wyświetlana czerwona ikona wykrzyknika lub pomarańczowa ikona powiadomienia. Dodatkowe informacje dotyczące modułu są wyświetlane w górnej części okna. Wyświetlany jest również proponowany sposób przywrócenia działania modułu. Aby zmienić stan danego modułu, należy w menu głównym kliknąć opcję **Ustawienia**, a następnie kliknąć wybrany moduł.



Czerwona ikona ze znakiem „!” sygnalizuje problemy krytyczne (maksymalny poziom ochrony komputera nie jest zapewniony). Możliwe przyczyny:

- **Ochrona antywirusowa i antyspyware wyłączona** — użytkownik może ponownie włączyć ochronę antywirusową i antyspyware, klikając opcję **Włącz ochronę w czasie rzeczywistym** w okienku **Stan ochrony** lub opcję **Włącz ochronę antywirusową i antyspyware** w okienku **Ustawienia** w oknie głównym programu.
- **Wyłączona zapora osobista ESET** — ten problem jest sygnalizowany czerwoną ikoną i powiadomieniem dotyczącym bezpieczeństwa obok elementu **Sieć**. Aby ponownie włączyć ochronę komunikacji sieciowej, należy kliknąć pozycję **Włącz tryb filtrowania**.
- **Baza sygnatur wirusów jest nieaktualna** — używana baza sygnatur wirusów jest nieaktualna.
- **Produkt nie został aktywowany** lub **Licencja wygasła** — jest to sygnalizowane przez zmianę koloru ikony stanu ochrony na czerwony. Po wygaśnięciu licencji program nie może być aktualizowany. Zalecane jest odnowienie licencji zgodnie z instrukcjami podanymi w oknie alertu.

Pomarańczowa ikona ze znakiem „i” oznacza, że produkt ESET wymaga interwencji użytkownika w związku z problemem niekrytycznym. Możliwe przyczyny:

- **Ochrona dostępu do stron internetowych jest wyłączona** — użytkownik może ponownie włączyć ochronę dostępu do stron internetowych, klikając powiadomienie dotyczące bezpieczeństwa, a następnie opcję **Włącz ochronę dostępu do stron internetowych**.

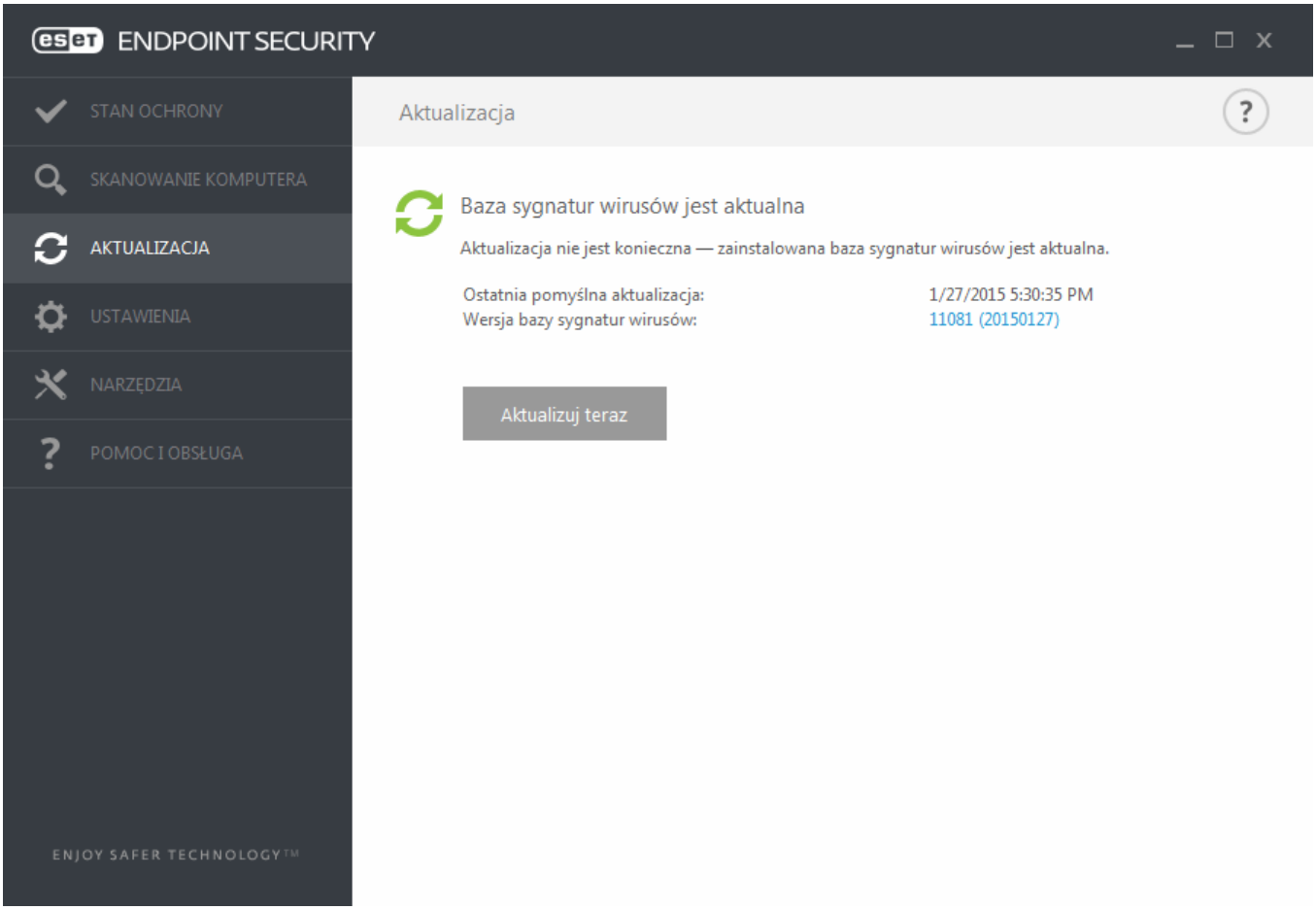
- **Licencja wkrótce wygaśnie** — jest to sygnalizowane przez ikonę stanu ochrony przedstawiającą wykrzyknik. Po wygaśnięciu licencji programu nie będzie można aktualizować, a kolor ikony stanu ochrony zmieni się na czerwony.

Jeśli nie można usunąć problemu za pomocą sugerowanych rozwiązań, należy kliknąć opcję **Pomoc i obsługa**, aby uzyskać dostęp do plików pomocy, lub przeszukać bazę wiedzy ESET. Jeśli nadal potrzebna jest pomoc, można przesłać zgłoszenie do działu obsługi klienta firmy ESET. Dział obsługi klienta ESET niezwłocznie odpowie na otrzymane zgłoszenie i pomoże znaleźć rozwiązanie.

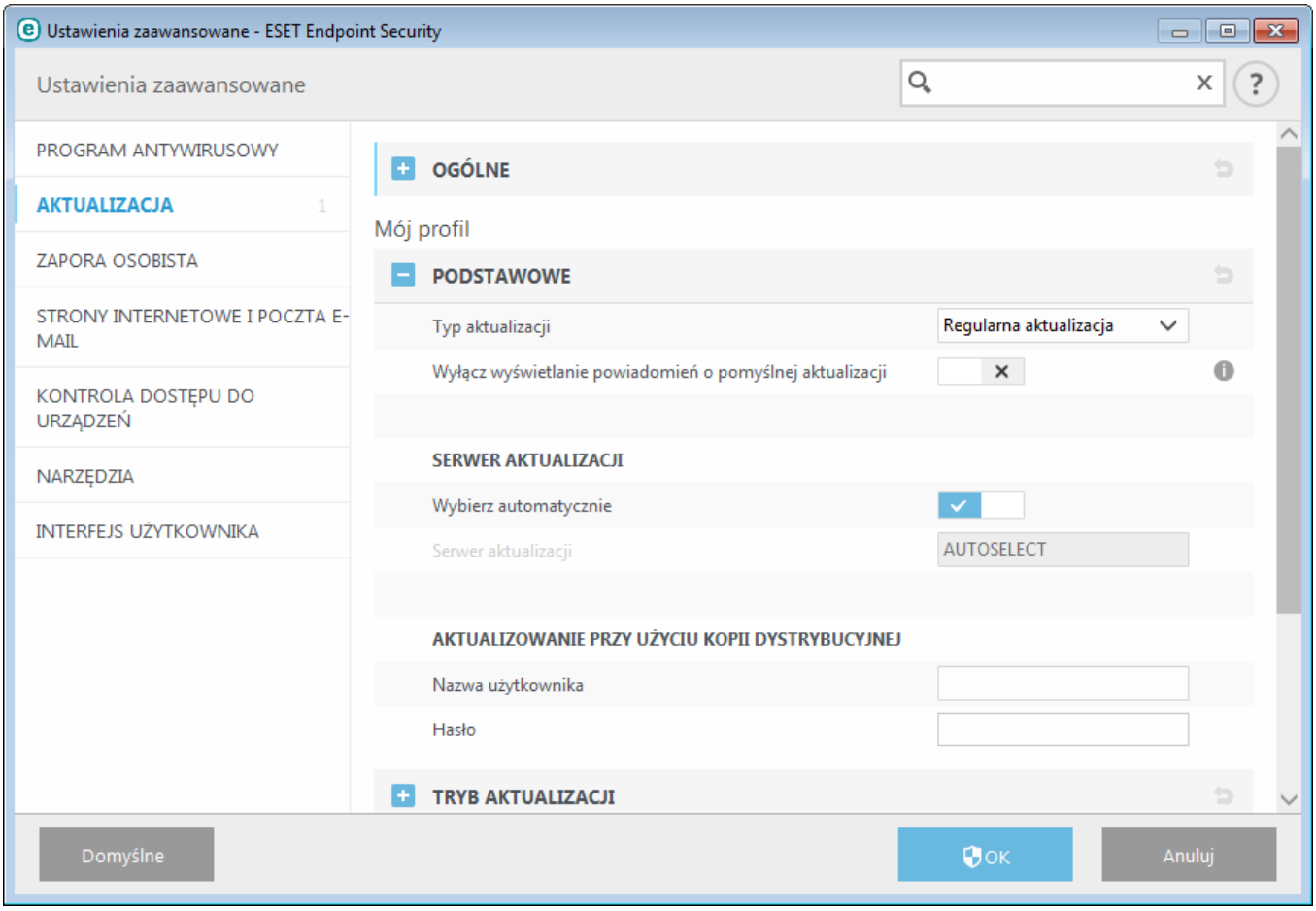
3.7.2 Ustawienia aktualizacji

Aktualizacje bazy sygnatur wirusów oraz komponentów programu są istotnym elementem procesu zapewniania kompleksowej ochrony przed szkodliwym kodem. Należy zwrócić szczególną uwagę na konfigurację i działanie aktualizacji. Aby sprawdzić dostępność nowszej aktualizacji bazy danych, w menu głównym należy wybrać kolejno opcje **Aktualizacja** > **Aktualizuj teraz**.

Jeśli **klucz licencyjny** nie został jeszcze wprowadzony, nie będzie można pobrać nowych aktualizacji i zostanie wyświetlony monit o aktywowanie produktu.



W oknie Ustawienia zaawansowane dostępne są dodatkowe opcje aktualizacji. Aby przejść do tego okna, w menu głównym kliknij kolejno opcje **Ustawienia** > **Ustawienia zaawansowane** albo naciśnij klawisz **F5** na klawiaturze. Aby skonfigurować zaawansowane opcje aktualizacji, np. tryb aktualizacji, dostęp do serwera proxy, połączenia z siecią LAN i tworzenie kopii sygnatur wirusów, kliknij przycisk **Aktualizacja** znajdujący się w drzewie ustawień zaawansowanych. W przypadku problemów z aktualizacją należy kliknąć przycisk **Wyczyść**, aby usunąć tymczasową pamięć podręczną aktualizacji. W menu **Serwer aktualizacji** domyślnie ustawiona jest opcja **AUTOSELECT**. Podczas korzystania z serwera ESET zalecane jest pozostawienie włączonej opcji domyślnej **Wybierz automatycznie**. Aby zrezygnować z wyświetlania powiadomień na pasku zadań w prawym dolnym rogu ekranu, należy wybrać opcję **Wyłącz wyświetlanie powiadomień o pomyślnej aktualizacji**.



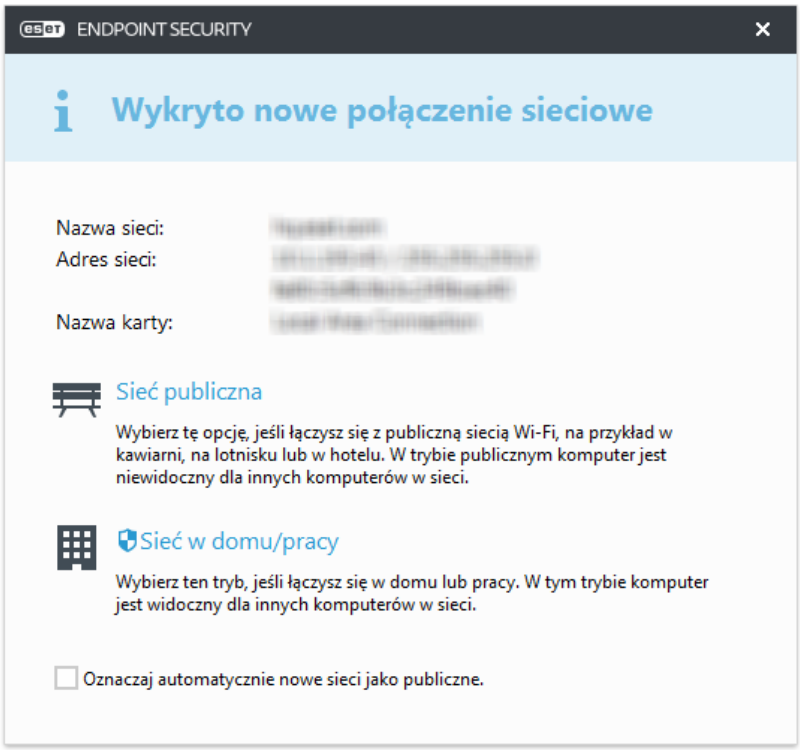
Dla uzyskania optymalnej funkcjonalności ważne jest automatyczne aktualizowanie programu. Jest to możliwe wyłącznie po wprowadzeniu prawidłowego **klucza licencyjnego** w sekcji **Pomoc i obsługa** > **Aktywuj produkt**.

Jeśli po zakończeniu instalacji nie wprowadzono **klucza licencyjnego**, można to zrobić w dowolnej chwili. Aby uzyskać szczegółowe informacje na temat aktywacji, przejdź do sekcji Aktywowanie programu ESET Endpoint Security i w oknie **Szczegóły licencji** wprowadź poświadczenia otrzymane wraz z oprogramowaniem zabezpieczającym firmy ESET.

3.7.3 Ustawienia stref

Aby komputer był chroniony w środowisku sieciowym, należy skonfigurować strefy zaufane. Konfigurując strefę zaufaną i zezwalając na udostępnianie, można pozwolić innym użytkownikom na uzyskiwanie dostępu do komputera. W celu uzyskania dostępu do ustawień stref zaufanych należy kliknąć kolejno pozycje **Ustawienia zaawansowane** (F5) > **Zapora osobista** > **Strefy**.

Wykrywanie strefy zaufanej odbywa się po zainstalowaniu programu ESET Endpoint Security oraz po każdym nawiązaniu przez komputer połączenia z nową siecią. Dlatego zwykle nie ma potrzeby definiowania strefy zaufanej. Po wykryciu nowej strefy domyślnie zostaje wyświetlone okno dialogowe, w którym można ustawić poziom ochrony dla tej strefy.



Ostrzeżenie: Nieprawidłowa konfiguracja strefy zaufanej może stwarzać zagrożenie dla bezpieczeństwa komputera.

UWAGA: Dla stacji roboczych ze strefy zaufanej domyślnie jest włączona przychodząca komunikacja RPC. Otrzymują one także uprawnienia do korzystania z udostępnianych plików i drukarek oraz z funkcji udostępniania pulpitu zdalnego.

3.7.4 Narzędzia do kontroli dostępu do stron internetowych

Jeśli funkcja kontroli dostępu do stron internetowych jest włączona w programie ESET Endpoint Security, aby zapewnić jej prawidłowe działanie, należy ją skonfigurować dla odpowiednich kont użytkownika. Instrukcje dotyczące tworzenia określonych ograniczeń obejmujących klienckie stacje robocze w celu zapewnienia im ochrony przed potencjalnie obraźliwymi materiałami można znaleźć w rozdziale Kontrola dostępu do stron internetowych.

3.8 Często zadawane pytania

W tym rozdziale omówiono niektóre często zadawane pytania oraz typowe problemy. Aby dowiedzieć się, jak rozwiązać dany problem, kliknij temat:

Aktualizowanie programu ESET Endpoint Security
Aktywowanie programu ESET Endpoint Security
Stosowanie bieżących poświadczeń do aktywowania nowego produktu
Usuwanie wirusa z komputera
Zezwalanie na komunikację określonej aplikacji
Tworzenie nowego zadania w harmonogramie
Planowanie zadania skanowania (co 24 godziny)
Łączenie posiadanego programu z rozwiązaniem ESET Remote Administrator
Konfigurowanie kopii dystrybucyjnej

Jeśli problem napotkany przez użytkownika nie jest omówiony na stronach pomocy wymienionych powyżej, można spróbować wyszukać informacje o nim na stronach pomocy programu ESET Endpoint Security, podając słowo kluczowe lub frazę opisujące problem.

Jeśli rozwiązania problemu lub odpowiedzi na pytanie nie uda się znaleźć na stronach pomocy, zapraszamy do odwiedzenia bazy wiedzy firmy ESET, gdzie dostępne są odpowiedzi na często pojawiające się pytania oraz omówienia problemów.

Usuwanie konia trojańskiego Sirefef (ZeroAccess)?
Lista kontrolna rozwiązywania problemów z kopią dystrybucyjną aktualizacji
Adresy i porty, które należy otworzyć w ustawieniach zapory innej firmy, aby zapewnić pełną funkcjonalność produktu firmy ESET

W razie potrzeby można skontaktować się z internetowym centrum obsługi technicznej i przedstawić pytania lub problem. Łącze do naszego internetowego formularza kontaktowego można znaleźć w panelu **Pomoc i obsługa** w oknie głównym programu.

3.8.1 Aktualizowanie programu ESET Endpoint Security

Aktualizowanie programu ESET Endpoint Security może się odbywać ręcznie lub automatycznie. Aby uruchomić proces aktualizacji, należy kliknąć przycisk **Aktualizuj teraz** w sekcji **Aktualizacja** w menu głównym.

W ramach domyślnych ustawień instalacji jest tworzone zadanie aktualizacji automatycznej wykonywane co godzinę. Aby zmienić odstęp czasu między aktualizacjami, należy przejść do opcji **Narzędzia** > **Harmonogram**. Aby uzyskać więcej informacji na temat harmonogramu, kliknij tutaj.

3.8.2 Aktywowanie programu ESET Endpoint Security

Po zakończeniu instalacji zostanie wyświetlony monit o aktywowanie produktu.

Istnieje kilka metod aktywacji produktu. Dostępność danego scenariusza w oknie aktywacji zależy od kraju oraz sposobu dystrybucji (na płycie CD/DVD, na stronie internetowej firmy ESET itd.).

Aby aktywować produkt ESET Endpoint Security bezpośrednio z poziomu programu, należy kliknąć ikonę na pasku zadań i z menu wybrać opcję **Aktywuj licencję produktu**. Produkt można również aktywować z menu głównego, wybierając pozycje **Pomoc i obsługa** > **Aktywuj produkt** lub **Stan ochrony** > **Aktywuj produkt**.

Aktywacji produktu ESET Endpoint Security można dokonać przy użyciu dowolnej z poniższych metod:

- **Klucz licencyjny** — niepowtarzalny ciąg znaków w formacie XXXX-XXXX-XXXX-XXXX-XXXX służący do identyfikacji właściciela licencji oraz do aktywowania licencji.
- **Administrator zabezpieczeń** — konto tworzone w portalu ESET License Administrator przy użyciu poświadczeń (adres e-mail + hasło). Ta metoda umożliwia zarządzanie wieloma licencjami z jednego miejsca.
- **Licencja offline** — automatycznie generowany plik, który zostanie przeniesiony do produktu ESET w celu przekazania informacji dotyczących licencji. Jeśli w ramach licencji możliwe jest pobranie pliku licencji offline (.lf),

ten plik może zostać użyty do przeprowadzenia aktywacji w trybie offline. Liczba licencji offline zostanie odjęta od ogólnej liczby dostępnych licencji. Szczegółowe informacje na temat tworzenia pliku offline można znaleźć w Podręczniku użytkownika programu ESET License Administrator.

Jeśli komputer należy do sieci zarządzanej, należy kliknąć opcję **Aktywuj później**, by administrator przeprowadził zdalną aktywację przy użyciu narzędzia ESET Remote Administrator. Z tej opcji można również skorzystać w celu aktywowania klienta w późniejszym czasie.

Jeśli znana jest nazwa użytkownika i hasło, ale nie wiadomo, w jaki sposób uruchomić program ESET Endpoint Security, należy kliknąć opcję **Mam nazwę i hasło użytkownika. Co muszę zrobić?**. Zostanie otwarty portal ESET License Administrator, w którym można przekonwertować poświadczenia w klucz licencyjny.

Licencję produktu można zmienić w dowolnej chwili. W tym celu w głównym oknie programu należy kliknąć kolejno opcje **Pomoc i obsługa** > **Zarządzaj licencją**. Zostanie wyświetlony identyfikator licencji publicznej używany do identyfikowania licencji przez obsługę firmy ESET. Nazwa użytkownika, pod którą zarejestrowano komputer, zapisana jest w sekcji **Informacje**, dostępnej po kliknięciu prawym przyciskiem myszy ikony na pasku zadań.

UWAGA: Program ESET Remote Administrator umożliwia aktywowanie komputerów klienckich w trybie cichym przy użyciu licencji udostępnionych przez administratora. Odpowiednie instrukcje zawiera Podręcznik użytkownika programu ESET Remote Administrator.

3.8.3 Stosowanie bieżących poświadczeń do aktywowania nowego produktu

Jeśli użytkownik ma już nazwę użytkownika oraz hasło, a chce otrzymać klucz licencyjny, może odwiedzić portal ESET License Administrator, gdzie możliwe jest przekonwertowanie poświadczeń na nowy klucz licencyjny.

3.8.4 Usuwanie wirusa z komputera

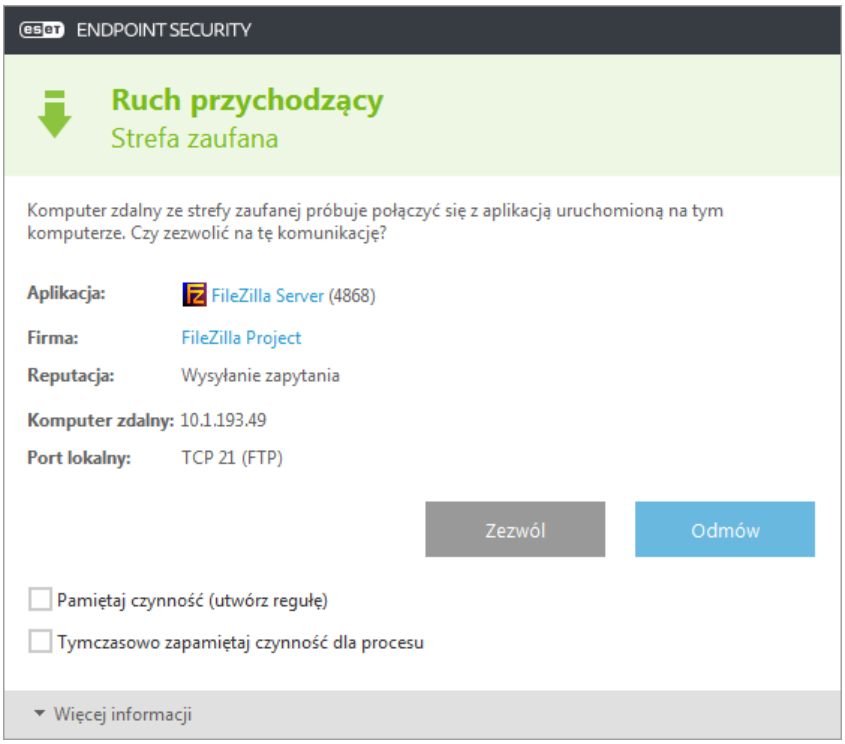
Jeśli komputer wykazuje symptomy zarażenia szkodliwym oprogramowaniem, na przykład działa wolniej lub często przestaje odpowiadać, zalecane jest wykonanie następujących czynności:

1. W głównym oknie programu kliknij opcję **Skanowanie komputera**.
2. Kliknij opcję **Skanowanie inteligentne**, aby rozpocząć skanowanie systemu.
3. Po zakończeniu skanowania przejrzyj dziennik zawierający liczbę obiektów przeskanowanych, zainfekowanych i wyleczonych.
4. Aby przeskanować tylko określoną część dysku, kliknij opcję **Skanowanie niestandardowe** i wybierz obiekty, które mają zostać przeskanowane w poszukiwaniu wirusów.

Dodatkowe informacje można znaleźć w regularnie uaktualnianym artykule bazy wiedzy firmy ESET.

3.8.5 Zezwalanie na komunikację określonej aplikacji

Jeśli w trybie interaktywnym zostanie wykryte nowe połączenie, dla którego nie ma reguły, zostanie wyświetlony monit o zezwolenie na połączenie lub jego odmowę. Jeśli ta sama czynność ma być wykonywana przez program ESET Endpoint Security przy każdej próbie nawiązania połączenia, należy zaznaczyć pole wyboru **Pamiętaj czynność (utwórz regułę)**.



W oknie konfiguracji zapory osobistej (znajdującym się w obszarze **Ustawienia zaawansowane** > **Zapora osobista** > **Podstawowe** > **Reguły**, po kliknięciu opcji **Edytuj**) można tworzyć nowe reguły dotyczące zapory osobistej dla aplikacji — zanim zostaną wykryte przez program ESET Endpoint Security.

W celu dodania reguły należy kliknąć przycisk **Dodaj**. Na karcie **Ogólne** należy wprowadzić nazwę, kierunek i protokół komunikacyjny reguły. To okno umożliwia zdefiniowanie działania podejmowanego przy stosowaniu reguły.

Na karcie **Lokalne** należy podać ścieżkę do pliku wykonywalnego aplikacji i lokalny port komunikacyjny. Jeśli trzeba wprowadzić adres i port zdalny, należy przejść do karty **Zdalny**. Nowo utworzona reguła zostanie zastosowana, gdy tylko aplikacja spróbuje ponownie nawiązać komunikację.

3.8.6 Tworzenie nowego zadania w harmonogramie

Aby utworzyć nowe zadanie w obszarze **Narzędzia** > **Harmonogram**, należy kliknąć przycisk **Dodaj zadanie** lub kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać opcję **Dodaj...**. Dostępnych jest pięć typów zaplanowanych zadań:

- **Uruchom aplikację zewnętrzną** — umożliwia zaplanowanie uruchomienia aplikacji zewnętrznej.
- **Administracja dziennikami** — pliki dziennika zawierają także pozostałości usuniętych rekordów. To zadanie regularnie przeprowadza optymalizację rekordów w plikach dzienników w celu usprawnienia działania.
- **Sprawdzanie plików przy uruchamianiu systemu** — umożliwia sprawdzenie plików, które mogą być wykonywane podczas uruchamiania systemu lub logowania.
- **Tworzenie migawki stanu komputera** — tworzy migawkę stanu komputera ESET SysInspector — szczegółowa analiza komponentów systemu (na przykład sterowników i aplikacji) oraz ocena poziomu ryzyka dotyczącego każdego komponentu.
- **Skanowanie komputera na żądanie** — umożliwia skanowanie plików i folderów na komputerze.
- **Najpierw skanowanie** — domyślnie 20 minut po zakończeniu instalacji lub ponownym uruchomieniu, zostanie przeprowadzone skanowanie komputera jako zadanie o niskim priorytecie.
- **Aktualizacja** — umożliwia zaplanowanie zadania polegającego na aktualizowaniu bazy sygnatur wirusów i aktualizowaniu modułów programu.

Ponieważ jednym z najczęściej używanych zadań planowanych jest **Aktualizacja**, poniżej został przedstawiony sposób dodawania nowego zadania aktualizacji:

Z menu rozwijanego **Zaplanowane zadanie** wybierz opcję **Aktualizacja**. Wprowadź nazwę zadania w polu **Nazwa zadania** i kliknij przycisk **Dalej**. Wybierz częstotliwość zadania. Dostępne są następujące opcje: **Jednorazowo**, **Wielokrotnie**, **Codziennie**, **Raz w tygodniu** i **Po wystąpieniu zdarzenia.** Wybranie opcji **Pomiń zadanie, gdy komputer jest zasilany z baterii** umożliwia zminimalizowanie wykorzystania zasobów systemowych, gdy komputer działa na zasilaniu akumulatorowym. Zadanie zostanie uruchomione w dniu tygodnia i o godzinie, które wskazano w polach **Wykonanie zadania**. Następnie zdefiniuj czynność podejmowaną w przypadku, gdy nie można wykonać lub zakończyć zadania w zaplanowanym czasie. Dostępne są następujące opcje:

- **W następnym zaplanowanym terminie**
- **Jak najwcześniej**
- **Natychmiast, gdy czas od ostatniego uruchomienia przekroczy określoną wartość** (interwał można określić za pomocą pola przewijania **Czas od ostatniego uruchomienia**)

W następnym kroku zostanie wyświetlone okno podsumowania z informacjami na temat bieżącego zaplanowanego zadania. Kliknij **Zakończ**, gdy zakończysz wprowadzanie zmian.

Zostanie wyświetlone okno dialogowe umożliwiające wybranie profili używanych z zaplanowanym zadaniem. Można tam ustawić profil główny i alternatywny. Profil alternatywny jest używany, gdy zadanie nie może być wykonane przy użyciu profilu głównego. Po potwierdzeniu przy użyciu przycisku **Zakończ** nowe zaplanowane zadanie zostanie dodane do listy aktualnie zaplanowanych zadań.

3.8.7 Planowanie zadania skanowania (co 24 godziny)

Aby zaplanować zwykłe zadanie, otwórz główne okno programu i kliknij opcję **Narzędzia** > **Harmonogram**. Poniżej przedstawiono krótką instrukcję planowania zadania, które spowoduje skanowanie dysków lokalnych co 24 godziny.

Aby zaplanować zadanie skanowania:

1. Kliknij przycisk **Dodaj** znajdujący się w głównym oknie sekcji Harmonogram.
2. Z menu rozwijanego wybierz opcję **Skanowanie komputera na żądanie**.
3. Wprowadź nazwę zadania i wybierz opcję **Wielokrotnie**.
4. Wybierz uruchamianie zadania co 24 godziny.
5. Wybierz działanie, które zostanie podjęte w przypadku niepowodzenia zaplanowanego zadania.
6. Przejrzyj podsumowanie planowanego zadania i kliknij przycisk **Zakończ**.
7. Z menu rozwijanego **Obiekty docelowe** wybierz opcję **Dyski lokalne**.
8. Aby zatwierdzić zadanie, kliknij przycisk **Zakończ**.

3.8.8 Łączenie programu ESET Endpoint Security z programem ESET Remote Administrator

Po zainstalowaniu na komputerze programu ESET Endpoint Security przed połączeniem się za pośrednictwem programu ESET Remote Administrator należy się upewnić, że na stacji roboczej klienta zainstalowany został również agent ERA. Agent ERA stanowi ważną część każdego rozwiązania klienckiego, które komunikuje się z serwerem ERA. Program ESET Remote Administrator używa narzędzia RD Sensor do wyszukiwania komputerów w sieci. Każdy komputer w sieci wykryty przez RD Sensor wyświetlany jest w konsoli internetowej.

Gdy agent zostanie już wdrożony, można przeprowadzić instalację zdalną innych produktów zabezpieczających firmy ESET na komputerze klienckim. Poszczególne kroki instalacji zdalnej opisano w Podręczniku użytkownika programu ESET Remote Administrator.

3.8.9 Konfigurowanie kopii dystrybucyjnej

Program ESET Endpoint Security można skonfigurować w taki sposób, by przechowywał kopie plików aktualizacji bazy sygnatur wirusów i dystrybuował je wśród innych stacji roboczych z uruchomionym programem ESET Endpoint Security lub ESET Endpoint Antivirus.

Konfigurowanie programu ESET Endpoint Security jako serwera kopii dystrybucyjnych w celu zapewnienia możliwości aktualizacji za pośrednictwem wewnętrznego serwera HTTP

Naciśnij klawisz **F5**, aby uzyskać dostęp do obszaru Ustawienia zaawansowane i rozwiń opcje **Aktualizacja** > **Podstawowe**. Upewnij się, że w pozycji **Serwer aktualizacji** ustawiono opcję **AUTOSELECT**. Wybierz opcje **Utwórz kopię dystrybucyjną aktualizacji** oraz **Udostępnij pliki aktualizacji za pośrednictwem wewnętrznego serwera HTTP** w obszarze **Ustawienia zaawansowane** > **Podstawowe** > **Kopia dystrybucyjna**.

Konfigurowanie serwera kopii dystrybucyjnych w celu zapewnienia możliwości aktualizacji za pośrednictwem udostępnionego folderu sieciowego

Utwórz udostępniony folder na urządzeniu lokalnym lub sieciowym. Wszyscy użytkownicy z uruchomionym oprogramowaniem zabezpieczającym ESET muszą mieć możliwość odczytu tego folderu, a ponadto musi istnieć możliwość dokonywania w nim zapisów z poziomu konta SYSTEMU lokalnego. Aktywuj opcję **Utwórz kopię dystrybucyjną aktualizacji** w obszarze **Ustawienia zaawansowane** > **Podstawowe** > **Kopia dystrybucyjna**. Przejdź do utworzonego folderu udostępnionego i wybierz go.

UWAGA: Aby nie przeprowadzać aktualizacji przez wewnętrzny serwer HTTP, należy wyłączyć opcję **Udostępnij pliki aktualizacji za pośrednictwem wewnętrznego serwera HTTP**.

3.8.10 Jak uaktualnić do systemu Windows 10 z produktem ESET Endpoint Security


Przed uaktualnieniem do systemu Windows 10 zdecydowanie warto przeprowadzić uaktualnienie do najnowszej wersji produktu ESET, a następnie pobrać najnowszą bazę sygnatur wirusów. Zapewni to maksymalną ochronę oraz pozwoli zachować ustawienia i informacje o licencji podczas uaktualniania do systemu Windows 10.

Wersja 6.x lub nowsza:

Kliknij odpowiednie łącze poniżej, aby pobrać i zainstalować najnowszą wersję w ramach przygotowań do uaktualnienia do systemu Microsoft Windows 10:

Pobierz program ESET Endpoint Security 6 w wersji 32-bitowej Pobierz program ESET Endpoint Antivirus 6 w wersji 32-bitowej

Pobierz program ESET Endpoint Security 6 w wersji 64-bitowej Pobierz program ESET Endpoint Antivirus 6 w wersji 64-bitowej

Wersja 5.x lub starsza:

Kliknij odpowiednie łącze poniżej, aby pobrać i zainstalować najnowszą wersję w ramach przygotowań do uaktualnienia do systemu Microsoft Windows 10:

Pobierz program ESET Endpoint Security 5 w wersji 32-bitowej Pobierz program ESET Endpoint Antivirus 5 w wersji 32-bitowej

Pobierz program ESET Endpoint Security 5 w wersji 64-bitowej Pobierz program ESET Endpoint Antivirus 5 w wersji 64-bitowej

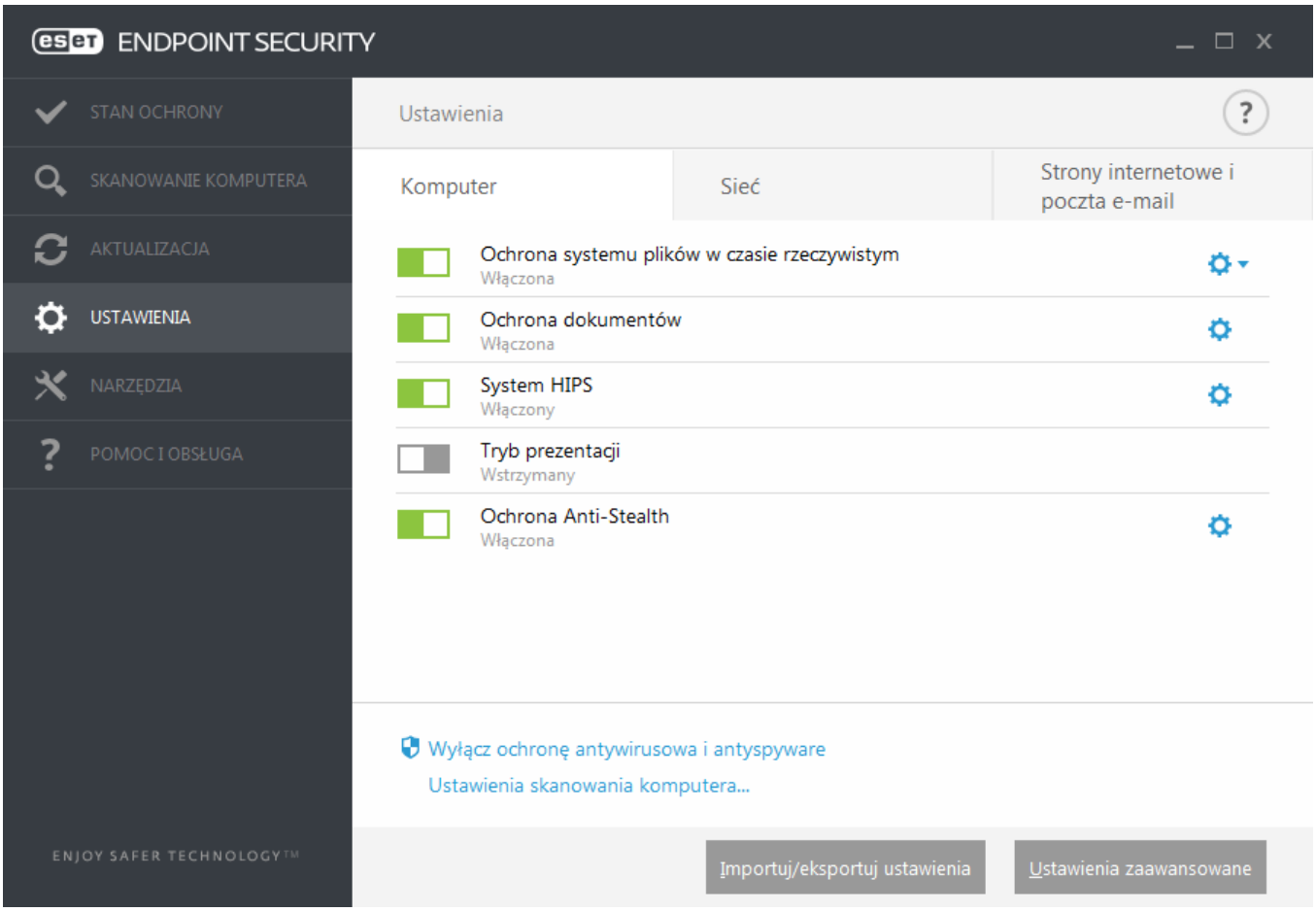
Inne wersje językowe:

Jeśli szukasz innej wersji językowej produktu ESET dla komputerów klienckich, odwiedź naszą stronę pobierania.

UWAGA: więcej informacji o zgodności produktów ESET z systemem Windows 10.

3.9 Praca z programem ESET Endpoint Security

Korzystając z ustawień programu ESET Endpoint Security można skonfigurować odpowiedni poziom ochrony komputera, Internetu, poczty e-mail i sieci.



Menu **Ustawienia** zawiera następujące sekcje:

- **Komputer**
- **Sieć**
- **Strony internetowe i poczta e-mail**

Ustawienia ochrony na poziomie **Komputer** umożliwiają włączenie lub wyłączenie następujących komponentów:

- **Ochrona systemu plików w czasie rzeczywistym** — wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu złośliwego kodu.
- **Ochrona dokumentów** — funkcja ochrony dokumentów pozwala na skanowanie dokumentów pakietu Microsoft Office przed ich otwarciem, a także skanowanie plików automatycznie pobieranych przez program Internet Explorer (np. elementów Microsoft ActiveX).
- **System HIPS** — system HIPS monitoruje zdarzenia występujące wewnątrz systemu operacyjnego i reaguje na nie zgodnie z niestandardowym zestawem reguł.
- **Tryb prezentacji** — funkcja przeznaczona dla użytkowników, którzy wymagają niczym niezakłócanego dostępu do swojego oprogramowania, chcą zablokować wszelkie wyskakujące okna i zależy im na zmniejszeniu obciążenia procesora. Po włączeniu Trybu prezentacji zostanie wyświetlony komunikat ostrzegawczy (potencjalne zagrożenie bezpieczeństwa), a główne okno programu zmieni kolor na pomarańczowy.
- **Ochrona Anti-Stealth** — umożliwia wykrywanie niebezpiecznych programów, takich jak programy typu rootkit, które potrafią ukrywać się przed systemem operacyjnym. Wykrycie ich standardowymi sposobami jest niemożliwe.

W sekcji **Sieć** można włączyć lub wyłączyć moduł **Zapora osobista**.

Strony internetowe i poczta e-mail pozwalają włączyć lub wyłączyć następujące komponenty programu:

- **Kontrola dostępu do stron internetowych** — blokuje strony internetowe, które mogą zawierać obraźliwe materiały. Dodatkowo administratorzy systemu mogą określić preferencje dotyczące dostępu dla 27 wstępnie zdefiniowanych kategorii stron internetowych.
- **Ochrona dostępu do stron internetowych** — włączenie tej opcji powoduje skanowanie całego ruchu sieciowego wykorzystującego protokoły HTTP i HTTPS w poszukiwaniu szkodliwego oprogramowania.
- **Ochrona programów poczty e-mail** — monitoruje komunikację odbieraną przy użyciu protokołów POP3 i IMAP.
- **Ochrona przed spamem** — umożliwia skanowanie w poszukiwaniu niepożądanych wiadomości e-mail lub spamu.
- **Ochrona przed atakami typu „phishing"** — chroni użytkownika przed próbami pozyskania haseł, danych bankowych lub innych poufnych informacji przez nielegalnie działające strony internetowe podszywające się pod strony internetowe uprawnione do pozyskiwania tego rodzaju informacji.

Aby tymczasowo wyłączyć pojedyncze moduły, należy kliknąć zielony przełącznik znajdujący się obok wybranego modułu. Należy pamiętać, że taka operacja może zmniejszyć poziom ochrony komputera.

Aby ponownie włączyć ochronę, należy kliknąć czerwony przełącznik, by przywrócić działanie wyłączonego komponentu zabezpieczeń.

UWAGA: Wszystkie mechanizmy ochrony wyłączone w ten sposób zostaną znowu włączone po ponownym uruchomieniu komputera.

Aby uzyskać dostęp do szczegółowych ustawień poszczególnych komponentów zabezpieczeń, należy kliknąć ikonę koła zębatego . obok dowolnego komponentu **.**

Na dole okna ustawień znajduje się kilka dodatkowych opcji. Opcja **Importuj/Eksportuj ustawienia** umożliwia załadowanie ustawień z pliku konfiguracyjnego z rozszerzeniem *.xml* lub zapisanie bieżących ustawień do takiego pliku. Szczegółowe informacje znajdują się w sekcji Importuj/eksportuj ustawienia.

Więcej szczegółowych opcji można wyświetlić, klikając pozycję **Ustawienia zaawansowane** lub naciskając klawisz **F5**.

3.9.1 Komputer

Moduł **Komputer** można znaleźć w obszarze **Ustawienia** > **Komputer**. Widoczne jest w nim zestawienie modułów ochrony opisanych w poprzednim rozdziale. W tej sekcji dostępne są następujące ustawienia:

Należy kliknąć koło zębate obok opcji **Ochrona systemu plików w czasie rzeczywistym**, a następnie pozycję **Edytuj wyłączenia**, by otworzyć okno ustawień Wyłączenia, w którym można wyłączać pliki i foldery ze skanowania.

UWAGA: Stan ochrony dokumentów może nie być dostępny do momentu włączenia tej opcji w obszarze **Ustawienia zaawansowane** (F5) > **Moduł antywirusowy** > **Ochrona dokumentów**. Po włączeniu tej opcji należy uruchomić komputer ponownie, klikając panel ustawień > Komputer, a następnie **Uruchom ponownie** w obszarze Kontrola dostępu do urządzeń. Można też zrobić to przy użyciu panelu Stan ochrony, klikając tam opcję **Uruchom ponownie komputer**.

Wstrzymaj ochronę antywirusową i antyspyware — za każdym razem, gdy ochrona antywirusowa i antyspyware zostaje tymczasowo wyłączona, użytkownik może wybrać z menu rozwijanego okres, przez jaki wybrany komponent będzie wyłączony, a następnie kliknąć pozycję **Zastosuj**, by wyłączyć komponent zabezpieczeń. Aby ponownie włączyć ochronę, należy kliknąć pozycję **Włącz ochronę antywirusową i antyspyware**.

Ustawienia skanowania komputera — kliknięcie tej opcji umożliwia zmodyfikowanie parametrów skanowania komputera (skanowania przeprowadzanego ręcznie).

3.9.1.1 Program antywirusowy

Ochrona antywirusowa zabezpiecza system przed szkodliwymi atakami, sprawdzając pliki, pocztę e-mail i komunikację internetową. W przypadku wykrycia zagrożenia moduł antywirusowy może je wyeliminować przez zablokowanie, a następnie wyleczenie, usunięcie lub przeniesienie do kwarantanny.

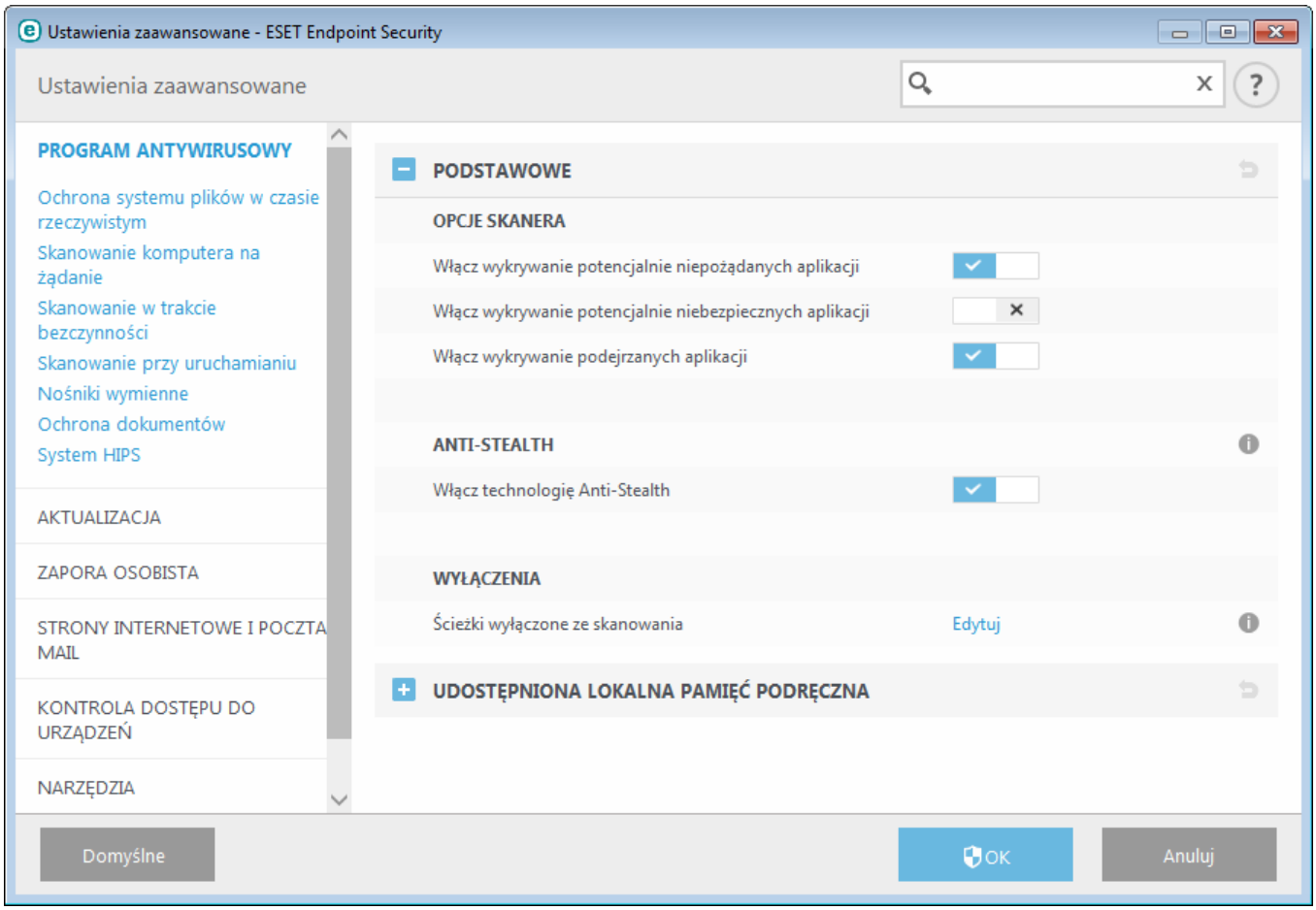
Aby szczegółowo skonfigurować ustawienia modułu antywirusowego, należy kliknąć opcję **Ustawienia zaawansowane** lub nacisnąć klawisz **F5**.

Opcje skanera dla wszystkich modułów ochrony (np. ochrona systemu plików w czasie rzeczywistym, ochrona dostępu do stron internetowych) pozwalają włączać i wyłączać wykrywanie następujących zagrożeń:

- **Potencjalnie niepożądane aplikacje** niekoniecznie były świadomie projektowane w złych intencjach, ale mogą negatywnie wpływać na wydajność komputera.
  Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
- **Potencjalnie niebezpieczne aplikacje** to legalne oprogramowanie komercyjne, które potencjalnie może zostać wykorzystane do szkodliwych celów. Są to między innymi narzędzia do dostępu zdalnego, programy do łamania haseł i programy rejestrujące znaki wprowadzane na klawiaturze (naciśnięcia klawiszy). Domyślnie opcja ta jest wyłączona.
  Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.
- **Podejrzane aplikacje** to programy skompresowane przy użyciu programów pakujących lub zabezpieczających. Programy zabezpieczające tego typu są często używane przez twórców szkodliwego oprogramowania w celu uniknięcia wykrycia.

Technologia Anti-Stealth to zaawansowany system wykrywania niebezpiecznych programów, np. programów typu rootkit, które potrafią ukrywać się przed systemem operacyjnym. Wykrycie ich standardowymi sposobami jest niemożliwe.

Wyłączenia pozwalają wykluczyć ze skanowania wybrane pliki i foldery. Aby zapewnić skanowanie wszystkich obiektów pod kątem zagrożeń, zaleca się tworzenie wyłączeń tylko wtedy, gdy jest to absolutnie konieczne. Do sytuacji, w których może być konieczne wykluczenie obiektu, może zaliczać się skanowanie wpisów dużych baz danych, które spowolniłyby pracę komputera podczas skanowania lub korzystanie z oprogramowania, które powoduje konflikt ze skanowaniem. Informacje na temat wyłączania obiektów ze skanowania można znaleźć w sekcji Wyłączenia.



3.9.1.1.1 Wykrycie infekcji

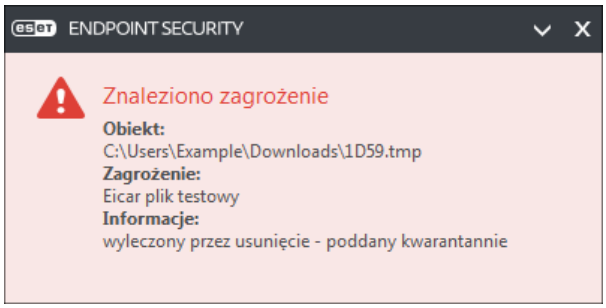
System może zostać zainfekowany z różnych źródeł, takich jak strony internetowe, foldery udostępnione, poczta e-mail lub urządzenia wymienne (USB, dyski zewnętrzne, płyty CD i DVD, dyskietki itp.).

Działanie standardowe

Ogólnym przykładem sposobu działania programu ESET Endpoint Security w momencie infekcji jest ich wykrywanie za pomocą funkcji:

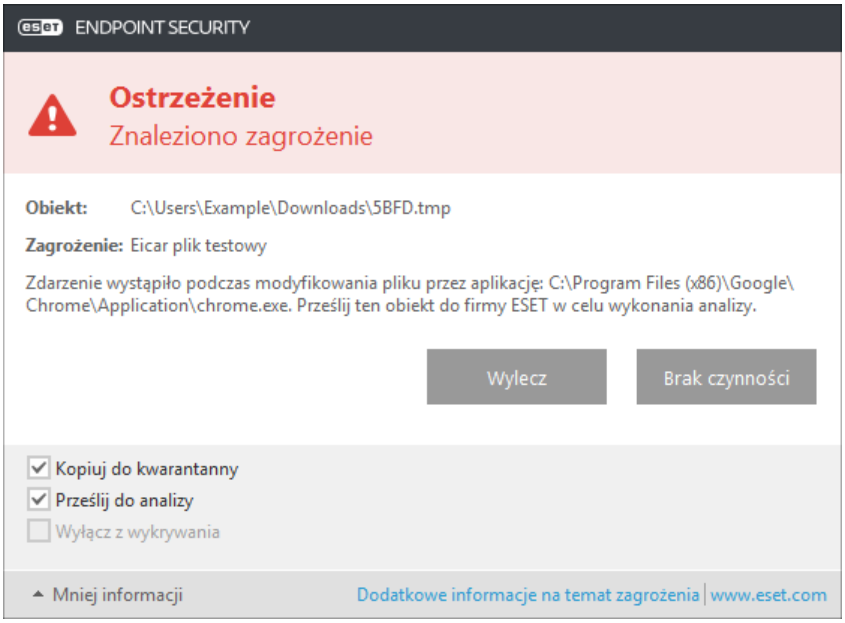
- Ochrona systemu plików w czasie rzeczywistym
- Ochrona dostępu do stron internetowych
- Ochrona programów poczty e-mail
- Skanowanie komputera na żądanie

Każda z tych funkcji stosuje poziom leczenia standardowego, próbując wyleczyć plik i przenieść go do folderu Kwarantanna lub przerywając połączenie. Okno powiadomień jest wyświetlane w obszarze powiadomień w prawym dolnym rogu ekranu. Więcej informacji dotyczących poziomów leczenia i sposobów działania można znaleźć w sekcji Leczenie.



Leczenie i usuwanie

Jeżeli nie określono wstępnie czynności do wykonania przez moduł ochrony plików w czasie rzeczywistym, pojawi się okno alertu z monitem o wybranie opcji. Zazwyczaj dostępne są opcje **Wylecz**, **Usuń** i **Brak czynności**. Nie zaleca się wyboru opcji **Brak czynności**, ponieważ pozostawia to zainfekowane pliki niewyleczone. Wyjątek stanowi sytuacja, w której użytkownik ma pewność, że plik jest nieszkodliwy i został wykryty błędnie.



Leczenie należy stosować w przypadku zainfekowanego pliku, do którego wirus dołączył szkodliwy kod. W takiej sytuacji należy najpierw podjąć próbę wyleczenia zainfekowanego pliku w celu przywrócenia go do stanu pierwotnego. Jeśli plik zawiera wyłącznie szkodliwy kod, jest usuwany w całości.

Jeśli zainfekowany plik jest zablokowany lub używany przez proces systemowy, jest zazwyczaj usuwany po odblokowaniu (zwykle po ponownym uruchomieniu systemu).

Wiele zagrożeń

Jeśli jakieś zainfekowane pliki nie zostały wyleczone podczas skanowania komputera (lub poziom leczenia został ustawiony na **Brak leczenia**), w oknie alertu wyświetlona zostanie prośba o wybranie czynności dotyczących tych plików.

Usuwanie plików w archiwach

W domyślnym trybie leczenia całe archiwum jest usuwane tylko wtedy, gdy zawiera wyłącznie zarażone pliki i nie ma w nim żadnych niezarażonych plików. Oznacza to, że archiwa nie są usuwane, jeśli zawierają również nieszkodliwe, niezainfekowane pliki. Należy zachować ostrożność podczas skanowania w trybie leczenia dokładnego, ponieważ w tym trybie każde archiwum zawierające co najmniej jeden zainfekowany plik jest usuwane bez względu na stan pozostałych zawartych w nim plików.

Jeśli komputer wykazuje objawy zainfekowania szkodliwym oprogramowaniem, na przykład działa wolniej lub często przestaje odpowiadać, zalecane jest wykonanie następujących czynności:

- Otwórz ESET Endpoint Security i kliknij Skanowanie komputera
- Kliknij opcję **Skanowanie inteligentne** (więcej informacji można znaleźć w Skanowanie komputera)
- Po zakończeniu skanowania przejrzyj dziennik, aby sprawdzić liczbę przeskanowanych, zainfekowanych i wyleczonych plików

Aby przeskanować tylko określoną część dysku, kliknij opcję **Skanowanie niestandardowe** i wybierz obiekty, które mają zostać przeskanowane w poszukiwaniu wirusów.

3.9.1.2 Udostępniona lokalna pamięć podręczna

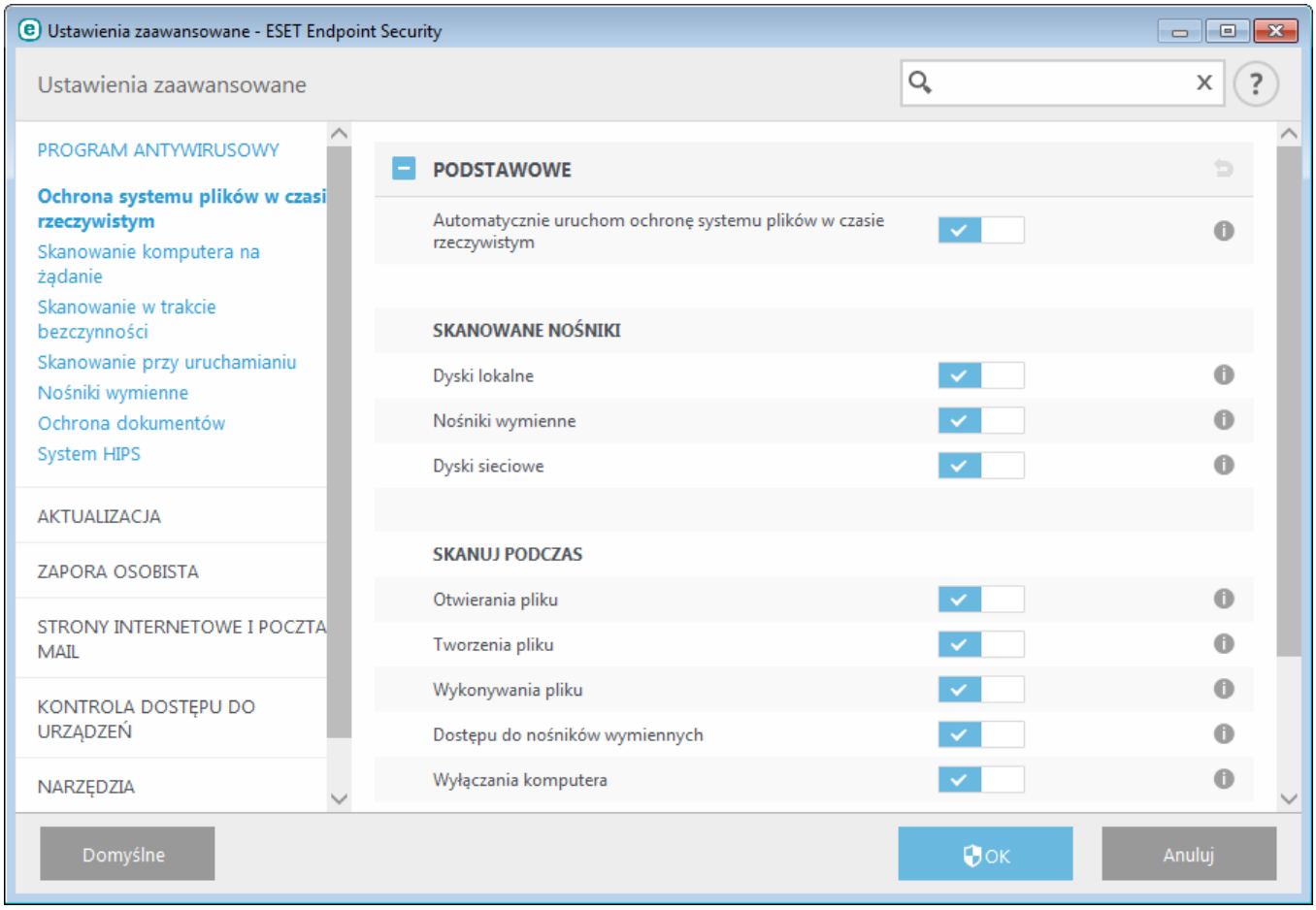
Udostępniona lokalna pamięć podręczna zwiększa wydajność w środowiskach zwirtualizowanych dzięki wyeliminowaniu skanowania duplikatów w sieci. Daje to pewność, że każdy plik zostanie przeskanowany tylko raz i będzie przechowywany w udostępnionej pamięci podręcznej. By zapisywać w lokalnej pamięci podręcznej informacje dotyczące skanowania plików i folderów w sieci, należy włączyć przełącznik **Opcja pamięci podręcznej**. Wykonanie nowego skanu spowoduje, że program ESET Endpoint Security wyszuka skanowane pliki w pamięci podręcznej. Jeśli pliki będą zgodne, zostaną wyłączone ze skanowania.

W ustawieniach **Serwer pamięci podręcznej** znajdują się następujące pozycje**:**

- **Nazwa hosta** — nazwa lub adres IP komputera, na którym umiejscowiona jest pamięć podręczna.
- **Port** — numer portu używanego do komunikacji (taki sam, jak w ustawieniu Udostępniona lokalna pamięć podręczna).
- **Hasło** — ustawienie hasła do udostępnionej lokalnej pamięci podręcznej, jeśli jest wymagane.

3.9.1.3 Ochrona systemu plików w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym sprawdza wszystkie zdarzenia związane z ochroną antywirusową systemu. Wszystkie pliki w momencie otwarcia, utworzenia lub uruchomienia na komputerze są skanowane w poszukiwaniu szkodliwego kodu. Ochrona systemu plików w czasie rzeczywistym jest włączana przy uruchamianiu systemu.



Ochrona systemu plików w czasie rzeczywistym jest domyślnie włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie. W szczególnych przypadkach (np. jeśli wystąpi konflikt z innym skanerem działającym w czasie rzeczywistym), ochronę w czasie rzeczywistym można wyłączyć, wyłączając opcję **Automatycznie uruchom ochronę systemu plików w czasie rzeczywistym** w obszarze **Ustawienia zaawansowane** w sekcji **Ochrona systemu plików w czasie rzeczywistym** > **Podstawowe**.

Skanowane nośniki

Domyślnie wszystkie typy nośników są skanowane w celu wykrycia potencjalnych zagrożeń:

Dyski lokalne — sprawdzane są wszystkie dyski twarde w komputerze.
Nośniki wymienne — sprawdzane są dyskietki, płyty CD i DVD, urządzenia pamięci masowej USB, urządzenia Bluetooth itp.
Dyski sieciowe — skanowane są wszystkie dyski mapowane.

Zalecane jest zachowanie ustawień domyślnych i modyfikowanie ich wyłącznie w szczególnych przypadkach, jeśli na przykład sprawdzanie pewnych nośników znacznie spowalnia przesyłanie danych.

Skanuj podczas

Domyślnie wszystkie pliki są skanowane podczas otwierania, tworzenia i wykonywania. Zalecane jest zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym:

- **Otwierania pliku** — włącza lub wyłącza skanowanie plików przy ich otwieraniu.
- **Tworzenia pliku** — włącza lub wyłącza skanowanie plików przy ich tworzeniu.
- **Wykonywania pliku** — włącza lub wyłącza skanowanie plików przy ich wykonywaniu.
- **Dostępu do nośników wymiennych** — włącza lub wyłącza skanowanie wywoływane przez próbę uzyskania dostępu do określonego wymiennego nośnika pamięci.
- **Wyłączania komputera** — włącza lub wyłącza skanowanie uruchamiane podczas wyłączania komputera.

Moduł ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników. Sprawdzanie jest wywoływane wystąpieniem różnych zdarzeń systemowych, na przykład uzyskaniem dostępu do pliku. Korzystając z metod wykrywania zastosowanych w ramach technologii ThreatSense (opisanych w sekcji Ustawienia parametrów technologii ThreatSense, funkcja ochrony systemu plików w czasie rzeczywistym może działać inaczej w przypadku plików nowo tworzonych, a inaczej w przypadku już istniejących. Na przykład funkcję ochrony systemu plików w czasie rzeczywistym można skonfigurować na dokładniejsze monitorowanie nowo utworzonych plików.

Aby zminimalizować obciążenie systemu podczas korzystania z ochrony w czasie rzeczywistym, przeskanowane pliki nie są skanowane ponownie (dopóki nie zostaną zmodyfikowane). Pliki są niezwłocznie skanowane ponownie po każdej aktualizacji bazy sygnatur wirusów. Taki sposób postępowania jest kontrolowany za pomocą funkcji **Inteligentna optymalizacja**. Po wyłączeniu opcji **Inteligentna optymalizacja** wszystkie pliki są skanowane za każdym razem, gdy uzyskiwany jest do nich dostęp. Aby zmodyfikować to ustawienie, należy nacisnąć klawisz **F5** w celu otwarcia okna Ustawienia zaawansowane i kliknąć kolejno pozycje **Moduł antywirusowy** > **Ochrona systemu plików w czasie rzeczywistym**. Następnie należy kliknąć kolejno **parametr technologii ThreatSense** > **Inne** i zaznaczyć lub odznaczyć opcję **Włącz inteligentną optymalizację**.

3.9.1.3.1 Dodatkowe parametry ThreatSense

Dodatkowe parametry ThreatSense dla nowo utworzonych i zmodyfikowanych plików — prawdopodobieństwo występowania infekcji w nowo utworzonych lub zmodyfikowanych plikach jest stosunkowo większe niż w przypadku istniejących już plików. Dlatego program sprawdza takie pliki z zastosowaniem dodatkowych parametrów skanowania. Oprócz typowych metod skanowania przy użyciu sygnatur stosowana jest również zaawansowana heurystyka, która wykrywa nowe zagrożenia jeszcze przed opublikowaniem aktualizacji bazy sygnatur wirusów. Poza nowo utworzonymi plikami skanowanie obejmuje też archiwa samorozpakowujące (SFX) i programy spakowane (skompresowane wewnętrznie pliki wykonywalne). Domyślnie archiwa są skanowane do dziesiątego poziomu zagnieżdżenia i są sprawdzane niezależnie od ich rozmiaru. Aby zmienić ustawienia skanowania archiwów, należy wyłączyć opcję **Domyślne ustawienia skanowania archiwów**.

Więcej informacji na temat **programów spakowanych**, **archiwów samorozpakowujących** oraz **zaawansowanej heurystyki** można znaleźć w sekcji Ustawienia parametrów technologii ThreatSense.

Dodatkowe parametry ThreatSense dla wykonywanych plików — domyślnie podczas wykonywania plików używana jest zaawansowana heurystyka. Gdy ta opcja jest włączona, zalecamy pozostawienie włączonych opcji inteligentnej optymalizacji oraz ESET Live Grid w celu ograniczenia wpływu na wydajność systemu.

3.9.1.3.2 Poziomy leczenia

W ramach ochrony w czasie rzeczywistym dostępne są trzy poziomy leczenia (aby uzyskać do nich dostęp, należy kliknąć pozycję **Ustawienia parametrów technologii ThreatSense** w sekcji **Ochrona systemu plików w czasie rzeczywistym**, a następnie kliknąć **Leczenie**).

Brak leczenia — Zainfekowane pliki nie będą automatycznie leczone. Wyświetlane jest okno z ostrzeżeniem, a użytkownik może wybrać czynność do wykonania. Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie czynności należy wykonać w razie wystąpienia infekcji.

Leczenie normalne — program próbuje automatycznie wyleczyć lub usunąć zarażony plik zgodnie ze wstępnie zdefiniowaną czynnością (zależnie od typu infekcji). O wykryciu i usunięciu zainfekowanego pliku informuje powiadomienie wyświetlane w prawym dolnym rogu ekranu. Jeśli automatyczne wybranie właściwej czynności nie będzie możliwe, w programie będą dostępne inne czynności kontynuacyjne. Aplikacja zadziała tak samo także wtedy, gdy nie będzie możliwe wykonanie wstępnie zdefiniowanej czynności.

Leczenie dokładne — program leczy lub usuwa wszystkie zarażone pliki. Jedyny wyjątek stanowią pliki systemowe. Jeśli ich wyleczenie nie jest możliwe, użytkownik jest monitowany o wybranie odpowiedniej czynności w oknie z ostrzeżeniem.

Ostrzeżenie: Jeśli archiwum zawiera zarażone pliki, problem można rozwiązać na dwa sposoby. W trybie standardowym (Leczenie standardowe) usunięcie całego archiwum nastąpi w sytuacji, gdy będą zarażone wszystkie znajdujące się w nim pliki. W trybie **Leczenie dokładne** całe archiwum zostanie usunięte po wykryciu pierwszego zarażonego pliku, niezależnie od stanu pozostałych plików w tym archiwum.

3.9.1.3.3 Sprawdzanie skuteczności ochrony w czasie rzeczywistym

Aby sprawdzić, czy funkcja ochrony w czasie rzeczywistym działa i wykrywa wirusy, można użyć pliku z witryny eicar.com. Jest to przygotowany nieszkodliwy plik testowy wykrywany przez wszystkie programy antywirusowe. Został on utworzony przez instytut EICAR (European Institute for Computer Antivirus Research) w celu testowania działania programów antywirusowych. Plik jest dostępny do pobrania pod adresem http://www.eicar.org/download/eicar.com

UWAGA: Przed przystąpieniem do sprawdzenia skuteczności ochrony w czasie rzeczywistym należy wyłączyć zaporę. Włączona zapora wykryje plik testowy i uniemożliwi jego pobranie. Należy pamiętać o ponownym włączeniu zapory natychmiast po sprawdzeniu skuteczności ochrony systemu plików w czasie rzeczywistym.

3.9.1.3.4 Zmienianie ustawień ochrony w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym jest najbardziej istotnym elementem zapewniającym bezpieczeństwo systemu. Podczas zmieniania jej parametrów należy zawsze zachować ostrożność. Modyfikowanie ustawień ochrony jest zalecane tylko w określonych przypadkach.

Po zainstalowaniu programu ESET Endpoint Security wszystkie ustawienia są optymalizowane w celu zapewnienia maksymalnego poziomu bezpieczeństwa systemu. W celu przywrócenia ustawień domyślnych należy kliknąć ikonę ↩ obok każdej z kart w oknie (**Ustawienia zaawansowane** > **Moduł antywirusowy** > **Ochrona systemu plików w czasie rzeczywistym**).

3.9.1.3.5 Co zrobić, jeśli ochrona w czasie rzeczywistym nie działa

W tym rozdziale opisano problemy, które mogą wystąpić podczas korzystania z ochrony w czasie rzeczywistym oraz sposoby ich rozwiązywania.

Ochrona w czasie rzeczywistym jest wyłączona

Jeśli ochrona w czasie rzeczywistym została przypadkowo wyłączona przez użytkownika, należy ją włączyć ponownie. Aby ponownie włączyć ochronę w czasie rzeczywistym, należy w głównym oknie programu przejść do opcji **Ustawienia**, a następnie kliknąć przycisk **Ochrona systemu plików w czasie rzeczywistym**.

Jeśli ochrona w czasie rzeczywistym nie jest inicjowana przy uruchamianiu systemu, najczęściej jest to spowodowane usunięciem zaznaczenia pola wyboru **Automatycznie uruchom ochronę systemu plików w czasie**

rzeczywistym. Aby włączyć tę opcję, należy przejść do okna **Ustawienia zaawansowane** (klawisz **F5**) i kliknąć kolejno pozycje **Ochrona antywirusowa** > **Ochrona systemu plików w czasie rzeczywistym** > **Podstawowe**. Należy upewnić się, że włączona jest opcja **Automatycznie uruchom ochronę systemu plików w czasie rzeczywistym**.

Ochrona w czasie rzeczywistym nie wykrywa ani nie leczy zagrożeń

Należy się upewnić, że na komputerze nie ma zainstalowanych innych programów antywirusowych. Jednoczesne włączenie dwóch modułów ochrony w czasie rzeczywistym może powodować ich konflikt. Zaleca się odinstalowanie innych programów antywirusowych znajdujących się w systemie przed zainstalowaniem programu ESET.

Ochrona w czasie rzeczywistym nie jest uruchamiana

Jeśli ochrona w czasie rzeczywistym nie jest inicjowana przy uruchamianiu systemu (a opcja **Automatycznie uruchom ochronę systemu plików w czasie rzeczywistym** jest włączona), może to być spowodowane konfliktami z innymi programami. W celu uzyskania pomocy w rozwiązaniu tego problemu, należy skontaktować się z działem obsługi klienta firmy ESET.

3.9.1.4 Skanowanie komputera na żądanie

Skaner na żądanie jest ważnym składnikiem programu ESET Endpoint Security. Służy on do badania plików i folderów na komputerze. Z punktu widzenia bezpieczeństwa ważne jest, aby skanowanie komputera było przeprowadzane nie tylko w przypadku podejrzenia infekcji, ale regularnie w ramach rutynowych działań związanych z bezpieczeństwem. Zalecane jest regularne (np. raz w miesiącu) przeprowadzanie dokładnego skanowania systemu w celu wykrycia wirusów, które nie zostają wykryte przez funkcję Ochrona systemu plików w czasie rzeczywistym. Mogłoby się to zdarzyć, gdyby Ochrona systemu plików w czasie rzeczywistym była wyłączona w danym momencie, gdyby baza sygnatur wirusów była nieaktualna lub gdyby plik nie został rozpoznany jako wirus podczas zapisywania go na dysku.

Dostępne są dwa typy operacji **Skanowanie komputera**. Opcja **Skanowanie inteligentne** umożliwia szybkie przeskanowanie systemu bez konieczności dodatkowego konfigurowania parametrów skanowania. Opcja **Skanowanie niestandardowe** umożliwia wybranie jednego ze wstępnie zdefiniowanych profili skanowania oraz określenie obiektów skanowania.

Zobacz rozdział Postęp skanowania, aby uzyskać więcej informacji o procesie skanowania.

Skanowanie inteligentne

Tryb skanowania inteligentnego umożliwia szybkie uruchomienie skanowania komputera i wyleczenie zainfekowanych plików bez konieczności podejmowania dodatkowych działań przez użytkownika. Zaletą skanowania inteligentnego jest łatwość obsługi i brak konieczności szczegółowej konfiguracji skanowania. W ramach skanowania inteligentnego sprawdzane są wszystkie pliki na dyskach lokalnych, a wykryte infekcje są automatycznie leczone lub usuwane. Automatycznie ustawiany jest domyślny poziom leczenia. Szczegółowe informacje na temat typów leczenia można znaleźć w sekcji Leczenie.

Skanowanie niestandardowe

Skanowanie niestandardowe stanowi optymalne rozwiązanie, jeśli użytkownik chce sam określić parametry skanowania, takie jak skanowane obiekty i metody skanowania. Zaletą skanowania niestandardowego jest możliwość szczegółowej konfiguracji parametrów. Konfiguracje można zapisywać w zdefiniowanych przez użytkownika profilach skanowania, które mogą być przydatne, jeśli skanowanie jest przeprowadzane wielokrotnie z zastosowaniem tych samych parametrów.

Aby wybrać skanowane obiekty, należy wybrać kolejno opcje **Skanowanie komputera** > **Skanowanie niestandardowe**, a następnie wybrać odpowiednią pozycję z menu rozwijanego **Skanowane obiekty** lub wybrać żądane obiekty w strukturze drzewa. Skanowane obiekty można również wskazać przez wprowadzenie ścieżki do folderu lub plików, które mają zostać uwzględnione. Jeśli użytkownik chce tylko przeskanować system bez wykonywania dodatkowych działań związanych z leczeniem, należy wybrać opcję **Skanuj bez leczenia**. Podczas przeprowadzania skanowania można wybrać jeden z trzech poziomów leczenia, klikając kolejno opcje **Ustawienia...** > **Parametry technologii ThreatSense** > **Leczenie**.

Skanowanie komputera w trybie skanowania niestandardowego jest odpowiednie dla zaawansowanych

użytkowników, którzy mają już doświadczenie w posługiwaniu się programami antywirusowymi.

Skanowanie nośników wymiennych

Podobnie jak skanowanie inteligentne, ta opcja umożliwia szybkie uruchomienie skanowania nośników wymiennych (takich jak płyta CD/DVD/dysk USB) aktualnie podłączonych do komputera. Jest ona przydatna w przypadku, gdy użytkownik podłączy do komputera dysk USB i chce uruchomić skanowanie jego zawartości w celu wykrycia szkodliwego oprogramowania i innych potencjalnych zagrożeń.

Ten typ skanowania można również uruchomić, klikając opcję **Skanowanie niestandardowe** i wybierając opcję **Nośniki wymienne** z menu rozwijanego **Skanowane obiekty**, a następnie klikając przycisk **Skanuj**.

W celu wybrania czynności, która ma zostać wykonana po zakończeniu skanowania (Brak czynności, Wyłączenie, Ponowne uruchomienie, Uśpij) można posłużyć się menu rozwijanym **Czynność po skanowaniu**.

Aktywacja wyłączania po skanowaniu — powoduje zaplanowane wyłączenie komputera po ukończeniu skanowania na żądanie. Na 60 sekund przed automatycznym wyłączeniem zostanie wyświetlone okno potwierdzenia umożliwiające jego anulowanie. Aby zrezygnować z zamknięcia systemu, należy kliknąć przycisk **Anuluj**.

UWAGA: Zaleca się uruchamianie skanowania komputera co najmniej raz w miesiącu. Skanowanie można skonfigurować jako zaplanowane zadanie za pomocą opcji **Narzędzia** > **Harmonogram**.

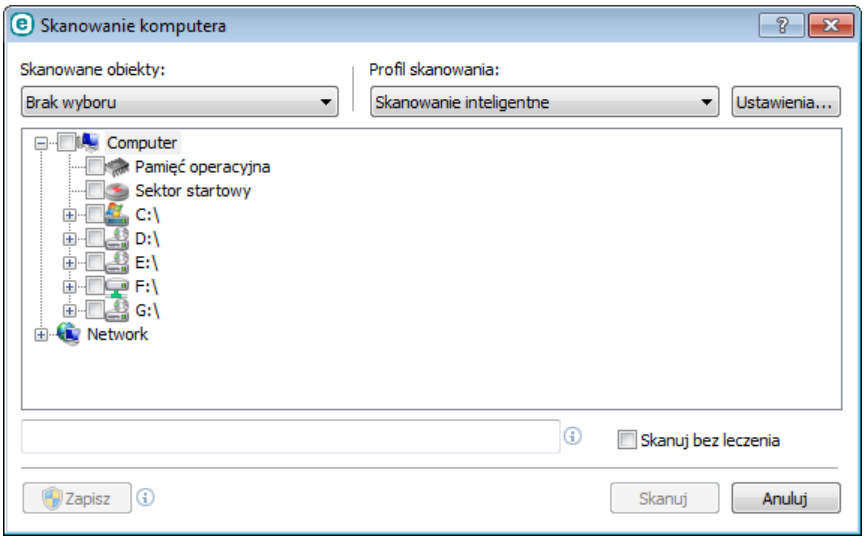
3.9.1.4.1 Program uruchamiający skanowanie niestandardowe

Jeśli użytkownik chce przeprowadzić wyłącznie skanowanie określonego obiektu, możliwe jest użycie narzędzia Skanowanie niestandardowe. W tym celu należy kliknąć kolejno opcje **Skanowanie komputera** > **Skanowanie niestandardowe**, a następnie wybrać z menu rozwijanego opcję **Skanowane obiekty** lub wybrać żądane obiekty w strukturze (drzewie) folderów.

W oknie skanowanych obiektów można określić, jakie obiekty (pamięć, dyski, sektory, pliki i foldery) będą sprawdzane w poszukiwaniu infekcji. Obiekty można wybierać ze struktury drzewa zawierającej wszystkie urządzenia dostępne w komputerze. W menu rozwijanym **Skanowane obiekty** można wybrać wstępnie zdefiniowane obiekty do skanowania:

- **Ustawienia profilu** — powoduje wybranie obiektów skonfigurowanych w wybranym profilu skanowania.
- **Nośniki wymienne** — sprawdzane będą dyskietki, urządzenia pamięci masowej USB, dyski CD i DVD.
- **Dyski lokalne** — wybierane są wszystkie dyski twarde w komputerze.
- **Dyski sieciowe** — powoduje wybranie wszystkich mapowanych dysków sieciowych.
- **Brak wyboru** — wybór obiektów zostaje anulowany.

Aby szybko przejść do skanowanego obiektu lub bezpośrednio dodać żądany obiekt (folder lub plik), należy wprowadzić go w pustym polu znajdującym się poniżej listy folderów. Jest to możliwe tylko wtedy, gdy nie wybrano żadnych obiektów w strukturze drzewa, a w menu **Skanowane obiekty** jest wybrana opcja **Brak wyboru**.



Zainfekowane elementy nie będą automatycznie leczone. Skanowanie bez leczenia umożliwia ocenę skuteczności bieżącego stopnia ochrony. Jeśli użytkownik chce tylko przeskanować system bez wykonywania dodatkowych działań związanych z leczeniem, należy wybrać opcję **Skanuj bez leczenia**. Ponadto można wybrać jeden z trzech poziomów leczenia, klikając kolejno opcje **Ustawienia...** > **Parametry technologii ThreatSense** > **Leczenie**. Informacje na temat skanowania są umieszczane w dzienniku skanowania.

W menu rozwijanym **Profil skanowania** można wybrać profil, który ma być używany podczas skanowania wybranych obiektów. Profilem domyślnym jest **Skanowanie inteligentne**. Istnieją jeszcze dwa wstępnie zdefiniowane profile skanowania: **Skanowanie dokładne** i **Skanowanie z poziomu menu kontekstowego**. W tych profilach skanowania stosowane są różne parametry aparatu ThreatSense. Kliknij przycisk **Ustawienia**, aby szczegółowo skonfigurować wybrany profil skanowania w menu Profil skanowania. Dostępne opcje opisano w sekcji **Inne** w części Ustawienia parametrów technologii ThreatSense.

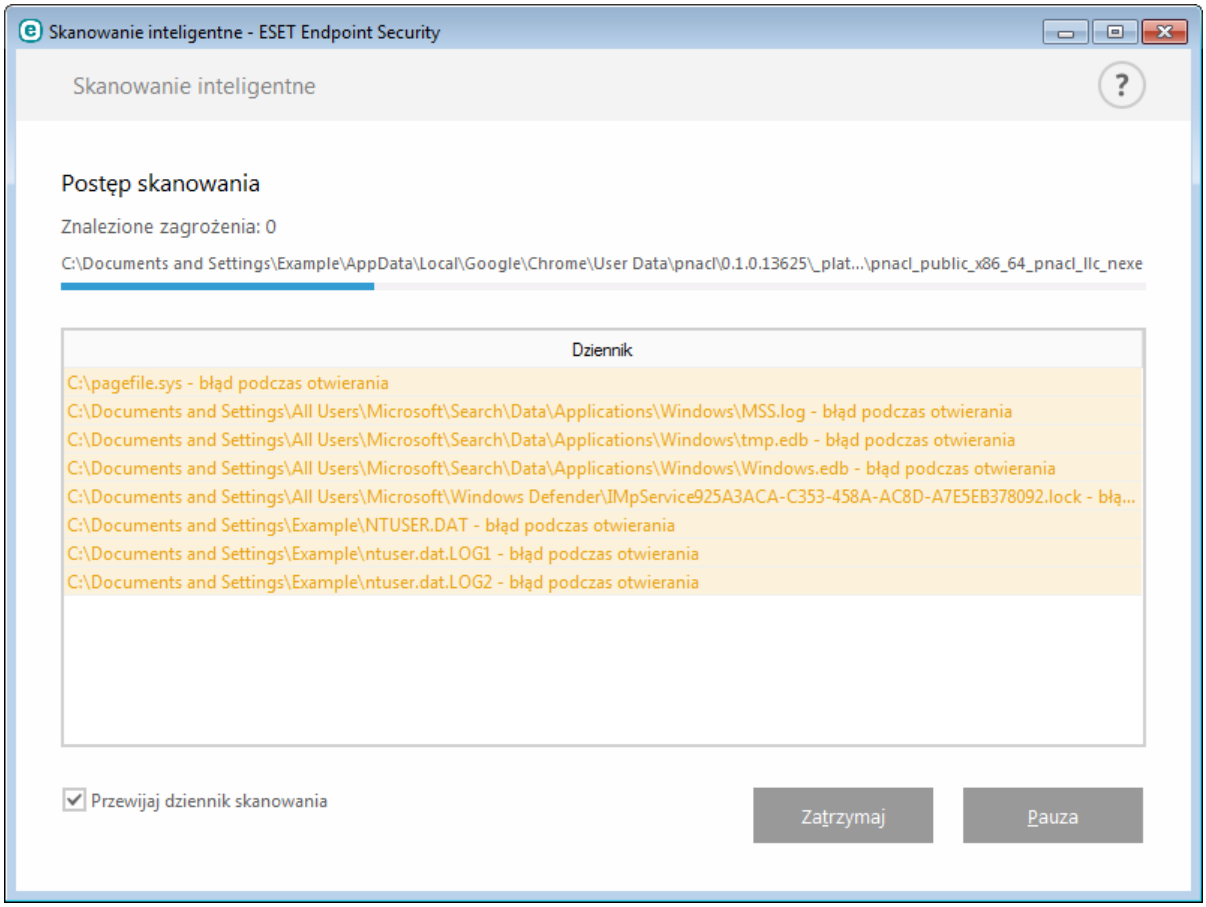
Kliknij przycisk **Zapisz**, aby zapisać zmiany dokonane podczas wybierania obiektów wraz z obiektami wybranymi w strukturze drzewa.

Kliknij przycisk **Skanowanie**, aby przeprowadzić skanowanie z wykorzystaniem ustawionych parametrów niestandardowych.

Skanuj jako administrator pozwala na przeprowadzenie skanowania z uprawnieniami administratora. Tę opcję należy kliknąć, jeśli obecny użytkownik nie ma uprawnień pozwalających na dostęp do plików, które mają być skanowane. Uwaga: ten przycisk jest niedostępny, jeśli aktualny użytkownik nie może wywoływać operacji UAC jako administrator.

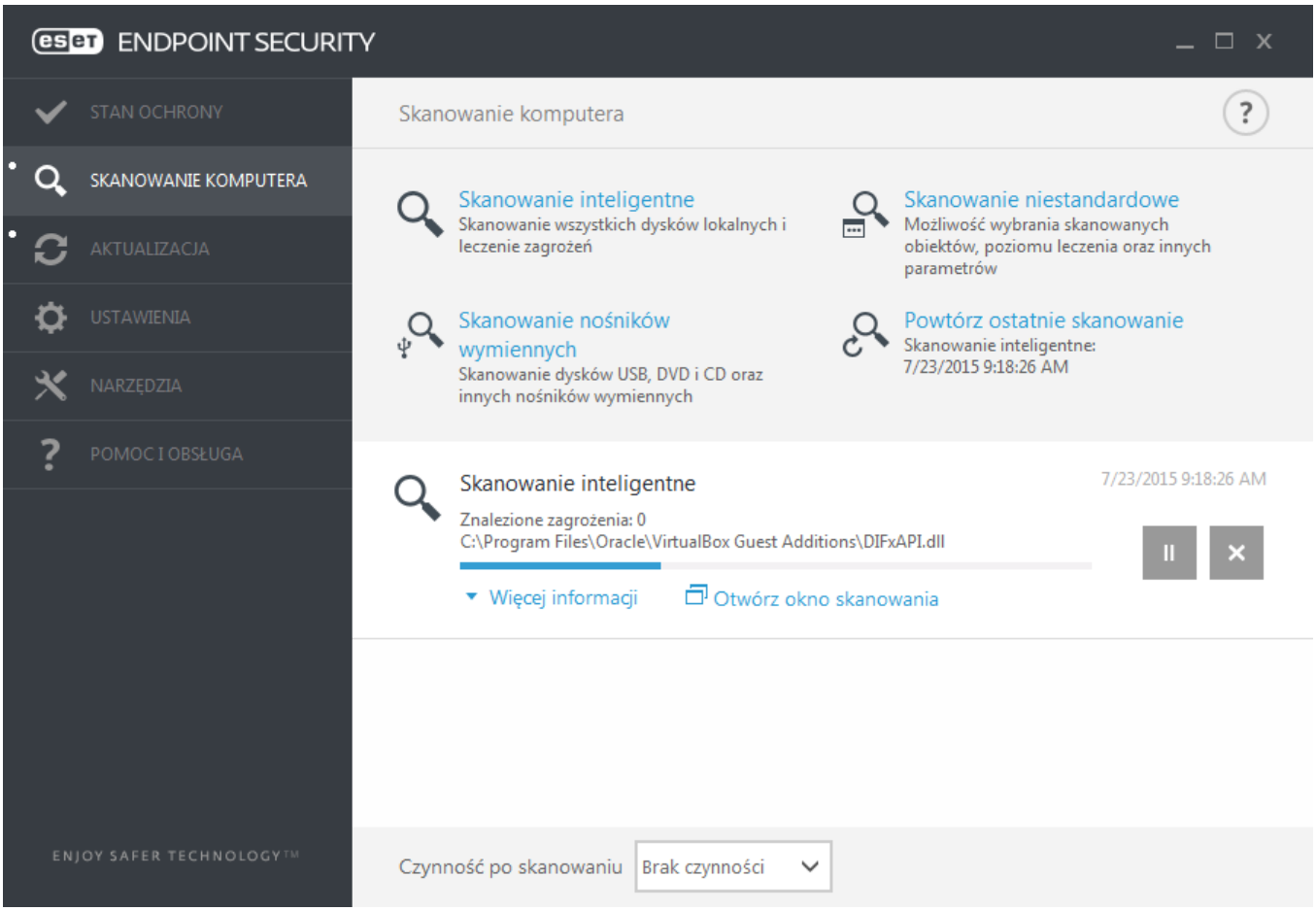
3.9.1.4.2 Postęp skanowania

W oknie postępu skanowania wyświetlany jest bieżący stan skanowania oraz informacje dotyczące liczby znalezionych plików zawierających złośliwy kod.



UWAGA: Jest całkowicie normalne, że nie można przeskanować części plików, na przykład plików zabezpieczonych hasłem lub plików używanych przez system na prawach wyłączności (zwykle dotyczy to pliku *pagefile.sys* i określonych plików dziennika).

Postęp skanowania — pasek postępu wskazuje stan przeskanowanych już obiektów w odniesieniu do obiektów pozostałych do przeskanowania. Ta wartość postępu skanowania jest obliczana na podstawie całkowitej liczby obiektów zakwalifikowanych do skanowania.
Obiekt docelowy — nazwa i położenie obecnie skanowanego obiektu.
Znalezione zagrożenia — łączna liczba zagrożeń wykrytych podczas skanowania.
Przerwij — umożliwia wstrzymanie skanowania.
Wznów — ta opcja jest widoczna, gdy skanowanie jest wstrzymane. Kliknięcie opcji **Wznów** powoduje kontynuowanie skanowania.
Zatrzymaj — umożliwia przerwanie skanowania.
Przewijaj dziennik skanowania — po włączeniu tej opcji dziennik skanowania będzie automatycznie przewijany w miarę dodawania nowych wpisów, co zapewni widoczność najnowszych wpisów.



3.9.1.5 Kontrola dostępu do urządzeń

ESET Endpoint Security udostępnia funkcje automatycznej kontroli korzystania z urządzeń (CD, DVD, USB/...). Przy użyciu tego modułu można skanować, blokować i dostosowywać rozszerzone filtry i uprawnienia oraz określać uprawnienia dostępu użytkowników do danego urządzenia i pracy z nim. Może to być przydatne w sytuacji, gdy administrator komputera zamierza uniemożliwić korzystanie z urządzeń z niepożądaną zawartością.

Obsługiwane urządzenia zewnętrzne:

- Pamięć masowa (dysk twardy, dysk wymienny USB)
- Płyta CD/DVD
- Drukarka USB
- Pamięć masowa FireWire
- Urządzenie Bluetooth
- Czytnik kart inteligentnych
- Urządzenie do tworzenia obrazów
- Modem
- Port LPT/COM
- Urządzenie przenośne
- Urządzenia dowolnego typu

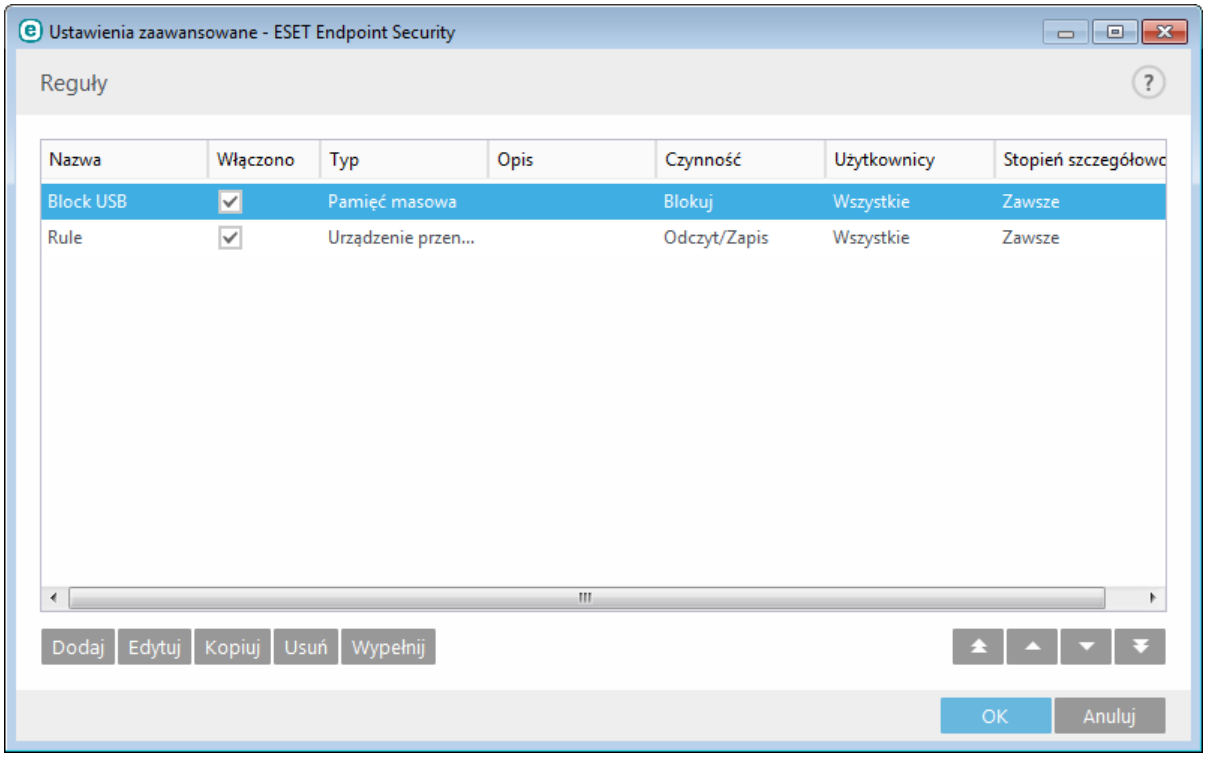
Opcje ustawień kontroli dostępu do urządzeń można zmienić w obszarze **Ustawienia zaawansowane** (F5) > **Kontrola dostępu do urządzeń**.

Włączenie przełącznika obok opcji **Zintegruj z systemem** aktywuje funkcję kontroli dostępu do urządzeń w programie ESET Endpoint Security. Aby zmiana została zastosowana, należy uruchomić komputer ponownie. Po włączeniu kontroli dostępu do urządzeń **reguły** zostaną uaktywnione, co umożliwi otwarcie okna Edytor reguł.

W przypadku podłączenia urządzenia blokowanego przez istniejącą regułę zostanie wyświetlone okno powiadomienia i dostęp do urządzenia nie będzie możliwy.

3.9.1.5.1 Edytor reguł kontroli dostępu do urządzeń

W oknie **Edytor reguł kontroli dostępu do urządzeń** są wyświetlane istniejące reguły. Umożliwia ono również dokładną kontrolę urządzeń zewnętrznych podłączanych przez użytkowników do komputera.



Można dopuszczać lub blokować określone urządzenia na podstawie użytkowników, grup użytkowników lub dowolnych spośród dostępnych parametrów dodatkowych, które można określić w konfiguracji reguł. Lista reguł zawiera pewne informacje o regułach, takie jak nazwa, typ urządzenia zewnętrznego, czynność wykonywana po jego podłączeniu do komputera i stopień ważności w dzienniku.

Kliknięcie przycisku **Dodaj** lub **Edytuj** umożliwia zarządzanie regułą. Odznaczenie pola wyboru **Włączona** obok reguły powoduje jej wyłączenie do momentu jej ponownego użycia w przyszłości. Można zaznaczyć jedną lub większą liczbę reguł i kliknąć opcję **Usuń**, aby trwale usunąć reguły.

Kopiuj — umożliwia utworzenie nowej reguły ze wstępnie zdefiniowanymi opcjami pochodzącymi z innej wybranej reguły.

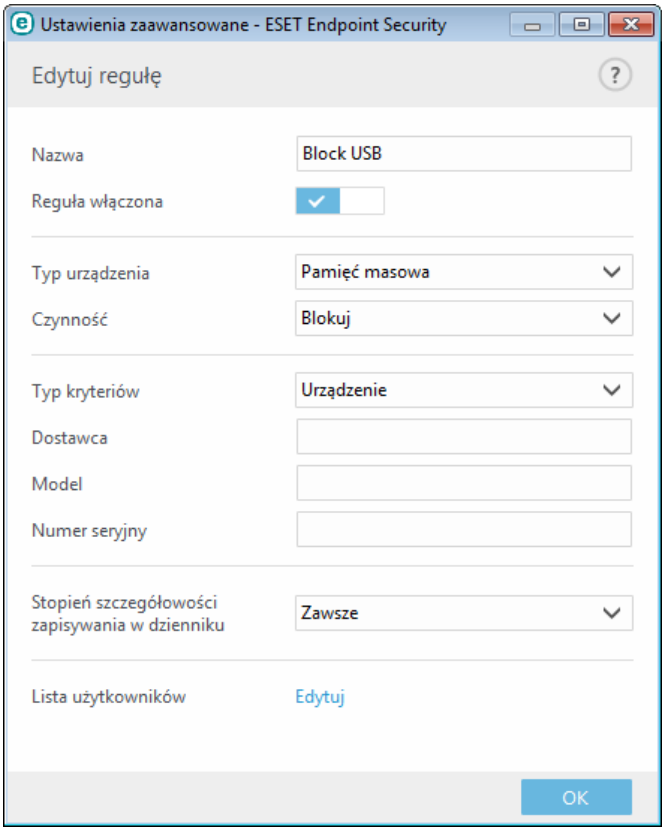
Kliknięcie przycisku **Wypełnij** umożliwia automatyczne wprowadzenie parametrów nośników wymiennych dla urządzeń podłączonych do komputera.

Reguły są wymienione według priorytetów, przy czym reguły o wyższych priorytetach znajdują się wyżej na liście. Reguły można przenosić pojedynczo lub grupami, klikając opcje **Na początek/W górę/W dół/Na koniec**.

W dzienniku kontroli dostępu do urządzeń rejestrowane są wszystkie zdarzenia, w przypadku których uruchamiana jest funkcja kontroli dostępu do urządzeń. Wpisy dziennika można wyświetlać w oknie głównym programu ESET Endpoint Security w obszarze **Narzędzia** > **Pliki dziennika**.

3.9.1.5.2 Dodawanie reguł kontroli dostępu do urządzeń

Reguła kontroli dostępu do urządzeń definiuje czynność podejmowaną w chwili, gdy urządzenie spełniające kryteria reguły zostanie podłączone do komputera.



W celu łatwiejszego rozpoznawania reguł należy wprowadzać ich krótkie opisy w polu **Nazwa**. Kliknięcie przełącznika obok pozycji **Reguła włączona** pozwala wyłączać i włączać regułę. Jest to przydatne, gdy użytkownik nie chce trwale usuwać danej reguły.

Typ urządzenia

Typ urządzenia zewnętrznego (Pamięć masowa, Urządzenie przenośne, Bluetooth, FireWire itd.) można wybrać z menu rozwijanego. Informacje dotyczące typów urządzeń są pobierane z systemu operacyjnego i jeśli urządzenie jest podłączone do komputera, można je zobaczyć w systemowym Menedżerze urządzeń. Do urządzeń pamięci masowej zalicza się dyski zewnętrzne oraz konwencjonalne czytniki kart pamięci podłączone za pomocą złącza USB lub FireWire. Czytniki kart inteligentnych obejmują wszystkie czytniki kart z wbudowanym układem scalonym, takich jak karty SIM lub karty uwierzytelniające. Przykładami urządzeń do tworzenia obrazów są skanery i aparaty fotograficzne. Ponieważ te urządzenia udostępniają wyłącznie informacje dotyczące realizowanych przez nie czynności, nie dostarczając informacji dotyczących użytkowników, można je tylko zablokować globalnie.

Czynność

Można zezwalać na dostęp do urządzeń innych niż urządzenia pamięci masowej lub go blokować. Reguły dotyczące urządzeń pamięci masowej umożliwiają natomiast wybranie jednego z poniższych ustawień:

- **Odczyt/zapis** — dozwolony będzie pełny dostęp do urządzenia.
- **Blokuj** — dostęp do urządzenia zostanie zablokowany.
- **Tylko do odczytu** — dozwolony będzie wyłącznie dostęp do urządzenia w trybie do odczytu.
- **Ostrzeżenie** — za każdym razem po podłączeniu urządzenia użytkownik zostanie powiadomiony, czy jest ono dozwolone czy zablokowane i zostanie wygenerowany wpis dziennika. Urządzenia nie są zapamiętywane, a powiadomienie będzie wyświetlane przy każdym następnym połączeniu z tym samym urządzeniem.

Należy pamiętać, że nie dla każdego typu urządzenia dostępne są wszystkie czynności (uprawnienia). W przypadku urządzeń pamięci masowej dostępne są wszystkie cztery czynności.. W przypadku urządzeń innych niż urządzenia pamięci masowej, dostępne są tylko trzy czynności (np. opcja **Tylko do odczytu** jest niedostępna dla urządzeń

Bluetooth, dlatego można tylko zezwolić na dostęp do tych urządzeń, blokować dostęp lub wyświetlać ostrzeżenie).

Typ kryteriów — należy wybrać pozycję **Grupa urządzeń** lub **Urządzenie**.

Poniżej przedstawiono dodatkowe parametry, które można wykorzystać do uszczegółowienia reguł i dopasowania ich do urządzeń. W parametrach nie jest rozróżniana wielkość liter:

- **Dostawca** — filtrowanie według nazwy lub identyfikatora dostawcy.
- **Model** — podana nazwa urządzenia.
- **Numer seryjny** — urządzenia zewnętrzne mają zwykle numery seryjne. W przypadku dysków CD i DVD jest to numer seryjny danego nośnika, a nie napędu.

UWAGA: Jeśli te parametry nie zostaną zdefiniowane, te pola zostaną pominięte przez regułę podczas dopasowywania. W odniesieniu do parametrów filtrowania we wszystkich polach testowych rozróżniana jest wielkość liter i nie są obsługiwane symbole wieloznaczne (*, ?).

PORADA: W celu wyświetlenia informacji na temat urządzenia należy utworzyć regułę dla urządzeń tego typu, podłączyć urządzenie do komputera, a następnie zapoznać się ze szczegółami urządzenia w dzienniku kontroli dostępu do urządzeń.

Stopień szczegółowości

- **Zawsze** — rejestrowanie wszystkich zdarzeń.
- **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszenia konfiguracji programu.
- **Informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Brak** — nie są rejestrowane żadne dzienniki.

Reguły mogą być ograniczane do pewnych użytkowników lub grup użytkowników znajdujących się na liście **Lista użytkowników**:

- **Dodaj** — umożliwia otwarcie okna dialogowego **Typ obiektu: Użytkownicy lub Grupy**, w którym można wybrać pożądanych użytkowników.
- **Usuń** — umożliwia usunięcie wybranego użytkownika z filtru.

UWAGA: Przy użyciu reguł użytkownika można filtrować wszystkie urządzenia (np. urządzenia do tworzenia obrazów, które nie dostarczają informacji na temat użytkowników, tylko na temat wykonywanych czynności).

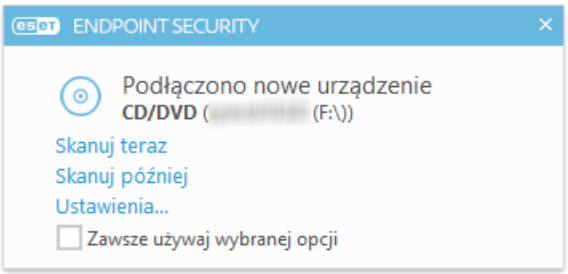
3.9.1.6 Nośniki wymienne

Program ESET Endpoint Security udostępnia funkcję automatycznego skanowania nośników wymiennych (CD, DVD, USB i innych). Ten moduł pozwala na skanowanie włożonego nośnika. Dzięki temu administrator komputera może uniemożliwić użytkownikom korzystanie z nośników wymiennych z niepożądaną zawartością.

Czynność do wykonania po włożeniu nośnika wymiennego — umożliwia wybór domyślnej czynności, która zostanie wykonana po włożeniu do komputera nośnika wymiennego (CD/DVD/USB). Jeśli wybrana jest opcja **Pokaż opcje skanowania**, wyświetlone zostanie okno z powiadomieniem umożliwiające wybranie czynności:

- **Nie skanuj** — nie zostaną wykonane żadne czynności, a okno **Podłączono nowe urządzenie** zostanie zamknięte.
- **Automatyczne skanowanie urządzeń** — włożony nośnik wymienny zostanie poddany skanowaniu na żądanie.
- **Pokaż opcje skanowania** — powoduje otwarcie sekcji Nośniki wymienne w ustawieniach.

Po włożeniu nośnika wymiennego pojawi się następujące okno dialogowe:



Skanuj teraz — powoduje rozpoczęcie skanowania nośnika wymiennego.

Skanuj później — skanowanie nośnika wymiennego zostanie odłożone.

Ustawienia — powoduje otwarcie opcji Ustawienia zaawansowane.

Zawsze używaj wybranej opcji — po wybraniu tej opcji, gdy nośnik wymienny po raz kolejny zostanie włożony, wykonana zostanie ta sama czynność.

Ponadto program ESET Endpoint Security oferuje funkcję Kontrola dostępu do urządzeń, która umożliwia definiowanie reguł dotyczących używania urządzeń zewnętrznych na danym komputerze. Więcej szczegółowych informacji dotyczących funkcji Kontrola dostępu do urządzeń można znaleźć w sekcji Kontrola dostępu do urządzeń.

3.9.1.7 Skanowanie w trakcie bezczynności

Skanowanie w trakcie bezczynności można włączyć w obszarze **Ustawienia zaawansowane** po kliknięciu opcji **Moduł antywirusowy** > **Skanowanie w trakcie bezczynności** > **Podstawowe**. W celu włączenia tej funkcji należy ustawić przełącznik widoczny obok pozycji **Włącz skanowanie w trakcie bezczynności** w pozycji **Włączone**. Gdy komputer jest w stanie bezczynności, skanowanie komputera w trybie cichym jest wykonywane na wszystkich dyskach lokalnych. Zob. także Uruchamianie wykrywania stanu bezczynności w celu uzyskania pełnej listy warunków, które muszą zostać spełnione w celu uruchomienia skanera w trybie bezczynności.

Domyślnie skaner w trybie bezczynności nie pracuje, gdy komputer (notebook) jest zasilany z baterii. Można zmienić to ustawienie, włączając opcję **Uruchom, nawet jeśli komputer jest zasilany z baterii** w Ustawieniach zaawansowanych.

Włączenie przełącznika opcji **Włącz zapisywanie w dzienniku** w Ustawieniach zaawansowanych umożliwia rejestrowanie danych wyjściowych skanowania komputera w sekcji Pliki dziennika (w oknie głównym programu należy kliknąć przycisk **Narzędzia** > **Pliki dziennika** i wybrać opcję **Skanowanie komputera** z menu rozwijanego **Dziennik**).

Wykrywanie stanu bezczynności będzie uruchamiane, gdy komputer znajdzie się w jednym z następujących stanów:

- Wygaszacz ekranu
- Blokada komputera
- Wylogowanie użytkownika

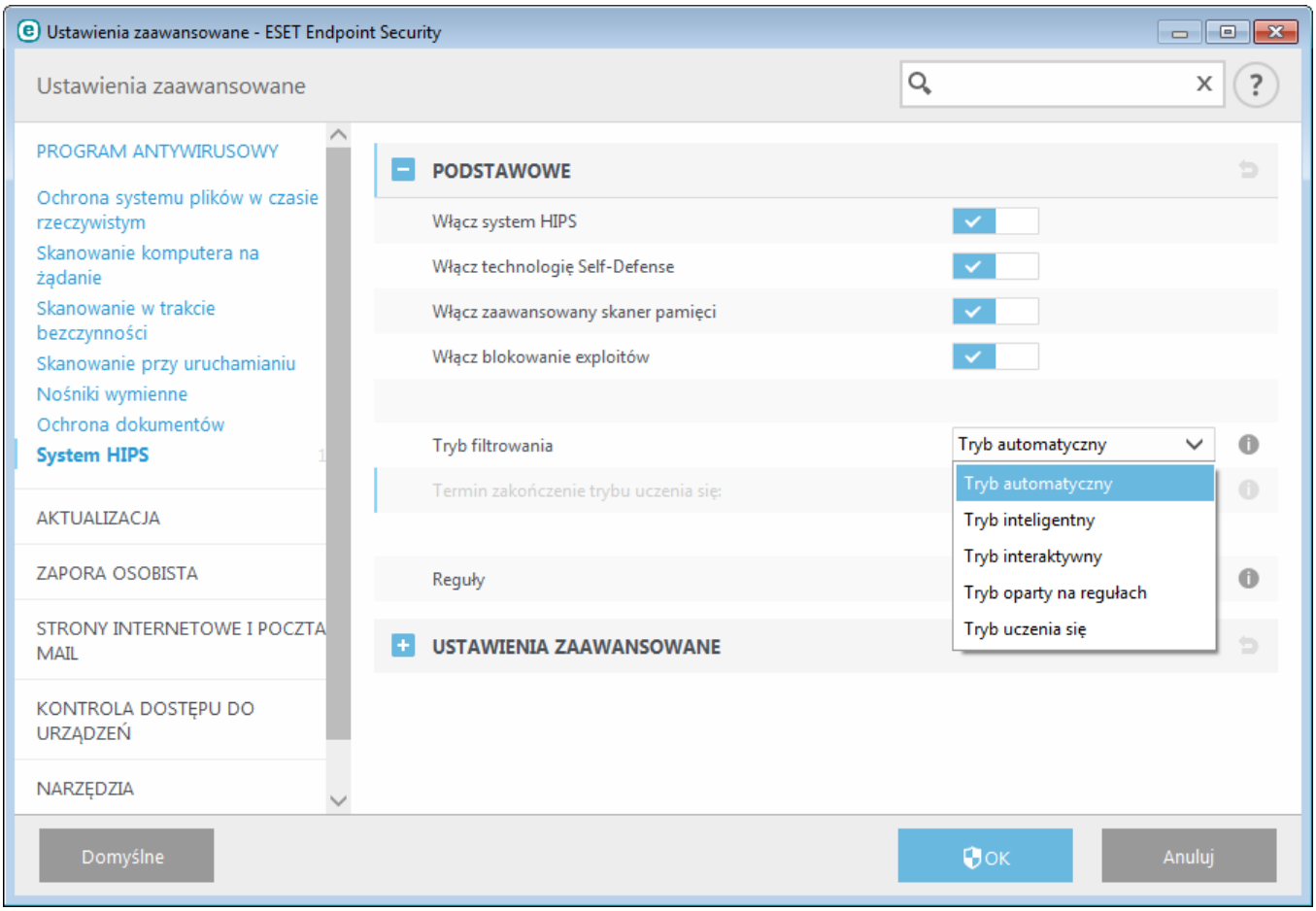
W celu zmodyfikowania parametrów skanowania w trakcie bezczynności (np. metod wykrywania) należy kliknąć pozycję Ustawienia parametrów technologii ThreatSense.

3.9.1.8 System zapobiegania włamaniom działający na hoście (HIPS)

Zmiany w ustawieniach systemu HIPS powinni wprowadzać jedynie doświadczeni użytkownicy. Nieprawidłowe skonfigurowanie ustawień systemu HIPS może spowodować niestabilność systemu.

System zapobiegania włamaniom działający na hoście (ang. Host-based Intrusion Prevention System, HIPS) chroni system operacyjny przed szkodliwym oprogramowaniem i niepożądanymi działaniami mającymi na celu wywarcie negatywnego wpływu na komputer użytkownika. W rozwiązaniu tym używana jest zaawansowana analiza behawioralna powiązana z metodami wykrywania stosowanymi w filtrze sieciowym. Dzięki temu system HIPS monitoruje uruchomione procesy, pliki i klucze rejestru. System HIPS jest modułem oddzielnym względem ochrony systemu plików w czasie rzeczywistym i nie jest zaporą. Monitoruje on tylko procesy uruchomione w systemie operacyjnym.

Ustawienia systemu HIPS można znaleźć w obszarze **Ustawienia zaawansowane** (F5) > **Moduł antywirusowy** > **System HIPS** > **Podstawowe**. Stan systemu HIPS (włączony/wyłączony) widoczny jest w oknie głównym programu ESET Endpoint Security, w obszarze **Ustawienia** > **Komputer**.



W programie ESET Endpoint Security stosowana jest wbudowana technologia Self-defense, która zapobiega uszkodzeniu lub wyłączeniu ochrony antywirusowej i antyspyware przez szkodliwe oprogramowanie, co daje pewność, że komputer jest chroniony w sposób nieprzerwany. Wyłączenie systemu HIPS lub technologii Self-Defense wymaga ponownego uruchomienia systemu Windows.

Zaawansowany skaner pamięci działa w połączeniu z blokadą programów typu Exploit w celu wzmocnienia ochrony przed szkodliwym oprogramowaniem, które unika wykrycia przez produkty do ochrony przed szkodliwym oprogramowaniem poprzez zastosowanie zaciemniania kodu i/lub szyfrowania. Zaawansowany skaner pamięci jest domyślnie włączony. Więcej informacji na temat ochrony tego typu można znaleźć w słowniczku.

Blokada programów typu Exploit ma na celu wzmocnienie używanych zazwyczaj typów aplikacji, takich jak przeglądarki internetowe, przeglądarki plików PDF, programy poczty e-mail oraz składniki pakietu MS Office.

Blokada programów typu Exploit jest domyślnie włączona. Więcej informacji na temat ochrony tego typu można znaleźć w słowniczku.

Filtrowanie może działać w jednym z czterech trybów:

Tryb automatyczny — dozwolone są wszystkie operacje z wyjątkiem operacji zablokowanych przez wstępnie zdefiniowane reguły chroniące komputer.

Tryb interaktywny — użytkownik jest monitowany o potwierdzenie operacji.

Tryb oparty na regułach — operacje są blokowane.

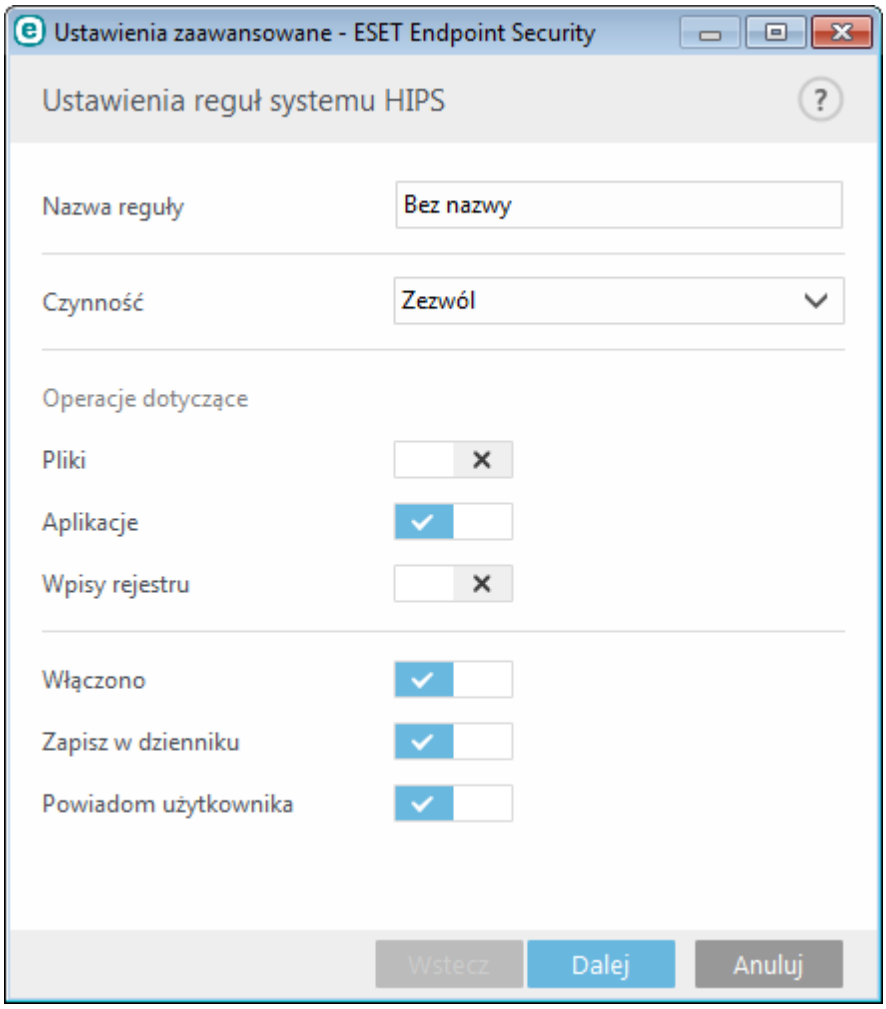
Tryb uczenia się — operacje są dozwolone, a po każdej operacji jest tworzona reguła. Reguły utworzone w tym trybie można przeglądać w oknie Edytor reguł. Mają one niższy priorytet niż reguły utworzone ręcznie i utworzone w trybie automatycznym. Po wybraniu trybu uczenia się z menu rozwijanego trybu filtrowania HIPS udostępnione zostanie ustawienie **Termin zakończenia trybu uczenia się**. Użytkownik może wskazać, na jaki czas chce włączyć tryb uczenia się. Maksymalny dostępny czas to 14 dni. Po upływie wskazanego czasu zostanie wyświetlony monit o przeprowadzenie edycji reguł utworzonych przez system HIPS w trybie uczenia się. Można również wybrać różne tryby filtrowania lub odroczyć podjęcie decyzji i kontynuować korzystanie z trybu uczenia się.

Tryb inteligentny — użytkownik będzie powiadamiany wyłącznie o szczególnie podejrzanych zdarzeniach.

System HIPS monitoruje zdarzenia w systemie operacyjnym i reaguje na nie na podstawie reguł podobnych do reguł używanych przez zaporę osobistą. Kliknięcie opcji **Edytuj** powoduje otwarcie okna zarządzania regułami systemu HIPS. Tutaj można wybierać, tworzyć, edytować i usuwać reguły.

W poniższym przykładzie pokazano, jak ograniczyć niepożądane działania aplikacji:

1. Nadaj nazwę regule i w menu rozwijanym **Czynność** wybierz polecenie **Blokuj**.
2. Użyj przełącznika **Powiadom użytkownika**, aby wyświetlać powiadomienie za każdym razem, gdy reguła jest stosowana.
3. Wybierz co najmniej jedną operację, w odniesieniu do której reguła będzie stosowana. W oknie **Aplikacje źródłowe** z menu rozwijanego wybierz opcję **Wszystkie aplikacje**, aby zastosować nową regułę do wszystkich aplikacji próbujących wykonać dowolną z wybranych czynności na aplikacjach w odniesieniu do podanych aplikacji.
4. Wybierz opcję **Zmodyfikuj stan innej aplikacji** (wszystkie operacje są opisane w pomocy dotyczącej produktu, do której można uzyskać dostęp przez naciśnięcie klawisza F1).
5. Z menu rozwijanego wybierz opcję **Określone aplikacje** i **dodaj** jedną lub więcej aplikacji, które mają być objęte ochroną.
6. Kliknij przycisk **Zakończ**, aby zapisać nową regułę.



3.9.1.8.1 Ustawienia zaawansowane

Poniższe opcje są przydatne podczas debugowania i analizowania działania aplikacji:

Sterowniki zawsze mogą być ładowane — wybrane sterowniki zawsze mogą być ładowane bez względu na skonfigurowany tryb filtrowania, chyba że zostaną wyraźnie zablokowane przez regułę użytkownika.

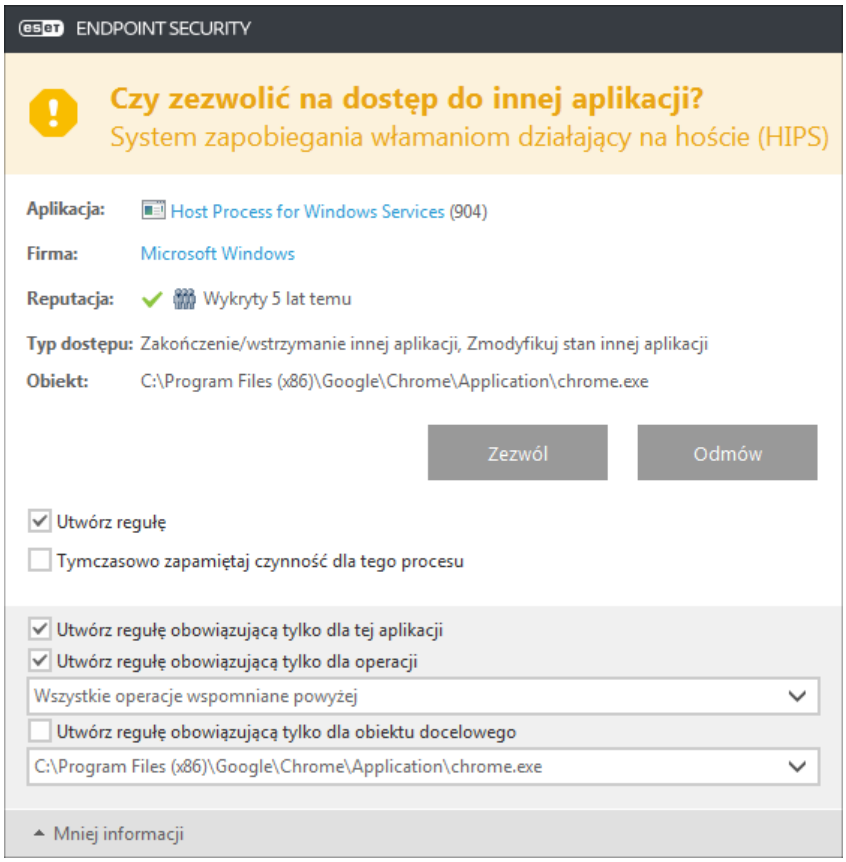
Zapisuj w dzienniku informacje o wszystkich zablokowanych operacjach — wszystkie zablokowane operacje zostaną zarejestrowane w dzienniku systemu HIPS.

Powiadamiaj o zmianach w aplikacjach uruchomieniowych — wyświetla powiadomienie na pulpicie za każdym razem, gdy aplikacja jest dodawana lub usuwana z listy aplikacji wykonywanych przy uruchamianiu systemu.

Zaktualizowaną wersję tej strony pomocy można znaleźć w artykule bazy wiedzy.

3.9.1.8.2 Okno interaktywne systemu HIPS

Jeśli czynnością domyślną ustawioną dla danej reguły jest **Pytaj**, po każdym uruchomieniu danej reguły wyświetlone zostanie okno dialogowe. Można wybrać opcję **Odmów** lub **Zezwól**. Jeśli użytkownik nie wybierze żadnej opcji przed upływem ustalonego czasu, nowa reakcja zostanie wybrana na podstawie reguł.



Okno dialogowe umożliwia tworzenie reguł w oparciu o dowolne nowe czynności wykrywane przez system HIPS, a następnie określenie warunków, na jakich dana czynność ma być dozwolona lub zabroniona. Dokładne parametry można ustawić po kliknięciu przycisku **Więcej informacji**. Utworzone w ten sposób reguły są traktowane tak samo jak reguły utworzone ręcznie, dlatego reguła utworzona z poziomu okna dialogowego może być ogólniejsza niż reguła, która spowodowała otwarcie tego okna. Oznacza to, że po utworzeniu takiej reguły ta sama operacja może spowodować otwarcie tego samego okna.

Opcja **Tymczasowo zapamiętaj czynność dla tego procesu** powoduje stosowanie czynności (**Zezwól/Odmów**) do czasu zmiany reguł lub trybu filtrowania, aktualizacji modułu HIPS lub ponownego uruchomienia systemu. Po wystąpieniu dowolnej z tych trzech czynności reguły tymczasowe zostaną usunięte.

3.9.1.9 Tryb prezentacji

Tryb prezentacji to funkcja przeznaczona dla użytkowników, którzy wymagają niczym niezakłócanego dostępu do swojego oprogramowania, chcą zablokować wszelkie wyskakujące okna i zależy im na zmniejszeniu obciążenia procesora. Tryb prezentacji może być również wykorzystywany podczas prezentacji, które nie mogą być przerywane działaniem programu antywirusowego. Po włączeniu tego trybu wyłączane są wszystkie wyskakujące okna i nie są uruchamiane zaplanowane zadania. Ochrona systemu pozostaje aktywna w tle, ale nie wymaga interwencji użytkownika.

Kliknięcie kolejno opcji **Ustawienia** > **Komputer**, a następnie użycie przełącznika obok opcji **Tryb prezentacji** umożliwia ręczne włączenie trybu prezentacji. W obszarze **Ustawienia zaawansowane** (klawisz F5) należy kliknąć kolejno opcje **Narzędzia** > **Tryb prezentacji**, a następnie użyć przełącznika obok opcji **Automatycznie włączaj tryb prezentacji przy uruchamianiu aplikacji w trybie pełnoekranowym**, aby program ESET Endpoint Security automatycznie uruchamiał tryb prezentacji w momencie uruchamiania aplikacji w trybie pełnoekranowym. Włączenie trybu prezentacji stanowi potencjalne zagrożenie bezpieczeństwa, dlatego ikona stanu ochrony na pasku zadań zmieni kolor na pomarańczowy, sygnalizując ostrzeżenie. W głównym oknie programu również widoczne będzie ostrzeżenie w postaci komunikatu **Tryb prezentacji włączony** wyświetlanego na pomarańczowo.

Po włączeniu opcji **Automatycznie włączaj tryb prezentacji przy uruchamianiu aplikacji w trybie pełnoekranowym** tryb prezentacji będzie włączany po uruchomieniu aplikacji w trybie pełnego ekranu i automatycznie wyłączany po zakończeniu jej działania. Ta opcja jest szczególnie przydatna, gdy tryb prezentacji ma być uaktywniany natychmiast po uruchomieniu gry lub aplikacji pełnoekranowej, albo po rozpoczęciu prezentacji.

Można również wybrać opcję **Automatycznie wyłączaj tryb prezentacji po** w celu określenia liczby minut, po upływie której tryb prezentacji będzie automatycznie wyłączany.

UWAGA: Jeśli zapora osobista działa w trybie interaktywnym i jest włączony tryb prezentacji, mogą wystąpić problemy z nawiązaniem połączenia internetowego. Może się to okazać kłopotliwe w przypadku uruchomienia gry, która komunikuje się z Internetem. W zwykłych warunkach pojawiłby się monit o potwierdzenie tego działania (jeśli nie zdefiniowano żadnych reguł komunikacji ani wyjątków), ale w trybie prezentacji interakcja ze strony użytkownika jest wyłączona. W takim przypadku rozwiązaniem jest zdefiniowanie reguły komunikacji dla każdego programu, który może kolidować z takim zachowaniem, lub zastosowanie innego trybu filtrowania w zaporze osobistej. Należy pamiętać, że jeśli przy włączonym trybie prezentacji zostanie otwarta strona internetowa lub aplikacja mogąca stanowić zagrożenie dla bezpieczeństwa, jej ewentualnemu zablokowaniu nie będzie towarzyszyć żaden komunikat ani ostrzeżenie, ponieważ interakcja ze strony użytkownika jest wyłączona.

3.9.1.10 Skanowanie przy uruchamianiu

Domyślnie przeprowadzane jest automatyczne sprawdzenie plików podczas uruchamiania systemu oraz podczas aktualizacji bazy sygnatur wirusów. To skanowanie jest zależne od ustawień w sekcji Konfiguracja harmonogramu i zadania.

Opcje skanowania podczas uruchamiania systemu są częścią zadania zaplanowanego **Sprawdzanie plików przy uruchamianiu systemu**. Aby zmodyfikować te ustawienia skanowania przy uruchamianiu, należy przejść do opcji **Narzędzia** > **Harmonogram**, kliknąć **Automatyczne sprawdzanie plików przy uruchamianiu**, a następnie **Edytuj**. W ostatnim kroku zostanie wyświetlone okno Automatyczne sprawdzanie plików przy uruchamianiu (więcej szczegółów można znaleźć w następnym rozdziale).

Szczegółowe informacje na temat tworzenia zadań zaplanowanych i zarządzania nimi można znaleźć w rozdziale Tworzenie nowych zadań.

3.9.1.10.1 Automatyczne sprawdzanie plików przy uruchamianiu

Podczas tworzenia zaplanowanego zadania sprawdzania plików przy uruchamianiu systemu dostępnych jest kilka opcji umożliwiających dostosowanie następujących parametrów:

W menu rozwijanym **Zazwyczaj używane pliki** można określić dokładność skanowania plików otwieranych podczas uruchamiania systemu na podstawie zaawansowanego niejawnego algorytmu. Pliki są rozmieszczone w kolejności malejącej, zgodnie z następującymi kryteriami:

- **Wszystkie zarejestrowane pliki** (najwięcej skanowanych plików)
- **Rzadko używane pliki**
- **Zazwyczaj używane pliki**
- **Często używane pliki**
- **Tylko najczęściej używane pliki** (najmniej skanowanych plików)

Poziom skanowania obejmuje także dwie szczególne grupy:

- **Pliki uruchamiane przed zalogowaniem użytkownika** — są to pliki w takich lokalizacjach, do których można uzyskać dostęp bez zalogowania użytkownika (prawie wszystkie lokalizacje wykorzystywane podczas uruchomienia systemu, takie jak usługi, obiekty pomocnika przeglądarki, powiadamianie usługi winlogon, wpisy harmonogramu systemu Windows, znane biblioteki DLL itp.).
- **Pliki uruchamiane po zalogowaniu użytkownika** — są to pliki w takich lokalizacjach, do których można uzyskać dostęp dopiero po zalogowaniu się użytkownika (pliki, które są uruchamiane tylko dla określonego użytkownika, zazwyczaj pliki znajdujące się w folderze *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Listy plików do skanowania są stałe w każdej z wcześniej wymienionych grup.

Priorytet skanowania — poziom priorytetu używany do określenia momentu uruchomienia skanowania:

- **W trakcie bezczynności** — zadanie zostanie wykonane tylko wtedy, gdy system jest bezczynny.
- **Najniższy** — kiedy obciążenie systemu jest możliwie najmniejsze
- **Niższy** — przy niskim obciążeniu systemu
- **Normalny** — przy przeciętnym obciążeniu systemu.

3.9.1.11 Ochrona dokumentów

Funkcja Ochrona dokumentów pozwala na skanowanie dokumentów pakietu Microsoft Office przed ich otwarciem, a także skanowanie plików automatycznie pobieranych przez program Internet Explorer (np. elementów Microsoft ActiveX). Oprócz ochrony systemu plików w czasie rzeczywistym dostępna jest również ochrona dokumentów. Opcję tę można wyłączyć, aby zwiększyć wydajność systemu na komputerach, na których nie znajduje się dużo dokumentów programu Microsoft Office.

Opcja **Integracja z systemem** umożliwia aktywowanie systemu ochrony. Aby zmodyfikować tę opcję, należy nacisnąć klawisz F5 w celu otwarcia okna Ustawienia zaawansowane i w drzewie ustawień zaawansowanych kliknąć kolejno pozycje **Antywirus** > **Ochrona dokumentów**.

Funkcja ta jest aktywowana przez aplikacje używające interfejsu Microsoft Antivirus API (np. Microsoft Office w wersji 2000 lub wyższej albo Microsoft Internet Explorer w wersji 5.0 lub wyższej).

3.9.1.12 Wyłączenia

Wyłączenia pozwalają wykluczyć ze skanowania wybrane pliki i foldery. Aby zapewnić skanowanie wszystkich obiektów pod kątem zagrożeń, zaleca się tworzenie wyłączeń tylko wtedy, gdy jest to absolutnie konieczne. Do sytuacji, w których może być konieczne wykluczenie obiektu, może zaliczać się skanowanie wpisów dużych baz danych, które spowolniłyby pracę komputera podczas skanowania lub korzystanie z oprogramowania, które powoduje konflikt ze skanowaniem (np. oprogramowania do tworzenia kopii zapasowych).

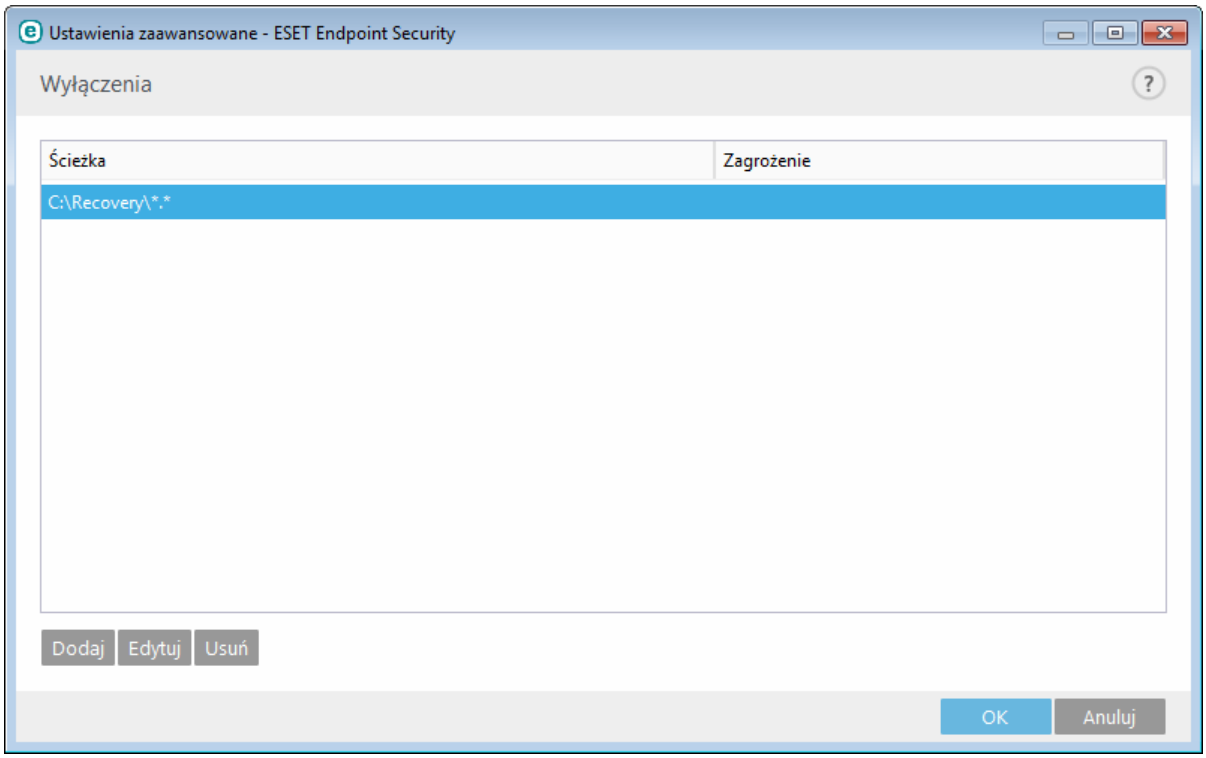
Aby wyłączyć obiekt ze skanowania:

1. Kliknij opcję **Dodaj**.
2. Wprowadź ścieżkę do obiektu lub wybierz obiekt w strukturze drzewa.

Można też dodać grupę plików, używając symboli wieloznacznych. Znak zapytania (?) reprezentuje jeden dowolny znak, a gwiazdka (*) reprezentuje dowolny ciąg złożony z dowolnej liczby znaków (w tym ciąg pusty).

Przykłady

- Aby wyłączyć ze skanowania wszystkie pliki z danego folderu, należy wpisać ścieżkę do tego folderu i zastosować maskę „*.*”.
- Aby wyłączyć ze skanowania cały dysk z jego wszystkimi plikami i podfolderami, należy zastosować maskę „D:*”.
- Aby wyłączyć ze skanowania jedynie pliki DOC, należy użyć maski „*.doc”.
- Jeśli nazwa pliku wykonywalnego składa się z określonej liczby znaków (i znaki te różnią się od siebie), a znana jest tylko pierwsza litera (np. „D”), należy zastosować następujący format: „D????.exe”. Znaki zapytania zastępują wszystkie brakujące (nieznane) znaki.



UWAGA: Zagrożenie w pliku nie zostanie wykryte przez moduł ochrony systemu plików w czasie rzeczywistym ani moduł skanowania komputera, jeśli plik spełnia kryteria wykluczenia ze skanowania.

Kolumny

Ścieżka — ścieżka dostępu do wyłączonych plików i folderów.

Zagrożenie — gdy obok wyłączonego pliku wyświetlana jest nazwa zagrożenia, oznacza to, że plik będzie pomijany tylko przy wyszukiwaniu tego zagrożenia, a nie całkowicie. Jeśli później plik zostanie zainfekowany innym szkodliwym oprogramowaniem, moduł antywirusowy go wykryje. Ten rodzaj wyłączeń można stosować tylko w przypadku określonych typów infekcji. Można je skonfigurować w oknie alertu o zagrożeniu sygnalizującym infekcję (należy kliknąć przycisk **Pokaż opcje zaawansowane**, a następnie wybrać opcję **Wyłącz z wykrywania**) lub klikając kolejno opcje **Narzędzia** > **Kwarantanna**, klikając prawym przyciskiem myszy plik poddany kwarantannie i wybierając z menu kontekstowego opcję **Przywróć i wyłącz ze skanowania**.

Elementy sterujące

Dodaj — pozwala dodać obiekty, które mają być pomijane podczas wykrywania.

Edytuj — pozwala edytować zaznaczone elementy.

Usuń — służy do usuwania zaznaczonych elementów.

3.9.1.13 Ustawienia parametrów technologii ThreatSense

Technologia ThreatSense obejmuje wiele zaawansowanych metod wykrywania zagrożeń. Jest ona proaktywna, co oznacza, że zapewnia ochronę już od pierwszych godzin rozprzestrzeniania się nowego zagrożenia. Stosowana jest w niej kombinacja kilku metod (analiza kodu, emulacja kodu, sygnatury rodzajowe, sygnatury wirusów), które razem znacznie zwiększają bezpieczeństwo systemu. Korzystając z tej technologii skanowania, można kontrolować kilka strumieni danych jednocześnie, maksymalizując skuteczność i wskaźnik wykrywalności. Ponadto technologia ThreatSense pomyślnie eliminuje programy typu rootkit.

Za pomocą opcji ustawień parametrów technologii ThreatSense można określić kilka parametrów skanowania:

- Typy i rozszerzenia plików, które mają być skanowane;
- Kombinacje różnych metod wykrywania;
- Poziomy leczenia itp.

Aby otworzyć okno konfiguracji, należy kliknąć przycisk **Ustawienia parametrów technologii ThreatSense**, znajdujący się w oknie Ustawienia zaawansowane każdego modułu, w którym wykorzystywana jest technologia ThreatSense (zobacz poniżej). Różne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Mając to na uwadze, technologię ThreatSense można konfigurować indywidualnie dla następujących modułów ochrony:

- Ochrona systemu plików w czasie rzeczywistym
- Skanowanie w trakcie bezczynności
- Skanowanie przy uruchamianiu
- Ochrona dokumentów
- Ochrona programów poczty e-mail
- Ochrona dostępu do stron internetowych
- Skanowanie komputera

Parametry technologii ThreatSense są w wysokim stopniu zoptymalizowane pod kątem poszczególnych modułów, a ich modyfikacja może znacząco wpływać na działanie systemu. Na przykład ustawienie opcji skanowania spakowanych programów za każdym razem lub włączenie zaawansowanej heurystyki w module ochrony systemu plików w czasie rzeczywistym może spowodować spowolnienie działania systemu (normalnie tymi metodami skanowane są tylko nowo utworzone pliki). Zaleca się pozostawienie niezmienionych parametrów domyślnych technologii ThreatSense dla wszystkich modułów z wyjątkiem modułu Skanowanie komputera.

Skanowane obiekty

W sekcji Obiekty można określić, które pliki i składniki komputera będą skanowane w poszukiwaniu infekcji.

Pamięć operacyjna — umożliwia skanowanie w poszukiwaniu szkodliwego oprogramowania, które atakuje pamięć operacyjną komputera.

Sektory startowe — umożliwia skanowanie sektorów startowych w poszukiwaniu wirusów w głównym rekordzie rozruchowym.

Pliki poczty — program obsługuje następujące rozszerzenia: DBX (Outlook Express) oraz EML.

Archiwa — program obsługuje następujące rozszerzenia: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE i wiele innych.

Archiwa samorozpakowujące — archiwa samorozpakowujące się (SFX) to archiwa, które nie wymagają do dekompresji żadnych specjalnych programów.

Programy spakowane — po uruchomieniu — w odróżnieniu od archiwów standardowych — dekompresują swoją zawartość do pamięci. Poza standardowymi statycznymi programami spakowanymi (UPX, yoda, ASPack, FSG itd.) skaner umożliwia również rozpoznawanie innych typów programów spakowanych, dzięki emulowaniu ich kodu.

Opcje skanowania

Tu można wybrać metody stosowane podczas skanowania systemu w poszukiwaniu infekcji. Dostępne są następujące opcje:

Heurystyka — heurystyka jest metodą analizy pozwalającą wykrywać działanie szkodliwych programów. Główną zaletą tej technologii jest to, że umożliwia wykrywanie szkodliwego oprogramowania, które w chwili pobierania ostatniej aktualizacji bazy danych sygnatur wirusów jeszcze nie istniało lub nie było znane. Wadą może być ryzyko (niewielkie) wystąpienia tzw. fałszywych alarmów.

Zaawansowana heurystyka/DNA/Inteligentne sygnatury — zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym opracowanym przez firmę ESET. Został on napisany w językach programowania wysokiego poziomu i zoptymalizowany pod kątem wykrywania robaków i koni trojańskich. Zastosowanie zaawansowanej heurystyki znacząco usprawnia wykrywanie zagrożeń w produktach firmy ESET. Sygnatury pozwalają niezawodnie wykrywać i identyfikować wirusy. Dzięki systemowi automatycznej aktualizacji nowe sygnatury są udostępniane w ciągu kilku godzin od stwierdzenia zagrożenia. Wadą sygnatur jest to, że pozwalają wykrywać tylko znane wirusy (lub ich nieznacznie zmodyfikowane wersje).

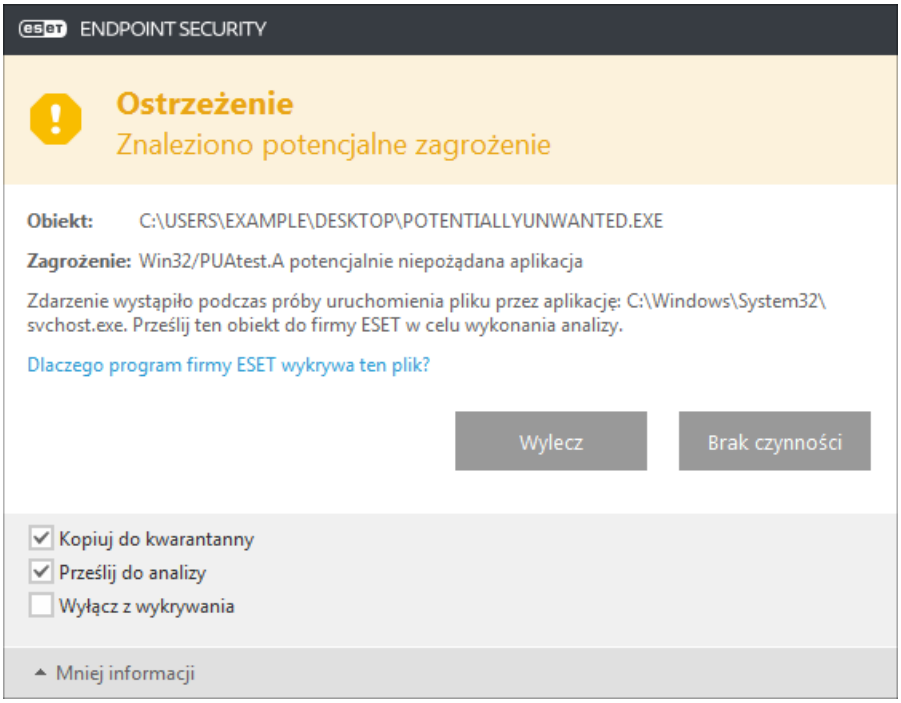
Potencjalnie niepożądana aplikacja to program, który zawiera oprogramowanie typu adware, instaluje paski narzędzi lub wykonuje inne niejasne działania. W niektórych sytuacjach użytkownik może uznać, że korzyści

związane z potencjalnie niepożądaną aplikacją są większe niż zagrożenia. Z tego powodu ESET przydziela takim aplikacjom kategorię niskiego ryzyka w porównaniu do innych typów złośliwego oprogramowania, takich jak konie trojańskie czy robaki.

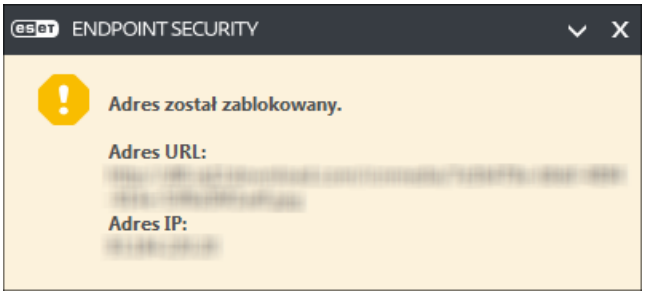
Ostrzeżenie — znaleziono potencjalne zagrożenie

W przypadku wykrycia potencjalnie niepożądanej aplikacji użytkownik ma możliwość wybrania czynności:

1. **Wylecz/Rozłącz**: ta opcja przerywa wykonywanie czynności i uniemożliwia potencjalnemu zagrożeniu przedostanie się do systemu.
2. **Brak czynności**: ta opcja umożliwia potencjalnemu zagrożeniu przedostanie się do systemu.
3. Aby w przyszłości umożliwić uruchamianie aplikacji na komputerze bez zakłóceń, należy kliknąć opcję **Więcej informacji/Pokaż opcje zaawansowane** i zaznaczyć pole wyboru obok opcji **Wyłącz z wykrywania**.

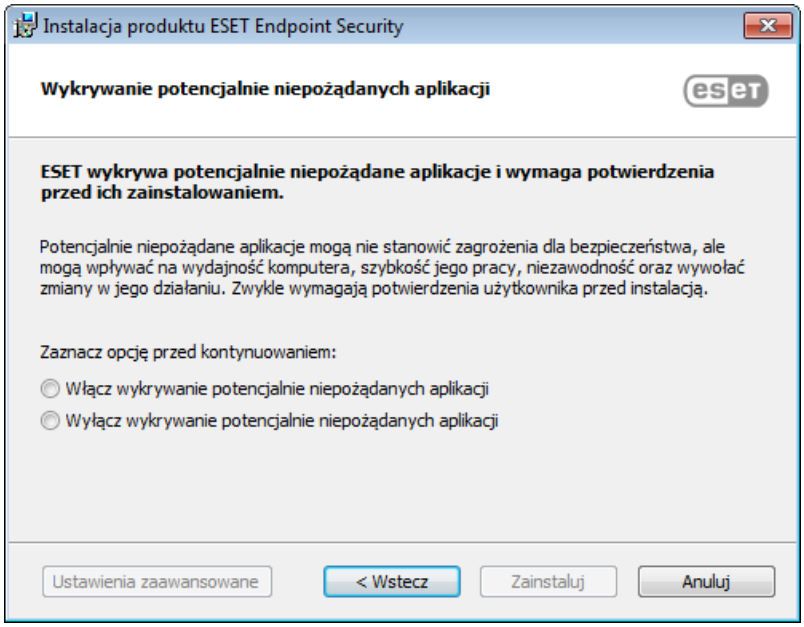


W przypadku wykrycia potencjalnie niepożądanej aplikacji, której nie można wyleczyć, w prawym dolnym rogu ekranu zostanie wyświetlone okno powiadomienia **Adres został zablokowany**. Więcej informacji na temat tego zdarzenia można znaleźć, przechodząc z menu głównego do opcji **Narzędzia** > **Pliki dziennika** > **Filtrowane witryny internetowe**.



Potencjalnie niepożądane aplikacje — ustawienia

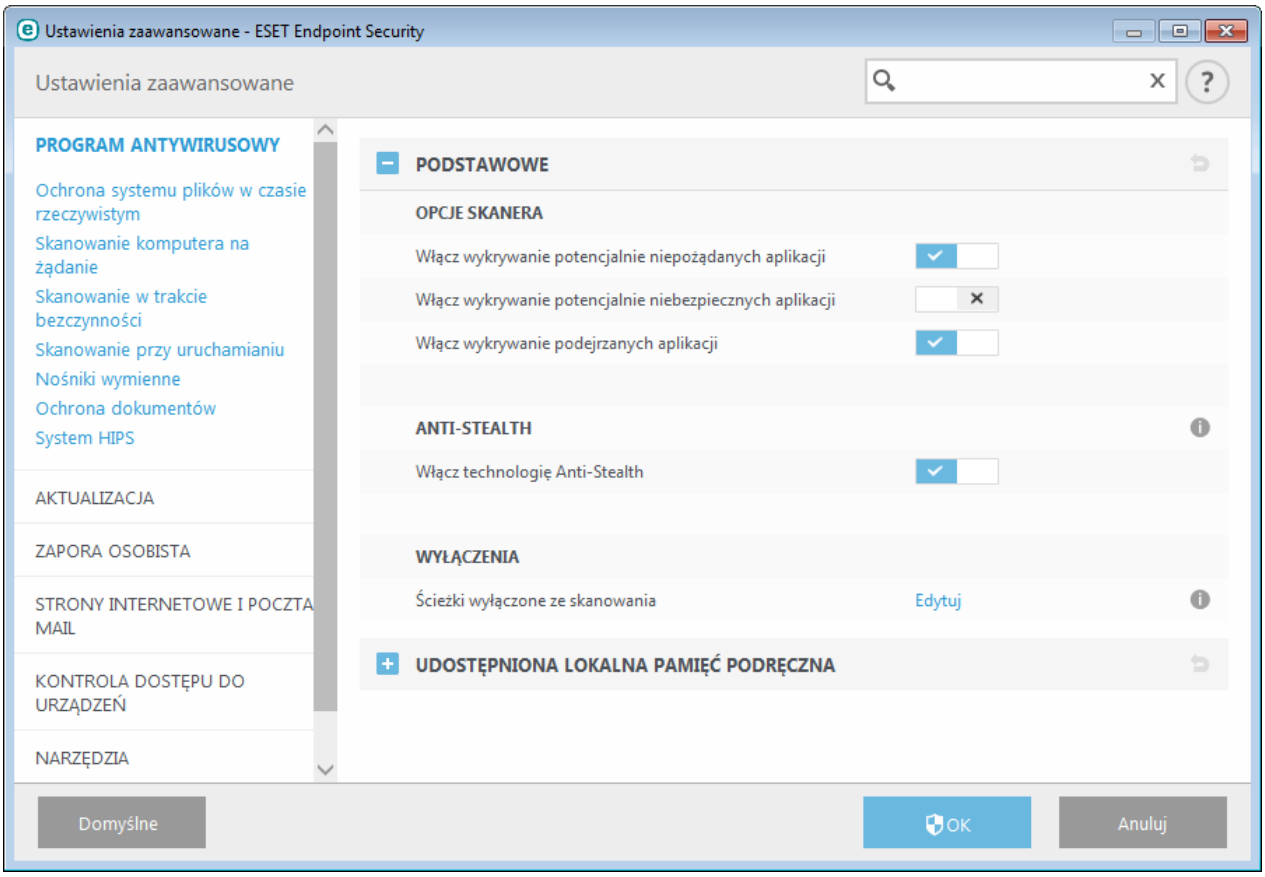
Podczas instalowania produktu ESET można zdecydować, czy włączone ma być wykrywanie potencjalnie niepożądanych aplikacji, jak widać poniżej:



Potencjalnie niepożądane aplikacje mogą instalować oprogramowanie typu adware i paski narzędzi lub obejmować inne niepożądane i niebezpieczne funkcje.

Te ustawienia można zmienić w dowolnym momencie w ustawieniach programu. Aby włączyć lub wyłączyć wykrywanie potencjalnie niepożądanych, niebezpiecznych lub podejrzanych aplikacji, należy wykonać poniższe instrukcje:

1. Otwórz produkt ESET. Otwieranie produktu ESET
2. Naciśnij klawisz **F5**, by uzyskać dostęp do obszaru **Ustawienia zaawansowane**.
3. Kliknij opcję **Ochrona antywirusowa** i zgodnie z własnym uznaniem włącz lub wyłącz opcje **Włącz wykrywanie potencjalnie niepożądanych aplikacji**, **Włącz wykrywanie potencjalnie niebezpiecznych aplikacji** oraz **Włącz wykrywanie podejrzanych aplikacji**. Potwierdź, klikając przycisk **OK**.



Potencjalnie niepożądane aplikacje — otoki oprogramowania

Otoka oprogramowania to szczególnego typu modyfikacja aplikacji stosowana na niektórych stronach internetowych obsługujących hosting plików. To narzędzie strony trzeciej, które instaluje oprogramowanie pobrane przez użytkownika, instalując jednak przy tym dodatkowe oprogramowanie, takie jak paski narzędzi i oprogramowanie typu adware. Dodatkowe oprogramowanie może również modyfikować ustawienia strony głównej oraz wyszukiwania w przeglądarce użytkownika. Ponadto strony obsługujące hosting plików często nie powiadamiają dostawcy oprogramowania ani użytkownika pobierającego pliki o wprowadzonych modyfikacjach, a zrezygnowanie z tych modyfikacji jest zwykle utrudnione. Z tego względu oprogramowanie ESET klasyfikuje otoki oprogramowania jako jeden z rodzajów potencjalnie niepożądanych aplikacji, oferując użytkownikom możliwość zaakceptowania lub zrezygnowania z pobierania.

Zaktualizowaną wersję tej strony pomocy zawiera ten artykuł bazy wiedzy ESET.

Potencjalnie niebezpieczne aplikacje — potencjalnie niebezpieczne aplikacje to klasyfikacja używana w odniesieniu do komercyjnych, legalnych programów, takich jak narzędzia do dostępu zdalnego, aplikacje służące do łamania haseł oraz programy zapisujące znaki wpisywane na klawiaturze (ang. keylogger). Domyślnie opcja ta jest wyłączona.

Leczenie

Ustawienia leczenia określają sposób działania skanera w stosunku do zainfekowanych plików. Istnieją 3 poziomy leczenia:

Brak leczenia — Zainfekowane pliki nie będą automatycznie leczone. Wyświetlane jest okno z ostrzeżeniem, a użytkownik może wybrać czynność do wykonania. Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie czynności należy wykonać w razie wystąpienia infekcji.

Leczenie normalne — program próbuje automatycznie wyleczyć lub usunąć zarażony plik zgodnie ze wstępnie zdefiniowaną czynnością (zależnie od typu infekcji). O wykryciu i usunięciu zainfekowanego pliku informuje powiadomienie wyświetlane w prawym dolnym rogu ekranu. Jeśli automatyczne wybranie właściwej czynności nie będzie możliwe, w programie będą dostępne inne czynności kontynuacyjne. Aplikacja zadziała tak samo także wtedy, gdy nie będzie możliwe wykonanie wstępnie zdefiniowanej czynności.

Leczenie dokładne — program leczy lub usuwa wszystkie zarażone pliki. Jedyny wyjątek stanowią pliki systemowe.

Jeśli ich wyleczenie nie jest możliwe, użytkownik jest monitowany o wybranie odpowiedniej czynności w oknie z ostrzeżeniem.

Ostrzeżenie: Jeśli archiwum zawiera zarażone pliki, problem można rozwiązać na dwa sposoby. W trybie standardowym (Leczenie standardowe) usunięcie całego archiwum nastąpi w sytuacji, gdy będą zarażone wszystkie znajdujące się w nim pliki. W trybie **Leczenie dokładne** całe archiwum zostanie usunięte po wykryciu pierwszego zarażonego pliku, niezależnie od stanu pozostałych plików w tym archiwum.

Wyłączenia

Rozszerzenie jest częścią nazwy pliku oddzieloną kropką. Określa ono typ i zawartość pliku. Ta sekcja ustawień parametrów technologii ThreatSense umożliwia określanie typów plików, które mają być skanowane.

Inne

Podczas konfigurowania ustawień parametrów technologii ThreatSense dotyczących skanowania komputera na żądanie w sekcji **Inne** dostępne są również następujące opcje:

Skanuj alternatywne strumienie danych (ADS) — alternatywne strumienie danych używane w systemie plików NTFS to skojarzenia plików i folderów, których nie można sprawdzić za pomocą standardowych technik skanowania. Wiele wirusów stara się uniknąć wykrycia, udając alternatywne strumienie danych.

Uruchom skanowanie w tle z niskim priorytetem — każde skanowanie wymaga użycia pewnej ilości zasobów systemowych. W przypadku używania programów, które wymagają dużej ilości zasobów systemowych, można uruchomić skanowanie w tle z niskim priorytetem, oszczędzając zasoby dla innych aplikacji.

Zapisuj w dzienniku informacje o wszystkich obiektach — wybranie tej opcji powoduje, że w pliku dziennika są zapisywane informacje o wszystkich skanowanych plikach, nawet tych niezainfekowanych. Jeśli na przykład infekcja zostanie znaleziona w archiwum, w dzienniku zostaną uwzględnione również pliki niezainfekowane zawarte w tym archiwum.

Włącz inteligentną optymalizację — po włączeniu funkcji Inteligentna optymalizacja używane są optymalne ustawienia, które zapewniają połączenie maksymalnej skuteczności z największą szybkością skanowania. Poszczególne moduły ochrony działają w sposób inteligentny, stosując różne metody skanowania w przypadku różnych typów plików. Jeśli funkcja inteligentnej optymalizacji jest wyłączona, podczas skanowania są stosowane jedynie określone przez użytkownika dla poszczególnych modułów ustawienia technologii ThreatSense.

Zachowaj znacznik czasowy ostatniego dostępu — wybranie tej opcji pozwala zachować oryginalny znacznik czasowy dostępu do plików zamiast przeprowadzania ich aktualizacji (na przykład na potrzeby systemów wykonywania kopii zapasowych danych).

Limity

W sekcji Limity można określić maksymalny rozmiar obiektów i poziomy zagnieżdżonych archiwów, które mają być skanowane:

Ustawienia obiektów

Maksymalny rozmiar obiektu — określa maksymalny rozmiar obiektów do skanowania. Dany moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Ta opcja powinna być modyfikowana tylko przez zaawansowanych użytkowników, którzy mają określone powody do wyłączenia większych obiektów ze skanowania. Wartość domyślna: *bez limitu*.

Maksymalny czas skanowania dla obiektu (s) — określa maksymalny czas skanowania obiektu. W przypadku wprowadzenia wartości zdefiniowanej przez użytkownika moduł antywirusowy zatrzyma skanowanie obiektu po upływie danego czasu, niezależnie od tego, czy skanowanie zostało ukończone. Wartość domyślna: *bez limitu*.

Ustawienia skanowania archiwów

Poziom zagnieżdżania archiwów — określa maksymalną głębokość skanowania archiwów. Wartość domyślna: *10*.

Maksymalny rozmiar pliku w archiwum — ta opcja pozwala określić maksymalny rozmiar plików, które mają być skanowane w rozpakowywanych archiwach. Wartość domyślna: *bez limitu*.

UWAGA: Nie zalecamy modyfikowania wartości domyślnych. W zwykłych warunkach nie ma potrzeby ich zmieniać.

3.9.1.13.1 Wyłączenia

Rozszerzenie jest częścią nazwy pliku oddzieloną kropką. Określa ono typ i zawartość pliku. Ta sekcja ustawień parametrów technologii ThreatSense umożliwia określanie typów plików, które mają być skanowane.

Domyślnie skanowane są wszystkie pliki. Do listy plików wyłączonych ze skanowania można dodać dowolne rozszerzenie.

Wykluczenie plików jest czasami konieczne, jeśli skanowanie pewnych typów plików uniemożliwia prawidłowe działanie programu, który z niektórych z nich korzysta. Na przykład podczas używania serwerów programu Microsoft Exchange może być wskazane wyłączenie rozszerzeń EDB, EML i TMP.

Przy użyciu przycisków **Dodaj** i **Usuń** można włączyć lub wyłączyć skanowanie plików o konkretnych rozszerzeniach. W celu dodania do listy nowego rozszerzenia należy kliknąć przycisk **Dodaj**, wpisać rozszerzenie w pustym polu i kliknąć przycisk **OK**. Gdy wybrana jest opcja **Wprowadź wiele wartości**, można dodać wiele rozszerzeń plików oddzielonych wierszami, przecinkami lub średnikami. W przypadku włączenia opcji wielokrotnego wyboru rozszerzenia będą wyświetlane na liście. Aby usunąć wybrane rozszerzenie z listy, należy je zaznaczyć, a następnie kliknąć przycisk **Usuń**. W celu edytowania wybranego rozszerzenia należy nacisnąć przycisk **Edytuj**.

Można używać symboli specjalnych: * (gwiazdka) oraz ? (znak zapytania). Gwiazdka oznacza dowolny ciąg znaków, a znak zapytania oznacza dowolny symbol.

UWAGA: aby zobaczyć dokładne rozszerzenie (jeśli istnieje) pliku w systemie operacyjnym Windows, należy anulować wybór opcji **Ukryj rozszerzenia znanych typów plików** na karcie **Panel sterowania** > **Opcje folderów** > **Widok**, a następnie zastosować zmianę.

3.9.2 Sieć

Zapora osobista kontroluje cały przychodzący i wychodzący ruch sieciowy komputera. Jej działanie polega na zezwalaniu na pojedyncze połączenia sieciowe lub ich odrzucaniu na podstawie reguł filtrowania ustalonych przez użytkownika. Zapora zapewnia ochronę przed atakami z komputerów zdalnych i umożliwia blokowanie niektórych potencjalnie niebezpiecznych usług. Zapora osobista obejmuje również funkcje wykrywania włamań i zapobiegania im (IDS/IPS), które umożliwiają sprawdzanie zawartości dozwolonego ruchu sieciowego i blokowanie ruchu uznawanego za potencjalnie szkodliwy.

Aby przejść do konfiguracji **zapory osobistej**, należy otworzyć okno **Ustawienia** w obszarze **Sieć**. Można tam dostosować tryb filtrowania stosowany w odniesieniu do zapory osobistej ESET. Można również uzyskać dostęp do bardziej zaawansowanych ustawień, klikając kolejno koło zębate > **Skonfiguruj** obok pozycji **Zapora osobista** lub naciskając klawisz **F5** w celu uzyskania dostępu do obszaru Ustawienia zaawansowane.

Ochrona przed atakami z sieci (IDS) — analizowanie zawartości w ruchu sieciowym i ochrona przed atakami z sieci. Wszelki ruch sieciowy uznany za szkodliwy zostanie zablokowany. Istnieje możliwość wyłączenia ochrony przed atakami z sieci na określony czas poprzez kliknięcie opcji .

Ochrona przed botnetami — szybkie i precyzyjne wykrywanie szkodliwego oprogramowania w systemie. Istnieje możliwość wyłączenia ochrony przed botnetami na określony czas poprzez kliknięcie opcji .

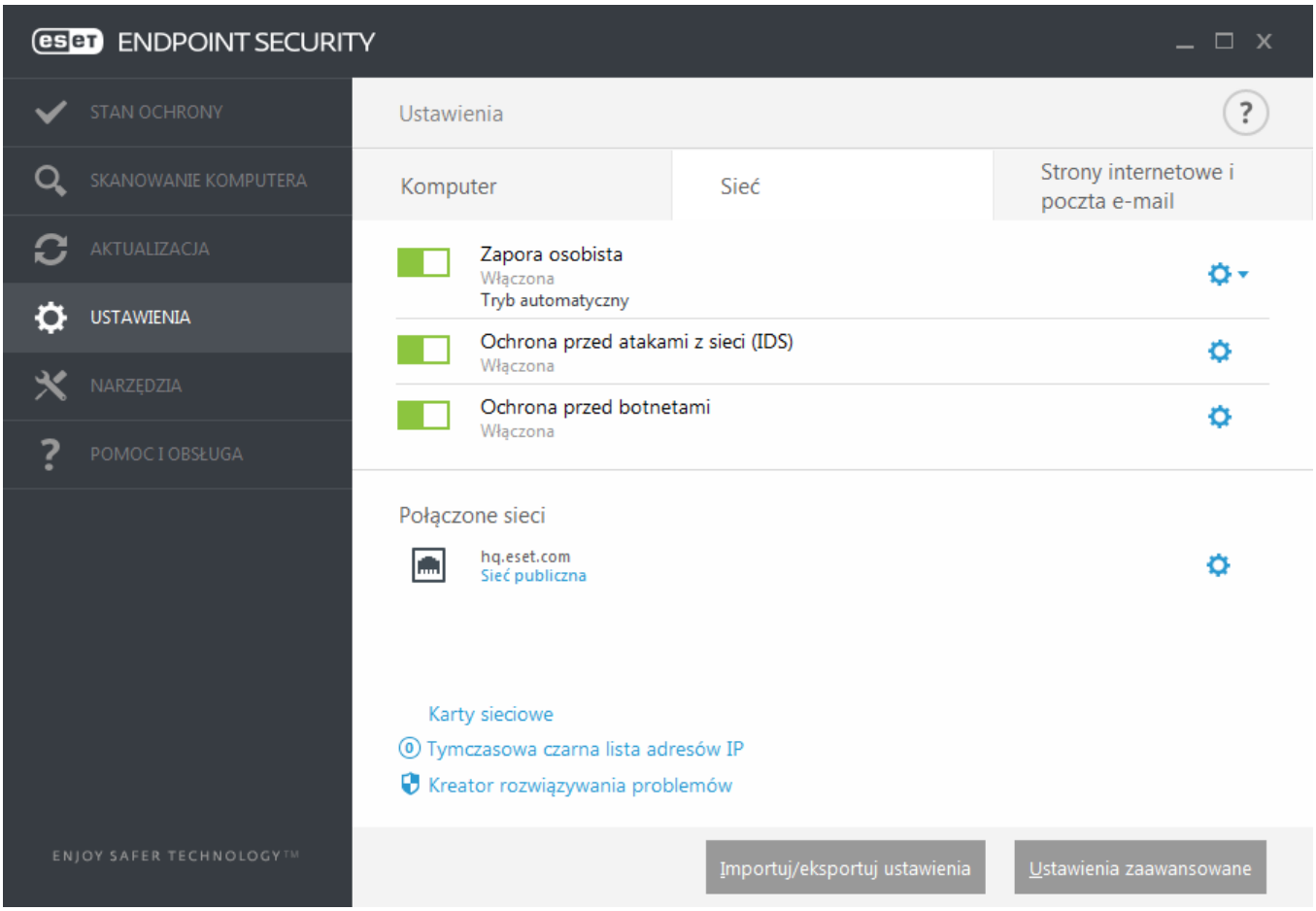
Połączone sieci — tutaj wyświetlane są sieci, z którymi połączone są karty sieciowe. Po kliknięciu koła zębatego zostanie wyświetlony monit o wybranie typu zabezpieczeń sieci, z którą użytkownik jest połączony przy użyciu karty sieciowej.

Karty sieciowe — tutaj wyświetlane są poszczególne karty sieciowe wraz z przypisanymi do nich profilami zapory oraz strefami zaufanymi. Szczegółowe informacje można znaleźć w sekcji Karty sieciowe.

Tymczasowa czarna lista adresów IP — wyświetla listę adresów IP, które zostały wykryte jako źródło ataków i dodane do czarnej listy w celu blokowania połączeń przez podany okres. Aby uzyskać więcej informacji na ten temat, kliknij tę opcję i naciśnij klawisz F1.

Kreator rozwiązywania problemów — ułatwia rozwiązywanie problemów z komunikacją spowodowanych działaniem zapory osobistej ESET. Szczegółowe informacje można znaleźć w sekcji Kreator rozwiązywania

problemów.



Kliknięcie koła zębatego widocznego obok pozycji **Zapora osobista** umożliwia dostęp do następujących ustawień:

Konfiguruj... — otwiera okno Zapora osobista w obszarze Ustawienia zaawansowane, gdzie można określić sposób obsługiwania komunikacji sieciowej przez zaporę.

Blokuj cały ruch — wszystkie połączenia przychodzące i wychodzące będą blokowane przez zaporę osobistą. Tej opcji należy używać tylko w przypadku podejrzenia krytycznych zagrożeń bezpieczeństwa, które wymagają odłączenia systemu od sieci. Gdy filtrowanie ruchu sieciowego jest w trybie **Blokuj cały ruch**, w celu przywrócenia normalnego działania zapory należy kliknąć pozycję **Wyłącz blokowanie całego ruchu**.

Wstrzymaj zaporę (zezwól na cały ruch) — to przeciwieństwo blokowania całego ruchu sieciowego. Wybranie tej opcji oznacza wyłączenie filtrowania przez zaporę osobistą i zezwolenie na wszystkie połączenia przychodzące i wychodzące. Gdy filtrowanie ruchu sieciowego odbywa się w tym trybie, w celu ponownego włączenia zapory należy kliknąć opcję **Włącz zaporę**.

Tryb automatyczny — (gdy włączony jest inny tryb filtrowania) — tę opcję należy kliknąć w celu zmiany trybu filtrowania na automatyczny (z regułami zdefiniowanymi przez użytkownika).

Tryb interaktywny — (gdy włączony jest inny tryb filtrowania) — tę opcję należy kliknąć w celu zmiany trybu filtrowania na interaktywny.

3.9.2.1 Zapora osobista

Zapora osobista kontroluje cały przychodzący i wychodzący ruch sieciowy komputera. Jej działanie polega na zezwalaniu na pojedyncze połączenia sieciowe lub ich odmawianiu w oparciu o określone reguły filtrowania. Zapewnia ochronę przez atakami ze zdalnych komputerów i umożliwia blokowanie pewnych usług. Zapewnia również ochronę antywirusową protokołów HTTP, POP3 i IMAP. Ta funkcjonalność stanowi bardzo istotny element zabezpieczeń komputera.

Włącz ochronę przed atakami z sieci (IDS) — analizowanie zawartości w ruchu sieciowym i ochrona przed atakami z sieci. Wszelki ruch sieciowy uznany za szkodliwy zostanie zablokowany.

Włącz ochronę przed botnetami — wykrywanie i blokowanie komunikacji ze szkodliwymi serwerami przeznaczonymi do sterowania i kontrolowania na podstawie typowych wzorców, obserwowanych, gdy komputer jest zarażony i bot próbuje nawiązać komunikację.

Zapora osobista w programie ESET Endpoint Security udostępnia cztery tryby filtrowania. Ustawienia trybów filtrowania można znaleźć w oknie **Ustawienia zaawansowane** (klawisz F5), klikając pozycję **Zapora osobista**. Zachowanie zapory zmienia się w zależności od trybu filtrowania. Tryby filtrowania mają również wpływ na wymagany poziom interakcji użytkownika.

Filtrowanie może działać w jednym z czterech trybów:

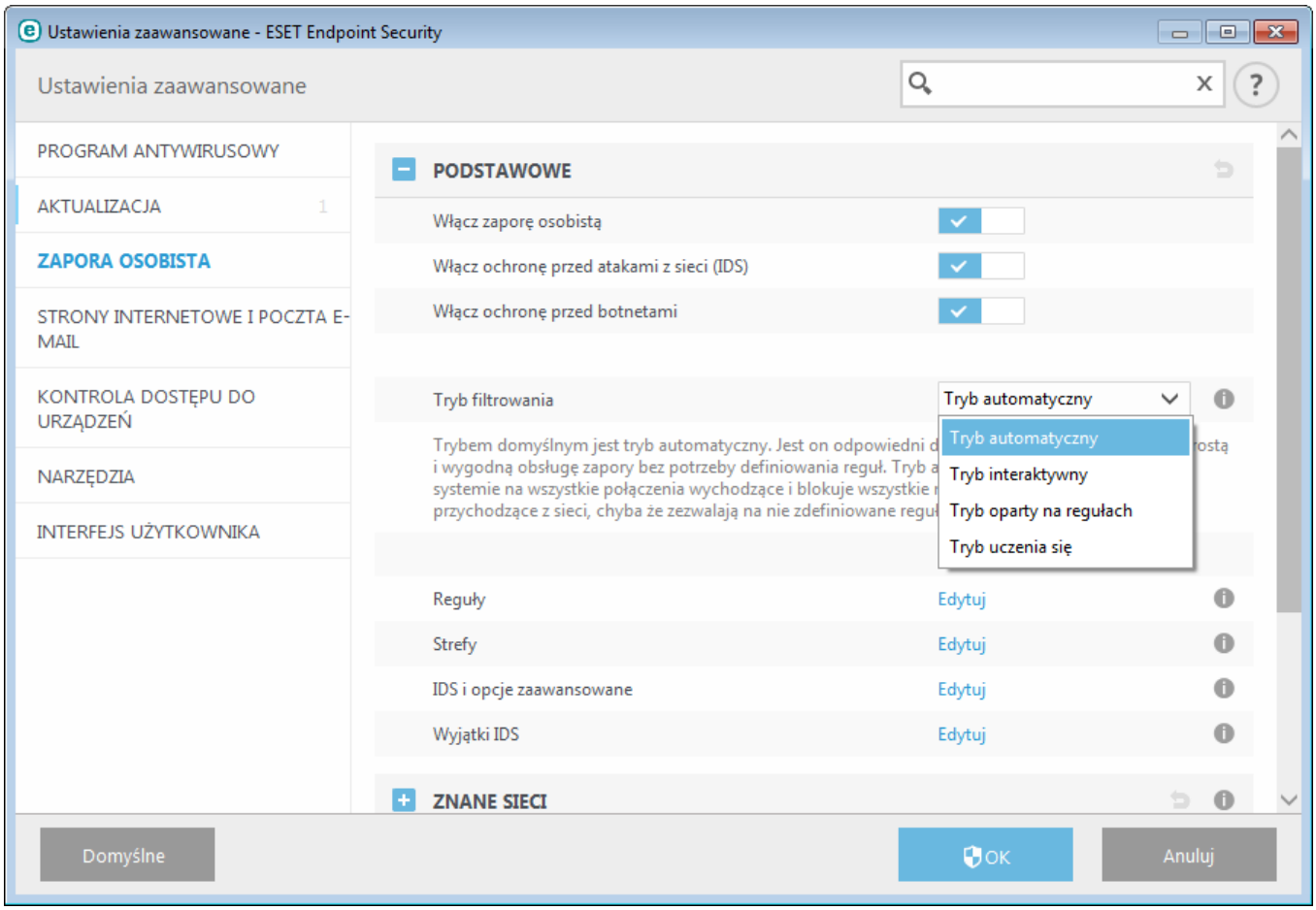
Tryb automatyczny — jest trybem domyślnym. Ten tryb jest odpowiedni dla użytkowników preferujących prostą i wygodną obsługę zapory bez potrzeby definiowania reguł. Można tworzyć niestandardowe, definiowane przez użytkownika tryby, lecz w trybie automatycznym nie jest to wymagane. Tryb automatyczny zezwala na każdy ruch wychodzący w danym systemie i blokuje większość ruchu przychodzącego (z wyjątkiem ruchu ze strefy zaufanej, zgodnie z zezwoleniami ustawionymi w sekcji IDS i opcje zaawansowane/Dozwolone usługi oraz ruchu przychodzącego stanowiącego odpowiedź na niedawną komunikację wychodzącą z tą samą lokalizacją zdalną).

Tryb interaktywny — umożliwia tworzenie niestandardowej konfiguracji zapory osobistej. Po wykryciu połączenia, którego nie dotyczą żadne istniejące reguły, zostanie wyświetlone okno dialogowe informujące o nieznanym połączeniu. Okno to umożliwia zezwolenie na komunikację lub jej odmowę, a podjęta decyzja może zostać zapisana jako nowa reguła zapory osobistej. Jeśli użytkownik zdecyduje się na utworzenie nowej reguły, wszystkie przyszłe połączenia danego typu będą dozwolone lub blokowane zgodnie z tą regułą.

Tryb oparty na regułach — blokuje wszystkie połączenia nieokreślone przez odpowiednią regułę jako dozwolone. Ten tryb pozwala zaawansowanym użytkownikom na definiowanie reguł, które zezwalają jedynie na pożądane i bezpieczne połączenia. Pozostałe nieokreślone połączenia będą blokowane przez zaporę osobistą.

Tryb uczenia się — automatycznie tworzy oraz zapisuje reguły. Ten tryb jest odpowiedni do początkowej konfiguracji zapory osobistej. Interakcja ze strony użytkownika nie jest wymagana, ponieważ program ESET Endpoint Security zapisuje reguły zgodnie ze wstępnie zdefiniowanymi parametrami. Tryb uczenia się nie jest bezpieczny i powinien być używany tylko, dopóki nie zostaną utworzone wszystkie reguły dla niezbędnych połączeń.

Profile mogą służyć do dostosowania zachowania zapory osobistej programu ESET Endpoint Security, dzięki możliwości określenia różnych zestawów reguł dla różnych sytuacji.



Reguły — w tym miejscu można dodawać reguły i definiować sposób obsługi ruchu sieciowego przez zaporę osobistą.

Strefy — w tym miejscu można tworzyć strefy składające się z wielu adresów IP.

IDS i opcje zaawansowane — możliwość konfiguracji zaawansowanych opcji filtrowania oraz działań systemu IDS (służącego do wykrywania różnego typu ataków i prób wykorzystania luk w zabezpieczeniach).

Wyjątki IDS — opcja ta umożliwia dodawanie wyjątków systemu IDS i dostosowywanie sposobu jego reagowania na szkodliwe działania.

3.9.2.1.1 Tryb uczenia się

W trybie uczenia się automatycznie tworzone są i zapisywane wszelkie reguły komunikacji ustanowione w systemie. Interakcja ze strony użytkownika nie jest wymagana, ponieważ program ESET Endpoint Security zapisuje reguły zgodnie ze wstępnie zdefiniowanymi parametrami.

Stosowanie tego trybu może narażać system na zagrożenia i jest zalecane tylko przy wstępnej konfiguracji zapory osobistej.

Aby wyświetlić opcje trybu uczenia się, należy uaktywnić go, wybierając kolejno pozycje **Ustawienia zaawansowane** (klawisz F5) > **Zapora osobista** > **Ustawienia trybu uczenia się**. Sekcja ta zawiera następujące elementy:

Ostrzeżenie: Podczas działania w trybie uczenia się zapora osobista nie filtruje komunikacji. Wszystkie połączenia przychodzące i wychodzące są dozwolone. W tym trybie komputer nie jest w pełni chroniony przez zaporę osobistą.

Typ komunikacji — należy wybrać określone parametry tworzenia reguł dla każdego typu komunikacji. Istnieją cztery typy komunikacji:

Ruch przychodzący ze strefy zaufanej — przykładem połączenia przychodzącego w ramach strefy zaufanej mógłby być komputer zdalny ze strefy zaufanej, który próbuje nawiązać komunikację z aplikacją uruchomioną na komputerze lokalnym.

Ruch wychodzący ze strefy zaufanej — lokalna aplikacja próbuje ustanowić połączenie z innym komputerem z sieci lokalnej lub z innej sieci znajdującej się w strefie zaufanej.

Przychodzący ruch internetowy — komputer zdalny próbuje porozumieć się z aplikacją uruchomioną na komputerze lokalnym.

Wychodzący ruch internetowy — aplikacja lokalna próbuje nawiązać połączenie z innym komputerem.

W każdej sekcji można zdefiniować parametry, które będą dodawane do nowo tworzonych reguł:

Dodaj port lokalny — umożliwia dodanie numeru portu lokalnego dla komunikacji sieciowej. Dla połączeń wychodzących numery są zazwyczaj generowane losowo. Z tego powodu zaleca się włączenie tej opcji tylko dla połączeń przychodzących.

Dodaj aplikację — umożliwia dodanie nazwy aplikacji lokalnej. Opcja ta jest przeznaczona dla przyszłych reguł poziomu aplikacji (reguł, które definiują komunikację dla całej aplikacji). Na przykład można włączyć komunikację tylko dla przeglądarki internetowej lub programu poczty e-mail.

Dodaj port zdalny — umożliwia dodanie numeru portu zdalnego komunikacji sieciowej. Można na przykład włączyć lub zablokować określoną usługę związaną ze standardowym numerem portu (HTTP — 80, POP3 — 110 itd.).

Dodaj zdalny adres IP/strefę zaufaną — zdalny adres IP lub strefa mogą zostać użyte jako parametr dla nowych reguł określających wszystkie połączenia sieciowe pomiędzy systemem lokalnym a tymi zdalnymi adresami/strefami. Opcja ta jest przeznaczona do definiowania czynności dla określonego komputera lub grupy komputerów w sieci.

Maksymalna liczba różnych reguł dla aplikacji — jeśli aplikacja do komunikacji używa różnych portów, aby różnicować adresy IP itp., zapora w trybie uczenia się określa odpowiednią liczbę reguł dla tej aplikacji. Opcja ta umożliwia ograniczenie liczby reguł, które mogą zostać utworzone dla jednej aplikacji.

3.9.2.2 Profile zapory

Profile umożliwiają sterowanie działaniem zapory osobistej programu ESET Endpoint Security. Podczas tworzenia lub edytowania reguły zapory osobistej można przypisać tę regułę do określonego profilu lub zastosować ją we wszystkich profilach. Gdy profil jest aktywny w interfejsie sieciowym, stosowane są tylko reguły globalne (reguły, dla których nie określono profilu) oraz reguły przypisane do wybranego profilu. Aby z łatwością modyfikować sposób działania zapory osobistej, można utworzyć wiele profili z różnymi regułami przypisanymi do kart sieciowych lub do poszczególnych sieci.

Należy kliknąć opcję **Edytuj** obok pozycji **Lista profili**, by otworzyć okno **Profile zapory**, w którym można edytować profile.

Kartę sieciową można skonfigurować tak, by po podłączeniu do określonej sieci używany był profil skonfigurowany dla tej sieci. W obszarze **Ustawienia zaawansowane** (F5) > **Zapora osobista** > **Znane sieci** można również przypisać określony profil, który ma być stosowany w danej sieci. Z listy **Znane sieci** należy wybrać sieć i kliknąć opcję **Edytuj** w celu przypisania do określonej sieci profilu zapory z menu rozwijanego **Profil zapory**. Jeśli do danej sieci nie przypisano profilu, użyty zostanie profil domyślny karty sieciowej. Jeśli karta sieciowa została skonfigurowana tak, by nie używać profilu sieci, profil domyślny karty zostanie zastosowany bez względu na to, z którą siecią jest połączona. Jeśli nie istnieje profil sieci ani profil konfiguracji karty, używany jest globalny profil domyślny. W celu przypisania profilu do karty sieciowej należy wybrać daną kartę sieciową, kliknąć opcję **Edytuj** obok pozycji **Profile przypisane do kart sieciowych**, wybrać profil z menu rozwijanego **Domyślny profil zapory**, a następnie kliknąć polecenie **Zapisz**.

Kiedy zapora osobista zostanie przełączona do innego profilu, w prawym dolnym rogu ekranu, tuż obok zegara systemowego, zostanie wyświetlone powiadomienie.

3.9.2.2.1 Profile przypisane do kart sieciowych

Zmieniając profile, można w szybki sposób wprowadzić liczne zmiany w zachowaniu zapory. Dla poszczególnych profili można ustawić i zastosować reguły niestandardowe. Wpisy kart sieciowych dotyczące wszystkich kart obecnych w urządzeniu są automatycznie dodawane do listy **Karty sieciowe**.

Kolumny

Nazwa — nazwa karty sieciowej.

Domyślny profil zapory — domyślny profil wykorzystywany jest wówczas, gdy sieć, z którą użytkownik jest połączony, nie ma skonfigurowanego profilu lub karta sieciowa użytkownika jest skonfigurowana w taki sposób, by nie korzystać z profilu sieciowego.

Preferuj profil sieci — gdy włączona jest opcja **Preferowanie profilu zapory połączonej sieci**, karta sieciowa w miarę możliwości korzystać będzie z profilu zapory przypisanego do połączonej sieci.

Elementy sterujące

Dodaj — pozwala dodać nową kartę sieciową.

Edytuj — pozwala edytować istniejące karty sieciowe.

Usuń — należy wybrać kartę sieciową, a następnie kliknąć opcję **Usuń** w celu usunięcia karty sieciowej z listy.

OK/Anuluj — opcję **OK** należy kliknąć w celu zapisania zmian, a opcję **Anuluj** w celu zamknięcia okna bez wprowadzania zmian.

3.9.2.3 Konfigurowanie i używanie reguł

Reguły stanowią zestaw warunków używanych do testowania wszystkich połączeń sieciowych i wszystkich działań przypisanych do tych warunków. Za pomocą reguł zapory osobistej można zdefiniować działania, które mają być podejmowane w przypadku nawiązania różnego rodzaju połączeń sieciowych. Aby uzyskać dostęp do ustawień filtrowania reguł, należy przejść do obszaru **Ustawienia zaawansowane** (F5) > **Zapora osobista** > **Podstawowe**. Część wstępnie zdefiniowanych reguł jest powiązana z polami wyboru **dozwolonych usług** (IDS i opcje zaawansowane). Takich reguł nie można wyłączyć bezpośrednio i trzeba użyć w tym celu powiązanych z nimi pól wyboru.

Inaczej niż w poprzedniej wersji programu ESET Endpoint Security, reguły są klasyfikowane kolejno od góry do dołu. Czynność związana z pierwszą pasującą regułą jest stosowana w odniesieniu do każdego połączenia sieciowego poddawanego ocenie. Jest to istotna zmiana funkcjonalna w stosunku do poprzedniej wersji, gdzie priorytet reguł był ustalany automatycznie, a bardziej szczegółowe reguły miały wyższy priorytet od tych bardziej ogólnych.

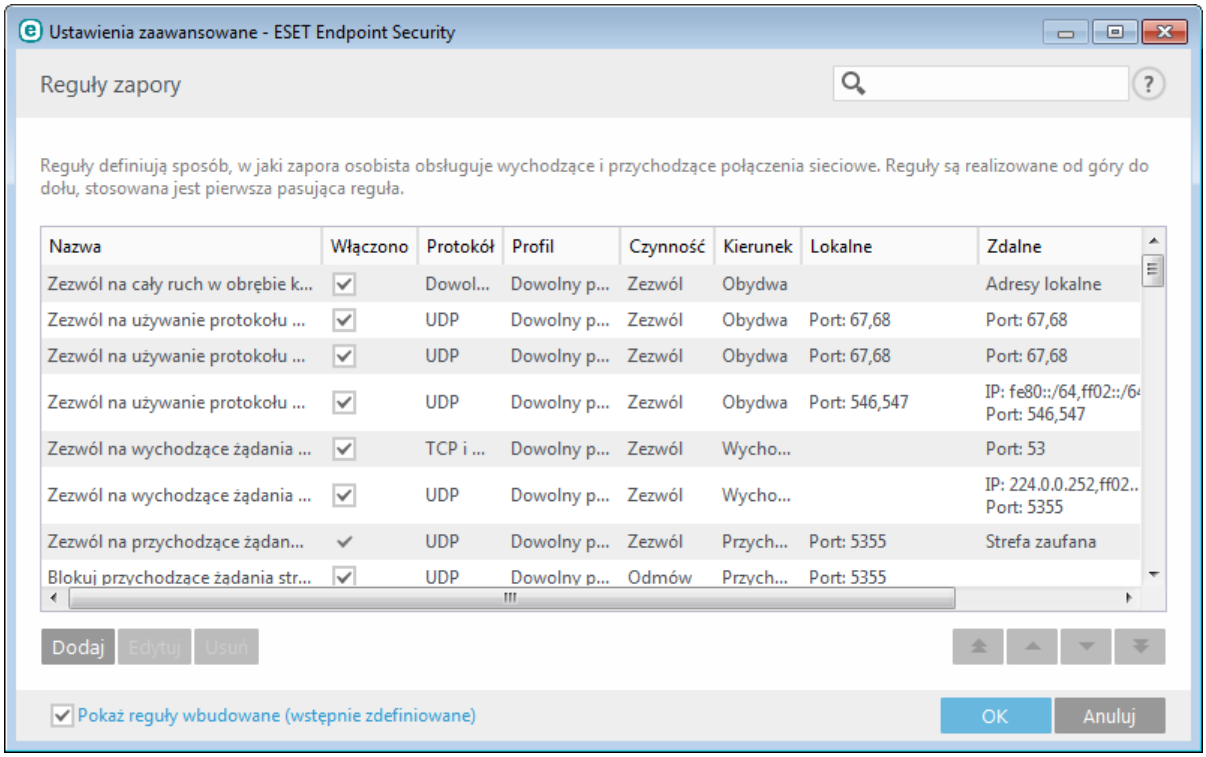
Połączenia można podzielić na przychodzące i wychodzące. Połączenia przychodzące są inicjowane przez komputer zdalny, który stara się nawiązać połączenie z systemem lokalnym. Połączenia wychodzące działają w sposób odwrotny — system lokalny kontaktuje się z komputerem zdalnym.

W przypadku wykrycia nowego, nieznanego połączenia należy dokładnie rozważyć, czy zezwolić na to połączenie, czy odmówić. Niepożądane, niezabezpieczone lub nieznane połączenia stanowią zagrożenie dla bezpieczeństwa systemu. Gdy zostanie nawiązane takie połączenie, zalecamy zwrócenie szczególnej uwagi na komputer zdalny i aplikację, która próbuje połączyć się z komputerem użytkownika. Wiele ataków polega na próbie pozyskania i wysłania prywatnych danych lub pobraniu niebezpiecznych aplikacji na stacje robocze hosta. Zapora osobista umożliwia użytkownikowi wykrycie i przerwanie takich połączeń.

3.9.2.3.1 Reguły zapory

Kliknięcie opcji **Edytuj** obok pozycji **Reguły** na karcie **Podstawowe** umożliwia wyświetlenie okna **Reguły zapory** z listą wszystkich reguł. Opcje **Dodaj**, **Edytuj** oraz **Usuń** umożliwiają dodawanie, konfigurowanie oraz usuwanie reguł. Aby ustalić priorytet danej reguły można ustalić, należy ją zaznaczyć i kliknąć jedną z opcji **Na początek/W górę/W dół/Na koniec**.

PORADA: Reguły można wyszukiwać na podstawie nazwy, protokołu lub portu przy użyciu pola **Wyszukaj**.



Kolumny

Nazwa — nazwa reguły.

Włączono — informacja o tym, czy reguły są włączone czy wyłączone. Aktywowanie reguły wymaga zaznaczenia odpowiedniego pola wyboru.

Protokół — protokół, którego dotyczy reguła.

Profil — wskazuje profil, którego dotyczy reguła.

Czynność — wskazuje stan komunikacji (blokuj/zezwalaj/pytaj).

Kierunek — kierunek komunikacji (przychodząca/wychodząca/obie).

Lokalny — adres IP i port komputera lokalnego.

Zdalny — adres IP i port komputera zdalnego.

Aplikacje — aplikacje, których dotyczy reguła.

Elementy sterujące

Dodaj — umożliwia utworzenie nowej reguły.

Edytuj — pozwala edytować istniejące reguły.

Usuń — umożliwia usuwanie istniejących reguł.

Pokaż reguły wbudowane (wstępnie zdefiniowane) — reguły wstępnie zdefiniowane w programie ESET Endpoint Security, które zezwalają na daną komunikację lub blokują ją. Wstępnie zdefiniowane reguły można wyłączyć, ale nie można ich usuwać.

Na początek/W górę/W dół/Na koniec — te opcje umożliwiają dostosowywanie priorytetów reguł (reguły są wykonywane kolejno od góry do dołu).

3.9.2.3.2 Obsługa reguł

Modyfikacja jest wymagana wtedy, gdy monitorowane parametry ulegną zmianie. W razie wprowadzenia zmian, które powodują, że reguła nie spełnia warunków, a określone działania nie mogą zostać wykonane, dane połączenie może zostać odrzucone. Może to spowodować problemy w działaniu aplikacji, której dotyczy reguła. Przykładem może być zmiana adresu sieciowego lub numeru portu strony zdalnej.

Górna część okna zawiera trzy karty:

- **Ogólne** — umożliwia podanie nazwy reguły, kierunku połączenia, czynności (**Zezwól**, **Odmów**, **Pytaj**), protokołu i profilu, w którym reguła ma być stosowana.
- **Lokalne** — udostępnia informacje o lokalnej stronie połączenia: lokalny port lub zakres portów oraz nazwę aplikacji korzystającej z połączenia. Umożliwia również dodanie wstępnie zdefiniowanej lub utworzonej strefy z zakresem adresów IP poprzez kliknięcie opcji **Dodaj**.
- **Zdalny** — ta karta zawiera informacje o porcie zdalnym (zakresie portów). Użytkownik może tutaj określić listy zdalnych adresów IP lub stref dla danej reguły. Może również dodać wstępnie zdefiniowaną lub utworzoną strefę z zakresem adresów IP poprzez kliknięcie opcji **Dodaj**.

Podczas tworzenia nowej reguły należy w polu **Nazwa** wprowadzić nazwę reguły. Z menu rozwijanego **Kierunek** wybierz kierunek, którego dotyczy reguła, a z menu rozwijanego **Czynność** wybierz czynność, która ma zostać wykonana, gdy połączenie spełnia regułę.

Protokół określa używany w regule protokół transmisji. Z menu rozwijanego wybierz protokół, który ma zostać użyty dla danej reguły.

Typ/kod ICMP oznacza komunikat ICMP identyfikowany na podstawie liczby (np. 0 oznacza „Odpowiedź echa").

Wszystkie reguły są domyślnie włączone dla **dowolnego profilu**. Zamiast tego można wybrać własny profil zapory z menu rozwijanego **Profile**.

Po włączeniu opcji **Zapisz w dzienniku** wszelkie działania związane z regułą będą rejestrowane w dzienniku. **Powiadom użytkownika** powoduje wyświetlenie powiadomienia po zastosowaniu reguły.

Poniżej znajduje się przykład, w którym tworzymy nową regułę, by zezwolić przeglądarce internetowej na uzyskanie dostępu do sieci. W tym przykładzie należy skonfigurować następujące elementy:

- Na karcie **Ogólne** należy włączyć połączenia wychodzące korzystające z protokołów TCP i UDP.
- Na karcie **Lokalne** dodaj aplikację przeglądarki (dla programu Internet Explorer jest to plik iexplore.exe).
- Na karcie **Zdalne** włącz port o numerze 80, jeśli chcesz zezwolić na standardowe przeglądanie Internetu.

UWAGA: Należy pamiętać, że reguły wstępnie zdefiniowane można modyfikować w ograniczonym zakresie.

3.9.2.4 Strefa zaufana

Strefa zaufana to grupa adresów sieciowych, w przypadku których zapora osobista zezwala na ruch przychodzący z zastosowaniem ustawień domyślnych. Wewnątrz strefy zaufanej ustawienia takich funkcji, jak udostępnianie plików i pulpit zdalny są konfigurowane w sekcji IDS i opcje zaawansowane.

Rzeczywista strefa zaufana jest obliczana dynamicznie i osobno dla każdej karty sieciowej na podstawie tego, z jaką siecią komputer jest aktualnie połączony. Adresy, które w Edytorze stref zdefiniowano jako znajdujące się wewnątrz strefy zaufanej, zawsze są traktowane jako zaufane. Jeśli karta sieciowa jest połączona ze znaną siecią, adresy skonfigurowane dla tej sieci w części **Dodatkowe adresy zaufane** są dodawane do strefy zaufanej tej karty sieciowej. Jeśli typ zabezpieczeń sieci to W domu/pracy, do strefy zaufanej dodawane są wszystkie bezpośrednio połączone podsieci. Rzeczywistą strefę zaufaną poszczególnych kart sieciowych można wyświetlić w oknie **Ustawienia**, w obszarze **Sieć** > **Karty sieciowe**.

UWAGA: Ustalanie stref zaufanych na podstawie interfejsu nie jest obsługiwane w systemach operacyjnych Windows XP. W tych systemach operacyjnych dla wszystkich kart sieciowych wyznaczana jest ta sama strefa zaufana, co jest również widoczne na stronie Karty sieciowe.

3.9.2.5 Konfigurowanie stref

Strefy to grupy adresów IP. Są przydatne, gdy użytkownik chce wykorzystać ten sam zestaw adresów w licznych regułach. Strefy te można konfigurować w pozycji **Ustawienia zaawansowane** > **Zapora osobista** > **Podstawowe**, klikając przycisk **Edytuj** obok pozycji **Strefy**. Aby dodać nową strefę, należy kliknąć opcję **Dodaj**, wprowadzić **Nazwę** strefy, jej **Opis**, a następnie dodać zdalny adres IP w polu **Adres zdalnego komputera (IPv4, IPv6, zakres, maska)**.

W oknie dialogowym **Strefy zapory** użytkownik może określić nazwę strefy, jej opis oraz listę adresów sieciowych (zobacz również Edytor znanych sieci).

3.9.2.6 Znane sieci

W przypadku korzystania z komputera, który często łączy się z sieciami publicznymi lub z sieciami spoza sieci używanej w pracy, zalecamy zweryfikowanie wiarygodności nowych sieci, z którymi nawiązywane jest połączenie. Po zdefiniowaniu sieci program ESET Endpoint Security może rozpoznawać zaufane sieci (W domu/pracy) przy użyciu różnych parametrów sieciowych skonfigurowanych w obszarze **Identyfikacja sieci**. Adresy IP komputerów przyłączających się do sieci są często podobne do adresu sieci zaufanej. W takich sytuacjach nieznana sieć może być uznana przez program ESET Endpoint Security za sieć zaufaną (W domu/pracy). W celu uniknięcia tego typu sytuacji zalecamy korzystanie z opcji **Uwierzytelnianie sieci**.

Gdy karta sieciowa połączy się z siecią lub gdy jej ustawienia sieciowe zostaną ponownie skonfigurowane, program ESET Endpoint Security przeszuka listę znanych sieci pod kątem rekordu odpowiadającego nowej sieci. Jeśli dane w pozycjach **Identyfikacja sieci** i **Uwierzytelnianie sieci** (opcjonalnie) okażą się zgodne, sieć zostanie oznaczona jako połączona w tym interfejsie. Gdy nie zostanie znaleziona żadna znana sieć, po przeprowadzeniu konfiguracji identyfikacji sieci zostanie utworzona nowa sieć, co umożliwi zidentyfikowanie tej sieci przy okazji kolejnego połączenia z nią. Domyślnie w odniesieniu do nowego połączenia sieciowego użyty zostanie typ zabezpieczeń **Publiczna**. W oknie dialogowym **Wykryto nowe połączenie sieciowe** należy wybrać typ zabezpieczeń. Dostępne opcje to **Publiczna** lub **W domu/pracy**. Jeśli karta sieciowa jest połączona ze znaną siecią, przy czym ta sieć jest oznaczona jako **W domu/pracy**, lokalne podsieci karty sieciowej zostają dodane do strefy zaufanej.

UWAGA: Włączenie opcji **Oznaczaj automatycznie nowe sieci jako publiczne** spowoduje, że okno dialogowe **Wykryto nowe połączenie sieciowe** nie będzie wyświetlane, a sieci, z którymi będą nawiązywane połączenia będą automatycznie oznaczane jako publiczne. W związku z tym niektóre funkcje (na przykład udostępnianie plików oraz pulpit zdalny) staną się niedostępne w nowych sieciach.

Znane sieci można skonfigurować ręcznie w oknie Edytor znanych sieci.

3.9.2.6.1 Edytor znanych sieci

Znane sieci można konfigurować ręcznie w obszarze **Ustawienia zaawansowane** > **Zapora osobista** > **Znane sieci** po kliknięciu opcji **Edytuj**.

Kolumny

Nazwa — nazwa znanej sieci.

Typ zabezpieczeń — wskazuje, czy ustawiony typ sieci to **W domu/pracy** czy **Publiczna**.

Profil zapory — należy wybrać profil z menu rozwijanego **Wyświetl reguły używane w profilu**, aby wyświetlić filtr reguł profilu.

Elementy sterujące

Dodaj — pozwala utworzyć nową znaną sieć.

Edytuj — pozwala edytować istniejące znane sieci.

Usuń — aby usunąć sieć z listy znanych sieci, należy ją zaznaczyć i kliknąć opcję **Usuń**.

Na początek/W górę/W dół/Na koniec — możliwość dostosowania priorytetów znanych sieci (sieci są klasyfikowane kolejno od góry do dołu).

Ustawienia konfiguracji sieci dostępne są na następujących kartach:

Sieć

Tutaj można zdefiniować nazwę sieci i wybrać typ zabezpieczeń sieci (**Publiczna** lub **W domu/pracy**). Z menu rozwijanego **Profil zapory** należy wybrać profil dla danej sieci. Jeśli w odniesieniu do sieci używany jest typ zabezpieczeń **W domu/pracy**, wszystkie bezpośrednio z nią połączone podsieci są uznawane za zaufane. Jeśli na przykład z daną siecią połączona jest karta sieciowa o adresie IP 192.168.1.5, a maska podsieci to 255.255.255.0, podsieć 192.168.1.0/24 jest dodawana do strefy zaufanej tej karty sieciowej. Jeśli karta sieciowa obsługuje więcej adresów/podsieci, wszystkie będą traktowane jako zaufane, niezależnie od ustawienia **Identyfikacja sieci** znanej sieci.

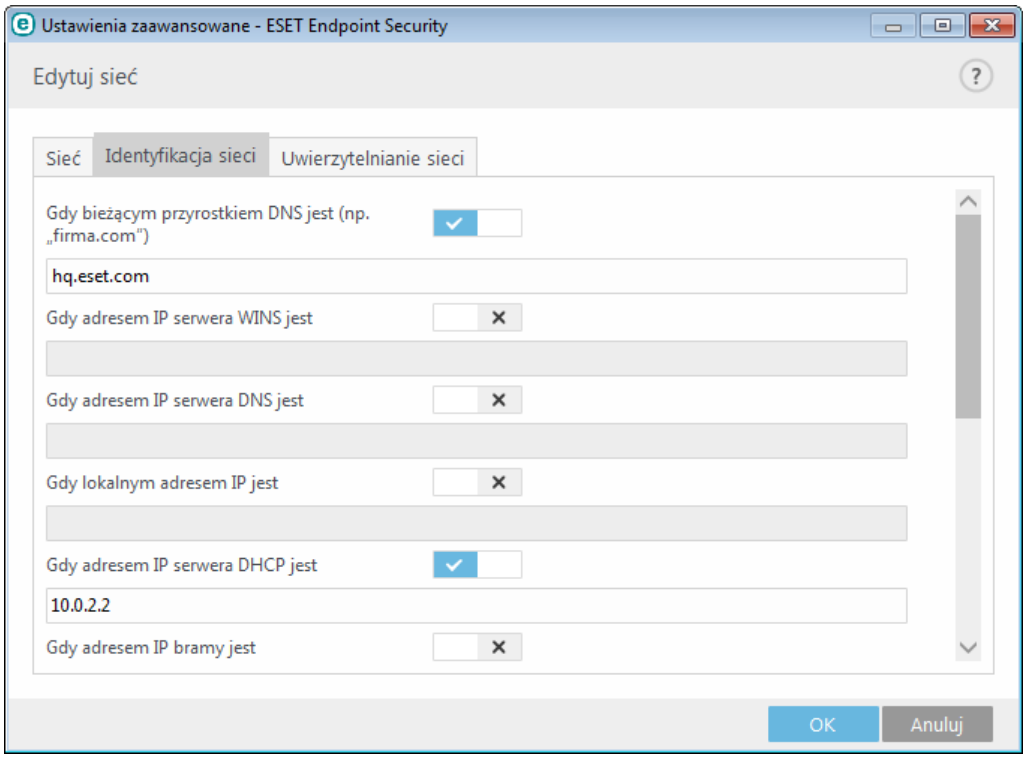
Ponadto adresy dodawane w obszarze **Dodatkowe adresy zaufane** są zawsze dodawane do strefy zaufanej kart sieciowych połączonych z tą siecią (niezależnie od typu zabezpieczeń sieci).

Aby sieć została oznaczona jako połączona na liście połączonych sieci, spełnione muszą być następujące warunki:

- Identyfikacja sieci — wszystkie podane parametry muszą być zgodne z parametrami aktywnego połączenia.
- Uwierzytelnianie sieci — w przypadku wybrania serwera uwierzytelniającego musi dojść do pomyślnego uwierzytelnienia przy użyciu serwera uwierzytelniania ESET.
- Ograniczenia sieci (wyłącznie Windows XP) — wszystkie wybrane ograniczenia globalne muszą być spełnione.

Identyfikacja sieci

Identyfikacja sieci dokonywana jest na podstawie parametrów karty sieciowej podłączonej do sieci lokalnej. Wszystkie wybrane parametry są porównywane z parametrami rzeczywistymi aktywnych połączeń sieciowych. Dozwolone są adresy IPv4 oraz IPv6.

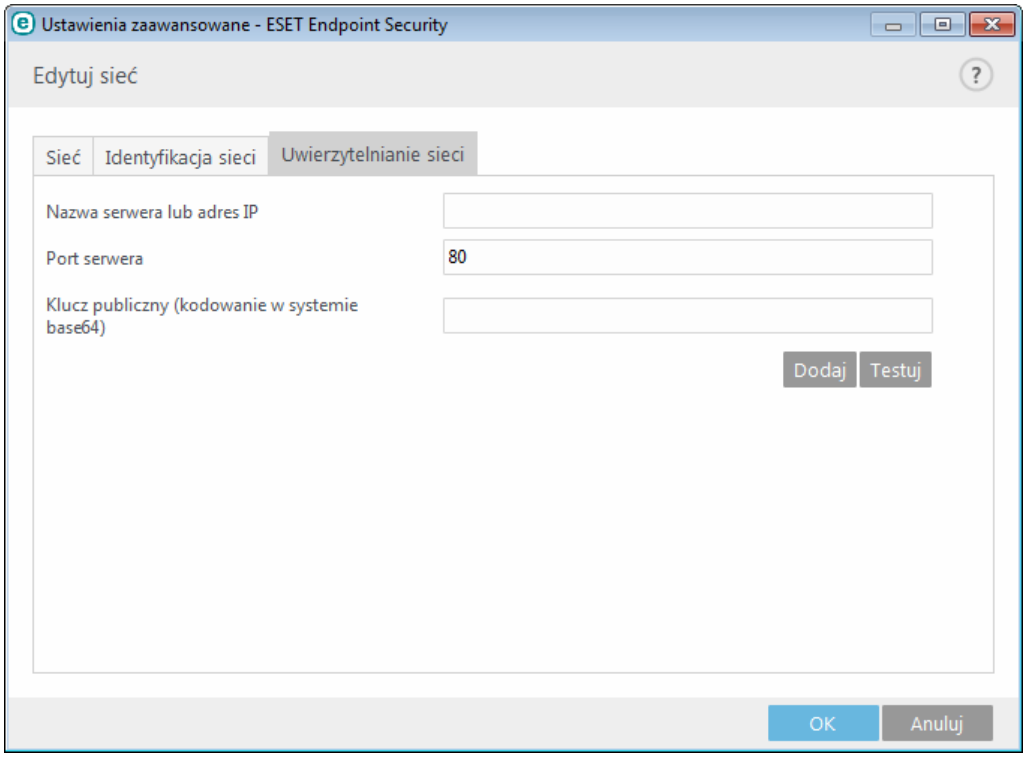


Uwierzytelnianie sieci

Moduł uwierzytelniania sieci wyszukuje określony serwer w sieci i korzysta z szyfrowania asymetrycznego (RSA) w celu uwierzytelnienia tego serwera. Nazwa uwierzytelnianej sieci musi być zgodna z nazwą strefy podaną w ustawieniach serwera uwierzytelniania. W nazwie rozróżniana jest wielkość liter. Należy podać nazwę serwera, port nasłuchu serwera oraz klucz publiczny odpowiadający kluczowi prywatnemu serwera (patrz sekcja Uwierzytelnianie sieci — konfiguracja serwera). Nazwę serwera można wprowadzić w postaci adresu IP, nazwy DNS lub nazwy NetBios, po której można podać ścieżkę wskazującą lokalizację klucza na serwerze (np. nazwa_serwera_/katalog1/katalog2/uwierzytelnianie). Można zdefiniować serwery alternatywne do użytku. Wystarczy dopisać je do ścieżki oddzielone średnikami.

Klucz publiczny można zaimportować przy użyciu dowolnego z następujących typów plików:

- Zaszyfrowany klucz publiczny PEM (.pem) — ten klucz można wygenerować przy użyciu serwera uwierzytelniania ESET (patrz sekcja Uwierzytelnianie sieci — konfiguracja serwera).
- Zaszyfrowany klucz publiczny
- Certyfikat klucza publicznego (.crt)



Aby sprawdzić ustawienia, kliknij przycisk **Testuj**. Jeśli uwierzytelnianie zakończy się pomyślnie, zostanie wyświetlone powiadomienie *Uwierzytelnianie serwera powiodło się*. Jeśli uwierzytelnianie nie jest poprawnie skonfigurowane, zostanie wyświetlony jeden z następujących komunikatów o błędzie:

Uwierzytelnianie serwera nie powiodło się. Nieprawidłowy lub niezgodny podpis.
Podpis serwera jest niezgodny z wprowadzonym kluczem publicznym.

Uwierzytelnianie serwera nie powiodło się. Niezgodna nazwa sieci.
Nazwa skonfigurowanej sieci nie zgadza się z nazwą strefy serwera uwierzytelniania. Sprawdź obie te nazwy. Powinny być identyczne.

Uwierzytelnianie serwera nie powiodło się. Nieprawidłowa odpowiedź serwera lub brak odpowiedzi.
Brak odpowiedzi ma miejsce, gdy serwer nie jest uruchomiony lub gdy jest niedostępny. Nieprawidłowa odpowiedź może być odebrana w przypadku, gdy podany adres jest używany na innym serwerze HTTP.

Wprowadzono nieprawidłowy klucz publiczny.
Należy sprawdzić, czy plik wprowadzonego klucza publicznego nie jest uszkodzony.

Ograniczenia sieci (dotyczy tylko systemu Windows XP)

W nowoczesnych systemach operacyjnych (Windows Vista i nowsze) poszczególne karty sieciowe mają własne strefy zaufane i aktywne profile zapory. Niestety w systemie Windows XP ta architektura nie jest obsługiwana, w związku z czym dla wszystkich kart sieciowych używane są zawsze wspólna strefa zaufana i aktywny profil zapory. Stanowi to potencjalne zagrożenie bezpieczeństwa w przypadku, gdy urządzenie nawiązuje równoczesne połączenia z wieloma sieciami. Wówczas ruch generowany w sieci niezaufanej może być zakwalifikowany przy użyciu strefy zaufanej i profilu zapory, które skonfigurowano w odniesieniu do innej połączonej sieci. W celu zminimalizowania zagrożeń bezpieczeństwa i uniknięcia globalnego stosowania jednej konfiguracji sieci, gdy urządzenie łączy się z inną (potencjalnie niezaufaną) siecią, można zastosować wymienione poniżej ograniczenia.

W systemie Windows XP ustawienia połączonych sieci (strefa zaufana i profil zapory) są stosowane globalnie, chyba że zastosowane zostanie co najmniej jedno z tych ograniczeń i nie zostanie ono spełnione:

a. Tylko jedno połączenie jest aktywne
b. Nie nawiązano połączenia bezprzewodowego
c. Nie nawiązano niezabezpieczonego połączenia bezprzewodowego

3.9.2.6.2 Uwierzytelnianie sieci — konfiguracja serwera

Proces uwierzytelniania może zostać uruchomiony z dowolnego komputera lub serwera podłączonego do sieci, która ma zostać uwierzytelniona. Aplikacja serwera uwierzytelniania ESET musi być zainstalowana na komputerze lub serwerze, który będzie zawsze dostępny na potrzeby uwierzytelniania, gdy klient podejmie próbę połączenia się z siecią. Plik instalacyjny aplikacji serwera uwierzytelniania ESET jest dostępny do pobrania w witrynie firmy ESET.

Po zainstalowaniu aplikacji serwera uwierzytelniania ESET pojawi się okno dialogowe (dostęp do tej aplikacji można uzyskać, klikając kolejno pozycje **Start** > **Programy** > **ESET** > **Serwer uwierzytelniania ESET**).

Aby skonfigurować serwer uwierzytelniania, należy wprowadzić nazwę sieci służącej do uwierzytelniania i port nasłuchu serwera (domyślnie: 80) oraz wskazać lokalizację, w której ma być przechowywana para kluczy (publiczny i prywatny). Następnie należy wygenerować klucz publiczny i prywatny, które będą używane w procesie uwierzytelniania. Klucz prywatny pozostanie na serwerze, a klucz publiczny należy zaimportować po stronie klienta w sekcji Uwierzytelnianie sieci w trakcie konfigurowania sieci w ustawieniach zapory.

3.9.2.7 Zapisywanie w dzienniku

Zapora osobista programu ESET Endpoint Security zapisuje wszystkie ważne zdarzenia w pliku dziennika, który można wyświetlić bezpośrednio z poziomu menu głównego. Kliknij przycisk **Narzędzia** > **Pliki dziennika** a następnie wybierz opcję **Zapora osobista** z menu rozwijanego **Dziennik**. Aby włączyć zapisywanie w dzienniku zdarzeń związanych z zaporą osobistą, przejdź do obszaru **Ustawienia zaawansowane** > **Narzędzia** > **Pliki dziennika** i dla minimalnej szczegółowości zapisów w dzienniku wybierz ustawienie **Diagnostyczne.** Rejestrowane będą wszystkie odrzucone połączenia.

Pliki dziennika można wykorzystać podczas wykrywania błędów i włamań do systemu. Dzienniki zapory osobistej programu ESET zawierają następujące dane:

- **Czas** — data i godzina wystąpienia zdarzenia.
- **Zdarzenie** — nazwa zdarzenia.
- **Źródło** — adres sieciowy źródła.
- **Obiekt docelowy** — adres sieciowy obiektu docelowego.
- **Protokół** — protokół komunikacji sieciowej.
- **Reguła/nazwa robaka** — zastosowana reguła lub nazwa robaka w przypadku jego zidentyfikowania.
- **Aplikacja** — aplikacja, której dotyczy zdarzenie.
- **Użytkownik** — nazwa użytkownika zalogowanego w momencie wykrycia infekcji.

Dokładna analiza tych danych może pomóc w wykryciu prób złamania zabezpieczeń systemu. Wiele innych czynników wskazuje na potencjalne zagrożenia bezpieczeństwa i pozwala na zminimalizowanie ich skutków. Do przykładowych wskaźników potencjalnych zagrożeń należą: zbyt częste połączenia z nieznanych lokalizacji, wielokrotne próby nawiązania połączenia, połączenia nawiązywane przez nieznane aplikacje oraz użycie nietypowych numerów portów.

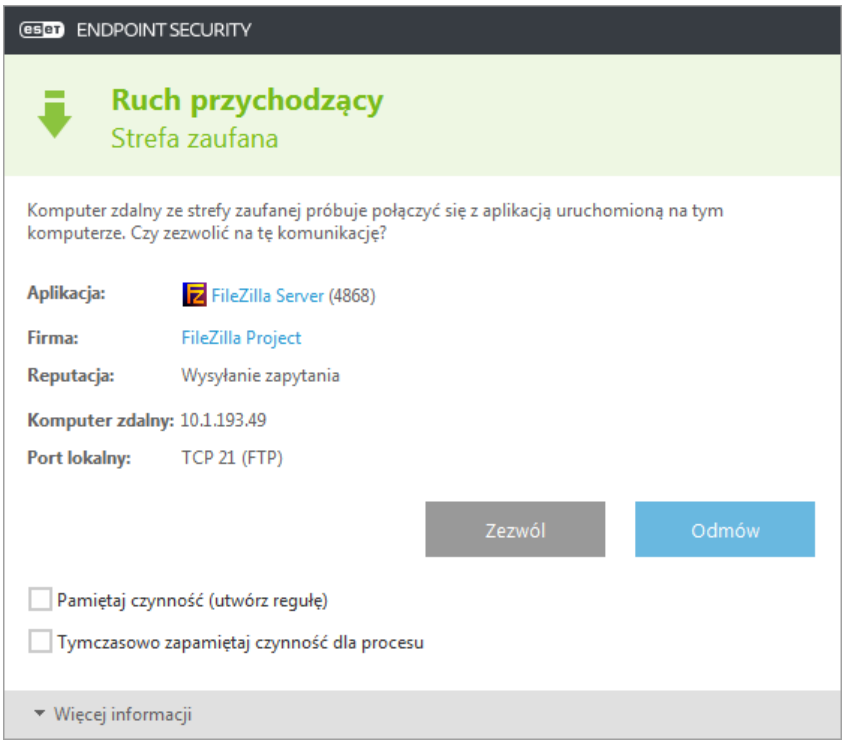
3.9.2.8 Ustanawianie połączenia — wykrywanie

Zapora osobista wykrywa każde nowo utworzone połączenie sieciowe. Aktywny tryb zapory określa, jakie działania są realizowane dla nowego połączenia. Jeśli uaktywniono opcję **Tryb automatyczny** lub **Tryb oparty na regułach**, zapora osobista będzie wykonywać zdefiniowane wstępnie czynności bez udziału użytkownika.

W trybie interaktywnym wyświetlane jest okno informacyjne z powiadomieniem o wykryciu nowego połączenia sieciowego wraz ze szczegółowymi informacjami na ten temat. Użytkownik może zezwolić na połączenie lub je odrzucić (odmowa). Jeśli użytkownik wielokrotnie zezwala na to samo połączenie przy użyciu okna dialogowego, zalecane jest utworzenie nowej reguły dla tego połączenia. W tym celu należy wybrać opcję **Pamiętaj czynność (utwórz regułę)** i zapisać czynność jako nową regułę dla zapory osobistej. Jeśli zapora wykryje w przyszłości to samo połączenie, zostanie zastosowana istniejąca już reguła bez wymogu interakcji ze strony użytkownika.

Ustawienie **Tymczasowo zapamiętaj czynność dla procesu** powoduje stosowanie czynności (**Zezwól**/**Odmów**) do

czasu ponownego uruchomienia aplikacji, zmiany reguł lub trybu filtrowania, aktualizacji modułu zapory lub ponownego uruchomienia systemu. Po wystąpieniu dowolnej z tych czynności reguły tymczasowe zostaną usunięte.



Należy ostrożnie podchodzić do tworzenia nowych reguł, zezwalając tylko na połączenia, które są bezpieczne. Jeśli wszystkie połączenia są dozwolone, zapora osobista nie spełnia swojego zadania. Oto ważne parametry połączeń:

- **Strona zdalna** — należy zezwalać na połączenia tylko z zaufanymi i znanymi adresami.
- **Aplikacja lokalna** — nie zaleca się zezwalania na połączenia z nieznanymi aplikacjami i procesami.
- **Numer portu** — w zwykłych warunkach powinna być dozwolona komunikacja za pośrednictwem typowych portów (np. ruch internetowy — port numer 80).

W celu rozprzestrzeniania się wirusy często używają połączeń internetowych i ukrytych, co ułatwia im infekowanie systemów zdalnych. Jeśli reguły są prawidłowo skonfigurowane, zapora osobista staje się użytecznym narzędziem ochrony przed wieloma próbami ataku prowadzonymi przy użyciu szkodliwego kodu.

3.9.2.9 Rozwiązywanie problemów z zaporą osobistą ESET

Jeśli na komputerze z zainstalowany programem ESET Endpoint Security pojawią się problemy z łącznością, istnieje kila sposobów, by sprawdzić, czy powoduje je zapora osobista ESET. Zapora osobista ESET może być również przydatna w tworzeniu nowych reguł lub wyjątków służących do rozwiązania problemów z łącznością.

Zapoznaj się z następującymi tematami pomocnymi w rozwiązywaniu problemów z zaporą osobistą:

- Kreator rozwiązywania problemów
- Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika
- Tworzenie wyjątków na podstawie powiadomień zapory
- Zaawansowane logowanie PCAP
- Rozwiązywanie problemów z filtrowaniem protokołów

3.9.2.9.1 Kreator rozwiązywania problemów

Kreator rozwiązywania problemów dyskretnie monitoruje wszystkie zablokowane połączenia i prowadzi użytkownika przez proces rozwiązywania problemów, by rozwiązać problemy zapory z konkretnymi aplikacjami lub urządzeniami. Następnie kreator sugeruje wprowadzenie nowego zestawu reguł, jeśli zostanie on zatwierdzony przez użytkownika. **Kreator rozwiązywania problemów** można znaleźć w głównym menu w pozycji **Ustawienia** > **Sieć**.

3.9.2.9.2 Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika

Zapora osobista ESET domyślnie nie zapisuje w dzienniku wszystkich zablokowanych połączeń. Aby sprawdzić, co zostało zablokowane przez zaporę osobistą, należy włączyć opcję zapisywania w dzienniku w sekcji **Rozwiązywanie problemów** menu **Ustawienia zaawansowane** w pozycji **Zapora osobista** > **IDS i opcje zaawansowane**. Jeśli w dzienniku znajduje się coś, co nie powinno być blokowane przez zaporę osobistą, można dla tego elementu utworzyć regułę lub wyjątek IDS, klikając go prawym przyciskiem myszy i wybierając pozycję **Nie blokuj w przyszłości podobnych zdarzeń**. Należy pamiętać, że dziennika wszystkich zablokowanych połączeń może zawierać tysiące pozycji i może być trudno znaleźć w nim określone połączenie. Po rozwiązaniu problemu można wyłączyć zapisywanie w dzienniku.

Więcej informacji na temat dziennika można znaleźć w sekcji Pliki dziennika.

Uwaga: Aby zobaczyć kolejność, w jakiej zapora osobista blokowała określone połączenia, należy skorzystać z zapisywania w dzienniku. Tworzenie reguł na podstawie dziennika umożliwia również tworzenie reguł dokładnie odpowiadających wymaganiom użytkownika.

3.9.2.9.2.1 Utwórz regułę z dziennika

W nowej wersji programu ESET Endpoint Security możliwe jest tworzenie reguł na podstawie dziennika. W menu głównym kliknij opcję **Narzędzia** > **Pliki dziennika**. Z menu rozwijanego wybierz opcję **Zapora osobista**, kliknij prawym przyciskiem myszy wybrany wpis dziennika i z menu kontekstowego wybierz opcję **Nie blokuj w przyszłości podobnych zdarzeń**. W oknie powiadomienia zostanie wyświetlona nowa reguła.

Aby umożliwić tworzenie nowych reguł na podstawie dziennika, w programie ESET Endpoint Security należy skonfigurować następujące ustawienia:

- w obszarze **Diagnostyka** w menu **Ustawienia zaawansowane** (F5) > **Narzędzia** > **Pliki dziennika** należy ustawić minimalną szczegółowość zapisów w dzienniku;
- należy włączyć funkcję **Wyświetlaj także powiadomienia po wykryciu ataku przychodzącego na luki zabezpieczeń** w obszarze **Ustawienia zaawansowane** (F5) > **Zapora osobista** > **IDS i opcje zaawansowane** > **Wykrywanie włamań**.

3.9.2.9.3 Tworzenie wyjątków na podstawie powiadomień zapory osobistej

Gdy zapora osobista ESET wykryje szkodliwe działanie sieci, wyświetlone zostanie okno powiadomień zawierające opis zdarzenia. Powiadomienie to zawiera łącze umożliwiające dowiedzenie się więcej o zdarzeniu i w razie potrzeby ustalenie wyjątku dla tego zdarzenia.

UWAGA: Jeśli aplikacja lub urządzenie sieci nie implementuje poprawnie standardów sieci, może to spowodować powtarzające się wyzwalanie powiadomień zapory o IDS. Aby zapobiec wykrywaniu tej aplikacji lub tego urządzenia przez zaporę osobistą ESET, można utworzyć wyjątek bezpośrednio z powiadomienia.

3.9.2.9.4 Zaawansowane logowanie PCAP

Funkcja ta ma za zadanie zapewnienie pomocy technicznej ESET bardziej złożonych plików dziennika. Z funkcji tej należy korzystać wyłącznie na prośbę pomocy technicznej firmy ESET, gdyż może ona spowodować wygenerowanie obszernego pliku dziennika i spowolnienie pracy komputera.

1. Należy wybrać kolejno opcje **Ustawienia zaawansowane** > **Narzędzia** > **Diagnostyka** i włączyć opcję **Włącz zaawansowane rejestrowanie filtrowania protokołów**.
2. Spróbuj odtworzyć napotkany problem.
3. Wyłącz zaawansowane logowanie PCAP.
4. Plik dziennika PCAP znajduje się w tym samym katalogu, gdzie generowane są diagnostyczne zrzuty pamięci:

- System Microsoft Windows Vista lub nowszy

  C:\ProgramData\ESET\ESET Endpoint Security\Diagnostics

- System Microsoft Windows XP

  C:\Documents and Settings\All Users\...

3.9.2.9.5 Rozwiązywanie problemów z filtrowaniem protokołów

W przypadku wystąpienia problemów z przeglądarką lub programem poczty e-mail pierwszym krokiem jest ustalenie, czy powodem jest filtrowanie protokołów. W tym celu należy tymczasowo wyłączyć filtrowanie protokołów aplikacji w ustawieniach zaawansowanych (należy pamiętać o jej ponownym włączeniu po zakończeniu tych działań, gdyż w przeciwnym wypadku przeglądarka i program poczty e-mail pozostaną niezabezpieczone). Jeśli po wyłączeniu tej funkcji problem ustąpi, należy skorzystać z poniższej listy typowych problemów i sposobów ich rozwiązania:

Problemy z aktualizacją lub bezpieczną komunikacją

Gdy aplikacja sygnalizuje brak możliwości przeprowadzenia aktualizacji lub braki w zabezpieczeniach kanału komunikacji:

- Jeśli filtrowanie protokołu SSL jest włączone, należy spróbować tymczasowo wyłączyć tę opcję. Jeśli to pomoże, można nadal używać filtrowania protokołu SSL, umożliwiając aktualizację poprzez wykluczenie komunikacji, która przysparza problemów:
  Zmień tryb filtrowania protokołu SSL na interaktywny. Ponownie uruchom aktualizację. Powinno zostać wyświetlono okno dialogowe z informacją na temat szyfrowanego ruchu sieciowego. Sprawdź, czy dotyczy aplikacji, w której występuje rozwiązywany problem i czy certyfikat pochodzi z serwera, z którego pobierana jest aktualizacja. Następnie wybierz opcję zapamiętania czynności dla tego certyfikatu i kliknij przycisk Ignoruj. Jeśli nie zostaną wyświetlone żadne inne istotne okna dialogowe, można przywrócić automatycznych tryb filtrowania, a problem powinien być rozwiązany.
- Jeśli aplikacja, której dotyczy problem nie jest przeglądarką ani programem poczty e-mail, można ją całkowicie wykluczyć z filtrowania protokołów (w przypadku przeglądarki lub programu poczty e-mail spowodowałoby to jednak narażenie na zagrożenia). Dowolna aplikacja, w odniesieniu do której stosowane było wcześniej filtrowanie komunikacji powinna znajdować się już na liście wyświetlonej podczas dodawania wyjątku, zatem nie powinno być konieczne ręczne dodawanie aplikacji.

Problem z uzyskiwaniem dostępu do urządzenia w sieci użytkownika

Jeśli w sieci użytkownika niemożliwe jest korzystanie z dowolnych funkcji urządzenia (może to być otwieranie strony kamery internetowej lub odtwarzanie filmu na domowym odtwarzaczu multimedialnym), należy spróbować dodać adresy IPv4 i IPv6 urządzenia do listy adresów wyłączonych.

Problemy z konkretną stroną internetową

Wybrane strony internetowe można wyłączyć z filtrowania protokołów przy użyciu funkcji zarządzania adresami URL. Jeśli na przykład nie można uzyskać dostępu do strony https://www.gmail.com/intl/en/mail/help/about.html,

należy spróbować dodać *gmail.com* do listy adresów wyłączonych.

Błąd „Niektóre aplikacje zdolne do importowania certyfikatu głównego są nadal uruchomione”

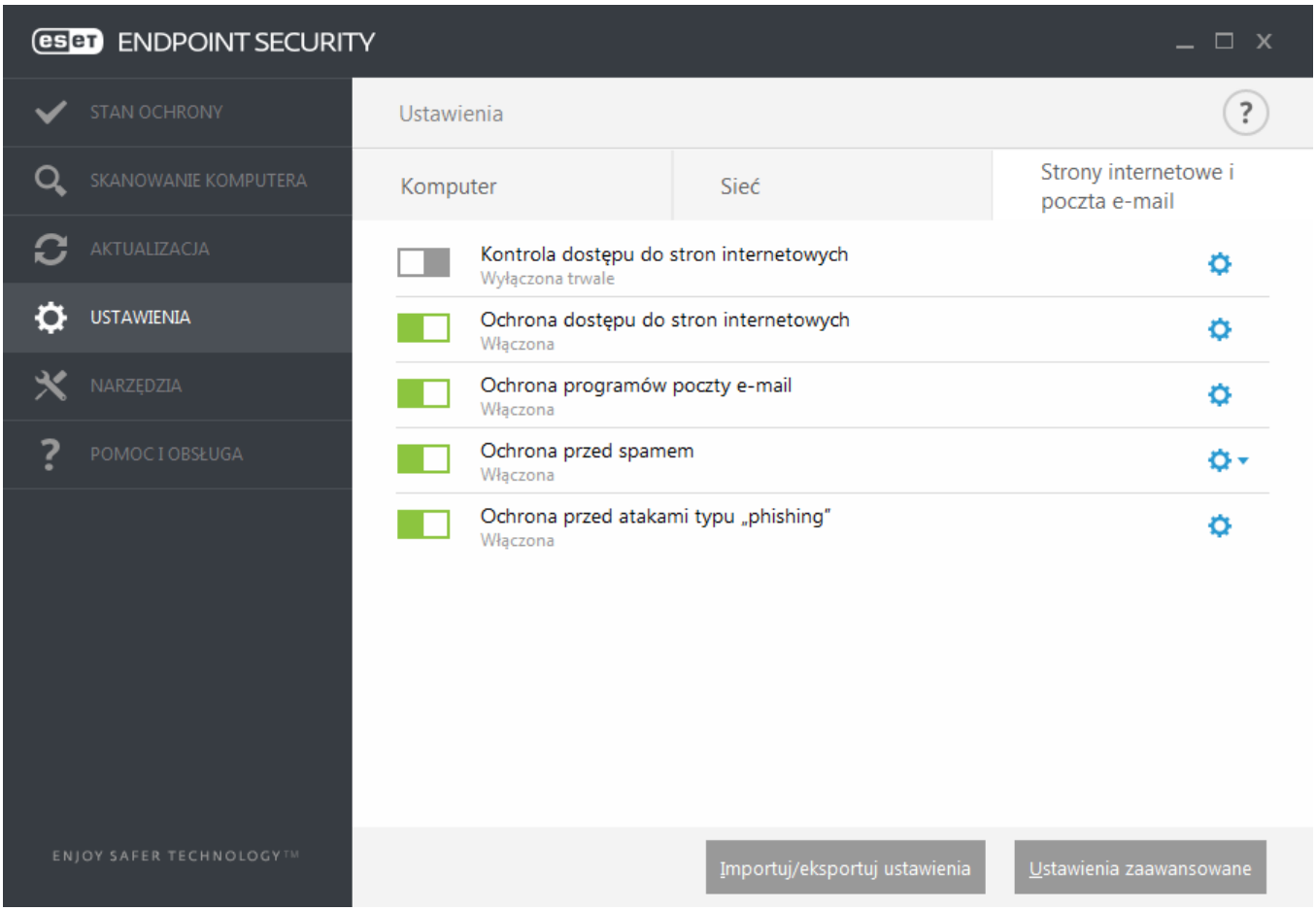
Po włączeniu filtrowania protokołu SSL program ESET Endpoint Security importuje certyfikat do magazynu certyfikacji zainstalowanych aplikacji, by zapewnić odpowiednie ustawienia zaufania w odniesieniu do sposobu filtrowania protokołu SSL. W niektórych aplikacjach nie jest to możliwe, gdy są one uruchomione. Dotyczy to programów Firefox i Opera. Należy sprawdzić, czy nie są uruchomione (najlepszym sposobem jest otwarcie Menedżera zadań i sprawdzenie, czy na karcie Procesy znajdują się pozycje firefox.exe lub opera.exe). Po zamknięciu tych programów należy ponowić próbę.

Błąd związany z niezaufanym wydawcą lub nieprawidłową sygnaturą

Najprawdopodobniej oznacza to, że opisany powyżej import się nie powiódł. Najpierw należy zadbać o to, by żadna z wymienionych aplikacji nie była uruchomiona. Następnie trzeba wyłączyć filtrowanie protokołu SSL i włączyć je ponownie. To spowoduje ponowne uruchomienie importu.

3.9.3 Strony internetowe i poczta e-mail

Ustawienia dotyczące stron internetowych i poczty e-mail można znaleźć w obszarze **Ustawienia** > **Strony internetowe i poczta e-mail**. Z tego miejsca można uzyskać dostęp do bardziej szczegółowych ustawień programu.



Moduł **Kontrola dostępu do stron internetowych** umożliwia konfigurowanie ustawień zapewniających administratorom zautomatyzowane narzędzia pomagające w ochronie stacji roboczych oraz w ustalaniu ograniczeń związanych z przeglądaniem Internetu. Celem funkcji Kontrola dostępu do stron internetowych jest uniemożliwianie dostępu do stron zawierających nieodpowiednie lub szkodliwe treści. Więcej informacji można znaleźć w sekcji Kontrola dostępu do stron internetowych.

Obsługa komunikacji przez Internet jest standardową funkcją komputerów osobistych. Niestety komunikacja internetowa stała się głównym sposobem przenoszenia szkodliwego kodu. Z tego względu ważne jest umiejętne dobranie ustawień funkcji **Ochrona dostępu do stron internetowych**.

Funkcja **Ochrona programów poczty e-mail** umożliwia kontrolowanie wiadomości e-mail odbieranych przy użyciu

protokołów POP3 oraz IMAP. Dzięki zastosowaniu wtyczki do programu poczty e-mail, program ESET Endpoint Security umożliwia kontrolowanie całości komunikacji obsługiwanej przez program poczty e-mail (POP3, MAPI, IMAP i HTTP).

Moduł **Ochrona przed spamem** filtruje niepożądane wiadomości e-mail.

Kliknięcie koła zębatego widocznego obok pozycji **Ochrona przed spamem** spowoduje wyświetlenie następujących opcji:

Konfiguruj... — otwarcie ustawień zaawansowanych ochrony programów poczty e-mail przed spamem.

Biała lista/czarna lista/lista wyłączeń użytkownika — umożliwia otwarcie okna dialogowego, w którym można dodawać, edytować i usuwać adresy e-mail uznawane za bezpieczne lub niebezpieczne. Na podstawie zdefiniowanych tutaj reguł wiadomości e-mail wysyłane z tych adresów nie będą skanowane lub będą uznawane za spam. Kliknięcie **Listy wyłączeń użytkownika** umożliwia otwarcie okna dialogowego, w którym można dodawać, edytować i usuwać adresy e-mail uznawane za sfałszowane metodą spoofingu i służące do wysyłania spamu. Wiadomości e-mail nadane z adresu występującego na liście wyłączeń są zawsze skanowane pod kątem spamu.

Ochrona przed atakami typu „phishing” to kolejna warstwa zabezpieczeń, zapewniająca wzmocnienie ochrony przed stronami internetowymi służącymi do prób bezprawnego pozyskiwania haseł oraz innych informacji poufnych. Ochrona przed atakami typu „phishing” to opcja, którą można znaleźć w okienku **Ustawienia**, w obszarze **Strony internetowe i poczta e-mail**. Więcej informacji można znaleźć w sekcji Ochrona przed atakami typu „phishing”.

Zamknij — ten przełącznik służy do wyłączania ochrony stron internetowych/poczty e-mailoraz ochrony przed spamem w przeglądarkach internetowych oraz programach poczty e-mail  .

3.9.3.1 Filtrowanie protokołów

Ochrona antywirusowa protokołów aplikacji jest realizowana z wykorzystaniem technologii ThreatSense, w której połączono wszystkie zaawansowane metody wykrywania szkodliwego oprogramowania. Filtrowanie protokołów odbywa się automatycznie, niezależnie od przeglądarki internetowej i programu pocztowego. Aby zmodyfikować ustawienia komunikacji szyfrowanej (SSL), należy wybrać kolejno opcje **Strony internetowe i poczta e-mail** > **SSL**.

Włącz ochronę zawartości protokołów aplikacji — przy użyciu tej opcji można wyłączyć filtrowanie protokołów. Należy pamiętać, że opcja ta ma wpływ na wiele komponentów programu ESET Endpoint Security (ochrona dostępu do stron internetowych, ochrona protokołów poczty e-mail, ochrona przed atakami typu „phishing”, kontrola dostępu do stron internetowych), które po jej wyłączeniu nie będą działać.

Wyłączone aplikacje — przy użyciu tej opcji można wyłączyć z filtrowania protokołów określone aplikacje. Jest przydatna, gdy filtrowanie protokołów powoduje problemy ze zgodnością.

Wyłączone adresy IP — przy użyciu tej opcji można wyłączyć z filtrowania protokołów określone adresy zdalne. Jest przydatna, gdy filtrowanie protokołów powoduje problemy ze zgodnością.

Przeglądarki internetowe i programy poczty e-mail — opcja używana wyłącznie w systemie operacyjnym Windows XP. Umożliwia wybranie aplikacji, w których cały ruch sieciowy będzie filtrowany w ramach filtrowania protokołów, bez względu na używane porty.

3.9.3.1.1 Przeglądarki internetowe i programy poczty e-mail

UWAGA: Począwszy od poprawki Windows Vista Service Pack 1 i systemu Windows Server 2008, do sprawdzania komunikacji sieciowej używana jest nowa architektura Windows Filtering Platform (WFP). W związku z tym, że technologia WFP używa specjalnych technik monitorowania, sekcja **Przeglądarki internetowe i programy poczty e-mail** jest niedostępna.

Ponieważ po Internecie krąży ogromna ilość szkodliwego kodu, bardzo ważny aspekt ochrony komputera stanowi zadbanie o bezpieczne przeglądanie stron internetowych. Potajemne przenikanie szkodliwego oprogramowania do systemu ułatwiają luki w zabezpieczeniach przeglądarek internetowych i spreparowane łącza. Dlatego głównym zadaniem programu ESET Endpoint Security jest zabezpieczenie przeglądarek internetowych. Jako przeglądarkę internetową można oznaczyć każdą aplikację korzystającą z sieci. Aplikacje, które używały już protokołów do komunikacji lub aplikacje z wybranej ścieżki można wprowadzić na listę Internet i programy poczty e-mail.

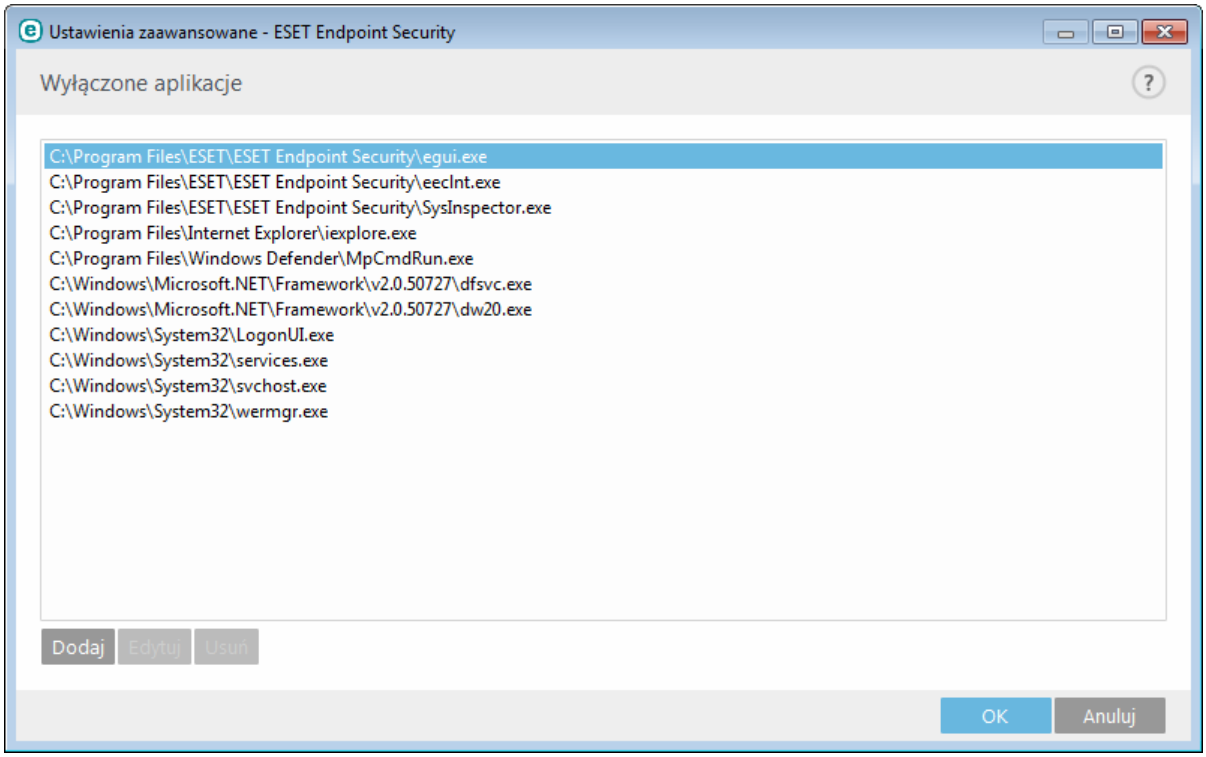
3.9.3.1.2 Aplikacje wyłączone

Aby wykluczyć z filtrowania protokołów komunikację prowadzoną przez określone aplikacje korzystające z sieci, należy dodać je do listy. Komunikacja prowadzona przez te aplikacje za pośrednictwem protokołów HTTP, POP3 oraz IMAP nie będzie sprawdzana pod kątem obecności zagrożeń. Zalecamy korzystanie z tej techniki tylko w przypadkach, gdy aplikacje nie działają poprawnie przy włączonym filtrowaniu protokołów.

Aplikacje i usługi objęte już wpływem filtrowania protokołów zostaną automatycznie wyświetlone po kliknięciu opcji **Dodaj**.

Edytuj — umożliwia edytowanie wybranych pozycji na liście.

Usuń — umożliwia usunięcie z listy wybranych pozycji.



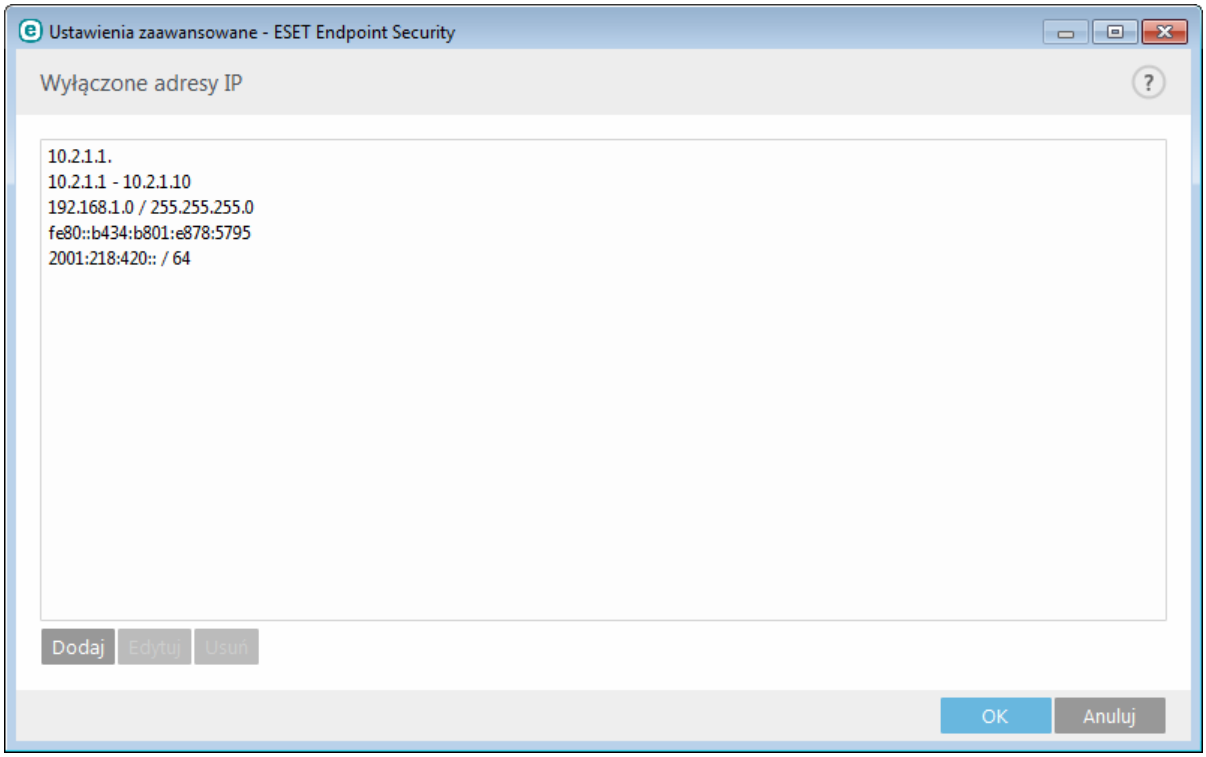
3.9.3.1.3 Wyłączone adresy IP

Adresy IP z tej listy zostaną wyłączone z filtrowania zawartości protokołów. Komunikacja z tymi adresami prowadzona za pośrednictwem protokołów HTTP, POP3 oraz IMAP nie będzie sprawdzana pod kątem obecności zagrożeń. Zalecamy użycie tej opcji tylko w przypadku adresów, o których wiadomo, że są godne zaufania.

Dodaj — ta opcja pozwala na dodanie adresu IP/zakresu adresów/podsieci, do których ma zostać zastosowana dana reguła.

Edytuj — umożliwia edytowanie wybranych pozycji na liście.

Usuń — umożliwia usunięcie z listy wybranych pozycji.



3.9.3.1.4 SSL/TLS

Program ESET Endpoint Security umożliwia sprawdzanie komunikacji z zastosowaniem protokołu SSL pod kątem zagrożeń. W przypadku sprawdzania komunikacji chronionej protokołem SSL można stosować różne tryby skanowania z użyciem certyfikatów zaufanych, nieznanych lub takich, które zostały wyłączone ze sprawdzania komunikacji chronionej przez protokół SSL.

Włącz filtrowanie protokołu SSL/TLS — gdy filtrowanie protokołu jest wyłączone, program nie skanuje komunikacji odbywającej się za pośrednictwem protokołu SSL.

Tryb filtrowania protokołu SSL/TLS jest dostępny w następujących opcjach:

Tryb automatyczny — wybranie tej opcji powoduje skanowanie całej komunikacji chronionej protokołem SSL oprócz komunikacji chronionej za pomocą certyfikatów wyłączonych ze sprawdzania. W przypadku nawiązania nowego połączenia z użyciem nieznanego, podpisanego certyfikatu użytkownik nie zostanie powiadomiony, a połączenie będzie automatycznie filtrowane. Gdy dostęp do serwera uzyskiwany jest przy użyciu certyfikatu niezaufanego oznaczonego jako zaufany (znajdującego się na liście zaufanych certyfikatów), komunikacja z serwerem nie zostanie blokowana, a jej treść jest filtrowana.

Tryb interaktywny — po wprowadzeniu przez użytkownika nowej witryny chronionej protokołem SSL (przy użyciu nieznanego certyfikatu) wyświetlane jest okno dialogowe umożliwiające wybranie czynności. W tym trybie można utworzyć listę certyfikatów SSL, które zostaną wyłączone ze skanowania.

Blokuj szyfrowaną komunikację z wykorzystaniem nieaktualnego protokołu SSL v2 — komunikacja używająca wcześniejszej wersji protokołu SSL będzie automatycznie blokowana.

Certyfikat główny

Certyfikat główny — aby w przeglądarkach internetowych/programach poczty e-mail komunikacja przy użyciu protokołu SSL przebiegała prawidłowo, konieczne jest dodanie certyfikatu głównego firmy ESET do listy znanych certyfikatów głównych (wydawców). Opcja **Dodaj certyfikat główny do znanych przeglądarek** powinna być włączona. Należy wybrać tę opcję w celu automatycznego dodania certyfikatu głównego firmy ESET do znanych przeglądarek (np. Opera i Firefox). Certyfikat jest dodawany automatycznie do przeglądarek korzystających z systemowego magazynu certyfikacji (np. Internet Explorer).

Aby zastosować certyfikat w przypadku nieobsługiwanych przeglądarek, należy kliknąć opcję **Wyświetl certyfikat** > **Szczegóły** > **Kopiuj do pliku**, a następnie ręcznie zaimportować go do przeglądarki.

Ważność certyfikatu

Jeżeli nie można zweryfikować certyfikatu w magazynie zaufanych głównych urzędów certyfikacji — w niektórych przypadkach certyfikat strony internetowej nie może być zweryfikowany przy użyciu magazynu zaufanych głównych urzędów certyfikacji. Oznacza to, że został on podpisany przez jakąś osobę (np. przez administratora serwera internetowego lub małej firmy) i uznanie go za zaufany certyfikat niekoniecznie wiąże się z ryzykiem. Większość dużych przedsiębiorstw (np. banki) korzysta z certyfikatów podpisanych przez jeden z zaufanych głównych urzędów certyfikacji. Jeśli pole wyboru **Pytaj o ważność certyfikatu** jest zaznaczone (ustawienie domyślne), zostanie wyświetlony monit o wybranie czynności, która ma zostać podjęta przy nawiązywaniu szyfrowanego połączenia. Można wybrać opcję **Blokuj komunikację używającą certyfikatu**, aby zawsze przerywać szyfrowane połączenia z witrynami, na których używane są niezweryfikowane certyfikaty.

Jeśli certyfikat jest nieprawidłowy lub uszkodzony — oznacza to, że wygasła jego ważność lub został nieprawidłowo podpisany. W takim przypadku zalecamy pozostawienie zaznaczenia opcji **Blokuj komunikację używającą certyfikatu**.

Lista znanych certyfikatów umożliwia dostosowanie sposobu działania programu ESET Endpoint Security w odniesieniu do poszczególnych certyfikatów SSL.

3.9.3.1.4.1 Szyfrowana komunikacja SSL

Jeśli system jest skonfigurowany tak, by korzystać ze skanowania protokołu SSL, okno dialogowe z monitem o wybranie działania wyświetlane jest w dwóch sytuacjach:

Pierwsza z nich to sytuacja, gdy na stronie internetowej używany jest nieweryfikowalny lub nieprawidłowy certyfikat, a program ESET Endpoint Security skonfigurowany jest tak, by pytać użytkownika w takich przypadkach (domyślne ustawienia to „tak” dla certyfikatów nieweryfikowalnych i „nie” dla nieprawidłowych). W oknie dialogowym wyświetlane jest wówczas pytanie, czy **zezwolić** na połączenie, czy je **zablokować**.

Druga z nich to sytuacja, gdy w obszarze **Tryb ochrony protokołu SSL** ustawiony jest **tryb interaktywny**. Wówczas dla każdej strony internetowej wyświetlane jest okno dialogowe z pytaniem, czy **skanować** ruch sieciowy, czy go **ignorować**. Niektóre aplikacje sprawdzają, czy ich ruch SSL nie jest przez kogoś modyfikowany lub sprawdzany. W takich sytuacjach program ESET Endpoint Security musi **ignorować** ruch sieciowy, by umożliwić dalsze działanie aplikacji.

W obu przypadkach użytkownik może zaznaczyć opcję zapamiętania wybranych działań. Zapisane działania są przechowywane na **Liście znanych certyfikatów**.

3.9.3.1.4.2 Lista znanych certyfikatów

Lista znanych certyfikatów może posłużyć do dostosowania zachowania programu ESET Endpoint Security do określonych certyfikatów SSL, a także do zapamiętania wybieranych czynności, jeśli w obszarze **Tryb filtrowania protokołu SSL/TLS** jest wybrana opcja **Tryb Interaktywny**. Listę tę można wyświetlać i edytować w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **SSL/TLS** > **Lista znanych certyfikatów**.

Okno **Lista znanych certyfikatów** obejmuje następujące elementy:

Kolumny

Nazwa — nazwa certyfikatu.

Wystawca certyfikatu — nazwa podmiotu, który utworzył certyfikat.

Podmiot certyfikatu — pole podmiotu służy do identyfikacji podmiotu związanego z kluczem publicznym przechowywanym w polu podmiotu klucza publicznego.

Dostęp — w celu zezwolenia/zablokowania komunikacji zabezpieczanej przez ten certyfikat bez względu na to, czy jest zaufana należy użyć opcji **Zezwól** lub **Blokuj** w pozycji **Czynność dostępu**. Aby zezwolić na stosowanie zaufanych certyfikatów i aby pytać o niezaufane, należy wybrać opcję **Automatycznie**. Aby program zawsze pytał o czynności użytkownika, należy wybrać opcję **Pytaj**.

Skanuj — w celu skanowania lub ignorowania komunikacji zabezpieczanej przez ten certyfikat należy użyć opcji **Skanuj** lub **Ignoruj** w obszarze **Czynność skanowania**. Wybranie opcji **Automatycznie** umożliwia skanowanie w trybie automatycznym oraz pytanie w trybie interaktywnym. Aby program zawsze pytał o czynności użytkownika, należy wybrać opcję **Pytaj**.

Elementy sterujące

Dodaj — certyfikat można załadować ręcznie w postaci pliku o rozszerzeniu *.cer*, *.crt* lub *.pem*. Aby przesłać lokalny certyfikat, należy kliknąć opcję Plik, Aby określić lokalizację certyfikatu w Internecie, należy kliknąć opcję **Adres URL**.

Edytuj — należy wybrać certyfikat do skonfigurowania i kliknąć opcję **Edytuj**.

Usuń — należy wybrać certyfikat do usunięcia i kliknąć opcję **Usuń**.

OK/Cancel — aby zapisać zmiany, należy kliknąć opcję **OK**. Aby wyjść bez zapisywania, należy kliknąć opcję **Anuluj**.

3.9.3.2 Ochrona programów poczty e-mail

3.9.3.2.1 Programy poczty e-mail

Integracja programu ESET Endpoint Security z programami pocztowymi zwiększa poziom aktywnej ochrony przed szkodliwym kodem rozsyłanym w wiadomościach e-mail. Jeśli dany program pocztowy jest obsługiwany, można włączyć funkcję integracji w programie ESET Endpoint Security. Po jej aktywowaniu pasek narzędzi programu ESET Endpoint Security jest wstawiany bezpośrednio do programu poczty e-mail (w nowszych wersjach programu Windows Live Mail pasek nie jest wstawiany), umożliwiając skuteczniejszą ochronę poczty. Ustawienia integracji można znaleźć w obszarze **Ustawienia** > **Ustawienia zaawansowane** > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Programy poczty e-mail**.

Integracja z programami poczty e-mail

Do obsługiwanych obecnie programów poczty e-mail należą: Microsoft Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. Ochrona poczty e-mail działa na zasadzie wtyczki do tych programów. Główną zaletą wtyczki jest fakt, że jej działanie jest niezależne od używanego protokołu. Gdy program poczty e-mail odbierze zaszyfrowaną wiadomość, następuje jej odszyfrowanie i przesłanie do skanera antywirusowego. Pełna lista obsługiwanych programów poczty e-mail i ich wersji znajduje się w następującym artykule w bazie wiedzy firmy ESET.

Nawet gdy integracja nie jest włączona, komunikacja za pośrednictwem poczty e-mail jest chroniona przez moduł

ochrony programów poczty e-mail (POP3, IMAP).

Jeśli podczas pracy z programem poczty e-mail system działa wolniej niż zwykle, można włączyć opcję **Wyłącz sprawdzanie po zmianie zawartości skrzynki odbiorczej**. Taka sytuacja może mieć miejsce podczas pobierania poczty e-mail z pliku Kerio Outlook Connector Store.

Skanowane wiadomości

Włącz ochronę poczty e-mail przez wtyczki klienckie — w przypadku wyłączenia ochrony programów poczty e-mail przez program poczty e-mail sprawdzanie programów poczty e-mail przez filtrowanie protokołów pozostanie włączone.
Wiadomości odbierane — umożliwia włączanie i wyłączanie sprawdzania odbieranych wiadomości.
Wiadomości wysyłane — umożliwia włączanie i wyłączanie sprawdzania wysyłanych wiadomości.
Wiadomości przeczytane — umożliwia włączanie i wyłączanie sprawdzania przeczytanych wiadomości.

Czynność wykonywana dla zainfekowanej wiadomości

Brak czynności — zaznaczenie tej opcji powoduje, że program będzie wykrywał zainfekowane załączniki, ale nie będzie podejmował żadnych działań.
Usuń wiadomość — program powiadomi użytkownika o infekcji i usunie wiadomość.
Przenieś wiadomość do folderu Elementy usunięte — zainfekowane wiadomości będą automatycznie przenoszone do folderu Elementy usunięte.
Przenieś wiadomość do folderu — zainfekowane wiadomości będą automatycznie przenoszone do wskazanego folderu.

Folder — możliwość wskazania niestandardowego folderu, do którego mają trafiać po wykryciu zainfekowane wiadomości e-mail.

Powtórz skanowanie po aktualizacji — umożliwia włączanie i wyłączanie ponownego skanowania wiadomości po dokonaniu aktualizacji bazy sygnatur wirusów.

Akceptuj wyniki skanowania z innych modułów — zaznaczenie tej opcji powoduje, że moduł ochrony poczty e-mail uwzględnia wyniki skanowania przeprowadzonego przez inne moduły ochrony (skanowanie za pośrednictwem protokołów POP3 oraz IMAP).

UWAGA: zalecamy włączenie opcji **Włącz ochronę poczty e-mail przez wtyczki klienckie** oraz **Włącz ochronę poczty e-mail przez filtrowanie protokołów**.

3.9.3.2.2 Protokoły poczty e-mail

Protokoły IMAP i POP3 to najbardziej rozpowszechnione protokoły używane do obsługi komunikacji przychodzącej w aplikacjach klienckich do obsługi poczty e-mail. Program ESET Endpoint Security zapewnia ochronę w ramach tych protokołów, niezależnie od tego, jaki program poczty e-mail jest w użyciu i nie jest wymagane przeprowadzenie ponownej konfiguracji programu poczty e-mail.

Sprawdzanie protokołów IMAP/IMAPS oraz POP3/POP3S można skonfigurować w obszarze Ustawienia zaawansowane. Dostęp do tego ustawienia można uzyskać po rozwinięciu pozycji **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Protokoły poczty e-mail**.

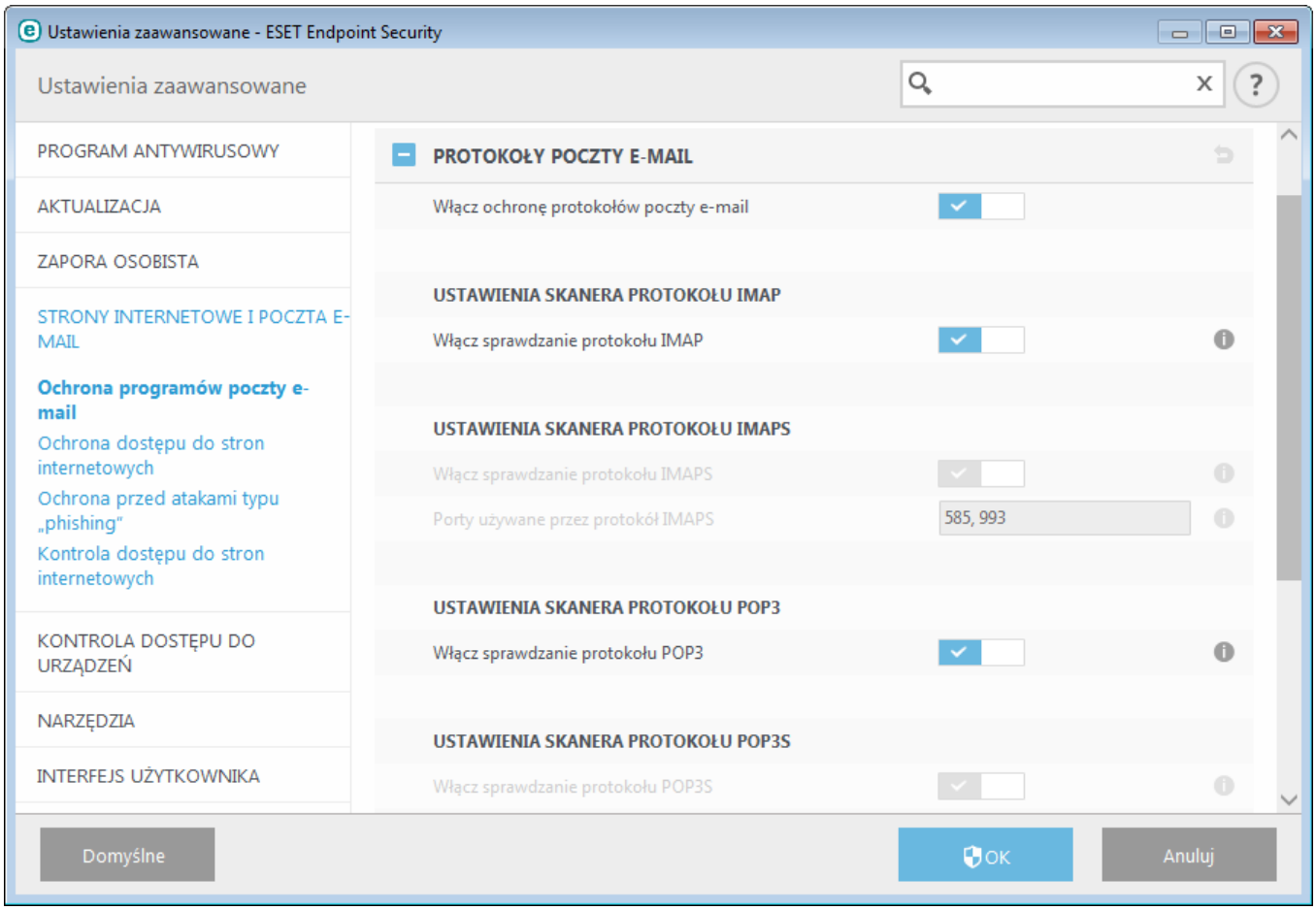
Włącz ochronę protokołów poczty e-mail — umożliwia sprawdzanie protokołów poczty e-mail.

W systemie Windows Vista oraz nowszych protokoły IMAP i POP3 są automatycznie wykrywane i skanowane na wszystkich portach. W systemie Windows XP dla wszystkich aplikacji skanowane są tylko porty skonfigurowane w obszarze **Porty używane przez protokół IMAP/POP3**, natomiast w przypadku aplikacji oznaczonych jako Przeglądarki internetowe i programy poczty e-mail skanowane są wszystkie porty.

Program ESET Endpoint Security obsługuje również skanowanie protokołów IMAPS i POP3S, korzystających z szyfrowanego kanału przy przesyłaniu danych pomiędzy serwerem a klientem. Program ESET Endpoint Security sprawdza komunikację przy użyciu protokołów SSL (Secure Socket Layer) oraz TLS (Transport Layer Security). W programie skanowany jest wyłącznie ruch w portach zdefiniowanych w obszarze **Porty używane przez protokół IMAPS/POP3S**, niezależnie od wersji systemu operacyjnego.

Komunikacja szyfrowana nie podlega skanowaniu, gdy stosowane są ustawienia domyślne. Aby włączyć skanowanie

komunikacji szyfrowanej, należy przejść do opcji SSL/TLS w obszarze Ustawienia zaawansowane, kliknąć kolejno opcje **Strony internetowe i poczta e-mail** > **SSL/TLS** i wybrać opcję **Włącz filtrowanie protokołu SSL/TLS**.



3.9.3.2.3 Alerty i powiadomienia

W ramach ochrony poczty e-mail sprawdzana jest komunikacja przychodząca za pośrednictwem protokołów POP3 oraz IMAP. Przy użyciu wtyczki do programu Microsoft Outlook i innych programów poczty e-mail oprogramowanie ESET Endpoint Security sprawdza całą komunikację realizowaną przez dany program pocztowy (za pośrednictwem protokołów POP3, MAPI, IMAP oraz HTTP). Podczas analizowania wiadomości przychodzących program stosuje wszystkie zaawansowane metody skanowania dostępne w ramach technologii ThreatSense. Dzięki temu szkodliwe programy są wykrywane nawet zanim zostaną porównane z bazą danych sygnatur wirusów. Skanowanie komunikacji za pośrednictwem protokołów POP3 oraz IMAP odbywa się niezależnie od użytkowanego klienta poczty e-mail.

Ustawienia tej funkcji są dostępne w obszarze **Ustawienia zaawansowane** po wybraniu kolejno pozycji **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Alerty i powiadomienia**.

Ustawienia parametrów technologii ThreatSense — zaawansowane ustawienia skanera antywirusowego pozwalające określić skanowane elementy, metody wykrywania zagrożeń itd. Kliknięcie tej opcji umożliwia wyświetlenie okna ze szczegółowymi ustawieniami skanera antywirusowego.

Po sprawdzeniu wiadomości e-mail może do niej zostać dołączone powiadomienie o wynikach skanowania. Można wybrać spośród opcji **Oznacz otrzymaną i przeczytaną wiadomość e-mail, Dołącz notatkę do tematu otrzymanej i przeczytanej zainfekowanej wiadomości** oraz **Oznacz wysyłaną wiadomość e-mail**. Należy pamiętać, że w rzadkich przypadkach, takie powiadomienia mogą być pomijane w przypadku kłopotliwych wiadomości w formacie HTML lub wiadomości fałszowanych przez szkodliwe oprogramowanie. Powiadomienia mogą być dodawane do wszystkich odebranych i przeczytanych wiadomości oraz do wysyłanych wiadomości. Dostępne opcje:

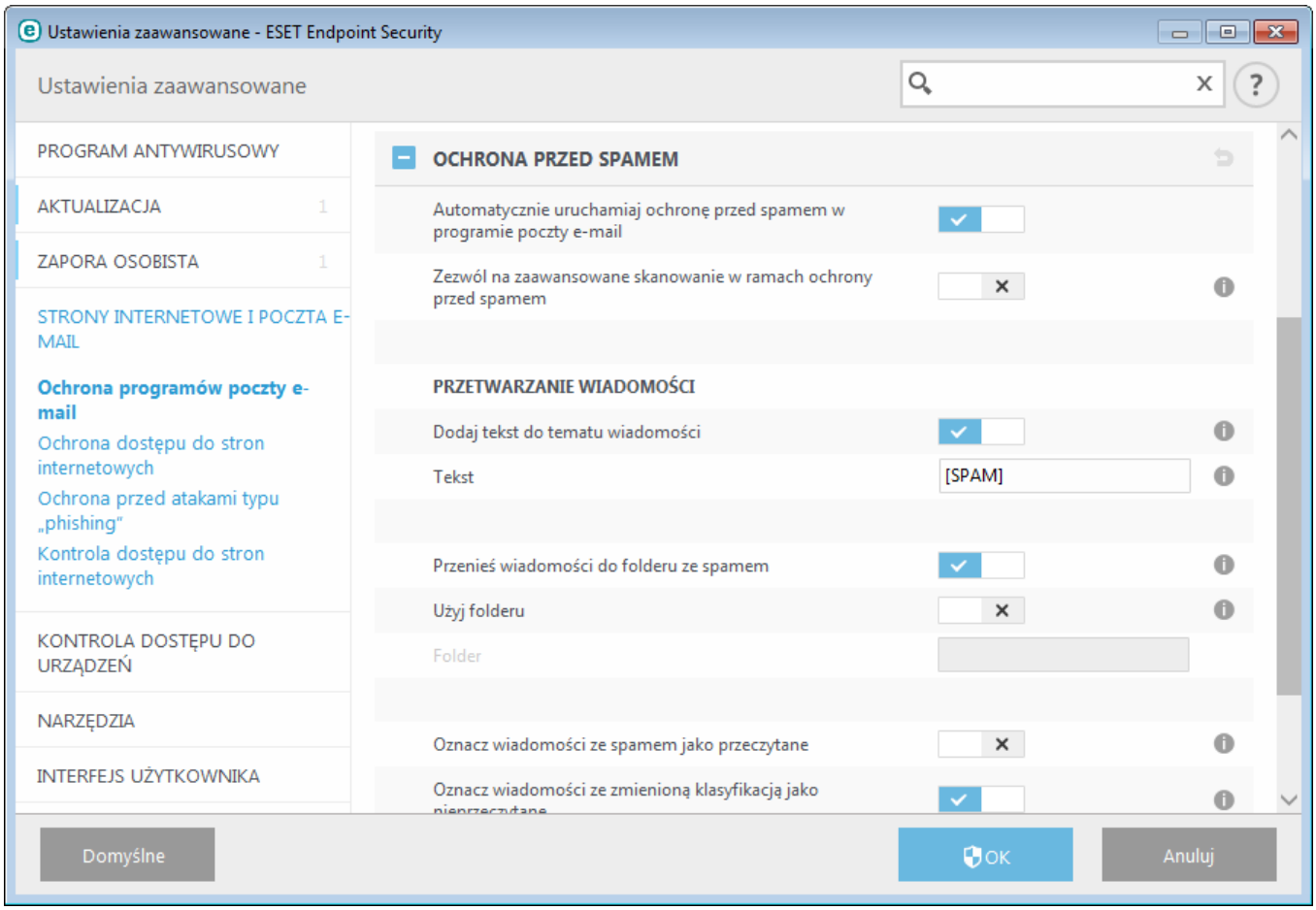
- **Nigdy** — powiadomienia w ogóle nie będą dodawane.
- **Tylko zainfekowane wiadomości** — oznaczane będą tylko wiadomości zawierające szkodliwe oprogramowanie (ustawienie domyślne.
- **Cała poczta** — program będzie dołączać powiadomienia do wszystkich przeskanowanych wiadomości e-mail.

Dołącz notatkę do tematu wysyłanej zainfekowanej wiadomości — należy wyłączyć tę opcję, aby funkcja ochrony poczty e-mail nie umieszczała w temacie zainfekowanej wiadomości ostrzeżenia o wirusie. Ta opcja umożliwia później proste odfiltrowanie zainfekowanych wiadomości na podstawie analizy ich tematów (o ile program pocztowy udostępnia taką funkcję). Zwiększa ona też wiarygodność wiadomości dla odbiorcy, a w przypadku wykrycia zagrożenia udostępnia cenne informacje na temat poziomu zagrożenia, jakie stanowi dana wiadomość lub jej nadawca.

Szablon komunikatu dołączanego do tematu zainfekowanej wiadomości — edytowanie tego szablonu pozwala zmodyfikować format przedrostka tematu zainfekowanej wiadomości e-mail. Korzystając z tej funkcji można zastąpić temat wiadomości *„Witaj”* podanym przedrostkiem *„[wirus]”* w następującym formacie: *„[wirus] Witaj”*. Zmienna *%NAZWA_WIRUSA%* zawiera nazwę wykrytego zagrożenia.

3.9.3.2.4 Ochrona przed spamem

Niepożądana poczta e-mail — spam — to jeden z najpoważniejszych problemów komunikacji elektronicznej. Spam stanowi obecnie aż 80% wszystkich wysyłanych wiadomości e-mail. Ochrona przed spamem służy jako rozwiązanie zabezpieczające przed tym problemem. Wysoką wydajność filtrowania przez moduł antyspamowy przeciwdziałający zainfekowaniu poczty osiągnięto dzięki połączeniu kilku metod zabezpieczania poczty e-mail.



Jedną z istotnych zasad stosowanych w celu wykrywania spamu jest możliwość identyfikacji niepożądanej poczty e-mail na podstawie wstępnie zdefiniowanych zaufanych adresów (białej listy) i adresów kojarzonych ze spamem (czarnej listy). Wszystkie adresy z listy kontaktów użytkownika są automatycznie dodawane do białej listy. Dodawane są również wszystkie inne adresy, które użytkownik oznaczył jako bezpieczne.

Główną metodą wykrywania spamu jest skanowanie właściwości wiadomości e-mail. Odebrane wiadomości są skanowane pod kątem podstawowych kryteriów antyspamowych (z zastosowaniem definicji wiadomości, heurystyki statystycznej, algorytmów rozpoznawania oraz innych unikalnych metod) i na podstawie obliczonej wartości wskaźnika klasyfikowane jako będące lub niebędące spamem.

Automatycznie uruchamiaj ochronę przed spamem w programie poczty e-mail - po włączeniu tej opcji funkcja ochrony przed spamem będzie automatycznie uaktywniana podczas uruchamiania komputera.

Zezwól na zaawansowane skanowanie w ramach ochrony przed spamem — powoduje okresowe pobieranie

dodatkowych danych antyspamowych, co rozszerza możliwości ochrony przed spamem i prowadzi do uzyskania lepszych wyników.

Ochrona antyspamowa w programie ESET Endpoint Security umożliwia skonfigurowanie różnych ustawień związanych z obsługą list adresowych. Dostępne są następujące opcje:

Przetwarzanie wiadomości

Dodaj tekst do tematu wiadomości — umożliwia dodawanie niestandardowego tekstu na początku wiersza tematu wiadomości zaklasyfikowanej jako spam. Domyślnie jest to ciąg „[SPAM]”.

Przenieś wiadomości do folderu ze spamem — gdy ta opcja jest włączona, wiadomości ze spamem są przenoszone do domyślnego folderu na niepożądane wiadomości, natomiast wiadomości z klasyfikacją zmienioną na inną niż spam są przenoszone do skrzynki odbiorczej. Po kliknięciu wiadomości e-mail prawym przyciskiem myszy i wybraniu pozycji ESET Endpoint Security z menu kontekstowego użytkownik może wybrać jedną z dostępnych opcji.

Użyj folderu — ta opcja powoduje przenoszenie spamu do folderu wskazanego przez użytkownika.

Oznacz wiadomości zawierające spam jako przeczytane — włączenie tej opcji powoduje automatyczne oznaczanie wiadomości ze spamem jako przeczytanych. Pozwala to skupić uwagę jedynie na pożądanych wiadomościach.

Oznacz wiadomość ze zmienioną klasyfikacją jako nieprzeczytaną — wiadomości pierwotnie uznane za spam, a następnie przekwalifikowane na pożądane będą wyświetlane jako wiadomości nieprzeczytane.

Zapisywanie w dzienniku wyniku spamu — mechanizm antyspamowy programu ESET Endpoint Security przypisuje każdej przeskanowanej wiadomości wynik spamu. Wiadomość zostanie zarejestrowana w dzienniku ochrony przed spamem (**ESET Endpoint Security** > **Narzędzia** > **Pliki dziennika** > **Ochrona przed spamem**).

- **Brak** — wynik skanowania w poszukiwaniu spamu nie zostanie zapisany w dzienniku.
- **Klasyfikacja zmieniona przez użytkownika na spam** — ta opcja umożliwia zarejestrowanie wyniku spamu dla wiadomości oznaczonych jako SPAM.
- **Wszystkie** — wszystkie wiadomości będą rejestrowane w dzienniku razem z wynikiem spamu.

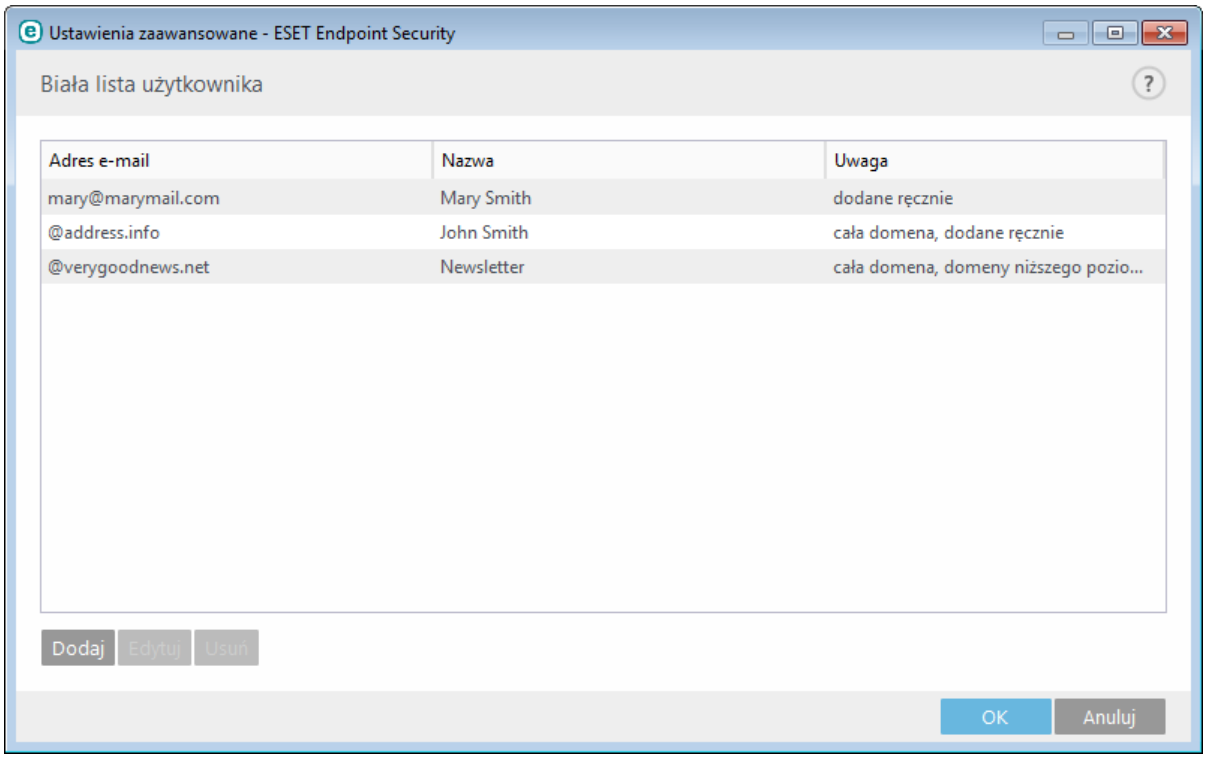
UWAGA: Po kliknięciu wiadomości w folderze na niepożądane wiadomości e-mail można wybrać opcję **Zmień klasyfikację wybranych wiadomości na pożądane wiadomości**, co spowoduje przeniesienie wiadomości do skrzynki odbiorczej. Po kliknięciu w skrzynce odbiorczej wiadomości uznanej za spam można wybrać opcję **Zmień klasyfikację wiadomości na spam**, co spowoduje przeniesienie wiadomości do folderu na niepożądane wiadomości e-mail. Można zaznaczyć kilka wiadomości i wykonać tę czynność w odniesieniu do nich wszystkich równocześnie.

UWAGA: Program ESET Endpoint Security umożliwia ochronę przed spamem w programach Microsoft Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.

3.9.3.2.4.1 Czarna lista/biała lista/lista wyłączeń

W celu zapewnienia ochrony przed niechcianą pocztą w programie ESET Endpoint Security można klasyfikować adresy e-mail przy użyciu specjalnych list. Biała lista zawiera adresy e-mail uznawane za bezpieczne. Wiadomości od użytkowników z białej listy są zawsze dostępne w folderze poczty przychodzącej. Czarna lista zawiera adresy zaklasyfikowane jako adresy, z których wysyłany jest spam. Oznacza to, że wszystkie wiadomości pochodzące od nadawców z tej listy będą oznaczane jako spam. Na liście wyłączeń mogą znajdować się adresy e-mail zawsze sprawdzane pod kątem spamu, jak również adresy z niepożądanych wiadomości e-mail, które początkowo mogły nie zostać rozpoznane jako spam.

Wszystkie listy można edytować w głównym oknie programu ESET Endpoint Security po wybraniu opcji **Ustawienia zaawansowane** > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Książki adresowe ochrony przed spamem**. Służą do tego przyciski Dodaj, Edytuj i Usuń dostępne w oknie dialogowym każdej z list. Można też wybrać opcję **Ustawienia** > **Strony internetowe i poczta e-mail** po kliknięciu ikony koła zębatego widocznej obok pozycji **Ochrona przed spamem**.



Domyślnie program ESET Endpoint Security dodaje do białej listy wszystkie adresy z książek adresowych obsługiwanych programów poczty e-mail. Czarna lista jest domyślnie pusta. Lista wyłączeń zawiera domyślnie tylko własne adresy e-mail użytkownika.

3.9.3.2.4.2 Dodawanie adresów do białej i czarnej listy

Adresy e-mail osób, z którymi użytkownik często się komunikuje można dodać do białej listy. Zagwarantuje to, że żadna wiadomość pochodząca z takiego adresu nie zostanie nigdy sklasyfikowana jako spam. Znane adresy kojarzone ze spamem mogą zostać dodane do czarnej listy, co spowoduje, że zawsze będą klasyfikowane jako spam. Aby dodać nowy adres do białej lub czarnej listy, należy kliknąć prawym przyciskiem myszy wiadomość e-mail i wybrać opcję **ESET Endpoint Security** > **Dodaj do białej listy** lub **Dodaj do czarnej listy** albo kliknąć przycisk **Adres zaufany** lub **Adres spamu** na pasku narzędzi modułu antyspamowego programu ESET Endpoint Security w programie poczty e-mail.

Podobnie tą samą procedurę stosuje się w przypadku adresów kojarzonych ze spamem. Jeśli dany adres e-mail znajduje się na czarnej liście, każda przysłana z niego wiadomość jest klasyfikowana jako spam.

3.9.3.2.4.3 Oznaczanie wiadomości jako spam lub pożądane wiadomości

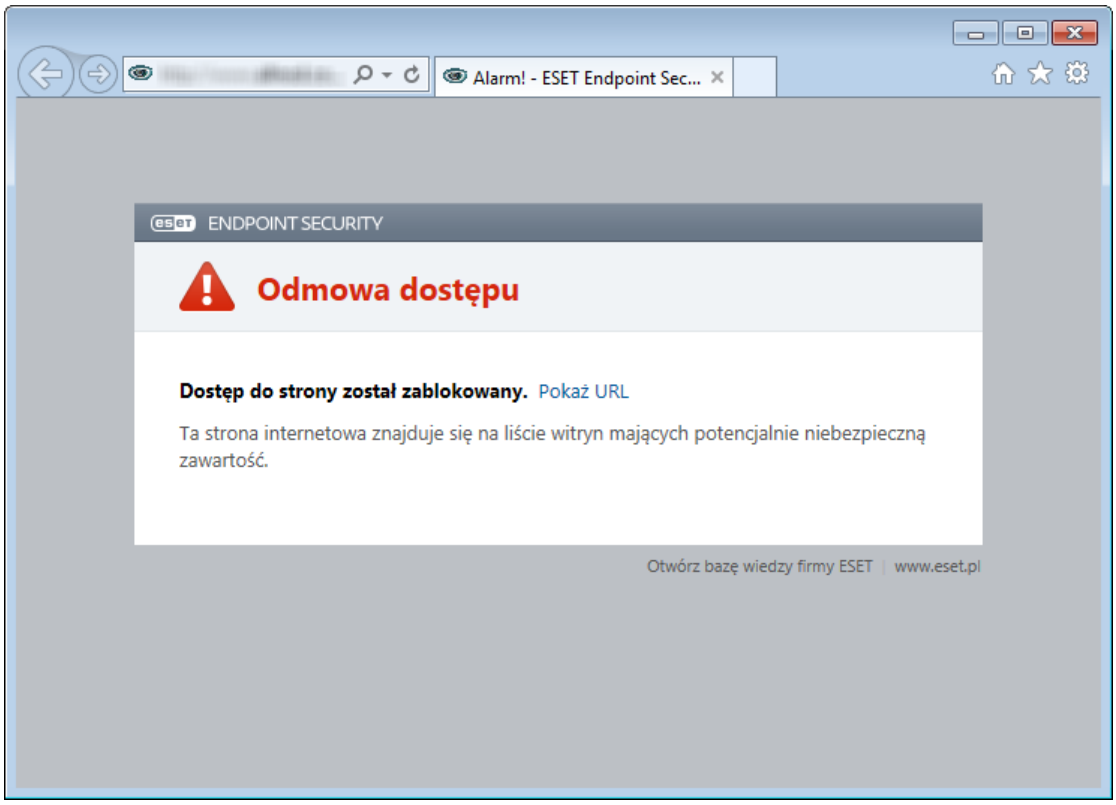
Dowolną wiadomość wyświetloną w programie poczty e-mail można oznaczyć jako spam. W tym celu należy kliknąć prawym przyciskiem myszy wybraną wiadomość, a następnie kliknąć kolejno opcje **ESET Endpoint Security** > **Zmień klasyfikację wybranych wiadomości na spam** lub kliknąć przycisk **Spam** na pasku narzędzi modułu antyspamowego programu ESET Endpoint Security, umieszczonym w górnej części okna programu poczty e-mail.

Wiadomości ze zmienioną klasyfikacją są automatycznie przenoszone do folderu ze spamem, ale adresy e-mail ich nadawców nie są dodawane do **czarnej listy**. W podobny sposób można oznaczać wiadomości jako „nie-spam”, klikając kolejno opcje **ESET Endpoint Security** > **Zmień klasyfikację wybranych wiadomości na pożądane wiadomości** lub klikając opcję **Pożądana wiadomość** na pasku narzędzi modułu antyspamowego programu ESET Endpoint Security, umieszczonym w górnej części okna programu poczty e-mail. Jeśli wiadomości z folderu **Wiadomości-śmieci** zostaną sklasyfikowane jako niebędące spamem, zostaną przeniesione do folderu **Skrzynka odbiorcza**. Oznaczenie wiadomości jako pożądanej powoduje automatyczne dodanie adresu jej nadawcy do **białej listy**.

3.9.3.3 Ochrona dostępu do stron internetowych

Obsługa komunikacji przez Internet jest standardową funkcją w większości komputerów osobistych. Niestety komunikacja internetowa stała się głównym sposobem przenoszenia szkodliwego kodu. Ochrona dostępu do stron internetowych polega na monitorowaniu realizowanej między przeglądarkami internetowymi i zdalnymi serwerami komunikacji zgodnej z regułami protokołów HTTP (ang. Hypertext Transfer Protocol) i HTTPS (komunikacja szyfrowana).

Dostęp do stron internetowych, o których wiadomo, że zawierają szkodliwe treści jest blokowany zanim zawartość zostanie pobrana. Wszystkie pozostałe strony internetowe są skanowane przy użyciu technologii skanowania ThreatSense podczas ładowania i zostają zablokowane w przypadku wykrycia szkodliwej zawartości. Funkcja Ochrona dostępu do stron internetowych obejmuje dwa poziomy ochrony — blokowanie na podstawie czarnej listy oraz blokowanie na podstawie zawartości.



Stanowczo zalecane jest, aby ochrona dostępu do stron internetowych była włączona. Dostęp do tej opcji można uzyskać w głównym oknie programu ESET Endpoint Security, po wybraniu kolejno pozycji **Ustawienia** > **Strony internetowe i poczta e-mail** > **Ochrona dostępu do stron internetowych**.

W obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona dostępu do stron internetowych** dostępne są następujące opcje:

- **Protokoły sieciowe** — możliwość skonfigurowania monitorowania w odniesieniu do protokołów standardowych, które są używane w większości przeglądarek internetowych.
- **Zarządzanie adresami URL** — możliwość wskazania adresów HTTP, które mają być blokowane, dozwolone lub wyłączone ze sprawdzania.
- **Ustawienia parametrów technologii ThreatSense** — zaawansowane ustawienia skanera antywirusowego umożliwiające skonfigurowanie takich ustawień, jak typy skanowanych obiektów (np. wiadomości e-mail, archiwa), metody wykrywania zagrożeń związanych z dostępem do stron internetowych itp.

3.9.3.3.1 Protokoły sieciowe

W programie ESET Endpoint Security domyślnie skonfigurowano monitorowanie protokołu HTTP używanego w większości przeglądarek internetowych.

W systemie Windows Vista i nowszych ruch sieciowy HTTP jest monitorowany zawsze, na wszystkich portach i w odniesieniu do wszystkich aplikacji. W systemie Windows XP można modyfikować opcję **Porty używane przez protokół HTTP** w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona dostępu do stron internetowych** > **Protokoły sieciowe** > **Ustawienia skanera protokołu HTTP**. Ruch sieciowy HTTP jest monitorowany na wskazanych portach w odniesieniu do wszystkich aplikacji oraz na wszystkich portach w przypadku aplikacji oznaczonych jako Przeglądarki internetowe i programy poczty e-mail.

Program ESET Endpoint Security obsługuje również sprawdzanie protokołu HTTPS. W przypadku komunikacji za pośrednictwem protokołu HTTPS informacje między serwerem a klientem przesyłane są przez kanał szyfrowany. Program ESET Endpoint Security sprawdza połączenia, używając protokołów SSL (Secure Socket Layer) i TLS (Transport Layer Security). W programie skanowany jest wyłącznie ruch w portach zdefiniowanych w obszarze **Porty używane przez protokół HTTPS**, niezależnie od wersji systemu operacyjnego.

Komunikacja szyfrowana nie podlega skanowaniu, gdy stosowane są ustawienia domyślne. Aby włączyć skanowanie komunikacji szyfrowanej, należy przejść do opcji SSL/TLS w obszarze Ustawienia zaawansowane, kliknąć kolejno opcje **Strony internetowe i poczta e-mail** > **SSL/TLS** i wybrać opcję **Włącz filtrowanie protokołu SSL/TLS**.

3.9.3.3.2 Zarządzanie adresami URL

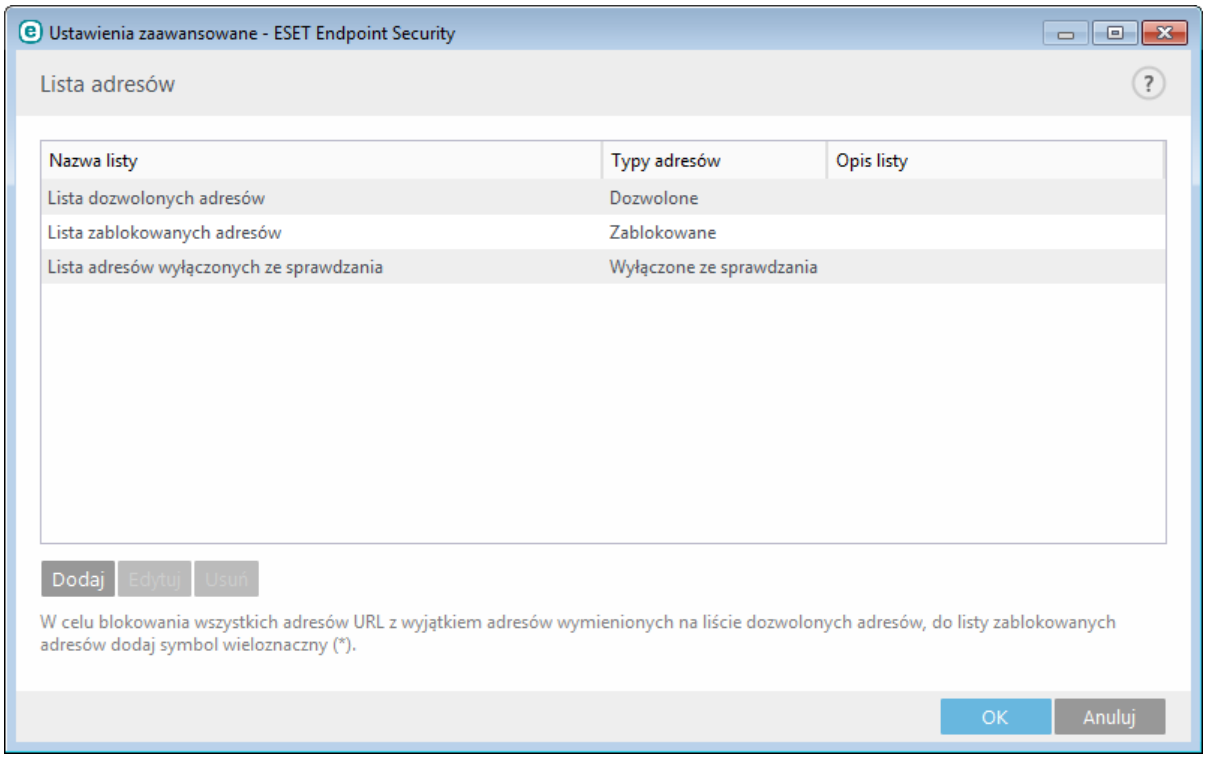
W sekcji Zarządzanie adresami URL możliwe jest wskazanie adresów HTTP, które mają być blokowane, dozwolone lub wyłączone ze sprawdzania.

Strony internetowe wyszczególnione na **Liście zablokowanych adresów** nie będą dostępne, chyba że zostaną również uwzględnione na **Liście dozwolonych adresów**. Strony internetowe z **Listy adresów wyłączonych ze sprawdzania** nie są poddawane skanowaniu w poszukiwaniu szkodliwego kodu w momencie uzyskiwania do nich dostępu.

Jeśli oprócz filtrowania stron internetowych HTTP mają być również filtrowane adresy HTTPS, należy wybrać opcję **Włącz filtrowanie protokołu SSL**. W przeciwnym razie dodane zostaną tylko domeny HTTPS, które już były odwiedzane, a nie pełny adres URL.

Na wszystkich listach można używać symboli specjalnych: * (gwiazdka) i ? (znak zapytania). Gwiazdka zastępuje dowolną liczbę znaków, natomiast znak zapytania oznacza jeden znak. Szczególną ostrożność należy zachować podczas określania adresów wyłączonych, ponieważ ta lista powinna zawierać jedynie adresy zaufane i bezpieczne. Ponadto należy sprawdzić, czy symbole * oraz ? są na tej liście stosowane prawidłowo. Informacje na temat bezpiecznego uwzględnienia domeny wraz ze wszystkimi domenami podrzędnymi można znaleźć w sekcji Dodawanie adresu HTTP lub maski domeny. Aby uaktywnić listę, należy włączyć opcję **Lista aktywna**. Aby otrzymywać powiadomienia podczas wprowadzania adresu z bieżącej listy, należy włączyć opcję **Powiadom o zastosowaniu**.

Jeśli blokowane mają być wszystkie adresy HTTP z wyjątkiem adresów wyszczególnionych na aktywnej **Liście dozwolonych adresów**, należy dodać symbol * do aktywnej **Listy zablokowanych adresów**.



Dodaj — utworzenie nowej listy, stanowiącej dodatek do list wstępnie zdefiniowanych. Ta opcja może okazać się przydatna, gdy użytkownik chce w sposób logiczny podzielić różne grupy adresów. Na przykład jedna lista zablokowanych adresów może zawierać adresy z zewnętrznej czarnej listy publicznej, natomiast druga lista może obejmować własną czarną listę użytkownika, co ułatwi uaktualnianie listy zewnętrznej bez ingerowania w listę użytkownika.

Edytuj — modyfikowanie istniejących list. Ta opcja umożliwia dodawanie oraz usuwanie adresów z list.

Usuń — usunięcie istniejącej listy. Opcja dostępna wyłącznie w przypadku list utworzony przy użyciu przycisku **Dodaj** — niedostępna dla list domyślnych.

3.9.3.4 Ochrona przed atakami typu „phishing”

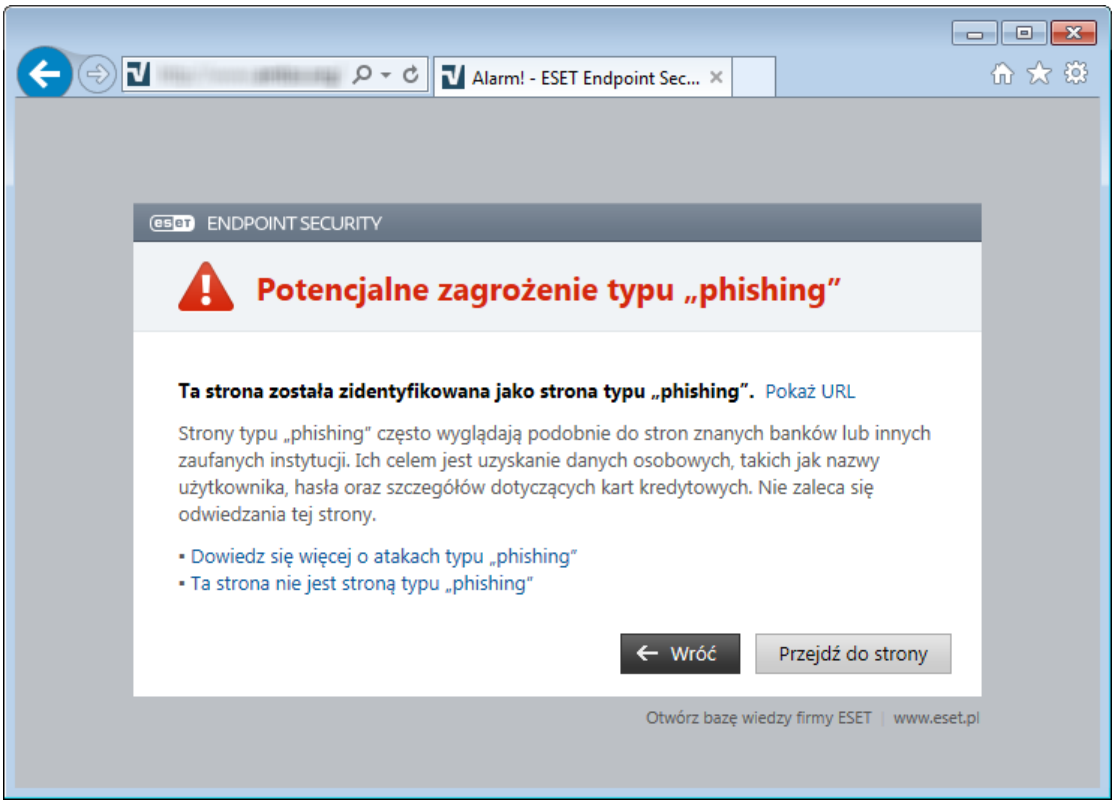
Terminem „phishing” określa się działania przestępcze, w których są stosowane socjotechniki (manipulowanie użytkownikami w celu uzyskania poufnych informacji). Działania takie są podejmowane z myślą o uzyskaniu dostępu do prywatnych danych, np. numerów kont bankowych, kodów PIN itp. Więcej informacji o tych działaniach znajduje się w słowniczku. Program ESET Endpoint Security chroni komputer przed atakami typu „phishing”, blokując strony internetowe znane z rozpowszechniania takich treści.

Zdecydowanie zalecamy włączenie ochrony przed atakami typu „phishing” w programie ESET Endpoint Security. W tym celu należy otworzyć **Ustawienia zaawansowane** (klawisz F5) i przejść do opcji **Strony internetowe i poczta e-mail** > **Ochrona przed atakami typu „phishing”**.

Więcej informacji na temat dostępnej w programie ESET Endpoint Security ochrony przed atakami typu „phishing” można znaleźć w tym artykule bazy wiedzy.

Wyświetlanie strony wykorzystywanej w atakach typu phishing

Po przejściu do strony znanej z ataków typu „phishing” w przeglądarce internetowej zostanie wyświetlone następujące okno dialogowe. Aby mimo to otworzyć tę stronę internetową, można kliknąć opcję **Przejdź do strony** (niezalecane).



UWAGA: Dodane do białej listy strony, które potencjalnie mogą być wykorzystywane do ataków typu „phishing”, domyślnie zostaną usunięte z listy po kilku godzinach. Aby zezwolić na dostęp do strony na stałe, należy użyć narzędzia Zarządzanie adresami URL. W obszarze **Ustawienia zaawansowane** (F5) należy kliknąć kolejno opcje **Strony internetowe i poczta e-mail** > **Ochrona dostępu do stron internetowych** > **Zarządzanie adresami URL** > **Lista adresów**, a następnie kliknąć przycisk **Edytuj** i dodać do listy stronę internetową, która ma być edytowana.

Raportowanie stron wykorzystywanych do ataków typu „phishing”

Łącze Zgłoś umożliwia zgłaszanie witryn wykorzystywanych do ataków typu „phishing” oraz szkodliwych witryn do analizy przez firmę ESET.

UWAGA: Przed przesłaniem strony do firmy ESET należy się upewnić, że spełnia ona co najmniej jedno z następujących kryteriów:
- strona nie jest w ogóle wykrywana,
- strona jest błędnie wykrywana jako zagrożenie. W takim przypadku można zgłosić błędną klasyfikację strony jako „phishing”.

Stronę można również przesłać pocztą e-mail. Należy wysłać wiadomość e-mail na adres samples@eset.com. Należy pamiętać o podaniu opisowego tematu wiadomości oraz wszystkich możliwych informacji na temat podejrzanej strony (może to być adres strony internetowej, na której znajduje się adres/łącze do podejrzanej strony, sposób uzyskania informacji o stronie itp.).

3.9.4 Kontrola dostępu do stron internetowych

W sekcji Kontrola dostępu do stron internetowych można skonfigurować ustawienia służące do ochrony firmy przed ryzykiem odpowiedzialności prawnej. Funkcja kontroli dostępu do stron internetowych umożliwia zarządzanie dostępem do stron internetowych stanowiących naruszenie praw własności intelektualnej. Celem tego mechanizmu jest uniemożliwienie pracownikom dostępu do stron zawierających nieodpowiednie lub szkodliwe treści, a także do stron, które mogą negatywnie wpływać na wydajność pracy.

Kontrola dostępu do stron internetowych umożliwia blokowanie stron internetowych, które mogą zawierać obraźliwe materiały. Ponadto pracodawcy oraz administratorzy systemu mogą zablokować dostęp do ponad 27 wstępnie zdefiniowanych kategorii i ponad 140 podkategorii witryn internetowych.

Kontrola dostępu do stron internetowych jest domyślnie wyłączona. W celu włączenia kontroli dostępu do stron internetowych należy nacisnąć klawisz F5, aby przejść do obszaru **Ustawienia zaawansowane** i rozwinąć kolejno pozycje **Strony internetowe i poczta e-mail** > **Kontrola dostępu do stron internetowych**. Wybranie opcji **Zintegruj z**

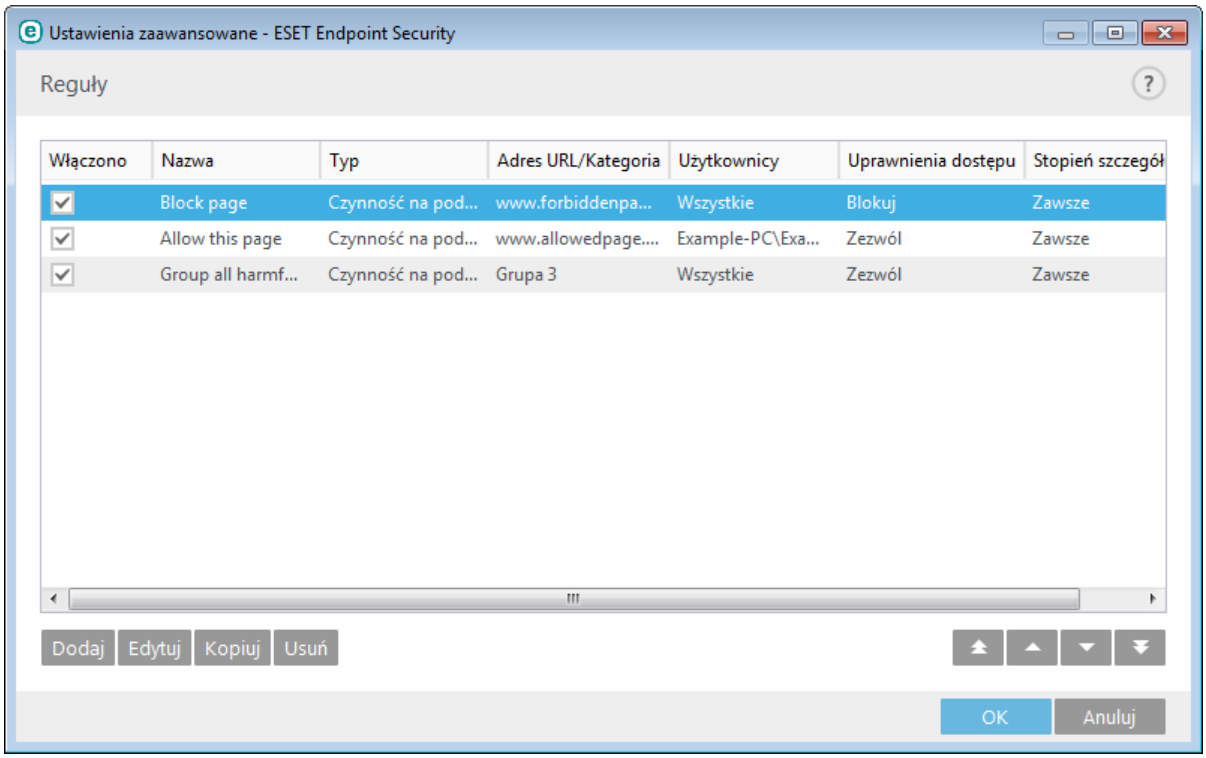
systemem powoduje włączenie Kontroli dostępu do stron internetowych w programie ESET Endpoint Security. Kliknięcie przycisku **Edytuj** obok **reguł** umożliwia dostęp do okna Edytor reguł kontroli dostępu do stron internetowych.

W polach **Komunikat na zablokowanych stronach** i **Grafika na zablokowanych stronach** można z łatwością skonfigurować komunikaty wyświetlane w przypadku zablokowania strony.

PORADA: Oto przykładowy komunikat dotyczący zablokowanej strony internetowej: *Strona internetowa została zablokowana, ponieważ uznano ją za nieodpowiednią lub jej zawartość jest szkodliwa. Skontaktuj się z administratorem w celu uzyskania dodatkowych informacji.* Można też podać tam adres internetowy lub ścieżkę sieciową do obrazu niestandardowego, na przykład *http://test.com/test.jpg*. Wielkość obrazu niestandardowego jest ustawiona automatycznie na wartość 90 x 30. Nieprzygotowane obrazy będą automatycznie dostosowywane do tego rozmiaru.

3.9.4.1 Reguły

W oknie **Edytor reguł** wyświetlane są istniejące reguły działające na podstawie adresu URL lub na podstawie kategorii.



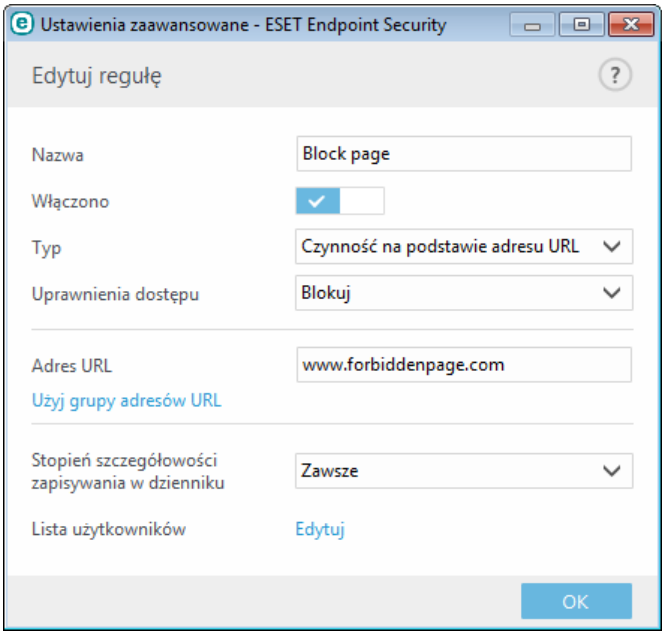
Lista reguł zawiera pewne informacje o regułach, takie jak nazwa, typ blokowania, czynność wykonywana po dopasowaniu reguły kontroli dostępu do stron internetowych i stopień ważności w dzienniku.

Kliknięcie przycisku **Dodaj** lub **Edytuj** umożliwia zarządzanie regułą. Kliknięcie przycisku **Kopiuj** umożliwia utworzenie nowej reguły ze wstępnie zdefiniowanymi opcjami pochodzącymi z innej wybranej reguły. Naciśnięcie klawisza **Ctrl** i kliknięcie poszczególnych pozycji umożliwia zaznaczenie wielu reguł i usunięcie wszystkich zaznaczonych reguł. Pole wyboru **Włączone** pozwala wyłączać i włączać regułę. Jest to użyteczne, gdy użytkownik nie chce trwale usunąć danej reguły, ponieważ może zajść potrzeba zastosowania jej w przyszłości.

Reguły są sortowane według priorytetu, przy czym ważniejsze reguły umieszczone są na górze. Ocena reguł na podstawie adresu URL zawsze uzyskuje wyższy priorytet niż ocena na podstawie kategorii. Jeśli na przykład reguła na podstawie adresu URL znajduje się na liście reguł pod regułą ustaloną na podstawie kategorii, reguła ustalona na podstawie adresu URL ma wyższy priorytet i będzie oceniana jako pierwsza.

3.9.4.1.1 Dodawanie reguł kontroli dostępu do stron internetowych

W oknie Reguły kontroli dostępu do stron internetowych można ręcznie tworzyć i modyfikować istniejące reguły dostępu do stron internetowych.



W celu łatwiejszego rozpoznawania reguł należy wprowadzać ich krótkie opisy w polu **Nazwa**. Klikając przełącznik **Włączone** można wyłączać i włączać regułę. Jest to przydatne, gdy użytkownik nie chce trwale usuwać danej reguły.

Typ czynności

- **Czynność na podstawie adresu URL** — w odniesieniu do reguł kontrolujących dostęp do danej strony internetowej należy wprowadzić adres URL w polu **URL**.
- **Czynność na podstawie kategorii** — po wybraniu tej opcji należy ustawić kategorię czynności przy użyciu menu rozwijanego.

Na liście adresów URL nie można używać symboli specjalnych: * (gwiazdka) oraz ? (znak zapytania). Podczas tworzenia grupy adresów URL, w której znajdują się strony internetowe o wielu domenach najwyższego poziomu, każda z tych domen musi być dodana osobno. W przypadku dodania domeny do grupy cała zawartość umieszczona w tej domenie i wszystkich domenach podrzędnych (np. *sub.przykladowa_strona.com*) będzie zablokowana lub dozwolona zgodnie z wybraną przez użytkownika czynnością na podstawie adresu URL.

Uprawnienia dostępu

- **Zezwól** — dostęp do tego adresu URL/kategorii będzie możliwy.
- **Ostrzeż** — ostrzega o danym adresie URL / kategorii.
- **Blokuj** — blokuje dany adres URL / kategorię.

Adres URL lub **Użyj grupy adresów URL** — umożliwia użycie łącza do adresu URL lub grupy łączy do adresów URL w celu zezwalania, blokowania lub ostrzegania w przypadku wykrycia jednego z tych adresów URL.

Stopień szczegółowości zapisywania w dzienniku:

- **Zawsze** — rejestrowanie całości komunikacji internetowej.
- **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszenia konfiguracji programu.
- **Informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Brak** — nie są tworzone żadne dzienniki.

Lista użytkowników

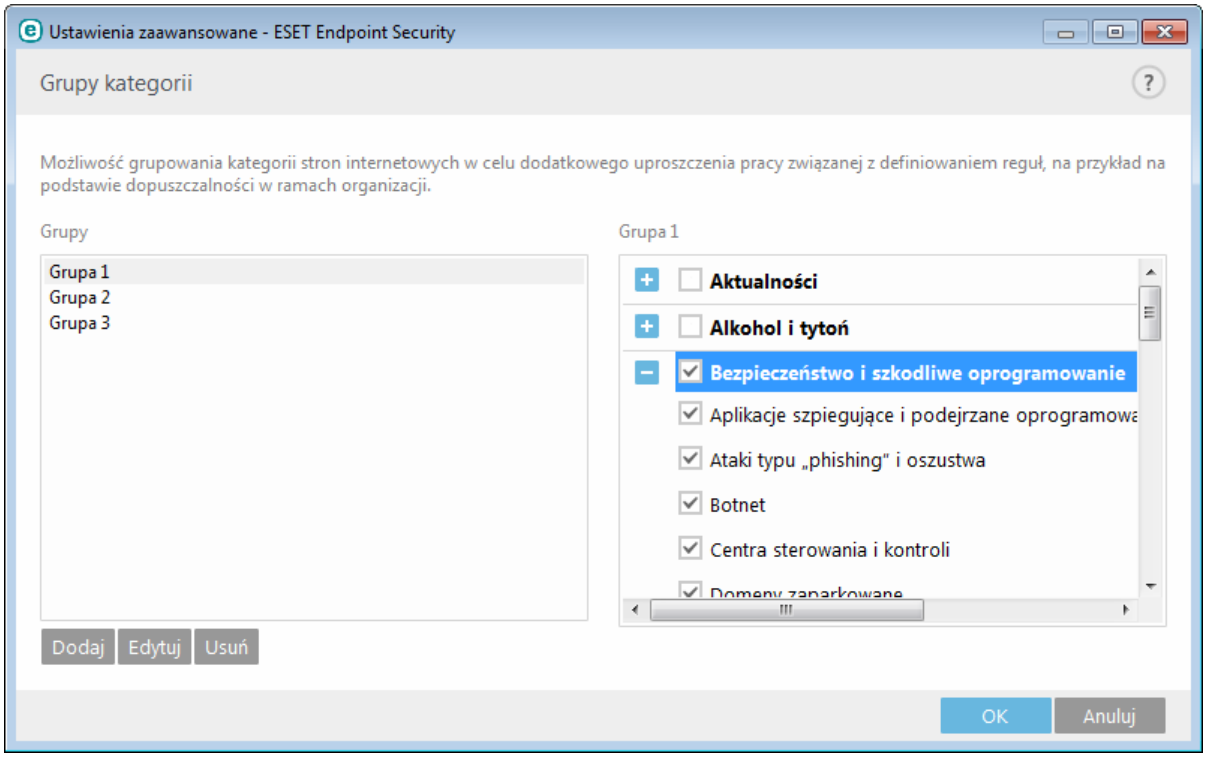
- **Dodaj** — umożliwia otwarcie okna dialogowego **Wybieranie użytkowników lub grup**, w którym można odpowiednich użytkowników. Jeśli nie zostanie wprowadzony żaden użytkownik, reguła będzie stosowana w odniesieniu do wszystkich użytkowników.
- **Usuń** — umożliwia usunięcie wybranego użytkownika z filtru.

3.9.4.2 Grupy kategorii

Okno Grupy kategorii jest podzielone na dwie części. Prawa część okna zawiera listę kategorii i podkategorii. Aby wyświetlić podkategorie danej kategorii, należy ją wybrać na liście Kategoria.

Każda grupa zawiera podkategorie dla dorosłych i/lub z pewnych względów nieodpowiednie, jak również kategorie uznawane za akceptowalne. Po otwarciu okna Grupy kategorii i kliknięciu pierwszej grupy można dodawać kategorie/podkategorie do listy odpowiednich grup (np. Przemoc czy Broń) lub usuwać je z niej. Po utworzeniu reguły ze wstępnie zdefiniowanymi czynnościami strony internetowe zawierające nieodpowiednie treści można blokować lub informować o tym użytkowników.

W celu dodania lub usunięcia podkategorii w ramach określonej grupy należy skorzystać z pola wyboru.



Poniżej podano przykłady kategorii, których użytkownicy mogą nie znać:

Różne — zazwyczaj prywatne (lokalne) adresy IP, na przykład w sieci intranet, 192.168.0.0/16 itp. Po wygenerowaniu kodu błędu 403 lub 404, witryna zostaje również zaliczona do tej kategorii.
Nierozpoznane — ta kategoria obejmuje strony internetowe, które nie zostały rozpoznane z powodu błędu podczas nawiązywania połączenia z aparatem bazy danych kontroli dostępu do stron internetowych.
Niezaliczone do żadnej kategorii — nieznane strony internetowe, które nie znalazły się jeszcze w bazie danych kontroli dostępu do stron internetowych.
Serwery proxy — strony internetowe, np. zapewniające anonimowość, przekierowujące lub publiczne serwery proxy, których można użyć w celu uzyskania (anonimowego) dostępu do stron internetowych zazwyczaj zablokowanych przez filtr kontroli dostępu do stron internetowych.
Udostępnianie plików — te strony internetowe zawierają duże ilości danych, takich jak zdjęcia, nagrania wideo lub e-booki. Te witryny mogą zawierać treści potencjalnie obraźliwe lub przeznaczone dla osób dorosłych.

UWAGA: Dana podkategoria może należeć do dowolnej grupy. Istnieją pewne podkategorie, które nie należą do żadnej ze wstępnie zdefiniowanych grup (na przykład Gry). Aby dopasować żądaną podkategorię za pomocą filtra kontroli dostępu do stron internetowych, należy ją dodać do żądanej grupy.

3.9.4.3 Grupy adresów URL

W ramach grup adresów URL można tworzyć grupę zawierającą kilka łączy do adresów URL, dla których użytkownik chce utworzyć regułę (zezwól/nie zezwalaj w odniesieniu do określonych stron internetowych).

Aby utworzyć nową grupę adresów URL, należy kliknąć opcję **Dodaj**. Zaznaczenie grupy adresów URL i kliknięcie przycisku **Dodaj** w prawej dolnej części okna powoduje dodanie do listy nowego adresu URL, a kliknięcie opcji **Importuj** umożliwia zaimportowanie pliku z adresami URL (wartości muszą być oddzielone podziałami wiersza, na przykład w formacie *.txt z kodowaniem UTF-8). W celu skonfigurowania czynności, która ma być wykonywana w odniesieniu do określonej grupy adresów URL należy otworzyć **Edytor reguł kontroli dostępu do stron internetowych**, wybrać grupę adresów URL z menu rozwijanego, dostosować inne parametry, a następnie kliknąć przycisk **OK**.

UWAGA: Blokowanie i zezwalanie dotyczące konkretnych stron internetowych zapewnia bardziej precyzyjną kontrolę niż blokowanie i zezwalanie na poziomie całych kategorii stron. Podczas zmieniania tych ustawień oraz dodawania kategorii i stron do listy należy postępować uważnie.

3.9.5 Aktualizowanie programu

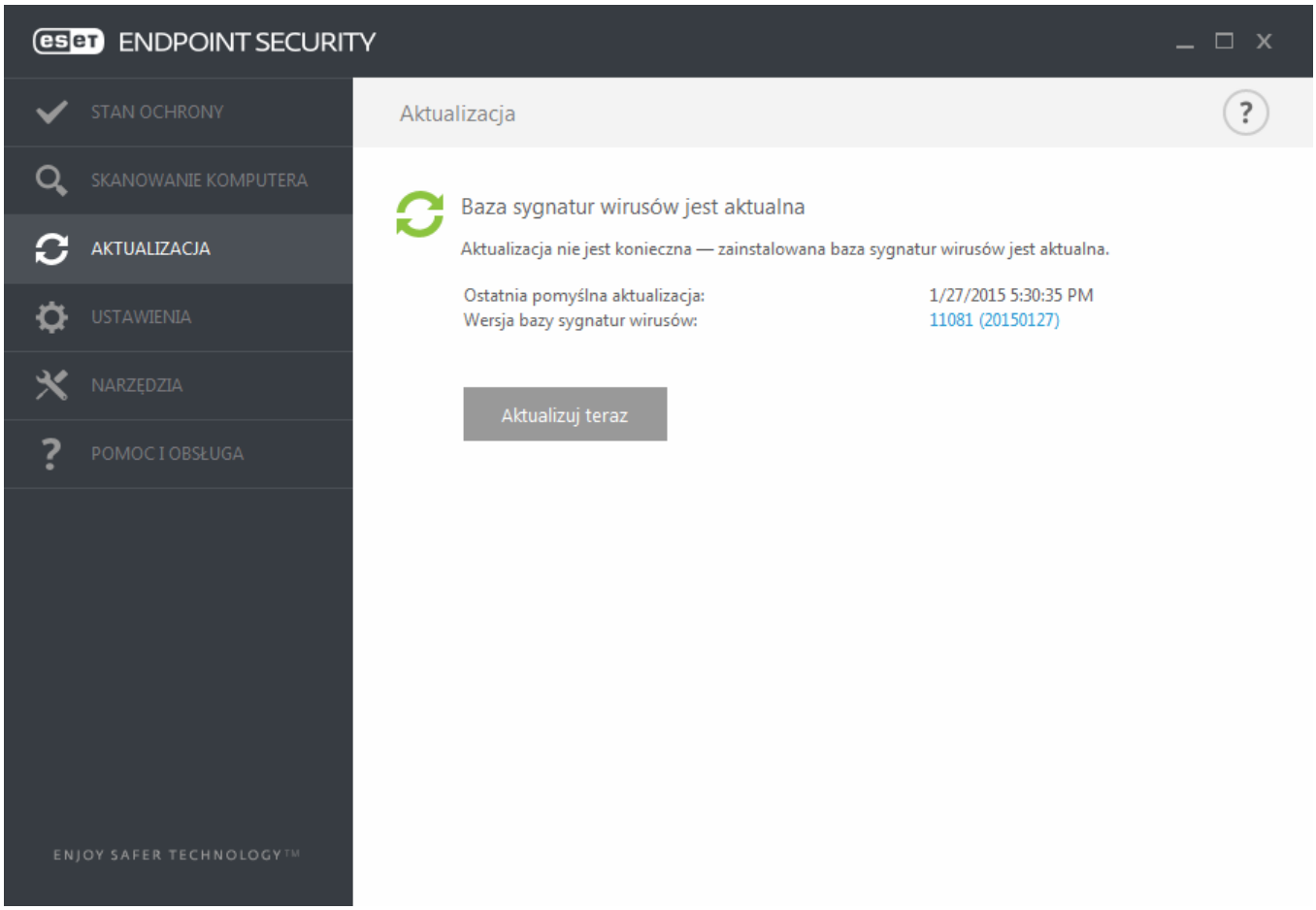
Regularne aktualizowanie programu ESET Endpoint Security to najlepszy sposób na uzyskanie najwyższego poziomu bezpieczeństwa komputera. Moduł aktualizacji zapewnia aktualność programu na dwa sposoby: przez aktualizowanie bazy sygnatur wirusów oraz aktualizowanie komponentów systemu.

Klikając w głównym oknie programu przycisk **Aktualizacja**, można sprawdzić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację. W głównym oknie jest również wyświetlana wersja bazy sygnatur wirusów. Ten liczbowy wskaźnik stanowi aktywne łącze do witryny internetowej firmy ESET zawierającej listę wszystkich sygnatur dodanych podczas określonej aktualizacji.

Ponadto dostępna jest opcja ręcznego rozpoczęcia procesu aktualizacji: **Aktualizuj bazę sygnatur wirusów**. Aktualizacja bazy sygnatur wirusów oraz aktualizacja komponentów programu są istotnymi elementami procesu zapewniania kompleksowej ochrony przed złośliwym kodem. Należy zwrócić uwagę na konfigurację i działanie funkcji aktualizacji. Jeśli użytkownik nie podał danych licencji podczas instalacji, klucz licencyjny można podać w celu uzyskania dostępu do serwerów aktualizacji firmy ESET, klikając opcję **Aktywuj produkt** podczas aktualizacji.

W przypadku aktywacji programu ESET Endpoint Security przy użyciu pliku licencji offline bez nazwy użytkownika i hasła i próby aktualizacji informacja w kolorze czerwonym **Aktualizacja bazy sygnatur wirusów zakończyła się błędem** oznacza możliwość pobrania tylko z kopii dystrybucyjnej.

UWAGA: Klucz licencyjny jest podawany przez firmę ESET przy zakupie produktu ESET Endpoint Security.

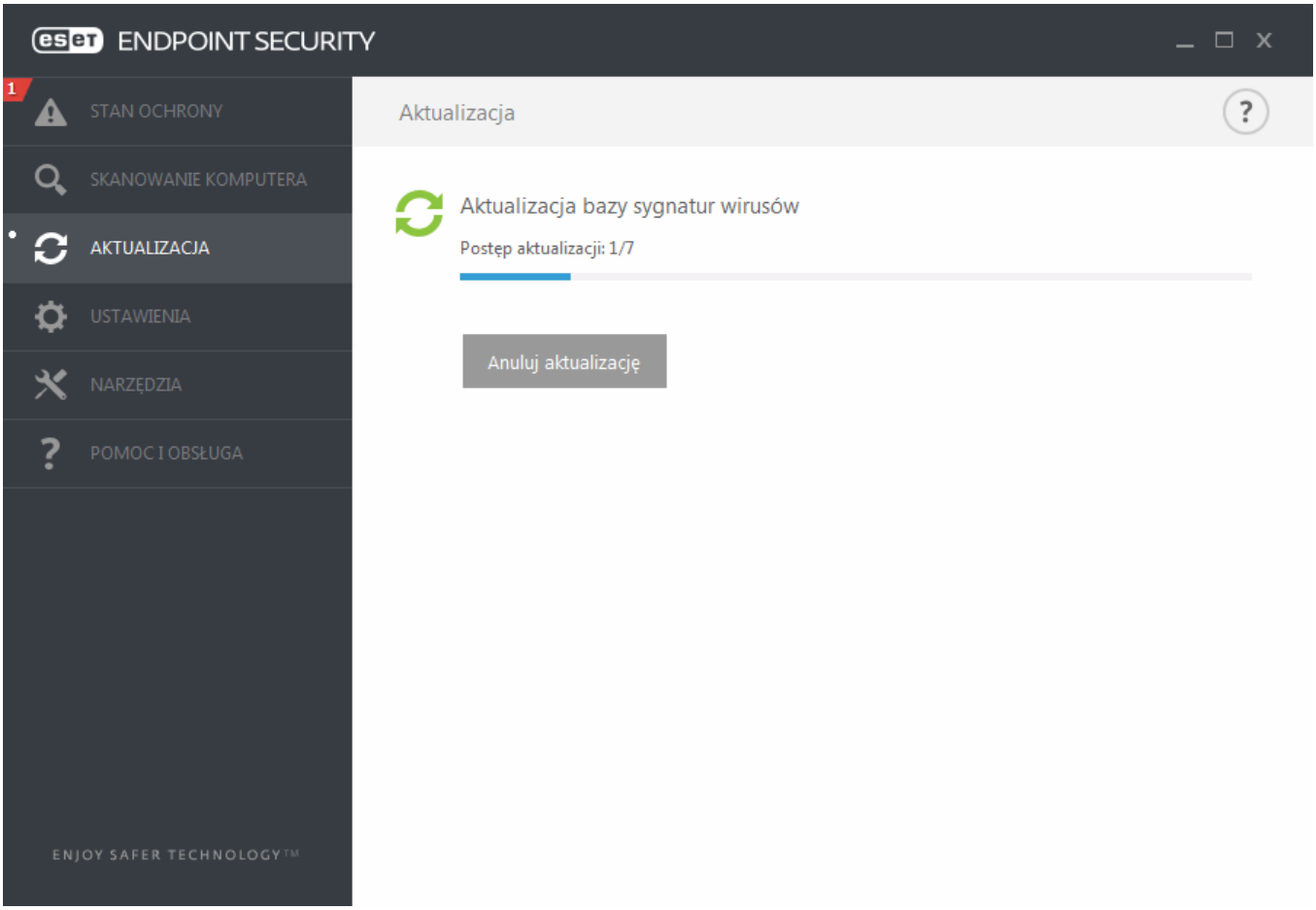


Ostatnia pomyślna aktualizacja — data ostatniej aktualizacji. Powinna to być niedawna data, co będzie oznaczało, że baza sygnatur wirusów jest aktualna.

Wersja bazy sygnatur wirusów — numer bazy sygnatur wirusów, który jest jednocześnie aktywnym łączem do witryny internetowej firmy ESET. Kliknięcie numeru powoduje wyświetlenie listy wszystkich sygnatur dodanych w ramach danej aktualizacji.

Procedura aktualizacji

Po kliknięciu przycisku **Aktualizuj bazę sygnatur wirusów** rozpoczyna się pobieranie danych. W jego trakcie jest wyświetlany pasek postępu i czas pozostały do końca pobierania. Aby przerwać aktualizację, należy kliknąć przycisk **Anuluj aktualizację**.

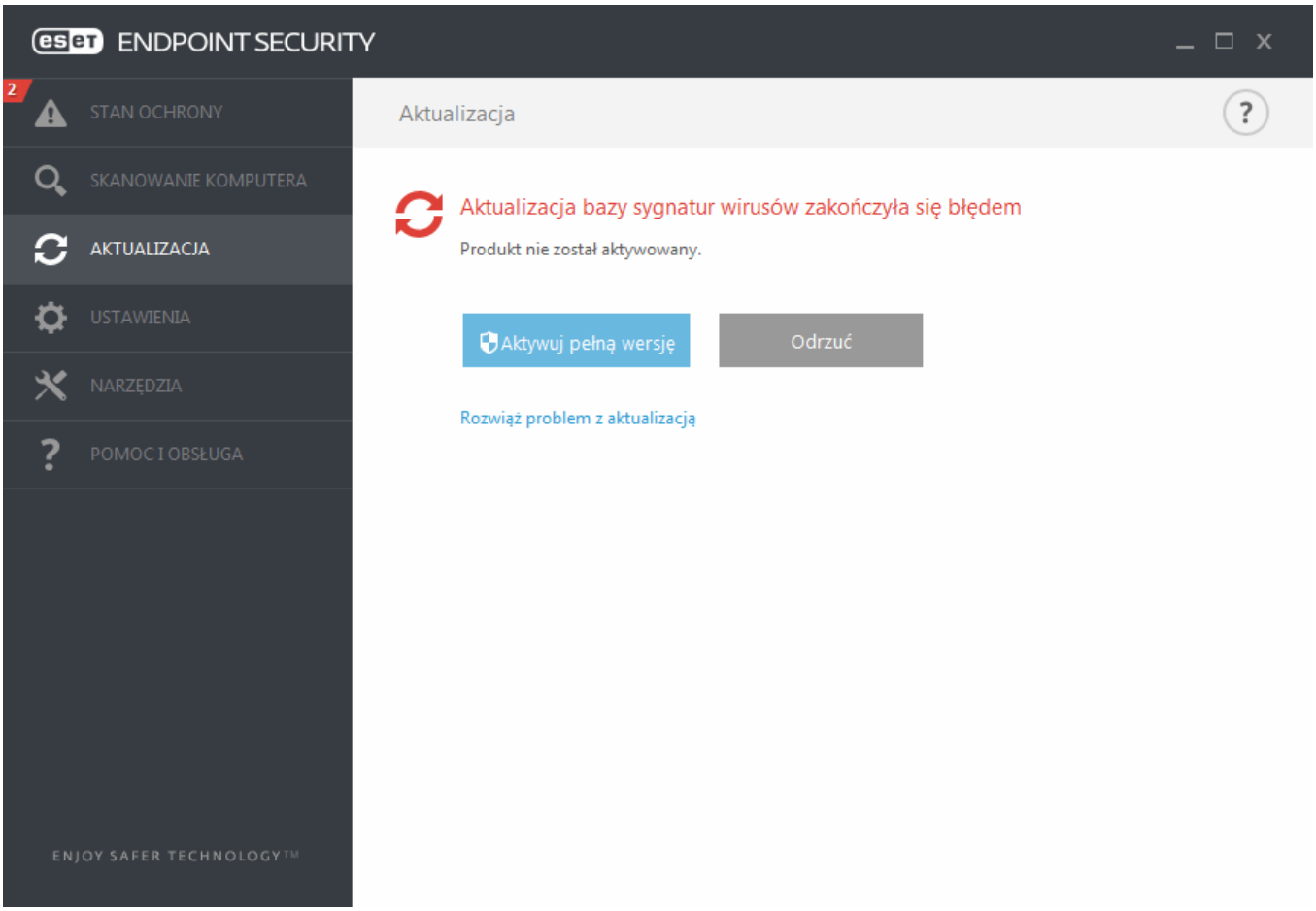


Ważne: W normalnych warunkach po prawidłowym pobraniu aktualizacji w oknie **Aktualizacja** pojawia się komunikat **Aktualizacja nie jest konieczna — zainstalowana baza sygnatur wirusów jest aktualna**. Jeżeli tak nie jest, program jest nieaktualny i jest bardziej podatny na zarażenie. Należy wówczas jak najszybciej zaktualizować bazę sygnatur wirusów.

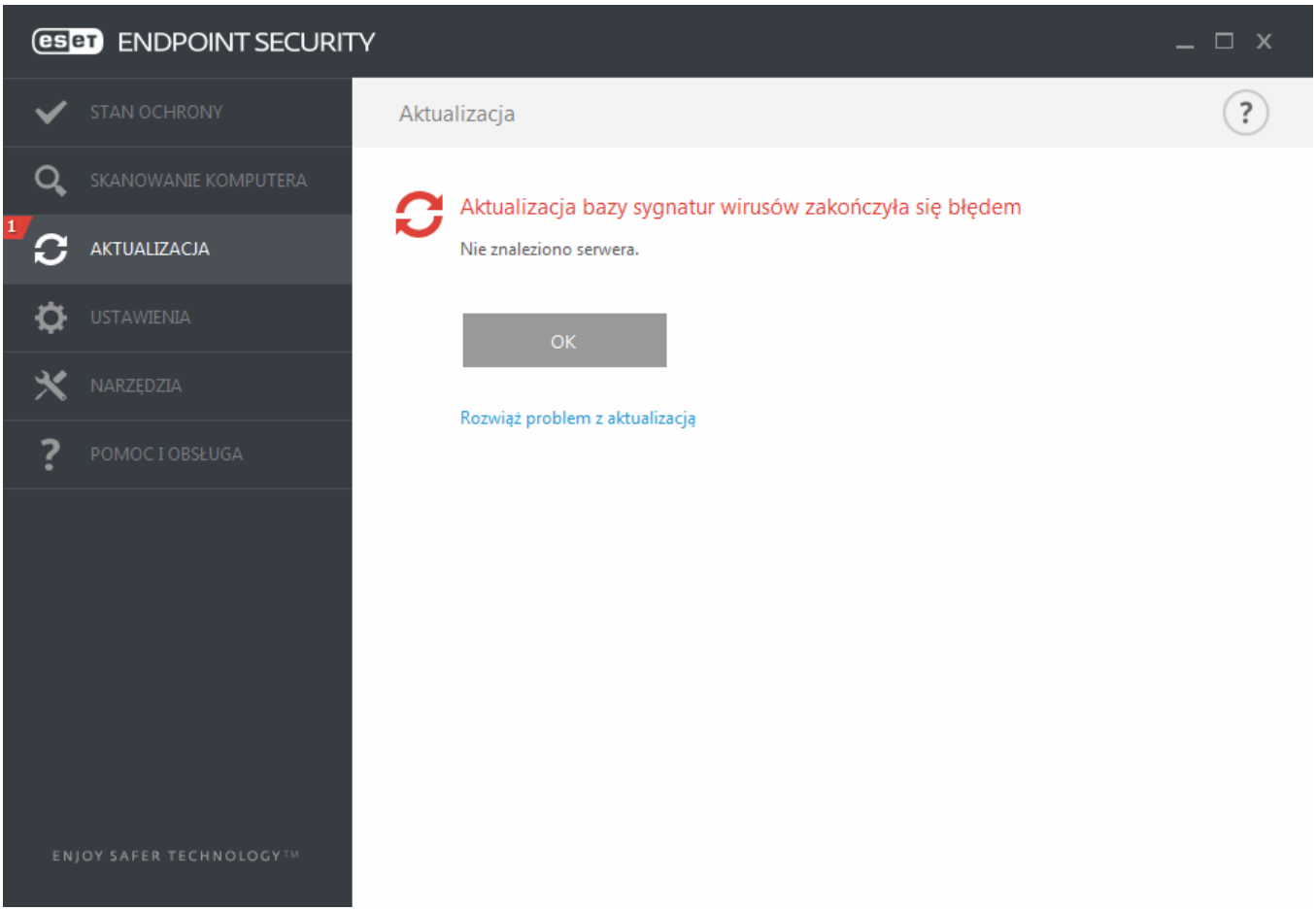
Baza sygnatur wirusów jest nieaktualna — ten komunikat o błędzie jest wyświetlany po kilku nieudanych próbach aktualizacji bazy sygnatur wirusów. Zaleca się sprawdzenie ustawień aktualizacji. Najczęstszym powodem wystąpienia tego błędu jest niewłaściwe wprowadzenie danych uwierzytelniających lub nieprawidłowe skonfigurowanie ustawień połączenia.

Poprzednie powiadomienie związane jest z następującymi dwiema wiadomościami **Aktualizacja bazy sygnatur wirusów nie powiodła się** o niepowodzeniu aktualizacji:

1. **Nieprawidłowa licencja** — w konfiguracji aktualizacji wprowadzono nieprawidłowy klucz licencyjny. Zalecane jest sprawdzenie danych uwierzytelniających. W oknie Ustawienia zaawansowane dostępne są dodatkowe opcje aktualizacji. Aby przejść do tego okna, kliknij w menu głównym opcję **Ustawienia**, a następnie kliknij opcję **Ustawienia zaawansowane** albo naciśnij klawisz F5 na klawiaturze. W menu głównym kliknij kolejno opcje **Pomoc i obsługa** > **Zarządzanie licencją**, aby wprowadzić nowy klucz licencyjny.



2. **Wystąpił błąd podczas pobierania plików aktualizacji.** — potencjalna przyczyna błędu to nieprawidłowe ustawienia połączenia internetowego. Zalecamy sprawdzenie połączenia z Internetem (np. przez otwarcie w przeglądarce internetowej dowolnej strony). Jeśli strona nie zostanie otwarta, prawdopodobnie połączenie z Internetem nie zostało nawiązane lub komputer ma problemy z komunikacją. W razie braku aktywnego połączenia z Internetem należy skontaktować się z dostawcą usług internetowych (ISP).



UWAGA: Więcej informacji można znaleźć w tym artykule bazy wiedzy firmy ESET.

3.9.5.1 Ustawienia aktualizacji

Ustawienia aktualizacji są dostępne w drzewie **Ustawienia zaawansowane** (F5) po kliknięciu pozycji **Aktualizacja** > **Podstawowe**. Ta sekcja umożliwia określenie informacji o źródle aktualizacji, w tym używanych serwerów aktualizacji i dotyczących ich danych uwierzytelniających.

Ogólne

Aktualnie stosowany profil aktualizacji wyświetlany jest w menu rozwijanym **Wybrany profil**. Aby utworzyć nowy profil, kliknij opcję **Edytuj** obok pozycji **Lista profili**, wprowadź własną nazwę w polu **Nazwa profilu**, a następnie kliknij przycisk **Dodaj**.

Jeśli przy próbie pobrania aktualizacji bazy sygnatur wirusów wystąpią trudności, kliknij opcję **Wyczyść** w celu usunięcia tymczasowych plików aktualizacji lub wyczyszczenia pamięci podręcznej.

Alerty o nieaktualnej bazie sygnatur wirusów

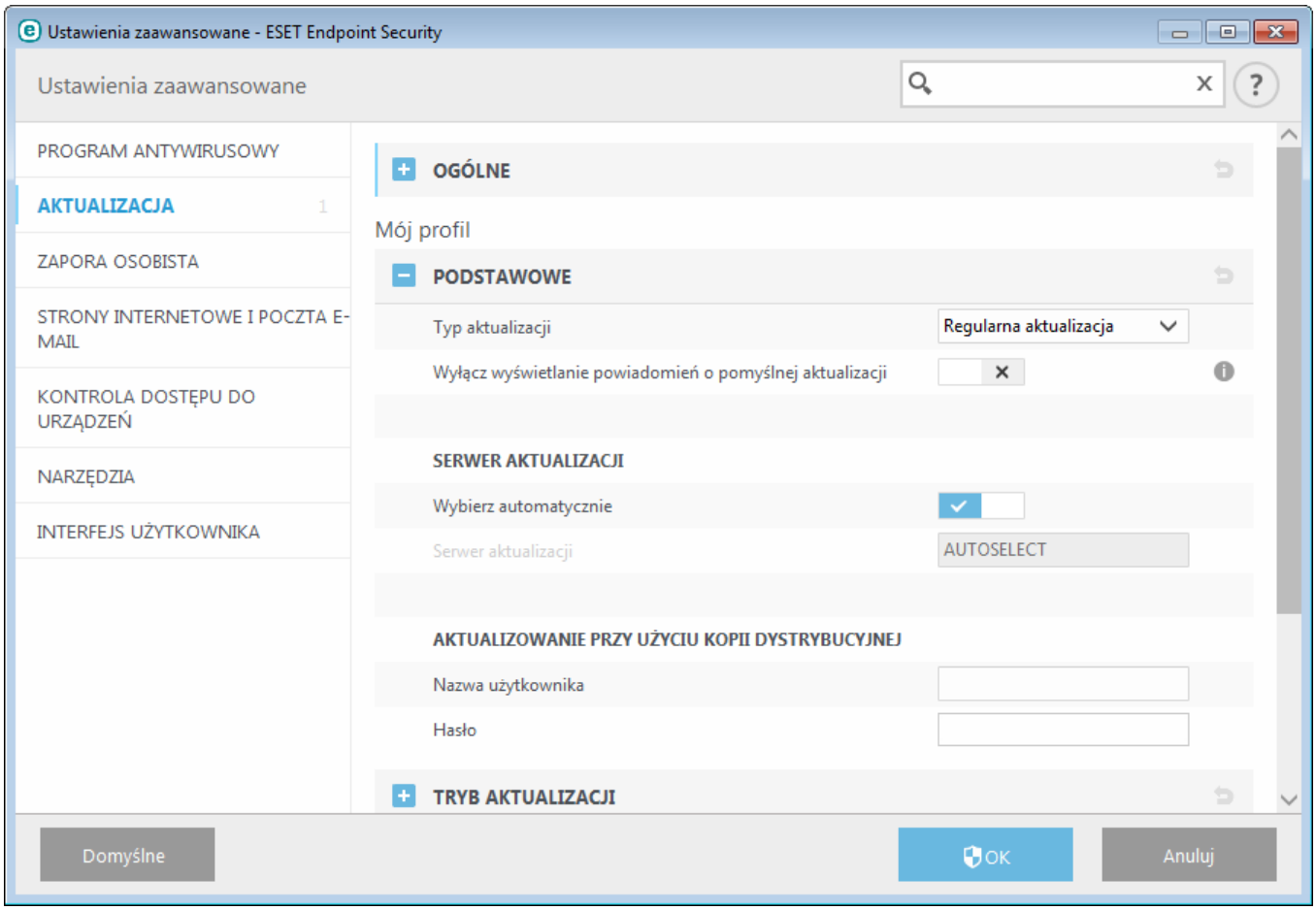
Automatycznie ustaw maksymalny wiek bazy danych — umożliwia ustawienie maksymalnego czasu (w dniach), po upływie którego baza sygnatur wirusów zostanie zgłoszona jako nieaktualna. Wartość domyślna to 7.

Cofanie zmian

W razie podejrzeń, że nowa aktualizacja bazy wirusów i/lub modułów programu może być niestabilna lub uszkodzona, można wycofać zmiany i wrócić do poprzedniej wersji oraz wyłączyć aktualizacje na określony czas. Można także włączyć aktualizacje, które zostały wcześniej wyłączone na czas nieokreślony.

Program ESET Endpoint Security zapisuje migawki bazy sygnatur wirusów i modułów programu przeznaczone do użycia z funkcją *cofania zmian*. Aby tworzyć migawki bazy danych wirusów, należy pozostawić przełącznik opcji **Utwórz kopie wcześniejszych plików aktualizacji** włączony. Pole **Liczba kopii przechowywanych lokalnie** określa liczbę przechowywanych migawek wcześniejszych baz danych wirusów.

Po kliknięciu opcji **Cofanie zmian** (**Ustawienia zaawansowane** (F5) > **Aktualizacja** > **Ogólne**) należy z menu rozwijanego wybrać okres, w którym aktualizacje bazy sygnatur wirusów i modułów programu będą wstrzymane.



Poprawność pobierania aktualizacji zależy od prawidłowego wprowadzenia wszystkich parametrów aktualizacji. Jeśli używana jest zapora, należy się upewnić, że nie blokuje ona programowi ESET dostępu do Internetu (na przykład komunikacji HTTP).

Podstawowe

Domyślnie w menu **Typ aktualizacji** ustawiona jest opcja **Regularna aktualizacja**. Zapewnia ona automatyczne pobieranie plików aktualizacji z serwera firmy ESET przy jak najmniejszym obciążaniu sieci. Aktualizacje w wersji wstępnej (opcja **Aktualizacja w wersji wstępnej**) są aktualizacjami, które przeszły wszechstronne testy wewnętrzne i wkrótce zostaną udostępnione do ogólnego użytku. Włączenie aktualizacji w wersji wstępnej przynosi korzyść w postaci dostępu do najnowszych metod wykrywania i poprawek. Aktualizacje te mogą być jednak czasem niestabilne i NIE NALEŻY ich używać na produkcyjnych serwerach i stacjach roboczych, od których wymaga się maksymalnej dostępności i stabilności. Opcja **Opóźniona aktualizacja** umożliwia dokonywanie aktualizacji ze specjalnych serwerów aktualizacji, zapewniających dostęp do nowych wersji baz wirusów z opóźnieniem co najmniej X godzin, czyli baz przetestowanych w prawdziwym środowisku i z tego powodu uważanych za stabilne.

Wyłącz wyświetlanie powiadomień o pomyślnej aktualizacji — powoduje wyłączenie powiadomień na pasku zadań w prawym dolnym rogu ekranu. Opcja ta może być użyteczna w przypadku aplikacji lub gier działających w trybie pełnoekranowym. Należy pamiętać, że włączenie trybu prezentacji powoduje wyłączenie wszystkich powiadomień.

Aktualizuj z nośnika wymiennego — umożliwia aktualizację z nośnika wymiennego, który zawiera kopię dystrybucyjną. W przypadku wybrania opcji **Automatycznie** aktualizacja zostanie uruchomiona w tle. W celu wyświetlania okien dialogowych aktualizacji należy wybrać opcję **Zawsze pytaj**.

W menu **Serwer aktualizacji** domyślnie ustawiona jest opcja AUTOSELECT. Serwer aktualizacji to określenie

lokalizacji, w której są przechowywane aktualizacje. W przypadku korzystania z serwera ESET zalecane jest pozostawienie włączonej opcji domyślnej.

W przypadku korzystania z lokalnego serwera HTTP, znanego też jako Kopia dystrybucyjna, należy wprowadzić następujące ustawienia serwera aktualizacji:
http://nazwa_komputera_lub_jego_adres_IP:2221

W przypadku korzystania z lokalnego serwera HTTP z protokołem SSL należy wprowadzić następujące ustawienia serwera aktualizacji:
https://nazwa_komputera_lub_jego_adres_IP:2221

W przypadku korzystania z lokalnego folderu udostępnionego należy wprowadzić następujące ustawienia serwera aktualizacji:
\\nazwa_lub_adres_IP_komputera\folder_udostępniony

Aktualizowanie przy użyciu kopii dystrybucyjnej

Do uwierzytelniania na serwerach aktualizacji używany jest **klucz licencyjny** wygenerowany i dostarczony użytkownikowi po zakupie programu. W przypadku korzystania z lokalnego serwera kopii dystrybucyjnych można zdefiniować poświadczenia umożliwiające klientom zalogowanie się do serwera kopii dystrybucyjnych przed pobraniem aktualizacji. Domyślnie weryfikacja tych danych nie jest wymagana, co oznacza, że pola **Nazwa użytkownika** i **Hasło** można pozostawić puste.

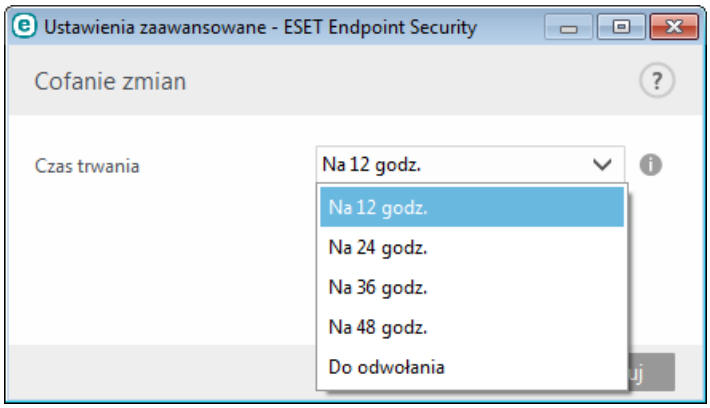
3.9.5.1.1 Profile aktualizacji

Dla różnych konfiguracji i zadań aktualizacji można tworzyć profile aktualizacji. Tworzenie profili aktualizacji jest przydatne zwłaszcza w przypadku użytkowników mobilnych, którym potrzebny jest alternatywny profil dla połączenia internetowego, którego właściwości regularnie się zmieniają.

W menu rozwijanym **Wybrany profil** wyświetlany jest aktualnie wybrany profil i jest on ustawiony domyślnie jako **Mój profil**. Aby utworzyć nowy profil, kliknij opcję **Edytuj** obok pozycji **Lista profili**, wprowadź własną nazwę w polu **Nazwa profilu**, a następnie kliknij przycisk **Dodaj**.

3.9.5.1.2 Cofanie aktualizacji

Po kliknięciu opcji **Cofanie zmian** (**Ustawienia zaawansowane** (F5) > **Aktualizacja** > **Profil**) należy z menu rozwijanego wybrać okres, w którym aktualizacje bazy sygnatur wirusów i modułów programu będą wstrzymane.



Wybranie opcji **Do odwołania** umożliwia odroczenie regularnych aktualizacji na czas nieokreślony do czasu ręcznego przywrócenia funkcji aktualizacji. Wybór tej opcji nie jest zalecany, ponieważ wnosi ona potencjalne zagrożenie bezpieczeństwa.

Baza sygnatur wirusów jest przywracana do najstarszej przechowywanej wersji i zapisywana w postaci migawki w systemie plików lokalnego komputera.

Przykład: Przyjmijmy, że numer 10646 oznacza najnowszą wersję bazy sygnatur wirusów. Wersje 10645 i 10643 są przechowywane jako migawki bazy sygnatur wirusów. Należy zauważyć, że wersja 10644 nie jest dostępna, ponieważ przykładowo komputer był wyłączony i przed pobraniem wersji 10644 została udostępniona nowsza aktualizacja. Jeśli w polu **Liczba kopii przechowywanych lokalnie** ustawiono wartość 2, to po kliknięciu przycisku

Cofanie zmian zostanie przywrócona wersja bazy sygnatur wirusów (i modułów programu) numer 10643. Ten proces może zająć nieco czasu. To, czy wersja bazy sygnatur wirusów została przywrócona, można sprawdzić w głównym oknie programu ESET Endpoint Security w sekcji Aktualizacja.

3.9.5.1.3 Tryb aktualizacji

Karta **Tryb aktualizacji** zawiera opcje związane z aktualizacją komponentów programu. Użytkownik może skonfigurować wstępnie sposób działania programu po wykryciu dostępności aktualizacji któregoś z jego komponentów.

Aktualizacja komponentu programu ma na celu dodanie nowych funkcji lub wprowadzenie zmian w funkcjach, które występowały już w starszych wersjach programu. Może ona być wykonywana automatycznie, bez interwencji użytkownika. Istnieje też możliwość powiadamiania użytkownika o aktualizacjach. Po zainstalowaniu aktualizacji komponentu programu konieczne może być ponowne uruchomienie komputera. W sekcji **Aktualizacja komponentu programu** są dostępne trzy opcje:

- **Pytaj przed pobraniem aktualizacji komponentów programu** — jest to opcja domyślna. Po udostępnieniu aktualizacji komponentów programu wyświetlony zostanie monit o udzielenie lub odmowę zgody na ich pobranie i zainstalowanie.
- **Zawsze aktualizuj komponenty programu** — aktualizacje komponentów programu będą pobierane i instalowane automatycznie. Należy pamiętać, że może się pojawić potrzeba ponownego uruchomienia komputera.
- **Nigdy nie aktualizuj komponentów programu** — aktualizacje komponentu programu nie będą w ogóle wykonywane. Ta opcja jest przeznaczona dla instalacji serwerowych, ponieważ możliwość ponownego uruchomienia serwera pojawia się zazwyczaj dopiero wtedy, gdy są wobec niego wykonywane czynności konserwacyjne.

UWAGA: Wybór najodpowiedniejszej opcji zależy od stacji roboczej, której będzie dotyczyć ustawienie. Należy pamiętać o różnicach między stacjami roboczymi a serwerami. Na przykład automatyczne ponowne uruchomienie serwera po aktualizacji programu mogłoby spowodować poważne szkody.

Jeśli aktywna jest opcja **Pytaj przed pobraniem aktualizacji**, to po udostępnieniu nowej aktualizacji wyświetlone zostanie powiadomienie.

Jeśli plik aktualizacji ma rozmiar większy niż wybrana wartość ustawienia **Pytaj, jeśli plik aktualizacji jest większy niż (kB)**, wyświetlone zostanie powiadomienie.

3.9.5.1.4 Serwer proxy HTTP

Aby przejść do opcji konfiguracji serwera proxy dla danego profilu aktualizacji, należy kliknąć pozycję **Aktualizacja** w drzewie **Ustawienia zaawansowane** (F5), a następnie kliknąć opcję **Serwer proxy HTTP**. Należy kliknąć menu rozwijane **Tryb proxy** i wybrać jedną spośród trzech następujących opcji:

- Nie używaj serwera proxy
- Połączenie przez serwer proxy
- Użyj globalnych ustawień serwera proxy

Wybór opcji **Użyj globalnych ustawień serwera proxy** spowoduje użycie opcji konfiguracyjnych serwera proxy określonych już w gałęzi **Narzędzia** > **Serwer proxy** w drzewie ustawień zaawansowanych.

Wybierz opcję **Nie używaj serwera proxy**, aby podczas aktualizacji ESET Endpoint Security nie używać serwera proxy.

Opcję **Połączenie przez serwer proxy** należy zaznaczyć w przypadku, gdy:

- Podczas aktualizacji programu ESET Endpoint Security ma być używany serwer proxy inny niż wybrany w ustawieniach globalnych (**Narzędzia** > **Serwer proxy**). W takiej sytuacji należy wprowadzić dodatkowe ustawienia: adres **serwera proxy**, jego **port** komunikacyjny (domyślnie 3128) oraz **nazwę użytkownika** i **hasło**, jeśli są wymagane w przypadku danego serwera proxy.
- Nie skonfigurowano ustawień serwera proxy na poziomie globalnym, ale program ESET Endpoint Security będzie łączyć się z serwerem proxy w celu aktualizacji.
- Komputer jest podłączony do Internetu za pośrednictwem serwera proxy. Podczas instalacji programu ustawienia są odczytywane z opcji programu Internet Explorer, ale jeśli ulegną później zmianie (np. użytkownik zmieni

dostawcę Internetu), należy upewnić się, że ustawienia serwera proxy HTTP wyświetlone w tym oknie są poprawne. W przeciwnym razie program nie będzie mógł nawiązać połączenia z serwerami aktualizacji.

Ustawieniem domyślnym dla serwera proxy jest **Użyj globalnych ustawień serwera proxy**.

UWAGA: Dane uwierzytelniające, tzn. **Nazwa użytkownika** i **Hasło**, dotyczą dostępu do serwera proxy. Pola te należy wypełnić tylko wtedy, gdy jest wymagane podanie nazwy użytkownika i hasła. Należy pamiętać, że nie są to nazwa użytkownika ani hasło programu ESET Endpoint Security. Pola te należy wypełnić tylko wtedy, gdy wiadomo, że w celu korzystania z Internetu niezbędne jest hasło serwera proxy.

3.9.5.1.5 Połącz z siecią LAN jako

W celu pobrania aktualizacji z serwera lokalnego z systemem operacyjnym Windows w wersji NT domyślnie wymagane jest uwierzytelnianie każdego połączenia sieciowego.

Aby skonfigurować takie konto, należy wybrać odpowiednią opcję z menu **Typ użytkownika lokalnego**:

- **Konto systemowe (domyślnie)**,
- **Bieżący użytkownik**,
- **Określony użytkownik**.

Aby użyć konta systemowego w celu uwierzytelniania, należy wybrać opcję **Konto systemowe (domyślnie)**. Zazwyczaj uwierzytelnianie nie jest przeprowadzane, jeśli w głównej sekcji ustawień aktualizacji nie podano danych uwierzytelniających.

Aby mieć pewność, że uwierzytelnianie jest przeprowadzanie przez program przy użyciu konta aktualnie zalogowanego użytkownika, należy zaznaczyć opcję **Bieżący użytkownik**. Wadą tego rozwiązania jest to, że program nie jest w stanie połączyć się z serwerem aktualizacji, jeśli w danym momencie nie jest zalogowany żaden użytkownik.

Jeśli program ma używać podczas uwierzytelniania określonego konta użytkownika, należy wybrać opcję **Określony użytkownik**. Z tej metody należy skorzystać, jeśli nie uda się nawiązać połączenia za pomocą domyślnego konta systemowego. Należy pamiętać, że wskazane konto użytkownika musi zapewniać dostęp do katalogu z plikami aktualizacyjnymi na serwerze lokalnym. W przeciwnym razie program nie będzie mógł ustanowić połączenia ani pobrać aktualizacji.

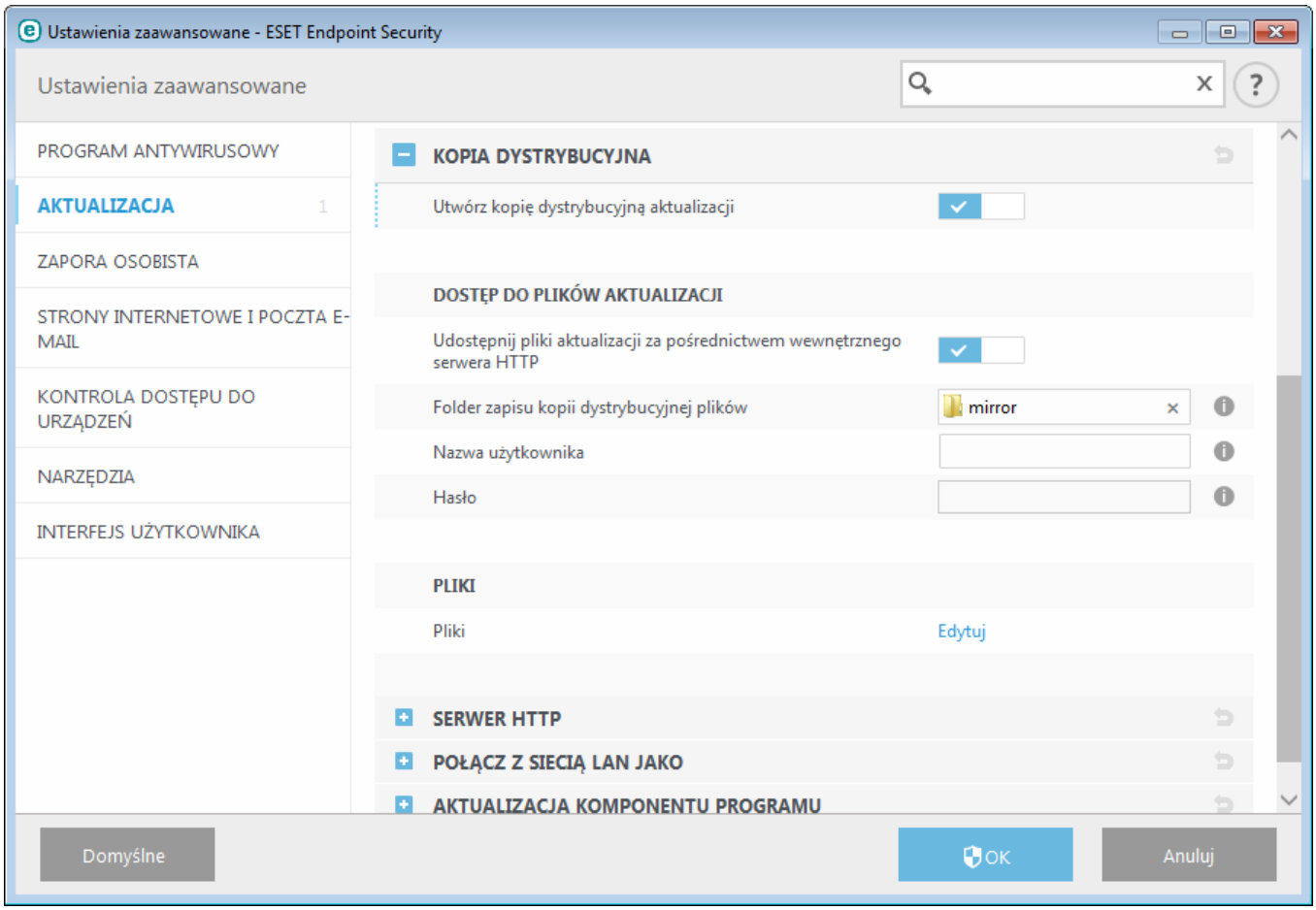
Ostrzeżenie: Jeśli została wybrana opcja **Bieżący użytkownik** lub **Określony użytkownik**, przy zmianie tożsamości w programie na żądanego użytkownika może wystąpić błąd. Zalecane jest wprowadzenie danych uwierzytelniających w sieci LAN w głównej sekcji ustawień aktualizacji. Należy wprowadzić dane uwierzytelniające w tej sekcji ustawień aktualizacji w następujący sposób: *nazwa_domeny**użytkownik* (w przypadku grupy roboczej *nazwa_grupy_roboczej* *nazwa*) oraz hasło. W przypadku aktualizacji z wersji HTTP serwera lokalnego uwierzytelnianie nie jest wymagane.

Jeśli połączenie z serwerem pozostaje aktywne nawet po pobraniu aktualizacji, należy włączyć opcję **Przerwij połączenie z serwerem po zakończeniu aktualizacji**, by wymusić jego przerwanie.

3.9.5.1.6 Kopia dystrybucyjna

Program ESET Endpoint Security umożliwia tworzenie kopii plików aktualizacji, których można używać do aktualizowania innych stacji roboczych w sieci. Korzystanie z *kopii dystrybucyjnej*, czyli kopii plików aktualizacji, w środowisku sieci LAN jest wygodne, ponieważ eliminuje potrzebę pobierania tych plików przez każdą stację roboczą bezpośrednio z serwera aktualizacji dostawcy. Aktualizacje są pobierane na lokalny serwer kopii dystrybucyjnych, a następnie dystrybuowane do wszystkich stacji roboczych, by uniknąć ryzyka generowania nadmiernego ruchu sieciowego. Aktualizowanie klienckich stacji roboczych przy użyciu kopii dystrybucyjnej pozwala na oszczędne korzystanie z przepustowości połączenia internetowego.

Opcje konfiguracji lokalnego serwera kopii dystrybucyjnych znajdują się w ustawieniach zaawansowanych w pozycji **Aktualizacja**. Aby uzyskać do nich dostęp, należy nacisnąć klawisz **F5** w celu otwarcia Ustawień zaawansowanych, kliknąć pozycję **Aktualizacja** i wybrać kartę **Kopia dystrybucyjna**.



Aby utworzyć kopię dystrybucyjną na klienckiej stacji roboczej, należy wybrać opcję **Utwórz kopię dystrybucyjną aktualizacji**. Powoduje to uaktywnienie innych opcji konfiguracji kopii dystrybucyjnej, na przykład sposobu udostępniania plików aktualizacji oraz ścieżki dostępu do plików kopii dystrybucyjnej aktualizacji.

Dostęp do plików aktualizacji

Udostępnij pliki aktualizacji za pośrednictwem wewnętrznego serwera HTTP — włączenie tej opcji powoduje, że dostęp do plików aktualizacji można uzyskać za pośrednictwem protokołu HTTP. Podawanie danych uwierzytelniających jest wymagane.

UWAGA: W systemie Windows XP musi być zainstalowany dodatek Service Pack 2 lub nowszy, aby możliwe było korzystanie z serwera HTTP.

Metody uzyskiwania dostępu do serwera kopii dystrybucyjnych opisano szczegółowo w sekcji Aktualizowanie przy użyciu kopii dystrybucyjnej. Istnieją dwie podstawowe metody uzyskiwania dostępu do kopii dystrybucyjnej: folder z plikami aktualizacji może być udostępniany jako folder sieciowy lub klienty mogą uzyskiwać dostęp do kopii dystrybucyjnej umieszczonej na serwerze HTTP.

Folder przeznaczony do przechowywania plików aktualizacji na potrzeby kopii dystrybucyjnej należy podać w sekcji **Folder przechowywania kopii dystrybucyjnej aktualizacji**. Należy kliknąć przycisk **Folder**, aby przejść do folderu na komputerze lokalnym lub do udostępnionego folderu sieciowego. Jeśli dany folder wymaga autoryzacji, należy wprowadzić dane uwierzytelniające w polach **Nazwa użytkownika** i **Hasło**. Jeśli wybrany folder docelowy znajduje się na dysku sieciowym w systemie operacyjnym Windows NT, 2000 lub XP, należy wprowadzić nazwę użytkownika, któremu przyznano uprawnienia zapisu do tego folderu, oraz skojarzone z nią hasło. Nazwę użytkownika i hasło należy wprowadzić w formacie *domena/użytkownik* lub *grupa_robocza/użytkownik*. Należy pamiętać o podaniu odpowiednich haseł.

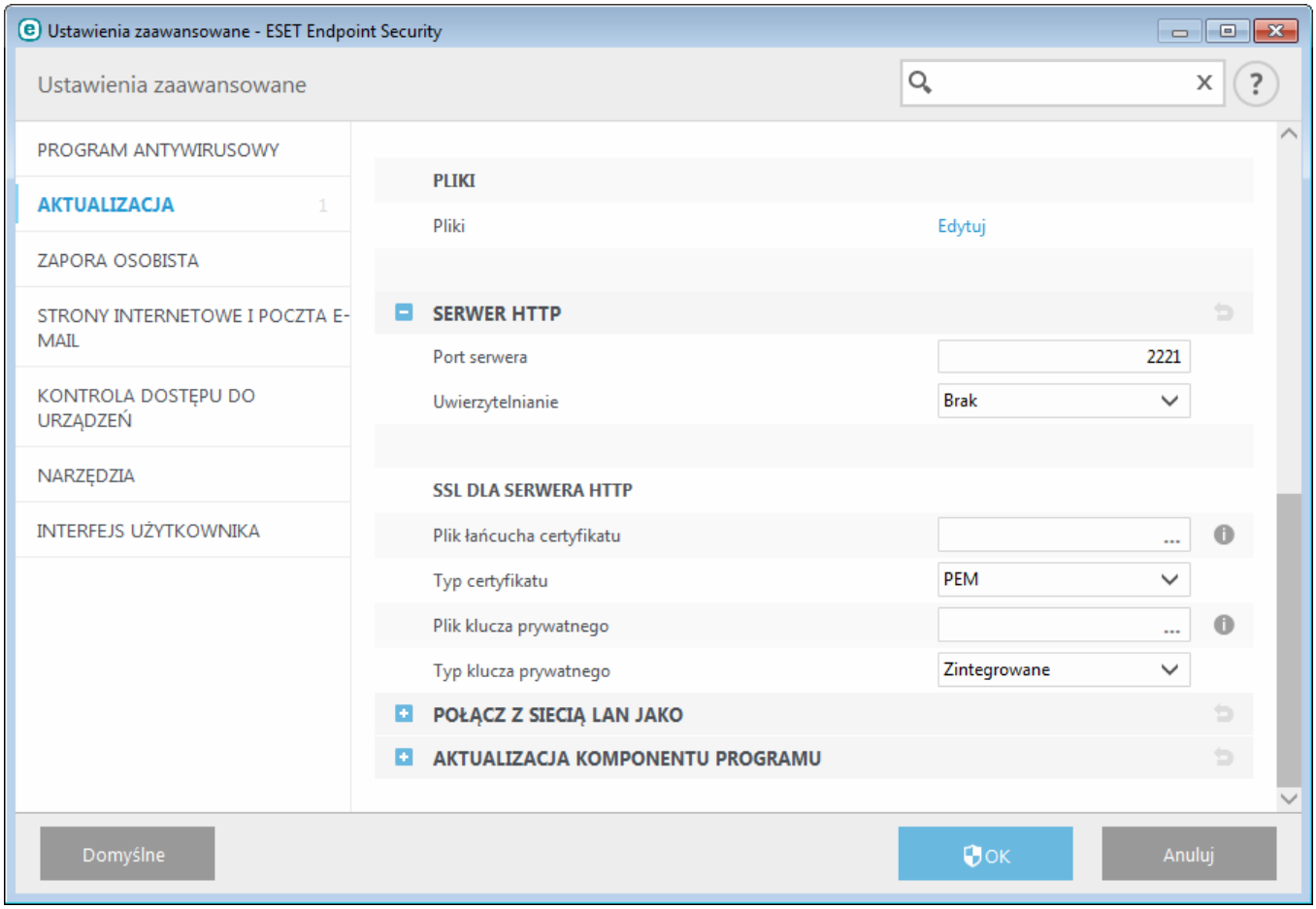
Pliki — podczas konfigurowania kopii dystrybucyjnej można wybrać wersje językowe plików aktualizacji, które mają zostać pobrane. Wybrane języki muszą być obsługiwane przez serwer kopii dystrybucyjnych skonfigurowany przez użytkownika.

Serwer HTTP

Port serwera — domyślnie dla portu serwera ustawiona jest wartość 2221.

Uwierzytelnianie — określenie metody uwierzytelniania dostępu do plików aktualizacji. Dostępne są następujące opcje: **Brak**, **Podstawowe** i **NTLM**. Wybór opcji **Podstawowe** spowoduje stosowanie kodowania base64 i podstawowej metody uwierzytelniania opartej na nazwie użytkownika i haśle. Opcja **NTLM** umożliwia uwierzytelnianie przy użyciu bezpiecznego kodowania. Na potrzeby uwierzytelniania używane jest konto użytkownika utworzone na stacji roboczej udostępniającej pliki aktualizacji. Ustawienie domyślne **Brak** zapewnia dostęp do plików aktualizacji bez konieczności uwierzytelniania.

Jeśli ma zostać uruchomiony serwer HTTP z obsługą HTTPS (SSL), należy dołączyć **plik łańcucha certyfikatu** lub wygenerować certyfikat podpisany samodzielnie. Dostępne są następujące typy certyfikatów: ASN, PEM oraz PFX. Aby dodatkowo zwiększyć bezpieczeństwo, przy pobieraniu plików aktualizacji można użyć protokołu HTTPS. Przy zastosowaniu tego protokołu śledzenie transferu danych i poświadczeń podczas logowania jest niemal niemożliwe. Domyślne ustawienie opcji **Typ klucza prywatnego** to **Zintegrowany** (w związku z tym opcja **Plik klucza prywatnego** jest domyślnie wyłączona). Oznacza to, że klucz prywatny stanowi część wybranego pliku łańcucha certyfikatu.



Połącz z siecią LAN jako

Typ użytkownika lokalnego — ustawienia **Konto systemowe (domyślnie)**, **Bieżący użytkownik** oraz **Określony użytkownik** będą wyświetlane w odpowiednich menu rozwijanych. Ustawienia **Nazwa użytkownika** i **Hasło** są opcjonalne. Zobacz również Połącz z siecią LAN jako.

Jeśli połączenie z serwerem pozostaje aktywne nawet po pobraniu aktualizacji, należy wybrać opcję **Przerwij połączenie z serwerem po zakończeniu aktualizacji**, by wymusić jego przerwanie.

Aktualizacja komponentu programu

Automatycznie aktualizuj komponenty — umożliwia instalację nowych funkcji i aktualizacji funkcji istniejących. Aktualizacja może być wykonywana automatycznie, bez interwencji użytkownika. Istnieje też możliwość powiadamiania użytkownika o aktualizacjach. Po zainstalowaniu aktualizacji komponentu programu konieczne może być ponowne uruchomienie komputera.

Zaktualizuj teraz komponenty — aktualizuje komponenty programu do najnowszej wersji.

3.9.5.1.6.1 Aktualizowanie przy użyciu kopii dystrybucyjnej

Istnieją dwie podstawowe metody konfigurowania kopii dystrybucyjnej, będącej repozytorium, z którego klienty mogą pobierać pliki aktualizacji. Folder z plikami aktualizacji może być udostępniany jako folder sieciowy lub jako serwer HTTP.

Uzyskiwanie dostępu do kopii dystrybucyjnej przy użyciu wewnętrznego serwera HTTP

Jest to ustawienie domyślne, wybrane we wstępnie zdefiniowanej konfiguracji programu. Aby zezwolić na dostęp do kopii dystrybucyjnej przy użyciu serwera HTTP, należy przejść do sekcji **Ustawienia zaawansowane** > **Aktualizacja** > **Kopia dystrybucyjna** i wybrać opcję **Utwórz kopię dystrybucyjną aktualizacji**.

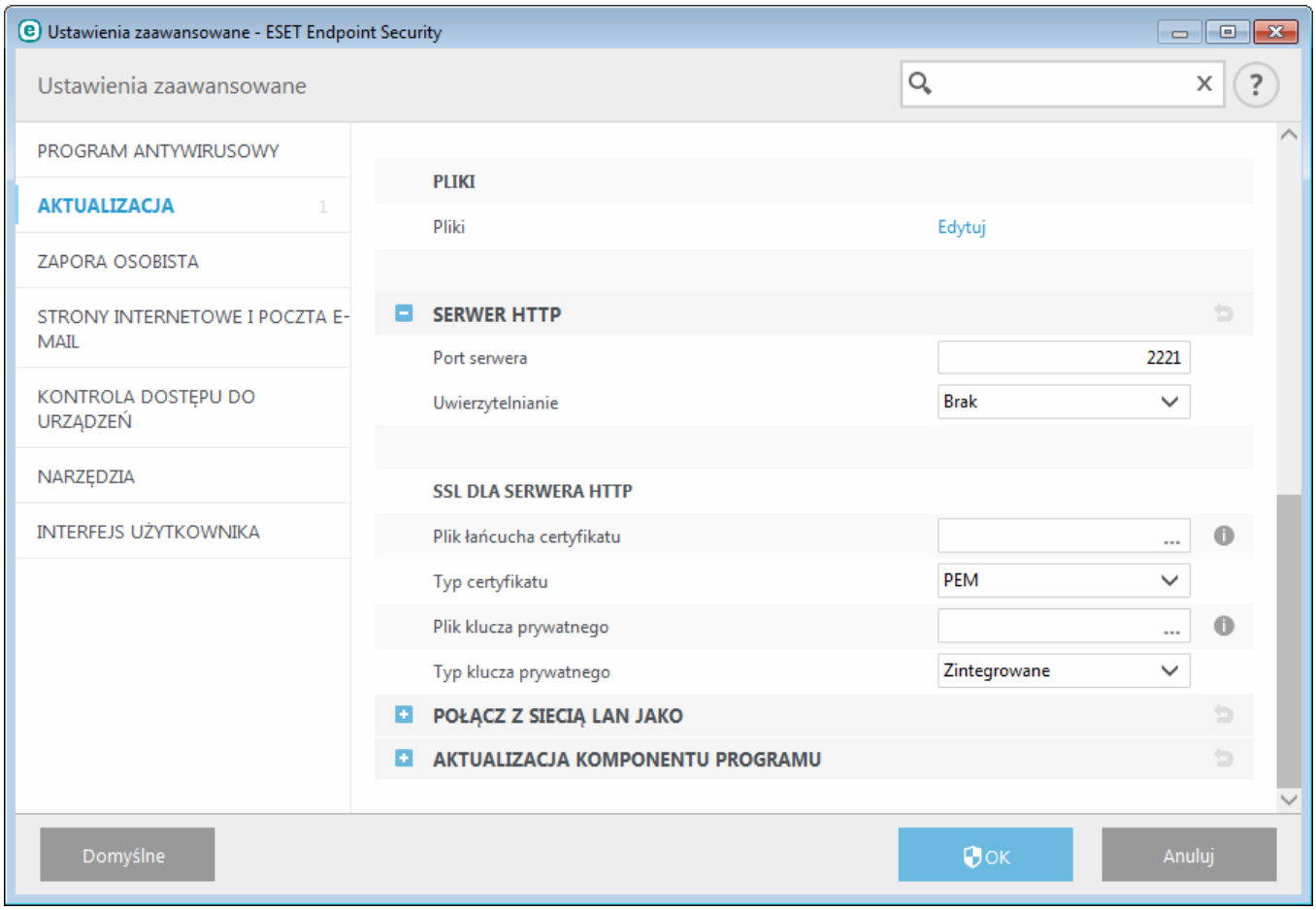
W sekcji **Serwer HTTP** na karcie **Kopia dystrybucyjna** można podać **Port serwera**, na którym będzie nasłuchiwać serwer HTTP, oraz typ uwierzytelniania stosowanego na serwerze HTTP (w polu **Uwierzytelnianie**). Domyślnie ustawiony jest port serwera numer **2221**. W ramach opcji **Uwierzytelnianie** można określić metodę uwierzytelniania dostępu do plików aktualizacji. Dostępne są następujące opcje: **Brak**, **Podstawowe** i **NTLM**. Wybór opcji **Podstawowe** spowoduje stosowanie kodowania base64 i podstawowej metody uwierzytelniania opartej na nazwie użytkownika i haśle. Opcja **NTLM** umożliwia uwierzytelnianie przy użyciu bezpiecznego kodowania. Na potrzeby uwierzytelniania używane jest konto użytkownika utworzone na stacji roboczej udostępniającej pliki aktualizacji. Ustawienie domyślne **Brak** zapewnia dostęp do plików aktualizacji bez konieczności uwierzytelniania.

Ostrzeżenie: Aby dostęp do plików aktualizacji był możliwy za pośrednictwem serwera HTTP, folder kopii dystrybucyjnej musi znajdować się na tym samym komputerze co instancja programu ESET Endpoint Security, w której ten folder został utworzony.

SSL dla serwera HTTP

Jeśli ma zostać uruchomiony serwer HTTP z obsługą HTTPS (SSL), należy dołączyć **plik łańcucha certyfikatu** lub wygenerować certyfikat podpisany samodzielnie. Dostępne są następujące typy certyfikatów: **PEM, PFX** i **ASN**. Aby dodatkowo zwiększyć bezpieczeństwo, przy pobieraniu plików aktualizacji można użyć protokołu HTTPS. Przy zastosowaniu tego protokołu śledzenie transferu danych i poświadczeń podczas logowania jest niemal niemożliwe. Domyślne ustawienie opcji **Typ klucza prywatnego** to **Zintegrowany**, co oznacza, że klucz prywatny jest częścią wybranego pliku łańcucha certyfikatu.

UWAGA: Po kilku nieudanych próbach zaktualizowania bazy sygnatur wirusów przy użyciu kopii dystrybucyjnej w okienku Aktualizacja w menu głównym zostanie wyświetlony błąd **Nieprawidłowa nazwa użytkownika i/lub hasło**. Zalecamy przejście do obszaru **Ustawienia zaawansowane** > **Aktualizacja** > **Kopia dystrybucyjna** i sprawdzenie nazwy użytkownika oraz hasła. Najczęstszym powodem wystąpienia tego błędu jest wprowadzenie nieprawidłowych danych uwierzytelniających.



Po skonfigurowaniu serwera kopii dystrybucyjnych należy dodać nowy serwer aktualizacji na klienckich stacjach roboczych. W tym celu:

- Otwórz okno **Ustawienia zaawansowane** (klawisz F5) i kliknij kolejno opcje **Aktualizacja** > **Podstawowe**.
- Wyłącz opcję **Wybierz automatycznie** i w polu **Serwer aktualizacji** dodaj nowy serwer w jednym z następujących formatów:
  http://adres_IP_serwera:2221
  https://adres_IP_serwera:2221 (jeśli używany jest protokół SSL)

Uzyskiwanie dostępu do kopii dystrybucyjnej za pośrednictwem udziałów systemowych

Najpierw na urządzeniu lokalnym lub sieciowym należy utworzyć folder udostępniony. Podczas tworzenia folderu przeznaczonego do przechowywania kopii dystrybucyjnych konieczne jest zapewnienie dostępu z uprawnieniami do *zapisu* dla użytkownika, który będzie zapisywać pliki aktualizacyjne w folderze, oraz dostępu z uprawnieniami do *odczytu* dla wszystkich użytkowników, którzy będą aktualizować program ESET Endpoint Security, korzystając z tego folderu kopii dystrybucyjnej.

Następnie należy skonfigurować dostęp do kopii dystrybucyjnej w sekcji **Ustawienia zaawansowane** > **Aktualizacja** > na karcie **Kopia dystrybucyjna**, wyłączając opcję **Udostępnij pliki aktualizacji za pośrednictwem wewnętrznego serwera HTTP**. Ta opcja jest domyślnie włączona w pakiecie instalacyjnym programu.

Jeśli folder udostępniony znajduje się na innym komputerze w sieci, należy wprowadzić dane uwierzytelniające niezbędne do uzyskania dostępu do tego komputera. Aby wprowadzić dane uwierzytelniające, należy w programie ESET Endpoint Security otworzyć okno **Ustawienia zaawansowane** (klawisz F5) i kliknąć kolejno opcje **Aktualizacja** > **Połącz z siecią LAN jako**. Jest to ustawienie identyczne z ustawieniem używanym na potrzeby aktualizacji, które zostało ono opisane w sekcji Połącz z siecią LAN jako.

Po skonfigurowaniu kopii dystrybucyjnej należy podać na klienckich stacjach roboczych lokalizację serwera aktualizacji w formacie *\\ŚCIEŻKA_UNC\ŚCIEŻKA* w opisany poniżej sposób:

1. W programie ESET Endpoint Security otwórz okno **Ustawienia zaawansowane** i kliknij kolejno opcje **Aktualizacja** > **Podstawowe**.
2. Kliknij pole **Serwer aktualizacji** i dodaj nowy serwer, stosując format *ŚCIEŻKA_UNC**ŚCIEŻKA*.

UWAGA: Aby zapewnić prawidłowe działanie aktualizacji, ścieżkę do folderu kopii dystrybucyjnej należy podać w formacie UNC. Pobieranie aktualizacji ze zmapowanych dysków może nie działać.

Ostatnia sekcja kontroluje komponenty programu (PCU). Domyślnie pobrane komponenty programu są przygotowane do skopiowania do lokalnej kopii dystrybucyjnej. Jeśli opcja **Aktualizacja komponentu programu** jest włączona, nie trzeba klikać opcji **Uaktualnij**, ponieważ pliki zostaną automatycznie skopiowane do lokalnej kopii dystrybucyjnej po ich udostępnieniu. Więcej informacji na temat aktualizacji komponentów programu można znaleźć w sekcji Tryb aktualizacji.

3.9.5.1.6.2 Rozwiązywanie problemów z aktualizacją przy użyciu kopii dystrybucyjnej

W większości przypadków problemy występujące podczas aktualizacji przy użyciu serwera kopii dystrybucyjnych są powodowane przez co najmniej jedną z następujących przyczyn: nieprawidłowe skonfigurowanie opcji folderu kopii dystrybucyjnej, nieprawidłowe dane uwierzytelniające w folderze kopii dystrybucyjnej, nieprawidłowa konfiguracja na lokalnych stacjach roboczych próbujących pobrać pliki aktualizacji z kopii dystrybucyjnej. Przyczyny te mogą występować razem. Poniżej omówiono najczęstsze problemy dotyczące aktualizacji przy użyciu kopii dystrybucyjnej:

Program **ESET Endpoint Security zgłasza wystąpienie błędu podczas łączenia się z serwerem kopii dystrybucyjnej** — ten problem jest prawdopodobnie spowodowany nieprawidłowym skonfigurowaniem serwera aktualizacji (ścieżki sieciowej do folderu kopii dystrybucyjnej), z którego lokalne stacje robocze pobierają aktualizacje. Aby sprawdzić folder, należy kliknąć przycisk **Start** systemu Windows, kliknąć polecenie **Uruchom**, wpisać nazwę folderu i kliknąć przycisk **OK**. Powinna zostać wyświetlona zawartość folderu.

Program **ESET Endpoint Security wymaga nazwy użytkownika i hasła** — ten problem jest prawdopodobnie spowodowany nieprawidłowymi danymi uwierzytelniającymi (nazwa użytkownika i hasło) w sekcji aktualizacji. Nazwa użytkownika i hasło umożliwiają uzyskanie dostępu do serwera aktualizacji, który zostanie użyty do zaktualizowania programu. Należy się upewnić, że dane uwierzytelniające są poprawne i zostały wprowadzone we właściwym formacie, na przykład *domena/nazwa_użytkownika* lub *grupa_robocza/nazwa_użytkownika* plus odpowiednie hasło. Należy pamiętać, że jeśli serwer kopii dystrybucyjnej jest dostępny „dla wszystkich”, nie oznacza to przyznania uprawnień dostępu dla każdego użytkownika. „Wszyscy” nie oznacza dowolnego nieautoryzowanego użytkownika. Oznacza to jedynie, że folder jest dostępny dla wszystkich użytkowników w ramach domeny. Dlatego nawet w takim przypadku należy wprowadzić nazwę użytkownika domeny i hasło w sekcji ustawień aktualizacji.

Program **ESET Endpoint Security zgłasza wystąpienie błędu podczas łączenia się z serwerem kopii dystrybucyjnej** — komunikacja za pośrednictwem portu określonego dla serwera HTTP udostępniającego kopię dystrybucyjną jest zablokowana.

3.9.5.2 Tworzenie zadań aktualizacji

Aktualizacje można uruchamiać ręcznie, klikając przycisk **Aktualizuj bazę sygnatur wirusów** w oknie głównym, które pojawia się po kliknięciu w menu głównym przycisku **Aktualizacja**.

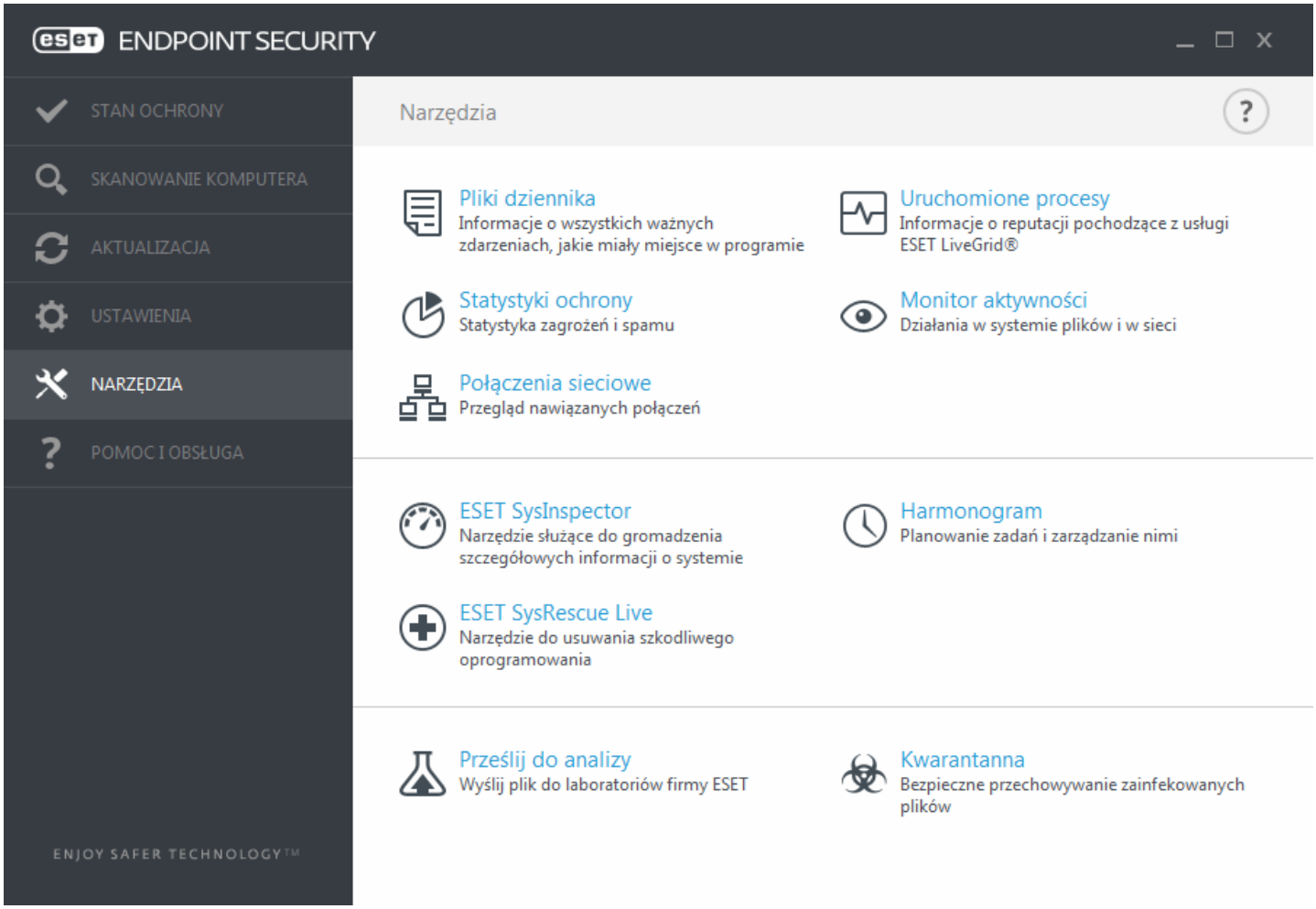
Inną możliwością jest wykonywanie aktualizacji jako zaplanowanych zadań. Aby skonfigurować zaplanowanie zadanie, kliknij kolejno opcje **Narzędzia** > **Harmonogram**. Domyślnie w programie ESET Endpoint Security aktywne są następujące zadania:

- **Regularna aktualizacja automatyczna**
- **Aktualizacja automatyczna po nawiązaniu połączenia modemowego**
- **Aktualizacja automatyczna po zalogowaniu użytkownika**

Każde z zadań aktualizacji można zmodyfikować zgodnie z potrzebami użytkownika. Oprócz domyślnych zadań aktualizacji można tworzyć nowe zadania z konfiguracją zdefiniowaną przez użytkownika. Więcej szczegółowych informacji na temat tworzenia i konfigurowania zadań aktualizacji można znaleźć w sekcji Harmonogram.

3.9.6 Narzędzia

Menu **Narzędzia** zawiera moduły, które upraszczają administrowanie programem i udostępniają dodatkowe opcje dla użytkowników zaawansowanych.



To menu zawiera następujące narzędzia:

- Pliki dziennika
- Statystyki ochrony
- Monitor aktywności
- Uruchomione procesy (jeśli usługa ESET Live Grid jest włączona w programie ESET Endpoint Security)
- Harmonogram
- Kwarantanna
- Połączenia sieciowe (jeśli jest włączona w programie ESET Endpoint Security)
- ESET SysInspector

Prześlij do analizy — umożliwia przesłanie podejrzanego pliku do analizy w laboratorium firmy ESET. Okno dialogowe wyświetlane po kliknięciu tej opcji opisano w sekcji Przesyłanie plików do analizy.

ESET SysRescue — kliknięcie tej pozycji powoduje przekierowanie do strony narzędzia ESET SysRescue Live, gdzie można pobrać obraz narzędzia ESET SysRescue Live lub Kreator Live CD/USB dla systemów operacyjnych Microsoft Windows.

3.9.6.1 Pliki dziennika

Pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce w programie, oraz przegląd wykrytych zagrożeń. Dzienniki są bardzo istotnym narzędziem przy analizowaniu systemu, wykrywaniu zagrożeń i rozwiązywaniu problemów. Dziennik jest aktywnie tworzony w tle i nie wymaga żadnych działań ze strony użytkownika. Informacje są zapisywane zgodnie z bieżącymi ustawieniami szczegółowości dziennika. Możliwe jest przeglądanie komunikatów tekstowych i dzienników bezpośrednio w programie ESET Endpoint Security. Ponadto możliwe jest archiwizowanie plików dziennika.

Pliki dziennika są dostępne z poziomu głównego okna programu po kliknięciu opcji **Narzędzia** > **Pliki dziennika**. Wybierz żądany typ dziennika z rozwijanego menu **Dziennik**. Dostępne są następujące dzienniki:

- **Wykryte zagrożenia** — dziennik zagrożeń zawiera szczegółowe informacje na temat infekcji wykrytych przez moduły programu ESET Endpoint Security. Podaje on między innymi: datę i godzinę zagrożenia, jego nazwę, lokalizację, przeprowadzone działanie oraz nazwę użytkownika zalogowanego w czasie wykrycia zagrożenia. Dwukrotne kliknięcie dowolnej pozycji dziennika powoduje wyświetlenie jej szczegółów w oddzielnym oknie.
- **Zdarzenia** — wszystkie ważne działania wykonywane przez program ESET Endpoint Security są zapisywane w dzienniku zdarzeń. Dziennik zdarzeń zawiera informacje na temat zdarzeń i błędów, które wystąpiły w programie. Jego zadaniem jest ułatwianie rozwiązywania problemów przez administratorów i użytkowników systemu. Zawarte w nim informacje często mogą pomóc znaleźć rozwiązanie problemu występującego w programie.
- **Skanowanie komputera** — w tym oknie wyświetlane są wszystkie wyniki skanowania. Każdy wiersz odpowiada jednej operacji skanowania. Dwukrotne kliknięcie dowolnego wpisu powoduje wyświetlenie szczegółowych informacji na temat danej operacji skanowania.
- **System HIPS** — zawiera zapisy związane z określonymi regułami, które zostały zaznaczone do rejestrowania. Pozycje dziennika zawierają informacje o aplikacji, która wywołała operację, wyniku (zezwolenie lub zablokowanie reguły) oraz nazwie utworzonej reguły.
- **Zapora osobista** — w dzienniku zapory są wyświetlane wszystkie ataki zdalne wykryte przez zaporę osobistą. Zawiera on informacje o wszystkich atakach skierowanych przeciwko danemu komputerowi. W kolumnie *Zdarzenie* są wymienione wykryte ataki. W kolumnie *Obiekt źródłowy* znajdują się informacje o intruzie. W kolumnie *Protokół* podany jest protokół sieciowy wykorzystany podczas ataku. Analiza dziennika zapory może pomóc w odpowiednio wczesnym wykryciu próby zainfekowania komputera, dzięki czemu można zapobiec nieautoryzowanemu dostępowi do systemu. Więcej szczegółowych informacji dotyczących określonych ataków sieciowych można znaleźć w sekcji IDS i opcje zaawansowane.
- **Filtrowane witryny internetowe** — Ta lista umożliwia przeglądanie listy witryn zablokowanych przez funkcje Ochrona dostępu do stron internetowych lub Kontrola dostępu do stron internetowych. W dziennikach odnotowane są: czas, adres URL, nazwa użytkownika oraz aplikacja, która nawiązała połączenie z daną witryną.
- **Ochrona przed spamem** — zawiera zapisy dotyczące wiadomości e-mail oznaczonych jako spam.
- **Kontrola dostępu do stron internetowych** — wyświetla zablokowane lub dozwolone adresy URL i szczegółowe dane dotyczące sposobu ich kategoryzacji. Kolumna *Wykonana czynność* zawiera informacje o sposobie, w jaki zostały zastosowane reguły filtrowania.
- **Kontrola dostępu do urządzeń** — zawiera zapisy związane z nośnikami wymiennymi i urządzeniami, które były podłączane do komputera. W pliku dziennika zapisywane są informacje dotyczące tylko tych urządzeń, z którymi są związane reguły kontroli dostępu do urządzeń. Jeśli dana reguła nie odpowiada podłączonemu urządzeniu, nie jest dla niego tworzony wpis w dzienniku. Można tu również znaleźć takie szczegóły jak typ urządzenia, numer seryjny, nazwa dostawcy i rozmiar nośnika (jeśli jest dostępny).

Informacje wyświetlane w każdym obszarze okna można skopiować do schowka, zaznaczając żądaną pozycję i klikając przycisk **Kopiuj** (lub naciskając klawisze **Ctrl+C**). Do zaznaczenia wielu pozycji można użyć klawiszy **Ctrl** i **Shift**.

Kliknięcie opcji **Filtrowanie** umożliwia otwarcie okna **Filtrowanie dziennika**, w którym można zdefiniować kryteria filtrowania.

Kliknięcie prawym przyciskiem myszy określonego rekordu powoduje wyświetlenie menu kontekstowego. W menu kontekstowym są dostępne następujące opcje:

- **Pokaż** — umożliwia wyświetlenie w nowym oknie szczegółowych informacji na temat wybranego dziennika.
- **Filtruj same rekordy** — po aktywacji tego filtru widoczne będą tylko rekordy tego samego typu (diagnostyczne, ostrzeżenia itd.).
- **Filtruj/Znajdź** — po kliknięciu tej opcji w oknie Wyszukaj w dzienniku można zdefiniować kryteria filtrowania dla określonych wpisów w dzienniku.
- **Włącz filtr** — umożliwia aktywację ustawień filtra.
- **Wyłącz filtr** — umożliwia wyczyszczenie wszystkich ustawień filtrowania (opisanych powyżej).
- **Kopiuj/Kopiuj wszystko** — umożliwia skopiowanie danych dotyczących wszystkich rekordów wyświetlanych w oknie.
- **Usuń/Usuń wszystko** — umożliwia usunięcie wybranych rekordów albo wszystkich wyświetlanych rekordów (konieczne jest posiadanie uprawnień administratora).
- **Eksportuj...** — umożliwia wyeksportowanie danych dotyczących rekordów w formacie XML.
- **Eksportuj wszystko...** — umożliwia wyeksportowanie informacji o wszystkich rekordach w formacie XML.
- **Przewijaj dziennik** — pozostawienie tej opcji włączonej powoduje, że w oknie **Pliki dziennika** stare dzienniki są przewijane automatycznie i wyświetlane są aktywne dzienniki.

3.9.6.1.1 Wyszukaj w dzienniku

W dziennikach są przechowywane informacje o ważnych zdarzeniach systemowych. Funkcja filtrowania dziennika umożliwia wyświetlenie rekordów dotyczących określonego typu zdarzenia.

Podaj szukane słowo kluczowe w polu **Znajdź tekst**. Aby wyszukać słowo kluczowe tylko w określonych kolumnach, zmień stosowany filtr na liście rozwijanej **Wyszukaj w kolumnach**.

Typy rekordów — wybierz jeden lub więcej typów rekordów dziennika na liście rozwijanej:

- **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszenia konfiguracji programu, a także wszystkich rekordów wyższych kategorii.
- **Informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Błędy** — rejestrowanie błędów typu „Błąd podczas pobierania pliku” oraz błędów krytycznych.
- **Krytyczne** — rejestrowanie tylko błędów krytycznych (np. błąd uruchomienia ochrony antywirusowejlub wbudowanej zapory).

Okres — podaj okres, z którego mają pochodzić rekordy wyświetlane w wynikach wyszukiwania.

Tylko całe wyrazy — zaznacz to pole wyboru, aby wyszukać określone całe wyrazy w celu zawężenia wyników.

Uwzględniaj wielkość liter — włącz tę opcję, jeśli istotne jest, czy litery tekstu są wielkie, czy małe.

Szukaj w górę — wyniki wyszukiwania znajdujące się wyżej w dokumencie będą wyświetlane w pierwszej kolejności.

3.9.6.2 Ustawienia serwera proxy

W dużych sieciach lokalnych komputery mogą komunikować się z Internetem za pośrednictwem serwera proxy. Korzystając z tych opcji konfiguracji można zdefiniować następujące ustawienia. W przeciwnym razie program nie będzie mógł być automatycznie aktualizowany. W programie ESET Endpoint Security ustawienia serwera proxy są dostępne w dwóch sekcjach drzewa ustawień zaawansowanych.

Po pierwsze ustawienia serwera proxy można skonfigurować w oknie **Ustawienia zaawansowane**, klikając kolejno opcje **Narzędzia** > **Serwer proxy**. Określenie serwera proxy na tym poziomie powoduje zdefiniowanie globalnych ustawień serwera proxy dla całego programu ESET Endpoint Security. Wprowadzone w tym miejscu parametry będą używane przez wszystkie moduły, które wymagają połączenia internetowego.

Aby określić ustawienia serwera proxy na tym poziomie, zaznacz pozycję **Użyj serwera proxy**, a następnie wprowadź adres serwera proxy w polu **Serwer proxy** oraz jego numer portu — w polu **Port**.

Jeśli komunikacja z serwerem proxy wymaga uwierzytelniania, zaznacz pozycję **Serwer proxy wymaga uwierzytelniania** i w odpowiednich polach wprowadź **nazwę użytkownika** i **hasło**. Kliknięcie przycisku **Wykryj** spowoduje automatyczne wykrycie i wprowadzenie ustawień serwera proxy. Zostaną skopiowane parametry określone w programie Internet Explorer.

UWAGA: Nazwę użytkownika oraz hasło należy wprowadzić w ustawieniach **serwera proxy** ręcznie.

Ustawienia serwera proxy można również skonfigurować w obszarze Ustawienia zaawansowane (**Ustawienia zaawansowane** > **Aktualizacja** > **Serwer proxy HTTP**, wybierając opcję **Połączenie przez serwer proxy** z menu rozwijanego **Tryb proxy**). Te ustawienia mają zastosowanie do danego profilu aktualizacji i są zalecane w odniesieniu do komputerów przenośnych, ponieważ w ich przypadku aktualizacje sygnatur wirusów są często pobierane z lokalizacji zdalnych. Więcej informacji na temat tego ustawienia można znaleźć w sekcji Zaawansowane ustawienia aktualizacji.

3.9.6.3 Harmonogram

Harmonogram służy do zarządzania zaplanowanymi zadaniami i uruchamiania ich ze wstępnie zdefiniowaną konfiguracją.

Dostęp do harmonogramu można uzyskać z poziomu głównego okna programu ESET Endpoint Security, klikając **Narzędzia** > **Harmonogram**. Okno **Harmonogram** zawiera listę wszystkich zaplanowanych zadań oraz ich skonfigurowane właściwości, takie jak wstępnie zdefiniowany dzień, godzina i używany profil skanowania.

Okno Harmonogram umożliwia planowanie następujących zadań: aktualizowanie bazy sygnatur wirusów, skanowanie, sprawdzanie plików przy uruchamianiu systemu i administrowanie dziennikami. Zadania można dodawać i usuwać bezpośrednio w oknie Harmonogramu, klikając przycisk **Dodaj zadanie** lub **Usuń** widoczny w jego dolnej części. Klikając prawym przyciskiem myszy w oknie Harmonogramu zadań, można: wyświetlić szczegółowe informacje, zażądać natychmiastowego wykonania zadania, dodać nowe zadanie lub usunąć istniejące zadanie. Poszczególne pozycje można aktywować i dezaktywować za pomocą wyświetlanych obok nich pól wyboru.

Domyślnie w oknie **Harmonogram** są wyświetlane następujące zaplanowane zadania:

- **Administracja dziennikami**
- **Regularna aktualizacja automatyczna**
- **Aktualizacja automatyczna po nawiązaniu połączenia modemowego**
- **Aktualizacja automatyczna po zalogowaniu użytkownika**
- **Automatyczne sprawdzanie plików przy uruchamianiu** (po zalogowaniu użytkownika)
- **Automatyczne sprawdzanie plików przy uruchamianiu** (po pomyślnej aktualizacji bazy sygnatur wirusów)
- **Automatyczne pierwsze skanowanie**

Aby zmodyfikować konfigurację istniejącego zaplanowanego zadania (zarówno domyślnego, jak i zdefiniowanego przez użytkownika), kliknij prawym przyciskiem myszy zadanie i wybierz opcję **Edytuj...** lub wybierz zadanie, które ma zostać zmodyfikowane, i kliknij przycisk **Edytuj**.

Dodawanie nowego zadania

1. Kliknij przycisk **Dodaj zadanie** w dolnej części okna.
2. Wprowadź nazwę zadania.

3. Wybierz odpowiednie zadanie z menu rozwijanego:

- **Uruchom aplikację zewnętrzną** — umożliwia zaplanowanie uruchomienia aplikacji zewnętrznej.
- **Administracja dziennikami** — pliki dziennika zawierają także pozostałości usuniętych rekordów. To zadanie regularnie przeprowadza optymalizację rekordów w plikach dzienników w celu usprawnienia działania.
- **Sprawdzanie plików przy uruchamianiu systemu** — umożliwia sprawdzenie plików, które mogą być wykonywane podczas uruchamiania systemu lub logowania.
- **Tworzenie skanowania komputera** — tworzy migawkę stanu komputera w programie ESET SysInspector, gromadząc szczegółowe informacje dotyczące komponentów systemu (na przykład sterowników i aplikacji) wraz z oceną poziomu ryzyka w odniesieniu do każdego komponentu.
- **Skanowanie komputera na żądanie** — umożliwia skanowanie plików i folderów na komputerze.
- **Pierwsze skanowanie** — domyślnie 20 minut po zakończeniu instalacji lub ponownym uruchomieniu, zostanie przeprowadzone skanowanie komputera jako zadanie o niskim priorytecie.
- **Aktualizacja** — umożliwia zaplanowanie zadania polegającego na aktualizowaniu bazy sygnatur wirusów i aktualizowaniu modułów programu.

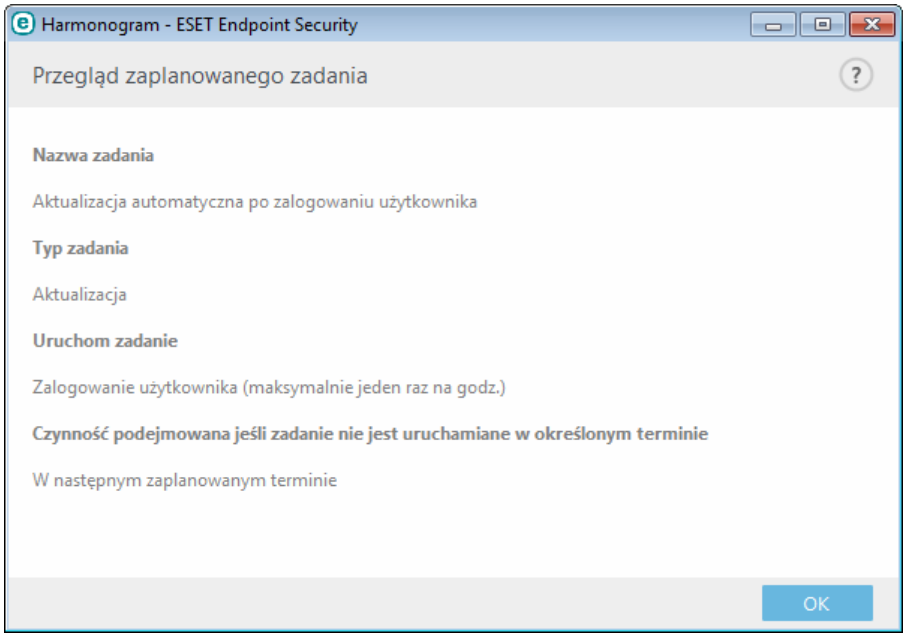
4. W celu aktywowania zadania należy użyć przełącznika **Włączono** (można to zrobić później poprzez zaznaczenie lub odznaczenie pola wyboru na liście zaplanowanych zadań), kliknąć **Dalej** i wybrać jedną z opcji określających częstotliwość jego wykonywania:

- **Jednorazowo** — zadanie zostanie wykonane w wybranym dniu o wybranej godzinie.
- **Wielokrotnie** — zadanie będzie wykonywane w określonych przedziałach czasowych.
- **Codziennie** — zadanie będzie uruchamiane codziennie o określonej godzinie.
- **Cotygodniowo** — zadanie będzie wykonywane w wybranym dniu tygodnia o ustalonej godzinie.
- **Po wystąpieniu zdarzenia** — zadanie będzie wykonywane po wystąpieniu określonego zdarzenia.

5. Wybranie opcji **Pomiń zadanie, gdy komputer jest zasilany z baterii** umożliwia zminimalizowanie wykorzystania zasobów systemowych, gdy komputer działa na zasilaniu akumulatorowym. Zadanie zostanie uruchomione w dniu tygodnia i o godzinie, które wskazano w polach **Wykonanie zadania**. Jeśli zadanie nie mogło zostać uruchomione o ustalonej porze, można określić, kiedy ma zostać wykonane ponownie:

- **W następnym zaplanowanym terminie**
- **Jak najwcześniej**
- **Natychmiast, gdy czas od ostatniego uruchomienia przekroczy określoną wartość** (interwał można określić za pomocą pola przewijania **Czas od ostatniego uruchomienia**)

Zaplanowane zadanie można przejrzeć po kliknięciu go prawym przyciskiem i wybraniu opcji **Pokaż szczegóły zadania**.



3.9.6.4 Statystyki ochrony

Aby wyświetlić wykres danych statystycznych dotyczących modułów ochrony programu ESET Endpoint Security, należy kliknąć opcję **Narzędzia** > **Statystyki ochrony**. Z rozwijanego menu **Statystyka** należy wybrać żądany moduł ochrony, aby wyświetlić odpowiedni wykres i legendę. Po wskazaniu kursorem pozycji w legendzie na wykresie wyświetlone zostaną tylko dane dotyczące tej pozycji.

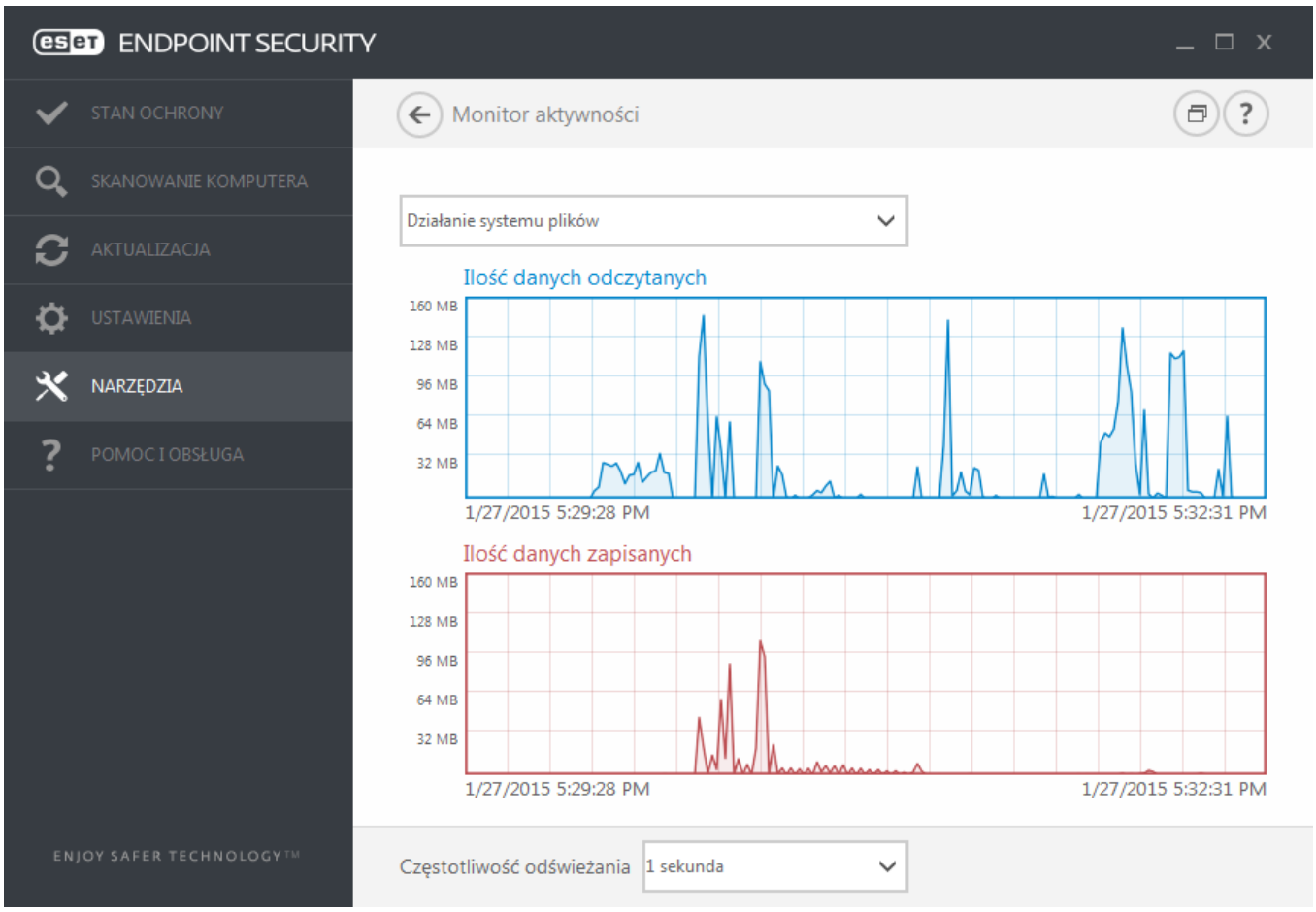
Dostępne są następujące wykresy statystyczne:

- **Ochrona antywirusowa i antyspyware** — wyświetla liczbę zarażonych i wyleczonych obiektów.
- **Ochrona systemu plików** — wyświetlane są tylko obiekty odczytane z systemu plików lub w nim zapisane.
- **Ochrona programów poczty e-mail** — zawiera jedynie obiekty wysłane lub odebrane za pośrednictwem programów poczty e-mail.
- **Ochrona dostępu do stron internetowych i ochrona przed atakami typu „phishing”** — wyświetlane są tylko obiekty pobrane przez przeglądarki internetowe.
- **Ochrona przed spamem programów poczty e-mail** — udostępnia historię statystyki antyspamowej od ostatniego uruchomienia.

Obok wykresów danych statystycznych wyświetlana jest liczba wszystkich przeskanowanych obiektów, liczba zainfekowanych obiektów, liczba wyleczonych obiektów oraz liczba niezainfekowanych obiektów. Kliknięcie pozycji **Resetuj** umożliwia usunięcie danych statystycznych, a kliknięcie pozycji **Resetuj wszystkie** — usunięcie wszystkich istniejących danych.

3.9.6.5 Monitor aktywności

Aby wyświetlić aktualny wykres **Działanie systemu plików**, kliknij opcję **Narzędzia** > **Monitor aktywności**. U dołu wykresu znajduje się oś czasu, na której w czasie rzeczywistym rejestrowane są działania w systemie plików (na podstawie wybranego przedziału czasowego). Aby zmienić czas trwania tego przedziału, wybierz odpowiednią wartość z menu rozwijanego **Częstotliwość odświeżania**.



Dostępne są następujące opcje:

- **Krok: 1 sekunda** — wykres jest odświeżany co sekundę, a oś czasu odpowiada ostatnim 10 minutom.
- **Krok: 1 minuta (ostatnie 24 godziny)** — wykres jest odświeżany co minutę, a oś czasu odpowiada ostatnim 24 godzinom.
- **Krok: 1 godzina (ostatni miesiąc)** — wykres jest odświeżany co godzinę, a oś czasu odpowiada ostatniemu miesiącowi.
- **Krok: 1 godzina (wybrany miesiąc)** — wykres jest odświeżany co godzinę, a oś czasu odpowiada ostatnim X wybranym miesiącom.

Na osi pionowej w obszarze **Wykres działań w systemie plików** prezentowana jest ilość danych odczytanych (kolor niebieski) i zapisanych (kolor czerwony). Obydwie wartości są podawane w KB/MB/GB. Po wskazaniu kursorem danych odczytanych lub zapisanych (na legendzie umieszczonej pod wykresem) wyświetlane będą tylko dane dotyczące wybranego typu działania.

Można także wybrać **Działanie w sieci** z menu rozwijanego. Wykres oraz opcje dla ustawienia **Działania w systemie plików** i **Działanie w sieci** są identyczne, ale w drugim przypadku prezentowana jest ilość danych odebranych (kolor niebieski) i wysłanych (kolor czerwony).

3.9.6.6 ESET SysInspector

ESET SysInspector to aplikacja dokładnie sprawdzająca komputer, przeprowadzająca szczegółową analizę komponentów systemu, na przykład sterowników i aplikacji, połączeń sieciowych lub ważnych wpisów w rejestrze, oraz oceniająca poziom ryzyka w odniesieniu do każdego komponentu. Na podstawie tych informacji można określić przyczynę podejrzanego zachowania systemu, które może wynikać z niezgodności oprogramowania lub sprzętu bądź zarażenia szkodliwym oprogramowaniem.

W oknie programu SysInspector wyświetlane są następujące informacje na temat utworzonych dzienników:

- **Godzina** — godzina utworzenia dziennika.
- **Komentarz** — krótki komentarz.
- **Użytkownik** — nazwa użytkownika, który utworzył dziennik.
- **Stan** — stan procesu tworzenia dziennika.

Dostępne są następujące czynności:

- **Otwórz** — powoduje otwarcie utworzonego dziennika. Można również kliknąć dany plik dziennika prawy przyciskiem myszy i z menu kontekstowego wybrać opcję **Pokaż**.
- **Porównaj** — umożliwia porównanie dwóch istniejących dzienników.
- **Utwórz...** — umożliwia utworzenie nowego dziennika. Przed podjęciem próby uzyskania dostępu do dziennika należy poczekać, aż narzędzie ESET SysInspector zakończy działanie (zostanie wyświetlony stan dziennika Utworzono).
- **Usuń** — powoduje usunięcie wybranych dzienników z listy.

W menu kontekstowym wyświetlanym po wybraniu jednego lub większej liczby dzienników dostępne są następujące pozycje:

- **Pokaż** — umożliwia otwarcie wybranego dziennika w programie ESET SysInspector (tak samo jak po dwukrotnym kliknięciu dziennika).
- **Porównaj** — umożliwia porównanie dwóch istniejących dzienników.
- **Utwórz...** — umożliwia utworzenie nowego dziennika. Przed podjęciem próby uzyskania dostępu do dziennika należy poczekać, aż narzędzie ESET SysInspector zakończy działanie (zostanie wyświetlony stan dziennika Utworzono).
- **Usuń wszystko** — powoduje usunięcie wszystkich dzienników.
- **Eksportuj...** — umożliwia wyeksportowanie dziennika do pliku *.xml* lub skompresowanego pliku *.xml*.

3.9.6.7 ESET Live Grid

ESET Live Grid to zaawansowany system wczesnego ostrzegania wykorzystujący kilka opartych na chmurze technologii. Pomaga wykrywać nowe zagrożenia na podstawie reputacji i poprawia skuteczność skanowania dzięki białym listom. Informacje o nowych zagrożeniach są przesyłane strumieniowo w czasie rzeczywistym do chmury, dzięki czemu laboratorium antywirusowe firmy ESET jest w stanie szybko reagować i zapewnić stały poziom ochrony. Użytkownik może sprawdzić reputację działających procesów i plików bezpośrednio z poziomu interfejsu programu lub menu kontekstowego, korzystając z dodatkowych informacji dostępnych dzięki technologii ESET Live Grid. Podczas instalacji produktu ESET Endpoint Security należy wybrać jedną z następujących opcji:

1. Użytkownik może nie włączać technologii ESET Live Grid. Nie spowoduje to utraty żadnych funkcji oprogramowania, jednak w niektórych przypadkach program ESET Endpoint Security może reagować na nowe zagrożenia wolniej niż w ramach aktualizacji bazy sygnatur wirusów.
2. W systemie ESET Live Grid można skonfigurować przesyłanie anonimowych informacji o nowych zagrożeniach i lokalizacjach nowego niebezpiecznego kodu, który został wykryty. Ten plik może być przesyłany do firmy ESET w celu szczegółowej analizy. Zbadanie zagrożeń pomoże firmie ESET ulepszać metody ich wykrywania.

System ESET Live Grid zgromadzi informacje o komputerze użytkownika powiązane z nowo wykrytymi zagrożeniami. Te informacje mogą zawierać próbkę lub kopię pliku, w którym wystąpiło zagrożenie, ścieżkę dostępu do tego pliku, nazwę pliku, datę i godzinę, proces, za którego pośrednictwem zagrożenie pojawiło się na komputerze, oraz informacje o systemie operacyjnym komputera.

Domyślnie w programie ESET Endpoint Security skonfigurowane jest przesyłanie podejrzanych plików do szczegółowej analizy w laboratorium firmy ESET. Pliki z określonymi rozszerzeniami, takimi jak *doc* lub *xls*, są zawsze wyłączane z procesu przesyłania. Można również dodać inne rozszerzenia, jeśli istnieją pliki, które użytkownik lub jego firma życzy sobie wyłączyć z procesu przesyłania.

System reputacji ESET Live Grid obejmuje działającą w chmurze białą listę i czarną listę. Dostęp do ustawień technologii ESET Live Grid można uzyskać po naciśnięciu klawisza **F5** w celu przejścia do obszaru Ustawienia zaawansowane, po czym należy przejść do pozycji **Narzędzia** > **ESET Live Grid**.

Włącz system reputacji ESET Live Grid (zalecane) — system reputacji ESET Live Grid poprawia wydajność rozwiązań firmy ESET do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.

Przesyłaj anonimowe statystyki — umożliwia firmie ESET gromadzenie informacji o nowo wykrytych zagrożeniach, takich jak nazwa zagrożenia, data i godzina jego wykrycia, metoda wykrycia i skojarzone metadane, wersja i konfiguracja produktu, w tym informacje o systemie.

Prześlij pliki — podejrzane pliki przypominające zagrożenia lub pliki, których zawartość lub działanie jest nietypowe, są przesyłane do firmy ESET w celu wykonania analizy.

Wybranie opcji **Włącz zapisywanie w dzienniku** powoduje utworzenie dziennika zdarzeń, w którym będą rejestrowane wysyłane pliki i informacje statystyczne. Umożliwia to dodawanie zapisów w dzienniku zdarzeń podczas wysyłania plików lub danych statystycznych.

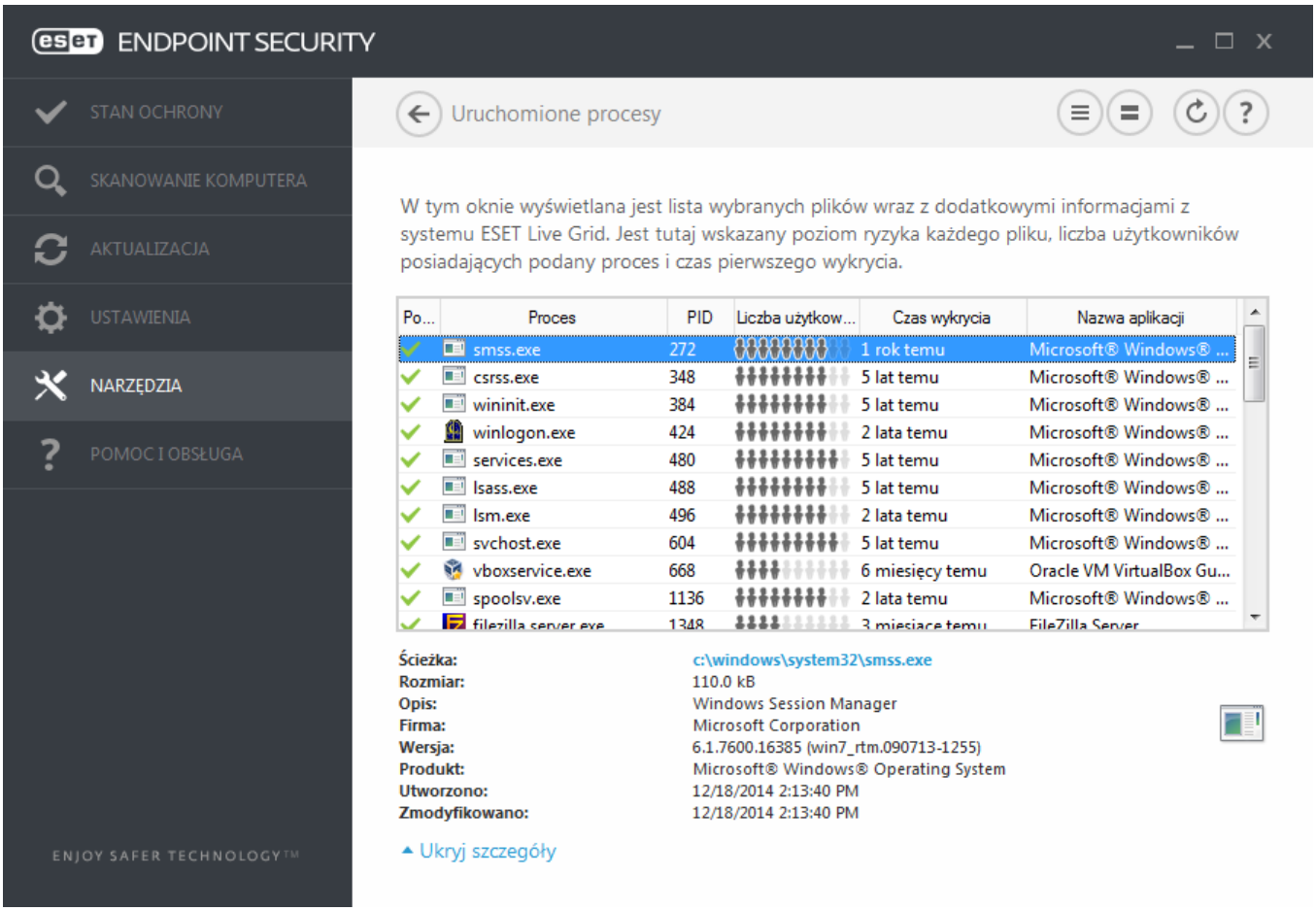
Kontaktowy adres e-mail (opcjonalnie) — wraz z podejrzanymi plikami można wysyłać adres e-mail, który będzie używany do kontaktowania się z użytkownikiem, gdy przeprowadzenie analizy będzie wymagało dodatkowych informacji. Należy pamiętać, że specjaliści z firmy ESET kontaktują się z użytkownikiem tylko w szczególnych przypadkach, gdy wymagane są dodatkowe informacje.

Wyłączenia — filtr wyłączeń umożliwia wyłączenie określonych plików lub folderów z przesyłania (może na przykład posłużyć do wyłączenia plików zawierających dane poufne, takich jak dokumenty lub arkusze kalkulacyjne). Wymienione pliki nigdy nie będą wysyłane do analizy w firmie ESET, nawet jeśli będą zawierały podejrzany kod. Najpopularniejsze typy plików należących do tej kategorii (np. DOC) są wyłączone domyślnie. Do listy wyłączonych plików można dodawać inne typy plików.

Jeśli system ESET Live Grid był używany wcześniej i został wyłączony, mogą jeszcze pozostawać pakiety do wysłania. Takie pakiety zostaną wysłane do firmy ESET nawet po dezaktywacji. Po przesłaniu wszystkich bieżących informacji nie będą już tworzone nowe pakiety.

3.9.6.8 Uruchomione procesy

Funkcja Uruchomione procesy wyświetla uruchomione na komputerze programy lub procesy oraz natychmiastowo i w sposób ciągły informuje firmę ESET o nowych infekcjach. Program ESET Endpoint Security dostarcza szczegółowych informacji o uruchomionych procesach i chroni użytkowników dzięki zastosowaniu technologii ESET Live Grid.



Poziom ryzyka — w większości przypadków produkt ESET Endpoint Security i technologia ESET Live Grid przypisują obiektom (plikom, procesom, kluczom rejestru itd.) poziomy ryzyka, używając do tego wielu reguł heurystyki. Na podstawie tych reguł badana jest charakterystyka danego obiektu, a następnie oceniana możliwość jego szkodliwego działania. Na podstawie analizy heurystycznej obiektom przypisywane są poziomy ryzyka od 1 (Czysty — kolor zielony) do 9 (Ryzykowny — kolor czerwony).

Proces — nazwa obrazu programu lub procesu, który jest obecnie uruchomiony na komputerze. Aby zobaczyć wszystkie procesy uruchomione na komputerze, można również skorzystać z Menedżera zadań systemu Windows. Aby otworzyć Menedżera zadań, należy kliknąć prawym przyciskiem myszy puste miejsce na pasku zadań i kliknąć opcję Menedżer zadań albo nacisnąć klawisze **Ctrl**+**Shift**+**Esc** na klawiaturze.

PID — jest to identyfikator uruchomionych procesów w systemach operacyjnych Windows.

UWAGA: Znane aplikacje oznaczone jako Czysty (kolor zielony) są całkowicie bezpieczne (biała lista) i zostaną wyłączone ze skanowania, co zwiększy prędkość skanowania dostępnego po włączeniu opcji Skanowanie komputera i Ochrona systemu plików w czasie rzeczywistym na komputerze użytkownika.

Liczba użytkowników — liczba użytkowników korzystających z danej aplikacji. Te informacje są zbierane przez technologię ESET Live Grid.

Czas wykrycia — okres od wykrycia aplikacji przez technologię ESET Live Grid.

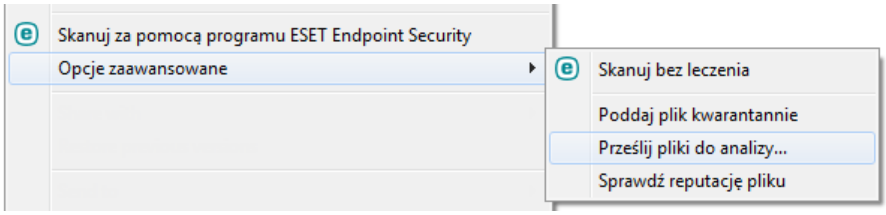
Uwaga: Poziom bezpieczeństwa aplikacji oznaczony jako Nieznany (kolor pomarańczowy) nie zawsze wskazuje, że stanowi ona złośliwe oprogramowanie. Zwykle jest to po prostu nowa aplikacja. W przypadku braku pewności co do bezpieczeństwa pliku można przesłać plik do analizy w laboratorium firmy ESET. Jeśli okaże się, że jest to szkodliwa aplikacja, możliwość jej wykrycia zostanie dodana do jednej z przyszłych aktualizacji bazy sygnatur wirusów.

Nazwa aplikacji — nazwa programu lub procesu.

Kliknięcie danej aplikacji u dołu spowoduje wyświetlenie następujących informacji u dołu okna:

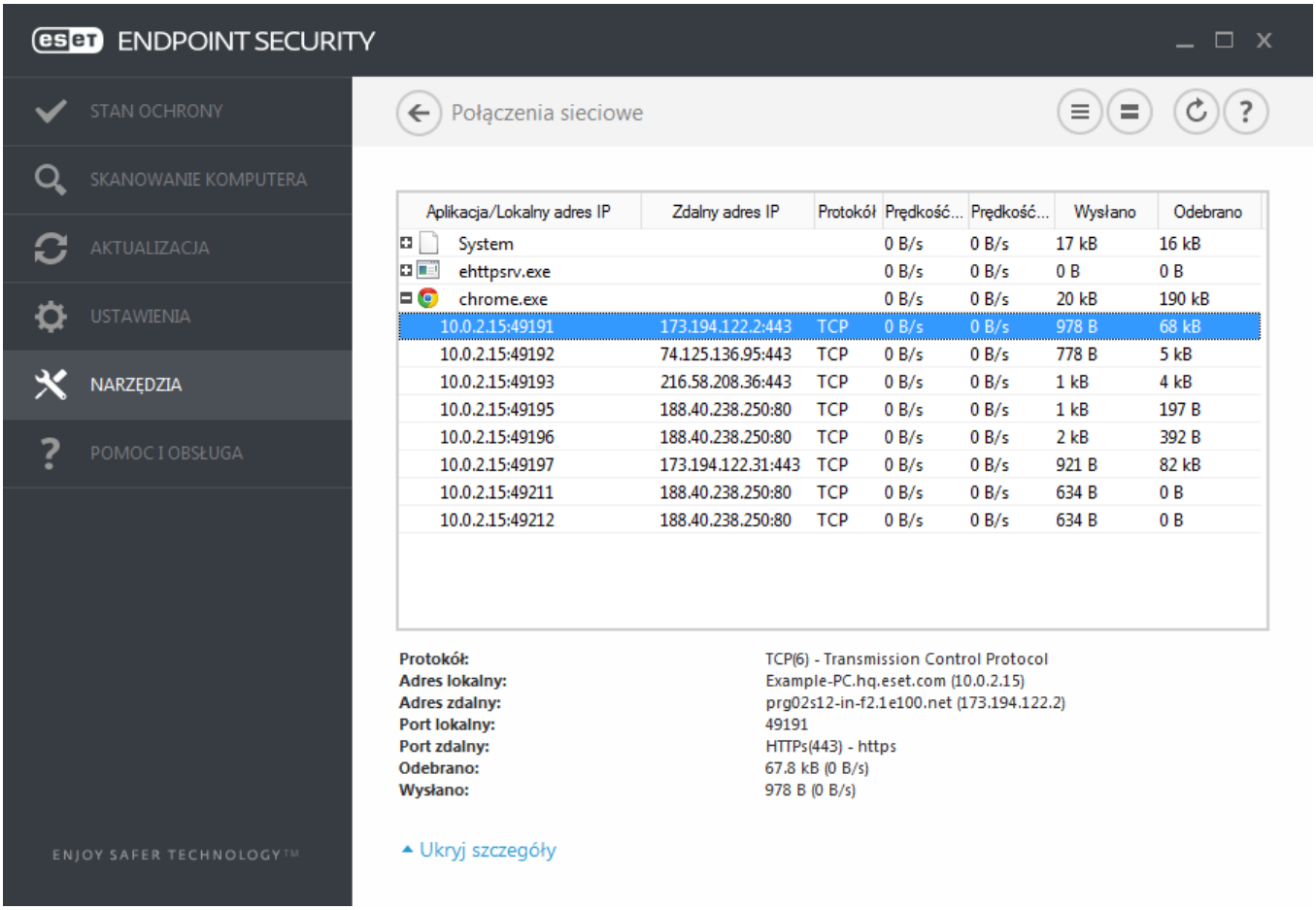
- **Ścieżka** — lokalizacja aplikacji na komputerze.
- **Rozmiar** — rozmiar pliku w kilobajtach (KB) lub megabajtach (MB).
- **Opis** — charakterystyka pliku oparta na jego opisie w systemie operacyjnym.
- **Firma** — nazwa dostawcy lub procesu aplikacji.
- **Wersja** — informacje od wydawcy aplikacji.
- **Produkt** — nazwa aplikacji i/lub nazwa handlowa.
- **Data utworzenia** — data i godzina utworzenia aplikacji.
- **Data modyfikacji** — data i godzina ostatniej modyfikacji aplikacji.

UWAGA: Można również sprawdzić reputację plików, które nie funkcjonują jako uruchomione programy/procesy. W tym celu należy zaznaczyć pliki, które mają zostać sprawdzone, kliknąć je prawym przyciskiem myszy i z menu kontekstowego wybrać kolejno pozycje **Opcje zaawansowane** > **Sprawdź reputację pliku przy użyciu systemu ESET Live Grid**.



3.9.6.9 Połączenia sieciowe

W sekcji Połączenia sieciowe wyświetlana jest lista aktywnych i oczekujących połączeń. Dzięki temu łatwiej jest kontrolować wszystkie aplikacje nawiązujące połączenia wychodzące.



W pierwszym wierszu jest wyświetlana nazwa aplikacji i szybkość transmisji danych. Aby zobaczyć listę połączeń nawiązanych przez aplikację (i inne szczegółowe informacje), należy kliknąć znak **+**.

Kolumny

Aplikacja/Lokalny adres IP — nazwa aplikacji, lokalne adresy IP i porty komunikacyjne.

Zdalny adres IP — adres IP i numer portu konkretnego komputera zdalnego.

Protokół — używany protokół transmisji danych.

Prędkość przekazywania/Prędkość pobierania — bieżąca szybkość wysyłania i odbierania danych.

Wysłano/Odebrano — ilość danych przesłanych w ramach połączenia.

Pokaż szczegóły — wybranie tej opcji pozwala wyświetlić szczegółowe informacje na temat wybranego połączenia.

Zaznaczenie aplikacji lub adresu IP na ekranie Połączenia sieciowe i kliknięcie tej pozycji prawym przyciskiem myszy spowoduje wyświetlenie menu kontekstowego o następującej strukturze:

Rozwiąż nazwy komputerów w sieci — jeśli jest to możliwe, wszystkie adresy sieciowe są wyświetlane w formacie DNS, a nie w postaci liczbowych adresów IP.

Pokaż tylko połączenia TCP — na liście są wyświetlane tylko połączenia realizowane w ramach pakietu protokołów TCP.

Pokaż połączenia nasłuchujące — zaznaczenie tej opcji powoduje wyświetlanie tylko tych połączeń, w których w danym czasie nie odbywa się wymiana danych, ale dla których zarezerwowano w systemie otwarty port i trwa oczekiwanie na nawiązanie komunikacji.

Pokaż połączenia wewnątrz komputera — zaznaczenie tej opcji powoduje wyświetlanie tylko tych połączeń, których stroną zdalną jest system lokalny, czyli tak zwanych połączeń *hosta lokalnego*.

Kliknięcie połączenia prawym przyciskiem myszy powoduje wyświetlenie dodatkowych opcji:

Odmów komunikacji dla połączenia — kończy ustanowione połączenie. Ta opcja jest dostępna tylko po kliknięciu aktywnego połączenia.

Szybkość odświeżania — wybierz częstotliwość odświeżania aktywnych połączeń.

Odśwież teraz — powoduje zaktualizowanie okna Połączenia sieciowe.

Kolejne opcje są dostępne tylko po kliknięciu aplikacji lub procesu, a nie aktywnego połączenia:

Tymczasowo odmów połączenia dla procesu — powoduje odrzucenie bieżących połączeń danej aplikacji. Jeśli zostanie ustanowione nowe połączenie, zapora użyje wstępnie zdefiniowanej reguły. Opis ustawień można znaleźć w sekcji Reguły i strefy.

Tymczasowo zezwól na połączenie procesu — powoduje zezwolenie na bieżące połączenia danej aplikacji. Jeśli zostanie ustanowione nowe połączenie, zapora użyje wstępnie zdefiniowanej reguły. Opis ustawień można znaleźć w sekcji Reguły i strefy.

3.9.6.10 Przesyłanie plików do analizy

Okno dialogowe przesyłania próbek umożliwia wysłanie do firmy ESET pliku lub witryny internetowej do analizy. Aby je otworzyć, należy przejść do opcji **Narzędzia** > **Przesyłanie próbki do analizy**. W przypadku znalezienia na komputerze podejrzanego pliku lub podejrzanej witryny w Internecie, można je wysłać do laboratorium firmy ESET, gdzie zostanie poddany analizie. Jeśli okaże się, że jest to szkodliwa aplikacja lub witryna internetowa, możliwość jej wykrycia zostanie dodana do jednej z przyszłych aktualizacji.

Plik można też przesłać pocztą e-mail. W tym celu należy go skompresować za pomocą programu WinRAR lub WinZIP, szyfrując archiwum przy użyciu hasła „infected”. Tak przygotowane archiwum należy wysłać na adres samples@eset.com. Prosimy pamiętać o wpisaniu opisowego tematu wiadomości i podaniu wszystkich możliwych informacji na temat podejrzanego pliku (może to być np. adres witryny internetowej, z której został on pobrany).

UWAGA: Przed przesłaniem próbki do firmy ESET należy się upewnić, że spełnia ona co najmniej jedno z następujących kryteriów:
- plik lub witryna internetowa nie są w ogóle wykrywane
- plik lub witryna internetowa są błędnie wykrywane jako zagrożenie.

Nie odpowiadamy na otrzymane wiadomości, chyba że do przeprowadzenia analizy potrzebujemy dodatkowych informacji.

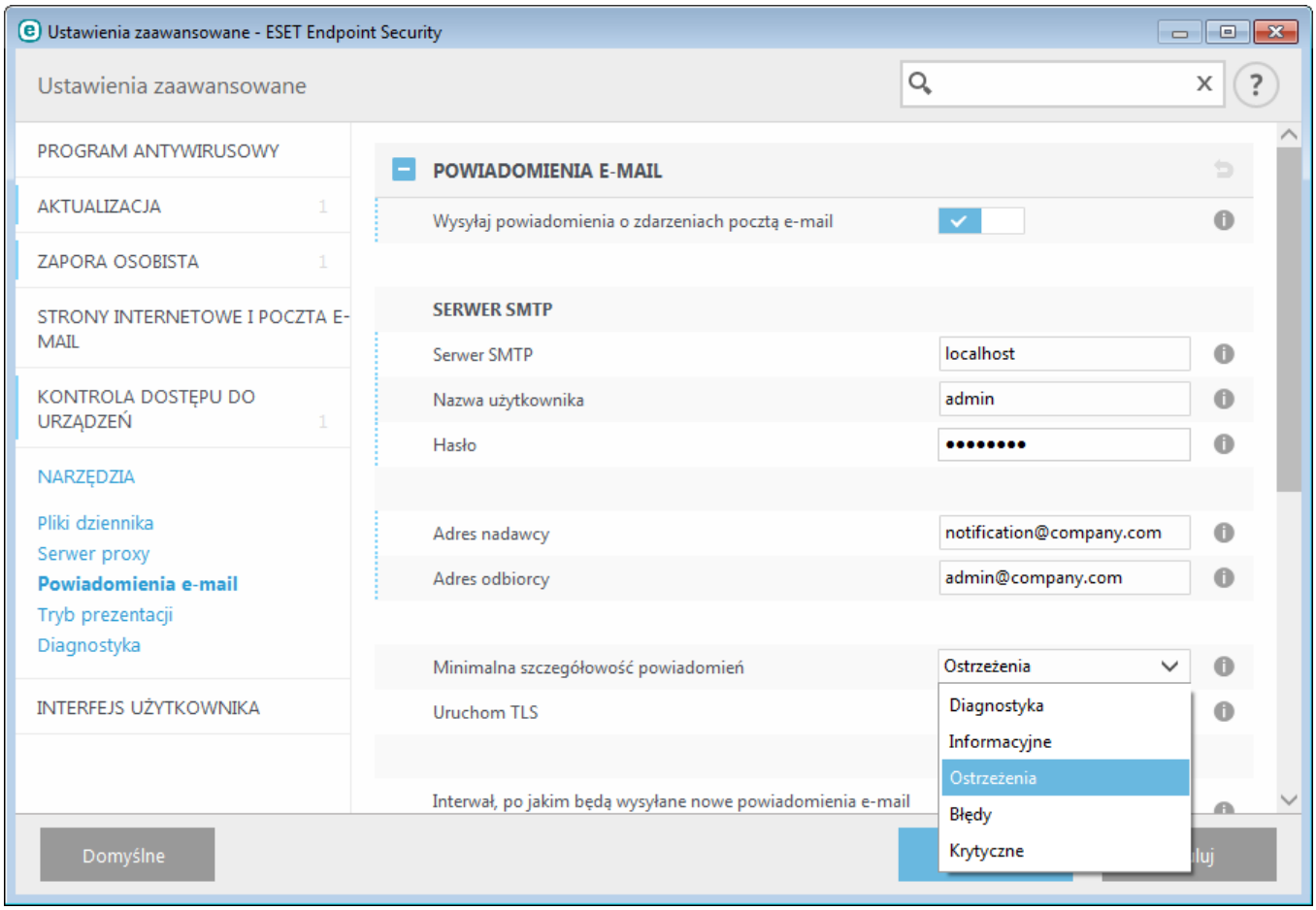
Z menu rozwijanego **Powód przesyłania próbki** należy wybrać opis, który najlepiej charakteryzuje przekazywaną wiadomość:
- **Podejrzany plik**
- **Podejrzana witryna** (witryna internetowa, która jest zainfekowana przez szkodliwe oprogramowanie)
- **Plik z fałszywym alarmem** (plik, który został wykryty jako zainfekowany, ale nie był zainfekowany)
- **Witryna internetowa z fałszywym alarmem**
- **Inne**

Plik/witryna - Ścieżka do pliku lub witryny, którą użytkownik zamierza przesłać.

Kontaktowy adres e-mail — adres ten jest wysyłany do firmy ESET razem z podejrzanymi plikami. Może on zostać wykorzystany w celu nawiązania kontaktu, jeśli analiza wymaga dalszych informacji na temat przesłanych plików. Wprowadzenie adresu kontaktowego jest opcjonalne. Jeśli nie jest to konieczne, firma ESET nie odpowiada na zgłoszenia. Nasze serwery codziennie odbierają dziesiątki tysięcy plików, dlatego nie da się odpowiedzieć każdemu nadawcy.

3.9.6.11 Powiadomienia e-mail

Program ESET Endpoint Security może automatycznie wysyłać powiadomienia e-mail po wystąpieniu zdarzenia o wybranym poziomie szczegółowości. Aby aktywować powiadomienia e-mail, należy włączyć opcję **Wysyłaj powiadomienia o zdarzeniach pocztą e-mail**.



Serwer SMTP

Serwer SMTP — serwer SMTP używany do wysyłania powiadomień (na przykład *smtp.provider.com:587*, wstępnie

zdefiniowany port to 25).

UWAGA: Serwery SMTP z szyfrowaniem TLS są obsługiwane przez program ESET Endpoint Security.

Nazwa użytkownika i **Hasło** — jeśli serwer SMTP wymaga uwierzytelniania, należy wypełnić te pola, podając prawidłową nazwę użytkownika i hasło dostępu do tego serwera SMTP.

Adres nadawcy — w tym polu można wpisać adres nadawcy, który będzie wyświetlany w nagłówkach wiadomości e-mail z powiadomieniami.

Adres odbiorcy — w tym polu można podać adres odbiorcy, który będzie wyświetlany w nagłówkach wiadomości e-mail z powiadomieniami.

Z menu rozwijanego **Minimalna szczegółowość powiadomień** można wybrać początkowy stopień ważności powiadomień, które będą wysyłane.

- **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszenia konfiguracji programu, a także wszystkich rekordów wyższych kategorii.
- **Informacyjne** — rejestrowanie komunikatów informacyjnych, takich jak niestandardowe zdarzenia sieciowe, w tym powiadomień o pomyślnych aktualizacjach, a także wszystkich rekordów wyższych kategorii.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych i komunikatów ostrzegawczych (funkcja Anti-Stealth nie działa prawidłowo lub aktualizacja nie powiodła się).
- **Błędy** — rejestrowanie błędów (np. nieuruchomienie ochrony dokumentów) oraz błędów krytycznych.
- **Krytyczne** — rejestrowanie tylko błędów krytycznych (np. błąd uruchomienia ochrony antywirusowej lub zainfekowanie systemu).

Uruchom TLS — umożliwia wysyłanie alertów i powiadomień z obsługą szyfrowania TLS.

Interwał, po jakim będą wysyłane nowe powiadomienia e-mail (min) — podany w minutach czas, po upływie którego nowe powiadomienia zostaną wysłane w wiadomości e-mail. Ustawienie wartości 0 spowoduje, że powiadomienia będą wysyłane natychmiast.

Wysyłaj każe powiadomienie w osobnej wiadomości e-mail — po włączeniu tej opcji odbiorca będzie otrzymywał osobną wiadomość e-mail z każdym powiadomieniem. Może to zaskutkować znaczną liczbą wiadomości e-mail odebranych w krótkim czasie.

Format wiadomości

Format wiadomości o zdarzeniu — format wiadomości o zdarzeniach wyświetlanych na komputerach zdalnych.

Format wiadomości z ostrzeżeniem o zagrożeniu — alerty o zagrożeniach oraz powiadomienia mają wstępnie zdefiniowany format domyślny. Zaleca się nie zmieniać tego formatu. W pewnych okolicznościach (takich jak korzystanie z automatycznego systemu przetwarzania poczty) zmiana formatu może być jednak konieczna.

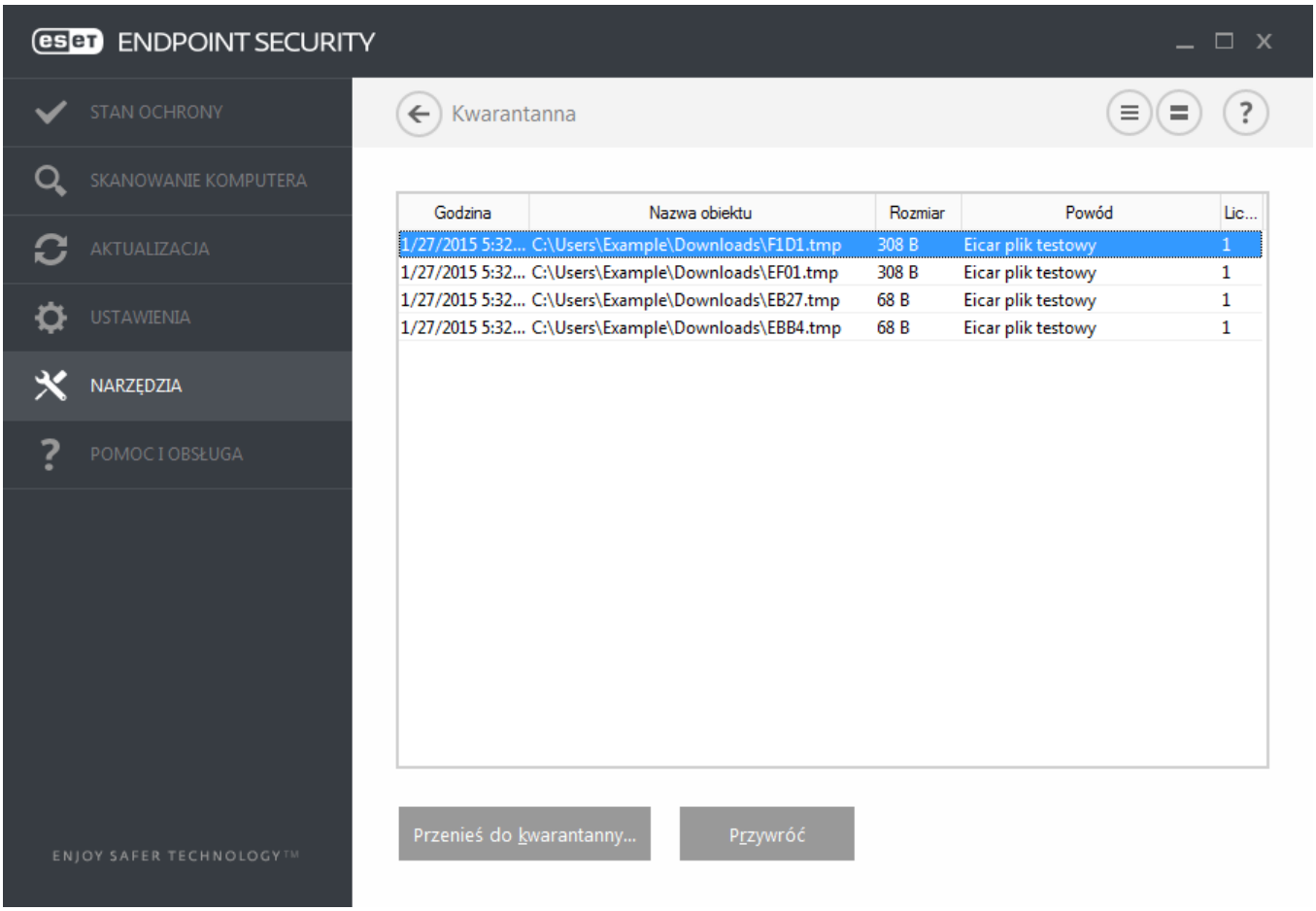
Użyj alfabetu lokalnego — konwertuje wiadomość e-mail z użyciem kodowania znaków ANSI na podstawie ustawień regionalnych systemu Windows (np. windows-1250). W przypadku pozostawienia tej opcji bez zaznaczenia, wiadomość zostanie przekształcona i zakodowana w postaci 7-bitowych znaków ASCII (na przykład „ą” zostanie zamienione na „a”, a nieznane symbole na „?”).

Użyj lokalnego kodowania znaków — źródło wiadomości e-mail zostanie zakodowane w formacie Quoted-printable (QP), w którym wykorzystywane są znaki ASCII oraz prawidłowo przekazywane w wiadomościach e-mail specjalne znaki narodowe w formacie 8-bitowym (ąćęłńóśźż).

3.9.6.12 Kwarantanna

Główną funkcją kwarantanny jest bezpieczne przechowywanie zainfekowanych plików. Pliki należy poddawać kwarantannie w przypadku, gdy nie można ich wyleczyć, gdy ich usunięcie nie jest bezpieczne lub zalecane oraz gdy są one nieprawidłowo wykrywane przez program ESET Endpoint Security.

Kwarantanną można objąć dowolny plik. Takie działanie jest zalecane, jeśli plik zachowuje się w podejrzany sposób, ale nie jest wykrywany przez skaner antywirusowy. Pliki poddane kwarantannie można przesyłać do analizy w laboratorium firmy ESET.



Pliki przechowywane w folderze kwarantanny mogą być wyświetlane w tabeli zawierającej datę i godzinę poddania kwarantannie, ścieżkę do pierwotnej lokalizacji zainfekowanego pliku, rozmiar pliku w bajtach, powód (np. obiekt dodany przez użytkownika) oraz liczbę zagrożeń (np. jeśli plik jest archiwum zawierającym wiele infekcji).

Poddawanie plików kwarantannie

Program ESET Endpoint Security automatycznie poddaje kwarantannie usunięte pliki (jeśli nie wyłączono tej opcji w oknie alertu). W razie potrzeby można ręcznie poddać kwarantannie dowolny podejrzany plik, klikając przycisk **Kwarantanna**. Oryginalny plik zostanie usunięty z pierwotnej lokalizacji. Tę samą czynność można również wykonać z poziomu menu kontekstowego. Należy kliknąć prawym przyciskiem myszy w oknie **Kwarantanna** i wybrać polecenie **Kwarantanna**.

Przywracanie plików z kwarantanny

Pliki poddane kwarantannie można przywrócić do ich pierwotnej lokalizacji. W celu przywrócenia pliku z kwarantanny należy kliknąć prawym przyciskiem myszy w oknie Kwarantanna i wybrać z menu kontekstowego opcję **Przywróć**. Jeśli plik został oznaczony jako potencjalnie niepożądana aplikacja, dostępna będzie również opcja **Przywróć i wyłącz ze skanowania**. Menu kontekstowe zawiera także opcję **Przywróć do...**, umożliwiającą przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.

Usuwanie z kwarantanny — należy kliknąć dany element prawym przyciskiem myszy i wybrać opcję **Usuń z kwarantanny** lub zaznaczyć element, który ma zostać usunięty, i nacisnąć klawisz **Delete** na klawiaturze. Można również zaznaczyć kilka elementów i usunąć je równocześnie.

UWAGA: Jeżeli program przez pomyłkę podda kwarantannie nieszkodliwy plik, po jego przywróceniu należy wyłączyć ten plik ze skanowania i wysłać go do działu obsługi klienta firmy ESET.

Przesyłanie pliku z kwarantanny

Jeśli poddano kwarantannie podejrzany plik, który nie został wykryty przez program, lub jeśli plik został błędnie oceniony jako zagrożenie i poddany kwarantannie, należy go przesłać do laboratorium firmy ESET. Aby przesłać plik z kwarantanny, należy kliknąć go prawym przyciskiem myszy i z menu kontekstowego wybrać polecenie **Prześlij do analizy**.

3.9.6.13 Microsoft Windows Update

Funkcja aktualizacji systemu Windows stanowi istotny element ochrony użytkowników przed szkodliwym oprogramowaniem. Z tego powodu konieczne jest instalowanie aktualizacji systemu Microsoft Windows, gdy tylko stają się dostępne. Program ESET Endpoint Security powiadamia o brakujących aktualizacjach zgodnie z poziomem określonym przez użytkownika. Dostępne są następujące poziomy:

- **Brak aktualizacji** — żadne aktualizacje systemu nie będą proponowane do pobrania.
- **Aktualizacje opcjonalne** — proponowane będzie pobranie aktualizacji o priorytecie niskim lub wyższym.
- **Aktualizacje zalecane** — proponowane będzie pobranie aktualizacji o priorytecie zwykłym lub wyższym.
- **Ważne aktualizacje** — proponowane będzie pobranie aktualizacji o priorytecie „ważne” lub wyższym.
- **Aktualizacje krytyczne** — proponowane będzie tylko pobranie aktualizacji krytycznych.

Aby zapisać zmiany, należy kliknąć przycisk **OK**. Okno Aktualizacje systemu zostanie wyświetlone po sprawdzeniu stanu serwera aktualizacji. Dlatego informacje o aktualizacjach systemu mogą nie być dostępne natychmiast po zapisaniu zmian.

3.9.7 Interfejs użytkownika

W sekcji **Interfejs użytkownika** można skonfigurować działanie graficznego interfejsu użytkownika programu.

Korzystając z narzędzia Elementy interfejsu użytkownika, można dostosować wygląd programu i stosowane w nim efekty wizualne.

Aby zapewnić maksymalne bezpieczeństwo oprogramowania zabezpieczającego, można zapobiec wprowadzaniu w nim wszelkich nieupoważnionych zmian przy użyciu narzędzia Ustawienia dostępu.

Konfigurując ustawienia sekcji Alerty i powiadomienia, można zmienić zachowanie powiadomień systemowych i alertów dotyczących wykrytych zagrożeń. Pozwala to dostosować je do swoich potrzeb.

Jeśli wyświetlanie niektórych powiadomień zostanie wyłączone, będą się one pojawiać w obszarze **Elementy interfejsu użytkownika** > **Stany aplikacji**. Można tam sprawdzić ich stany, a także wyłączyć wyświetlanie tych powiadomień.

Integracja z menu kontekstowym jest wyświetlana po kliknięciu wybranego obiektu prawym przyciskiem myszy. Przy użyciu tego narzędzia można zintegrować elementy sterujące programu ESET Endpoint Security z menu kontekstowym.

Tryb prezentacji jest przydatny dla użytkowników, którzy chcą korzystać z aplikacji bez zakłóceń powodowanych przez wyskakujące okna, zaplanowane zadania czy komponenty mocno obciążające procesor i pamięć RAM.

3.9.7.1 Elementy interfejsu użytkownika

Opcje konfiguracji interfejsu użytkownika w programie ESET Endpoint Security umożliwiają dostosowanie środowiska pracy do potrzeb użytkownika. Te opcje konfiguracji są dostępne w gałęzi **Interfejs użytkownika** > **Elementy interfejsu użytkownika** drzewa ustawień zaawansowanych programu ESET Endpoint Security.

W sekcji **Elementy interfejsu użytkownika** można dostosować środowisko pracy. W menu rozwijanym **Tryb uruchamiania interfejsu GUI** do wyboru są następujące tryby uruchamiania graficznego interfejsu użytkownika (GUI):

Pełny — umożliwia wyświetlanie pełnego interfejsu GUI.

Minimalny — graficzny interfejs użytkownika jest uruchomiony, ale wyświetlane są tylko powiadomienia dla użytkownika.

Ręczny — nie są wyświetlane powiadomienia ani alerty.

Cichy — nie jest wyświetlany graficzny interfejs użytkownika ani powiadomienia i alerty. Ten tryb może być przydatny w sytuacjach, gdy konieczne jest oszczędzanie zasobów systemowych. Tryb Cichy może uruchomić wyłącznie administrator.

UWAGA: Jeśli komputer zostanie uruchomiony ponownie, gdy wybrany jest tryb uruchamiania interfejsu GUI, wyświetlane będą powiadomienia, ale nie graficzny interfejs użytkownika. Aby przywrócić tryb pełny wyświetlania interfejsu GUI, należy uruchomić graficzny interfejs użytkownika jako administrator, z menu Start wybierając kolejno pozycje **Wszystkie programy** > **ESET** > ESET Endpoint Security. Można też zrobić to za pomocą narzędzia ESET Remote Administrator przy użyciu reguły.

Aby wyłączyć ekran powitalny programu ESET Endpoint Security, należy usunąć zaznaczenie opcji **Pokaż ekran powitalny przy uruchamianiu**.

Aby program ESET Endpoint Security emitował sygnał dźwiękowy po wystąpieniu ważnego zdarzenia podczas skanowania, np. po wykryciu zagrożenia lub po zakończeniu skanowania, należy zaznaczyć opcję **Użyj sygnałów dźwiękowych**.

Integruj z menu kontekstowym — włącza integrację elementów sterujących programu ESET Endpoint Security z menu kontekstowym.

Stany

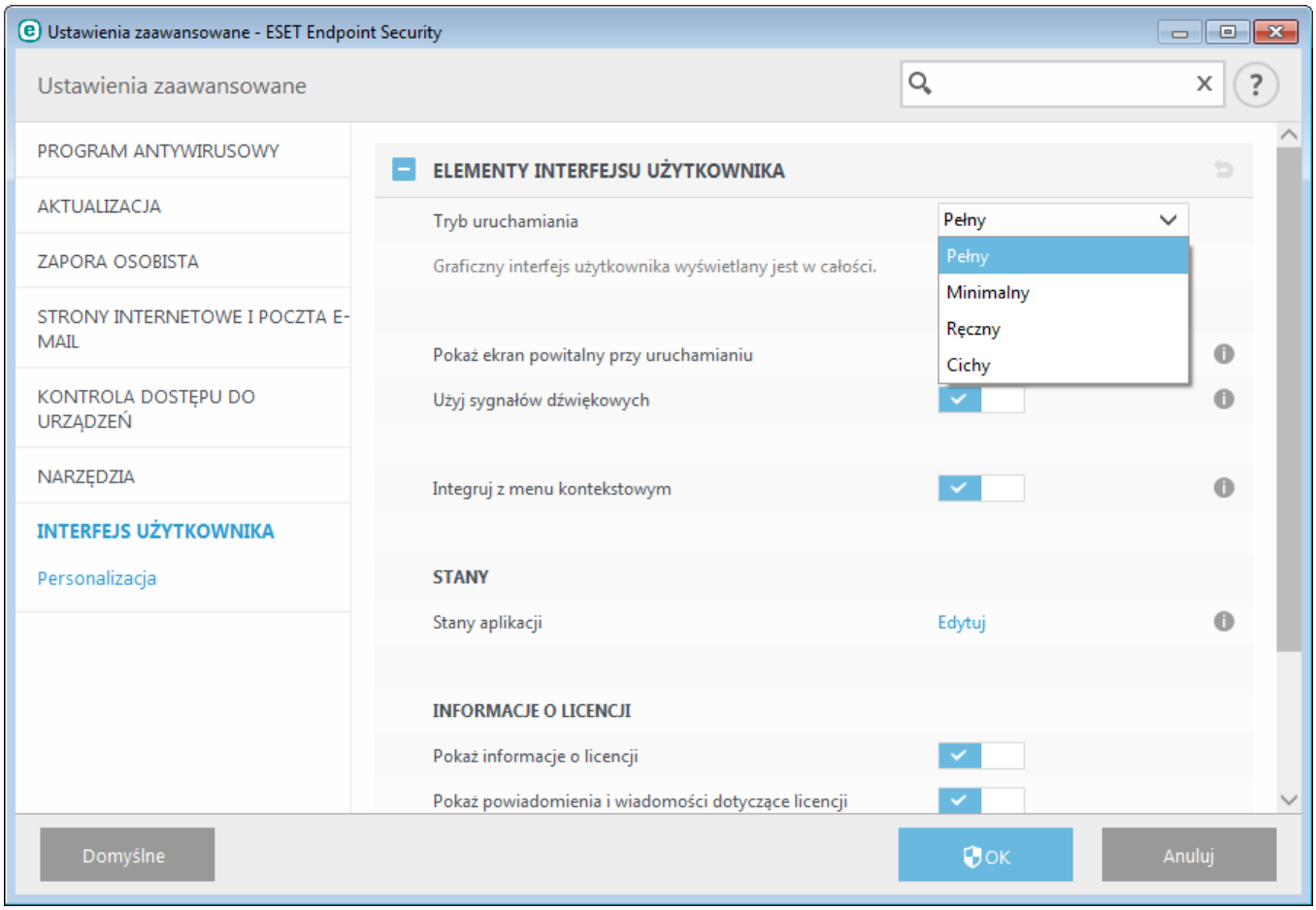
Stany aplikacji — kliknięcie przycisku **Edytuj** umożliwia zarządzanie stanami wyświetlanymi na panelu **Stan ochrony** w menu głównym (ich wyłączanie).

Informacje o licencji

Pokaż informacje o licencji — w przypadku wyłączenia tej opcji informacje o licencji nie będą wyświetlane na ekranie **Stan ochrony** ani **Pomoc i obsługa**.

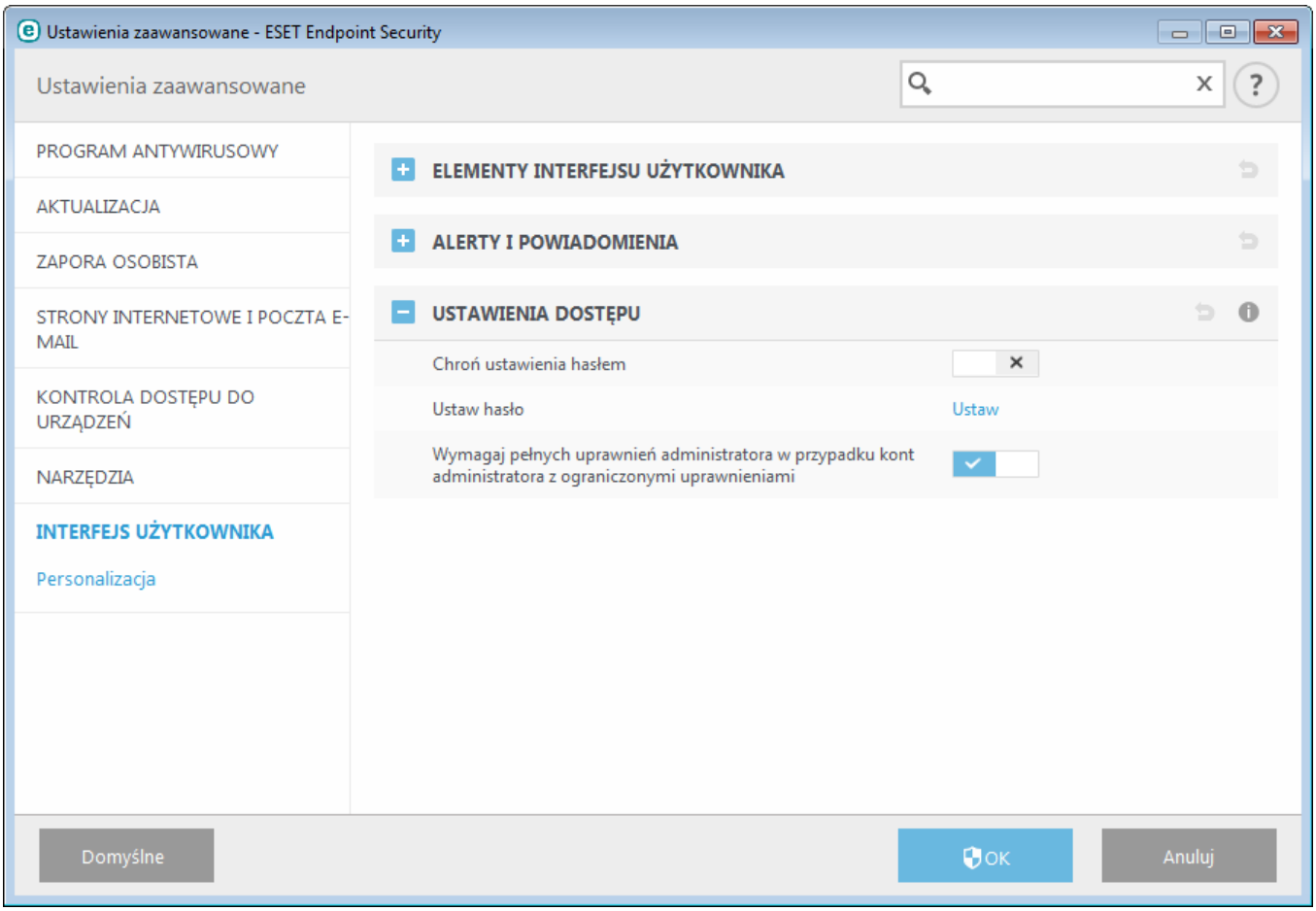
Pokaż komunikaty i powiadomienia dotyczące licencji — w przypadku wyłączenia tej opcji powiadomienia i komunikaty będą wyświetlane tylko w przypadku wygaśnięcia licencji.

UWAGA: ustawienia informacji o licencji są stosowane, ale nie są dostępne w przypadku programu ESET Endpoint Security aktywowanego w ramach licencji MSP.


Ustawienia zaawansowane - ESET Endpoint Security
Ustawienia zaawansowane
PROGRAM ANTYWIRUSOWY
AKTUALIZACJA
ZAPORA OSOBISTA
STRONY INTERNETOWE I POCZTA E-MAIL
KONTROLA DOSTĘPU DO URZĄDZEŃ
NARZĘDZIA
INTERFEJS UŻYTKOWNIKA
Personalizacja
ELEMENTY INTERFEJSU UŻYTKOWNIKA
Tryb uruchamiania
Pełny
Graficzny interfejs użytkownika wyświetlany jest w całości.
Pełny
Minimalny
Ręczny
Cichy
Pokaż ekran powitalny przy uruchamianiu
Użyj sygnałów dźwiękowych
Integruj z menu kontekstowym
STANY
Stany aplikacji
Edytuj
INFORMACJE O LICENCJI
Pokaż informacje o licencji
Pokaż powiadomienia i wiadomości dotyczące licencji
Domyślne
OK
Anuluj

3.9.7.2 Ustawienia dostępu

Aby zapewnić maksymalny poziom ochrony systemu, program ESET Endpoint Security musi być prawidłowo skonfigurowany. Wszelkie niefachowe zmiany mogą spowodować utratę cennych danych. Aby zapobiec nieautoryzowanemu wprowadzaniu zmian, parametry konfiguracji programu ESET Endpoint Security można chronić za pomocą hasła. Ustawienia konfiguracji ochrony hasła można znaleźć w obszarze **Ustawienia zaawansowane** (klawisz F5), klikając kolejno **Ustawienia dostępu** > **Interfejs użytkownika**.



Chroń ustawienia hasłem — należy tu podać ustawienia hasła. Kliknięcie umożliwia otwarcie okna Ustawienie hasła.

Aby określić lub zmienić hasło służące do ochrony ustawień, należy kliknąć opcję **Ustaw**.

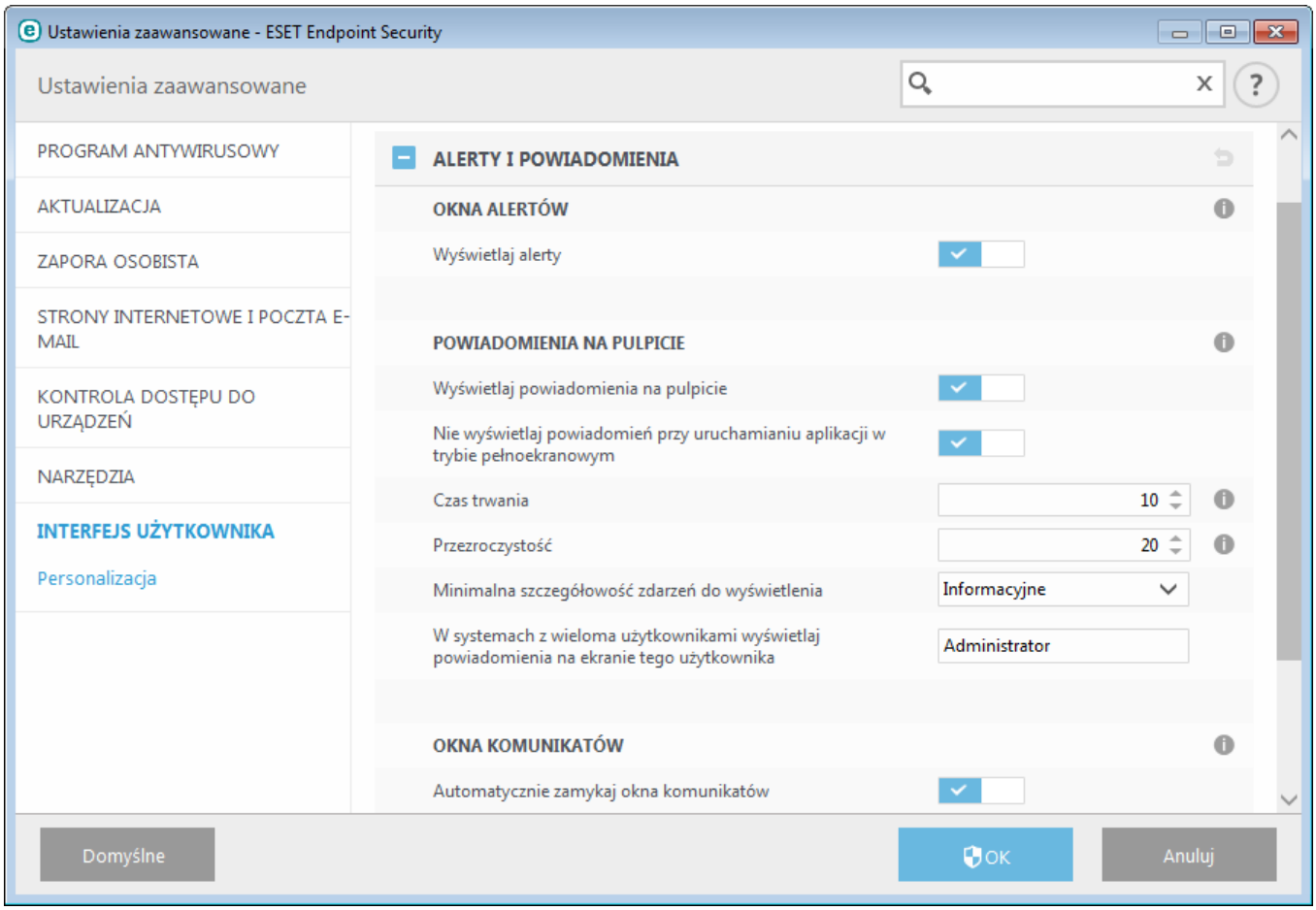
Wymagaj pełnych uprawnień administratora w przypadku kont administratora z ograniczonymi uprawnieniami — tę opcję należy pozostawić włączoną, aby użytkownik bez uprawnień administratora musiał podać nazwę użytkownika i hasło administratora w przypadku modyfikowania określonych ustawień systemowych (opcja podobna do funkcji Kontrola konta użytkownika w systemie Windows Vista). Modyfikacje te uwzględniają wyłączenie modułów ochrony lub wyłączenie zapory.

Dotyczy tylko systemu Windows XP:

Wymagaj uprawnień administratora (system bez obsługi UAC) — włączenie tej opcji powoduje wyświetlanie przez program ESET Endpoint Security monitu o podanie poświadczeń administratora.

3.9.7.3 Alerty i powiadomienia

Sekcja **Alerty i powiadomienia** w obszarze **Interfejs użytkownika** umożliwia skonfigurowanie sposobu obsługi alertów o zagrożeniach i powiadomień systemowych (np. powiadomień o pomyślnych aktualizacjach) w programie ESET Endpoint Security. Można tu też ustawić czas wyświetlania i przezroczystość powiadomień wyświetlanych na pasku zadań (ta opcja dotyczy tylko systemów operacyjnych obsługujących takie powiadomienia).



Okna alertów

Wyłączenie opcji **Wyświetlaj alerty** spowoduje anulowanie wszystkich okien alertów i jest zalecane jedynie w specyficznych sytuacjach. W przypadku większości użytkowników zaleca się pozostawienie ustawienia domyślnego tej opcji (włączona).

Powiadomienia na pulpicie

Powiadomienia na pulpicie i porady w dymkach mają charakter informacyjny i nie wymagają działań ze strony użytkownika. Są one wyświetlane w obszarze powiadomień w prawym dolnym rogu ekranu. Aby włączyć wyświetlanie powiadomień na pulpicie, należy zaznaczyć opcję **Wyświetlaj powiadomienia na pulpicie**. Włączenie opcji **Nie wyświetlaj powiadomień przy uruchamianiu aplikacji w trybie pełnoekranowym** umożliwia blokowanie wszystkich powiadomień, które nie są interaktywne. Szczegółowe opcje, takie jak czas wyświetlania powiadomienia i przezroczystość okien, można zmodyfikować poniżej.

Z menu rozwijanego **Minimalna szczegółowość zdarzeń do wyświetlenia** można wybrać stopień ważności alertów i powiadomień, które będą wyświetlane. Dostępne są następujące opcje:

- **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszenia konfiguracji programu, a także wszystkich rekordów wyższych kategorii.
- **Informacyjne** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenia** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Błędy** — rejestrowanie błędów typu „Błąd podczas pobierania pliku” oraz błędów krytycznych.
- **Krytyczne** — rejestrowanie tylko błędów krytycznych (np. błąd uruchomienia ochrony antywirusowej lub

wbudowanej zapory).

Ostatnia funkcja w tej sekcji umożliwia określenie miejsca docelowego powiadomień w środowisku wielu użytkowników. W polu **W systemach z wieloma użytkownikami wyświetlaj powiadomienia na ekranie tego użytkownika** można wskazać użytkownika, który będzie otrzymywać powiadomienia dotyczące systemu i innych kwestii w środowisku umożliwiającym równoczesne połączenie wielu użytkownikom. Zazwyczaj taką osobą jest administrator systemu lub administrator sieci. Ta opcja jest szczególnie przydatna w przypadku serwerów terminali, pod warunkiem, że wszystkie powiadomienia systemowe są wysyłane do administratora.

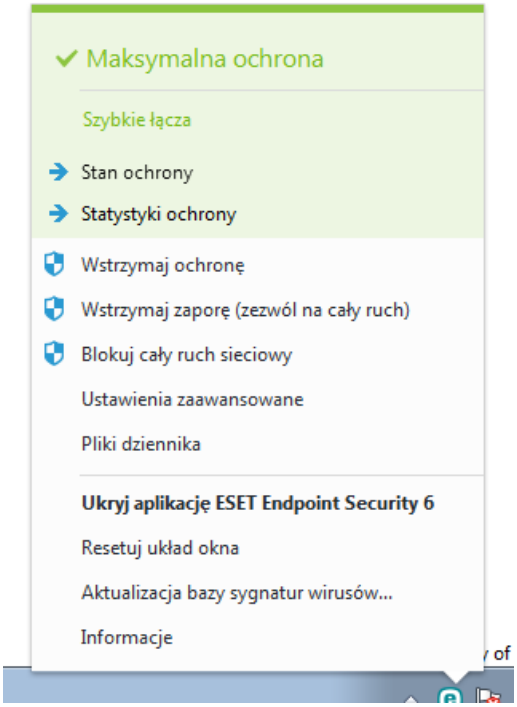
Okna komunikatów

Aby wyskakujące okna były automatycznie zamykane po upływie określonego czasu, należy zaznaczyć opcję **Automatycznie zamykaj okna komunikatów**. Jeśli użytkownik nie zamknie okna alertu ręcznie, zostanie ono zamknięte automatycznie po upływie określonego czasu.

Komunikaty wymagające potwierdzeń — wyświetlenie listy komunikatów potwierdzeń, na której można wybrać, które elementy mają być wyświetlane a które nie.

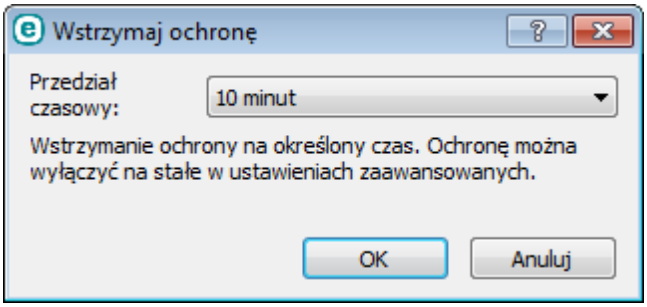
3.9.7.4 Ikona na pasku zadań

Dostęp do części najważniejszych opcji konfiguracji oraz funkcji można uzyskać po kliknięciu prawym przyciskiem myszy ikony na pasku zadań .



Zablokuj sieć — zapora osobista będzie blokować cały wychodzący i przychodzący ruch sieciowy i internetowy.

Wstrzymaj ochronę — powoduje wyświetlenie okna dialogowego potwierdzenia, które służy do wyłączenia ochrony antywirusowej i antyspyware zabezpieczającej przed atakami przez kontrolowanie komunikacji w zakresie plików, stron internetowych i poczty e-mail.



Menu rozwijane **Przedział czasowy** przedstawia okres czasu, przez który ochrona antywirusowa i antyspyware będzie

wyłączona.

Wstrzymaj zaporę (zezwól na cały ruch) — umożliwia dezaktywowanie zapory. Więcej informacji można znaleźć w sekcji Sieć.

Blokuj cały ruch sieciowy — blokuje cały ruch sieciowy. Ruch sieciowy można odblokować, klikając opcję **Wyłącz blokowanie całego ruchu sieciowego**.

Ustawienia zaawansowane — wybranie tej opcji powoduje wyświetlenie drzewa **Ustawienia zaawansowane**. Dostęp do ustawień zaawansowanych można również uzyskać poprzez naciśnięcie klawisza F5 lub wybranie kolejno opcji **Ustawienia** > **Ustawienia zaawansowane**.

Pliki dziennika — pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce w programie, oraz udostępniają zestawienie wykrytych zagrożeń.

Ukryj ESET Endpoint Security — umożliwia ukrycie na ekranie okna programu ESET Endpoint Security.

Resetuj układ okna — umożliwia przywrócenie domyślnych wymiarów i położenia okna programu ESET Endpoint Security.

Aktualizacja bazy sygnatur wirusów — umożliwia uruchomienie aktualizacji bazy sygnatur wirusów w celu zapewnienia odpowiedniego poziomu ochrony przed szkodliwym kodem.

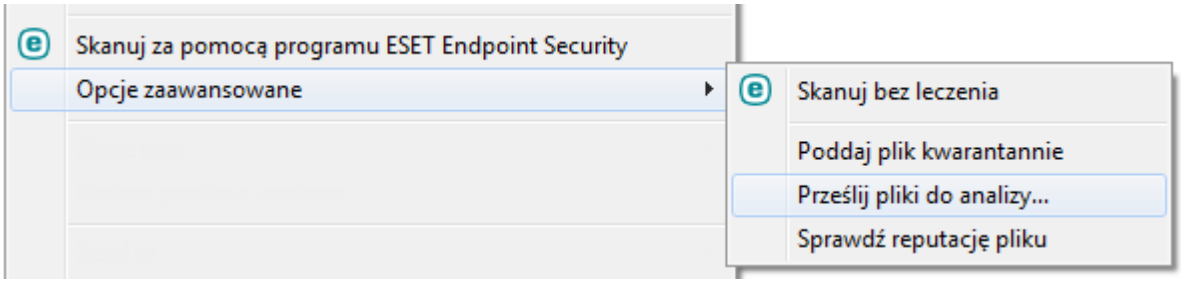
Informacje — zapewnia dostęp do informacji o systemie, szczegółowych informacji o zainstalowanej wersji programu ESET Endpoint Security i zainstalowanych modułach programu, a także o dacie ważności. Informacje dotyczące systemu operacyjnego oraz zasobów systemowych można znaleźć u dołu strony.

3.9.7.5 Menu kontekstowe

Menu kontekstowe jest wyświetlane po kliknięciu obiektu (pliku) prawym przyciskiem myszy. W menu wyszczególnione są wszystkie czynności, które można wykonać w odniesieniu do obiektu.

Elementy sterujące programu ESET Endpoint Security można zintegrować z menu kontekstowym. Ustawienia tej funkcji są dostępne w drzewie ustawień zaawansowanych po wybraniu opcji **Interfejs użytkownika** > **Elementy interfejsu użytkownika**.

Integruj z menu kontekstowym — włącza integrację elementów sterujących programu ESET Endpoint Security z menu kontekstowym.



3.10 Użytkownik zaawansowany

3.10.1 Menedżer profili

Menedżer profili jest używany w dwóch sekcjach programu ESET Endpoint Security: **Skanowanie komputera na żądanie** oraz **Aktualizacja**.

Skanowanie komputera na żądanie

Preferowane parametry skanowania mogą zostać zapisane i użyte w przyszłości. Zalecane jest utworzenie osobnego profilu (z ustawionymi różnymi obiektami i metodami skanowania oraz innymi parametrami) dla każdego regularnie przeprowadzanego skanowania.

Aby utworzyć nowy profil, należy otworzyć okno ustawień zaawansowanych (klawisz F5) i kliknąć kolejno opcje **Moduł antywirusowy** > **Skanowanie komputera na żądanie**, a następnie opcję **Edytuj** obok pozycji **Lista profili**. W

menu rozwijanym **Wybrany profil** widoczne są istniejące profile skanowania. Więcej informacji o tworzeniu profilu skanowania dostosowanego do indywidualnych potrzeb można znaleźć w sekcji Ustawienia parametrów technologii ThreatSense, w której opisano poszczególne parametry ustawień skanowania.

Przykład: Załóżmy, że użytkownik chce utworzyć własny profil skanowania, a żądana konfiguracja częściowo pokrywa się z konfiguracją Skanowanie inteligentne. Użytkownik nie chce jednak skanować programów spakowanych ani potencjalnie niebezpiecznych aplikacji oraz chce zastosować ustawienie **Leczenie dokładne**. W oknie **Menedżer profili** należy wprowadzić nazwę nowego profilu, a następnie kliknąć opcję **Dodaj**. Nowy profil należy wybrać z menu rozwijanego **Wybrany profil** w celu dostosowania pozostałych parametrów zgodnie z wymogami, po czym należy kliknąć **OK**, by zapisać nowy profil.

Aktualizacja

Edytor profili w sekcji Ustawienia aktualizacji pozwala na tworzenie nowych profili aktualizacji. Tworzenie i używanie własnych, niestandardowych profili (tzn. innych niż domyślny **Mój profil** jest przydatne tylko w sytuacji, gdy komputer na różne sposoby łączy się z serwerami aktualizacji.

Przykładem może być komputer przenośny, który zwykle łączy się z serwerem lokalnym (z kopią dystrybucyjną) w sieci lokalnej, ale po odłączeniu od niej (np. podczas podróży służbowej) pobiera aktualizacje bezpośrednio z serwerów firmy ESET korzystając z dwóch profili: jednego na potrzeby połączenia z lokalnym serwerem, a drugiego do komunikacji z serwerami firmy ESET. Po skonfigurowaniu tych profili należy kliknąć kolejno opcje **Narzędzia** > **Harmonogram** i edytować parametry zadań aktualizacji. Jeden profil należy ustawić jako główny, a drugi jako alternatywny.

Wybrany profil — obecnie używany profil aktualizacji. Aby go zmienić, należy wybrać inny profil z menu rozwijanego.

Lista profili — możliwość tworzenia nowych lub usuwania istniejących profili aktualizacji.

3.10.2 Diagnostyka

Diagnostyka umożliwia wykonywanie zrzutów pamięci w przypadku awarii aplikacji związanych z procesami oprogramowania firmy ESET (na przykład *ekrn*). Jeśli aplikacja ulega awarii, generowany jest zrzut pamięci. Może to pomóc programistom w usuwaniu błędów i eliminowaniu rozmaitych problemów związanych z programem ESET Endpoint Security. Należy kliknąć menu rozwijane dostępne obok pozycji **Typ zrzutu** i wybrać jedną z trzech dostępnych opcji:

- **Zamknij** (domyślna) — wybranie tej opcji powoduje wyłączenie tej funkcji.
- **Mini** — umożliwia zarejestrowanie najmniejszego zbioru użytecznych informacji, które mogą być pomocne w wykryciu przyczyny nieoczekiwanej awarii aplikacji. Ten rodzaj pliku zrzutu jest przydatny w sytuacji ograniczonej ilości wolnego miejsca na dysku, jednak ze względu na ograniczoną ilość zawartych w nim informacji analiza jego zawartości może nie wystarczyć do wykrycia błędów, które nie były bezpośrednio spowodowane przez wątek działający w chwili wystąpienia problemu.
- **Pełny** — umożliwia zarejestrowanie całej zawartości pamięci systemu, gdy aplikacja nieoczekiwanie przestanie działać. Pełny zrzut pamięci może zawierać dane z procesów, które były uruchomione w trakcie jego tworzenia.

Włącz zaawansowane rejestrowanie filtrowania protokołów — umożliwia rejestrowanie wszystkich danych przesyłanych przez mechanizm filtrowania protokołów w formacie PCAP. Pomaga to programistom w diagnozowaniu i rozwiązywaniu problemów związanych z filtrowaniem protokołów.

Pliki dziennika można znaleźć w tych lokalizacjach:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics w systemie Windows Vista i nowszych wersjach Windows lub w ścieżce *C:\Documents and Settings\All Users\...* w przypadku starszych wersji Windows.

Katalog docelowy — katalog, w którym po wystąpieniu awarii zostanie zapisany zrzut pamięci.

Otwórz folder diagnostyki — aby otworzyć ten katalog w nowym oknie *Eksploratora Windows*, należy kliknąć przycisk **Otwórz**.

3.10.3 Import i eksport ustawień

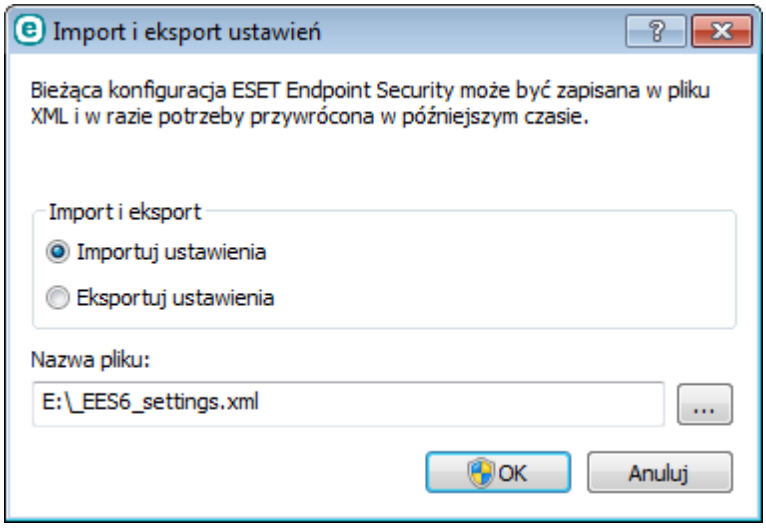
Dostosowany plik konfiguracyjny XML programu ESET Endpoint Security można importować i eksportować za pośrednictwem menu **Ustawienia**.

Importowanie i eksportowanie plików konfiguracyjnych przydaje się, jeśli trzeba wykonać kopię zapasową bieżącej konfiguracji programu ESET Endpoint Security do użycia w późniejszym terminie. Funkcja eksportu ustawień jest również pomocna dla użytkowników, którzy chcą używać preferowanej konfiguracji na wielu komputerach — ustawienia można łatwo przenieść, importując je z pliku *.xml*.

Importowanie konfiguracji jest bardzo łatwe. W głównym oknie programu kliknij kolejno opcje **Ustawienia** > **Importuj/eksportuj ustawienia**, a następnie wybierz opcję **Importuj ustawienia**. Wprowadź nazwę pliku konfiguracyjnego lub kliknij przycisk **...**, aby wyszukać plik konfiguracyjny do zaimportowania.

Czynności wykonywane podczas eksportu konfiguracji są bardzo podobne. W głównym oknie programu kliknij kolejno opcje **Ustawienia** > **Importuj/eksportuj ustawienia**. Wybierz opcję **Eksportuj ustawienia** i podaj nazwę pliku konfiguracyjnego (np. *eksport.xml*). Wybierz za pomocą przeglądania lokalizację na komputerze, w której ma zostać zapisany plik konfiguracyjny.

UWAGA: przy eksportowaniu ustawień może pojawić się błąd, jeśli nie masz wystarczających uprawnień do zapisania eksportowanego pliku w określonym katalogu.



3.10.4 Wiersz polecenia

Moduł antywirusowy programu ESET Endpoint Security można uruchomić z poziomu wiersza polecenia — ręcznie (polecenie „ecls") lub za pomocą pliku wsadowego (BAT). Sposób używania skanera ESET uruchamianego z wiersza polecenia:

```
ecls [OPCJE..] PLIKI..
```

Podczas uruchamiania skanera na żądanie z poziomu wiersza polecenia można używać następujących parametrów i przełączników:

Opcje

/base-dir=FOLDER	Załaduj moduły z FOLDERU.
/quar-dir=FOLDER	Poddaj FOLDER kwarantannie.
/exclude=MASKA	Wyłącz MASKĘ zgodności plików ze skanowania.
/subdir	Skanuj podfoldery (parametr domyślny).
/no-subdir	Nie skanuj podfolderów.
/max-subdir-level=POZIOM	Maksymalny podpoziom folderów w ramach folderów do przeskanowania.
/symlink	Uwzględniaj łącza symboliczne (parametr domyślny).
/no-symlink	Pomijaj łącza symboliczne.
/ads	Skanuj alternatywne strumienie danych (parametr domyślny).
/no-ads	Nie skanuj alternatywnych strumieni danych.
/log-file=PLIK	Zapisuj wyniki w PLIKU.

/log-rewrite	Zastąp plik wyników (domyślnie — dołącz).
/log-console	Rejestruj wyniki w konsoli (parametr domyślny).
/no-log-console	Nie rejestruj wyników w konsoli.
/log-all	Zapisuj również informacje o niezainfekowanych plikach.
/no-log-all	Nie zapisuj informacji o niezainfekowanych plikach (parametr domyślny).
/aind	Pokaż wskaźnik aktywności.
/auto	Skanuj i automatycznie lecz wszystkie lokalne dyski.

Opcje skanera

/files	Skanuj pliki (parametr domyślny).
/no-files	Nie skanuj plików.
/memory	Skanuj pamięć.
/boots	Skanuj sektory rozruchowe.
/no-boots	Nie skanuj sektorów rozruchowych (parametr domyślny).
/arch	Skanuj archiwa (parametr domyślny).
/no-arch	Nie skanuj archiwów.
/max-obj-size=ROZMIAR	Skanuj tylko pliki mniejsze niż ROZMIAR w MB (wartość domyślna 0 = brak ograniczenia).
/max-arch-level=POZIOM	Maksymalny podpoziom archiwów w ramach archiwów (zagnieżdżenie archiwów) do przeskanowania.
/scan-timeout=LIMIT	Skanuj archiwa z maksymalnym LIMITEM sekund.
/max-arch-size=ROZMIAR	Skanuj tylko pliki z archiwum, jeśli są mniejsze niż ROZMIAR (wartość domyślna 0 = brak ograniczenia).
/max-sfx-size=ROZMIAR	Skanuj tylko pliki z archiwum samorozpakowującego, jeśli są mniejsze niż ROZMIAR w MB (wartość domyślna 0 = brak ograniczenia).
/mail	Skanuj pliki poczty e-mail (parametr domyślny).
/no-mail	Nie skanuj plików poczty e-mail.
/mailbox	Skanuj skrzynki pocztowe (parametr domyślny).
/no-mailbox	Nie skanuj skrzynek pocztowych.
/sfx	Skanuj archiwa samorozpakowujące (parametr domyślny).
/no-sfx	Nie skanuj archiwów samorozpakowujących.
/rtp	Skanuj programy spakowane (parametr domyślny).
/no-rtp	Nie skanuj programów spakowanych.
/unsafe	Skanuj w poszukiwaniu potencjalnie niebezpiecznych aplikacji.
/no-unsafe	Nie skanuj w poszukiwaniu potencjalnie niebezpiecznych aplikacji (parametr domyślny).
/unwanted	Skanuj w poszukiwaniu potencjalnie niepożądanych aplikacji.
/no-unwanted	Nie skanuj w poszukiwaniu potencjalnie niepożądanych aplikacji (parametr domyślny).
/suspicious	skanuj pod kątem podejrzanych aplikacji (domyślnie)
/no-suspicious	nie skanuj pod kątem podejrzanych aplikacji
/pattern	Używaj sygnatur (parametr domyślny).
/no-pattern	Nie używaj sygnatur.
/heur	Włącz heurystykę (parametr domyślny).
/no-heur	Wyłącz heurystykę.
/adv-heur	Włącz zaawansowaną heurystykę (parametr domyślny).
/no-adv-heur	Wyłącz zaawansowaną heurystykę.
/ext=ROZSZERZENIA	Skanuj tylko ROZSZERZENIA oddzielone dwukropkami.
/ext-exclude=ROZSZERZENIA	Wyłącz ze skanowania ROZSZERZENIA oddzielone dwukropkami.

/clean-mode=TRYB	używaj TRYBU leczenia zainfekowanych obiektów Dostępne są następujące opcje: • brak — nie nastąpi automatyczne leczenie. • standardowy (domyślny) — program ecls.exe podejmie próbę automatycznego wyleczenia lub usunięcia zainfekowanych plików. • dokładny — program ecls.exe podejmie próbę automatycznego wyleczenia lub usunięcia zainfekowanych plików bez interwencji użytkownika (użytkownik zostanie powiadomiony już po usunięciu plików). • rygorystyczny — program ecls.exe usunie pliki bez podjęcia próby ich wyleczenia, bez względu na ich zawartość. • usuwanie — program ecls.exe usunie pliki bez podjęcia próby ich wyleczenia, ale nie obejmie to ważnych plików, takich jak pliki systemu Windows.
/quarantine	Kopiuj zainfekowane pliki (jeśli zostały wyleczone) do kwarantanny (uzupełnienie czynności wykonywanej podczas leczenia).
/no-quarantine	Nie kopiuj zainfekowanych plików do kwarantanny.

Opcje ogólne

/help	Pokaż pomoc i zakończ.
/version	Pokaż informacje o wersji i zakończ.
/preserve-time	Zachowaj znacznik czasowy ostatniego dostępu.

Kody zakończenia

0	Nie znaleziono zagrożenia.
1	Zagrożenie zostało wykryte i usunięte.
10	Niektórych plików nie można przeskanować (mogą stanowić zagrożenia).
50	Znaleziono zagrożenie.
100	Błąd.

UWAGA: Kody zakończenia o wartości wyższej niż 100 oznaczają, że plik nie został przeskanowany i dlatego może być zainfekowany.

3.10.5 Wykrywanie stanu bezczynności

Ustawienia wykrywania stanu bezczynności można skonfigurować w obszarze **Ustawienia zaawansowane** po wybraniu kolejno opcji **Ochrona antywirusowa** > **Skanowanie w trakcie bezczynności** > **Wykrywanie stanu bezczynności**. Te ustawienia określają element wywołujący funkcję Skanowanie w trakcie bezczynności, gdy:

- wygaszacz ekranu jest uruchomiony,
- komputer jest zablokowany,
- użytkownik jest wylogowany.

Użycie pól wyboru dla poszczególnych stanów umożliwia włączanie i wyłączanie różnych wywołań wykrywania stanu bezczynności.

3.10.6 ESET SysInspector

3.10.6.1 Wprowadzenie do programu ESET SysInspector

Program ESET SysInspector dokładnie sprawdza stan komputera i wyświetla kompleksowe zestawienie zgromadzonych danych. Informacje o zainstalowanych sterownikach i aplikacjach, połączeniach sieciowych lub ważnych wpisach w rejestrze ułatwiają śledzenie podejrzanego zachowania systemu, które może wynikać z niezgodności programowej lub sprzętowej bądź zainfekowania szkodliwym oprogramowaniem.

Dostęp do programu ESET SysInspector można uzyskać na dwa sposoby: korzystając z wersji zintegrowanej w programie ESET Security albo bezpłatnie pobierając wersję autonomiczną (SysInspector.exe) z witryny internetowej firmy ESET. Obie wersje mają identyczne funkcje i te same elementy interfejsu. Jedyna różnica polega na sposobie zarządzania danymi wyjściowymi. W przypadku obu wersji można wyeksportować zapisy bieżącego stanu systemu do pliku *XML* i zapisać je na dysku. Jednak wersja zintegrowana umożliwia ponadto przechowywanie migawek systemu bezpośrednio pod pozycją **Narzędzia** > **ESET SysInspector** (z wyjątkiem programu ESET Remote Administrator). Więcej informacji można znaleźć w sekcji Program ESET SysInspector jako element oprogramowania ESET Endpoint Security.

Przeskanowanie komputera przy użyciu programu ESET SysInspector wymaga nieco czasu. Może to potrwać od 10 sekund do kilku minut w zależności od konfiguracji sprzętowej, systemu operacyjnego i liczby aplikacji zainstalowanych na komputerze.

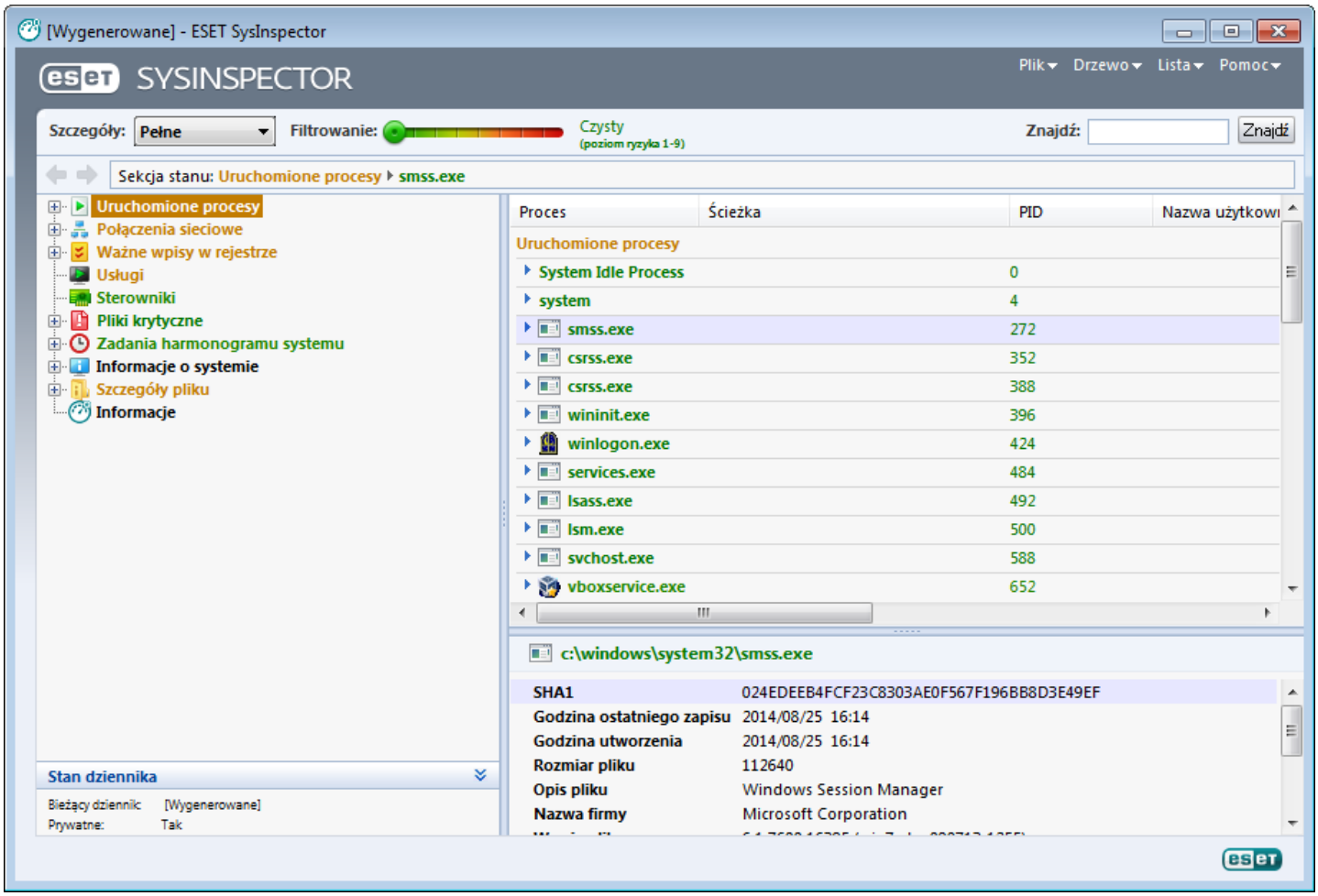
3.10.6.1.1 Uruchamianie programu ESET SysInspector

Aby uruchomić program ESET SysInspector, wystarczy uruchomić plik wykonywalny *SysInspector.exe* pobrany z witryny firmy ESET. Jeśli jest już zainstalowane jedno z rozwiązań ESET Security, program ESET SysInspector można uruchomić bezpośrednio z menu Start (po kliknięciu opcji **Programy** > **ESET** > **ESET Endpoint Security**).

Po włączeniu aplikacji zostanie przeprowadzona inspekcja systemu, która może potrwać do kilku minut.

3.10.6.2 Interfejs użytkownika i użycie aplikacji

W celu zachowania przejrzystości okno główne zostało podzielone na cztery główne sekcje: Formanty programu (u góry), okno Nawigacja (z lewej strony), okno Opis (z prawej strony) oraz okno Szczegóły (u dołu). W sekcji Stan dziennika są wyświetlane podstawowe parametry dziennika (stosowany filtr, typ filtru, informacja, czy dziennik powstał w wyniku porównania itd.).



3.10.6.2.1 Sterowanie programem

W tej części opisano wszystkie elementy sterujące dostępne w programie ESET SysInspector.

Plik

Klikając pozycję **Plik**, można zapisać bieżący stan systemu, w celu zbadania go w późniejszym terminie, albo otworzyć zapisany wcześniej dziennik. Jeśli dziennik ma zostać opublikowany, zaleca się jego wygenerowanie przy użyciu opcji **Przeznaczone do wysłania**. W dzienniku o takiej formie pomijane są informacje poufne (nazwa bieżącego użytkownika, nazwa komputera, nazwa domeny, uprawnienia bieżącego użytkownika, zmienne środowiskowe itp.).

UWAGA: Zapisane wcześniej raporty programu ESET SysInspector można otwierać, przeciągając je i upuszczając w głównym oknie programu.

Drzewo

Umożliwia rozwijanie i zwijanie wszystkich węzłów oraz eksportowanie wybranych sekcji do skryptu usługi.

Lista

Zawiera funkcje ułatwiające nawigację w obrębie programu oraz wykonywanie innych czynności, np. wyszukiwanie informacji w trybie online.

Pomoc

Zawiera informacje dotyczące aplikacji i jej funkcji.

Szczegóły

To ustawienie ułatwia pracę z informacjami wyświetlanymi w oknie głównym. W trybie podstawowym użytkownik ma dostęp do informacji umożliwiających wyszukiwanie rozwiązań typowych problemów z systemem. W trybie średnim program wyświetla rzadziej używane informacje. W trybie pełnym program ESET SysInspector wyświetla wszystkie informacje potrzebne do rozwiązywania bardzo konkretnych problemów.

Filtrowanie

Filtrowanie elementów wykorzystuje się najczęściej do wyszukiwania podejrzanych plików lub wpisów rejestru w systemie. Korygując ustawienie suwaka, można filtrować elementy według ich poziomu ryzyka. Jeśli suwak znajdzie się w skrajnym lewym położeniu (poziom ryzyka 1), wyświetlone zostaną wszystkie elementy. Przesunięcie suwaka w prawo spowoduje, że elementy o niższym poziomie ryzyka niż bieżący poziom zostaną odfiltrowane, natomiast wyświetlane będą tylko te elementy, które są bardziej podejrzane niż wyświetlany poziom. Po ustawieniu suwaka w skrajnym prawym położeniu wyświetlane są tylko elementy znane jako szkodliwe.

Wszystkie elementy o poziomie ryzyka od 6 do 9 mogą stanowić zagrożenie bezpieczeństwa. Jeśli użytkownik nie korzysta z oprogramowania zabezpieczającego firmy ESET, w przypadku wykrycia takich elementów przez program ESET SysInspector zalecane jest przeskanowanie systemu przy użyciu narzędzia ESET Online Scanner. Usługa ESET Online Scanner jest bezpłatna.

UWAGA: Poziom ryzyka elementu można łatwo ustalić, porównując jego kolor z kolorem na suwaku Poziom ryzyka.

Funkcja Porównaj

Podczas porównywania dwóch dzienników, można wybrać opcję wyświetlenia wszystkich pozycji, wyświetlenia tylko dodanych pozycji, wyświetlenia tylko usuniętych pozycji lub wyświetlenia tylko zastąpionych pozycji.

Znajdź

Korzystając z funkcji wyszukiwania, można szybko znaleźć określony element, podając jego nazwę lub część nazwy. Wyniki wyszukiwania są wyświetlane w oknie opisu.

Powrót

Klikając strzałkę wstecz lub dalej, można powrócić do poprzednio wyświetlanych informacji w oknie opisu. Alternatywą dla przycisków Wstecz i Dalej są odpowiednio klawisz Backspace i spacja.

Sekcja Stan

W tej sekcji wyświetlany jest bieżący węzeł w oknie nawigacji.

Ważne: Elementy wyróżnione kolorem czerwonym są nieznane, dlatego oznaczono je jako potencjalnie niebezpieczne. Zaznaczenie elementu kolorem czerwonym nie oznacza automatycznie, że można usunąć dany plik. Należy się najpierw upewnić, że pliki są faktycznie niebezpieczne lub niepotrzebne.

3.10.6.2.2 Nawigacja w programie ESET SysInspector

W programie ESET SysInspector różne rodzaje informacji są podzielone na kilka podstawowych sekcji, określanych mianem węzłów. Po rozwinięciu każdego węzła w jego podwęzły można znaleźć dodatkowe szczegóły, jeśli są dostępne. Aby rozwinąć lub zwinąć węzeł, należy kliknąć dwukrotnie jego nazwę. Można także kliknąć symbol + lub − znajdujący się obok jego nazwy. Przeglądając strukturę drzewa węzłów i podwęzłów w oknie nawigacji, w oknie opisu można wyświetlać różne informacje szczegółowe dotyczące każdego węzła. Natomiast przeglądając elementy w oknie opisu, można wyświetlać dodatkowe informacje na temat poszczególnych elementów w oknie szczegółów.

Poniżej opisano główne węzły w oknie nawigacji oraz powiązane z nimi informacje w oknie opisu i w oknie szczegółów.

Uruchomione procesy

Ten węzeł zawiera informacje o aplikacjach i procesach uruchomionych w chwili generowania dziennika. W oknie opisu można znaleźć dodatkowe szczegóły dotyczące poszczególnych procesów. Są to na przykład informacje o bibliotekach dynamicznych używanych przez proces i ich lokalizacji w systemie, nazwa dostawcy aplikacji czy poziom ryzyka przypisany do danego pliku.

W oknie szczegółów wyświetlane są dodatkowe informacje dotyczące elementów zaznaczonych w oknie opisu, takie jak rozmiar pliku czy jego skrót.

UWAGA: W skład systemu operacyjnego wchodzi wiele ważnych składników jądra, które działają nieprzerwanie oraz zapewniają podstawowe funkcje o newralgicznym znaczeniu dla innych aplikacji użytkownika. W niektórych przypadkach takie procesy są wyświetlane w narzędziu ESET SysInspector ze ścieżką rozpoczynającą się od ciągu \??\. Te symbole zapewniają optymalizację tych procesów przed ich uruchomieniem i są bezpieczne dla systemu.

Połączenia sieciowe

Okno opisu zawiera listę procesów i aplikacji komunikujących się w sieci przy użyciu protokołu wybranego w oknie nawigacji (TCP lub UDP) oraz adres zdalny, z którym jest połączona dana aplikacja. Można również sprawdzić adresy IP serwerów DNS.

W oknie szczegółów wyświetlane są dodatkowe informacje dotyczące elementów zaznaczonych w oknie opisu, takie jak rozmiar pliku czy jego skrót.

Ważne wpisy w rejestrze

Zawiera listę wybranych wpisów rejestru, które są często związane z różnymi problemami z systemem, np. wpisy wskazujące programy uruchamiane razem z systemem, obiekty pomocnika przeglądarki (BHO) itd.

W oknie opisu można sprawdzić, które pliki są powiązane z określonymi wpisami w rejestrze. W oknie szczegółów znajdują się dodatkowe informacje.

Usługi

Okno opisu zawiera listę plików zarejestrowanych jako usługi systemu Windows. W oknie szczegółów można sprawdzić ustawiony sposób uruchamiania danej usługi, jak również przejrzeć informacje szczegółowe dotyczące pliku.

Sterowniki

Lista sterowników zainstalowanych w systemie.

Pliki krytyczne

W oknie opisu wyświetlana jest zawartość plików krytycznych związanych z systemem operacyjnym Microsoft Windows.

Zadania harmonogramu systemu

Zawiera listę zadań wywoływanych przez Harmonogram zadań systemu Windows o określonej porze lub z ustalonym interwałem.

Informacje o systemie

Zawiera szczegółowe informacje o sprzęcie i oprogramowaniu, ustawionych zmiennych środowiskowych, uprawnieniach użytkownika i systemowych dziennikach zdarzeń.

Szczegóły pliku

Lista ważnych plików systemowych i plików w folderze Program Files. Dodatkowe informacje dotyczące poszczególnych plików można znaleźć w oknach opisu i szczegółów.

Informacje

Informacje o wersji programu ESET SysInspector i lista jego modułów.

3.10.6.2.2.1 Skróty klawiaturowe

Podczas pracy z programem ESET SysInspector można korzystać z następujących skrótów klawiszowych:

Plik

Ctrl+O	Otwarcie istniejącego dziennika.
Ctrl+S	Zapisanie utworzonych dzienników.

Generuj

Ctrl+G	Wygenerowanie standardowego zapisu bieżącego stanu komputera.
Ctrl+H	Wygenerowanie zapisu bieżącego stanu komputera, w którym mogą się też znaleźć informacje poufne.

Filtrowanie elementów

1, O	Czysty (wyświetlane są elementy o poziomie ryzyka 1–9).
2	Czysty (wyświetlane są elementy o poziomie ryzyka 2—9).
3	Czysty (wyświetlane są elementy o poziomie ryzyka 3–9).
4, U	Nieznany (wyświetlane są elementy o poziomie ryzyka 4–9).
5	Nieznany (wyświetlane są elementy o poziomie ryzyka 5–9).
6	Nieznany (wyświetlane są elementy o poziomie ryzyka 6–9).
7, B	Ryzykowny (wyświetlane są elementy o poziomie ryzyka 7–9).
8	Ryzykowny (wyświetlane są elementy o poziomie ryzyka 8–9).
9	Ryzykowny (wyświetlane są elementy o poziomie ryzyka 9).
-	Obniżenie poziomu ryzyka.
+	Podwyższenie poziomu ryzyka.
Ctrl+9	Tryb filtrowania, poziom jednakowy lub wyższy.
Ctrl+0	Tryb filtrowania, tylko jednakowy poziom.

Widok

Ctrl+5	Widok wg dostawcy, wszyscy dostawcy.
Ctrl+6	Widok wg dostawcy, tylko Microsoft.
Ctrl+7	Widok wg dostawcy, wszyscy pozostali dostawcy.
Ctrl+3	Wyświetlenie szczegółów w trybie Pełne.
Ctrl+2	Wyświetlenie szczegółów w trybie Średnie.
Ctrl+1	Tryb podstawowy.
BackSpace	Przejście o krok wstecz.
Spacja	Przejście o krok w przód.
Ctrl+W	Rozwinięcie drzewa.
Ctrl+Q	Zwinięcie drzewa.

Inne funkcje

Ctrl+T	Przejście do pierwotnej lokalizacji elementu po zaznaczeniu go w wynikach wyszukiwania.
Ctrl+P	Wyświetlenie podstawowych informacji o elemencie.
Ctrl+A	Wyświetlenie pełnych informacji o elemencie.

Ctrl+C Skopiowanie drzewa bieżącego elementu.
Ctrl+X Skopiowanie elementów.
Ctrl+B Wyszukanie informacji o wybranych plikach w Internecie.
Ctrl+L Otwarcie folderu zawierającego wybrany plik.
Ctrl+R Otwarcie odpowiedniego wpisu w edytorze rejestru.
Ctrl+Z Skopiowanie ścieżki do pliku (jeśli element jest powiązany z plikiem).
Ctrl+F Przełączenie do pola wyszukiwania.
Ctrl+D Zamknięcie wyników wyszukiwania.
Ctrl+E Uruchomienie skryptu usługi.

Porównywanie

Ctrl+Alt+O Otwarcie dziennika oryginalnego/porównawczego.
Ctrl+Alt+R Anulowanie porównania.
Ctrl+Alt+1 Wyświetlenie wszystkich wpisów.
Ctrl+Alt+2 Wyświetlenie tylko dodanych wpisów; w dzienniku zostaną wyświetlone wpisy występujące w bieżącym dzienniku.
Ctrl+Alt+3 Wyświetlenie tylko usuniętych wpisów; w dzienniku zostaną wyświetlone wpisy występujące w poprzednim dzienniku.
Ctrl+Alt+4 Wyświetlenie tylko zastąpionych wpisów (z uwzględnieniem plików).
Ctrl+Alt+5 Wyświetlenie tylko różnic między dziennikami.
Ctrl+Alt+C Wyświetlenie porównania.
Ctrl+Alt+N Wyświetlenie bieżącego dziennika.
Ctrl+Alt+P Otwarcie poprzedniego dziennika.

Inne

F1 Wyświetlenie pomocy.
Alt+F4 Zamknięcie programu.
Alt+Shift+F4 Zamknięcie programu bez wcześniejszego monitu.
Ctrl+I Statystyki dziennika.

3.10.6.2.3 Porównywanie

Korzystając z funkcji porównania, użytkownik może porównać dwa istniejące dzienniki. W wyniku działania tej funkcji powstaje zestawienie wpisów, którymi różnią się dzienniki. Jest to pomocne narzędzie do wykrywania złośliwego kodu, przydatne, gdy użytkownik chce śledzić zmiany w systemie.

Po uruchomieniu aplikacji jest tworzony nowy dziennik, który jest wyświetlany w nowym oknie. Aby zapisać dziennik w pliku, należy kliknąć kolejno opcje **Plik** > **Zapisz dziennik**. Pliki dzienników można otwierać i przeglądać w późniejszym terminie. Aby otworzyć istniejący dziennik, należy kliknąć kolejno opcje **Plik** > **Otwórz dziennik**. W głównym oknie programu ESET SysInspector zawsze wyświetlany jest tylko jeden dziennik naraz.

Zaletą porównywania dwóch dzienników jest możliwość wyświetlania aktualnie aktywnego dziennika i dziennika zapisanego w pliku. Aby porównać dzienniki, należy kliknąć kolejno opcje **Plik** > **Porównaj dziennik** i wybrać opcję **Wybierz plik**. Wybrany dziennik zostanie porównany z dziennikiem aktywnym w głównym oknie programu. W dzienniku porównawczym zostaną wyświetlone jedynie różnice między tymi dwoma dziennikami.

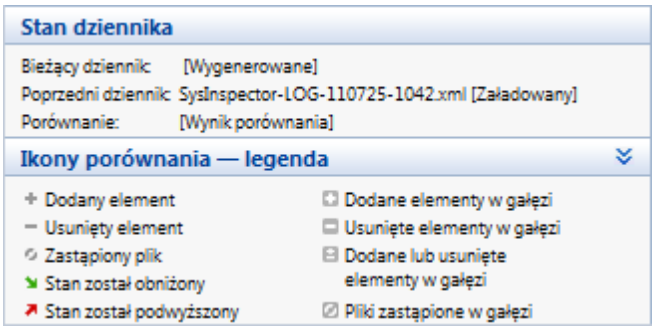
UWAGA: W przypadku porównywania dwóch plików dziennika należy kliknąć kolejno opcje **Plik** > **Zapisz dziennik**, aby zapisać dane w pliku ZIP (zapisywane są oba pliki). Po otwarciu tego pliku w późniejszym terminie zawarte w nim dzienniki zostaną automatycznie porównane.

Obok wyświetlonych elementów w programie ESET SysInspector widoczne są symbole określające różnice między porównywanymi dziennikami.

Opis wszystkich symboli wyświetlanych obok wpisów:

- Nowa wartość, nieobecna w poprzednim dzienniku.
- Sekcja struktury drzewa zawiera nowe wartości.
- Wartość usunięta, obecna jedynie w poprzednim dzienniku.
- Sekcja struktury drzewa zawiera usunięte wartości.
- Zmodyfikowano wartość/plik.
- Sekcja struktury drzewa zawiera zmodyfikowane wartości/pliki.
- Poziom ryzyka zmniejszył się/był wyższy w poprzednim dzienniku.
- Poziom ryzyka zwiększył się/był niższy w poprzednim dzienniku.

W sekcji wyjaśnień (wyświetlanej w lewym dolnym rogu) znajduje się opis wszystkich symboli wraz z nazwami porównywanych dzienników.



Dziennik porównawczy można zapisać w pliku i otworzyć później.

Przykład

Wygenerowano dziennik zawierający pierwotne informacje o systemie i zapisano go w pliku o nazwie stary.xml. Po wprowadzeniu zmian w systemie otwarto program ESET SysInspector w celu wygenerowania nowego dziennika. Zapisano go w pliku *nowy.xml*.

Aby prześledzić zmiany między tymi dwoma dziennikami, należy kliknąć kolejno opcje **Plik** > **Porównaj dzienniki**. Program utworzy dziennik porównawczy zawierający różnice między dziennikami.

Ten sam rezultat można osiągnąć, wpisując w wierszu polecenia następujące polecenie:

SysIsnpector.exe nowy.xml stary.xml

3.10.6.3 Parametry wiersza polecenia

Program ESET SysInspector obsługuje generowanie raportów z poziomu wiersza polecenia z zastosowaniem następujących parametrów:

/gen	wygenerowanie raportu bezpośrednio z wiersza polecenia bez uruchamiania graficznego interfejsu użytkownika
/privacy	generowanie dziennika z informacji poufnych pominięte
/zip	zapisanie dziennika wynikowego w skompresowanym archiwum zip
/silent	ograniczenie okna postępu podczas generowania dziennika z poziomu wiersza poleceń
/blank	uruchomienie programu SysInspector ESET bez generowania/ładowania dziennika

Przykłady

Użycie:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Aby załadować określony dziennik bezpośrednio do przeglądarki, należy użyć polecenia: *SysInspector.exe .\clientlog.xml*
Aby wygenerować dziennik z wiersza polecenia, należy użyć polecenia: *SysInspector.exe /gen=.\mynewlog.xml*
Aby wygenerować dziennik z wyłączeniem informacji poufnych bezpośrednio w pliku skompresowanym, należy użyć polecenia: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Aby porównać dwa pliki dziennika i przejrzeć różnice, należy użyć polecenia: *SysInspector.exe new.xml old.xml*

UWAGA: Jeśli nazwa pliku/folderu zawiera spację, należy ją ująć w cudzysłów.

3.10.6.4 Skrypt usługi

Skrypt serwisowy to narzędzie, które zapewnia pomoc klientom używającym programu ESET SysInspector, usuwając z systemu niepożądane obiekty.

Skrypt usługi umożliwia wyeksportowanie całego dziennika programu ESET SysInspector lub jego wybranych części. Po wyeksportowaniu można oznaczyć niepożądane obiekty do usunięcia. Następnie można uruchomić zmodyfikowany dziennik, aby usunąć oznaczone obiekty.

Skrypt usługi jest przeznaczony dla zaawansowanych użytkowników mających doświadczenie w diagnozowaniu problemów z systemem. Nieodpowiednie modyfikacje mogą prowadzić do uszkodzenia systemu operacyjnego.

Przykład

Jeśli użytkownik podejrzewa, że komputer został zainfekowany wirusem, który nie jest wykrywany przez posiadany program antywirusowy, należy wykonać instrukcje przedstawione poniżej:

1. Uruchom program ESET SysInspector, aby wygenerować nowy zapis bieżącego stanu systemu.
2. Zaznacz pierwszy element w lewej sekcji (w strukturze drzewa), naciśnij klawisz Shift i zaznacz ostatni element, co spowoduje zaznaczenie wszystkich elementów.
3. Kliknij wybrane obiekty prawym przyciskiem myszy i wybierz w opcję Eksportuj wybrane sekcje do skryptu usługi**.**
4. Zaznaczone obiekty zostaną wyeksportowane do nowego dziennika.
5. Najważniejszy krok w całej procedurze: otwórz nowy dziennik i zmień atrybut - na + dla wszystkich obiektów, które chcesz usunąć. Upewnij się, że nie zostały oznaczone żadne ważne pliki/obiekty systemu operacyjnego.
6. Uruchom program ESET SysInspector, kliknij kolejno pozycje **Plik** > **Uruchom skrypt usługi** i wprowadź ścieżkę do skryptu.
7. Kliknij przycisk **OK**, aby uruchomić skrypt.

3.10.6.4.1 Tworzenie skryptu usługi

Aby wygenerować skrypt, należy kliknąć prawym przyciskiem myszy dowolny element drzewa menu w lewej części głównego okna programu ESET SysInspector. Z menu kontekstowego należy wybrać opcję **Eksportuj wszystkie sekcje do skryptu usługi** lub **Eksportuj wybrane sekcje do skryptu usługi**.

UWAGA: Nie można wyeksportować skryptu usługi, gdy porównywane są dwa dzienniki.

3.10.6.4.2 Struktura skryptu usługi

Pierwszy wiersz nagłówka skryptu zawiera informację o wersji aparatu (ev), wersji interfejsu graficznego (gv) i wersji dziennika (lv). Na podstawie tych danych można śledzić zmiany w pliku XML służącym do wygenerowania skryptu, aby zapobiec ewentualnym niespójnościom podczas wykonywania. Tej części skryptu nie należy zmieniać.

Pozostała część pliku jest podzielona na sekcje zawierające pozycje dostępne do edycji. Modyfikowanie pliku polega na wskazaniu elementów, które mają być przetwarzane przez skrypt. Oznaczenie wybranego elementu do przetwarzania wymaga zastąpienia poprzedzającego go znaku „-” znakiem „+”. Kolejne sekcje skryptu są oddzielane pustymi wierszami. Każda sekcja nosi numer i tytuł.

01) Running processes (Uruchomione procesy)

Ta sekcja zawiera listę wszystkich procesów uruchomionych w systemie. Każdy proces jest identyfikowany przez ścieżkę UNC, po której następuje odpowiadający mu ujęty w gwiazdki (*) skrót CRC16.

Przykład:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

W tym przykładzie wybrany został proces module32.exe (oznaczony znakiem „+”), co spowoduje jego zakończenie

po wykonaniu skryptu.

02) Loaded modules (Załadowane moduły)

Ta sekcja zawiera listę aktualnie używanych modułów systemowych.

Przykład:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

W tym przykładzie moduł khbekhb.dll został oznaczony znakiem „+”. Po uruchomieniu skryptu procesy korzystające z tego modułu zostaną wykryte i zakończone.

03) TCP connections (Połączenia TCP)

Ta sekcja zawiera informacje o trwających połączeniach TCP.

Przykład:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Po uruchomieniu skryptu zlokalizowani zostaną właściciele gniazd odpowiadających zaznaczonym połączeniom TCP i gniazda te zostaną zamknięte, zwalniając tym samym zasoby systemowe.

04) UDP endpoints (Punkty końcowe UDP)

Ta sekcja zawiera informacje o istniejących punktach końcowych UDP.

Przykład:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Po uruchomieniu skryptu zlokalizowani zostaną właściciele gniazd odpowiadających zaznaczonym punktom końcowym UDP i gniazda te zostaną zamknięte.

05) DNS server entries (Wpisy serwera DNS)

Ta sekcja zawiera informacje o aktualnej konfiguracji serwera DNS.

Przykład:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Po uruchomieniu skryptu zaznaczone wpisy serwera DNS zostaną usunięte.

06) Important registry entries (Ważne wpisy w rejestrze)

Ta sekcja zawiera informacje o ważnych wpisach w rejestrze.

Przykład:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Po uruchomieniu skryptu zaznaczone wpisy zostaną usunięte, nadpisane bajtami zerowymi lub przywrócone do wartości domyślnych. Działanie podejmowane dla danego wpisu rejestru zależy od jego kategorii i odpowiadającej mu wartości klucza.

07) Services (Usługi)

Ta sekcja zawiera listę usług zarejestrowanych w systemie.

Przykład:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Po wykonaniu skryptu zaznaczone usługi oraz usługi od nich zależne zostaną zatrzymane i odinstalowane.

08) Drivers (Sterowniki)

Ta sekcja zawiera listę zainstalowanych sterowników.

Przykład:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Uruchomienie skryptu spowoduje przerwanie działania wybranych sterowników. Należy pamiętać, że niektóre sterowniki nie umożliwiają przerywania ich pracy.

09) Critical files (Pliki krytyczne)

Ta sekcja zawiera informacje o plikach niezbędnych do prawidłowego funkcjonowania systemu operacyjnego.

Przykład:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Zaznaczone elementy zostaną usunięte albo zostaną im przywrócone wartości domyślne.

3.10.6.4.3 Wykonywanie skryptów usługi

Oznacz wszystkie żądane pozycje, a następnie zapisz i zamknij skrypt. Uruchom zmodyfikowany skrypt bezpośrednio z poziomu okna głównego programu ESET SysInspector, wybierając z menu Plik polecenie **Uruchom skrypt usługi**. Po otwarciu skryptu w programie zostanie wyświetlone okno z następującym komunikatem: **Czy na pewno uruchomić skrypt usługi „%Nazwa_skryptu%”?**. Po potwierdzeniu może się pojawić kolejne ostrzeżenie z informacją, że uruchamiany skrypt usługi nie został podpisany. Aby uruchomić skrypt, należy kliknąć przycisk **Uruchom**.

Pomyślne wykonanie skryptu zostanie zasygnalizowane w oknie dialogowym.

Jeśli skrypt udało się przetworzyć tylko częściowo, zostanie wyświetlone okno dialogowe z następującym komunikatem: **Skrypt serwisowy został częściowo uruchomiony. Czy wyświetlić raport o błędach?** Aby wyświetlić szczegółowy raport o błędach zawierający listę niewykonanych operacji, należy kliknąć przycisk **Tak**.

Jeśli skrypt nie został rozpoznany, zostanie wyświetlone okno dialogowe z następującym komunikatem: **Wybrany skrypt usługi nie jest podpisany. Uruchamianie niepodpisanych i nieznanych skryptów może poważnie zaszkodzić danym na komputerze. Czy na pewno uruchomić skrypt i wykonać działania?** Może to być spowodowane niespójnością skryptu (uszkodzony nagłówek, błędny tytuł sekcji, brak pustego wiersza między sekcjami itd.). Można ponownie otworzyć plik skryptu i poprawić w nim błędy albo utworzyć nowy skrypt.

3.10.6.5 Często zadawane pytania

Czy do uruchomienia programu ESET SysInspector wymagane są uprawnienia administratora?

Do uruchomienia programu ESET SysInspector nie są wymagane uprawnienia administratora, jednak dostęp do niektórych informacji gromadzonych przez ten program można uzyskać tylko z konta administratora. Uruchomienie tego programu przez użytkownika z uprawnieniami standardowymi lub ograniczonymi spowoduje zgromadzenie mniejszej ilości informacji na temat środowiska operacyjnego.

Czy program ESET SysInspector tworzy plik dziennika?

W programie ESET SysInspector można utworzyć plik dziennika rejestrujący konfigurację komputera. Aby zapisać ten plik, należy kliknąć kolejno opcje **Plik** > **Zapisz dziennik** w oknie głównym programu. Dzienniki są zapisywane w formacie XML. Domyślnie pliki są zapisywane w katalogu *%USERPROFILE%\Moje dokumenty*, a przyjęta konwencja tworzenia nazw plików to SysInspector-%COMPUTERNAME%-RRMMDD-GGMM.XML. W razie potrzeby przed zapisaniem dziennika można zmienić lokalizację i nazwę jego pliku.

W jaki sposób można wyświetlić plik dziennika utworzony w programie ESET SysInspector?

Aby wyświetlić plik dziennika utworzony przez program ESET SysInspector, należy uruchomić ten program i w menu głównym kliknąć opcję **Plik** > **Otwórz dziennik**. Można również przeciągnąć i upuścić pliki dziennika w oknie aplikacji ESET SysInspector. Jeśli użytkownik często wyświetla pliki dziennika w programie ESET SysInspector, warto utworzyć skrót do pliku SYSINSPECTOR.EXE na pulpicie. W celu wyświetlenia dziennika wystarczy wtedy przeciągnąć i upuścić plik dziennika na ten skrót. Ze względów bezpieczeństwa systemy Windows Vista i Windows 7 mogą nie zezwalać na

operacje przeciągania i upuszczania między oknami z różnymi uprawnieniami zabezpieczeń.

Czy jest dostępna specyfikacja formatu pliku dziennika? Co z SDK?

Ponieważ program jest nadal opracowywany, aktualnie nie są dostępne specyfikacje pliku dziennika ani SDK. Po wydaniu programu specyfikacje zostaną udostępnione, z uwzględnieniem opinii i potrzeb klientów.

W jaki sposób program ESET SysInspector ocenia ryzyko związane z danym obiektem?

W większości przypadków poziomy ryzyka w programie ESET SysInspector są przypisywane do obiektów (plików, procesów, kluczy rejestru itd.) przy użyciu zestawu reguł heurystycznych, które umożliwiają zbadanie właściwości i ocenę potencjału szkodliwego działania poszczególnych obiektów. Na podstawie analizy heurystycznej obiektom przypisywane są poziomy ryzyka od 1 (Czysty — kolor zielony) do 9 (Ryzykowny — kolor czerwony). W lewym okienku nawigacyjnym sekcje są pokolorowane zgodnie z najwyższym poziomem ryzyka występującego w nich obiektu.

Czy poziom ryzyka 6 (nieznany — kolor czerwony) oznacza, że obiekt jest niebezpieczny?

Oceny wydawane przez program ESET SysInspector nie gwarantują, że dany obiekt jest szkodliwy. Ostateczny werdykt powinien wydać ekspert ds. bezpieczeństwa. Program ESET SysInspector zaprojektowano po to, aby eksperci ds. bezpieczeństwa mogli dokonać szybkiej oceny sytuacji i uzyskać informacje o tym, które obiekty w systemie powinni dokładniej zbadać pod kątem nietypowego działania.

Dlaczego program ESET SysInspector nawiązuje połączenie z Internetem po uruchomieniu?

Podobnie jak wiele innych aplikacji program ESET SysInspector jest podpisany przy użyciu certyfikatu z podpisem cyfrowym w celu zapewnienia, że został opublikowany przez firmę ESET i nie uległ modyfikacji. W celu zweryfikowania certyfikatu system operacyjny kontaktuje się z urzędem certyfikacji, co pozwala sprawdzić tożsamość wydawcy oprogramowania. Jest to normalne zachowanie w przypadku wszystkich cyfrowo podpisanych programów działających w systemie Microsoft Windows.

Co to jest technologia Anti-Stealth?

Technologia Anti-Stealth zapewnia skuteczne wykrywanie programów typu rootkit.

Jeśli system zostanie zaatakowany przez złośliwy kod zachowujący się jak program typu rootkit, użytkownik będzie narażony na uszkodzenie lub kradzież danych. Bez specjalnego narzędzia wykrycie takich programów jest prawie niemożliwe.

Dlaczego czasami niektóre pliki oznaczone jako „Podpisane przez MS” mają jednocześnie inny wpis „Nazwa firmy”?

Podczas próby zidentyfikowania sygnatury cyfrowej pliku wykonywalnego narzędzie ESET SysInspector wyszukuje najpierw osadzonej w pliku sygnatury cyfrowej. Jeśli ją znajdzie, uzna plik za zweryfikowany. Jeśli sygnatura cyfrowa nie zostanie znaleziona, program ESI rozpoczyna wyszukiwanie odpowiedniego pliku CAT (katalog zabezpieczeń — *%systemroot%**system32**catroot*), który zawiera informacje na temat przetwarzanego pliku wykonywalnego. Jeśli odpowiedni plik CAT zostanie znaleziony, podczas weryfikowania pliku wykonywalnego zostanie zastosowana sygnatura cyfrowa z pliku CAT.

Dlatego właśnie niektóre pliki są oznaczone jako „Podpisane przez MS”, ale zawierają różne wpisy w pozycji „Nazwa firmy”.

3.10.6.6 Program ESET SysInspector jako element oprogramowania ESET Endpoint Security

Aby otworzyć sekcję ESET SysInspector w programie ESET Endpoint Security, kliknij kolejno pozycje **Narzędzia** > **ESET SysInspector**. System zarządzania w oknie programu ESET SysInspector jest podobny do obsługi dzienników skanowania lub zaplanowanych zadań na komputerze. Wszystkie operacje dotyczące migawek systemu (tworzenie, wyświetlanie, porównywanie, usuwanie i eksportowanie) są dostępne po jednym lub dwóch kliknięciach.

Okno programu ESET SysInspector zawiera podstawowe informacje o utworzonych migawkach, takie jak godzina utworzenia, krótki komentarz, nazwa użytkownika, który utworzył migawkę, oraz stan migawki.

Aby porównać, utworzyć lub usunąć migawki, należy skorzystać z odpowiadających tym funkcjom przycisków umieszczonych pod listą migawek w oknie programu ESET SysInspector. Te opcje są także dostępne w menu

kontekstowym. Aby wyświetlić wybraną migawkę systemu, w menu kontekstowym należy kliknąć opcję **Pokaż**. Aby wyeksportować wybrany zapis stanu bieżącego do pliku, należy kliknąć go prawym przyciskiem myszy i wybrać opcję **Eksportuj...**.

Poniżej przedstawiono szczegółowy opis dostępnych opcji:

- **Porównaj** — umożliwia porównanie dwóch istniejących już dzienników. Ta opcja jest przydatna, gdy użytkownik chce prześledzić różnice między aktualnym a starszym dziennikiem. Aby skorzystać z tej opcji, należy wybrać dwie migawki, które mają zostać porównane.
- **Utwórz...** — umożliwia utworzenie nowego rekordu. Najpierw należy wprowadzić krótki komentarz dotyczący rekordu. Postęp tworzenia migawki (dotyczący aktualnie generowanej migawki) można sprawdzić w kolumnie **Stan**. Wszystkie zakończone migawki mają stan **Utworzono**.
- **Usuń/Usuń wszystkie** — umożliwia usunięcie pozycji z listy.
- **Eksportuj...** — powoduje zapisanie wybranej pozycji w pliku XML (także w wersji skompresowanej).

3.11 Słowniczek

3.11.1 Typy zagrożeń

Infekcja oznacza atak szkodliwego oprogramowania, które usiłuje uzyskać dostęp do komputera użytkownika i (lub) uszkodzić jego zawartość.

3.11.1.1 Wirusy

Wirus komputerowy to fragment złośliwego kodu, który jest dołączony do plików znajdujących się na komputerze. Nazwa tego typu programów pochodzi od wirusów biologicznych, ponieważ stosują one podobne techniki przenoszenia się z jednego komputera na drugi. Słowo „wirus” jest często stosowane nieprawidłowo na oznaczenie każdego rodzaju zagrożenia. Taka interpretacja powoli jednak zanika i stosowane jest ściślejsze określenie: „szkodliwe (lub złośliwe) oprogramowanie” (ang. malware, malicious software).

Wirusy komputerowe atakują głównie pliki wykonywalne i dokumenty. W skrócie wirus komputerowy działa w następujący sposób. po uruchomieniu zarażonego pliku złośliwy kod jest wywoływany i wykonywany przed właściwym uruchomieniem oryginalnej aplikacji. Wirus może zarazić dowolne pliki, do których bieżący użytkownik ma uprawnienia do zapisu.

Wirusy komputerowe różnią się pod względem odgrywanej roli i stopnia stwarzanego zagrożenia. Niektóre z nich są bardzo niebezpieczne, ponieważ mogą celowo usuwać pliki z dysku twardego. Część wirusów nie powoduje jednak żadnych szkód — celem ich działania jest tylko zirytowanie użytkownika i zademonstrowanie umiejętności programistycznych ich twórców.

Jeśli komputer jest zarażony wirusem, którego nie udaje się wyleczyć, należy przesłać go do laboratorium firmy ESET na oględziny. W niektórych przypadkach zarażone pliki mogą być zmodyfikowane w takim stopniu, że ich wyleczenie jest niemożliwe i trzeba je zastąpić zdrowymi kopiami.

3.11.1.2 Robaki

Robak komputerowy jest programem zawierającym złośliwy kod, który atakuje komputery-hosty. Robaki rozprzestrzeniają się za pośrednictwem sieci. Podstawowa różnica między wirusem a robakiem polega na tym, że ten ostatni potrafi się samodzielnie rozprzestrzeniać — nie musi w tym celu korzystać z plików nosicieli ani z sektorów rozruchowych dysku. Robaki rozpowszechniają się przy użyciu adresów e-mail z listy kontaktów oraz wykorzystują luki w zabezpieczeniach aplikacji sieciowych.

Robaki są przez to znacznie bardziej żywotne niż wirusy komputerowe. Ze względu na powszechność dostępu do Internetu mogą one rozprzestrzenić się na całym świecie w ciągu kilku godzin po opublikowaniu, a w niektórych przypadkach nawet w ciągu kilku minut. Możliwość szybkiego i niezależnego powielania się powoduje, że są one znacznie groźniejsze niż inne rodzaje szkodliwego oprogramowania.

Robak uaktywniony w systemie może być przyczyną wielu niedogodności: może usuwać pliki, obniżać wydajność komputera, a nawet blokować działanie programów. Natura robaka komputerowego predestynuje go do stosowania

w charakterze „środka transportu” dla innych typów szkodliwego oprogramowania.

Jeśli komputer został zainfekowany przez robaka, zaleca się usunięcie zainfekowanych plików, ponieważ prawdopodobnie zawierają one szkodliwy kod.

3.11.1.3 Konie trojańskie

Komputerowe konie trojańskie uznawano dotychczas za klasę zagrożeń, które udają pożyteczne programy, aby skłonić użytkownika do ich uruchomienia.

W związku z tym, że jest to bardzo pojemna kategoria, dzieli się ją często na wiele podkategorii:

- **Program pobierający (ang. downloader)** — szkodliwe programy, które mogą pobierać z Internetu inne zagrożenia.
- **Program zakażający (ang. dropper)** — szkodliwe programy, które mogą umieszczać na zaatakowanych komputerach inne rodzaje szkodliwego oprogramowania.
- **Program otwierający furtki (ang. backdoor)** — szkodliwe programy, które komunikują się ze zdalnymi intruzami, umożliwiając im uzyskanie dostępu do komputera i przejęcie nad nim kontroli.
- **Program rejestrujący znaki wprowadzane na klawiaturze (ang. keylogger, keystroke logger)** — program, który rejestruje znaki wprowadzane przez użytkownika i wysyła informacje o nich zdalnym intruzom.
- **Program nawiązujący kosztowne połączenia (ang. dialer)** — szkodliwe programy mające na celu nawiązywanie połączeń z kosztownymi numerami telefonicznymi zamiast z usługodawcą internetowym użytkownika. Zauważenie przez użytkownika nowego połączenia jest prawie niemożliwe. Programy takie mogą przynosić straty użytkownikom modemów telefonicznych, które nie są już regularnie używane.

Jeśli na komputerze zostanie wykryty plik uznany za konia trojańskiego, zaleca się jego usunięcie, ponieważ najprawdopodobniej zawiera złośliwy kod.

3.11.1.4 Programy typu rootkit

Programy typu rootkit są szkodliwymi aplikacjami, które przyznają internetowym intruzom nieograniczony dostęp do systemu operacyjnego, ukrywając zarazem ich obecność. Po uzyskaniu dostępu do komputera (zwykle z wykorzystaniem luki w jego zabezpieczeniach) programy typu rootkit używają funkcji systemu operacyjnego, aby uniknąć wykrycia przez oprogramowanie antywirusowe: ukrywają procesy, pliki i dane w rejestrze systemu Windows. Z tego powodu wykrycie ich przy użyciu zwykłych technik testowania jest prawie niemożliwe.

Wykrywanie programów typu rootkit odbywa się na dwóch poziomach:

1. Podczas próby uzyskania dostępu do systemu: Nie są one jeszcze w nim obecne, a zatem są nieaktywne. Większość aplikacji antywirusowych potrafi wyeliminować programy typu rootkit na tym poziomie (przy założeniu, że rozpoznają takie pliki jako zainfekowane).
2. Gdy są niewidoczne dla zwykłych narzędzi testowych. W programie ESET Endpoint Security zastosowano technologię AntiStealth, która umożliwia wykrywanie i usuwanie także aktywnych programów typu rootkit.

3.11.1.5 Adware

Adware to oprogramowanie utrzymywane z reklam. Do tej kategorii zaliczane są programy wyświetlające treści reklamowe. Aplikacje adware często powodują automatyczne otwieranie wyskakujących okienek zawierających reklamy lub zmianę strony głównej w przeglądarce internetowej. Oprogramowanie adware jest często dołączane do bezpłatnych programów, dzięki czemu ich autorzy mogą pokryć koszty tworzenia tych (zazwyczaj użytecznych) aplikacji.

Oprogramowanie adware samo w sobie nie jest niebezpieczne — użytkownikom mogą jedynie przeszkadzać wyświetlane reklamy. Niebezpieczeństwo związane z oprogramowaniem adware polega jednak na tym, że może ono zawierać funkcje śledzące (podobnie jak oprogramowanie spyware).

Jeśli użytkownik zdecyduje się użyć bezpłatnego oprogramowania, należy zwrócić szczególną uwagę na jego program instalacyjny. Podczas instalacji jest zazwyczaj wyświetlane powiadomienie o instalowaniu dodatkowych programów adware. Często jest dostępna opcja umożliwiająca anulowanie instalacji programu adware i zainstalowanie programu głównego bez dołączonego oprogramowania reklamowego.

W niektórych przypadkach zainstalowanie programu bez dołączonego oprogramowania adware jest niemożliwe lub

powoduje ograniczenie funkcjonalności. Dzięki temu oprogramowanie adware może zostać zainstalowane w systemie w sposób legalny, ponieważ użytkownik wyraża na to zgodę. W takim przypadku należy kierować się względami bezpieczeństwa. Jeśli na komputerze wykryto plik rozpoznany jako oprogramowanie adware, zaleca się jego usunięcie, ponieważ zachodzi duże prawdopodobieństwo, że zawiera on szkodliwy kod.

3.11.1.6 Spyware

Do tej kategorii należą wszystkie aplikacje, które wysyłają prywatne informacje bez zgody i wiedzy użytkownika. Korzystają one z funkcji śledzących do wysyłania różnych danych statystycznych, na przykład listy odwiedzonych witryn internetowych, adresów e-mail z listy kontaktów użytkownika lub listy znaków wprowadzanych za pomocą klawiatury.

Twórcy oprogramowania spyware twierdzą, że te techniki mają na celu uzyskanie pełniejszych informacji o potrzebach i zainteresowaniach użytkowników oraz umożliwiają bardziej trafne kierowanie reklam do odbiorców. Problem polega jednak na tym, że nie ma wyraźnego rozgraniczenia między aplikacjami pożytecznymi i szkodliwymi, i nikt nie może mieć pewności, czy gromadzone informacje nie zostaną wykorzystane w niedozwolony sposób. Dane pozyskiwane przez aplikacje szpiegujące mogą zawierać kody bezpieczeństwa, kody PIN, numery kont bankowych itd. Aplikacja szpiegująca jest często umieszczana w bezpłatnej wersji programu przez jego autora w celu uzyskania środków pieniężnych lub zachęcenia użytkownika do nabycia edycji komercyjnej. Nierzadko podczas instalacji programu użytkownicy są informowani o obecności oprogramowania spyware, co ma ich skłonić do zakupu pozbawionej go wersji płatnej.

Przykładami popularnych bezpłatnych produktów, do których dołączone jest oprogramowanie szpiegujące, są aplikacje klienckie sieci P2P (ang. peer-to-peer). Programy Spyfalcon i Spy Sheriff (oraz wiele innych) należą do szczególnej podkategorii oprogramowania spyware. Wydają się zapewniać przed nim ochronę, ale w rzeczywistości same są takimi programami.

Jeśli na komputerze zostanie wykryty plik rozpoznany jako spyware, zaleca się jego usunięcie, ponieważ z dużym prawdopodobieństwem zawiera on szkodliwy kod.

3.11.1.7 Programy spakowane

Program spakowany to plik wykonywalny samorozpakowujący się w środowisku wykonawczym. Może zawierać wiele rodzajów szkodliwego oprogramowania w jednym pakiecie.

Najpopularniejsze programy spakowane to UPX, PE_Compact, PKLite i ASPack. To samo szkodliwe oprogramowanie można wykryć w inny sposób — kompresując je za pomocą innego programu pakującego. Programy spakowane potrafią przeprowadzać mutacje swoich „sygnatur” w czasie, co utrudnia wykrywanie i usuwanie szkodliwego oprogramowania.

3.11.1.8 Potencjalnie niebezpieczne aplikacje

Istnieje wiele legalnych programów, które ułatwiają administrowanie komputerami podłączonymi do sieci. Jednak w niewłaściwych rękach mogą one zostać użyte do wyrządzenia szkód. Program ESET Endpoint Security zawiera narzędzia pozwalające wykrywać takie zagrożenia.

Potencjalnie niebezpieczne aplikacje to kategoria, do której należą niektóre legalne programy komercyjne. Są to m.in. narzędzia do dostępu zdalnego, programy do łamania haseł i programy rejestrujące znaki wprowadzane na klawiaturze.

W przypadku wykrycia działającej na komputerze aplikacji potencjalnie niebezpiecznej, która nie została zainstalowana świadomie przez użytkownika, należy skonsultować się z administratorem sieci lub ją usunąć.

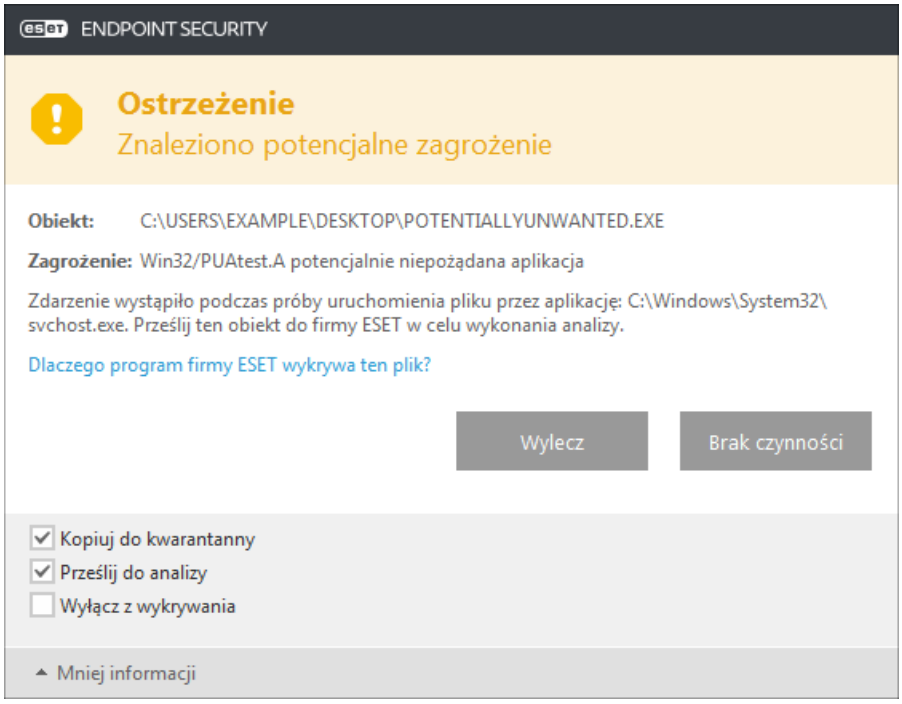
3.11.1.9 Potencjalnie niepożądane aplikacje

Potencjalnie niepożądana aplikacja to program, który zawiera oprogramowanie typu adware, instaluje paski narzędzi lub wykonuje inne niejasne działania. W niektórych sytuacjach użytkownik może uznać, że korzyści związane z potencjalnie niepożądaną aplikacją są większe niż zagrożenia. Z tego powodu ESET przydziela takim aplikacjom kategorię niskiego ryzyka w porównaniu do innych typów złośliwego oprogramowania, takich jak konie trojańskie czy robaki.

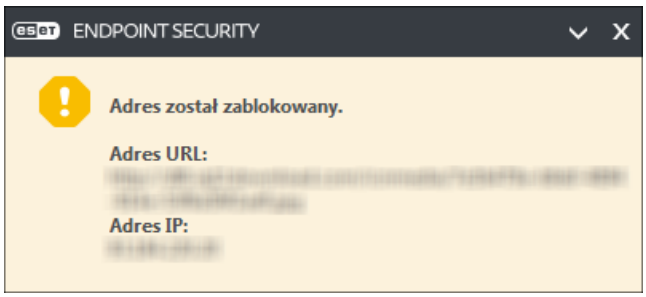
Ostrzeżenie — znaleziono potencjalne zagrożenie

W przypadku wykrycia potencjalnie niepożądanej aplikacji użytkownik ma możliwość wybrania czynności:

1. **Wylecz/Rozłącz**: ta opcja przerywa wykonywanie czynności i uniemożliwia potencjalnemu zagrożeniu przedostanie się do systemu.
2. **Brak czynności**: ta opcja umożliwia potencjalnemu zagrożeniu przedostanie się do systemu.
3. Aby w przyszłości umożliwić uruchamianie aplikacji na komputerze bez zakłóceń, należy kliknąć opcję **Więcej informacji/Pokaż opcje zaawansowane** i zaznaczyć pole wyboru obok opcji **Wyłącz z wykrywania**.

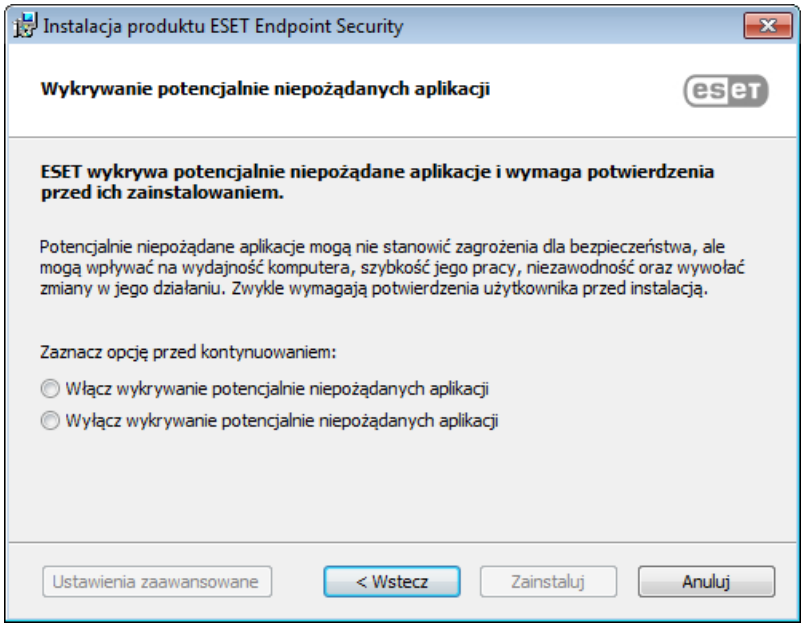


W przypadku wykrycia potencjalnie niepożądanej aplikacji, której nie można wyleczyć, w prawym dolnym rogu ekranu zostanie wyświetlone okno powiadomienia **Adres został zablokowany**. Więcej informacji na temat tego zdarzenia można znaleźć, przechodząc z menu głównego do opcji **Narzędzia** > **Pliki dziennika** > **Filtrowane witryny internetowe**.



Potencjalnie niepożądane aplikacje — ustawienia

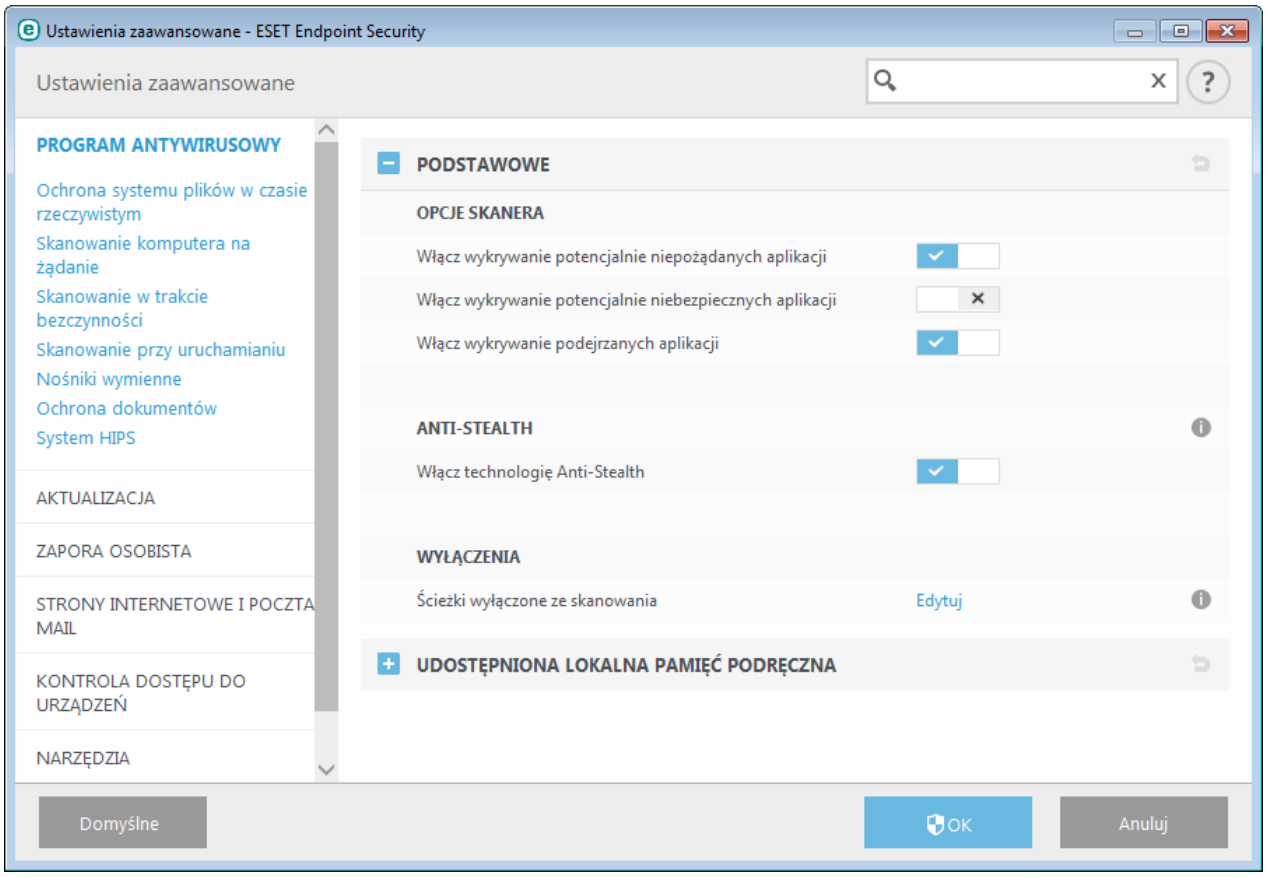
Podczas instalowania produktu ESET można zdecydować, czy włączone ma być wykrywanie potencjalnie niepożądanych aplikacji, jak widać poniżej:



Potencjalnie niepożądane aplikacje mogą instalować oprogramowanie typu adware i paski narzędzi lub obejmować inne niepożądane i niebezpieczne funkcje.

Te ustawienia można zmienić w dowolnym momencie w ustawieniach programu. Aby włączyć lub wyłączyć wykrywanie potencjalnie niepożądanych, niebezpiecznych lub podejrzanych aplikacji, należy wykonać poniższe instrukcje:

1. Otwórz produkt ESET. Otwieranie produktu ESET
2. Naciśnij klawisz **F5**, by uzyskać dostęp do obszaru **Ustawienia zaawansowane**.
3. Kliknij opcję **Ochrona antywirusowa** i zgodnie z własnym uznaniem włącz lub wyłącz opcje **Włącz wykrywanie potencjalnie niepożądanych aplikacji**, **Włącz wykrywanie potencjalnie niebezpiecznych aplikacji** oraz **Włącz wykrywanie podejrzanych aplikacji**. Potwierdź, klikając przycisk **OK**.



Potencjalnie niepożądane aplikacje — otoki oprogramowania

Otoka oprogramowania to szczególnego typu modyfikacja aplikacji stosowana na niektórych stronach internetowych obsługujących hosting plików. To narzędzie strony trzeciej, które instaluje oprogramowanie pobrane przez użytkownika, instalując jednak przy tym dodatkowe oprogramowanie, takie jak paski narzędzi i oprogramowanie typu adware. Dodatkowe oprogramowanie może również modyfikować ustawienia strony głównej oraz wyszukiwania w przeglądarce użytkownika. Ponadto strony obsługujące hosting plików często nie powiadamiają dostawcy oprogramowania ani użytkownika pobierającego pliki o wprowadzonych modyfikacjach, a zrezygnowanie z tych modyfikacji jest zwykle utrudnione. Z tego względu oprogramowanie ESET klasyfikuje otoki oprogramowania jako jeden z rodzajów potencjalnie niepożądanych aplikacji, oferując użytkownikom możliwość zaakceptowania lub zrezygnowania z pobierania.

Zaktualizowaną wersję tej strony pomocy zawiera ten artykuł bazy wiedzy ESET.

3.11.1.10 Botnet

Boty, zwane również robotami sieciowymi, to zautomatyzowane szkodliwe oprogramowanie skanujące bloki adresów sieciowych, infekujące niezabezpieczone komputery. Tego rodzaju programy umożliwiają hakerom przejmowanie kontroli nad wieloma komputerami równocześnie w celu przekształcenia ich w kolejne boty (określane również mianem zombie). Hakerzy wykorzystują zwykle boty do infekowania znacznej liczby komputerów. Duża grupa zainfekowanych w ten sposób komputerów tworzy sieć, określaną mianem botnetu. Gdy komputer zostanie zainfekowany i stanie się częścią botnetu, może posłużyć do przeprowadzania ataków typu odmowa usługi (DDoS), a także do realizowania zautomatyzowanych zadań przez Internet bez wiedzy użytkownika (na przykład do wysyłania spamu, wirusów lub do kradzieży danych osobowych i danych poufnych, takich jak poświadczenia bankowe czy numery kart kredytowych).

3.11.2 Typy ataków zdalnych

Istnieje wiele specjalnych technik, które pozwalają napastnikom na stworzenie zagrożenia dla bezpieczeństwa komputerów zdalnych. Techniki te można podzielić na kilka kategorii.

3.11.2.1 Ataki robaków

Robak komputerowy jest programem zawierającym szkodliwy kod, który atakuje komputery-hosty. Robaki rozprzestrzeniają się za pośrednictwem sieci. Robaki sieciowe wykorzystują luki w zabezpieczeniach różnych aplikacji. Ze względu na wszechobecność Internetu mogą one rozprzestrzenić się po całym świecie w ciągu kilku godzin po opublikowaniu.

Większości ataków robaków da się uniknąć stosując domyślne ustawienia ochrony w zaporze. Ważne jest również, by sieciach publicznych wybierać typ ochrony **Sieć publiczna** oraz by aktualizować swój system operacyjny i swoje programy za pomocą najnowszych poprawek zabezpieczeń.

3.11.2.2 Ataki typu „odmowa usługi" (DoS)

Atak typu „odmowa usługi" (DoS, *Denial of Service*) jest próbą uniemożliwienia użytkownikom dostępu do danego komputera lub sieci. Komunikacja między użytkownikami, którzy padli ofiara takiego ataku, jest utrudniona i nie odbywa się w sposób prawidłowy. Komputery będące celem ataku typu „odmowa usługi" zazwyczaj muszą być ponownie uruchomione w celu przywrócenia ich prawidłowego działania.

W większości przypadków ataki tego typu są wymierzone w serwery internetowe. W ich wyniku serwery są przez pewien czas niedostępne dla użytkowników.

3.11.2.3 Skanowanie portów

Skanowanie portów służy do ustalenia, które porty na hoście sieciowym są otwarte. Oprogramowanie przeznaczone do znajdowania takich portów to skaner portów.

Port komputera jest wirtualnym punktem, przez który przepływają dane przychodzące i wychodzące. Ma on niezwykle istotne znaczenie z punktu widzenia bezpieczeństwa. W dużej sieci informacje zbierane przez skanery portów mogą pomagać w identyfikowaniu potencjalnych luk w zabezpieczeniach. Takie korzystanie ze skanerów jest jak najbardziej dozwolone.

Skanowanie portów jest jednak często wykorzystywane przez hakerów próbujących naruszyć bezpieczeństwo systemów. Ich pierwszym działaniem jest wysyłanie pakietów do każdego portu. Zależnie od typu uzyskanej odpowiedzi można określić, które porty znajdują się w użyciu. Samo skanowanie nie powoduje żadnych uszkodzeń, ale należy pamiętać, że może ono prowadzić do ujawnienia potencjalnych luk w zabezpieczeniach i pozwolić intruzom na przejęcie kontroli nad komputerami zdalnymi.

Administratorom sieci zaleca się blokowanie wszystkich nieużywanych portów oraz zabezpieczanie używanych portów przed nieupoważnionym dostępem.

3.11.2.4 Preparowanie pakietów DNS

Preparując pakiety DNS (Domain Name Server — serwer nazw domeny), hakerzy mogą oszukać serwer DNS dowolnego komputera tak, aby ten klasyfikował fałszywe dane jako autentyczne i poprawne. Fałszywe informacje są przechowywane przez pewien czas w pamięci podręcznej, co pozwala atakującym sfałszować odpowiedzi serwera DNS dotyczące adresów IP. W efekcie użytkownicy próbujący uzyskać dostęp do witryn internetowych zamiast ich oryginalnej zawartości pobierają wirusy komputerowe lub robaki.

3.11.3 Poczta e-mail

Poczta e-mail, czyli poczta elektroniczna, to nowoczesna forma komunikacji oferująca wiele korzyści. Umożliwia szybką, elastyczną i bezpośrednią komunikację, a ponadto odegrała kluczową rolę w rozpowszechnianiu Internetu we wczesnych latach 90. ubiegłego wieku.

Niestety wysoki poziom anonimowości podczas korzystania z poczty e-mail i Internetu pozostawia obszar dla nielegalnych działań, na przykład rozsyłania spamu. Spam można podzielić na niechciane reklamy, fałszywe alarmy oraz wiadomości rozpowszechniające szkodliwe oprogramowanie. Zagrożenie dla użytkownika jest tym większe, że koszty wysyłania wiadomości są znikome, a autorzy spamu mają dostęp do wielu narzędzi i źródeł udostępniających nowe adresy e-mail. Dodatkowo objętość i różnorodność spamu bardzo utrudnia jego regulowanie. Im dłużej jest używany dany adres e-mail, tym większe jest prawdopodobieństwo, że znajdzie się on w bazie danych mechanizmu wysyłającego spam. Oto kilka wskazówek zapobiegawczych:

- Jeśli to możliwe, nie publikuj swojego adresu e-mail w Internecie.
- Informuj o swoim adresie e-mail tylko zaufane osoby.
- W miarę możliwości nie używaj popularnych aliasów — bardziej skomplikowane aliasy zmniejszają prawdopodobieństwo śledzenia.
- Nie odpowiadaj na spam, który znalazł się w skrzynce odbiorczej.
- Zachowuj ostrożność podczas wypełniania formularzy internetowych. Zwracaj szczególną uwagę na opcje typu „Tak, chcę otrzymywać informacje dotyczące...”.
- Używaj „wyspecjalizowanych” adresów e-mail, na przykład innego w pracy, innego do komunikacji ze znajomymi itd.
- Od czasu do czasu zmieniaj adres e-mail.
- Używaj rozwiązania antyspamowego.

3.11.3.1 Reklamy

Reklama internetowa jest jedną z najszybciej rozwijających się form działalności reklamowej. Główne zalety marketingowe reklamy tego typu to minimalne koszty oraz bezpośrednie, niemal natychmiastowe przekazywanie wiadomości. Wiele firm stosuje narzędzia marketingowe związane z pocztą e-mail, aby efektywnie komunikować się z obecnymi i potencjalnymi klientami.

Ten sposób reklamy jest pożądany, ponieważ użytkownicy mogą być zainteresowani otrzymywaniem informacji handlowych na temat określonych produktów. Wiele firm wysyła jednak dużą liczbę niepożądanych wiadomości o treści handlowej. W takich przypadkach reklama za pośrednictwem poczty e-mail wykracza poza dopuszczalne granice i staje się spamem.

Niepożądane wiadomości e-mail stanowią rzeczywisty problem, a ich liczba niestety nie maleje. Autorzy niepożądanych wiadomości e-mail próbują często stworzyć pozory, że przesyłany przez nich spam jest pożądany.

3.11.3.2 Fałszywe alarmy

Fałszywy alarm to nieprawdziwa wiadomość przesyłana przez Internet. Fałszywe alarmy są zwykle rozsyłane za pośrednictwem poczty e-mail lub narzędzi komunikacyjnych, takich jak Gadu-Gadu i Skype. Sama wiadomość to często żart lub plotka.

Fałszywe alarmy dotyczące wirusów komputerowych mają na celu wzbudzanie w odbiorcach strachu, niepewności i wątpliwości. Mają oni wierzyć, że istnieje „niewykrywalny wirus” usuwający pliki i pobierający hasła lub wykonujący w ich systemie jakieś inne szkodliwe działania.

Niektóre fałszywe alarmy zawierają prośbę do odbiorcy o przekazanie wiadomości wszystkim osobom z jego książki adresowej, co sprzyja dalszemu rozprzestrzenianiu się alarmu. Istnieją fałszywe alarmy na telefony komórkowe, a także spreparowane prośby o pomoc, informacje o ludziach oferujących wysłanie pieniędzy z zagranicy itd. W większości przypadków nie sposób określić intencji twórcy.

Wiadomość z prośbą o przekazanie jej do wszystkich znajomych z dużym prawdopodobieństwem jest takim fałszywym alarmem. W Internecie dostępnych jest wiele witryn, w których można zweryfikować prawdziwość wiadomości e-mail. Przed przekazaniem dalej wiadomości, która jest podejrzana, dobrze jest zweryfikować ją w Internecie.

3.11.3.3 Ataki typu „phishing”

Terminem „phishing” określa się działania przestępcze, obejmujące stosowanie socjotechnik (manipulowanie użytkownikami w celu uzyskania poufnych informacji). Działania takie są podejmowane z myślą o uzyskaniu dostępu do prywatnych danych, np. numerów kont bankowych, kodów PIN itp.

Dostęp jest zwykle uzyskiwany w wyniku podszycia się pod osobę lub firmę godną zaufania (np. instytucję finansową, towarzystwo ubezpieczeniowe) w spreparowanej wiadomości e-mail. Wiadomość taka jest łudząco podobna do oryginalnej, ponieważ zawiera materiały graficzne i tekstowe mogące pochodzić ze źródła, pod które podszywa się nadawca. W tego typu wiadomości znajduje się prośba o wprowadzenie (pod dowolnym pretekstem np. weryfikacji danych, operacji finansowych) pewnych poufnych informacji — numerów kont bankowych lub nazw użytkownika i haseł. Wszystkie dane tego typu mogą zostać po wysłaniu bez trudu przechwycone i wykorzystane do działań na szkodę użytkownika.

Banki, towarzystwa ubezpieczeniowe i inne wiarygodne firmy nigdy nie proszą o podanie nazwy użytkownika i hasła w wiadomościach e-mail przesyłanych bez uprzedzenia.

3.11.3.4 Rozpoznawanie spamu

Istnieje kilka elementów, które mogą pomóc w identyfikacji spamu (niepożądanych wiadomości e-mail) w skrzynce pocztowej. Jeśli wiadomość spełnia przynajmniej niektóre z następujących kryteriów, jest to najprawdopodobniej spam.

- Adres nadawcy nie należy do nikogo z listy kontaktów.
- Wiadomość zawiera ofertę uzyskania dużej sumy pieniędzy pod warunkiem uprzedniego wpłacenia niewielkiej kwoty.
- Wiadomość zawiera prośbę o wprowadzenie poufnych danych (takich jak numery kont bankowych, nazwy użytkowników i hasła) pod różnymi pretekstami, takimi jak weryfikacja danych czy konieczność przeprowadzenia operacji finansowych.
- Wiadomość jest napisana w obcym języku.
- Wiadomość zawiera prośbę o zakup produktu, którym użytkownik nie jest zainteresowany. W przypadku podjęcia decyzji o kupnie należy sprawdzić, czy nadawca wiadomości jest wiarygodnym dostawcą (należy skonsultować się z oryginalnym producentem produktu).
- Niektóre słowa zawierają literówki, aby oszukać filtr antyspamowy, na przykład „vaigra” zamiast „viagra” itp.

3.11.3.4.1 Reguły

W przypadku modułu antyspamowego i programów poczty e-mail reguł używa się do konfigurowania funkcji poczty elektronicznej. Reguły składają się z dwóch składników logicznych:

1. warunku (na przykład wiadomość przychodząca z określonego adresu),
2. działania (np. usunięcie wiadomości, przeniesienie jej do określonego folderu).

Liczba i kombinacje reguł zmieniają się w zależności od programu antyspamowego. Reguły służą w nim do przeciwdziałania spamowi (niechcianym wiadomościom). Typowe przykłady:

- 1. Warunek: przychodząca wiadomość e-mail zawiera pewne słowa spotykane zwykle w spamie.
  2. Czynność: usunięcie wiadomości.
- 1. Warunek: przychodząca wiadomość e-mail zawiera załącznik z rozszerzeniem EXE.
  2. Czynność: usunięcie załącznika i dostarczenie wiadomości do skrzynki odbiorczej.
- 1. Warunek: przychodząca wiadomość e-mail pochodzi od pracodawcy.
  2. Czynność: przeniesienie wiadomości do folderu „Praca”.

Zalecane jest stosowanie w programach antyspamowych różnych kombinacji reguł w celu ułatwienia administrowania i zwiększenia skuteczności filtrowania spamu.

3.11.3.4.2 Biała lista

Biała lista to wykaz obiektów lub osób, które uzyskały akceptację lub którym przyznano zezwolenie. Termin „biała lista poczty e-mail” oznacza listę kontaktów, od których użytkownik chce otrzymywać wiadomości. Tego typu białe listy są tworzone z wykorzystaniem słów kluczowych wyszukiwanych w adresach e-mail, nazwach domen lub adresach IP.

Jeśli biała lista działa w „trybie wyłączności”, korespondencja pochodząca z figurujących na niej adresów e-mail, domen i adresów IP nie będzie odbierana. Jeśli nie jest stosowana wyłączność, takie wiadomości nie będą usuwane, a jedynie w określony sposób odfiltrowywane.

Zasada działania białej listy jest odwrotna niż w przypadku czarnej listy. Białe listy są względnie łatwe w zarządzaniu, zwłaszcza w porównaniu z czarnymi listami. Zalecane jest korzystanie zarówno z białej, jak i z czarnej listy w celu skuteczniejszego odfiltrowywania spamu.

3.11.3.4.3 Czarna lista

W znaczeniu ogólnym czarna lista jest listą nieakceptowanych osób i zabronionych obiektów. W świecie wirtualnym jest to technika umożliwiająca odbieranie wiadomości od wszystkich użytkowników, którzy nie znajdują się na takiej liście.

Istnieją dwa typy czarnych list: tworzone przez użytkowników za pomocą aplikacji antyspamowych oraz dostępne w Internecie, profesjonalne, regularnie aktualizowane czarne listy sporządzane przez wyspecjalizowane instytucje.

Skuteczne blokowanie spamu wymaga stosowania czarnych list, jednak są one bardzo trudne w utrzymaniu, ponieważ codziennie pojawiają się nowe obiekty, które należy blokować. W celu najefektywniejszego filtrowania spamu zalecamy korzystanie zarówno z białej listy, jak i z czarnej listy.

3.11.3.4.4 Lista wyłączeń

Lista wyłączeń zawiera zwykle adresy e-mail, które mogą być sfałszowane metodą spoofingu i mogą służyć do wysyłania spamu. Wiadomości e-mail nadane z adresu występującego na liście wyłączeń są zawsze skanowane pod kątem spamu. Domyślnie lista wyłączeń zawiera wszystkie adresy e-mail znajdujące się na istniejących kontach pocztowych użytkownika.

3.11.3.4.5 Kontrola po stronie serwera

Kontrola po stronie serwera to technika umożliwiająca identyfikację masowo rozsyłanej poczty e-mail będącej spamem na podstawie liczby otrzymanych wiadomości oraz reakcji użytkowników. Każda wiadomość pozostawia na serwerze unikatowy cyfrowy „odcisk”, ustalony na podstawie jej zawartości. Taki unikatowy numer identyfikacyjny nie zawiera żadnych informacji na temat zawartości wiadomości e-mail. Dwie identyczne wiadomości mają identyczne „odciski”, natomiast różne wiadomości mają różne „odciski”.

Jeśli wiadomość zostaje oznaczona jako spam, jej „odcisk” jest wysyłany do serwera. Jeśli na serwerze odebranych zostanie więcej identycznych „odcisków” (odpowiadających określonym wiadomościom będącym spamem), „odcisk” ten zostanie umieszczony w bazie danych spamu. Podczas skanowania wiadomości przychodzących program wysyła ich „odciski” do serwera. Serwer zwraca informacje o „odciskach” odpowiadających wiadomościom już oznaczonym przez użytkowników jako spam.

3.11.4 Technologia firmy ESET

3.11.4.1 Blokada programów typu Exploit

Blokada programów typu Exploit ma na celu wzmocnienie używanych zazwyczaj aplikacji, takich jak przeglądarki internetowe, przeglądarki plików PDF, programy poczty e-mail oraz składniki pakietu MS Office. Jej działanie polega na monitorowaniu procesów pod kątem podejrzanych działań, które mogą wskazywać na wykorzystanie istniejącej luki w zabezpieczeniach. Stanowi ona dodatkową, przybliżającą do intruzów warstwę zabezpieczeń, co osiągnięto dzięki wykorzystaniu zupełnie innej technologii niż w przypadku technik skoncentrowanych na wykrywaniu samych szkodliwych plików.

Gdy blokada programów typu Exploit zidentyfikuje podejrzany proces, może zatrzymać ten proces natychmiast i zarejestrować dane dotyczące zagrożenia, które zostają następnie przesłane do systemu ESET Live Grid w chmurze. Te dane są przetwarzane przez laboratorium firmy ESET i wykorzystywane w celu zapewnienia wszystkim użytkownikom skuteczniejszej ochrony przed nieznanymi zagrożeniami oraz niespotykanymi dotąd atakami (nowo opublikowanym szkodliwym oprogramowaniem, na które nie ma jeszcze wstępnie skonfigurowanych środków zaradczych).

3.11.4.2 Zaawansowany skaner pamięci

Zaawansowany skaner pamięci działa w połączeniu z blokadą programów typu Exploit w celu zapewnienia skuteczniejszej ochrony przed szkodliwym oprogramowaniem, które unika wykrycia przez produkty do ochrony przed szkodliwym oprogramowaniem poprzez zastosowanie zaciemniania kodu i/lub szyfrowania. W przypadkach, gdy zwykła emulacja lub heurystyka może nie wykryć zagrożenia, zaawansowany skaner pamięci jest w stanie zidentyfikować podejrzane zachowanie i przeskanować zagrożenia, gdy ujawnią się w pamięci systemowej. To rozwiązanie działa skutecznie w odniesieniu do szkodliwego oprogramowania, w którym stosowane jest zaciemnianie kodu. W przeciwieństwie do blokady programów typu Exploit w tym narzędziu zastosowano metodę działania po wykonaniu, co jest równoznaczne z ryzykiem, że część szkodliwych działań mogła zostać przeprowadzona przed wykryciem zagrożenia. Jednak w przypadkach, gdy inne techniki wykrywania okażą się zawodne, stanowi ono dodatkową warstwę zabezpieczeń.

3.11.4.3 ESET Live Grid

Zbudowany na technologii ThreatSense.Net® zaawansowany system wczesnego ostrzegania ESET Live Grid gromadzi informacje przesyłane przez użytkowników programów ESET z całego świata i przekazuje je do laboratorium firmy ESET. Dostarczając nam próbki podejrzanych plików oraz metadane, system ESET Live Grid umożliwia nam natychmiastowe reagowanie na potrzeby naszych klientów oraz konfigurowanie narzędzi ESET tak, aby zapewniały ochronę przed najnowszymi zagrożeniami. Analitycy firmy ESET zajmujący się szkodliwym oprogramowaniem wykorzystują te informacje do opracowywania precyzyjnych zapisów rodzaju i zakresu globalnych zagrożeń. Umożliwia nam to skoncentrowanie się na odpowiednich celach. Dane systemu ESET Live Grid odgrywają istotną rolę w ustalaniu priorytetów w naszych procedurach automatycznych.

Ponadto wdrożony jest system reputacji, który umożliwia zwiększenie ogólnej skuteczności naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem. Gdy w systemie użytkownika sprawdzany jest plik wykonywalny, jego znacznik porównywany jest z zawartością bazy danych elementów uwzględnionych na białej i czarnej liście. Jeśli znajduje się na białej liście, sprawdzany plik zostaje uznany za czysty i oznaczony w celu wykluczenia ze skanowania w przyszłości. Jeśli znajduje się na czarnej liście, podjęte zostają odpowiednie działania, w zależności od rodzaju zagrożenia. W przypadku nieznalezienia znacznika plik zostaje dokładnie przeskanowany. W zależności od wyników tego skanowania pliki zostają skategoryzowane jako stanowiące zagrożenie lub niestanowiące zagrożenia. To rozwiązanie ma znaczący pozytywny wpływ na wydajność skanowania.

Ten system reputacji umożliwia skuteczne wykrywanie próbek szkodliwego oprogramowania, nawet przed przekazaniem odpowiednich sygnatur użytkownikom za pośrednictwem aktualizacji bazy sygnatur wirusów odbywających się kilka razy dziennie.

3.11.4.4 Ochrona przed botnetami

Funkcja ochrony przed botnetami umożliwia wykrywanie szkodliwego oprogramowania poprzez analizowanie protokołów komunikacji sieciowej. Szkodliwe oprogramowanie w postaci botnetów podlega częstym zmianom, w przeciwieństwie do protokołów sieciowych, które w ostatnich latach nie były modyfikowane. Dzięki tej nowej technologii narzędzia firmy ESET zwalczają szkodliwe oprogramowanie próbujące połączyć komputer użytkownika z siecią botnetów.

3.11.4.5 Blokada programów typu Exploit w środowisku Java

Blokada Java to rozszerzenie dotychczasowej ochrony stosowanej w rozwiązaniach ESET, polegającej na blokadzie programów typu Exploit. Służy do monitorowania środowiska Java w poszukiwaniu zachowań wskazujących na programy typu Exploit. Próbki zablokowanych obiektów można zgłosić do analityków zajmujących się szkodliwym oprogramowaniem, co umożliwi im utworzenie sygnatur blokujących próby użycia programów typu Exploit w środowisku Java na poszczególnych warstwach (blokowanie adresów URL, pobieranie plików itp.).