

ESET NOD32 Antivirus 4 Business Edition dla Mac OS X

Instrukcja instalacji i Podręcznik użytkownika

[Kliknij tutaj, aby pobrać najnowszą wersję niniejszego dokumentu](#)



ESET NOD32 Antivirus 4

Copyright ©2011 ESET, spol. s.r.o.

Oprogramowanie ESET NOD32 Antivirus zostało opracowane przez firmę ESET, spol. s r.o.

Więcej informacji można uzyskać w witrynie www.eset.com.

Wszelkie prawa zastrzeżone. Żadna część niniejszej dokumentacji nie może być powielana, przechowywana w systemie pobierania ani przesyłana w żadnej formie bądź przy użyciu jakichkolwiek środków elektronicznych, mechanicznych, przez fotokopiowanie, nagrywanie, skanowanie lub w inny sposób bez uzyskania pisemnego zezwolenia autora.

Firma ESET, spol. s r.o. zastrzega sobie prawo do wprowadzania zmian w dowolnych elementach opisanego oprogramowania bez uprzedniego powiadomienia.

Dział obsługi klienta — cały świat: www.eset.com/support

WER. 5. 9. 2011

Spis treści

1. ESET NOD32 Antivirus.....	4
1.1 Wymagania systemowe.....	4
2. Instalacja.....	5
2.1 Instalacja typowa.....	5
2.2 Instalacja niestandardowa.....	5
2.3 Instalacja zdalna.....	6
2.3.1 Tworzenie pakietu instalacji zdalnej.....	6
2.3.2 Instalacja zdalna na docelowych komputerach.....	7
2.3.3 Zdalne odinstalowanie.....	7
2.3.4 Zdalne uaktualnienie.....	7
2.4 Wprowadzanie nazwy użytkownika i hasła.....	7
2.5 Skanowanie komputera na żądanie.....	7
3. Przewodnik dla początkujących.....	8
3.1 Tryby interfejsu użytkownika — wprowadzenie.....	8
3.1.1 Sprawdzanie działania systemu.....	8
3.1.2 Postępowanie w przypadku, gdy program nie działa poprawnie.....	8
4. Praca z programem ESET NOD32 Antivirus.....	10
4.1 Antywirus i antyspyware.....	10
4.1.1 Ochrona systemu plików w czasie rzeczywistym.....	10
4.1.1.1 Ustawienia ochrony w czasie rzeczywistym.....	10
4.1.1.1.1 Skanowanie po wystąpieniu zdarzenia.....	10
4.1.1.1.2 Zaawansowane opcje skanowania.....	10
4.1.1.1.3 Wykluczenia ze skanowania.....	10
4.1.1.2 Modyfikowanie ustawień ochrony w czasie rzeczywistym.....	11
4.1.1.3 Sprawdzanie skuteczności ochrony w czasie rzeczywistym.....	11
4.1.1.4 Co należy zrobić, jeśli ochrona w czasie rzeczywistym nie działa.....	11
4.1.2 Skanowanie komputera na żądanie.....	11
4.1.2.1 Typ skanowania.....	12
4.1.2.1.1 Skanowanie inteligentne.....	12
4.1.2.1.2 Skanowanie niestandardowe.....	12
4.1.2.2 Skanowane obiekty.....	12
4.1.2.3 Profile skanowania.....	12
4.1.3 Ustawienia parametrów technologii ThreatSense.....	13
4.1.3.1 Obiekty.....	13
4.1.3.2 Opcje.....	13
4.1.3.3 Leczenie.....	14
4.1.3.4 Rozszerzenia.....	14
4.1.3.5 Limity.....	14
4.1.3.6 Inne.....	14
4.1.4 Wykryto infekcję.....	14
4.2 Aktualizowanie programu.....	15
4.2.1 Uaktualnianie do nowej kompilacji.....	15
4.2.2 Ustawienia aktualizacji.....	16
4.2.3 Tworzenie zadań aktualizacji.....	16
4.3 Harmonogram.....	16
4.3.1 Cel planowania zadań.....	17
4.3.2 Tworzenie nowych zadań.....	17
4.4 Kwarantanna.....	17
4.4.1 Poddawanie plików kwarantannie.....	18
4.4.2 Przywracanie plików z kwarantanny.....	18
4.4.3 Przesyłanie pliku z kwarantanny.....	18
4.5 Pliki dziennika.....	18
4.5.1 Konserwacja dziennika.....	18
4.5.2 Filtrowanie dziennika.....	18
4.6 Interfejs użytkownika.....	19
4.6.1 Alerty i powiadomienia.....	19
4.6.1.1 Zaawansowane ustawienia alertów i powiadomień.....	19
4.6.2 Uprawnienia.....	19
4.6.3 Menu kontekstowe.....	19
4.7 ThreatSense.Net.....	20
4.7.1 Podejrzane pliki.....	20
5. Użytkownik zaawansowany.....	22
5.1 Import i eksport ustawień.....	22
5.1.1 Import ustawień.....	22
5.1.2 Eksport ustawień.....	22
5.2 Ustawienia serwera proxy.....	22
5.3 Blokowanie nośników wymiennych.....	22
5.4 Administracja zdalna.....	22
6. Słowniczek.....	24
6.1 Typy infekcji.....	24
6.1.1 Wirusy.....	24
6.1.2 Robaki.....	24
6.1.3 Konie trojańskie.....	24
6.1.4 Adware.....	25
6.1.5 Spyware.....	25
6.1.6 Potencjalnie niebezpieczne aplikacje.....	25
6.1.7 Potencjalnie niepożądane aplikacje.....	25

1. ESET NOD32 Antivirus

W związku z rosnącą popularnością systemów operacyjnych opartych na platformie Unix autorzy szkodliwego oprogramowania przygotowują coraz więcej aplikacji skierowanych przeciw użytkownikom systemu Mac. Program ESET NOD32 Antivirus udostępnia zaawansowaną i skuteczną ochronę przed takimi zagrożeniami. Program ESET NOD32 Antivirus potrafi ponadto blokować szkodliwe programy przeznaczone dla systemu Windows, chroniąc komputery z systemem Mac wchodzące w interakcje z komputerami z systemem Windows i na odwrót. Mimo iż szkodliwe oprogramowanie przygotowane dla systemu Windows nie stanowi bezpośredniego zagrożenia dla systemu Mac, dezaktywacja oprogramowania, które zainfekowało komputer z systemem Mac, zapobiegnie jego rozprzestrzenianiu na komputery z systemem Windows przez sieć lokalną lub Internet.

1.1 Wymagania systemowe

Aby zapewnić płynne działanie programu ESET NOD32 Antivirus, komputer powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

ESET NOD32 Antivirus:

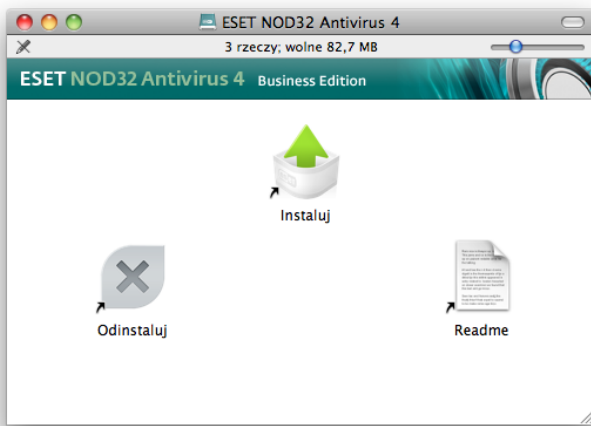
	Wymagania systemowe
Architektura procesora	32- lub 64-bitowy procesor Intel®
System operacyjny	Mac OS X 10.5 lub nowszy
Pamięć	512 MB
Wolne miejsce na dysku	100 MB

2. Instalacja

Przed rozpoczęciem procesu instalacji zamknij wszystkie otwarte programy. ESET NOD32 Antivirus zawiera komponenty, które mogą wchodzić w konflikty z innymi zainstalowanymi na komputerze programami antywirusowymi. Firma ESET zaleca usunięcie innych programów antywirusowych w celu uniknięcia potencjalnych problemów. Aby zainstalować program ESET NOD32 Antivirus, użyj płyty instalacyjnej CD lub pliku dostępnego w witrynie internetowej firmy ESET.

Aby uruchomić kreatora instalacji, wykonaj jeden z następujących kroków:

- Jeśli używasz płyty instalacyjnej CD, umieść ją w napędzie CD-ROM. Aby uruchomić instalatora, kliknij dwukrotnie ikonę instalacji programu ESET NOD32 Antivirus.
- Jeśli wykonujesz instalację za pomocą pobranego pliku, kliknij dwukrotnie ten plik, aby uruchomić instalatora.



Po uruchomieniu programu instalacyjnego kreator instalacji poprowadzi użytkownika przez podstawowe kroki konfiguracji. Po zaakceptowaniu Umowy licencyjnej użytkownika końcowego można wybrać jeden z następujących typów instalacji:

- [Instalacja typowa](#) ⁵
- [Instalacja niestandardowa](#) ⁵
- [Instalacja zdalna](#) ⁶

2.1 Instalacja typowa

Typowa instalacja obejmuje opcje konfiguracyjne odpowiednie dla większości użytkowników. Ustawienia te stanowią najlepszy kompromis między maksymalnym bezpieczeństwem a najwyższą wydajnością. Instalacja typowa jest wybierana domyślnie i zaleca się ją w przypadku, gdy użytkownik nie ma specjalnych wymagań w kwestii określonych ustawień.

Po zaznaczeniu trybu instalacji **Typowa (zalecane)** zostanie wyświetlony monit o podanie nazwy użytkownika i hasła, co pozwoli na automatyczne aktualizowanie programu. Odgrywa to istotną rolę w zapewnieniu ciągłej ochrony systemu. Wpisz dane w polach **Nazwa użytkownika** i **Hasło** (są to dane uwierzytelniające otrzymane po zakupie lub rejestracji produktu). Jeśli obecnie nie posiadasz nazwy użytkownika ani

hasła, możesz zaznaczyć opcję **Ustaw parametry aktualizacji później** i kontynuować instalację bez ich podawania.

System monitorowania zagrożeń ThreatSense.Net pomaga zapewnić natychmiastowe i ciągłe informowanie firmy ESET o nowych próbach ataków, tak aby mogła ona szybko reagować i chronić swoich klientów. System umożliwia zgłaszanie nowych zagrożeń do laboratorium firmy ESET, gdzie są one analizowane, przetwarzane i dodawane do bazy sygnatur wirusów. Domyślnie opcja **Włącz system monitorowania zagrożeń ThreatSense.Net** jest zaznaczona. Aby zmodyfikować szczegółowe ustawienia dotyczące przesyłania podejrzanych plików, kliknij przycisk **Ustawienia...** (Więcej informacji można znaleźć w sekcji [ThreatSense.Net](#) ²⁰).

Kolejnym krokiem procesu instalacji jest skonfigurowanie wykrywania potencjalnie niepożądanych aplikacji. Potencjalnie niepożądane aplikacje nie są z założenia tworzone w złych intencjach, ale mogą negatywnie wpływać na działanie systemu operacyjnego. Te aplikacje często są dołączane do innych programów i mogą być trudne do zauważenia podczas procesu instalacji. W trakcie instalacji tych aplikacji zazwyczaj wyświetlane jest powiadomienie, jednak mogą one zostać łatwo zainstalowane bez zgody użytkownika. Zaznacz opcję **Włącz wykrywanie potencjalnie niepożądanych aplikacji** (rozwiązanie zalecane), aby program ESET NOD32 Antivirus wykrywał tego typu zagrożenia. Jeśli nie chcesz włączać tej funkcji, zaznacz opcję **Wyłącz wykrywanie potencjalnie niepożądanych aplikacji**.

Kliknij przycisk **Instaluj**, aby zainstalować program ESET NOD32 Antivirus na standardowym dysku **Macintosh HD**. Jeśli chcesz wybrać inny dysk, kliknij przycisk **Zmień lokalizację instalacji...**

2.2 Instalacja niestandardowa

Instalacja niestandardowa jest przeznaczona dla doświadczonych użytkowników, którzy chcą modyfikować zaawansowane ustawienia podczas instalacji.

Po wybraniu trybu instalacji **Niestandardowa** należy wpisać swoje dane w polach **Nazwa użytkownika** i **Hasło** (są to dane uwierzytelniające otrzymane po zakupie lub rejestracji produktu). Jeśli obecnie nie posiadasz nazwy użytkownika ani hasła, możesz zaznaczyć opcję **Ustaw parametry aktualizacji później** i kontynuować instalację bez ich podawania. Nazwę użytkownika i hasło można podać w późniejszym terminie.

Jeśli używasz serwera proxy, możesz zaznaczyć opcję **Korzystam z serwera proxy** i określić jego ustawienia na tym etapie. Wprowadź adres IP lub URL serwera proxy w polu **Adres**. W polu **Port** określ port, na którym serwer proxy akceptuje połączenia (domyślnie 3128). W przypadku, gdy serwer proxy wymaga uwierzytelniania, należy w polach **Nazwa użytkownika** i **Hasło** podać poprawne dane umożliwiające dostęp do serwera. Jeśli wiadomo na pewno, że serwer proxy nie jest używany, zaznacz opcję **Nie korzystam z serwera proxy**. W razie braku pewności możesz zaznaczyć opcję **Użyj takich samych ustawień, jak ustawienia systemowe (zalecane)** i używać bieżących ustawień systemu.

Jeśli program ESET NOD32 Antivirus będzie zarządzany przez

aplikację ESET Remote Administrator (ERA), można wprowadzić parametry modułu ERA Server (nazwa serwera, port i hasło) w celu automatycznego utworzenia połączenia między programami ESET NOD32 Antivirus i ERA Server po zakończeniu instalacji.

W następnym kroku można w oknie **Zdefiniuj uprawnionych użytkowników** wskazać użytkowników mających pozwolenie na edytowanie konfiguracji programu. Na liście użytkowników z lewej strony zaznacz żądane osoby, a następnie kliknij przycisk **Dodaj**. Osoby te zostaną dodane do listy **Uprawnieni użytkownicy**. Aby byli widoczni wszyscy użytkownicy zdefiniowani w systemie, zaznacz opcję **Pokaż wszystkich użytkowników**.

System monitorowania zagrożeń ThreatSense.Net pomaga zapewnić natychmiastowe i ciągłe informowanie firmy ESET o nowych próbach ataków, tak aby mogła ona szybko reagować i chronić swoich klientów. System umożliwia zgłaszanie nowych zagrożeń do laboratorium firmy ESET, gdzie są one analizowane, przetwarzane i dodawane do bazy sygnatur wirusów. Domyślnie opcja **Włącz system monitorowania zagrożeń ThreatSense.Net** jest zaznaczona. Aby zmodyfikować szczegółowe ustawienia dotyczące przesyłania podejrzanych plików, kliknij przycisk **Ustawienia...** Więcej informacji można znaleźć w sekcji [ThreatSense.Net](#)^[20].

Kolejnym krokiem procesu instalacji jest skonfigurowanie wykrywania potencjalnie niepożądanych aplikacji. Potencjalnie niepożądane aplikacje nie są z założenia tworzone w złych intencjach, ale mogą negatywnie wpływać na działanie systemu operacyjnego. Te aplikacje często są dołączane do innych programów i mogą być trudne do zauważenia podczas procesu instalacji. W trakcie instalacji tych aplikacji zazwyczaj wyświetlane jest powiadomienie, jednak mogą one zostać łatwo zainstalowane bez zgody użytkownika. Zaznacz opcję **Włącz wykrywanie potencjalnie niepożądanych aplikacji** (rozwiązanie zalecane), aby program ESET NOD32 Antivirus wykrywał tego typu zagrożenia.

Kliknij przycisk **Instaluj**, aby zainstalować program ESET NOD32 Antivirus na standardowym dysku **Macintosh HD**. Jeśli chcesz wybrać inny dysk, kliknij przycisk **Zmień lokalizację instalacji...**

2.3 Instalacja zdalna

Funkcja instalacji zdalnej pozwala utworzyć pakiet instalacyjny, który można zainstalować na komputerach docelowych, korzystając z oprogramowania do obsługi pulpitu zdalnego. Programem ESET NOD32 Antivirus można wówczas zarządzać zdalnie za pomocą narzędzia ESET Remote Administrator.

Instalacja zdalna przebiega w dwóch etapach:

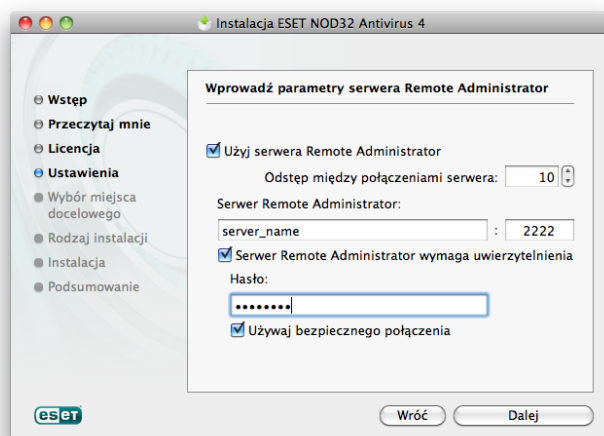
1. [Utworzenie pakietu instalacji zdalnej przez instalatora programu ESET](#)^[6]
2. [Zdalna instalacja za pomocą oprogramowania do obsługi pulpitu zdalnego](#)^[7]

2.3.1 Tworzenie pakietu instalacji zdalnej

Po wybraniu trybu instalacji **Zdalnej** zostanie wyświetlony monit o wprowadzenie nazwy użytkownika i hasła, co pozwoli na automatyczne aktualizowanie programu ESET NOD32 Antivirus. Wpisz dane w polach **Nazwa użytkownika** i **Hasło** (są to dane uwierzytelniające otrzymane po zakupie lub rejestracji produktu). Jeśli obecnie nie posiadasz nazwy użytkownika ani hasła, możesz zaznaczyć opcję **Ustaw parametry aktualizacji później** i kontynuować instalację bez ich podawania. Dane te można również wpisać bezpośrednio w programie w późniejszym terminie.

W następnym kroku należy skonfigurować połączenie internetowe. Jeśli używasz serwera proxy, możesz zaznaczyć opcję **Korzystam z serwera proxy** i określić jego ustawienia na tym etapie. Jeśli wiadomo na pewno, że serwer proxy nie jest używany, zaznacz opcję **Nie korzystam z serwera proxy**. W razie braku pewności możesz zaznaczyć opcję **Użyj takich samych ustawień, jak ustawienia systemowe** i używać bieżących ustawień systemu.

Wprowadź parametry programu ERA Server (nazwa serwera, port i hasło), aby po zakończeniu instalacji program ESET NOD32 Antivirus automatycznie łączył się z programem ERA Server.



W następnym kroku można w oknie **Zdefiniuj uprawnionych użytkowników** wskazać użytkowników mających pozwolenie na edytowanie konfiguracji programu. Na liście użytkowników z lewej strony zaznacz żądane osoby, a następnie kliknij przycisk **Dodaj**. Osoby te zostaną dodane do listy **Uprawnieni użytkownicy**. Aby byli widoczni wszyscy użytkownicy zdefiniowani w systemie, zaznacz opcję **Pokaż wszystkich użytkowników**.

System monitorowania zagrożeń ThreatSense.Net pomaga zapewnić natychmiastowe i ciągłe informowanie firmy ESET o nowych próbach ataków, tak aby mogła ona szybko reagować i chronić swoich klientów. System umożliwia zgłaszanie nowych zagrożeń do laboratorium firmy ESET, gdzie są one analizowane, przetwarzane i dodawane do bazy sygnatur wirusów. Domyślnie opcja **Włącz system monitorowania zagrożeń ThreatSense.Net** jest zaznaczona. Aby zmodyfikować szczegółowe ustawienia dotyczące przesyłania podejrzanych plików, kliknij przycisk **Ustawienia...** Więcej informacji można

znaleźć w sekcji [ThreatSense.Net](#) ^[20].

Kolejnym krokiem procesu instalacji jest skonfigurowanie wykrywania potencjalnie niepożądanych aplikacji. Potencjalnie niepożądane aplikacje nie są z założenia tworzone w złych intencjach, ale mogą negatywnie wpływać na działanie systemu operacyjnego. Te aplikacje często są dołączane do innych programów i mogą być trudne do zauważenia podczas procesu instalacji. W trakcie instalacji tych aplikacji zazwyczaj wyświetlane jest powiadomienie, jednak mogą one zostać łatwo zainstalowane bez zgody użytkownika. Zaznacz opcję **Włącz wykrywanie potencjalnie niepożądanych aplikacji** (rozwiązanie zalecane), aby program ESET NOD32 Antivirus wykrywał tego typu zagrożenia.

W ostatnim kroku kreatora instalacji wybierz folder docelowy. Instalator programu ESET utworzy pakiet instalacyjny (*EAV4_Remote_Install.pkg*) oraz dezinstalacyjny skrypt powłoki (*EAV4_Remote_UnInstall.sh*).

2.3.2 Instalacja zdalna na docelowych komputerach

Program ESET NOD32 Antivirus można instalować na docelowych komputerach za pomocą aplikacji Apple Remote Desktop lub dowolnego innego narzędzia, które obsługuje instalowanie standardowych pakietów komputerów Mac (*.pkg*), kopiowanie plików oraz wykonywanie skryptów powłoki na zdalnych komputerach.

Aby zainstalować program ESET NOD32 Antivirus przy użyciu narzędzia Apple Remote Desktop, wykonaj polecenie **Install packages...**, odszukaj plik *EAV4_Remote_Install.pkg* i kliknij przycisk **Install**.

Szczegółowe instrukcje administrowania komputerami klienckimi za pomocą narzędzia ESET Remote Administrator można znaleźć w podręczniku użytkownika programu ESET Remote Administrator.

2.3.3 Zdalne odinstalowanie

Aby odinstalować program ESET NOD32 Antivirus z komputerów klienckich:

1. w narzędziu Apple Remote Desktop wykonaj polecenie **Copy Items...**, odszukaj dezinstalacyjny skrypt powłoki (*EAV4_Remote_UnInstall.sh* — utworzony razem z pakietem instalacyjnym), a następnie skopiuj ten skrypt na docelowe komputery;
2. w narzędziu Apple Remote Desktop wykonaj polecenie **Send Unix Command...** Po pomyślnym zakończeniu dezinstalacji zostanie wyświetlony dziennik konsoli.

2.3.4 Zdalne uaktualnienie

Zdalnego uaktualnienia programu ESET NOD32 Antivirus dokonuje się za pomocą polecenia **Install packages...** dostępnego w narzędziu Apple Remote Desktop.

UWAGA: w trakcie uaktualniania do komputerów docelowych nie są stosowane ustawienia zapisane w pakiecie instalacji zdalnej programu ESET. Po uaktualnieniu należy użyć narzędzia ESET Remote Administrator w celu zdalnego skonfigurowania programu ESET NOD32 Antivirus.

2.4 Wprowadzanie nazwy użytkownika i hasła

W celu uzyskania optymalnej funkcjonalności należy ustawić w programie automatyczne pobieranie aktualizacji bazy sygnatur wirusów. Jest to możliwe tylko w przypadku prawidłowego wprowadzenia **nazwy użytkownika i hasła** w [ustawieniach aktualizacji](#) ^[16].

2.5 Skanowanie komputera na żądanie

Po zainstalowaniu programu ESET NOD32 Antivirus należy wykonać skanowanie komputera w poszukiwaniu szkodliwego kodu. W głównym menu programu należy kliknąć opcję **Skanowanie komputera**, a następnie opcję **Skanowanie inteligentne**. Więcej informacji o skanowaniach komputera na żądanie można znaleźć w sekcji [Skanowanie komputera na żądanie](#) ^[17].

3. Przewodnik dla początkujących

Niniejszy rozdział zawiera ogólny opis programu ESET NOD32 Antivirus i jego podstawowych ustawień.

3.1 Tryby interfejsu użytkownika — wprowadzenie

Główne okno programu ESET NOD32 Antivirus jest podzielone na dwie główne części. W okienku z prawej strony są wyświetlane informacje dotyczące opcji zaznaczonej w menu głównym z lewej strony.

Poniżej opisano opcje dostępne w menu głównym:

- **Stan ochrony** — przedstawia informacje o stanie ochrony programu ESET NOD32 Antivirus. W przypadku aktywowania opcji **Tryb zaawansowany** jest wyświetlane podmenu **Statystyki**.
- **Skanowanie komputera** — pozwala skonfigurować i uruchomić funkcję **Skanowanie komputera na żądanie**.
- **Aktualizacja** — powoduje wyświetlenie informacji o aktualizacjach bazy sygnatur wirusów.
- **Ustawienia** — umożliwia dostosowanie poziomu zabezpieczeń komputera. W przypadku aktywowania opcji **Tryb zaawansowany** jest wyświetlane podmenu **Antywirus i antyspyware**.
- **Narzędzia** — zapewnia dostęp do modułów **Pliki dziennika**, **Kwarantanna** i **Harmonogram**. Opcja jest wyświetlana wyłącznie po aktywowaniu opcji **Tryb zaawansowany**.
- **Pomoc** — udostępnia informacje o programie oraz umożliwia dostęp do plików pomocy, internetowej bazy wiedzy i witryny internetowej firmy ESET.

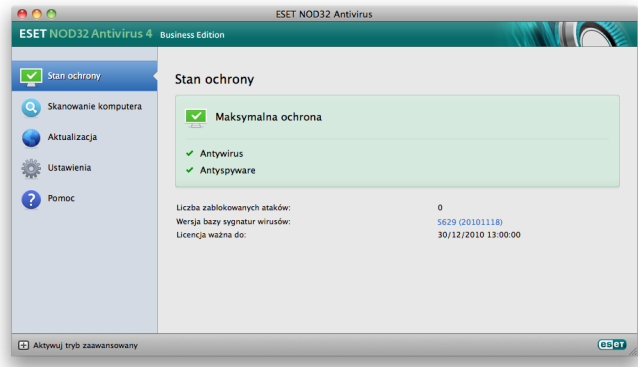
Interfejs użytkownika programu ESET NOD32 Antivirus pozwala na przełączanie między trybem standardowym i zaawansowanym. Tryb standardowy zapewnia dostęp do funkcji wymaganych do wykonywania typowych operacji. Żadne zaawansowane opcje nie są wyświetlane. W celu przełączenia z jednego trybu do drugiego należy kliknąć ikonę plusa (+) widoczną obok nagłówka **Aktywuj tryb zaawansowany/Aktywuj tryb standardowy**, w lewym dolnym rogu głównego okna programu.

Tryb standardowy zapewnia dostęp do funkcji wymaganych do wykonywania typowych operacji. Żadne zaawansowane opcje nie są wyświetlane.

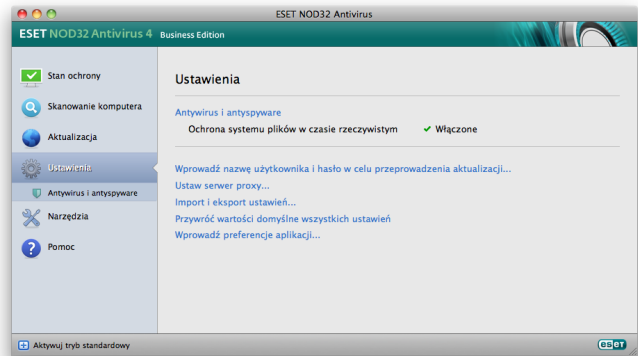
Przełączenie do trybu zaawansowanego powoduje dodanie do menu głównego opcji **Narzędzia**. Opcja **Narzędzia** umożliwia dostęp do podmenu modułów **Pliki dziennika**, **Kwarantanna** i **Harmonogram**.

UWAGA: Wszystkie pozostałe instrukcje w niniejszym podręczniku dotyczą **trybu zaawansowanego**.

Tryb standardowy:

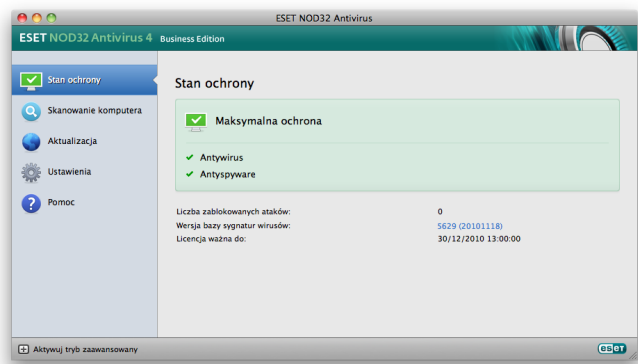


Tryb zaawansowany:



3.1.1 Sprawdzanie działania systemu

Aby wyświetlić okno **Stan ochrony**, należy kliknąć górną opcję w menu głównym. W podstawowym okienku zostaną wyświetlone podsumowujące informacje o działaniu programu ESET NOD32 Antivirus. Pojawi się także podmenu z opcją **Statystyki**. Po kliknięciu tej opcji można obejrzeć dokładniejsze informacje i statystyki dotyczące operacji skanowania komputera wykonanych w danym systemie. Okno Statystyki jest dostępne wyłącznie w trybie zaawansowanym.



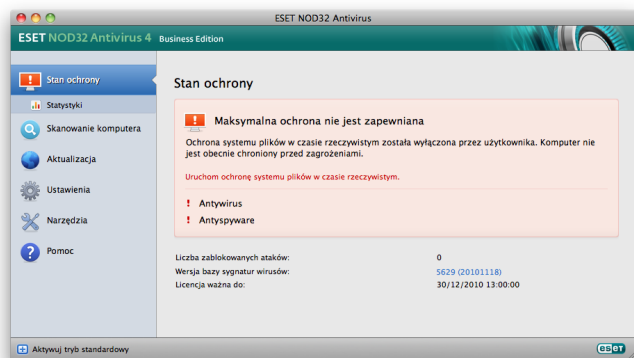
3.1.2 Postępowanie w przypadku, gdy program nie działa poprawnie

Jeśli włączone moduły działają poprawnie, są oznaczone zieloną ikoną znacznika wyboru. W przeciwnym razie wyświetlana jest czerwona ikona wykrzyknika lub żółta ikona powiadomienia, a w górnej części okna pojawiają się dodatkowe informacje dotyczące modułu. Wyświetlany jest również proponowany sposób przywrócenia działania modułu. Aby zmienić stan poszczególnych modułów, w menu głównym należy kliknąć opcję **Ustawienia**, a następnie kliknąć wybrany

moduł.

Jeśli nie można rozwiązać problemu za pomocą sugerowanego rozwiązania, należy kliknąć opcję **Pomoc** i przejść do plików pomocy lub przeszukać bazę wiedzy.

Aby uzyskać dodatkową pomoc, można skontaktować się z działem obsługi klienta firmy ESET za pośrednictwem [witryny internetowej firmy](#). Dział obsługi klienta szybko odpowie na otrzymane zgłoszenie i pomoże znaleźć rozwiązanie.



4. Praca z programem ESET NOD32 Antivirus

4.1 Antywirus i antyspyware

Ochrona antywirusowa zabezpiecza system przed szkodliwymi atakami, modyfikując potencjalnie niebezpieczne pliki. W przypadku wykrycia zagrożenia zawierającego szkodliwy kod moduł antywirusowy może je wyeliminować przez zablokowanie, a następnie usunąć lub przenieść do kwarantanny.

4.1.1 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.

4.1.1.1 Ustawienia ochrony w czasie rzeczywistym

Funkcja ochrony systemu plików w czasie rzeczywistym sprawdza wszystkie typy nośników. Skanowanie jest wywoływane wystąpieniem różnych zdarzeń. Wykorzystując metody wykrywania udostępniane przez technologię ThreatSense (opisane w sekcji [Ustawienia parametrów technologii ThreatSense](#)^[13]), funkcja ochrony systemu plików w czasie rzeczywistym może działać inaczej dla plików nowo tworzonych, a inaczej dla już istniejących. W przypadku nowo tworzonych plików można stosować głębszy poziom sprawdzania.

Ochrona 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, klikając ikonę ESET NOD32 Antivirus dostępną na pasku menu (u góry ekranu), a następnie zaznaczając opcję **Wyłącz ochronę systemu plików w czasie rzeczywistym**. Ochrona w czasie rzeczywistym może również zostać wyłączona w oknie głównym programu (**Ustawienia > Antywirus i antyspyware > Wyłącz**).

Aby zmodyfikować zaawansowane ustawienia ochrony w czasie rzeczywistym, należy przejść do opcji **Ustawienia > Wprowadź preferencje aplikacji... > Ochrona > Ochrona w czasie rzeczywistym** i kliknąć przycisk **Ustawienia...** umieszczony obok pozycji **Opcje zaawansowane** (opisano to w sekcji [Zaawansowane opcje skanowania](#)^[10]).

4.1.1.1.1 Skanowanie po wystąpieniu zdarzenia

Wystąpienie następujących zdarzeń domyślnie powoduje skanowanie każdego pliku: **Otwieranie pliku**, **Tworzenie pliku** oraz **Wykonywanie pliku**. Zaleca się zachowanie ustawień domyślnych, ponieważ zapewniają one maksymalny poziom ochrony komputera w czasie rzeczywistym.

4.1.1.1.2 Zaawansowane opcje skanowania

W tym oknie można wskazać typy obiektów, które mają być skanowane przez aparat ThreatSense, włączyć/wyłączyć funkcję **Zaawansowana heurystyka**, a także zmodyfikować ustawienia archiwizacji i pamięci podręcznej plików.

Nie zaleca się zmiany domyślnych wartości w części **Domyślne ustawienia archiwów**, chyba że wymaga tego konkretny problem, ponieważ większa liczba poziomów zagnieżdżenia archiwów może spowodować obniżenie wydajności systemu.

Funkcję skanowania z wykorzystaniem zaawansowanej heurystyki dostępną w ramach technologii ThreatSense można włączać osobno dla plików wykonywalnych, nowo tworzonych i zmodyfikowanych. Wystarczy zaznaczyć pole wyboru **Zaawansowana heurystyka** w odpowiednich sekcjach parametrów technologii ThreatSense.

Aby zminimalizować obciążenie systemu podczas korzystania z ochrony w czasie rzeczywistym, można ustawić rozmiar pamięci podręcznej optymalizacji. Funkcjonalność ta jest dostępna w przypadku korzystania z opcji **Włącz pamięć podręczną leczenia plików**. Po jej wyłączeniu wszystkie pliki są skanowane podczas każdego dostępu. Po umieszczeniu w pamięci podręcznej zeskanowane pliki nie będą ponownie skanowane (chyba że ulegną modyfikacji), aż do osiągnięcia zdefiniowanego rozmiaru pamięci podręcznej. Pliki są natychmiast skanowane ponownie po każdej aktualizacji bazy sygnatur wirusów.

Aby włączyć/wyłączyć tę funkcję, należy kliknąć opcję **Włącz pamięć podręczną leczenia plików**. W celu określenia liczby plików, jakie można umieścić w pamięci podręcznej, wystarczy wpisać żadaną wartość w polu **Rozmiar pamięci podręcznej**.

Dodatkowe parametry skanowania można skonfigurować w oknie **Ustawienia technologii ThreatSense**. W części **Obiekty** można wskazać obiekty, które mają być skanowane. W części **Opcje** można wybrać opcje skanowania, a w części **Poziom leczenia** — zakres leczenia plików. Można także określić typy (część **Rozszerzenia**) i wielkość (część **Limity**) plików skanowanych przez funkcję ochrony systemu plików w czasie rzeczywistym. Aby przejść do okna ustawień technologii ThreatSense, należy kliknąć przycisk **Ustawienia...** widoczny obok nagłówka **Technologia ThreatSense** w oknie Ustawienia zaawansowane. Więcej informacji o parametrach technologii ThreatSense można znaleźć w sekcji [Ustawienia parametrów technologii ThreatSense](#)^[13].

4.1.1.1.3 Wykluczenia ze skanowania

W tej części można wykluczyć ze skanowania wybrane pliki i foldery.

- **Ścieżka** — ścieżka do wykluczonych plików i folderów.
- **Zagrożenie** — gdy obok wykluczonego pliku widać nazwę zagrożenia, oznacza to, że plik będzie pomijany tylko przy wyszukiwaniu tego zagrożenia, a nie całkowicie. W związku z tym, jeśli później plik zostanie zainfekowany innym szkodliwym oprogramowaniem, moduł antywirusowy go wykryje.

- **Dodaj...** — pozwala dodać obiekty, które mają być pomijane podczas wykrywania. Należy wprowadzić ścieżkę do obiektu (można używać symboli wieloznacznych * i ?) albo zaznaczyć folder lub plik w strukturze drzewa.
- **Edytuj...** — pozwala zmodyfikować zaznaczone elementy.
- **Usuń** — służy do usuwania zaznaczonych elementów.
- **Domyślne** — powoduje anulowanie wszystkich wykluczeń.

4.1.1.2 Modyfikowanie ustawień ochrony w czasie rzeczywistym

Ochrona w czasie rzeczywistym jest najbardziej istotnym elementem zapewniającym bezpieczeństwo systemu. Dlatego modyfikowanie parametrów tej funkcji należy przeprowadzać z dużą ostrożnością. Zmianianie ustawień ochrony jest zalecane tylko w określonych przypadkach. Przykładem może być sytuacja, w której występuje konflikt z określoną aplikacją lub skanerem działającym w czasie rzeczywistym należącym do innego programu antywirusowego.

Po zainstalowaniu programu ESET NOD32 Antivirus wszystkie ustawienia są optymalizowane w celu zapewnienia użytkownikom maksymalnego poziomu bezpieczeństwa systemu. Aby przywrócić ustawienia domyślne, należy kliknąć przycisk **Domyślne** znajdujący się w prawej dolnej części okna **Ochrona systemu plików w czasie rzeczywistym** (otwieranego po wybraniu kolejno opcji **Ustawienia** > **Wprowadź preferencje aplikacji...** > **Ochrona** > **Ochrona w czasie rzeczywistym**).

4.1.1.3 Sprawdzanie skuteczności ochrony w czasie rzeczywistym

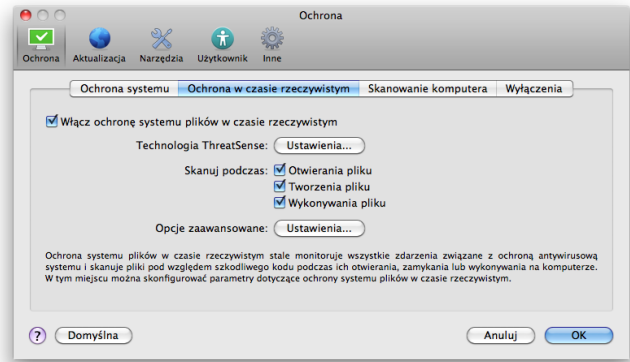
Aby sprawdzić, czy funkcja ochrony w czasie rzeczywistym działa i wykrywa wirusy, należy użyć pliku testowego eicar.com. Jest to specjalny nieszkodliwy plik wykrywany przez wszystkie programy antywirusowe. Został on utworzony przez instytut EICAR (ang. European Institute for Computer Antivirus Research) w celu testowania działania programów antywirusowych.

4.1.1.4 Co należy 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 uaktywnić ochronę w czasie rzeczywistym, w głównym oknie programu należy wybrać kolejno opcje **Ustawienia** > **Antywirus i antyspyware**, a następnie kliknąć łącze **Włącz ochronę systemu plików w czasie rzeczywistym** (z prawej strony). Ochronę systemu plików w czasie rzeczywistym można też włączyć w oknie **Ustawienia zaawansowane** (otwieranym po wybraniu kolejno opcji **Ochrona** > **Ochrona w czasie rzeczywistym**), zaznaczając pole wyboru **Włącz ochronę systemu plików w czasie rzeczywistym**.



Ochrona w czasie rzeczywistym nie wykrywa ani nie leczy infekcji

Należy upewnić się, 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.

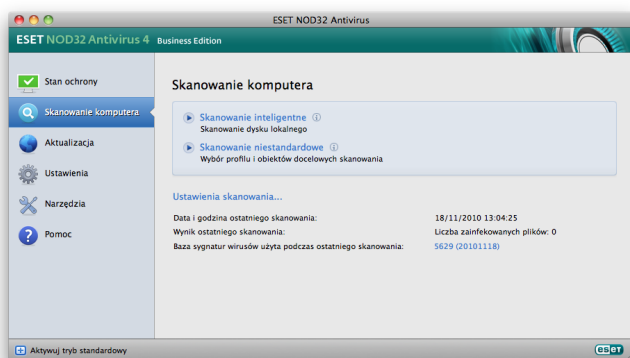
Ochrona w czasie rzeczywistym nie jest uruchamiana

Jeśli funkcja ochrony w czasie rzeczywistym nie jest inicjowana podczas uruchamiania systemu, być może jest to spowodowane konfliktami z innymi programami. W takim przypadku należy skonsultować się z personelem działu pomocy technicznej firmy ESET.

4.1.2 Skanowanie komputera na żądanie

Jeśli istnieje podejrzenie, że komputer jest zainfekowany (działa w sposób nieprawidłowy), należy wybrać kolejno opcje **Skanowanie komputera** > **Skanowanie inteligentne** w celu sprawdzenia komputera w poszukiwaniu infekcji. Aby zapewnić maksymalny poziom bezpieczeństwa, skanowanie komputera powinno być uruchamiane regularnie w ramach rutynowych działań związanych z bezpieczeństwem, a nie tylko w przypadku podejrzenia wystąpienia infekcji. Regularne skanowanie umożliwi wykrywanie zagrożeń, które podczas zapisywania zainfekowanych plików na dysku nie zostały wykryte przez skaner działający w czasie rzeczywistym. Jest to możliwe, jeśli w momencie wystąpienia infekcji skaner działający w czasie rzeczywistym był wyłączony lub baza sygnatur wirusów była nieaktualna.

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



4.1.2.1 Typ skanowania

Dostępne są dwa typy skanowania komputera na żądanie. 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.

4.1.2.1.1 Skanowanie inteligentne

Skanowanie inteligentne umożliwia szybkie uruchomienie skanowania komputera i wyleczenie zainfekowanych plików bez konieczności podejmowania dodatkowych działań przez użytkownika. Jego główną zaletą jest łatwa obsługa i brak szczegółowej konfiguracji skanowania. W ramach skanowania inteligentnego sprawdzane są wszystkie pliki we wszystkich folderach, a wykryte infekcje są automatycznie leczone lub usuwane. Jako poziom leczenia automatycznie ustawiana jest wartość domyślna. Szczegółowe informacje na temat typów leczenia można znaleźć w sekcji [Leczenie](#) ¹⁴.

4.1.2.1.2 Skanowanie niestandardowe

Skanowanie niestandardowe stanowi optymalne rozwiązanie, jeśli użytkownik chce 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 wykonywane wielokrotnie z zastosowaniem tych samych parametrów.

Aby wybrać skanowane obiekty, należy użyć opcji **Skanowanie komputera > Skanowanie niestandardowe**, a następnie zaznaczyć określone **Skanowane obiekty** w strukturze drzewa. Skanowany obiekt można również określić dokładniej, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Jeśli użytkownik chce tylko przeskanować system bez wykonywania dodatkowych działań związanych z leczeniem, należy zaznaczyć opcję **Skanuj bez leczenia**. Ponadto można wybrać jeden z trzech poziomów leczenia, klikając opcję **Ustawienia... > Leczenie**.

Skanowanie komputera w trybie skanowania niestandardowego jest przeznaczone dla zaawansowanych użytkowników, którzy mają już doświadczenie w posługiwaniu się programami antywirusowymi.

4.1.2.2 Skanowane obiekty

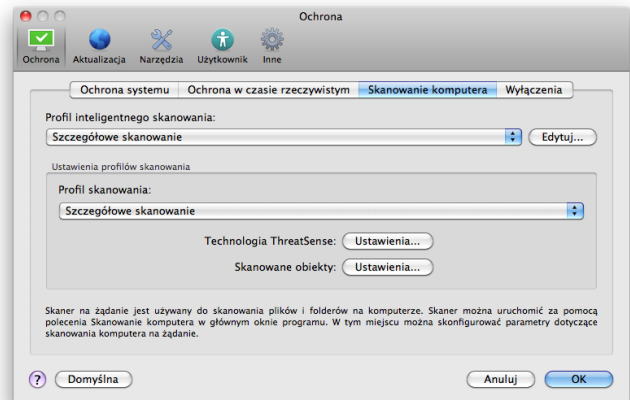
Struktura drzewa skanowanych obiektów umożliwia wybór plików i folderów, które mają być skanowane w poszukiwaniu wirusów. Foldery mogą również zostać zaznaczone zgodnie z ustawieniami profilu.

Skanowany obiekt można również dokładniej określić, wprowadzając ścieżkę do folderu lub plików, które mają zostać objęte skanowaniem. Skanowane obiekty można wybrać w strukturze drzewa zawierającej wszystkie foldery dostępne na komputerze.

4.1.2.3 Profile skanowania

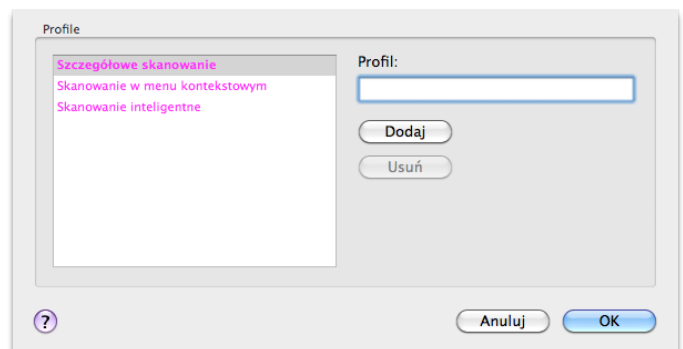
Preferowane ustawienia skanowania mogą zostać zapisane i użyte w przyszłości. Zaleca się utworzenie osobnego profilu (z ustawionymi różnymi obiektami i metodami skanowania oraz innymi parametrami) dla każdego regularnie używanego skanowania.

Aby utworzyć nowy profil, należy przejść do opcji **Ustawienia > Wprowadź preferencje aplikacji... > Ochrona > Skanowanie komputera** i kliknąć przycisk **Edytuj...** obok listy bieżących profili.



Więcej informacji o tworzeniu profilu skanowania dostosowanego do własnych potrzeb znajduje się w sekcji [Ustawienia parametrów technologii ThreatSense](#) ¹³, w której opisano każdy parametr ustawień skanowania.

Przykład: założmy, że użytkownik chce utworzyć własny profil skanowania, a żądana konfiguracja częściowo pokrywa się z konfiguracją w profilu Skanowanie inteligentne. Użytkownik nie chce jednak skanować plików spakowanych lub potencjalnie niebezpiecznych aplikacji oraz chce zastosować poziom leczenia Leczenie dokładne. W oknie **Lista profili skanera na żądanie** należy wprowadzić nazwę profilu, kliknąć przycisk **Dodaj** i potwierdzić, klikając przycisk **OK**. Następnie należy dostosować parametry do własnych potrzeb, konfigurując opcje **Technologia ThreatSense** oraz **Skanowane obiekty**.



4.1.3 Ustawienia parametrów technologii ThreatSense

ThreatSense to technologia obejmująca złożone metody 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 (analizy kodu, emulacji kodu, sygnatur rodzajowych, sygnatur wirusów), które współdziałają w celu znacznego zwiększenia bezpieczeństwa systemu. Aparat skanowania może kontrolować kilka strumieni danych jednocześnie, maksymalizując skuteczność i wskaźnik wykrywalności. Ponadto technologia ThreatSense pomyślnie eliminuje programy typu rootkit.

Opcje ustawień technologii ThreatSense pozwalają określić kilka parametrów skanowania:

- typy i rozszerzenia plików, które mają być skanowane;
- kombinacje różnych metod wykrywania;
- poziomy leczenia itp.

Aby otworzyć okno konfiguracji, należy wybrać kolejno opcje **Ustawienia > Antywirus i antyspyware > Zaawansowane ustawienia ochrony antywirusowej i antyspyware**, a następnie kliknąć przycisk **Ustawienia...** umieszczony na kartach funkcji **Ochrona systemu**, **Ochrona w czasie rzeczywistym** i **Skanowanie komputera** korzystających z technologii ThreatSense (zobacz poniżej). Poszczególne scenariusze zabezpieczeń mogą wymagać różnych konfiguracji. Technologię ThreatSense można konfigurować indywidualnie dla następujących modułów ochrony:

- **Ochrona systemu** > Automatyczne sprawdzanie plików wykonywanych podczas uruchamiania
- **Ochrona w czasie rzeczywistym** > Ochrona systemu plików w czasie rzeczywistym
- **Skanowanie komputera** > Skanowanie komputera na żądanie

Parametry technologii ThreatSense są w wysokim stopniu zoptymalizowane dla poszczególnych modułów i ich modyfikacja może znacząco wpłynąć na działanie systemu. Na przykład ustawienie opcji skanowania plików spakowanych za każdym razem lub włączenie zaawansowanej heurystyki w module ochrony systemu plików w czasie rzeczywistym może powodować spowolnienie działania systemu. Dlatego zaleca się pozostawienie niezmienionych parametrów domyślnych technologii ThreatSense dla wszystkich modułów z wyjątkiem modułu Skanowanie komputera.

4.1.3.1 Obiekty

Część **Obiekty** pozwala określić, które pliki komputera będą skanowane w poszukiwaniu infekcji.

- **Pliki** — skanowane są najczęściej używane typy plików (programy, obrazy, pliki audio, pliki wideo, pliki baz danych itd.).
- **Łąca symboliczne** — (tylko skaner na żądanie) skanowane są specjalne typy plików zawierających ciąg tekstowy interpretowany i otwierany przez system operacyjny jako ścieżka do innego pliku lub katalogu.
- **Pliki pocztowe** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są specjalne pliki zawierające wiadomości e-mail.

- **Skrzynki pocztowe** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są skrzynki pocztowe użytkowników istniejących w systemie. Niewłaściwe stosowanie tej opcji może prowadzić do konfliktu z używanym programem pocztowym. Więcej informacji o zaletach i wadach tej opcji można znaleźć w następującym [artykule bazy wiedzy](#).
- **Archiwa** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki skompresowane w archiwach (.rar, .zip, .arj, .tar itd.).
- **Archiwa samorozpakowujące** — (opcja niedostępna w przypadku ochrony w czasie rzeczywistym) skanowane są pliki znajdujące się w archiwach samorozpakowujących.
- **Pliki spakowane** — oprócz standardowych statycznych spakowanych plików skanowane są pliki, które (inaczej niż w przypadku standardowych typów archiwów) są rozpakowywane w pamięci (UPX, yoda, ASPack, FGS itp.).

4.1.3.2 Opcje

W części **Opcje** można wybrać metody, które mają być stosowane podczas skanowania systemu w poszukiwaniu infekcji. Dostępne są następujące opcje:

- **Baza sygnatur wirusów** — sygnatury umożliwiają dokładne i niezawodne wykrywanie i identyfikowanie infekcji według nazw przy użyciu bazy sygnatur wirusów.
- **Heurystyka** — heurystyka wykorzystuje algorytm analizujący (szkodliwe) działania podejmowane przez programy. Główną zaletą heurystyki jest możliwość wykrywania nowego szkodliwego oprogramowania, które wcześniej nie istniało lub nie zostało umieszczone na liście znanych wirusów (w bazie sygnatur wirusów).
- **Zaawansowana heurystyka** — zaawansowana heurystyka jest oparta na unikatowym algorytmie heurystycznym opracowanym przez firmę ESET. Został on zoptymalizowany pod kątem wykrywania robaków i koni trojańskich napisanych w językach programowania wysokiego poziomu. Dzięki temu algorytmowi znacznie wzrasta zdolność programu do wykrywania infekcji.
- **Adware/Spyware/Riskware** — do tej kategorii zaliczane jest oprogramowanie gromadzące różne poufne informacje na temat użytkowników bez ich świadomej zgody. Obejmuje ona również oprogramowanie wyświetlające materiały reklamowe.
- **Potencjalnie niepożądane aplikacje** — nie muszą one być tworzone w złych intencjach, ale mogą negatywnie wpływać na wydajność komputera. Zainstalowanie takiej aplikacji zazwyczaj wymaga zgody użytkownika. Po zainstalowaniu programu tego typu zachowanie systemu jest inne niż przed jego instalacją. Najbardziej widoczne zmiany to wyświetlanie wyskakujących okienek, aktywowanie i uruchamianie ukrytych procesów, zwiększone użycie zasobów systemowych, zmiany w wynikach wyszukiwania oraz komunikowanie się aplikacji ze zdalnymi serwerami.
- **Potencjalnie niebezpieczne aplikacje** — do aplikacji tych zaliczane są niektóre legalne programy komercyjne, które mogą zostać wykorzystane przez intruzów do prowadzenia niebezpiecznych działań, jeśli zostały zainstalowane bez wiedzy użytkownika. Są to między innymi narzędzia do dostępu zdalnego, dlatego ta opcja jest domyślnie wyłączona.

4.1.3.3 Leczenie

Ustawienia leczenia określają sposób czyszczenia zainfekowanych plików przez skaner. Istnieją 3 poziomy leczenia:

- **Brak leczenia** — zainfekowane pliki nie są automatycznie leczone. Program wyświetla okno z ostrzeżeniem, a użytkownik sam wybiera żądane działanie.
- **Leczenie standardowe** — program próbuje automatycznie wyleczyć lub usunąć zainfekowany plik. Jeśli automatyczny wybór właściwego działania nie jest możliwy, program umożliwia użytkownikowi wybór dostępnych działań. Dostępne działania są wyświetlane również wtedy, gdy wykonanie wstępnie zdefiniowanego działania nie jest możliwe.
- **Leczenie dokładne** — program leczy lub usuwa wszystkie zainfekowane pliki (w tym archiwa). Jedyny wyjątek stanowią pliki systemowe. Jeśli ich wyleczenie nie jest możliwe, użytkownik ma możliwość wyboru działania w oknie z ostrzeżeniem.

Ostrzeżenie: W domyślnym trybie Leczenie standardowe cały plik archiwum jest usuwany tylko wtedy, gdy wszystkie pliki w archiwum są zainfekowane. Nie jest usuwany, jeśli zawiera również niezainfekowane pliki. Jeśli zainfekowany plik archiwum zostanie wykryty w trybie Leczenie dokładne, jest usuwane całe archiwum, nawet jeśli zawiera również niezainfekowane pliki.

4.1.3.4 Rozszerzenia

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

Domyślnie skanowane są wszystkie pliki niezależnie od rozszerzenia. Do listy plików wykluczonych ze skanowania można dodać dowolne rozszerzenie. Przy użyciu przycisków **Dodaj** i **Usuń** można włączyć lub wyłączyć skanowanie określonych rozszerzeń.

Wykluczenie plików ze skanowania jest czasami konieczne, jeśli skanowanie pewnych typów plików uniemożliwia prawidłowe działanie programu, który tych plików używa. Na przykład wskazane może być wykluczenie rozszerzeń `.log`, `.cfg` i `.tmp`.

4.1.3.5 Limity

W części **Limity** można określić maksymalny rozmiar obiektów i poziomy zagnieżdżenia archiwów, które mają być skanowane:

- **Maksymalny rozmiar:** Określa maksymalny rozmiar obiektów do skanowania. Moduł antywirusowy będzie skanować tylko obiekty o rozmiarze mniejszym niż określony. Nie zaleca się zmieniania domyślnej wartości, ponieważ zazwyczaj nie ma ku temu powodu. Opcja ta powinna być zmieniana tylko przez zaawansowanych użytkowników mających określone powody do wykluczenia większych obiektów ze skanowania.

- **Maksymalny czas skanowania:** Określa maksymalny czas przyznany na skanowanie obiektu. Jeśli użytkownik określi taką wartość, moduł antywirusowy zatrzyma skanowanie danego obiektu po upływie tego czasu niezależnie od tego, czy skanowanie zostało zakończone.
- **Maksymalny poziom zagnieżdżenia:** Określa maksymalną głębokość skanowania archiwów. Nie zaleca się zmieniania wartości domyślnej (równiej 10); w normalnych warunkach nie powinno być powodów do jej modyfikacji. Jeśli skanowanie zostanie przedwcześnie zakończone z powodu liczby zagnieżdżonych archiwów, archiwum pozostanie niesprawdzone.
- **Maksymalny rozmiar pliku:** Opcja ta pozwala określić maksymalny rozmiar plików znajdujących się w archiwach (po rozpakowaniu tych plików), które mają być skanowane. Jeśli wskutek narzucenia tego limitu skanowanie zostanie przedwcześnie zakończone, archiwum pozostanie niesprawdzone.

4.1.3.6 Inne

Po włączeniu opcji Inteligentna optymalizacja są używane najbardziej optymalne ustawienia, gwarantujące połączenie najbardziej efektywnego poziomu skanowania z największą szybkością procesu. Poszczególne moduły ochrony działają w sposób inteligentny, wybiórczo stosując określone metody skanowania do konkretnych typów plików. Funkcja inteligentnej optymalizacji dostępna w produkcie nie ma ostatecznej postaci. Programiści firmy ESET stale wprowadzają zmiany, które następnie są integrowane z programem ESET NOD32 Antivirus za pomocą regularnych aktualizacji. Jeśli opcja Inteligentna optymalizacja jest wyłączona, podczas skanowania są wykorzystywane jedynie ustawienia poszczególnych modułów określone przez użytkownika w silniku skanowania przy użyciu technologii ThreatSense.

Skanuj alternatywny strumień danych (tylko skaner na żądanie)

Alternatywne strumienie danych (rozwidlenia zasobów/danych) używane w systemie plików to powiązania plików i folderów, które są niewidoczne dla standardowych technik skanowania. Wiele infekcji stara się uniknąć wykrycia, udając alternatywne strumienie danych.

4.1.4 Wykryto infekcję

Infekcje mogą przedostawać się do systemu różnymi drogami, np. za pośrednictwem: stron internetowych, folderów udostępnionych, poczty e-mail lub wymiennych urządzeń komputerowych (USB, dysków zewnętrznych, dysków CD i DVD, dyskietek itd.).

Jeśli komputer wykazuje symptomy zainfekowania szkodliwym oprogramowaniem, np. działa wolniej lub często przestaje odpowiadać, zaleca się wykonanie następujących czynności:

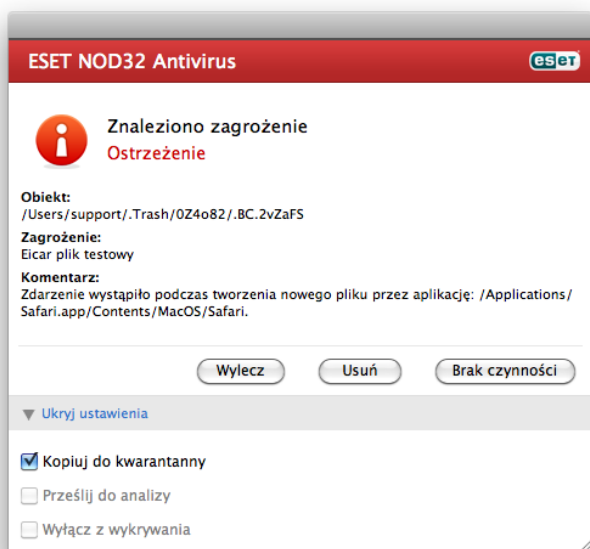
1. Uruchom program ESET NOD32 Antivirus i kliknij opcję **Skanowanie komputera**.
2. Kliknij opcję **Skanowanie inteligentne** (więcej informacji znajduje się w sekcji [Skanowanie inteligentne](#) ^[12]).

3. 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.

Ogólnym przykładem sposobu działania programu ESET NOD32 Antivirus w momencie infekcji może być sytuacja, w której infekcja zostaje wykryta przez działający w czasie rzeczywistym monitor systemu plików z ustawionym domyślnym poziomem leczenia. Następuje próba wyleczenia lub usunięcia pliku. W przypadku braku wstępnie zdefiniowanej czynności, którą ma wykonywać moduł ochrony w czasie rzeczywistym, zostanie wyświetlony monit o wybranie opcji w oknie alertu. Zazwyczaj dostępne są opcje **Wylecz**, **Usuń** i **Brak czynności**. Nie zaleca się wybierania opcji **Brak czynności**, ponieważ powoduje to pozostawienie zainfekowanych plików bez zmian. Jedynym wyjątkiem stanowi sytuacja, w której użytkownik ma pewność, że dany plik jest nieszkodliwy i został błędnie wykryty.

Leczenie i usuwanie — 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, zostanie usunięty w całości.



Usuwanie plików w archiwach — w domyślnym trybie leczenia całe archiwum jest usuwane tylko wtedy, gdy zawiera wyłącznie zainfekowane pliki i nie zawiera żadnych niezainfekowanych plików. Oznacza to, że archiwa nie są usuwane, jeśli zawierają również nieszkodliwe, niezainfekowane pliki. Podczas skanowania w trybie **Leczenie dokładne** należy jednak zachować ostrożność — każde archiwum zawierające co najmniej jeden zainfekowany plik jest usuwane bez względu na stan pozostałych zawartych w nim plików.

4.2 Aktualizowanie programu

Regularne aktualizowanie programu ESET NOD32 Antivirus jest niezbędne dla utrzymania maksymalnego poziomu bezpieczeństwa. Moduł aktualizacji zapewnia aktualność programu przez aktualizowanie bazy sygnatur wirusów.

Klikając w menu głównym opcję **Aktualizacja**, można sprawdzić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji oraz to, czy w tej chwili należy przeprowadzić aktualizację. Aby ręcznie rozpocząć proces aktualizacji, kliknij przycisk **Aktualizuj bazę danych sygnatur wirusów**.

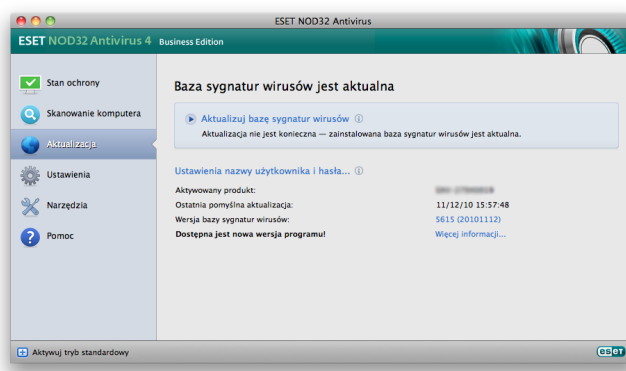
W normalnych okolicznościach, po prawidłowym pobraniu aktualizacji w oknie Aktualizacja pojawia się komunikat **Baza sygnatur wirusów jest aktualna**. Jeśli nie można zaktualizować bazy sygnatur wirusów, zalecamy sprawdzenie [ustawień aktualizacji](#)^[16]. Najczęstszą przyczyną takiego błędu są wprowadzone nieprawidłowo dane uwierzytelniania (nazwa użytkownika i hasło) lub niewłaściwie skonfigurowane [ustawienia połączenia](#)^[22].

W oknie Aktualizacja wyświetlane są też informacje na temat wersji bazy sygnatur wirusów. Ten liczbowy wskaźnik stanowi aktywne łącze do witryny internetowej firmy ESET zawierającej listę wszystkich sygnatur dodanych podczas określonej aktualizacji.

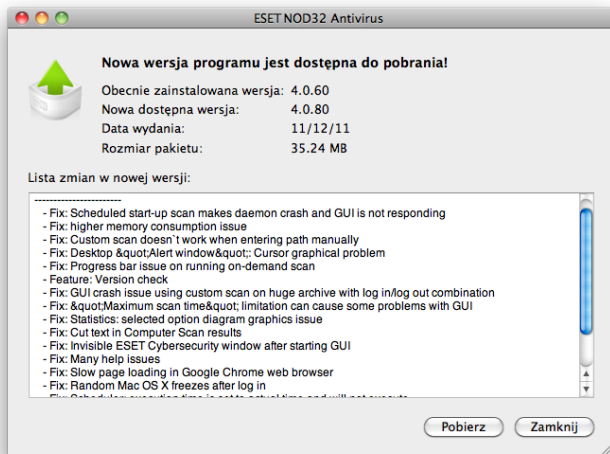
UWAGA: Nazwa użytkownika i hasło są podawane przez firmę ESET po zakupie programu ESET NOD32 Antivirus.

4.2.1 Uaktualnianie do nowej kompilacji

Używanie najnowszej kompilacji programu ESET NOD32 Antivirus gwarantuje maksymalne bezpieczeństwo. Aby sprawdzić dostępność nowej wersji, kliknij opcję **Aktualizacja** dostępną w menu głównym po lewej stronie. W przypadku dostępności nowej kompilacji u dołu okna pojawi się komunikat *Dostępna jest nowa wersja programu!* Aby wyświetlić nowe okno z informacją o numerze wersji nowej kompilacji oraz dziennikiem zmian, kliknij przycisk **Więcej informacji...**



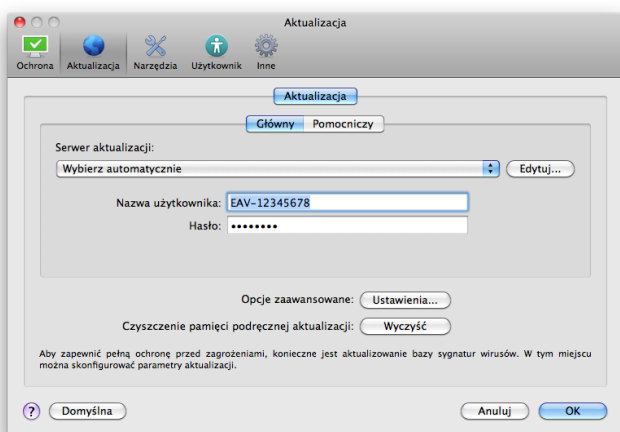
Aby pobrać najnowszą kompilację, kliknij przycisk **Pobierz**. Jeśli chcesz zamknąć okno i pobrać uaktualnienie później, kliknij przycisk **Zamknij**.



W wypadku kliknięcia przycisku **Pobierz** plik zostanie zapisany w folderze pobierania (lub w folderze domyślnym ustawionym przez przeglądarkę). Po zakończeniu pobierania uruchom plik i wykonaj instrukcje dotyczące instalacji. Twoja nazwa użytkownika i hasło zostaną automatycznie przeniesione do nowej instalacji. Zaleca się regularne sprawdzanie dostępności aktualizacji — zwłaszcza w wypadku instalowania programu ESET NOD32 Antivirus z płyty CD/DVD.

4.2.2 Ustawienia aktualizacji

W części z ustawieniami aktualizacji określone są informacje o źródle aktualizacji, takie jak serwery aktualizacji i dotyczące ich dane uwierzytelniające. Domyślnie w menu rozwijanym **Serwer aktualizacji** jest zaznaczona opcja **Wybierz automatycznie**. Zapewnia ona automatyczne pobieranie plików aktualizacji z serwera firmy ESET przy jak najmniejszym obciążeniu sieci.



Lista dostępnych serwerów aktualizacji jest wyświetlana w menu rozwijanym **Serwer aktualizacji**. Aby dodać nowy serwer aktualizacji, kliknij przycisk **Edytuj...** Następnie wpisz adres nowego serwera w polu wprowadzania danych **Serwer aktualizacji** i kliknij przycisk **Dodaj**. Uwierzytelnianie na serwerach aktualizacji bazuje na ustawieniach **Nazwa użytkownika** i **Hasło** wygenerowanych i dostarczonych użytkownikowi w momencie zakupu programu.

Aby włączyć używanie trybu testowego (pobieranie opracowywanych wersji aktualizacji), kliknij przycisk **Ustawienia...** znajdujący się obok nagłówka **Opcje**

zaawansowane, a następnie zaznacz pole wyboru **Włącz tryb testowania aktualizacji**. Aby wyłączyć wyświetlanie na pasku zadań powiadomienia po każdej udanej aktualizacji, zaznacz pole wyboru **Nie wyświetlaj powiadomienia o pomyślnej aktualizacji**.

Aby usunąć wszystkie tymczasowo przechowywane dane aktualizacji, kliknij przycisk **Wyczyść** umieszczony obok nagłówka **Czyszczenie pamięci podręcznej aktualizacji**. Opcji tej należy użyć w razie problemów z wykonaniem aktualizacji.

4.2.3 Tworzenie zadań aktualizacji

Aktualizacje można uruchamiać ręcznie, klikając opcję **Aktualizuj bazę sygnatur wirusów** w oknie głównym wyświetlanym po kliknięciu w menu głównym opcji **Aktualizacja**.

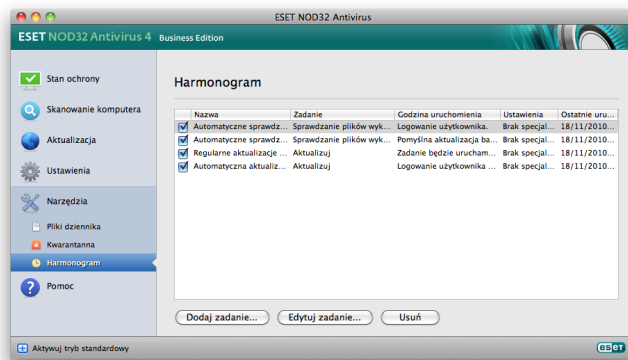
Inna możliwość to wykonywanie aktualizacji jako zaplanowanych zadań. Aby skonfigurować zaplanowanie zadanie, kliknij kolejno opcje **Zadania > Harmonogram**. Domyślnie w programie ESET NOD32 Antivirus są aktywne następujące zadania:

- Regularne aktualizacje automatyczne
- Automatyczna aktualizacja po zalogowaniu użytkownika

Każde z tych 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](#) [16].

4.3 Harmonogram

Moduł **Harmonogram** jest dostępny, gdy w programie ESET NOD32 Antivirus zostanie włączony tryb zaawansowany. Opcja **Harmonogram** znajduje się w menu głównym programu ESET NOD32 Antivirus, w kategorii **Narzędzia**. Okno **Harmonogram** zawiera listę wszystkich zaplanowanych zadań oraz ich właściwości konfiguracyjne, takie jak wstępnie zdefiniowany dzień, godzina i używany profil skanowania.



Domyślnie w oknie **Harmonogram** są wyświetlane następujące zaplanowane zadania:

- Regularne aktualizacje automatyczne
- Automatyczna aktualizacja po zalogowaniu użytkownika
- Automatyczne sprawdzanie plików przy uruchamianiu po

zalogowaniu użytkownika

- Automatyczne sprawdzanie plików przy uruchamianiu po pomyślnej aktualizacji bazy sygnatur wirusów
- Konserwacja dziennika (po włączeniu opcji **Pokaż zadania systemowe** w ustawieniach modułu Harmonogram)

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...**

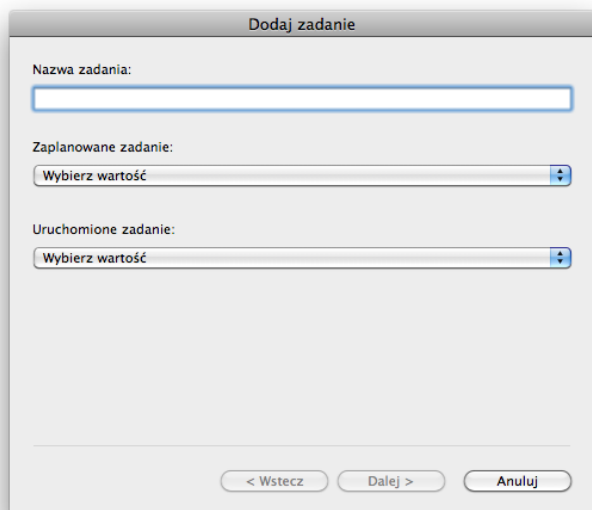
4.3.1 Cel planowania zadań

Harmonogram służy do zarządzania zaplanowanymi zadaniami oraz uruchamiania ich ze wstępnie zdefiniowaną konfiguracją i właściwościami. Konfiguracja i właściwości zawierają informacje, na przykład datę i godzinę, jak również określone profile używane podczas wykonywania zadania.

4.3.2 Tworzenie nowych zadań

Aby utworzyć nowe zadanie w harmonogramie, kliknij przycisk **Dodaj zadanie...** lub kliknij prawym przyciskiem myszy i z menu kontekstowego wybierz opcję **Dodaj...**. Dostępnych jest pięć typów zaplanowanych zadań:

- **Uruchom aplikację**
- **Aktualizuj**
- **Konserwacja dziennika**
- **Skanowanie komputera na żądanie**
- **Sprawdzanie plików wykonywanych przy uruchamianiu systemu**



Ponieważ jednym z najczęściej planowanych zadań jest aktualizacja, zostanie przedstawiony sposób dodawania nowego zadania aktualizacji.

Z menu rozwijanego **Zaplanowane zadanie** wybierz opcję **Aktualizuj**. W polu **Nazwa zadania** wprowadź nazwę zadania. W menu rozwijanym **Uruchom zadanie** wybierz częstotliwość, z jaką ma być wykonywane zadanie. Dostępne są następujące opcje: **Zdefiniowane przez użytkownika**, **Jednorazowo**, **Wielokrotnie**, **Codziennie**, **Co tydzień** i **Po wystąpieniu**

zdarzenia. Na podstawie wybranej częstotliwości wyświetlane są monity zawierające różne parametry aktualizacji. Następnie zdefiniuj czynność podejmowaną w przypadku, gdy nie można wykonać lub zakończyć zadania w zaplanowanym czasie. Dostępne są następujące trzy opcje:

- **Czekaj do następnego zaplanowanego terminu**
- **Uruchom zadanie jak najszybciej**
- **Uruchom zadanie natychmiast, jeśli od ostatniego wykonania upłynął określony czas** (upływ czasu można określić za pomocą pola przewijania **Minimalny odstęp między zadaniami**)

W następnym kroku zostanie wyświetlone okno z podsumowaniem informacji o bieżącym zaplanowanym zadaniu. Kliknij przycisk **Zakończ**.

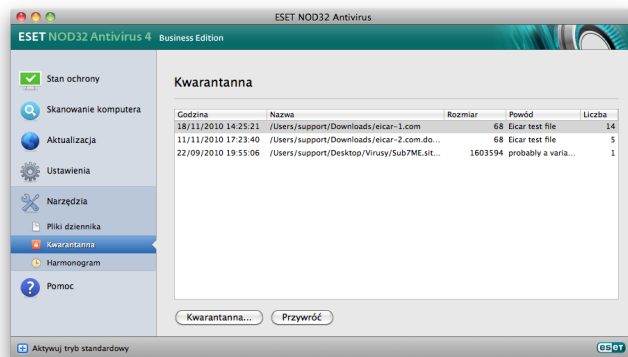
Nowe zaplanowane zadanie zostanie dodane do listy aktualnie zaplanowanych zadań.

W systemie istnieją predefiniowane ważne zaplanowane zadania zapewniające jego prawidłowe działanie. Są one domyślnie ukryte i nie należy ich zmieniać. Aby zmodyfikować tę opcję i sprawić, by zadania były widoczne, kliknij kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Narzędzia > Harmonogram**, a następnie wybierz opcję **Pokaż zadania systemowe**.

4.4 Kwarantanna

Głównym zadaniem 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 lub gdy są one nieprawidłowo wykrywane przez program ESET NOD32 Antivirus.

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. „dodane przez użytkownika”) oraz liczbę zagrożeń (np. jeśli plik jest archiwum zawierającym wiele zainfekowanych plików). Folder kwarantanny z plikami poddanymi

kwarantannie (*/Library/Application Support/Eset/cache/esets/quarantine*) pozostaje w systemie nawet po odinstalowaniu programu ESET NOD32 Antivirus. Pliki poddane kwarantannie są przechowywane w bezpiecznej, zaszyfrowanej postaci. Można je przywrócić po ponownym zainstalowaniu programu ESET NOD32 Antivirus.

4.4.1 Poddawanie plików kwarantannie

Program ESET NOD32 Antivirus automatycznie poddaje kwarantannie usunięte pliki (jeśli nie anulowano tej opcji w oknie alertu). W razie potrzeby można ręcznie poddać kwarantannie dowolny podejrzany plik, klikając przycisk **Kwarantanna....** W tym celu można również skorzystać z menu kontekstowego — kliknij prawym przyciskiem myszy w oknie **Kwarantanna**, a następnie kliknij kolejno plik, który chcesz poddać kwarantannie, i przycisk **Otwórz**.

4.4.2 Przywracanie plików z kwarantanny

Pliki poddane kwarantannie można przywracać do ich pierwotnej lokalizacji. W tym celu należy użyć przycisku **Przywróć**. Funkcja przywracania jest również dostępna w menu kontekstowym: w oknie **Kwarantanna** należy kliknąć wybrany plik prawym przyciskiem myszy i wybrać polecenie **Przywróć**. Menu kontekstowe zawiera także opcję **Przywróć do...** umożliwiającą przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.

4.4.3 Przesyłanie pliku z kwarantanny

Jeśli poddano kwarantannie podejrzany plik, który nie został wykryty przez program, lub jeśli plik został błędnie oceniony jako zainfekowany (na przykład w drodze analizy heurystycznej kodu) i następnie poddany kwarantannie, należy przesłać plik do laboratorium firmy ESET. Aby przesłać plik z kwarantanny, kliknij ten plik prawym przyciskiem myszy i z menu kontekstowego wybierz opcję **Prześlij plik do analizy**.

4.5 Pliki dziennika

Pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce w programie, oraz przegląd wykrytych zagrożeń. Zapisywanie informacji w dzienniku pełni istotną rolę przy analizie 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. Za pomocą programu ESET NOD32 Antivirus można bezpośrednio wyświetlać wiadomości tekstowe oraz wyświetlać i archiwizować dzienniki.

Pliki dziennika są dostępne z poziomu okna głównego programu ESET NOD32 Antivirus po kliknięciu kolejno opcji **Narzędzia > Pliki dziennika**. Żądany typ dziennika należy zaznaczyć w menu rozwijanym **Dziennik** znajdującym się u góry okna. Dostępne są następujące dzienniki:

1. **Wykryte zagrożenia** — po wybraniu tej opcji można zapoznać się ze wszystkimi informacjami na temat zdarzeń związanych z wykryciem infekcji.
2. **Zdarzenia** — ta opcja jest przeznaczona dla administratorów systemu i użytkowników na potrzeby rozwiązywania problemów. Wszystkie ważne czynności podejmowane przez program ESET NOD32 Antivirus są zapisywane w dziennikach zdarzeń.
3. **Skanowanie komputera** — w tym oknie są wyświetlane wyniki wszystkich ukończonych operacji skanowania. Dwukrotne kliknięcie dowolnego wpisu powoduje wyświetlenie szczegółowych informacji na temat danej operacji skanowania komputera na żądanie.

Informacje wyświetlane w każdym obszarze okna można skopiować bezpośrednio do schowka, wybierając żądaną pozycję i klikając przycisk **Kopiuje**.

4.5.1 Konserwacja dziennika

Dostęp do konfiguracji dzienników programu ESET NOD32 Antivirus można uzyskać z poziomu okna głównego programu. Kliknij kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Narzędzia > Pliki dziennika**. Można określić następujące opcje plików dziennika:

- **Automatycznie usuwaj starsze rekordy dzienników** — wpisy dziennika starsze niż podana liczba dni są usuwane automatycznie.
- **Automatycznie optymalizuj pliki dzienników** — umożliwia automatyczną defragmentację plików dziennika w przypadku przekroczenia określonego procentu nieużywanych rekordów.

Aby skonfigurować opcję **Domyślny filtr rekordów dziennika**, kliknij przycisk **Edytuj...**, a następnie zaznacz/usuń zaznaczenie żądanych typów dzienników.

4.5.2 Filtrowanie dziennika

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

Najczęściej używane typy dzienników zostały przedstawione poniżej:

- **Ostrzeżenia krytyczne** — krytyczne błędy systemowe (np. „Uruchomienie ochrony antywirusowej nie powiodło się”).
- **Błędy** — komunikaty o błędach, np. „Błąd podczas pobierania pliku”, oraz błędy krytyczne.
- **Ostrzeżenia** — komunikaty ostrzegawcze.
- **Rekordy informacyjne** — komunikaty informacyjne, w tym powiadomienia o pomyślnych aktualizacjach, alertach itp.
- **Rekordy diagnostyczne** — informacje potrzebne do ulepszenia konfiguracji programu i wszystkie rekordy wymienione powyżej.

4.6 Interfejs użytkownika

Opcje konfiguracji interfejsu użytkownika w programie ESET NOD32 Antivirus umożliwiają dostosowanie środowiska pracy do potrzeb użytkownika. Można uzyskać do nich dostęp, klikając kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Użytkownik > Interfejs**.

Znajduje się tutaj między innymi opcja Tryb zaawansowany, pozwalająca na przejście do trybu zaawansowanego. W trybie zaawansowanym są wyświetlane bardziej szczegółowe ustawienia i dodatkowe formanty programu ESET NOD32 Antivirus.

Jeśli podczas uruchamiania programu ma być wyświetlany ekran powitalny, zaznacz opcję **Pokaż ekran powitalny przy uruchamianiu**.

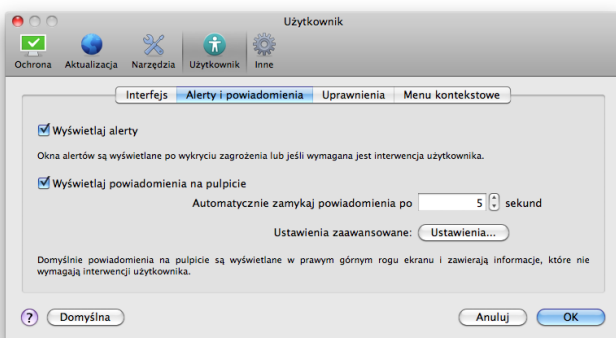
W części **Użyj standardowego menu** można wybrać opcję **W trybie standardowym** lub **W trybie zaawansowanym**, która spowoduje, że w głównym oknie programu w wybranym trybie wyświetlania będzie używane standardowe menu.

Aby włączyć wyświetlanie etykiet narzędzi, zaznacz opcję **Pokaż etykiety narzędzi**. Z kolei opcja **Pokaż ukryte pliki** umożliwia wyświetlanie i zaznaczanie ukrytych plików w części **Skanowane obiekty** znajdującej się w oknie **Skanowanie komputera**.

4.6.1 Alerty i powiadomienia

Sekcja **Alerty i powiadomienia** umożliwia konfigurację sposobu obsługi alertów o zagrożeniu i powiadomień systemowych w programie ESET NOD32 Antivirus.

Wyłączenie opcji **Wyświetlaj alerty** spowoduje anulowanie wyświetlania wszystkich okien alertów, dlatego należy jej używać tylko w szczególnych sytuacjach. W przypadku większości użytkowników zaleca się pozostawienie ustawienia domyślnego tej opcji (włączona).



Zaznaczenie opcji **Wyświetlaj powiadomienia na pulpicie** spowoduje wyświetlanie na pulpicie komputera okien alertów niewymagających interwencji ze strony użytkownika (domyślnie — w prawym górnym rogu ekranu). Za pomocą ustawienia **Automatycznie powiadomienia zamykaj po X s** można określić czas, przez jaki powiadomienia są widoczne.

4.6.1.1 Zaawansowane ustawienia alertów i powiadomień

Wyświetlaj tylko powiadomienia wymagające działania użytkownika

Ta opcja pozwala włączyć lub wyłączyć wyświetlanie komunikatów wymagających interwencji użytkownika.

Wyświetlaj tylko powiadomienia wymagające działania użytkownika podczas korzystania z aplikacji w trybie pełnego ekranu

Ta opcja jest przydatna w trakcie wykonywania prezentacji, grania czy wykonywania innych czynności wymagających dostępności całego ekranu.

4.6.2 Uprawnienia

Ustawienia programu ESET NOD32 Antivirus mogą odgrywać dużą rolę w całościowej polityce bezpieczeństwa firmy. Nieautoryzowane modyfikacje mogą rodzić zagrożenie dla stabilności i ochrony systemu. Dlatego administrator może zezwalać na modyfikowanie konfiguracji programu tylko wybranym użytkownikom.

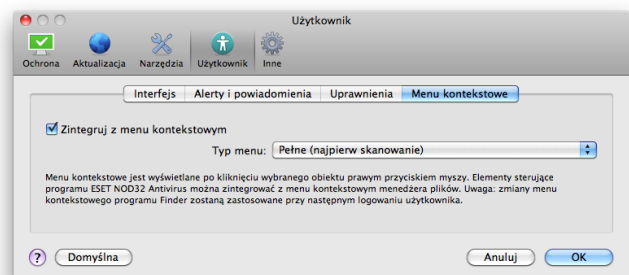
Aby wyznaczyć uprzywilejowanych użytkowników, kliknij kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Użytkownik > Uprawnienia**.

W celu zapewnienia maksymalnego bezpieczeństwa systemu ważne jest prawidłowe skonfigurowanie programu. Nieautoryzowane modyfikacje mogą powodować utratę ważnych danych. Aby utworzyć listę uprzywilejowanych użytkowników, wystarczy zaznaczyć ich na liście **Użytkownicy** znajdującej się z lewej strony, a następnie kliknąć przycisk **Dodaj**. Aby usunąć użytkownika, należy zaznaczyć jego nazwę na liście **Użytkownicy uprzywilejowani** po prawej stronie, a następnie kliknąć przycisk **Usuń**.

UWAGA: Jeśli lista uprzywilejowanych użytkowników jest pusta, wszyscy użytkownicy zdefiniowani w systemie mogą zmieniać ustawienia programu.

4.6.3 Menu kontekstowe

Integrację menu kontekstowego można włączyć, wybierając kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Użytkownik > Menu kontekstowe** i zaznaczając pole wyboru **Zintegruj z menu kontekstowym**.



4.7 ThreatSense.Net

System monitorowania zagrożeń ThreatSense.Net pomaga zapewnić natychmiastowe i ciągłe informowanie firmy ESET o nowych próbach ataków. Dwukierunkowy system monitorowania zagrożeń ThreatSense.Net ma jeden cel — udoskonalenie oferowanej ochrony. Najlepszą gwarancją wykrycia nowych zagrożeń natychmiast po ich pojawieniu się jest „połączenie” jak największej liczby naszych klientów i obsadzenie ich w roli tropicieli zagrożeń. Istnieją dwie możliwości:

1. Można nie włączać systemu monitorowania zagrożeń ThreatSense.Net. Funkcjonalność oprogramowania nie ulegnie zmniejszeniu, a użytkownik nadal będzie otrzymywać najlepszą ochronę.
2. System ThreatSense.Net można skonfigurować w taki sposób, aby anonimowe informacje o nowych zagrożeniach i lokalizacjach nowego niebezpiecznego kodu były przesyłane w postaci pojedynczego pliku. Ten plik może być przesyłany do firmy ESET w celu szczegółowej analizy. Analiza tych zagrożeń pomoże firmie ESET aktualizować bazę wirusów i poprawiać zdolność programu do wykrywania różnych form ataków.

System monitorowania zagrożeń ThreatSense.Net zgromadzi informacje o komputerze użytkownika powiązane z nowo wykrytymi zagrożeniami. Te informacje mogą zawierać próbkę lub kopię pliku, w którym wystąpiło zagrożenie, ścieżkę do tego pliku, nazwę pliku, datę i godzinę, proces, za pośrednictwem którego zagrożenie pojawiło się na komputerze, oraz informacje o systemie operacyjnym komputera.

Chociaż istnieje możliwość, że w wyniku tego pracownicy laboratorium firmy ESET mogą mieć dostęp do niektórych informacji dotyczących użytkownika lub jego komputera (np. do nazw użytkowników widocznych w ścieżce katalogu), nie będą one używane w ŻADNYM innym celu niż ulepszenie systemu monitorowania zagrożeń.

Do konfiguracji systemu ThreatSense.Net można przejść z okna Ustawienia zaawansowane, wybierając kolejno opcje **Narzędzia > ThreatSense.Net**. Zaznacz opcję **Włącz system monitorowania zagrożeń ThreatSense.Net**, aby uaktywnić tę funkcję, a następnie kliknij przycisk **Ustawienia...** znajdujący się obok nagłówka Opcje zaawansowane.

4.7.1 Podejrzane pliki

Opcja Podejrzane pliki umożliwia skonfigurowanie sposobu przesyłania zagrożeń do laboratorium firmy ESET w celu przeprowadzenia analizy.

Po wykryciu podejrzanego pliku na komputerze można go przesłać do analizy w laboratorium firmy. Jeśli plik okaże się szkodliwą aplikacją, informacje potrzebne do jej wykrywania zostaną dodane do kolejnej aktualizacji bazy sygnatur wirusów.

Przesyłanie podejrzanych plików — można zaznaczyć opcję **Podczas aktualizacji**, aby pliki były wysyłane do laboratorium firmy ESET w trakcie standardowych aktualizacji bazy sygnatur

wirusów. Można też wybrać opcję **Jak najszybciej**. Opcja ta jest odpowiednia dla komputerów ze stałym łączem internetowym.

Aby żadne pliki nie były przesyłane, należy zaznaczyć opcję **Nie przysyłaj**. Zaznaczenie opcji nieprzesyłania plików do analizy nie wpływa na przesyłanie informacji statystycznych, których ustawienia są konfigurowane w innym miejscu.

System monitorowania zagrożeń ThreatSense.Net gromadzi anonimowe informacje o komputerze użytkownika dotyczące nowo wykrytych zagrożeń. Mogą one obejmować nazwę infekcji, datę i godzinę jej wykrycia, numer wersji programu zabezpieczającego firmy ESET, wersję systemu operacyjnego oraz ustawienia regionalne. Zazwyczaj statystyka jest wysyłana do serwerów firmy ESET raz lub dwa razy dziennie.

Poniżej przedstawiono przykład wysyłanego pakietu danych statystycznych:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Przesyłanie anonimowych informacji statystycznych — użytkownik może sam określić termin wysyłania danych statystycznych. Po wybraniu opcji **Jak najszybciej** informacje statystyczne będą wysyłane natychmiast po ich utworzeniu. To ustawienie jest odpowiednie przy korzystaniu ze stałego łącza internetowego. W przypadku zaznaczenia opcji **Podczas aktualizacji** wszystkie informacje statystyczne będą wysyłane w trakcie pierwszej aktualizacji przypadającej po ich zgromadzeniu.

Jeśli użytkownik nie chce przysyłać żadnych anonimowych danych statystycznych, powinien zaznaczyć opcję **Nie przysyłaj**.

Sposób przesyłania — pozwala na wybranie sposobu przesyłania plików i informacji statystycznych do firmy ESET. Jeśli pliki i dane statystyczne mają być przesyłane wszystkimi dostępnymi sposobami, należy zaznaczyć opcję **ESET Remote Administrator Server lub ESET**. Zaznaczenie tylko opcji **ESET Remote Administrator Server** spowoduje wysyłanie informacji i plików wyłącznie do serwera zdalnej administracji, skąd następnie trafią one do laboratorium firmy ESET. W przypadku zaznaczenia opcji **ESET** podejrzane pliki i dane statystyczne będą wysyłane z programu bezpośrednio do laboratorium firmy ESET.

Filtr wyłączenia — umożliwia wykluczenie określonych plików i folderów z przesyłania. Warto na przykład wykluczyć pliki, które mogą zawierać poufne informacje, takie jak dokumenty lub arkusze kalkulacyjne. Najpopularniejsze typy plików należących do tej kategorii (np. *.doc*) są wykluczone domyślnie. Do listy wykluczonych plików można dodawać inne typy plików.

Kontaktowy adres e-mail (opcjonalnie) — adres e-mail może być wysyłany wraz z podejrzаныmi plikami. Służy wtedy do

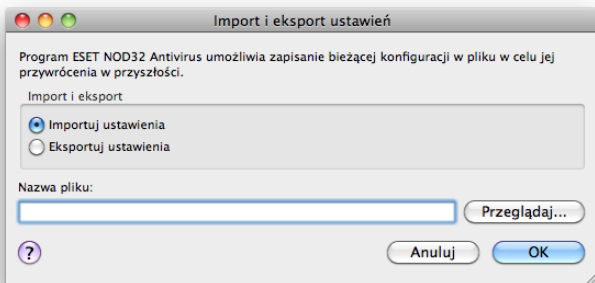
kontaktowania się z użytkownikiem w sytuacji, gdy przeprowadzenie analizy wymaga dodatkowych informacji. Należy podkreślić, że specjaliści z firmy ESET kontaktują się z użytkownikiem tylko w szczególnych przypadkach.

5. Użytkownik zaawansowany

5.1 Import i eksport ustawień

Importowanie i eksportowanie konfiguracji programu ESET NOD32 Antivirus jest dostępne w Trybie zaawansowanym w menu **Ustawienia**.

Do przechowywania konfiguracji podczas importowania i eksportowania są stosowane pliki archiwów. Funkcja eksportu i importu jest użyteczna, gdy konieczne jest utworzenie kopii zapasowej bieżącej konfiguracji programu ESET NOD32 Antivirus w celu użycia jej w późniejszym czasie. Funkcja eksportu ustawień jest również przydatna dla użytkowników, którzy chcą używać preferowanej konfiguracji programu ESET NOD32 Antivirus w wielu systemach — plik konfiguracji można łatwo zaimportować w celu przeniesienia żądanych ustawień.



5.1.1 Import ustawień

Importowanie konfiguracji jest bardzo łatwe. W menu głównym kliknij kolejno opcje **Ustawienia > Import i eksport ustawień...**, a następnie wybierz opcję **Importuj ustawienia**. Wprowadź nazwę pliku konfiguracyjnego lub kliknij przycisk **Przełączaj...**, aby wyszukać plik konfiguracyjny do zaimportowania.

5.1.2 Eksport ustawień

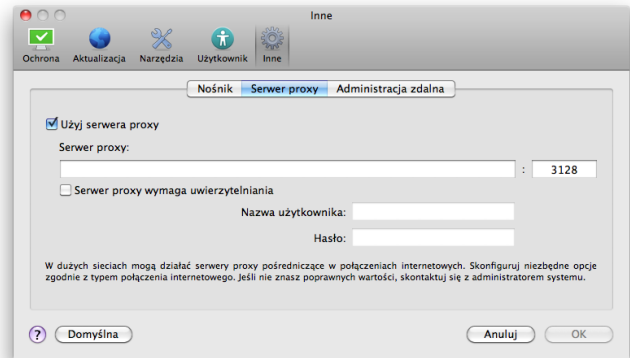
Czynności wykonywane podczas eksportu konfiguracji są bardzo podobne. W menu głównym kliknij kolejno opcje **Ustawienia > Import i eksport ustawień...** Wybierz opcję **Eksportuj ustawienia** i wprowadź nazwę pliku konfiguracyjnego. Wyszukaj i wybierz lokalizację na komputerze, w której ma zostać zapisany plik konfiguracyjny.

5.2 Ustawienia serwera proxy

Ustawienia serwera proxy można skonfigurować, wybierając kolejno opcje **Inne > Serwer proxy**. Określenie serwera proxy na tym poziomie powoduje zdefiniowanie globalnych ustawień serwera proxy dla całego programu ESET NOD32 Antivirus. Określone w tym miejscu parametry będą używane przez wszystkie moduły, które wymagają połączenia internetowego.

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

Jeśli komunikacja z serwerem proxy wymaga uwierzytelniania, zaznacz pole wyboru **Serwer proxy wymaga uwierzytelniania** i w odpowiednich polach wprowadź **nazwę użytkownika** i **hasło**.



5.3 Blokowanie nośników wymiennych

Na nośnikach wymiennych (CD, USB itd.) może znajdować się szkodliwy kod stwarzający zagrożenie dla komputera. Aby zablokować nośniki wymienne, zaznacz opcję **Włącz blokowanie nośników wymiennych**. Aby zezwolić na dostęp do określonych typów nośników, usuń zaznaczenie woluminów tych nośników.

5.4 Administracja zdalna

Program ESET Remote Administrator (ERA) to narzędzie służące do zarządzania zasadami zabezpieczeń i pozwalające uzyskać całościowy obraz zabezpieczeń wewnątrz danej sieci. Jest on szczególnie użyteczny w przypadku dużych sieci. Narzędzie ERA nie tylko zwiększa poziom bezpieczeństwa, ale również ułatwia zarządzanie programem ESET NOD32 Antivirus na klienckich stacjach roboczych.

Opcje ustawień administracji zdalnej są dostępne z poziomu okna głównego programu ESET NOD32 Antivirus. Kliknij kolejno opcje **Ustawienia > Wprowadź preferencje aplikacji... > Inne > Administracja zdalna**.

Włącz tryb administracji zdalnej, wybierając opcję **Połącz z serwerem ESET Remote Administrator**. Następnie można uzyskać dostęp do poniższych opcji:

Odstęp między połączeniami serwera — służy do określenia częstotliwości nawiązywania połączenia programu ESET NOD32 Antivirus z serwerem ERA Server. Jeśli dla tej opcji zostanie ustawiona wartość **0**, informacje będą przesyłane co 5 sekund.

ESET Remote Administrator Server — adres sieciowy serwera (na którym zainstalowany jest program ERA Server) oraz numer portu — to pole zawiera wstępnie zdefiniowany port serwera używany do nawiązywania połączenia sieciowego. Zaleca się pozostawienie domyślnego ustawienia portu (2222).

Serwer ESET Remote Administrator wymaga uwierzytelniania — służy do wprowadzenia hasła połączenia z serwerem ERA Server, jeśli jest wymagane.

Zwykle należy skonfigurować tylko serwer **Główny**. W przypadku używania kilku serwerów ERA w sieci można dodać kolejne, **Pomocnicze** połączenie z serwerem ERA Server. Będzie ono służyć jako rozwiązanie awaryjne. Jeśli serwer główny stanie się niedostępny, program ESET NOD32 Antivirus automatycznie nawiąże połączenie z serwerem pomocniczym ERA Server. Program ESET NOD32 Antivirus będzie także próbował ponownie nawiązać połączenie z serwerem głównym. Gdy to połączenie stanie się aktywne, program ESET NOD32 Antivirus przełączy się z powrotem na serwer główny. Skonfigurowanie dwóch profili serwera administracji zdalnej jest najlepszym rozwiązaniem w przypadku mobilnych klientów z przenośnymi komputerami nawiązującymi połączenia zarówno z poziomu sieci lokalnej, jak i spoza niej.

6. Słowniczek

6.1 Typy infekcji

Infekcja oznacza atak szkodliwego oprogramowania, które usiłuje uzyskać dostęp do komputera użytkownika i/lub uszkodzić jego zawartość.

6.1.1 Wirusy

Wirus komputerowy to program, który infekuje system i uszkadza pliki znajdujące się na komputerze. Nazwa tego typu programów pochodzi od wirusów biologicznych, ponieważ stosują one podobne metody przenoszenia się z jednego komputera na drugi.

Wirusy komputerowe atakują głównie pliki wykonywalne, skrypty i dokumenty. W celu powielenia wirus dokleja swój kod na końcu zaatakowanego pliku. Działanie wirusa komputerowego w skrócie przedstawia się następująco: po uruchomieniu zainfekowanego pliku wirus uaktywnia się (przed aplikacją, do której jest doklejony) i wykonuje zadanie określone przez jego twórcę. Dopiero wtedy następuje uruchomienie zaatakowanej aplikacji. Wirus nie może zainfekować komputera, dopóki użytkownik — przypadkowo lub rozmyślnie — nie uruchomi lub nie otworzy szkodliwego programu.

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 natomiast żadnych szkód — celem ich działania jest tylko zirytowanie użytkownika i zademonstrowanie umiejętności programistycznych ich twórców.

Należy zauważyć, że w porównaniu z końmi trojańskimi lub oprogramowaniem spyware wirusy stają się stopniowo coraz rzadsze, ponieważ nie przynoszą żadnych dochodów autorom szkodliwego oprogramowania. Ponadto termin „wirus” jest często błędnie używany w odniesieniu do wszystkich typów programów powodujących infekcje. Taka interpretacja powoli jednak zanika i stosowane jest nowe, ściślejsze określenie „szkodliwe oprogramowanie”.

Jeśli komputer został zaatakowany przez wirusa, konieczne jest przywrócenie zainfekowanych plików do pierwotnego stanu, czyli wyleczenie ich przy użyciu programu antywirusowego.

Przykłady wirusów: *OneHalf*, *Tenga* i *Yankee Doodle*.

6.1.2 Robaki

Robak komputerowy jest programem zawierającym szkodliwy kod, który atakuje komputery-hosty. Robaki rozprzestrzeniają się za pośrednictwem sieci. Podstawowa różnica między wirusem a robakiem polega na tym, że ten ostatni potrafi samodzielnie powielać się i przenosić — nie musi w tym celu korzystać z plików-nosicieli ani 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.

Przykłady popularnych robaków: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* i *Netsky*.

6.1.3 Konie trojańskie

Komputerowe konie trojańskie uznawano dotychczas za klasę wirusów, które udają pożyteczne programy, aby skłonić użytkownika do ich uruchomienia. Obecnie konie trojańskie już nie muszą się maskować. Ich jedynym celem jest jak najłatwiejsze przeniknięcie do systemu i wyrządzenie w nim szkód. Określenie „koń trojański” stało się bardzo ogólnym terminem używanym w odniesieniu do każdego wirusa, którego nie można zaliczyć do innej klasy infekcji.

W związku z tym, że jest to bardzo pojemna kategoria, dzieli się ją często na wiele podkategorii:

- Program pobierający (ang. downloader) — szkodliwy program, który może pobierać inne szkodliwe programy z Internetu.
- Program zakażający (ang. dropper) — rodzaj konia trojańskiego, którego działanie polega na umieszczaniu na zaatakowanych komputerach innych typów szkodliwego oprogramowania.
- Program furtki (ang. backdoor) — aplikacja, która komunikuje się ze zdalnymi intruzami, umożliwiając im uzyskanie dostępu do systemu 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 połączenia modemowe (ang. dialer) — program mający na celu nawiązywanie połączeń z kosztownymi numerami telefonicznymi. Zauważenie przez użytkownika nowego połączenia jest prawie niemożliwe. Programy takie mogą przynosić straty użytkownikom modemów telefonicznych, które nie są już regularnie eksploatowane.

- Konie trojańskie występują zwykle w postaci plików wykonywalnych. Jeśli na komputerze zostanie wykryty plik rozpoznany jako koń trojański, zaleca się jego usunięcie, ponieważ najprawdopodobniej zawiera szkodliwy kod.

Przykłady popularnych koni trojańskich: *NetBus*, *Trojandownloader*, *Small.ZLi* i *Slapper*.

6.1.4 Adware

Adware to skrót oznaczający oprogramowanie reklamowe, czyli 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, umożliwiając ich autorom pokrycie kosztów tworzenia tych (zazwyczaj użytecznych) aplikacji.

Oprogramowanie adware samo w sobie nie jest niebezpieczne — użytkownikom mogą przeszkadzać jedynie wyświetlane reklamy. Niebezpieczeństwo związane z programami adware polega jednak na tym, że mogą one zawierać funkcje śledzące (podobnie jak spyware — oprogramowanie szpiegujące).

Jeśli użytkownik zdecyduje się użyć bezpłatnego oprogramowania, powinien zwrócić szczególną uwagę na jego program instalacyjny. W programie instalacyjnym prawdopodobnie znajduje się powiadomienie o instalowaniu dodatkowych programów reklamowych. Często dostępna jest opcja umożliwiająca anulowanie instalacji programu reklamowego i zainstalowanie programu głównego bez dołączonego oprogramowania adware.

W niektórych przypadkach zainstalowanie programu bez dołączonego oprogramowania adware jest niemożliwe lub powoduje ograniczenie funkcjonalności. Dzięki temu oprogramowanie reklamowe może zostać zainstalowane w systemie w sposób legalny, ponieważ użytkownik wyraża na to zgodę. W takim przypadku należy kierować się względami bezpieczeństwa i nie ponosić konsekwencji błędnej decyzji. Jeśli na komputerze zostanie wykryty plik rozpoznany jako adware, zaleca się jego usunięcie, ponieważ istnieje duże prawdopodobieństwo, że zawiera on szkodliwy kod.

6.1.5 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, np. listy odwiedzonych witryn internetowych, adresów e-mail z listy kontaktów użytkownika lub listy znaków wprowadzanych na klawiaturze.

Twórcy oprogramowania spyware twierdzą, że te techniki mają na celu uzyskanie pełniejszych informacji o potrzebach i zainteresowaniach użytkowników oraz umożliwiają trafniejsze kierowanie reklam do odbiorców. Problem polega jednak na tym, że nie ma wyraźnego rozgraniczenia między aplikacjami użytecznymi a 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 użytkownicy są podczas instalacji programu informowani o obecności oprogramowania szpiegującego, 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 programami szpiegującymi.

Jeśli na komputerze zostanie wykryty plik rozpoznany jako spyware, zaleca się jego usunięcie, ponieważ najprawdopodobniej zawiera szkodliwy kod.

6.1.6 Potencjalnie niebezpieczne aplikacje

Istnieje wiele legalnych programów, które ułatwiają administrowanie komputerami połączonymi w sieć. Jednak w niewłaściwych rękach mogą one zostać użyte do wyrządzania szkód. Program ESET NOD32 Antivirus zawiera narzędzia pozwalające wykrywać takie zagrożenia.

Do „potencjalnie niebezpiecznych aplikacji” zaliczają się 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 usunąć ją.

6.1.7 Potencjalnie niepożądane aplikacje

Potencjalnie niepożądane aplikacje nie musiały być świadomie projektowane w złych intencjach, ale ich stosowanie może w jakimś stopniu obniżać wydajność komputera. Zainstalowanie takiej aplikacji zazwyczaj wymaga zgody użytkownika. Po zainstalowaniu programu tego typu zachowanie systemu jest inne niż przed jego instalacją. Najbardziej mogą się rzucać w oczy następujące zmiany:

- otwieranie nowych, nieznanych okien;
- aktywowanie i uruchamianie ukrytych procesów;
- zwiększone wykorzystanie zasobów systemowych;
- zmiany w wynikach wyszukiwania;
- łączenie się aplikacji z serwerami zdalnymi.