ESET Internet Security

Podręcznik użytkownika

Kliknij tutaj aby wyświetlić ten dokument jako Pomoc.

Digital Security
Progress. Protected.

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

Produkt ESET Internet Security został opracowany przez ESET, spol. s r.o.

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

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

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

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

WER. 19.03.2023

1 ESET Internet Security 1
1.1 Nowości 2
1.2 Który produkt posiadam? 3
1.3 Wymagania systemowe 4
1.3 Twoja wersja systemu Windows 7 jest przestarzała 4
1.3 System Windows 7 nie jest już obsługiwany przez firmę Microsoft 5
1.3 System Windows Vista nie jest już obsługiwany 5
1.4 Zapobieganie 6
1.5 Strony pomocy 7
2 Instalacja 8
2.1 Live Installer 9
2.2 Instalacja offline 10
2.3 Aktywacja produktu 12
2.3 Wprowadzanie klucza licencyjnego podczas aktywacji 13
2.3 Konta użytkowników ESET HOME 13
2.3 Aktywuj licencję testową 14
2.3 Bezpłatny klucz licencyjny produktu ESET 15
2.3 Aktywacja nie powiodła się — typowe scenariusze 16
2.3 Aktywacja nie powiodła się z powodu nadużycia licencji 16
2.3 Uaktualnienie licencji 17
2.3 Aktualizacja produktu 18
2.3 Starsza wersja licencji 19
2.3 Starsza wersja produktu 19
2.4 Narzędzie do rozwiązywania problemów z instalacją 20
2.5 Pierwsze skanowanie po instalacji 20
2.6 Uaktualnianie do nowszej wersji 21
2.6 Automatyczne uaktualnianie starszej wersji produktu 22
2.7 Polecanie produktu firmy ESET znajomym 22
2.7 Produkt ESET Internet Security zostanie zainstalowany 23
2.7 Zmień na inną linię produktów 23
2.7 Rejestracja 23
2.7 Postęp aktywacji 23
2.7 Aktywacja zakończona pomyślnie 23
3 Przewodnik dla początkujących 24
3.1 Połącz z ESET HOME 24
3.1 Logowanie do konta ESET HOME 25
3.1 Logowanie nie powiodło się — częste błędy 26
3.1 Dodaj urządzenie w ESET HOME 27
3.2 Główne okno programu 27
3.3 Aktualizacje 30
3.4 Konfigurowanie dodatkowych narzędzi zabezpieczających ESET 32
3.5 Skonfiguruj ochronę sieci 32
3.6 Włącz Anti-Theft 33
3.7 Narzędzia do kontroli rodzicielskiej 34
4 Praca z programem ESET Internet Security 34
4.1 Ochrona komputera 37
4.1 Silnik detekcji 38
4.1 Opcje zaawansowane silnika detekcji 43
4.1 Wykrycie infekcji 43
4.1 Ochrona systemu plików w czasie rzeczywistym 46

4.1 Poziomy leczenia 48
4.1 Zmienianie ustawień ochrony w czasie rzeczywistym 48
4.1 Sprawdzanie skuteczności ochrony w czasie rzeczywistym 48
4.1 Co zrobić, jeśli ochrona w czasie rzeczywistym nie działa 49
4.1 Wyłączenia procesów 49
4.1 Dodawanie i edytowanie wyłączeń procesów 50
4.1 Ochrona oparta na chmurze 51
4.1 Filtr wyłączeń w ramach ochrony opartej na chmurze 53
4.1 Skanowanie komputera 54
4.1 Program uruchamiający skanowanie niestandardowe 56
4.1 Postęp skanowania 58
4.1 Dziennik skanowania komputera 60
4.1 Skanowania w poszukiwaniu szkodliwego oprogramowania 62
4.1 Skanowanie w trakcie bezczynności 62
4.1 Profile skanowania 63
4.1 Skanowane obiekty 63
4.1 Kontrola dostępu do urządzeń 64
4.1 Edytor reguł kontroli dostępu do urządzeń 65
4.1 Wykryte urządzenia 66
4.1 Grupy urządzeń 66
4.1 Dodawanie reguł kontroli dostępu do urządzeń 67
4.1 Ochrona kamery internetowej 70
4.1 Edytor reguł ochrony kamery internetowej 70
4.1 System zapobiegania włamaniom działający na hoście (HIPS) 71
4.1 Okno interaktywne systemu HIPS 73
4.1 Wykryto potencjalne zachowanie oprogramowania wymuszającego okup 74
4.1 Zarządzanie regułami systemu HIPS 75
4.1 Ustawienia reguł systemu HIPS 76
4.1 Dodawanie ścieżki aplikacji/rejestru dla systemu HIPS 79
4.1 Ustawienia zaawansowane systemu HIPS 80
4.1 Sterowniki, które mogą być ładowane 80
4.1 Tryb gier 80
4.1 Skanowanie przy uruchamianiu 81
4.1 Automatyczne sprawdzanie plików przy uruchamianiu 81
4.1 Ochrona dokumentów 82
4.1 Wyłączenia 82
4.1 Pliki i foldery wyłączone ze skanowania 83
4.1 Dodawanie i edytowanie wyłączeń dotyczących wydajności 84
4.1 Format ścieżki wyłączenia 86
4.1 Zaawansowana konfiguracja wyłączeń 87
4.1 Dodawanie i edytowanie wyłączeń wykryć 89
4.1 Kreator tworzenia zaawansowanej konfiguracji wyłączeń 90
4.1 Wyłączenia systemu HIPS 91
4.1 Parametry technologii ThreatSense 92
4.1 Lista rozszerzeń plików wyłączonych ze skanowania 95
4.1 Dodatkowe parametry ThreatSense 96
4.2 Ochrona internetowa 96
4.2 Filtrowanie protokołów 98
4.2 Aplikacje wyłączone 98
4.2 Wyłączone adresy IP 99
4.2 Dodaj adres IPv4 100

4.2 Dodaj adres IPv6 100
4.2 SSL/TLS 100
4.2 Certyfikaty 102
4.2 Zaszyfrowany ruch sieciowy 102
4.2 Lista znanych certyfikatów 103
4.2 Lista aplikacji, dla których przeprowadzane jest filtrowanie protokołu SSL/TLS 104
4.2 Ochrona programów poczty e-mail 104
4.2 Integracja z programami poczty e-mail 105
4.2 Pasek narzędzi programu Microsoft Outlook 106
4.2 Pasek narzędzi do programów Outlook Express i Windows Mail 106
4.2 Okno dialogowe potwierdzenia 107
4.2 Ponowne skanowanie wiadomości 107
4.2 Protokoły poczty e-mail 108
4.2 Filtr protokołów POP3 i POP3S 109
4.2 Tagi e-mail 110
4.2 Ochrona przed spamem 110
4.2 Wynik przetwarzania adresów 112
4.2 Listy adresów antyspamowych 112
4.2 Listy adresów 113
4.2 Dodawanie/edytowanie adresu 115
4.2 Ochrona dostępu do stron internetowych 115
4.2 Ustawienia zaawansowane ochrony dostępu do stron internetowych 118
4.2 Protokoły sieciowe 118
4.2 Zarządzanie adresami URL 119
4.2 Lista adresów URL 120
4.2 Tworzenie nowej listy adresów URL 121
4.2 Jak dodać maskę adresu URL 122
4.2 Ochrona przed atakami typu „phishing” 122
4.3 Ochrona sieci 124
4.3 Ustawienia zaawansowane dotyczące ochrony sieci 126
4.3 Znane sieci 127
4.3 Edytor znanych sieci 127
4.3 Uwierzytelnianie sieci — konfiguracja serwera 130
4.3 Konfigurowanie stref 131
4.3 Strefy zapory 131
4.3 Zapora 132
4.3 Profile zapory 134
4.3 Okno dialogowe - Edytuj profile zapory sieciowej 134
4.3 Profile przypisane do kart sieciowych 135
4.3 Konfigurowanie i używanie reguł 135
4.3 Lista reguł zapory 136
4.3 Dodawanie lub edytowanie reguł zapory 137
4.3 Reguła zapory — lokalna 139
4.3 Reguła zapory — zdalna 140
4.3 Wykrywanie modyfikacji aplikacji 141
4.3 Lista aplikacji wyłączonych z wykrywania 142
4.3 Ustawienia trybu uczenia się 142
4.3 Ochrona przed atakami z sieci (IDS) 143
4.3 Ochrona przed atakami brute force 144
4.3 Reguły 144
4.3 Reguły IDS 146

4.3 Blokowanie podejrzanego zagrożenia ... 149
4.3 Rozwiązywanie problemów z ochroną sieci ... 149
4.3 Dozwolone usługi i opcje zaawansowane ... 150
4.3 Połączone sieci ... 152
4.3 Karty sieciowe ... 153
4.3 Czarna lista tymczasowa adresów IP ... 153
4.3 Dziennik ochrony sieci ... 154
4.3 Ustanawianie połączenia — wykrywanie ... 155
4.3 Rozwiązywanie problemów z zaporą ESET ... 157
4.3 Kreator rozwiązywania problemów ... 157
4.3 Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika ... 157
4.3 Tworzenie reguły na podstawie dziennika ... 158
4.3 Tworzenie wyjątków na podstawie powiadomień zapory osobistej ... 158
4.3 Zaawansowane zapisywanie w dzienniku dotyczące ochrony sieci ... 158
4.3 Rozwiązywanie problemów z filtrowaniem protokołów ... 159
4.3 Wykrycie nowej sieci ... 160
4.3 Zmiana aplikacji ... 161
4.3 Zaufana komunikacja przychodząca ... 161
4.3 Zaufana komunikacja wychodząca ... 162
4.3 Komunikacja przychodząca ... 164
4.3 Komunikacja wychodząca ... 165
4.3 Ustawienia widoku połączeń ... 166
4.4 Narzędzia zabezpieczające ... 166
4.4 Ochrona bankowości internetowej ... 167
4.4 Ustawienia zaawansowane ochrony bankowości internetowej ... 168
4.4 Chronione strony internetowe ... 169
4.4 Powiadomienie w przeglądarce ... 169
4.4 Kontrola rodzicielska ... 170
4.4 Wyjątki dla witryny internetowej ... 172
4.4 Konta użytkowników ... 174
4.4 Kategorie ... 175
4.4 Obsługa kont użytkowników ... 176
4.4 Skopiuj wyjątki z ustawień użytkownika ... 178
4.4 Skopiuj kategorie z konta ... 178
4.4 Włącz kontrolę rodzicielską ... 178
4.4 Anti-Theft ... 178
4.4 Zaloguj się na swoje konto ESET HOME. ... 180
4.4 Konfiguracja nazwy urządzenia ... 181
4.4 Anti-Theft włączono/wyłączono ... 181
4.4 Dodawanie nowego urządzenia nie powiodło się ... 181
4.5 Aktualizowanie programu ... 182
4.5 Ustawienia aktualizacji ... 184
4.5 Cofanie aktualizacji ... 186
4.5 Interwał czasu wycofywania ... 188
4.5 Aktualizacje produktów ... 189
4.5 Opcje połączenia ... 189
4.5 Tworzenie zadań aktualizacji ... 190
4.5 Okno dialogowe – Wymagane uruchomienie ponowne ... 190
4.6 Narzędzia ... 190
4.6 Inspekcja sieci ... 191
4.6 Urządzenie sieciowe w Inspekcji sieci ... 194

4.6 Powiadomienia | Inspekcja sieci ... 197
4.6 Narzędzia w programie ESET Internet Security ... 197
4.6 Pliki dziennika ... 199
4.6 Filtrowanie dziennika ... 201
4.6 Konfiguracja dzienników ... 202
4.6 Uruchomione procesy ... 203
4.6 Raport zabezpieczeń ... 205
4.6 Połączenia sieciowe ... 207
4.6 Działanie w sieci ... 209
4.6 ESET SysInspector ... 210
4.6 Harmonogram ... 211
4.6 Opcje planowanego skanowania ... 213
4.6 Przegląd zaplanowanego zadania ... 214
4.6 Szczegóły zadania ... 215
4.6 Częstotliwość wykonywania zadania ... 215
4.6 Czas zadania - Raz ... 215
4.6 Czas zadania - Codziennie ... 216
4.6 Czas zadania - Co tydzień ... 216
4.6 Czas zadania — zdarzenie wyzwalane ... 216
4.6 Pominięte zadanie ... 216
4.6 Szczegóły zadania - Aktualizacja ... 217
4.6 Szczegóły zadania - Uruchom aplikację ... 217
4.6 Leczenie systemu ... 218
4.6 ESET SysRescue Live ... 219
4.6 Kwarantanna ... 219
4.6 Serwer proxy ... 222
4.6 Wybieranie próbki do analizy ... 223
4.6 Wybieranie próbki do analizy — podejrzany plik ... 224
4.6 Wybieranie próbki do analizy — podejrzana witryna ... 224
4.6 Wybieranie próbki do analizy — plik z fałszywym alarmem ... 225
4.6 Wybieranie próbki do analizy — witryna z fałszywym alarmem ... 225
4.6 Wybieranie próbki do analizy — inne ... 226
4.6 Aktualizacja systemu Microsoft Windows® ... 226
4.6 Okno dialogowe – Aktualizacje systemu ... 226
4.6 Informacje o aktualizacjach ... 226
4.7 Interfejs użytkownika ... 227
4.7 Elementy interfejsu użytkownika ... 227
4.7 Ustawienia dostępu ... 228
4.7 Hasło do ustawień zaawansowanych ... 229
4.7 Ikona na pasku zadań ... 229
4.7 Obsługa czytnika ekranu ... 231
4.7 Pomoc i obsługa ... 231
4.7 Informacje o programie ESET Internet Security ... 232
4.7 Aktualności ESET ... 232
4.7 Przesyłanie danych konfiguracji systemu ... 233
4.7 Pomoc techniczna ... 234
4.8 Powiadomienia ... 234
4.8 Okno dialogowe - Stany aplikacji ... 235
4.8 Powiadomienia na pulpicie ... 235
4.8 Lista powiadomień na pulpicie ... 237
4.8 Interaktywne alerty ... 238

4.8 Komunikaty wymagające potwierdzeń ... 240
4.8 Nośniki wymienne ... 241
4.8 Przekazywanie ... 242
4.9 Ustawienia prywatności ... 244
4.10 Profile ... 245
4.11 Skróty klawiaturowe ... 246
4.12 Diagnostyka ... 247
4.12 Pomoc techniczna ... 249
4.12 Import i eksport ustawień ... 249
4.12 Przywracanie wszystkich ustawień w bieżącej sekcji ... 250
4.12 Przywróć ustawienia domyślne ... 250
4.12 Błąd podczas zapisywania konfiguracji ... 250
4.13 Skaner wiersza polecenia ... 251
4.14 Funkcja poleceń ESET CMD ... 253
4.15 Wykrywanie stanu bezczynności ... 255
5 Często zadawane pytania ... 255
5.1 Aktualizowanie programu ESET Internet Security ... 257
5.2 Usuwanie wirusa z komputera ... 257
5.3 Zezwalanie na komunikację określonej aplikacji ... 257
5.4 Włączanie kontroli rodzicielskiej na koncie ... 258
5.5 Tworzenie nowego zadania w harmonogramie ... 259
5.6 Planowanie cotygodniowego skanowania komputera ... 260
5.7 Jak usunąć błąd „Nie można przekierować ochrony bankowości internetowej do żądanej strony internetowej” ... 261
5.8 Odblokowywanie obszaru Ustawienia zaawansowane ... 263
5.9 Jak rozwiązać dezaktywację produktu z ESET HOME ... 264
5.9 Produkt dezaktywowano, a urządzenie zostało odłączone ... 264
5.9 Produkt nie został aktywowany ... 264
6 Program poprawy jakości doświadczeń użytkowników ... 265
7 Umowa licencyjna użytkownika końcowego ... 266
8 Zasady ochrony prywatności ... 279

ESET Internet Security

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

ESET Internet Security to kompletne rozwiązanie zabezpieczające, połączenie maksymalnej ochrony i minimalnego obciążenia systemu. Zaawansowane techniki oparte na sztucznej inteligencji potrafią zapobiegać przenikaniu do systemu wirusów, oprogramowania spyware, koni trojańskich, robaków, oprogramowania adware i programów typu rootkit oraz innych ataków bez obniżania wydajności komputera czy zakłócania jego pracy.

Funkcje i zalety

Przeprojektowany interfejs użytkownika	Interfejs użytkownika w tej wersji został przeprojektowany i uproszczony na podstawie wyników testów użyteczności. Wszystkie sformułowania w graficznym interfejsie użytkownika i powiadomieniach zostały dokładnie sprawdzone i poprawione. Interfejs teraz obsługuje języki pisane od prawej do lewej, na przykład hebrajski i arabski. Pomoc online została zintegrowana z programem ESET Internet Security i udostępnia dynamicznie aktualizowaną treść pomocy.
Moduł antywirusowy i antyspyware	Aktywnie wykrywa i leczy więcej znanych i nieznanych wirusów, robaków, koni trojańskich oraz programów typu rootkit. Zaawansowana heurystyka oznacza nawet nigdy przedtem niespotykane szkodliwe oprogramowanie, chroniąc użytkownika przed nieznanymi zagrożeniami i eliminując je, zanim zdążą wyrządzić szkody. Ochrona dostępu do stron internetowych i ochrona przed atakami typu „phishing” monitoruje komunikację między przeglądarkami internetowymi a zdalnymi serwerami (obsługuje połączenia SSL). Ochrona programów poczty e-mail oferuje sprawdzanie komunikacji przychodzącej za pośrednictwem protokołów POP3(S) oraz IMAP(S).
Regularna aktualizacja	Regularne aktualizowanie silnika detekcji (wcześniej nazywanego „bazą sygnatur wirusów”) i modułów programu to najlepszy sposób na zapewnienie maksymalnego bezpieczeństwa komputera.
ESET LiveGrid® (Reputacja oparta na chmurze)	Użytkownik może sprawdzić reputację działających procesów i plików bezpośrednio z poziomu programu ESET Internet Security.
Kontrola dostępu do urządzeń	Automatycznie skanuje wszystkie dyski flash USB, karty pamięci i płyty CD/DVD. Blokuje dyski przenośne w zależności od typu nośnika, producenta, rozmiaru i innych atrybutów.
Funkcja HIPS	Zachowanie systemu można dostosować bardziej szczegółowo, określając reguły dla rejestru systemu, aktywnych procesów i programów oraz konfigurując ustawienia zabezpieczeń.
Tryb gier	Opóźnia wyświetlanie wszystkich wyskakujących okienek, aktualizacji i innych obciążających system działań, aby zaoszczędzić zasoby systemu na potrzeby gier i innych pełnoekranowych aktywności.

Funkcje w programie ESET Internet Security

Ochrona bankowości internetowej	Funkcja Ochrona bankowości internetowej udostępnia zabezpieczoną przeglądarkę, której można używać podczas korzystania z bankowości elektronicznej i stron do wykonywania płatności. Dzięki temu wszystkie transakcje online są przeprowadzane w zaufanym i bezpiecznym środowisku.
Obsługa sygnatur sieciowych	sygnatury sieciowe umożliwiają szybkie wykrywanie i blokowanie szkodliwego ruchu do urządzeń użytkowników i od nich, związanego z botami i pakietami programów typu exploit. Tę funkcję można traktować jako rozwinięcie ochrony przed botnetami.
Inteligentna zapora	Uniemożliwia nieupoważnionym użytkownikom dostęp do komputera oraz do informacji osobistych.
ESET Antispam	Spam stanowi obecnie aż 50% wszystkich wysyłanych wiadomości e-mail. Ochrona przed spamem służy jako rozwiązanie zabezpieczające przed tym problemem.
Anti-Theft	Anti-Theft rozszerza zabezpieczenia na poziomie użytkownika w przypadku utraty lub kradzieży komputera. Po zainstalowaniu przez użytkownika programu ESET Internet Security oraz funkcji Anti-Theft jego urządzenie będzie wyświetlane w interfejsie sieciowym. Interfejs sieciowy umożliwia zarządzanie konfiguracją funkcji Anti-Theft i administrowanie tą funkcją na urządzeniu.
Kontrola rodzicielska	Ochrona członków rodziny przed potencjalnie obraźliwymi materiałami przez blokowanie różnych kategorii witryn internetowych.

Wszystkie funkcje programu ESET Internet Security działają bez żadnych ograniczeń tylko wtedy, gdy licencja jest aktywna. Zalecamy odnawianie licencji na kilka tygodni przed wygaśnięciem licencji programu ESET Internet Security.

Nowości

Nowości w programie ESET Internet Security w wersji 15

Ulepszona Inspekcja sieci (dawniej Sieć domowa)

Pomaga chronić sieć i urządzenia IoT oraz pokazuje urządzenia podłączone do routera. Dowiedz się, jak sprawdzić używane sieci i podłączone urządzenia.

ESET HOME (dawniej myESET)

Zapewnia lepszą widoczność i kontrolę nad bezpieczeństwem. Zainstaluj zabezpieczenia na nowych urządzeniach, dodawaj i udostępniaj licencje oraz otrzymuj ważne powiadomienia za pośrednictwem aplikacji mobilnej i portalu internetowego. Aby uzyskać więcej informacji, odwiedź Przewodnik pomocy online ESET HOME.

Ulepszony system zapobiegania włamaniom działający na hoście (HIPS)

Skanuje obszary pamięci, które mogą zostać zmodyfikowane za pomocą zaawansowanych technik wstrzykiwania szkodliwego oprogramowania. Ulepszenia rozszerzają jego możliwości technologiczne do wykrywania najbardziej wyrafinowanych form szkodliwego oprogramowania.

Obrazy i dodatkowe informacje na temat nowych funkcji w programie ESET Internet Security, patrz Co nowego w najnowszej wersji produktów ESET dla użytkowników domowych.

Aby wyłączyć powiadomienia **Co nowego**, przejdź do pozycji **Ustawienia zaawansowane** > **Powiadomienia** > **Powiadomienia na pulpicie**. Kliknij opcję **Edytuj** obok pozycji **Powiadomienia na pulpicie** i usuń zaznaczenie pola wyboru **Wyświetlaj powiadomienia o nowościach**. Aby uzyskać więcej informacji na temat powiadomień, zapoznaj się z sekcją Powiadomienia.

Który produkt posiadam?

Firma ESET oferuje wielowarstwowe zabezpieczenia, oddając w ręce użytkowników nowe produkty — od szybkiego i skutecznego rozwiązania antywirusowego po kompleksowe rozwiązanie zabezpieczające wywierające minimalny wpływ na działanie systemu:

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**

W celu sprawdzenia, który z produktów został zainstalowany należy otworzyć okno główne programu i przeczytać nazwę produktu widoczną u góry okna (szczegóły w tym artykule bazy wiedzy).

W poniższej tabeli wyszczególniono funkcje dostępne w poszczególnych produktach.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Silnik detekcji	✔	✔	✔
Zaawansowane uczenie maszynowe	✔	✔	✔
Blokada programów typu Exploit	✔	✔	✔
Ochrona przed atakami skryptowymi	✔	✔	✔
Ochrona przed atakami typu „phishing”	✔	✔	✔
Ochrona dostępu do stron internetowych	✔	✔	✔
HIPS (w tym ochrona przed oprogramowaniem wymuszającym okup)	✔	✔	✔
Ochrona przed spamem		✔	✔
Zapora		✔	✔
Inspekcja sieci		✔	✔
Ochrona kamery internetowej		✔	✔
Ochrona przed atakami z sieci		✔	✔
Ochrona przed botnetami		✔	✔
Ochrona bankowości internetowej		✔	✔
Kontrola rodzicielska		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Niektóre z powyższych produktów mogą być niedostępne w danym języku / regionie.

Wymagania systemowe

Aby program ESET Internet Security działał w sposób optymalny, system powinien spełniać następujące wymagania dotyczące sprzętu i oprogramowania:

Obsługiwane procesory

Procesor Intel lub AMD, 32-bitowy (x86) z instrukcjami SSE2 lub 64-bitowy (x64), 1 GHz lub szybszy
Procesor oparty na ARM64, 1 GHz lub szybszy

Obsługiwane systemy operacyjne*

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 z dodatkiem SP1 z najnowszymi aktualizacjami systemu Windows
Microsoft® Windows® Home Server 2011 64-bit

Dopilnuj, aby system operacyjny zawsze był aktualny.

Anti-Theft nie obsługuje systemu Microsoft Windows Home Server.

Inne

Aby aktywacja i aktualizacje programu ESET Internet Security działały prawidłowo, konieczne jest połączenie z Internetem.

Dwa programy antywirusowe działające jednocześnie na jednym urządzeniu powodują nieuniknione konflikty zasobów systemowych, co może spowodować takie spowolnienie systemu, że nie będzie się dało na nim pracować.

* Program ESET nie może zapewnić ochrony nieobsługiwanym systemom operacyjnym od lutego 2021 roku.

Twoja wersja systemu Windows 7 jest przestarzała

Problem

Korzystasz z przestarzałej wersji systemu operacyjnego. Aby zachować ochronę, dbaj o aktualność systemu operacyjnego.

Rozwiązanie

Masz zainstalowany program ESET Internet Security w systemie {GET_OSNAME} {GET_BITNESS}.

Sprawdź, czy masz zainstalowany dodatek Windows 7 Service Pack 1 (SP1) z najnowszymi aktualizacjami systemu Windows (co najmniej KB4474419 i KB4490628).

Jeśli nie masz skonfigurowanego automatycznego aktualizowania systemu Windows 7, kliknij **menu Start** > **Panel sterowania** > **System i zabezpieczenia** > **Windows Update** > **Sprawdź dostępne aktualizacje**, a następnie kliknij **Zainstaluj aktualizacje**.

Zobacz też: System Windows 7 nie jest już obsługiwany przez firmę Microsoft.

System Windows 7 nie jest już obsługiwany przez firmę Microsoft

Problem

Firma Microsoft zakończyła obsługę systemu Windows 7 w dniu 14 stycznia 2020 r. Co to oznacza?

Jeśli po zakończeniu obsługi dalej korzystasz z systemu Windows 7, komputer nadal będzie działał, ale może stać się bardziej narażony na zagrożenia bezpieczeństwa i wirusy. Komputer nie będzie już otrzymywać aktualizacji systemu Windows (w tym aktualizacji zabezpieczeń).

Rozwiązanie

Uaktualniasz system Windows 7 do systemu Windows 10? Zaktualizuj produkt firmy ESET

Proces uaktualniania jest stosunkowo łatwy, a w wielu przypadkach można to zrobić bez utraty plików. Przed przeniesieniem się na system Windows 10:

1. Sprawdź/zaktualizuj produkt firmy ESET
2. Wykonywanie zapasowych kopii ważnych danych
3. Przeczytaj artykuł firmy Microsoft pt. „Uaktualnianie do systemu Windows 10: często zadawane pytania” i zaktualizuj system Windows

Kupujesz nowy komputer lub nowe urządzenie? Przenieś produkt firmy ESET

Jeśli masz lub zamierzasz kupić nowe urządzenie lub nowy komputer, dowiedz się, jak przenieść istniejący produkt firmy ESET na nowe urządzenia.

Zobacz też Zakończył się okres świadczenia pomocy technicznej dotyczącej systemu Windows 7.

System Windows Vista nie jest już obsługiwany

Problem

Ze względu na ograniczenia techniczne systemu Windows Vista program ESET Internet Security nie będzie już zapewniał ochrony po **lutym 2021 roku**. Produkt firmy ESET **przestanie działać**. W rezultacie komputer może być narażony na infekcje.

Firma Microsoft zakończyła obsługę systemu Windows Vista w dniu 11 kwietnia 2017 r. Co to oznacza?

Jeśli po zakończeniu obsługi dalej korzystasz z systemu Windows Vista, komputer nadal będzie działał, ale może stać się bardziej narażony na zagrożenia bezpieczeństwa i wirusy. Komputer nie będzie już otrzymywać aktualizacji systemu Windows (w tym aktualizacji zabezpieczeń).

Rozwiązanie

Przenosisz się z systemu Windows Vista na Windows 10? Kup nowy komputer lub inne urządzenie i przenieś na nie produkt firmy ESET

Przed przeniesieniem się na system Windows 10:

1. Wykonywanie zapasowych kopii ważnych danych
2. Przeczytaj artykuł firmy Microsoft pt. „Uaktualnianie do systemu Windows 10: często zadawane pytania” i zaktualizuj system Windows
3. Zainstaluj lub przenieś istniejący produkt firmy ESET na nowe urządzenie.

Zobacz też Zakończył się okres świadczenia pomocy technicznej dotyczącej systemu Windows Vista.

Zapobieganie

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

Regularne aktualizowanie

Zgodnie z danymi statystycznymi uzyskanymi dzięki systemowi ESET LiveGrid® 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 pełnego skanowania komputera przynajmniej raz w miesiącu, ponieważ sygnatury szkodliwego oprogramowania mogą się zmieniać, a silnik detekcji jest aktualizowany 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.

Strony pomocy

Witamy w podręczniku użytkownika programu ESET Internet Security. Umieszczone tu informacje pomogą poznać ten program oraz zwiększyć bezpieczeństwo używania komputera.

Informacje wstępne

Przed przystąpieniem do korzystania z programu ESET Internet Security wskazane jest zapoznanie się z różnymi typami detekcji i ataków zdalnych, które mogą wystąpić podczas używania komputera.

Opracowaliśmy również listę nowych funkcji wprowadzonych w programie ESET Internet Security oraz przewodnik ułatwiający konfigurowanie ustawień podstawowych.

Jak korzystać ze stron pomocy programu ESET Internet Security

Tematy pomocy podzielono na kilka rozdziałów i podrozdziałów. Aby wyświetlić informacje o aktualnie otwartym oknie, należy nacisnąć klawisz **F1**.

W programie można wyszukiwać tematy pomocy na podstawie słów kluczowych. Można również przeszukać treść

pomocy, wpisując słowa lub frazy. Różnica między tymi dwiema metodami polega na tym, że słowo kluczowe może być logicznie powiązane ze stronami pomocy, których treść nie zawiera danego słowa. Wyszukiwanie słów i fraz polega na przeszukaniu zawartości wszystkich stron i wyświetleniu tylko tych, których treść zawiera szukane słowo lub frazę.

W celu zapewnienia zgodności oraz uniknięcia pomyłek w niniejszym podręczniku stosowana jest terminologia oparta na nazwach parametrów programu ESET Internet Security. Zastosowaliśmy również jednolity zbiór symboli do oznaczenia konkretnych tematów o określonym poziomie ważności.

Uwagi stanowią krótkie spostrzeżenia. Można je pominąć, lecz mogą również zawierać cenne informacje dotyczące określonych funkcji lub łącza do podobnych tematów.

Zagadnienia te wymagają uwagi czytelnika i zachęcamy do zapoznania się z nimi. Zazwyczaj zawierają istotne informacje niemające krytycznego znaczenia.

Są to informacje wymagające poświęcenia szczególnej uwagi i zachowania ostrożności. Ostrzeżenia zostały umieszczone specjalnie w celu uniknięcia potencjalnie szkodliwych błędów. Należy dokładnie zapoznać się z treścią ostrzeżenia, ponieważ dotyczy ono wrażliwych ustawień systemowych lub zagadnień związanych z ryzykiem.

Jest to przypadek użycia lub praktyczny przykład pomagający zrozumieć stosowanie danej funkcji.

Oznaczenie	Znaczenie
Pogrubiona czcionka	Nazwy elementów interfejsu takich, jak pola lub przyciski opcji.
Pochylona czcionka	Elementy zastępcze dla informacji wprowadzanych przez użytkownika. Na przykład nazwa pliku lub ścieżka oznaczają, że rzeczywista ścieżka lub nazwa pliku są wprowadzane przez użytkownika.
`Courier New`	Przykłady kodu lub poleceń.
Hiperłącze	Zapewnia szybki i łatwy dostęp do przywoływanych tematów lub zewnętrznych adresów internetowych. Hiperłącza są zaznaczone na niebiesko i mogą być podkreślone.
%ProgramFiles%	Katalog systemowy, w którym przechowywane są programy instalowane w systemie Windows.

Pomoc online stanowi podstawowe źródło treści pomocy. Po nawiązaniu połączenia z Internetem automatycznie zostanie wyświetlona najnowsza wersja Pomocy online.

Instalacja

Istnieje kilka metod instalacji produktu ESET Internet Security na komputerze. Metody instalacji mogą się różnić w zależności od kraju i sposobów dystrybucji:

- Instalator Live Installer — może być pobrany ze strony internetowej firmy ESET lub zainstalowany z płyty CD/DVD. Pakiet instalacyjny jest uniwersalny dla wszystkich języków (należy wybrać odpowiedni język). Instalator Live Installer jest niewielkim plikiem. Dodatkowe pliki wymagane do instalacji produktu ESET Internet Security zostaną pobrane automatycznie.

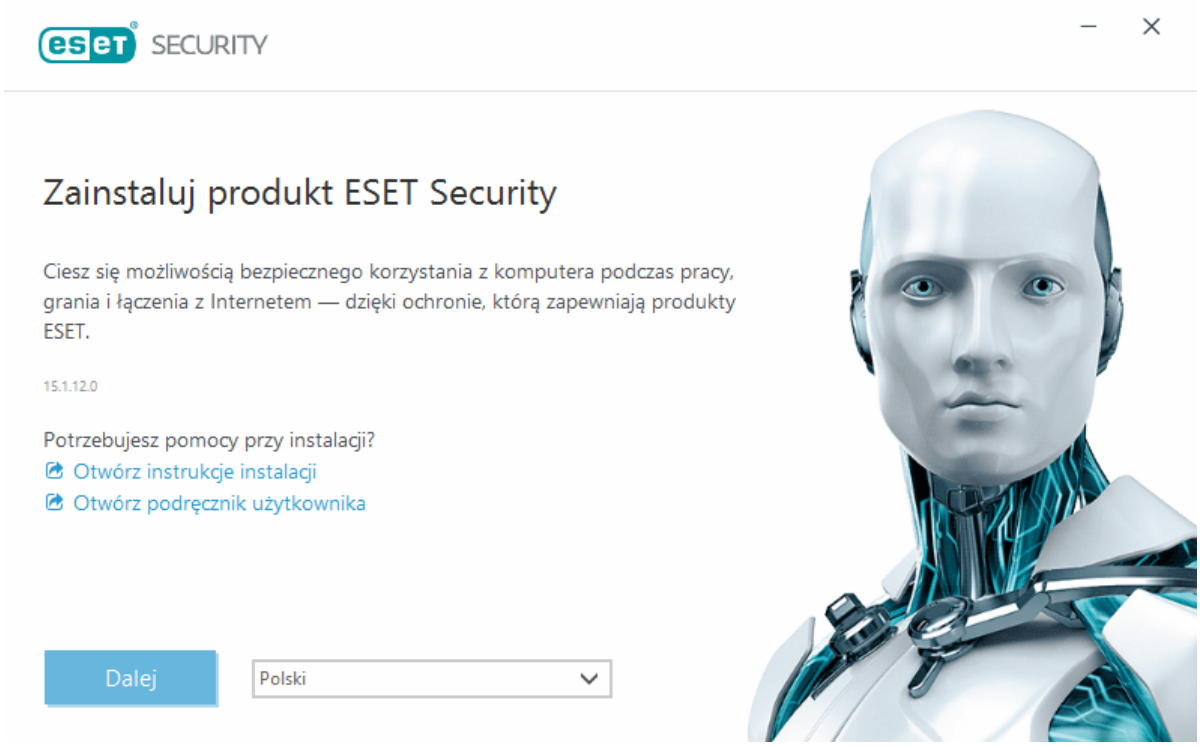
- Instalator offline — korzysta z pliku .exe, który jest większy niż plik instalatora Live Installer i do zakończenia instalacji nie wymaga połączenia z Internetem ani dodatkowych plików.

Przed instalacją produktu ESET Internet Security 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 bazie wiedzy ESET.

Instalator Live Installer

Po pobraniu pakietu instalacyjnego Live Installer należy dwukrotnie kliknąć plik instalacyjny i postępować zgodnie ze szczegółowymi instrukcjami wyświetlanymi w oknie kreatora instalacji.

W przypadku tego typu instalacji wymagane jest połączenie z Internetem.



1. Wybierz odpowiedni język z menu rozwijanego i kliknij przycisk **Kontynuuj**.

Jeśli instalujesz nowszą wersję w miejsce wersji starszej z ustawieniami chronionymi hasłem, wprowadź hasło. Hasło do konfiguracji można ustawić w oknie Konfiguracja dostępu.

2. Wybierz preferencje dotyczące dla następujących funkcji, przeczytaj Umowę licencyjną użytkownika końcowego oraz Politykę prywatności, a następnie kliknij przycisk **Kontynuuj** lub przycisk **Zezwalaj na wszystkie i kontynuuj**, aby włączyć wszystkie funkcje:

- System informacji zwrotnych ESET LiveGrid®
- Potencjalnie niepożądane aplikacje
- Program poprawy jakości doświadczeń użytkowników

Klikając przycisk **Kontynuuj** lub **Zezwalaj na wszystkie i kontynuuj**, akceptujesz Umowę licencyjną użytkownika końcowego i Politykę prywatności.

3. Aby aktywować zabezpieczenia urządzenia, zarządzać nimi i wyświetlać je za pomocą portalu ESET HOME, połącz urządzenie z kontem ESET HOME. Kliknij **Pomiń logowanie**, aby kontynuować bez łączenia się z kontem ESET HOME. Możesz połączyć urządzenie ze swoim kontem ESET HOME w późniejszym czasie.

4. Jeśli zdecydujesz się kontynuować bez połączenia z ESET HOME, wybierz opcję aktywacji. Jeśli instalujesz nowszą wersję na wersji starszej, klucz licencyjny zostanie wpisany automatycznie.

5. Na podstawie licencji kreator instalacji określa, który produkt firmy ESET ma zostać zainstalowany. Domyślnie wybierana jest wersja posiadająca największą liczbę funkcji zabezpieczających. Kliknij pozycję **Zmień produkt**, jeśli chcesz zainstalować inną wersję produktu ESET. Kliknij przycisk **Kontynuuj**, aby uruchomić proces instalacji. Może on chwilę potrwać.

Jeśli zostaną jakieś pozostałości (pliki lub foldery) produktów ESET odinstalowanych w przeszłości, zostanie wyświetlony komunikat z prośbą o ich usunięcie. Kliknij przycisk **Zainstaluj**, aby kontynuować.

6. Kliknij przycisk **Gotowe**, aby zamknąć kreator instalacji.

Narzędzie do rozwiązywania problemów z instalacją.

Po instalacji i aktywacji produktu rozpoczyna się pobieranie modułów. Zostaje zainicjowana ochrona, a niektóre funkcje mogą nie działać w pełni do czasu pełnego pobrania modułów.

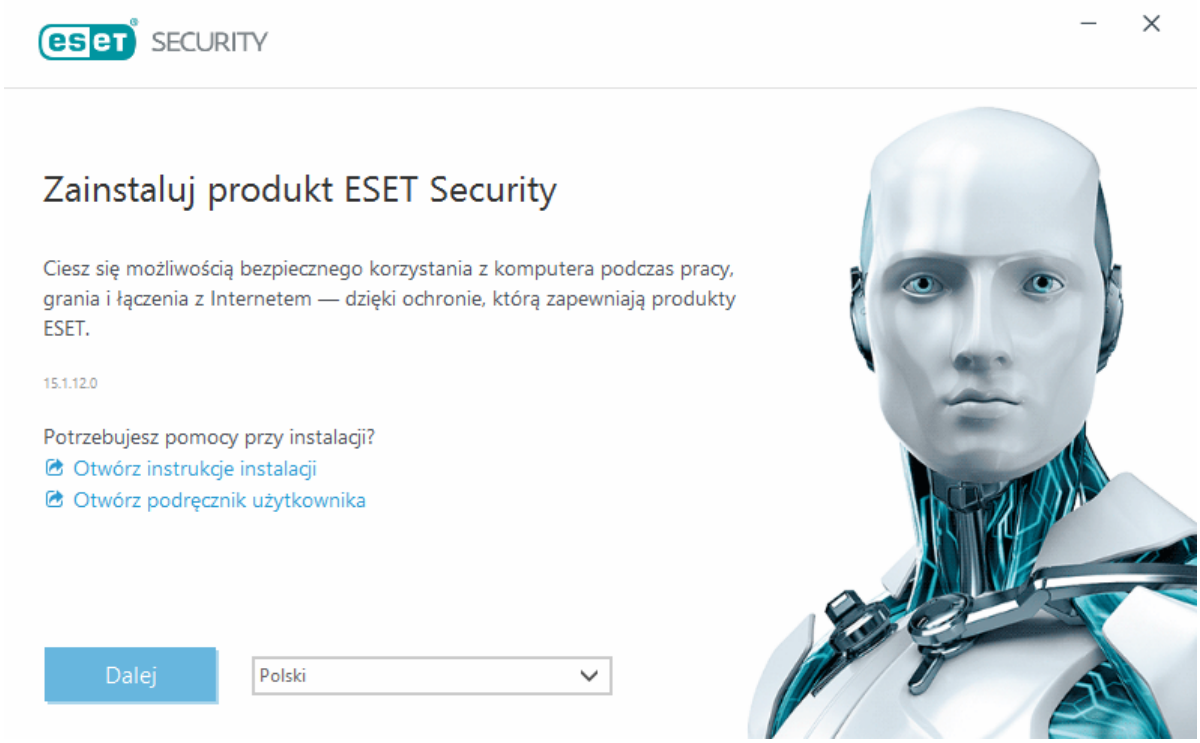
Instalacja offline

Pobierz i zainstaluj swój produkt ESET do systemu Windows przeznaczony dla użytkowników domowych przy użyciu instalatora offline (z pliku .exe) dostępnego poniżej. Wybierz wersję produktu ESET home do pobrania (32-bitową, 64-bitową lub ARM).

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Wersja 64-bitowa Wersja 32-bitowa ARM Ściągnij za darmo	Wersja 64-bitowa Wersja 32-bitowa ARM Ściągnij za darmo	Wersja 64-bitowa Wersja 32-bitowa ARM Ściągnij za darmo

Jeśli posiadasz aktywne połączenie internetowe, zainstaluj produkt ESET przy użyciu instalatora Live Installer.

Po uruchomieniu instalatora offline (z pliku .exe) kreator instalacji poprowadzi użytkownika przez czynności konfiguracyjne.



1. Wybierz odpowiedni język z menu rozwijanego i kliknij przycisk **Kontynuuj**.

Jeśli instalujesz nowszą wersję w miejsce wersji starszej z ustawieniami chronionymi hasłem, wprowadź hasło. Hasło do konfiguracji można ustawić w oknie Konfiguracja dostępu.

2. Wybierz preferencje dotyczące dla następujących funkcji, przeczytaj Umowę licencyjną użytkownika końcowego oraz Politykę prywatności, a następnie kliknij przycisk **Kontynuuj** lub przycisk **Zezwalaj na wszystkie i kontynuuj**, aby włączyć wszystkie funkcje:

- System informacji zwrotnych ESET LiveGrid®
- Potencjalnie niepożądane aplikacje
- Program poprawy jakości doświadczeń użytkowników

Klikając przycisk **Kontynuuj** lub **Zezwalaj na wszystkie i kontynuuj**, akceptujesz Umowę licencyjną użytkownika końcowego i Politykę prywatności.

3. Kliknij pozycję **Pomiń logowanie**. Jeśli posiadasz połączenie internetowe, możesz połączyć urządzenie z kontem ESET HOME.

4. Kliknij pozycję **Pomiń aktywację**. Produkt ESET Internet Security musi zostać aktywowany po zakończeniu instalacji, aby produkt był w pełni funkcjonalny. Aktywacja produktu wymaga aktywnego połączenia z Internetem.

5. Kreator instalacji zawiera informację, który produkt firmy ESET zostanie zainstalowany na podstawie pobranego instalatora offline. Kliknij przycisk **Kontynuuj**, aby uruchomić proces instalacji. Może on chwilę potrwać.

Jeśli zostaną jakieś pozostałości (pliki lub foldery) produktów ESET odinstalowanych w przeszłości, zostanie wyświetlony komunikat z prośbą o ich usunięcie. Kliknij przycisk **Zainstaluj**, aby kontynuować.

6. Kliknij przycisk **Gotowe**, aby zamknąć kreator instalacji.

Narzędzie do rozwiązywania problemów z instalacją.

Aktywacja produktu

Istnieje kilka dostępnych 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.).

- W przypadku nabycia pudełkowej wersji produktu lub otrzymania wiadomości e-mail ze szczegółami licencji, program należy aktywować, klikając opcję **Wprowadź klucz licencyjny**. Klucz licencyjny znajduje się zazwyczaj wewnątrz lub na tylnej stronie opakowania produktu. Aby aktywacja produktu przebiegła pomyślnie, klucz licencyjny należy wprowadzić w postaci, w jakiej został dostarczony. Klucz licencyjny — niepowtarzalny ciąg znaków w formacie XXXX-XXXX-XXXX-XXXX-XXXX lub XXXX-XXXXXXXX służący do identyfikacji właściciela licencji oraz do aktywowania licencji.

- Po wybraniu opcji Użyj kontaESET HOME wyświetlona zostanie prośba o zalogowanie się na konto ESET HOME.

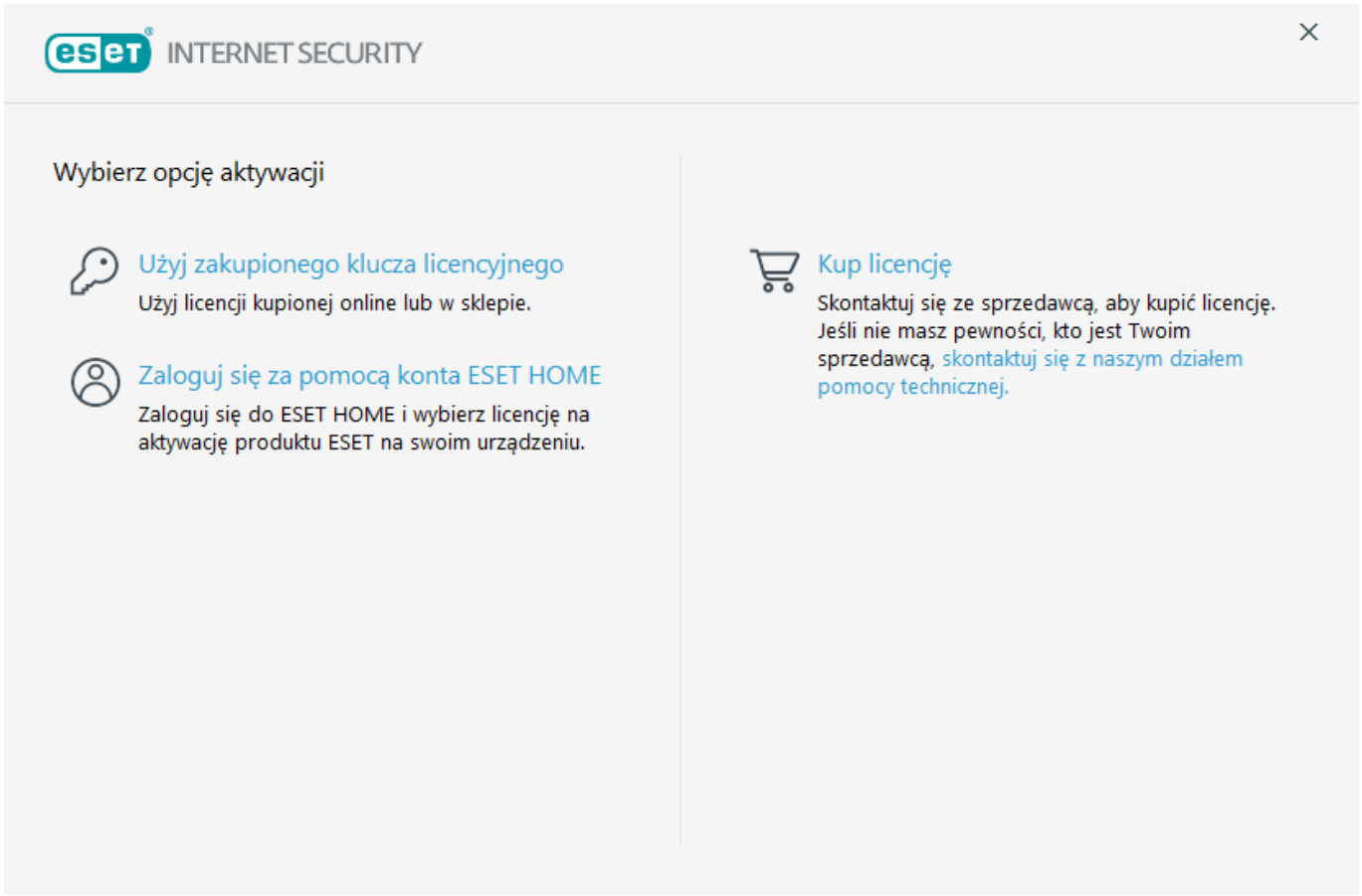
- Aby wypróbować program ESET Internet Security przed jego kupnem, wybierz opcję Darmowa wersja próbna. Wprowadź swój adres e-mail i nazwę kraju, aby aktywować program ESET Internet Security na okres próbny. Dane swojej licencji próbnej otrzymasz w wiadomości e-mail. Każdy klient może aktywować licencję tymczasową tylko raz.

- Jeśli nie masz licencji i chcesz ją nabyć, kliknij opcję **Kup licencję**. Spowoduje to przekierowanie do witryny lokalnego dystrybutora firmy ESET. Pełne licencje na produkty ESET do systemu Windows przeznaczone dla użytkowników domowych nie są bezpłatne.

Licencję produktu można zmienić w dowolnej chwili. W tym celu w głównym oknie programu należy kliknąć kolejno opcje **Pomoc i obsługa** > **Zmień licencję**. Zostanie wyświetlony identyfikator licencji publicznej używany do identyfikowania licencji przez dział pomocy technicznej firmy ESET.

Jeśli znane są nazwa użytkownika i hasło użyte podczas aktywacji starszych produktów ESET, ale nie wiadomo, w jaki sposób aktywować program ESET Internet Security, należy przekonwertować starsze poświadczenia na klucz licencyjny.

Aktywacja produktu nie powiodła się?



Wprowadzanie klucza licencyjnego podczas aktywacji

Aktualizacje automatyczne są ważnym elementem zabezpieczeń. Program ESET Internet Security będzie pobierać aktualizacje dopiero po aktywowaniu.

Należy dokładnie wprowadzić **klucz licencyjny**:

- Klucz licencyjny to niepowtarzalny ciąg znaków w formacie XXXX-XXXX-XXXX-XXXX-XXXX służący do identyfikacji właściciela licencji oraz do aktywowania licencji.

Aby zapewnić dokładność, zalecamy skopiowanie klucza licencyjnego z wiadomości e-mail dotyczącej rejestracji i wklejenie go.

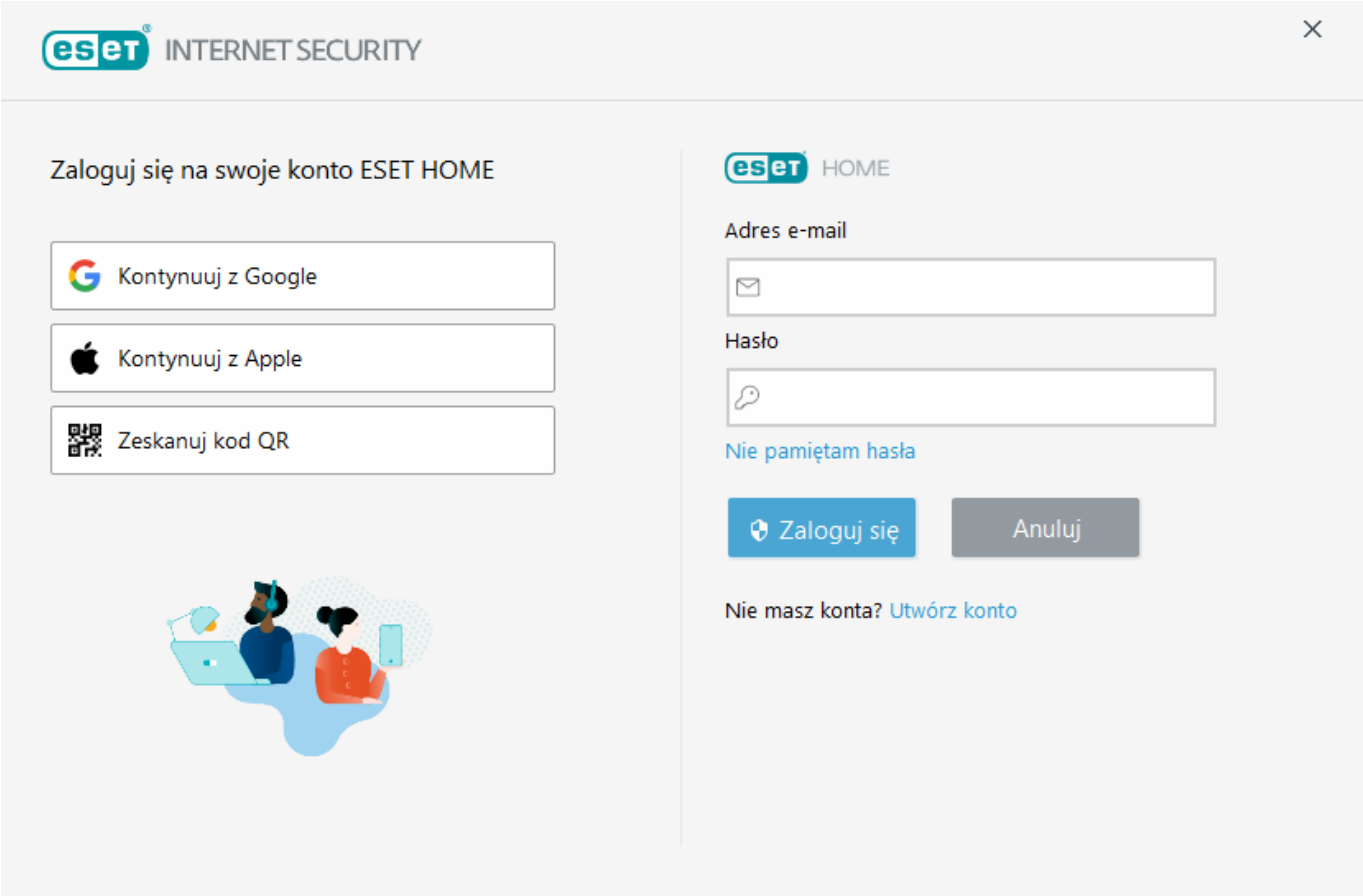
Jeśli klucz licencyjny nie został wprowadzony po zainstalowaniu programu, produkt nie zostanie aktywowany. Możesz aktywować produkt ESET Internet Security w głównym oknie programu > **Pomoc i wsparcie** > **Aktywuj licencję**.

Pełne licencje na produkty ESET do systemu Windows przeznaczone dla użytkowników domowych nie są bezpłatne.

Konta użytkowników ESET HOME

Połącz urządzenie z portalem ESET HOME, aby przeglądać wszystkie aktywowane licencje ESET i połączone urządzenia oraz zarządzać nimi. Za pośrednictwem portalu można odnawiać, uaktualniać lub rozszerzać licencje i wyświetlać ważne szczegóły licencji. W portalu zarządzania ESET HOME lub aplikacji mobilnej można konfigurować ustawienia funkcji Anti-Theft, dodawać różne licencje, pobierać produkty na urządzenia, sprawdzać

stan zabezpieczeń produktu lub udostępniać licencje za pośrednictwem poczty e-mail. Aby uzyskać więcej informacji, odwiedź witrynę pomocy online ESET HOME.



Po wybraniu opcji **Użyj konta ESET HOME** jako metody aktywacji lub podczas łączenia się z kontem ESET HOME podczas instalacji:

1. Zaloguj się na swoje konto ESET HOME.

> Jeśli nie posiadasz konta ESET HOME, kliknij **Utwórz konto**, aby się zarejestrować, lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.
> Jeśli nie pamiętasz hasła, kliknij **Nie pamiętam hasła** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.

2. W polu **Nazwa urządzenia** wprowadź nazwę, która będzie używana we wszystkich usługach ESET HOME, a następnie kliknij **Kontynuuj**.

3. Wybierz licencję, którą chcesz aktywować, lub dodaj nową licencję. Kliknij **Kontynuuj**, aby aktywować produkt ESET Internet Security.

Aktywuj licencję testową

Aby aktywować wersje testową programu ESET Internet Security, wprowadź prawidłowy adres e-mail w polu **Adres e-mail** oraz **Potwierdź adres e-mail**. Po aktywacji na podany adres e-mail otrzymasz wiadomość z wygenerowaną licencją ESET. Ten adres e-mail będzie również używany do przesyłania przypomnień o wygaśnięciu licencji produktu i innych wiadomości od firmy ESET. Wersja testowa może być aktywowana wyłącznie raz.

Wybierz kraj z menu rozwijanego **Kraj**, aby zarejestrować swoją kopię programu ESET Internet Security u lokalnego dystrybutora, który świadczy pomoc techniczną.

Bezpłatny klucz licencyjny produktu ESET

Pełna licencja programu ESET Internet Security nie jest darmowa.

Klucz licencyjny produktu ESET to niepowtarzalna kombinacja liter i cyfr oddzielonych dywizem dostarczona przez firmę ESET na potrzeby legalnego użytkowania programu ESET Internet Security zgodnie z Umową licencyjną użytkownika końcowego. Każdy użytkownik końcowy ma prawo używać klucza licencyjnego tylko w zakresie swoich uprawnień do korzystania z programu ESET Internet Security uzależnionych od liczby licencji przyznanych przez firmę ESET. Klucz licencyjny jest uważany za poufny i nie można go udostępniać. Można jednak udostępniać stanowiska z licencją za pomocą portalu ESET HOME.

Pewne witryny w Internecie mogą oferować „darmowe” klucze licencyjne produktów ESET. Należy jednak pamiętać o następujących kwestiach:

- Kliknięcie reklamy „darmowej licencji na produkt ESET” może narazić komputer lub urządzenie na niebezpieczeństwo i prowadzić do infekcji szkodliwym oprogramowaniem. Szkodliwe oprogramowanie bywa ukryte w zawartości nieoficjalnych witryn witrynach (np. filmach), witrynach wyświetlających reklamy w celu zarabiania na odwiedzinach użytkowników itp. Zazwyczaj są to pułapki.
- Firma ESET ma prawo blokować i blokuje pirackie licencje.
- Posiadanie piracki klucza licencyjnego jest niezgodne z Umową licencyjną użytkownika końcowego, którą należy zaakceptować w celu instalacji programu ESET Internet Security.
- Licencje na produkty ESET należy kupować wyłącznie przez oficjalne kanały, takie jak witryna www.eset.com, dystrybutorzy lub sprzedawcy produktów ESET (nie należy kupować licencji w nieoficjalnych zewnętrznych witrynach, np. eBay, ani licencji współdzielonych od osób trzecich).
- Pobranie produktu ESET Internet Security jest bezpłatne, ale aktywacja podczas instalacji wymaga ważnego klucza licencyjnego produktu ESET (tj. produkt można pobrać i zainstalować, ale bez aktywacji nie będzie on działać).
- Nie należy udostępniać licencji w Internecie ani mediach społecznościowych (może ona zostać rozpowszechniona).

Instrukcje dotyczące rozpoznawania i zgłaszania pirackiej licencji na produkt ESET zawiera artykuł w bazie wiedzy.

Jeśli masz wątpliwości co do zakupu produktu zabezpieczającego ESET, możesz skorzystać z wersji próbnej, która pomoże Ci podjąć decyzję:

1. Aktywuj program ESET Internet Security za pomocą bezpłatnej licencji próbnej
2. Przystąp do programu Beta firmy ESET
3. Jeśli używasz urządzenia mobilnego z systemem Android, zainstaluj aplikację freemium ESET Mobile Security.

Aby uzyskać zniżkę/przedłużyć licencję:

- Poleć program ESET Internet Security znajomemu
- Odnów licencję na produkt ESET (jeśli masz licencję, która wygasła) lub aktywuj ją na dłuższy okres

Aktywacja nie powiodła się — typowe scenariusze

Jeśli aktywacja ESET Internet Security nie powiedzie się, najbardziej typowe scenariusze to:

- Klucz licencyjny jest już używany
- Nieprawidłowy klucz licencyjny. Błąd w formularzu aktywacji produktu
- Brakujące lub nieprawidłowe informacje dodatkowe potrzebne do aktywacji.
- Nawiązanie komunikacji z bazą danych aktywacji nie powiodło się. Za 15 minut należy podjąć ponowną próbę aktywacji.
- Brak połączenia z serwerami aktywacji ESET lub jest ono wyłączone

Sprawdź, czy wprowadzony został odpowiedni klucz licencyjny, i spróbuj go ponownie aktywować. Jeśli do aktywacji używasz konta ESET HOME, zobacz Zarządzanie licencjami ESET HOME — Pomoc online.

Jeśli nadal nie można aktywować programu, Narzędzie do rozwiązywania problemów z aktywacją programu ESET przeprowadzi Cię przez typowe pytania, błędy i problemy dotyczące aktywacji i licencjonowania (dostępne w języku angielskim i kilku innych językach).

Aktywacja nie powiodła się z powodu nadużycia licencji

Problem

- Twoja licencja może być nadużywana lub nieprawidłowo wykorzystywana
- Aktywacja nie powiodła się z powodu nadużycia licencji

Rozwiązanie

Istnieje więcej urządzeń korzystających z licencji, niż pozwala na to Twoja licencja. Możesz być ofiarą piractwa komputerowego lub podrabiania. Tej licencji nie można używać do aktywacji innych produktów firmy ESET. Możesz od razu rozwiązać ten problem, jeśli masz uprawnienia do zarządzania licencją na koncie ESET HOME lub jeśli licencję kupiono z legalnego źródła. Jeśli nie masz konta, utwórz je.

Jeśli jesteś właścicielem licencji i system nie wyświetlił monitu o podanie adresu e-mail:

1. Aby zarządzać licencją ESET, otwórz przeglądarkę internetową i przejdź do strony https://home.eset.com. Przejdź do obszaru ESET License Manager, a następnie usuń lub dezaktywuj stanowiska. Aby uzyskać więcej informacji, zobacz Co zrobić w przypadku nadużycia licencji.

2. Instrukcje dotyczące rozpoznawania i zgłaszania pirackiej licencji na produkt ESET zawiera nasz artykuł.

3. W przypadku wątpliwości należy kliknąć **Wstecz** i napisać wiadomość e-mail do działu pomocy technicznej firmy ESET.

Jeśli nie jesteś właścicielem licencji, skontaktuj się z właścicielem licencji i poinformuj go o tym, że nie możesz aktywować produktu ESET ze względu na użycie licencji na zbyt wielu urządzeniach. Właściciel może rozwiązać ten problem z poziomu portalu ESET HOME.

Jeśli zostanie wyświetlony monit o potwierdzenie adresu e-mail (ma to miejsce w nielicznych przypadkach), podaj adres e-mail, który został użyty do zakupu lub aktywowania programu ESET Internet Security.

Uaktualnienie licencji

To okno powiadomienia pojawia się w sytuacji, gdy licencja aktywacyjna Twojego produktu ESET została zmieniona. Nowa licencja pozwala aktywować produkt z większą liczbą funkcji zabezpieczeń. W przypadku niewprowadzenia zmian ESET Internet Security jednorazowo wyświetli okno z komunikatem **Zmień na produkt z większą ilością funkcji zabezpieczeń**.

Tak (zalecane) – automatycznie zainstaluje produkt z większą liczbą funkcji zabezpieczeń.

Nie, dzięki – żadne zmiany nie zostaną wprowadzone, a powiadomienie zniknie na stałe.

Aby później zmienić produkt, zapoznaj się z artykułem bazy wiedzy firmy ESET. Więcej informacji na temat licencji ESET można znaleźć w artykule Licencjonowanie — często zadawane pytania.

W poniższej tabeli wyszczególniono funkcje dostępne w poszczególnych produktach.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Silnik detekcji	✔	✔	✔
Zaawansowane uczenie maszynowe	✔	✔	✔
Blokada programów typu Exploit	✔	✔	✔
Ochrona przed atakami skryptowymi	✔	✔	✔
Ochrona przed atakami typu „phishing”	✔	✔	✔
Ochrona dostępu do stron internetowych	✔	✔	✔
HIPS (w tym ochrona przed oprogramowaniem wymuszającym okup)	✔	✔	✔
Ochrona przed spamem		✔	✔
Zapora		✔	✔
Inspekcja sieci		✔	✔
Ochrona kamery internetowej		✔	✔
Ochrona przed atakami z sieci		✔	✔
Ochrona przed botnetami		✔	✔
Ochrona bankowości internetowej		✔	✔
Kontrola rodzicielska		✔	✔
Anti-Theft		✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Aktualizacja produktu

Pobrałeś instalatora domyślnego i zdecydowałeś się zmienić produkt, który ma zostać aktywowany, lub chcesz zmienić zainstalowany produkt na taki z większą liczbą funkcji zabezpieczeń.

Zmień produkt podczas instalacji.

W poniższej tabeli wyszczególniono funkcje dostępne w poszczególnych produktach.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Silnik detekcji	✔	✔	✔
Zaawansowane uczenie maszynowe	✔	✔	✔
Blokada programów typu Exploit	✔	✔	✔
Ochrona przed atakami skryptowymi	✔	✔	✔
Ochrona przed atakami typu „phishing”	✔	✔	✔
Ochrona dostępu do stron internetowych	✔	✔	✔
HIPS (w tym ochrona przed oprogramowaniem wymuszającym okup)	✔	✔	✔
Ochrona przed spamem		✔	✔
Zapora		✔	✔
Inspekcja sieci		✔	✔
Ochrona kamery internetowej		✔	✔
Ochrona przed atakami z sieci		✔	✔
Ochrona przed botnetami		✔	✔
Ochrona bankowości internetowej		✔	✔
Kontrola rodzicielska		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Starsza wersja licencji

To okno dialogowe pojawia się w sytuacji, gdy licencja użyta do aktywacji produktu ESET została zmieniona. Zmienionej licencji można używać tylko z innymi produktami firmy ESET z mniejszą liczbą funkcji zabezpieczeń. Produkt został automatycznie zmieniony, aby zapobiec utracie ochrony.

Więcej informacji na temat licencji ESET można znaleźć w artykule Licencjonowanie — często zadawane pytania.

W poniższej tabeli wyszczególniono funkcje dostępne w poszczególnych produktach.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Silnik detekcji	✔	✔	✔
Zaawansowane uczenie maszynowe	✔	✔	✔
Blokada programów typu Exploit	✔	✔	✔
Ochrona przed atakami skryptowymi	✔	✔	✔
Ochrona przed atakami typu „phishing”	✔	✔	✔
Ochrona dostępu do stron internetowych	✔	✔	✔
HIPS (w tym ochrona przed oprogramowaniem wymuszającym okup)	✔	✔	✔
Ochrona przed spamem		✔	✔
Zapora		✔	✔
Inspekcja sieci		✔	✔
Ochrona kamery internetowej		✔	✔
Ochrona przed atakami z sieci		✔	✔
Ochrona przed botnetami		✔	✔
Ochrona bankowości internetowej		✔	✔
Kontrola rodzicielska		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Starsza wersja produktu

Obecnie wykorzystywany produkt posiada więcej funkcjonalności niż ten, który zamierzasz aktywować. Utracisz ochronę przed kradzieżą i dostęp do powiązanych danych przechowywanych na portalu ESET HOME.

W poniższej tabeli wyszczególniono funkcje dostępne w poszczególnych produktach.

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium
Silnik detekcji	✔	✔	✔
Zaawansowane uczenie maszynowe	✔	✔	✔
Blokada programów typu Exploit	✔	✔	✔
Ochrona przed atakami skryptowymi	✔	✔	✔
Ochrona przed atakami typu „phishing”	✔	✔	✔
Ochrona dostępu do stron internetowych	✔	✔	✔
HIPS (w tym ochrona przed oprogramowaniem wymuszającym okup)	✔	✔	✔
Ochrona przed spamem		✔	✔
Zapora		✔	✔
Inspekcja sieci		✔	✔
Ochrona kamery internetowej		✔	✔
Ochrona przed atakami z sieci		✔	✔
Ochrona przed botnetami		✔	✔
Ochrona bankowości internetowej		✔	✔
Kontrola rodzicielska		✔	✔
Anti-Theft		✔	✔
Password Manager			✔
ESET Secure Data			✔
ESET LiveGuard			✔

Narzędzie do rozwiązywania problemów z instalacją

Jeśli podczas instalacji wystąpią problemy, Kreator instalacji udostępnia narzędzie do rozwiązywania problemów, które w miarę możliwości rozwiąże problem.

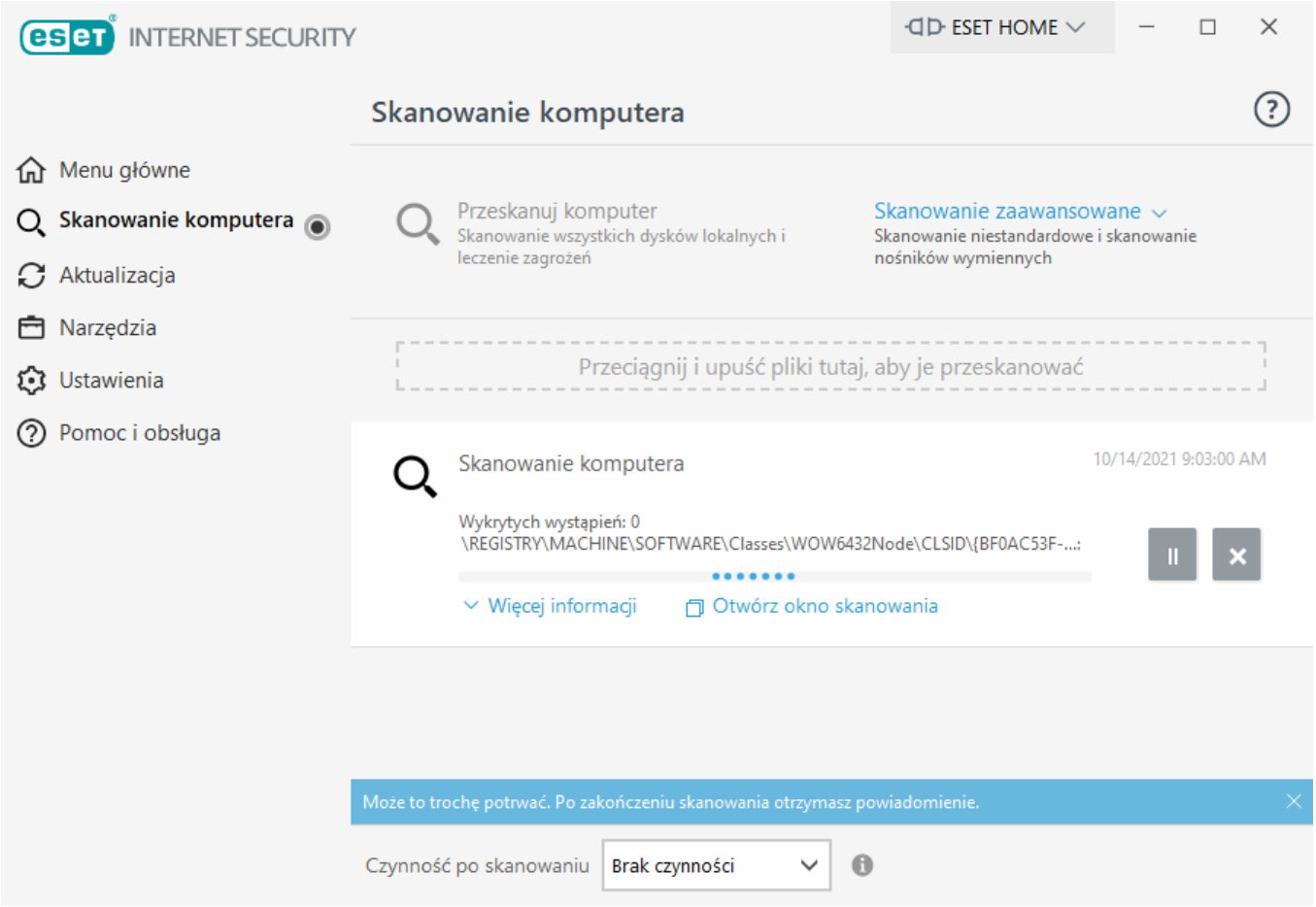
Aby uruchomić narzędzie, kliknij przycisk **Uruchom narzędzie do rozwiązywania problemów**. Po zakończeniu pracy narzędzia do rozwiązywania problemów postępuj zgodnie z zalecanym rozwiązaniem.

Jeśli problem będzie się powtarzał, zobacz listę typowych błędów instalacji i rozwiązań.

Pierwsze skanowanie po instalacji

Po zainstalowaniu programu ESET Internet Security po pierwszej pomyślnej aktualizacji rozpocznie się skanowanie komputera pod kątem obecności kodu szkodliwego oprogramowania.

Skanowanie komputera można też uruchomić ręcznie w oknie głównym programu, klikając **Skanowanie komputera** > **Skanowanie komputera**. Więcej informacji na temat skanowania komputera można znaleźć w rozdziale Skanowanie komputera.



Uaktualnianie do nowszej wersji

Nowsze wersje programu ESET Internet 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 powodować poważne konsekwencje na komputerach o określonych konfiguracjach, 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.
Należy się upewnić, że włączono opcję **Aktualizacji funkcji aplikacji** w obszarze **Ustawienia zaawansowane** (F5) > **Aktualizacja** > **Profile** > **Aktualizacje**.

2. Ręcznie przez kliknięcie w głównym oknie programu pozycji **Sprawdź dostępne aktualizacje** w sekcji **Aktualizacja**.

3. Ręcznie przez pobranie i zainstalowanie nowszej wersji już zainstalowanego programu.

Dodatkowe informacje i ilustrowane instrukcje znajdziesz w następujących artykułach:

- Aktualizacja produktów ESET — sprawdź najnowsze moduły produktów
- Jakie są typy aktualizacji i wersji produktów ESET?

Automatyczne uaktualnianie starszej wersji produktu

Zainstalowana wcześniej wersja produktu ESET nie jest już obsługiwana, dlatego produkt został uaktualniony do najnowszej wersji.

Typowe problemy z instalacją

Każda nowa wersja produktów ESET zawiera wiele poprawek i ulepszeń. Obecni klienci posiadający ważną licencję na produkt ESET mogą bezpłatnie przeprowadzić uaktualnienie do najnowszej wersji tego samego produktu.

Aby zakończyć instalację:

1. Kliknij przycisk **Zaakceptuj i kontynuuj**, aby zaakceptować postanowienia Umowy licencyjnej użytkownika końcowego i Polityki prywatności. Jeśli nie zgadzasz się z postanowieniami Umowy licencyjnej użytkownika końcowego, kliknij przycisk **Odinstaluj**. Nie można przywrócić poprzedniej wersji.

2. Kliknij pozycję **Zezwalaj na wszystko i kontynuuj**, aby zezwolić na korzystanie z systemu informacji zwrotnych ESET LiveGrid® i uczestnictwo w Programie poprawy jakości doświadczeń użytkowników, lub kliknij pozycję **Kontynuuj**, jeśli nie chcesz uczestniczyć w tych inicjatywach.

3. Po aktywowaniu nowego produktu ESET przy użyciu klucza licencyjnego zostanie wyświetlona strona główna. Jeśli informacje o licencji nie zostaną znalezione, będziesz korzystać z nowej licencji próbnej. Jeśli licencja użyta w poprzednim produkcie jest nieważna, aktywuj produkt ESET.

4. Do ukończenia instalacji wymagane jest ponowne uruchomienie urządzenia.

Polecanie produktu firmy ESET znajomym

W tej wersji produktu ESET Internet Security firma ESET oferuje korzyści za polecenie go rodzinie i znajomym. Polecać można nawet produkt aktywowany przy użyciu licencji na wersję próbną. Jeżeli jesteś użytkownikiem wersji próbnej, za każde skuteczne polecenie, które będzie skutkować aktywacją produktu, zarówno Ty, jak i znajomy otrzymacie dodatkowy okres licencji próbnej.

Polecać produkt można przy użyciu zainstalowanego programu ESET Internet Security. Możliwość polecania produktu zależy od programu, z którego się go poleca. Więcej informacji zawiera tabela poniżej.

Zainstalowany produkt	Produkt, który można polecić
ESET NOD32 Antivirus	ESET Internet Security
ESET Internet Security	ESET Internet Security
ESET Smart Security Premium	ESET Smart Security Premium

Polecanie produktu

Aby wysłać łącze polecające, kliknij pozycję **Poleć znajomemu** w menu głównym produktu ESET Internet Security. Kliknij pozycję **Poleć za pomocą łącza polecającego**. Produkt wygeneruje łącze polecające, które zostanie wyświetlone w nowym oknie. Skopiuj łącze i wyślij je rodzinie oraz znajomym. Łącze polecające można udostępnić na kilka sposobów bezpośrednio z produktu ESET: przy użyciu opcji **Udostępnij na Facebooku**, **Poleć kontaktom z**

Gmaila i **Udostępnij na Twitterze**.

Kiedy znajomy kliknie wysłane mu łącze polecające, zostanie przekierowany do strony internetowej, z której może pobrać produkt, i będzie mógł korzystać z BEZPŁATNEJ ochrony przez dodatkowy miesiąc. Jako użytkownik wersji próbnej otrzymasz powiadomienie o każdej aktywacji w wyniku przesłania przez Ciebie łącza polecającego, a Twoja licencja zostanie automatycznie przedłużona o miesiąc BEZPŁATNEJ ochrony. W ten sposób możesz wydłużyć bezpłatną ochronę o nawet 5 miesięcy. Liczbę aktywowanych łączy polecających możesz sprawdzić w oknie **Poleć znajomemu** w produkcie firmy ESET.

Funkcja polecania może być niedostępna w danym języku / regionie.

Produkt ESET Internet Security zostanie zainstalowany

Wyświetlić się może następujące okno dialogowe:

- Podczas procesu instalacji — kliknij przycisk **Kontynuuj**, aby zainstalować produkt ESET Internet Security.
- Podczas zmiany licencji w ESET Internet Security — kliknij przycisk **Aktywuj**, aby zmienić licencję i aktywować ESET Internet Security.

Opcja **Zmień produkt** znajdująca się na dole umożliwia przełączanie między różnymi produktami ESET do systemu Windows przeznaczonymi dla użytkowników domowych — zgodnie z posiadaną licencją ESET. Więcej informacji można znaleźć w sekcji Który produkt posiadam?.

Zmień na inną linię produktów

Zgodnie z licencją ESET, istnieje możliwość przełączania między różnymi produktami ESET do systemu Windows przeznaczonymi dla użytkowników domowych. Więcej informacji można znaleźć w sekcji Który produkt posiadam?.

Rejestracja

Zarejestruj swoją licencję, wypełniając pola zawarte w formularzu rejestracyjnym i klikając przycisk Aktywuj. Wypełnienie pól zaznaczonych w nawiasach jako wymagane jest obowiązkowe. Te informacje będą wykorzystywane wyłącznie w sprawach związanych z licencją ESET.

Postęp aktywacji

Trzeba poczekać kilka sekund na zakończenie procesu aktywacji (wymagany czas może zależeć od szybkości połączenia internetowego lub komputera).

Aktywacja zakończona pomyślnie

Proces aktywacji został zakończony. Wykonaj instrukcje w kreatorze konfiguracji po instalacji, aby zakończyć konfigurowanie programu ESET Internet Security.

Aktualizacja modułu rozpocznie się za kilka sekund. Regularne aktualizacje ESET Internet Security rozpoczną się natychmiast.

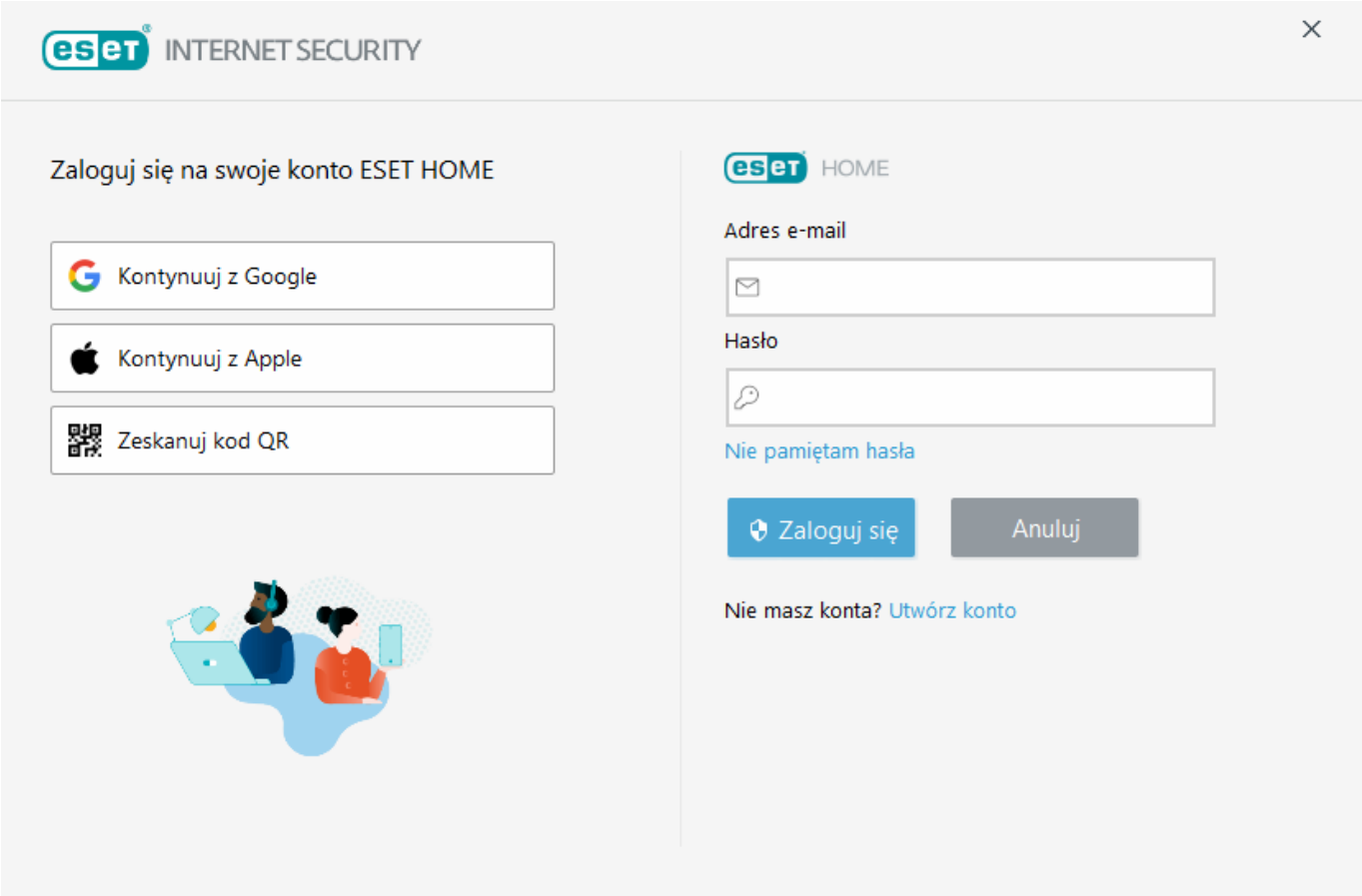
Skanowanie wstępne rozpocznie się automatycznie w ciągu 20 minut po aktualizacji modułu.

Przewodnik dla początkujących

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

Połącz z ESET HOME

Połącz urządzenie z portalem ESET HOME, aby przeglądać wszystkie aktywowane licencje ESET i połączone urządzenia oraz zarządzać nimi. Za pośrednictwem portalu można odnawiać, uaktualniać lub rozszerzać licencje i wyświetlać ważne szczegóły licencji. W portalu zarządzania ESET HOME lub aplikacji mobilnej można konfigurować ustawienia funkcji Anti-Theft, dodawać różne licencje, pobierać produkty na urządzenia, sprawdzać stan zabezpieczeń produktu lub udostępniać licencje za pośrednictwem poczty e-mail. Aby uzyskać więcej informacji, odwiedź witrynę pomocy online ESET HOME.



Połącz urządzenie z rozwiązaniem ESET HOME:

Jeśli łączysz się z ESET HOME podczas instalacji lub wybierasz opcję **Użyj konta ESET HOME** jako metody aktywacji, stosuje się do instrukcji w temacie Użyj kontaESET HOME.
Jeśli masz już zainstalowaną aplikację ESET Internet Security i aktywowaną licencję na swoim koncie ESET HOME, możesz połączyć swoje urządzenie z kontem ESET HOME w portalu ESET HOME. Postępuj zgodnie z instrukcjami w ESET HOME Przewodniku pomocy online i zezwól na połączenie w programie ESET Internet Security.

1. W głównym oknie programu kliknij **ESET HOME** > **Połącz z ESET HOME** lub kliknij **Połącz z ESET HOME** w obszarze powiadomienia **Połącz to urządzenie z kontem ESET HOME**.

2. Zaloguj się na swoje konto ESET HOME.

> Jeśli nie posiadasz konta ESET HOME, kliknij **Utwórz konto**, aby się zarejestrować, lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.
> Jeśli nie pamiętasz hasła, kliknij **Nie pamiętam hasła** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.

3. Wprowadź nazwę w polu **Nazwa urządzenia** i kliknij **Kontynuuj**.

4. Po nawiązaniu połączenia zostanie wyświetlone okno zawierające dodatkowe informacje. Kliknij **Gotowe**.

Logowanie do konta ESET HOME

Dostępnych jest kilka metod logowania się na konto ESET HOME:

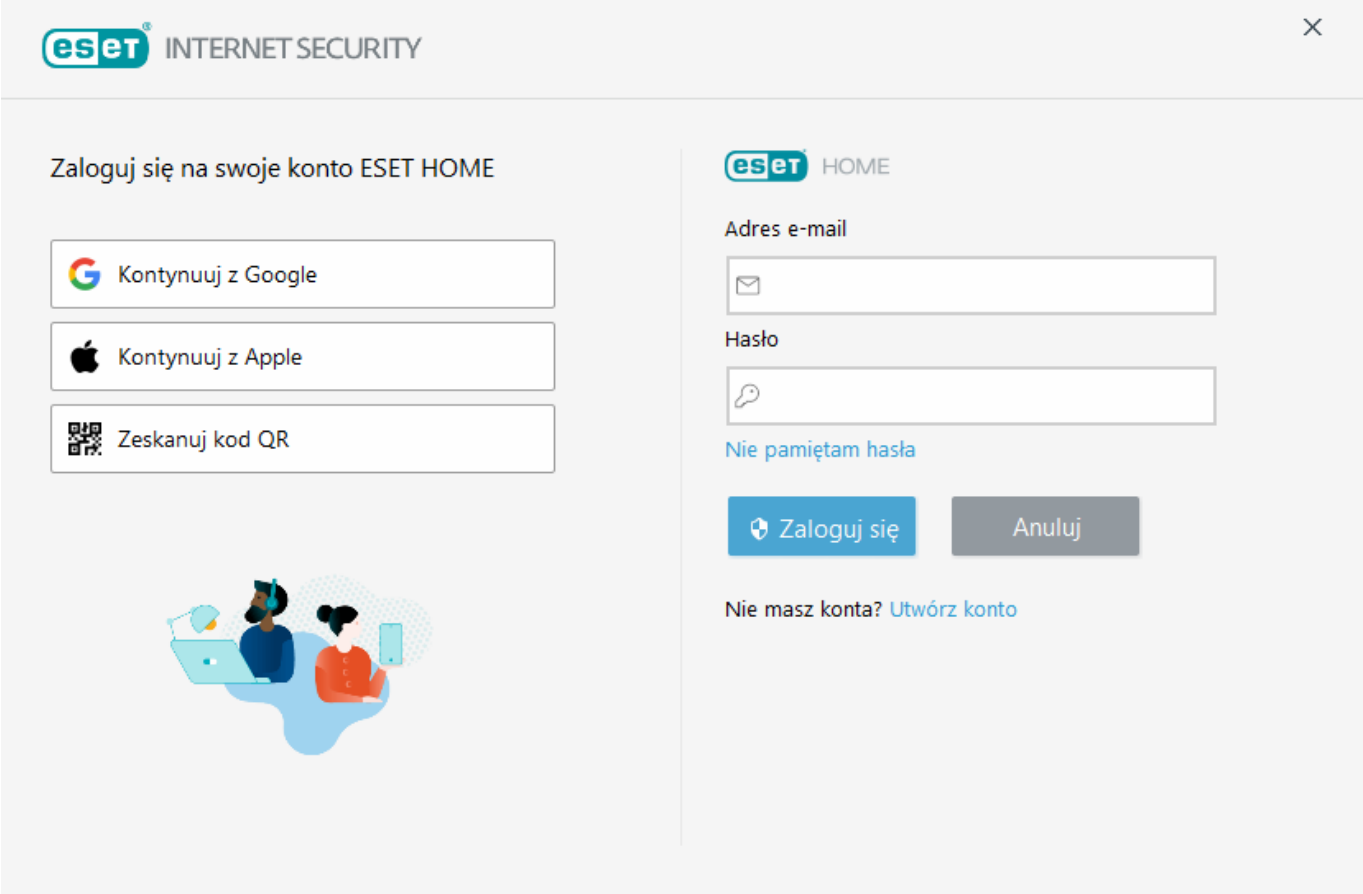
- **Użyj swojego adresu e-mail i hasła ESET HOME** — wpisz **adres e-mail** i **hasło** użyte do utworzenia konta ESET HOME, a następnie kliknij przycisk **Zaloguj się**.

- **Użyj swojego konta Google /AppleID** – kliknij **Kontynuuj za pomocą konta Google** lub **Kontynuuj przy użyciu Apple** i zaloguj się na odpowiednie konto. Po pomyślnym zalogowaniu zostaniesz przekierowany na stronę internetową potwierdzenia ESET HOME. Aby kontynuować, przejdź z powrotem do okna produktu ESET. Aby uzyskać więcej informacji na temat konta Google /loginu AppleID, zapoznaj się z instrukcjami na stronie pomocy online ESET HOME.

- **Zeskanuj kod QR —** kliknij opcję **Skanuj kod QR**, aby wyświetlić kod QR. Otwórz aplikację mobilną ESET HOME i zeskanuj kod QR lub skieruj aparat urządzenia na kod QR. Aby uzyskać więcej informacji, zobacz instrukcje w Pomocy online ESET HOME.

> Jeśli nie posiadasz konta ESET HOME, kliknij **Utwórz konto**, aby się zarejestrować, lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.
> Jeśli nie pamiętasz hasła, kliknij **Nie pamiętam hasła** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.

Logowanie nie powiodło się — częste błędy.



Logowanie nie powiodło się — częste błędy

Nie możemy znaleźć konta pasującego do wprowadzonego adresu e-mail

Wprowadzony adres e-mail nie są zgodne z żadnym kontem ESET HOME. Kliknij przycisk **Wstecz** i wpisz poprawny adres e-mail oraz hasło.

Aby się zalogować, musisz utworzyć konto ESET HOME. Jeśli nie masz kontaESET HOME, kliknij **Wstecz** > **Utwórz konto** lub zobacz artykuł Tworzenie nowego konta ESET HOME.

Nazwa użytkownika i hasło nie są zgodne ze sobą

Wprowadzone hasło nie jest zgodne z wprowadzonym adresem e-mail. Kliknij przycisk **Wstecz**, wpisz poprawne hasło i upewnij się, że wprowadzony adres e-mail jest poprawny. Jeśli nadal nie możesz się zalogować, kliknij opcję **Wstecz** > **Nie pamiętam hasła**, aby zresetować hasło, i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub zobacz Nie pamiętam hasła ESET HOME.

Wybrana opcja logowania nie pasuje do Twojego konta

Twoje konto jest powiązane z Kontem w mediach społecznościowych. Aby się zalogować do konta ESET HOME, kliknij **Kontynuuj za pomocą konta Google** lub **Kontynuuj za pomocą Apple** ID i zaloguj się na odpowiednie konto. Po pomyślnym zalogowaniu nastąpi przekierowanie na stronę internetową potwierdzenia ESET HOME. Możesz odłączyć swoje konto w mediach społecznościowych od swojego konta ESET HOME w portalu ESET HOME.

Nieprawidłowe hasło

Ten błąd może wystąpić, jeśli użytkownik produktu ESET Internet Security jest już połączony z ESET HOME i wprowadza zmiany, które wymagają zalogowania się (na przykład wyłączenie funkcji Anti-Theft), a wprowadzone hasło nie jest zgodne z kontem. Kliknij przycisk **Wstecz** i wpisz poprawne hasło. Jeśli nadal nie możesz się zalogować, kliknij opcję **Wstecz** > **Nie pamiętam hasła**, aby zresetować hasło, i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub zobacz Nie pamiętam hasła ESET HOME.

Dodaj urządzenie w ESET HOME

Jeśli masz już zainstalowaną aplikację ESET Internet Security i aktywowaną licencję na swoim koncie ESET HOME, możesz połączyć swoje urządzenie z kontem ESET HOME w portalu ESET HOME:

1. Wyślij żądanie połączenia do urządzenia.

2. ESET Internet Security wyświetla okno dialogowe **Połącz to urządzenie z kontem ESET HOME** z nazwą konta ESET HOME. Kliknij **Zezwól**, aby połączyć urządzenie ze wskazanym kontem ESET HOME.

i W przypadku braku interakcji żądanie połączenia zostanie automatycznie anulowane po około 30 minutach.

Główne okno programu

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

i **Ilustrowane instrukcje**
Patrz Otwieranie głównego okna programu produktów ESET dla systemu Windows, aby wyświetlić ilustrowane instrukcje dostępne w języku angielskim i kilku innych językach.

ESET HOME – Połącz urządzenie z rozwiązaniem ESET HOME. Użyj ESET HOME, aby wyświetlać i zarządzać następującymi elementami: ustawienia Anti-Theft oraz aktywowane licencje ESET i urządzenia, a także zarządzać nimi.

Poniżej opisano opcje dostępne w menu głównym:

Menu główne — przedstawia informacje o stanie ochrony zapewnianej przez program ESET Internet Security.

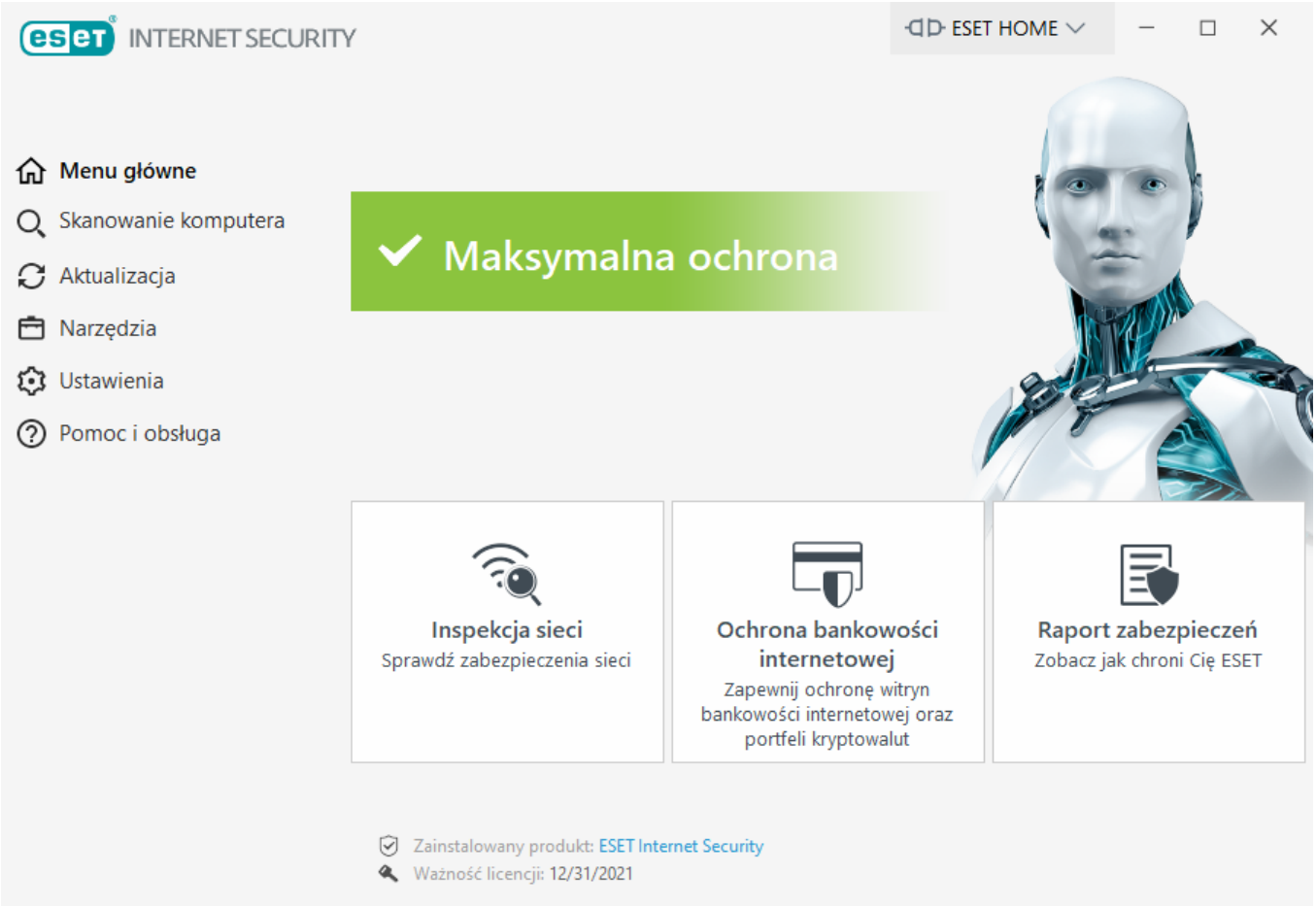
Skanowanie komputera — umożliwia skonfigurowanie i uruchomienie skanowania komputera oraz utworzenie skanowania niestandardowego.

Aktualizacja — wyświetla informacje o aktualizacjach silnika detekcji.

Narzędzia – zapewnia dostęp do modułów Inspekcja sieci, Ochrona bankowości internetowej, Anti-Theft i innych modułów, które upraszczają administrowanie programem i udostępniają dodatkowe opcje dla użytkowników zaawansowanych. Aby uzyskać więcej informacji, zobacz Narzędzia w programie ESET Internet Security.

Ustawienia — wybranie tej opcji umożliwia modyfikowanie poziomu zabezpieczeń komputera oraz dostępu do Internetu, ochrona sieci i narzędzia zabezpieczające.

Pomoc i obsługa — zapewnia dostęp do plików pomocy, bazy wiedzy firmy ESET, witryny internetowej firmy ESET i łączy umożliwiających przesłanie zgłoszenia do działu obsługi klienta.

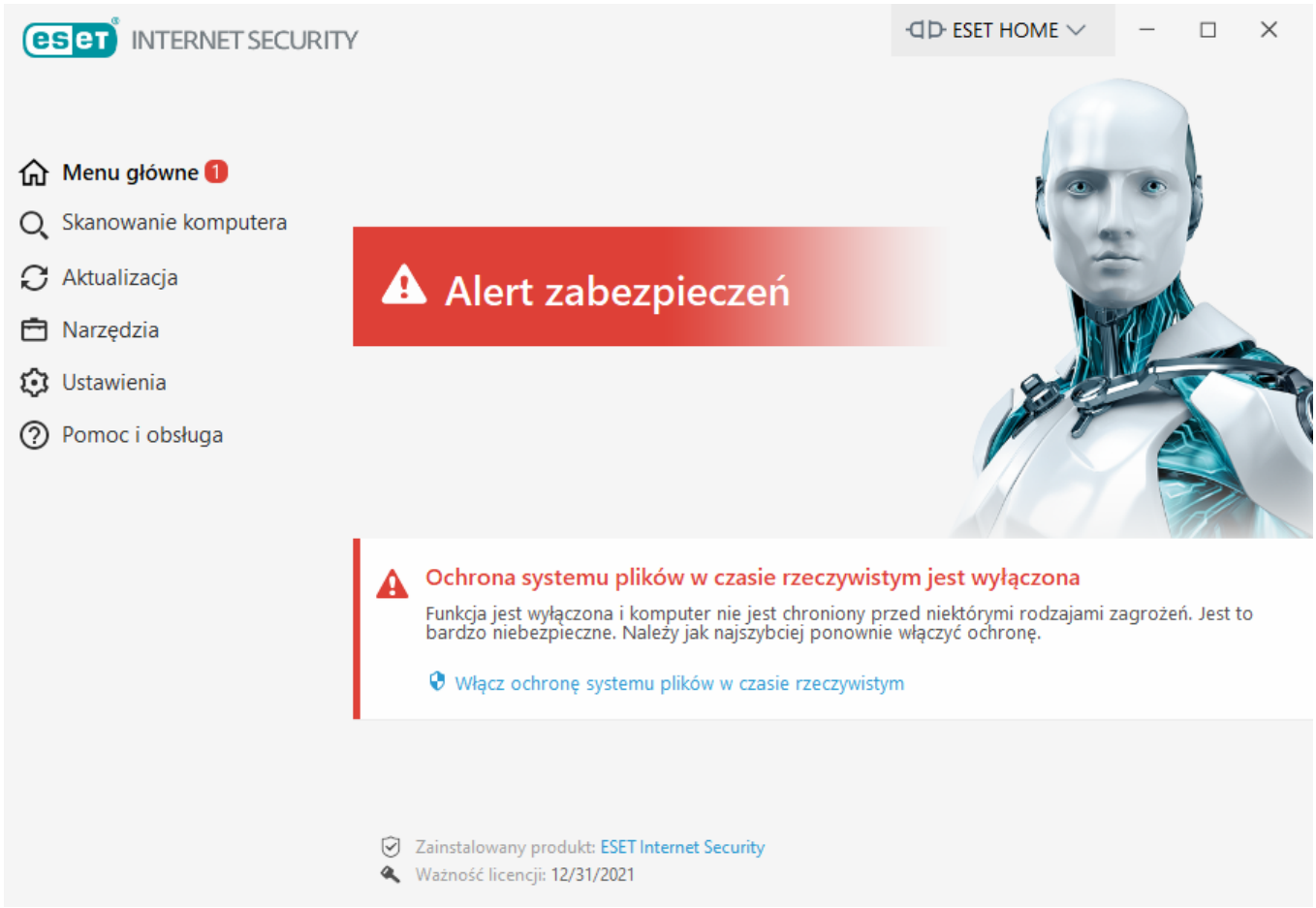


Ekran **Menu główne** zawiera ważne informacje na temat bieżącego poziomu ochrony komputera. W oknie stanu są również wyświetlane często używane funkcje programu ESET Internet Security. W tym miejscu można również znaleźć informacje na temat zainstalowanego produktu i datę wygaśnięcia licencji. Kliknij **ESET Internet Security**, jeśli chcesz zainstalować inną wersję produktu ESET. Więcej informacji o funkcjach poszczególnych produktów.

Zielona ikona oraz zielony stan **Ochrona aktywna** oznaczają maksymalny poziom bezpieczeństwa.

Postępowanie w przypadku, gdy program nie działa poprawnie?

Jeśli aktywny moduł ochrony działa poprawnie, jego ikona stanu ochrony jest zielona. Ikona czerwonego wykrzyknika lub pomarańczowego powiadomienia oznacza, że maksymalna ochrona nie jest zapewniona. Dodatkowe informacje o stanie ochrony każdego modułu oraz zalecane rozwiązania mające na celu przywrócenie pełnej ochrony będą wyświetlane w **Menu głównym**. Aby zmienić stan poszczególnych modułów, należy kliknąć opcję **Ustawienia**, a następnie wybrać moduł.



Czerwona ikona i czerwony status **Alertu zabezpieczeń** oznaczają problemy krytyczne. Istnieje kilka powodów wyświetlania tego stanu, na przykład:

- **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. Należy odnowić licencję zgodnie z instrukcjami podanymi w oknie alertu.
- **Silnik detekcji jest nieaktualny** — ten komunikat o błędzie jest wyświetlany po kilku nieudanych próbach aktualizacji silnika detekcji. Zaleca się sprawdzenie ustawień aktualizacji. Najczęstszym powodem wystąpienia tego błędu jest niewłaściwe wprowadzenie danych uwierzytelniających lub nieprawidłowe skonfigurowanie ustawień połączenia.
- **Ochrona systemu plików w czasie rzeczywistym jest wyłączona** — ochrona w czasie rzeczywistym została wyłączona przez użytkownika. Komputer nie jest chroniony przed zagrożeniami. Aby ponownie włączyć tę funkcję, należy kliknąć opcję **Włącz ochronę systemu plików w czasie rzeczywistym**.
- **Ochrona antywirusowa i antyspyware wyłączona**— można ponownie włączyć ochronę antywirusową i antyspyware, klikając opcję **Włącz ochronę antywirusową i antyspyware**.
- **Wyłączona zapora ESET** — ten problem jest także sygnalizowany czerwoną ikoną i powiadomieniem dotyczącym bezpieczeństwa obok elementu **Sieć**. Aby ponownie włączyć ochronę sieci, należy kliknąć opcję **Włącz zaporę**.

Pomarańczowa ikona oznacza ograniczoną ochronę. Na przykład istnieje problem z aktualizacją programu lub zbliża się data wygaśnięcia licencji.
Istnieje kilka powodów wyświetlania tego stanu, na przykład:

- **Ostrzeżenie optymalizacji Anti-Theft** — urządzenie nie jest zoptymalizowane do pracy z funkcją Anti-

Theft. Na przykład konto widmo (funkcja zabezpieczająca, która jest włączana automatycznie po oznaczeniu urządzenia jako utracone) może nie być utworzone na komputerze. Może wystąpić konieczność utworzenia konta widma z wykorzystaniem funkcji Optymalizacja w interfejsie sieciowym Anti-Theft.

- **Tryb gier jest aktywny**— włączenie trybu gier stanowi potencjalne zagrożenie dla bezpieczeństwa. Włączenie tej funkcji powoduje wyłączenie wszystkich wyskakujących okienek i zatrzymuje zaplanowane zadania.
- **Licencja wkrótce wygaśnie** — jest to sygnalizowane przez ikonę stanu ochrony przedstawiającą wykrzyknik obok zegara systemowego. Po wygaśnięciu licencji programu nie będzie można aktualizować, a kolor ikony stanu ochrony zmieni się na czerwony.

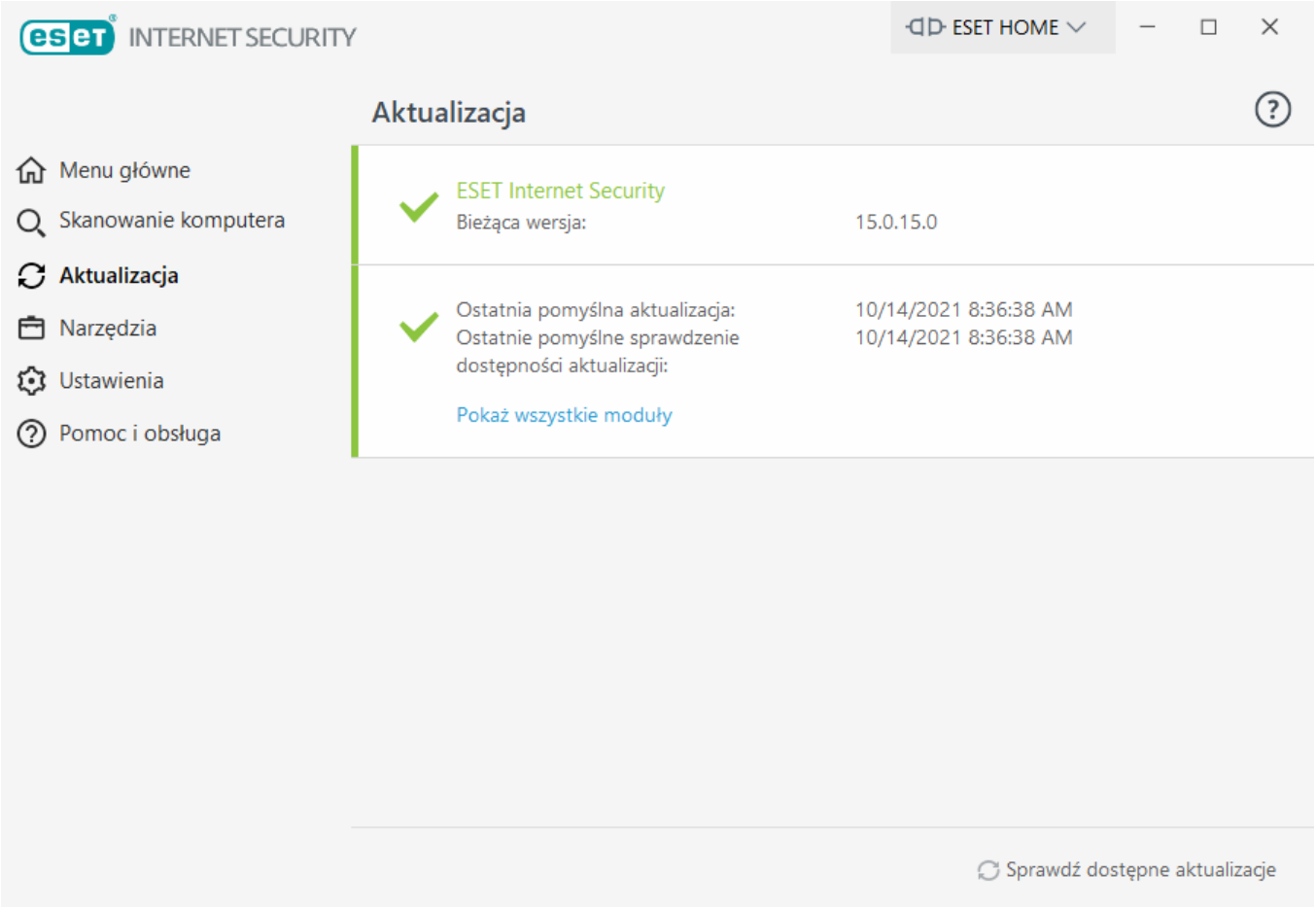
Jeśli nie uda się rozwiązać problemu przy użyciu proponowanych rozwiązań, kliknij opcję **Pomoc i obsługa**, aby uzyskać dostęp do plików pomocy lub przeszukać bazę wiedzy ESET. Jeśli nadal będzie potrzebna pomoc, możesz przesłać zgłoszenie do pomocy technicznej. Dział pomocy technicznej ESET niezwłocznie odpowie na otrzymane zgłoszenie i pomoże znaleźć rozwiązanie.

Aktualizacje

Regularne aktualizowanie programu ESET Internet Security to najlepszy sposób na zapewnienie najwyższego poziomu bezpieczeństwa komputera. Moduł aktualizacji zapewnia aktualność modułów programu i komponentów systemu.

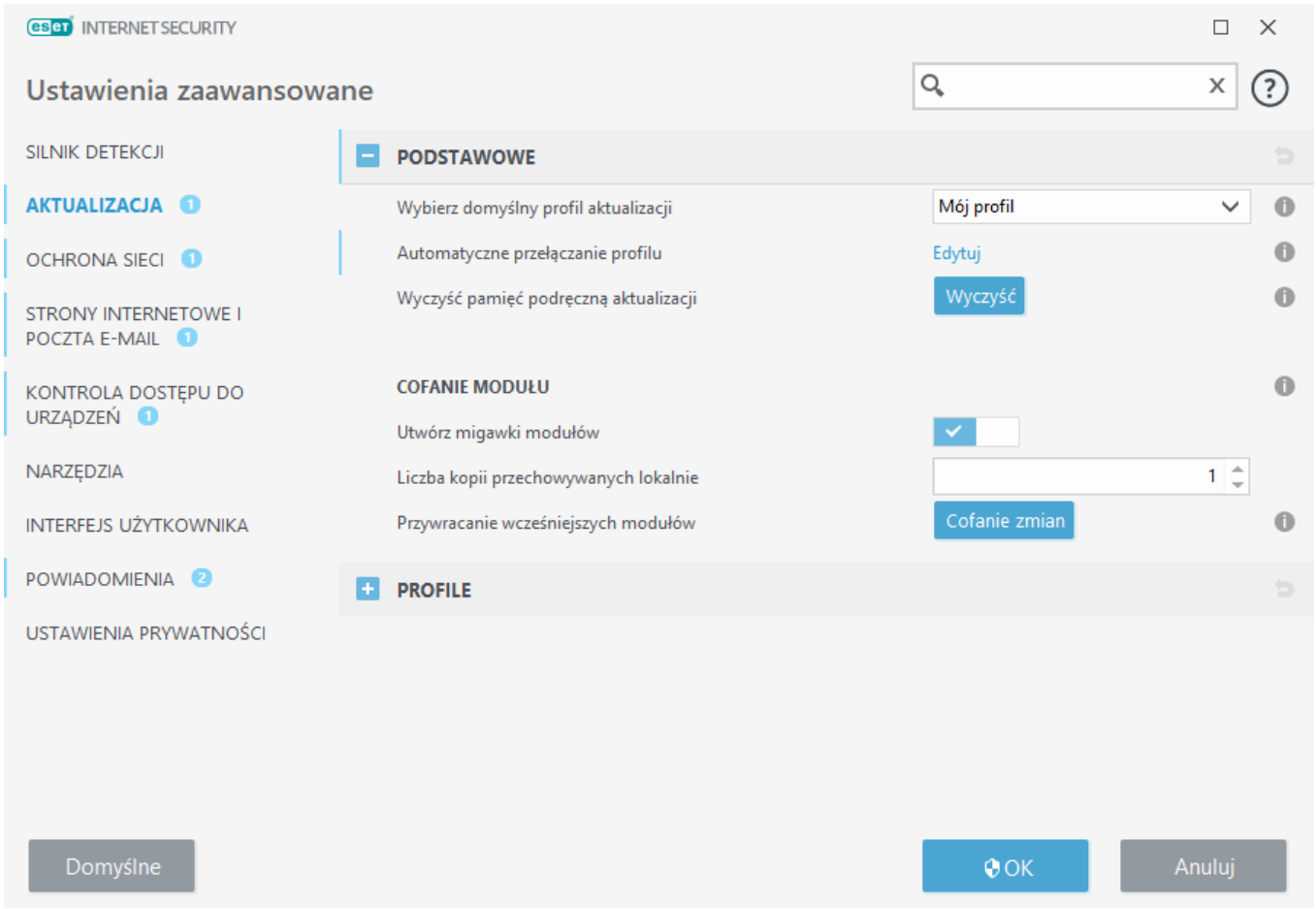
Klikając przycisk **Aktualizacja** w głównym oknie programu, można wyświetlić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację.

Oprócz aktualizacji automatycznych można kliknąć przycisk **Sprawdź aktualizacje**, aby przejść do ręcznej aktualizacji.



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 i połączenia z siecią LAN, kliknij pozycję **Aktualizacja** w drzewie ustawień zaawansowanych.

Jeśli wystąpią problemy podczas aktualizacji, należy kliknąć **Wyczyść** w celu wyczyszczenia tymczasowej pamięci podręcznej aktualizacji. Jeśli nadal nie będzie można zaktualizować modułów programu, patrz sekcja Rozwiązywanie problemów związanych z komunikatem „Aktualizacja modułów nie powiodła się”.



Konfigurowanie dodatkowych narzędzi zabezpieczających ESET

Przed rozpoczęciem korzystania z produktu ESET Internet Security możesz skonfigurować dodatkowe narzędzia zabezpieczające, aby zmaksymalizować ochronę:

- Kontrola rodzicielska
- Anti-Theft

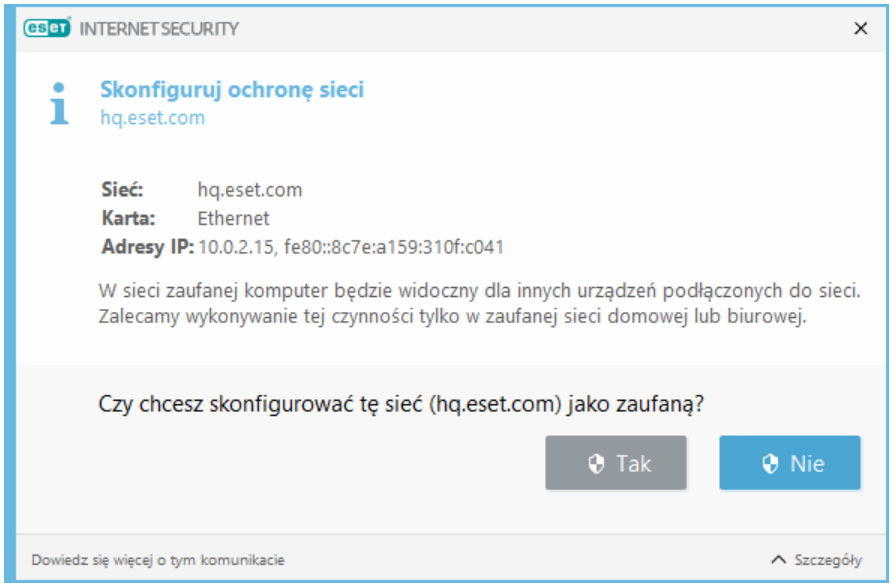
Więcej informacji na temat konfigurowania narzędzi zabezpieczających w produkcie ESET Internet Security można znaleźć w artykule w bazie wiedzy firmy ESET.

Skonfiguruj ochronę sieci

Niezbędna jest konfiguracja sieci połączonych z komputerem w celu jego ochrony. Możesz zezwolić innym użytkownikom na dostęp do komputera poprzez konfigurację strefy zaufanej, aby umożliwić udostępnianie. Kliknij **Menu** > **Ochrona sieci** > **Połączone sieci**, a następnie kliknij łącze znajdujące się pod połączoną siecią. Pojawi się wyskakujące okno zawierające opcje pozwalające na konfigurację wybranej sieci jako zaufanej.

Domyślnie ESET Internet Security używa ustawień systemu Windows po wykryciu nowej sieci. Aby wyświetlić okno dialogowe po wykryciu nowej sieci, zmień typ ochrony nowych sieci, aby zapytać użytkownika w sieciach znanych. Konfiguracja ochrony sieci przeprowadzana jest za każdym razem, gdy komputer łączy się z nową siecią.

W związku z tym zwykle nie ma potrzeby definiowania zaufanych stref.



Istnieją dwa tryby ochrony sieci, które można wybrać w oknie konfigurowania ochrony sieci:

- **Tak** — w przypadku sieci zaufanej (sieci domowej lub biurowej). Komputer i udostępnione pliki przechowywane na komputerze są widoczne dla innych użytkowników sieci, a zasoby systemowe są dostępne dla innych użytkowników w sieci. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do bezpiecznej sieci lokalnej.

- **Nie** — w przypadku sieci niezaufanej (sieci publicznej). Pliki i foldery w systemie nie są udostępniane innym użytkownikom w sieci ani nie są widoczne, a udostępnianie zasobów systemowych jest dezaktywowane. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do sieci bezprzewodowych.

Nieprawidłowa konfiguracja sieci może stwarzać zagrożenie dla bezpieczeństwa komputera.

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

Więcej informacji na temat tej funkcji zawiera poniższy artykuł z bazy wiedzy firmy ESET:

- Zmiana ustawień zapory połączenia sieciowego w produktach ESET do systemu Windows przeznaczonych dla użytkowników domowych

Włącz Anti-Theft

Urządzenia osobiste są ciągle narażone na zgubienie lub kradzież podczas naszych codziennych podróży z domu do pracy lub innych miejsc publicznych. Anti-Theft to funkcja, która zwiększa bezpieczeństwo na poziomie użytkownika w przypadku zgubienia lub kradzieży urządzenia. Anti-Theft umożliwi monitorowanie działań wykonywanych na urządzeniu oraz śledzenie brakującego urządzenia z wykorzystaniem lokalizacji na podstawie adresu w ESET HOME. Dzięki temu odzyskasz urządzenie i ochronisz swoje dane osobowe.

Dzięki zastosowaniu nowoczesnych technologii (np. wyszukiwania lokalizacji geograficznej adresu IP, rejestrowania zdjęć za pomocą kamery internetowej, ochrony kont użytkowników i monitorowania urządzenia)

funkcja Anti-Theft może pomóc zarówno właścicielowi, jak i organom ścigania w zlokalizowaniu komputera lub urządzenia w przypadku jego zgubienia lub kradzieży. W ESET HOME możesz zobaczyć, jaka aktywność jest wykonywana na komputerze lub urządzeniu.

Aby dowiedzieć się więcej na ten temat Anti-Theft w ESET HOME, zapoznaj się z ESET HOME Pomocą online.

Aby włączyć Anti-Theft i chronić urządzenie w przypadku zgubienia lub kradzieży, wybierz jedną z następujących opcji:

- Po zainstalowaniu produktu kliknij przycisk **Włącz Anti-Theft**, aby aktywować Anti-Theft.
- Jeśli na ekranie > **Menu główne** w głównym oknie programu pojawi się komunikat „Anti-Theft dostępne”, kliknij **Włącz Anti-Theft**.
- W głównym oknie programu kliknij pozycję **Narzędzia** > **Anti-Theft**.
- W głównym oknie programu kliknij pozycję **Ustawienia** > **Narzędzia zabezpieczające**. Kliknij ikonę suwaka przy pozycji **Anti-Theft** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Jeśli urządzenie nie jest podłączone do ESET HOME, musisz:
1. Zaloguj się na swoje konto ESET HOME, gdy włączasz Anti-Theft.
2. Konfiguracja nazwy urządzenia.

Anti-Theft nie obsługuje systemu Microsoft Windows Home Server.

Po włączeniu Anti-Theft możesz zoptymalizować bezpieczeństwo urządzenia w głównym oknie programu > **Narzędzia** > **Anti-Theft**.

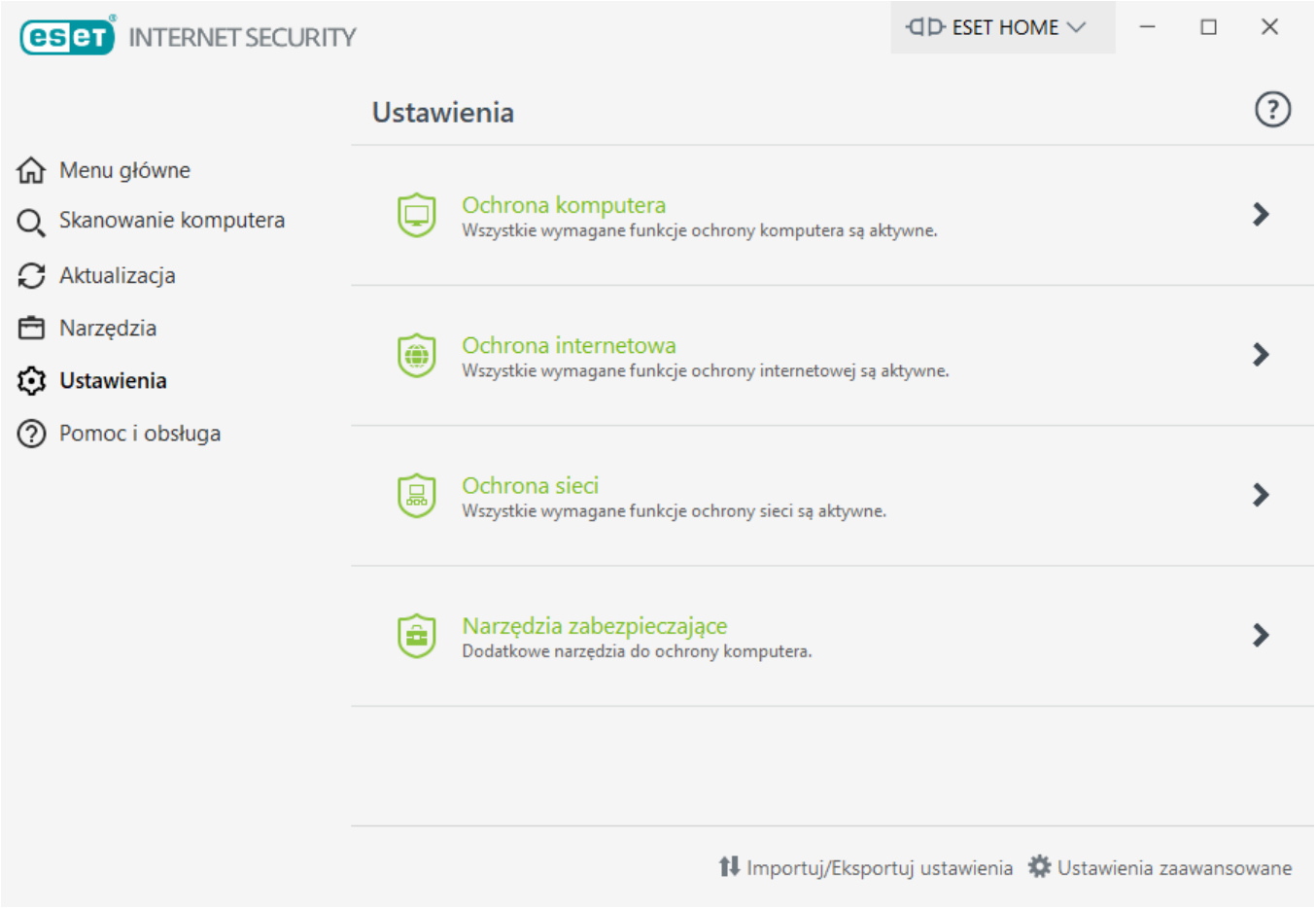
Narzędzia do kontroli rodzicielskiej

Jeśli w produkcie ESET Internet Security funkcja kontroli rodzicielskiej jest włączona, należy ją skonfigurować dla odpowiednich kont użytkowników.

Jeśli kontrola rodzicielska jest aktywna, a konta użytkowników nie zostały skonfigurowane, w **oknie głównym programu** zostanie wyświetlona informacja „Kontrola rodzicielska nie została skonfigurowana”. Kliknij pozycję **Skonfiguruj reguły** i zapoznaj się z sekcją Kontrola rodzicielska, aby uzyskać więcej informacji.

Praca z programem ESET Internet Security

Korzystając z ustawień programu ESET Internet Security, można skonfigurować odpowiedni poziom ochrony komputera i sieci.



Menu **Ustawienia** zawiera następujące sekcje:

Ochrona komputera

Ochrona internetowa

Ochrona sieci

Narzędzia zabezpieczające

Kliknięcie komponentu umożliwia dostosowanie ustawień zaawansowanych odpowiedniego modułu ochrony.

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 szkodliwego kodu.

- **Kontrola dostępu do urządzeń** — przy użyciu tego modułu można skanować, blokować i dostosowywać rozszerzone filtry i uprawnienia oraz określać poziom dostępu do danego urządzenia i pracy z nim (CD/DVD/USB...).

- **System HIPS** — system HIPS monitoruje zdarzenia występujące wewnątrz systemu operacyjnego i reaguje na nie zgodnie z odpowiednio dostosowanym zestawem reguł.

- **Tryb gier** — umożliwia włączanie i wyłączanie trybu gier. Po włączeniu trybu gier zostanie wyświetlony komunikat ostrzegawczy (potencjalne zagrożenie bezpieczeństwa), a główne okno programu zmieni kolor na pomarańczowy.

- **Ochrona kamery internetowej** — umożliwia kontrolowanie procesów i aplikacji uzyskujących dostęp do kamery internetowej podłączonej do komputera.

Ustawienia **Ochronainternetowa** umożliwiają włączanie i wyłączanie następujących komponentów:

- **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** — zapewnia kontrolę wiadomości odbieranych przy użyciu protokołów POP3(S) i IMAP(S).

- **Ochrona przed spamem** — umożliwia skanowanie w poszukiwaniu niepożądanych wiadomości e-mail, czyli spamu.

- **Ochrona przed atakami typu „phishing”** — filtruje witryny podejrzane o dystrybucję treści mających na celu wyłudzenie od użytkowników poufnych informacji.

W sekcji **Ochrona sieci** można włączać i wyłączać moduły Zapora, Ochrona przed atakami z sieci (IDS) oraz Ochrona przed botnetami.

Ustawienia **Narzędzi zabezpieczających** umożliwiają skonfigurowanie następujących modułów:

- **Ochrona bankowości internetowej** — zapewnia dodatkową warstwę ochrony przeglądarki zaprojektowaną w celu ochrony danych finansowych podczas przeprowadzania transakcji przez Internet. Włącz funkcję **Zabezpiecz wszystkie przeglądarki**, aby uruchamiać wszystkie obsługiwane przeglądarki internetowe w trybie bezpiecznym. Aby uzyskać więcej informacji, zobacz Ochrona bankowości internetowej.

- **Kontrola rodzicielska** — moduł Kontrola rodzicielska chroni dzieci, blokując nieodpowiednie lub szkodliwe treści w Internecie.

- **Anti-Theft** — włącz funkcję Anti-Theft, aby chronić komputer w przypadku zgubienia lub kradzieży.

Kontrola rodzicielska umożliwia blokowanie stron internetowych, które mogą zawierać obraźliwe materiały. Ponadto można zablokować dostęp do ponad 40 wstępnie zdefiniowanych kategorii i ponad 140 podkategorii witryn internetowych.

Aby ponownie włączyć wyłączony komponent zabezpieczeń, kliknij przełącznik , aby wyświetlić zielony znacznik .

> Gdy ochrona zostanie wyłączona w ten sposób, wszystkie wyłączone moduły zabezpieczeń zostaną włączone po ponownym uruchomieniu komputera.

Na dole okna ustawień znajduje się kilka dodatkowych opcji. Łącze **Ustawienia zaawansowane** umożliwia skonfigurowanie bardziej szczegółowych parametrów dla każdego modułu. Opcja **Importuj/Eksportuj ustawienia** umożliwia załadowanie ustawień z pliku konfiguracyjnego z rozszerzeniem .xml lub zapisanie bieżących ustawień do takiego pliku.

Ochrona komputera

Aby wyświetlić przegląd modułów ochrony, kliknij opcję **Ochrona komputera** w oknie **Ustawienia**:

- Ochrona systemu plików w czasie rzeczywistym
- Kontrola dostępu do urządzeń
- System zapobiegania włamaniom działający na hoście (HIPS)
- Tryb gier
- Ochrona kamery internetowej

Aby wstrzymać lub wyłączyć poszczególne moduły ochrony, kliknij ikonę suwaka .

⚠ Wyłączenie modułów ochrony może obniżyć poziom ochrony komputera.

Kliknij ikonę koła zębatego ⚙ obok modułu ochrony, aby uzyskać dostęp do zaawansowanych ustawień tego modułu.

W przypadku **ochrony systemu plików w czasie rzeczywistym** kliknij ikonę koła zębatego ⚙ i wybierz jedną z następujących opcji:

- **Konfiguruj** — otwiera Ustawienia zaawansowane Ochrony systemu plików w czasie rzeczywistym.
- **Edytuj wykluczenia** — otwiera okno Ustawienia wykluczeń, aby wykluczyć pliki i foldery ze skanowania.

W przypadku **ochrony kamery internetowej** kliknij ikonę koła zębatego ⚙ i wybierz jedną z następujących opcji:

- **Konfiguruj** — otwiera Ustawienia zaawansowane ochrony kamery internetowej.
- **Zablokuj dostęp do ponownego uruchomienia** — blokuje dostęp do kamery internetowej do czasu ponownego uruchomienia komputera.
- **Zablokuj dostęp na stałe** — blokuje dostęp do kamery internetowej, dopóki to ustawienie nie zostanie wyłączone.
- **Wyłącz całkowite blokowanie dostępu** — wyłącza możliwość blokowania dostępu do kamery internetowej. Ta opcja jest dostępna tylko wtedy, gdy dostęp do kamery internetowej jest zablokowany.



Wstrzymaj ochronę antywirusową i antyspyware — umożliwia wyłączenie wszystkich modułów ochrony antywirusowej i antyspyware. Po wyłączeniu ochrony zostaje wyświetlone okno, w którym można określić, jak długo ochrona ma być wyłączona, używając menu rozwijanego **Przedział czasowy**. Opcja ta powinna być używana wyłącznie przez doświadczonych użytkowników lub po uzyskaniu instrukcji od zespołu pomocy technicznej ESET.

Silnik detekcji

Silnik detekcji chroni system przed złośliwym oprogramowaniem, kontrolując pliki, pocztę e-mail i komunikację internetową. Jeśli na przykład zostanie wykryty obiekt sklasyfikowany jako szkodliwe oprogramowanie, rozpocznie się naprawa. Silnik detekcji najpierw blokuje zagrożenie, a następnie je leczy, usuwa lub przenosi do kwarantanny.

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

Zmiany w ustawieniach silnika detekcji powinni wprowadzać jedynie doświadczeni użytkownicy. Nieprawidłowe skonfigurowanie ustawień może spowodować obniżenie poziomu bezpieczeństwa.

W tej sekcji:

- Ochrona w czasie rzeczywistym i uczenie maszynowe — kategorie
- Skanowania w poszukiwaniu szkodliwego oprogramowania
- Konfiguracja raportowania

- Konfiguracja ochrony

Ochrona w czasie rzeczywistym i uczenie maszynowe — kategorie

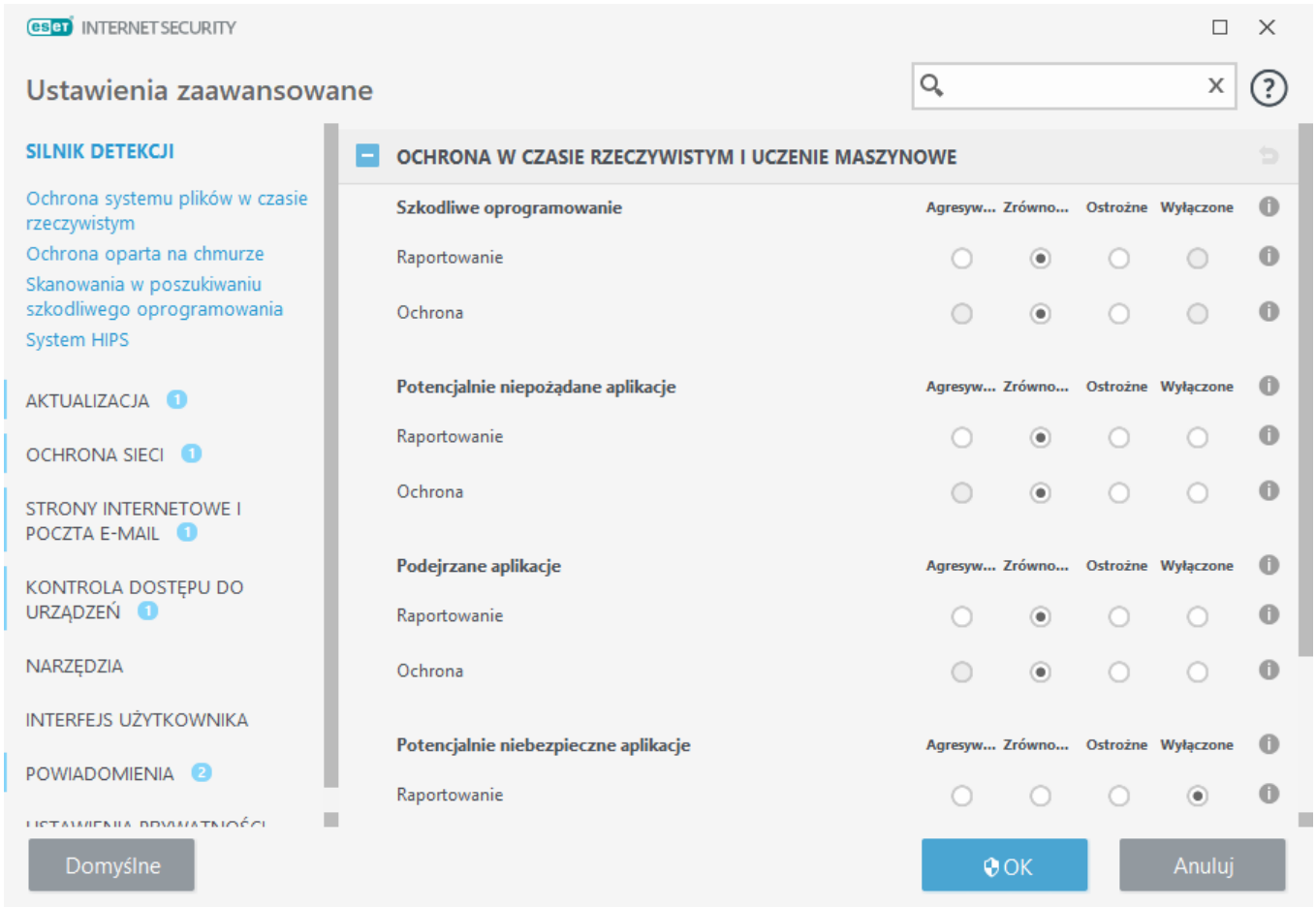
Ochrona w czasie rzeczywistym i uczenie maszynowe we wszystkich modułach ochrony (np. Ochrona systemu plików w czasie rzeczywistym, Ochrona dostępu do stron internetowych) umożliwia skonfigurowanie raportów i poziomów ochrony w następujących kategoriach:

- **Szkodliwe oprogramowanie** — wirus komputerowy to szkodliwy kod, który jest dołączany do istniejących plików na komputerze. 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). Wykrywanie szkodliwego oprogramowania jest przeprowadzane przez moduł silnika detekcji w połączeniu z komponentem uczenia maszynowego. Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.

- **Potencjalnie niepożądane aplikacje** — Grayware lub potencjalnie niepożądane aplikacje (PUA) to szeroka kategoria oprogramowania, które nie jest tak jednoznacznie niebezpieczne z założenia jak wirusy, konie trojańskie czy inne rodzaje szkodliwego oprogramowania. Może ono jednak instalować niechciane oprogramowanie, zmieniać sposób działania urządzenia cyfrowego lub wykonywać działania, których użytkownik nie zatwierdził lub których się nie spodziewał. 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.

- **Potencjalnie niebezpieczne aplikacje** — 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). Więcej informacji na temat aplikacji tego typu można znaleźć w słowniczku.



Ulepszona ochrona

Zaawansowane uczenie maszynowe stanowi obecnie część silnika detekcji. To zaawansowana, oparta na uczeniu maszynowym warstwa ochrony, która usprawnia wykrywanie zagrożeń. Więcej informacji o tym typie ochrony można znaleźć w słowniczku.

Skanowania w poszukiwaniu szkodliwego oprogramowania

Ustawienia skanera można skonfigurować osobno dla skanera w czasie rzeczywistym i skanera na żądanie. Domyślnie opcja **Wykorzystaj konfigurację ochrony w czasie rzeczywistym** jest włączona. Kiedy ta opcja jest włączona, ustawienia skanowania na żądanie są dziedziczone z sekcji **Ochrona w czasie rzeczywistym i uczenie maszynowe**. Więcej informacji zawiera sekcja Skanowania w poszukiwaniu szkodliwego oprogramowania.

Konfiguracja raportowania

W przypadku wykrycia (np. po znalezieniu zagrożenia sklasyfikowanego jako szkodliwe oprogramowanie) odpowiednie informacje zostają zarejestrowane w dzienniku wykryć i zostają wyświetlone powiadomienia, o ile skonfigurowano je w programie ESET Internet Security.

Dla każdej kategorii (określonej jako „KATEGORIA”) jest skonfigurowany próg raportowania:

1. Szkodliwe oprogramowanie

2.Potencjalnie niepożądane aplikacje

3.Potencjalnie niebezpieczne

4.Podejrzane aplikacje

W raportowaniu jest wykorzystywany silnik detekcji z uwzględnieniem komponentu uczenia maszynowego. Istnieje możliwość ustawienia wyższego poziomu raportowania niż określony próg ochrony. Te ustawienia raportowania nie wpływają na blokowanie, leczenie ani usuwanie obiektów.

Przed zmodyfikowaniem progu (poziomu) raportowania dla KATEGORII należy zapoznać się z następującymi informacjami:

Wartość progowa	Wyjaśnienie
Agresywne	Raportowanie dla KATEGORII ma ustawioną maksymalną czułość. Zgłaszana jest większa liczba wykryć. Ustawienie **Agresywne** może powodować błędne oznaczanie obiektów jako KATEGORIA.
Zrównoważone	Raportowanie dla KATEGORII skonfigurowane jako zrównoważone. Raportowanie szkodliwego oprogramowania zostało skonfigurowane jako zrównoważone, aby zoptymalizować częstotliwość wykrywania i wydajność.
Ostrożne	Raportowanie dla KATEGORII jest skonfigurowane tak, aby zminimalizować liczbę błędów polegających na traktowaniu bezpiecznego pliku jako zagrożenia, a przy tym zapewnić odpowiedni poziom ochrony. Obiekty są zgłaszane tylko wtedy, gdy działanie aplikacji odpowiada zachowaniu typowemu dla KATEGORII.
Wył.	Raportowanie dla KATEGORII jest wyłączone, dlatego zagrożenia danego typu nie są wyszukiwane, zgłaszane ani leczone. To ustawienie powoduje wyłączenie ochrony przed tego typu zagrożeniami. Wyłączenie nie jest możliwe w przypadku raportowania dotyczącego szkodliwego oprogramowania i stanowi wartość domyślną w przypadku potencjalnie niebezpiecznych aplikacji.

Dostępność modułów ochrony programu ESET Internet Security

Dostępność (włączony lub wyłączony) modułu ochrony w przypadku poszczególnych progów KATEGORII jest następująca:

	Agresywne	Zrównoważone	Ostrożne	Wyłączone**
Zaawansowany moduł uczenia maszynowego*	✔ (tryb agresywny)	✔ (tryb konserwatywny)	X	X
Moduł silnika detekcji	✔	✔	✔	X
Inne moduły ochrony	✔	✔	✔	X

* Dostępne programie ESET Internet Security w wersji 13.1 lub nowszej.
**Niezalecane

Określanie wersji produktu, wersji modułów programu i dat kompilacji

1. Kliknij opcję **Pomoc i obsługa** > **Informacje o programie ESET Internet Security**.

2. Na ekranie **Informacje** pierwszy wiersz tekstu zawiera numer wersji produktu ESET.

3. Kliknij opcję **Zainstalowane komponenty**, aby uzyskać informacje o określonych modułach.

Ważne uwagi

Kilka ważnych uwag przydatnych podczas konfigurowania odpowiedniego progu dla danego środowiska:

- W przypadku większości konfiguracji zalecamy jest próg **Zrównoważone**.
- Próg **Ostrożne** odpowiada poziomowi ochrony z poprzednich wersji programu ESET Internet Security (13.0 i starszych). Ten poziom jest zalecany w przypadku środowisk, gdzie priorytetem jest zredukowanie liczby fałszywych wykryć ze strony oprogramowania zabezpieczającego.
- Im wyższa wartość progowa, tym większa liczba wykryć, ale także większe prawdopodobieństwo obiektów błędnie zgłoszonych jako zagrożenia.
- W rzeczywistości nie ma gwarancji, że 100% zagrożeń zostanie wykrytych, a także prawdopodobieństwo uniknięcia nieprawidłowej kategoryzacji nieszkodliwych obiektów jako szkodliwe oprogramowanie wynosi 0%.
- Należy zadbać o aktualizowanie programu ESET Internet Security i jego modułów, aby zrównoważyć wydajność i skuteczność wykrywania oraz liczbę błędnie zgłoszonych obiektów.

Konfiguracja ochrony

Jeśli zostanie zgłoszony obiekt sklasyfikowany jako KATEGORIA, program zablokuje ten obiekt i wyleczy go, usunie lub przeniesie do kwarantanny.

Przed zmodyfikowaniem progu (poziomu) ochrony dla KATEGORII należy zapoznać się z następującymi informacjami:

Wartość progowa	Wyjaśnienie
Agresywne	Po włączeniu raportowania na poziomie agresywnym (lub niższym) wykryte potencjalne zagrożenia są blokowane i zostają podjęte próby ich naprawienia. Zalecamy wybranie tej opcji, jeżeli wszystkie punkty końcowe zostały przeskanowane przy wykorzystaniu ustawień agresywnych i do wyłączenia dodano błędnie zgłoszone obiekty.
Zrównoważone	Po włączeniu raportowania na poziomie ostrożnym (lub niższym) wykryte potencjalne zagrożenia są blokowane i zostają podjęte próby ich naprawienia (wyleczenia).
Ostrożne	Po włączeniu raportowania na poziomie ostrożnym wykryte podejrzane aplikacje są blokowane i zostają podjęte próby ich naprawienia (wyleczenia).
Wył.	Przydatne do identyfikacji i wykluczania obiektów błędnie uznanych za zagrożenia. Wyłączenie nie jest możliwe w przypadku ochrony przed szkodliwym oprogramowaniem i stanowi wartość domyślną w przypadku potencjalnie niebezpiecznych aplikacji.

Tabela przełożenia polityki dla programu ESET Internet Security w wersji 13.0 i starszych

W przypadku uaktualnienia z wersji 13.0 i starszych do wersji 13.1 i nowszych nowy stan progu będzie następujący:

Przełącznik kategorii przed uaktualnieniem	✓	✗
Nowy próg KATEGORII po uaktualnieniu	Zrównoważone	Wył.

Opcje zaawansowane silnika detekcji

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.

Włącz zaawansowane skanowanie przy użyciu interfejsu AMSI — narzędzie Microsoft Antimalware Scan Interface umożliwiające twórcom aplikacji korzystanie z nowych mechanizmów zabezpieczeń przed szkodliwym oprogramowaniem (tylko w systemie Windows 10).

Wykrycie infekcji

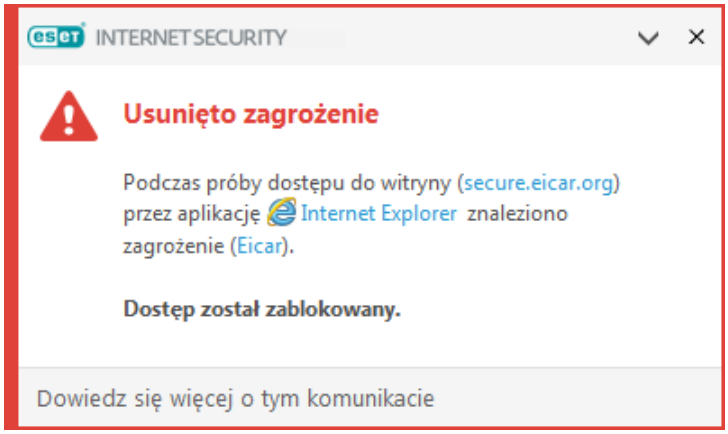
System może zostać zainfekowany z różnych źródeł, takich jak strony internetowe, foldery udostępnione, poczta e-mail lub urządzenia wymienne (USB, dyski zewnętrzne, płyty CD i DVD, itp.).

Działanie standardowe

Ogólnym przykładem sposobu działania programu ESET Internet 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. Szczegółowe informacje na temat wykrytych/wyleczonych obiektów zawierają Pliki dziennika. Więcej informacji dotyczących poziomów leczenia i sposobów działania można znaleźć w sekcji Poziom leczenia.



Skanowanie komputera w poszukiwaniu zainfekowanych plików

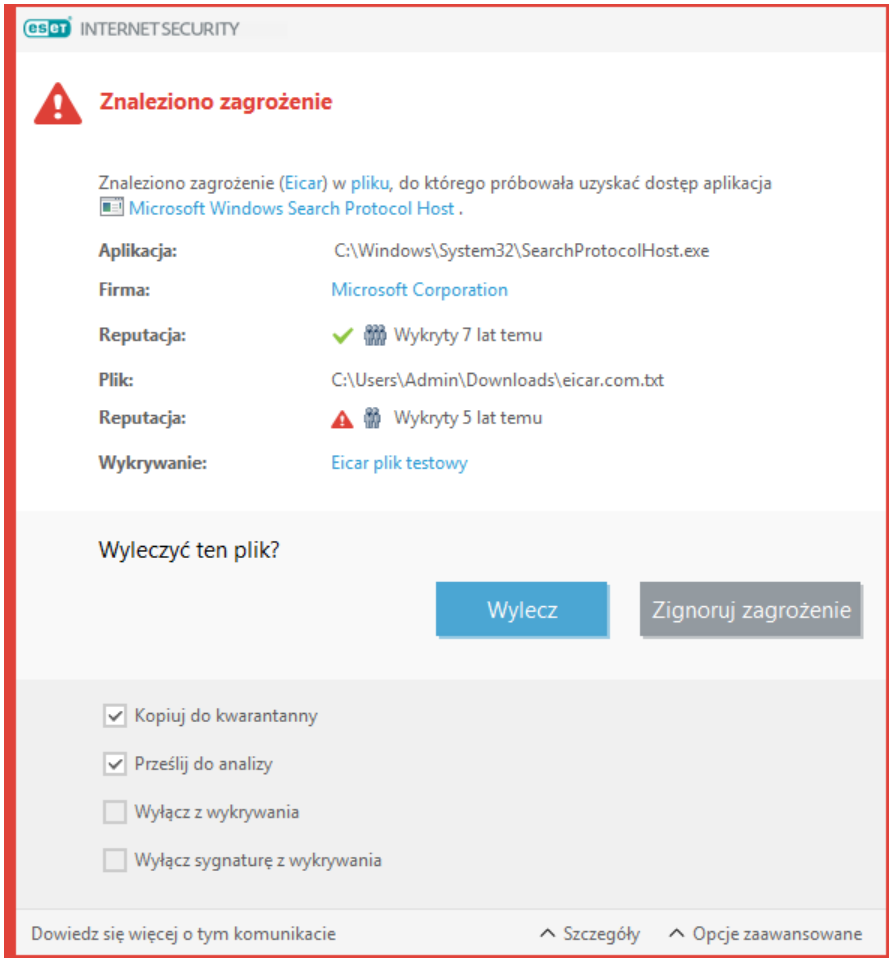
Jeśli komputer wykazuje objawy zainfekowania szkodliwym oprogramowaniem, na przykład działa wolniej lub często przestaje odpowiadać, zalecane jest wykonanie następujących czynności:

1. Otwórz ESET Internet Security i kliknij **Skanowanie komputera**.
2. Kliknij opcję **Skanowanie komputera** (więcej informacji można znaleźć w części Skanowanie komputera).
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.

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).

Przywracanie plików z kwarantanny

Kwarantanna jest dostępna z poziomu głównego okna programu ESET Internet Security po kliknięciu opcji **Narzędzia** > **Więcej narzędzi** > **Kwarantanna**.

Pliki poddane kwarantannie można również przywrócić do ich pierwotnej lokalizacji:

- Umożliwia to funkcja **Przywróć**, dostępna w menu kontekstowym otwieranym po kliknięciu prawym przyciskiem myszy danego pliku w obszarze Kwarantanna.
- Jeśli plik jest oznaczony jako potencjalnie niepożądana aplikacja, włączona jest opcja **Przywróć i wyłącz ze skanowania**. Zobacz też: Wyłączenia.
- Menu kontekstowe zawiera także opcję **Przywróć do**, która umożliwia przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.
- Funkcja przywracania nie jest dostępna w niektórych przypadkach, na przykład gdy pliki znajdują się w udziale sieciowym tylko do odczytu.

Wiele zagrożeń

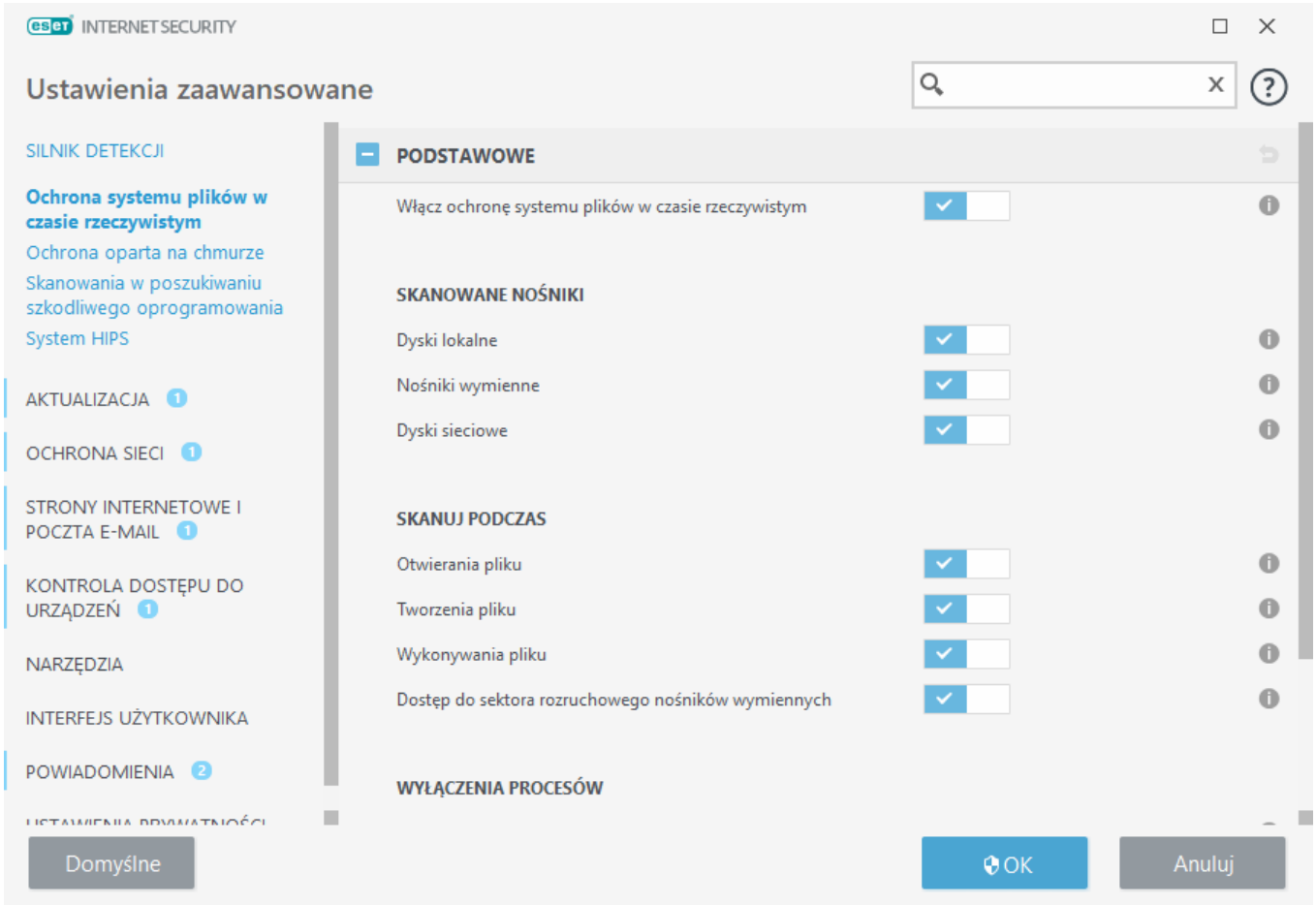
Jeśli jakieś zainfekowane pliki nie zostały wyleczone podczas skanowania komputera (lub poziom leczenia został ustawiony na **Brak leczenia**), w oknie alertu zostanie wyświetlony monit o wybranie czynności dotyczących tych plików. Należy wybrać odpowiednie czynności (są one ustawiane indywidualnie dla każdego pliku z listy), a następnie kliknąć przycisk **Zakończ**.

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.

Ochrona systemu plików w czasie rzeczywistym

Ochrona systemu plików w czasie rzeczywistym zabezpiecza przed szkodliwym kodem wszystkie pliki w systemie podczas ich otwierania, tworzenia i uruchamiania.



Ochrona systemu plików w czasie rzeczywistym jest domyślnie włączana przy uruchamianiu systemu i zapewnia nieprzerwane skanowanie. Ochronę w czasie rzeczywistym można wyłączyć, dezaktywując opcję **Uruchom ochronę systemu plików w czasie rzeczywistym** w obszarze **Ustawienia zaawansowane** w sekcji **Silnik detekcji** > **Ochrona systemu plików w czasie rzeczywistym** > **Podstawowe**.

Skanowane nośniki

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

- **Dyski lokalne** — skanuje wszystkie dyski systemowe i stałe dyski twarde (np.: *C:*\, *D:*\).
- **Nośniki wymienne** — skanuje dyski CD/DVD, pamięci USB, karty pamięci itp.
- **Dyski sieciowe** — skanuje wszystkie zamapowane dyski sieciowe (np.: *H:*\ jako *store04*) lub dyski sieciowe z dostępem bezpośrednim (np.: *store08*).

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** — wykonuje skanowanie podczas otwierania pliku.
- **Tworzenia pliku** — wykonuje skanowanie podczas tworzenia lub modyfikowania pliku.
- **Wykonywania pliku** — wykonuje skanowanie podczas uruchamiania pliku.
- **Dostęp do sektora rozruchowego nośników wymiennych** — kiedy do urządzenia zostanie włożony nośnik wymienny zawierający sektor startowy, sektor startowy jest natychmiast skanowany. Ta opcja nie umożliwia skanowania plików na nośniku wymiennym. Opcja skanowania plików na nośniku wymiennym znajduje się tutaj: **Skanowane nośniki** > **Nośniki wymienne**. Aby opcja **Dostęp do sektora startowego nośników wymiennych** działała prawidłowo, pozostaw włączoną opcję **Sektory startowe/UEFI** w parametrach ThreatSense.

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 silnika detekcji. 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, naciśnij klawisz **F5** w celu otwarcia okna **Ustawienia zaawansowane** i kliknij kolejno pozycje **Silnik detekcji** > **Ochrona systemu plików w czasie rzeczywistym**. Następnie należy kliknąć kolejno **parametr technologii ThreatSense** > **Inne** i zaznaczyć lub odznaczyć opcję **Włącz inteligentną optymalizację**.

Poziomy leczenia

Aby uzyskać dostęp do ustawień poziomów leczenia dla żądanego modułu ochrony, rozwiń pozycję **Parametry technologii ThreatSense** (na przykład **Ochrona systemu plików w czasie rzeczywistym),** a następnie zlokalizuj opcję **Leczenie > Poziom leczenia**.

Parametry ThreatSense mają następujące poziomy korygowania (tj. czyszczenia).

Naprawa w produkcie ESET Internet Security

Poziom leczenia	Opis
Zawsze naprawiaj wykrycie	Podjęcie próby naprawy podczas leczenia obiektów bez interwencji użytkownika. W niektórych rzadkich przypadkach (np. plików systemowych), jeśli nie można naprawić wykrycia, zgłoszony obiekt pozostanie w pierwotnej lokalizacji.
Napraw wykrycie, jeśli to bezpieczne — w przeciwnym razie pozostaw	Podjęcie próby naprawy podczas leczenia obiektów bez interwencji użytkownika. W niektórych przypadkach (np. plików systemowych lub archiwów zawierających zarówno czyste, jak i zainfekowane pliki), kiedy zagrożenia nie można naprawić, obiekt pozostanie w pierwotnej lokalizacji.
Napraw wykrycie, jeśli to bezpieczne — w przeciwnym razie spytaj	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów. W niektórych przypadkach, jeśli nie można wykonać żadnej akcji, użytkownikowi zostanie wyświetlony alert interaktywny umożliwiający wybór czynności zaradczej (np. usunięcia lub zignorowania). To ustawienie jest zalecane w większości przypadków.
Zawsze pytaj użytkownika	Użytkownik końcowy widzi interaktywne okno podczas leczenia obiektów i musi wybrać akcję naprawczą (na przykład usunąć lub zignorować). Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie kroki należy podjąć w przypadku wykrycia.

Zmienianie ustawień ochrony w czasie rzeczywistym

Ochrona 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 Internet Security wszystkie ustawienia są optymalizowane w celu zapewnienia maksymalnego poziomu bezpieczeństwa systemu. W celu przywrócenia ustawień domyślnych kliknij ikonę obok każdej z kart w oknie (**Ustawienia zaawansowane** > **Silnik detekcji** > **Ochrona systemu plików w czasie rzeczywistym**).

Sprawdzanie skuteczności ochrony w czasie rzeczywistym

Aby sprawdzić, czy funkcja ochrony w czasie rzeczywistym działa i wykrywa wirusy, można użyć pliku testowego z witryny *www.eicar.com*. Jest to przygotowany nieszkodliwy plik testowy wykrywany przez wszystkie programy antywirusowe. Został on utworzony przez firmę 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
Wpisanie tego adresu URL w przeglądarce powinno spowodować wyświetlenie komunikatu informującego, że zagrożenie zostało zlikwidowane.

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 użytkownik przypadkowo wyłączy ochronę w czasie rzeczywistym, należy ponownie aktywować tę funkcję. Aby ponownie aktywować ochronę w czasie rzeczywistym, przejdź do **Ustawień** w głównym oknie programu i kliknij pozycję **Ochrona komputera** > **Ochrona systemu plików w czasie rzeczywistym**.

Jeśli ochrona w czasie rzeczywistym nie jest inicjowana podczas uruchamiania systemu, najczęściej jest to spowodowane wyłączoną opcją **Włącz ochronę systemu plików w czasie rzeczywistym**. Aby włączyć tę opcję, przejdź do obszaru **Ustawienia zaawansowane** (**F5**) i kliknij kolejno pozycje **Silnik detekcji** > **Ochrona 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. Jeśli jednocześnie są zainstalowane dwa programy antywirusowe, mogą występować między nimi konflikty. 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 **Włącz ochronę systemu plików w czasie rzeczywistym** jest włączona), może to być spowodowane konfliktami z innymi programami. Aby rozwiązać ten problem, Utwórz Dziennik aplikacji SysInspector i prześlij go do pomocy technicznej ESET celem analizy.

Wyłączenia procesów

Funkcja Wyłączenia procesów umożliwia wykluczanie procesów aplikacji z ochrony systemu plików w czasie rzeczywistym. Aby zwiększyć szybkość tworzenia kopii zapasowych, spójność procesów i dostępność usług, podczas tworzenia kopii zapasowych używane są techniki, które mogą powodować konflikty z funkcją ochrony przed szkodliwym oprogramowaniem na poziomie plików. Jedynym skutecznym sposobem na uniknięcie takich sytuacji jest dezaktywacja oprogramowania chroniącego przed szkodliwym oprogramowaniem. Po wyłączeniu konkretnego procesu (np. związanego z tworzeniem kopii zapasowych) wszystkie operacje na plikach wykonywane przez ten proces będą ignorowane i uznawane za bezpieczne, umożliwiając niezakłócone działanie narzędzia do tworzenia kopii zapasowych. Zalecamy szczególną ostrożność podczas tworzenia wyłączeń — narzędzie do tworzenia kopii zapasowych może uzyskiwać dostęp do zainfekowanych plików bez wyzwalania alertów. Dlatego też rozszerzone uprawnienia są dozwolone tylko w module ochrony w czasie rzeczywistym.

Należy pamiętać, że wyłączenia rozszerzeń plików, wyłączenia systemu HIPS, zaawansowana konfiguracja wyłączeń oraz pliki i foldery wyłączone ze skanowania to różne zagadnienia.

Wyłączenia procesów pozwalają zminimalizować ryzyko występowania konfliktów i poprawiają wydajność wyłączonych aplikacji, co zwiększa ogólną wydajność i stabilność systemu operacyjnego. Wyłączenie procesu/aplikacji oznacza wyłączenie odpowiedniego pliku wykonywalnego (*.exe*).

Aby dodać pliki wykonywalne do listy wyłączonych procesów, należy wybrać kolejno **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Ochrona systemu plików w czasie rzeczywistym** > **Wyłączenia procesów**.

Głównym celem tej funkcji jest wyłączanie narzędzi do tworzenia kopii zapasowych. Wyłączenie procesu takiego narzędzia ze skanowania nie tylko pozwala zapewnić stabilność systemu, ale także nie wpływa na wydajność narzędzia, ponieważ wykonywanie kopii zapasowej nie jest dodatkowo spowalniane.

Kliknij przycisk **Edytuj**, aby otworzyć okno zarządzania **Wyłączenia procesów**, w którym możesz kliknąć przycisk Dodaj wyłączenia i przejść do pliku wykonywalnego (np. *Backup-tool.exe*), który ma zostać wyłączony ze skanowania.
Po dodaniu pliku *.exe* do listy wyłączeń program ESET Internet Security przestanie monitorować aktywność tego procesu. Nie będą też skanowane operacje na plikach wykonywane przez ten proces.

Jeśli podczas wyboru pliku wykonywalnego procesu nie zostanie użyta funkcja przeglądania, może być konieczne ręczne wpisanie pełnej ścieżki do odpowiedniego pliku. W przeciwnym razie wyłączenie nie będzie działać poprawnie i system HIPS może zgłaszać błędy.

Można też **edytować** istniejące procesy lub **usuwać** je z listy wyłączeń.

Wyłączenia tego rodzaju nie są uwzględniane przez funkcję ochrony dostępu do stron internetowych, więc w przypadku wyłączenia pliku wykonywalnego przeglądarki pobierane pliki będą nadal skanowane. W ten sposób nadal można wykryć infiltrację. To tylko przykładowy scenariusz — nie zalecamy tworzenia wyłączeń dla przeglądarek internetowych.

Dodawanie i edytowanie wyłączeń procesów

W tym oknie dialogowym można **dodawać** procesy wyłączone z silnika detekcji. Wyłączenia procesów pozwalają zminimalizować ryzyko występowania konfliktów i poprawiają wydajność wyłączonych aplikacji, co zwiększa ogólną wydajność i stabilność systemu operacyjnego. Wyłączenie procesu/aplikacji oznacza wyłączenie odpowiedniego pliku wykonywalnego (*.exe*).

Należy wybrać ścieżkę do pliku aplikacji objętej wyjątkiem, klikając pozycję ... (np. *C:\Program Files\Firefox\Firefox.exe*). NIE należy wprowadzać nazwy aplikacji.
Po dodaniu pliku *.exe* do listy wyłączeń program ESET Internet Security przestanie monitorować aktywność tego procesu. Nie będą też skanowane operacje na plikach wykonywane przez ten proces.

Jeśli podczas wyboru pliku wykonywalnego procesu nie zostanie użyta funkcja przeglądania, może być konieczne ręczne wpisanie pełnej ścieżki do odpowiedniego pliku. W przeciwnym razie wyłączenie nie będzie działać poprawnie i system HIPS może zgłaszać błędy.

Można też **edytować** istniejące procesy lub **usuwać** je z listy wyłączeń.

Ochrona oparta na chmurze

ESET LiveGrid® (zbudowany na technologii ESET ThreatSense.Net zaawansowany system wczesnego ostrzegania) gromadzi informacje przesyłane przez użytkowników programów ESET z całego świata i przekazuje je do laboratorium firmy ESET. Dostarczając próbki podejrzanych plików oraz metadane, system ESET LiveGrid® umożliwia nam natychmiastowe reagowanie na potrzeby naszych klientów oraz konfigurowanie narzędzi ESET tak, aby zapewniały ochronę przed najnowszymi zagrożeniami.

Dostępne są następujące opcje:

Włączenie systemu reputacji ESET LiveGrid®

System reputacji ESET LiveGrid® umożliwia dodawanie do białej listy oraz czarnej listy w chmurze.

Można sprawdzić reputację Działających procesów i plików bezpośrednio z poziomu interfejsu programu lub menu kontekstowego, korzystając z dodatkowych informacji dostępnych z systemu ESET LiveGrid®.

Włączenie systemu informacji zwrotnych ESET LiveGrid®

Oprócz systemu reputacji ESET LiveGrid® system informacji zwrotnych ESET LiveGrid® będzie zbierał informacje o komputerze związane z nowo wykrytymi zagrożeniami. Informacje te mogą obejmować:

- Próbki lub kopie plików, w których pojawiło się zagrożenie
- Ścieżki do plików
- Nazwa pliku
- Data i godzina
- Proces, w którym zagrożenie pojawiło się na komputerze
- Informacje o systemie operacyjnym komputera

Domyślnie w programie ESET Internet 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.

Więcej informacji na temat wysyłania powiązanych informacji można znaleźć w polityce prywatności.

Użytkownik może postanowić nie włączać funkcji ESET LiveGrid®

Nie utracisz żadnych funkcji oprogramowania, ale w niektórych przypadkach ESET Internet Security może reagować szybciej na nowe zagrożenia przy włączonej funkcji ESET LiveGrid®. Jeśli funkcja ESET LiveGrid® była używana wcześniej i została wyłączona, 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.

Więcej informacji na temat systemu ESET LiveGrid® można znaleźć w Słowniczku.
Zapoznaj się z naszymi ilustrowanymi instrukcjami dostępnymi w języku angielskim i kilku innych językach na temat tego, jak włączyć lub wyłączyć ESET LiveGrid® w programie ESET Internet Security.

Konfiguracja ochrony opartej na chmurze w obszarze Ustawienia zaawansowane

Aby uzyskać dostęp do ustawień ESET LiveGrid®, otwórz okno **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Ochrona oparta na chmurze.**

- **Włącz system reputacji ESET LiveGrid® (zalecane)** — system reputacji ESET LiveGrid® poprawia wydajność rozwiązań firmy ESET do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze.

- **Włącz system informacji zwrotnych ESET LiveGrid® — przesyła odpowiednie dane (określone w** sekcji **Przesyłanie próbek** poniżej) wraz z raportami o awariach i statystykami do laboratorium badawczego firmy ESET w celu dalszej analizy.

- **Wysyłaj raporty o awariach i dane diagnostyczne** — przesyła dane diagnostyczne dotyczące systemu ESET LiveGrid®, takie jak raporty o awariach czy zrzuty modułów pamięci. Zalecamy pozostawienie tej funkcji włączonej, gdyż pomaga ona firmie ESET w diagnozowaniu problemów, doskonaleniu swoich produktów i zapewnianiu lepszej ochrony użytkowników końcowych.

- **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.

- **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.

Przesyłanie próbek

Ręczne przesyłanie próbek — umożliwia ręczne przesyłanie próbek do firmy ESET z menu kontekstowego, funkcji Kwarantanna lub opcji Narzędzia.

Automatyczne przesyłanie wykrytych próbek

Wybierz, jakiego rodzaju próbki będą przesyłane firmie ESET w celu ich analizy i poprawy wykrywania w przyszłości (domyślny maksymalny dopuszczany rozmiar próbki wynosi 64 MB). Dostępne są następujące opcje:

- **Wszystkie wykryte próbki** — wszystkie obiekty wykryte przez silnik detekcji (w tym potencjalnie niepożądane aplikacje, jeśli odpowiednia opcja została włączona w ustawieniach skanera).

- **Wszystkie próbki oprócz dokumentów** — wszystkie wykryte obiekty oprócz **dokumentów** (patrz niżej).

- **Nie przesyłaj** — wykryte obiekty nie będą przesyłane firmie ESET.

Automatyczne przesyłanie podejrzanych próbek

Te próbki będą wysyłane firmie ESET również wtedy, gdy silnik detekcji ich nie wykryje. Mogą to być na przykład próbki, które prawie nie zostały wykryte, lub próbki, które jeden z modułów ochrony ESET Internet Security uważa za podejrzane lub zachowujące się w niejasny sposób (domyślny maksymalny dopuszczalny rozmiar próbki wynosi 64 MB).

- **Pliki wykonywalne** — obejmuje pliki wykonywalne, na przykład: .exe, .dll, .sys.
- **Archiwa** — obejmuje takie typy archiwów jak .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab.
- **Skrypty** — obejmuje takie typy skryptów jak .bat, .cmd, .hta, .js, .vbs, .ps1.
- **Inne** — obejmuje takie typy plików jak .jar, .reg, .msi, .sfw, .lnk.
- **Możliwy spam** — ta opcja umożliwia wysyłanie firmie ESET części lub całości potencjalnego spamu w postaci załącznika w celu dalszej analizy. Włączenie tej opcji usprawnia globalne wykrywanie spamu, zapewniając użytkownikowi ulepszone funkcje jego wykrywania również w przyszłości.
- **Dokumenty** – obejmuje dokumenty Microsoft Office lub PDF z treścią aktywną lub bez niej.

Rozwiń listę wszystkich uwzględnianych typów dokumentów

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

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 laboratoriów firmy ESET w celu analizy, nawet jeśli zawierają podejrzany kod. Najpopularniejsze typy plików należących do tej kategorii (np. .doc) są wyłączone domyślnie. Do listy wyłączonych plików można dodawać inne typy plików.

Aby wykluczyć pliki pobrane z `download.domain.com`, kliknij pozycję **Ustawienia zaawansowane** > **Silnik detekcji** > **Ochrona oparta na chmurze** > **Przesyłanie próbek**, a następnie kliknij **Edytuj** obok **Wykluczenia**. Dodaj wykluczenie `.download.domain.com`.

Maksymalny rozmiar próbek (MB) — określa maksymalny rozmiar próbek (1-64 MB).

Filtr wyłączeń w ramach ochrony opartej na chmurze

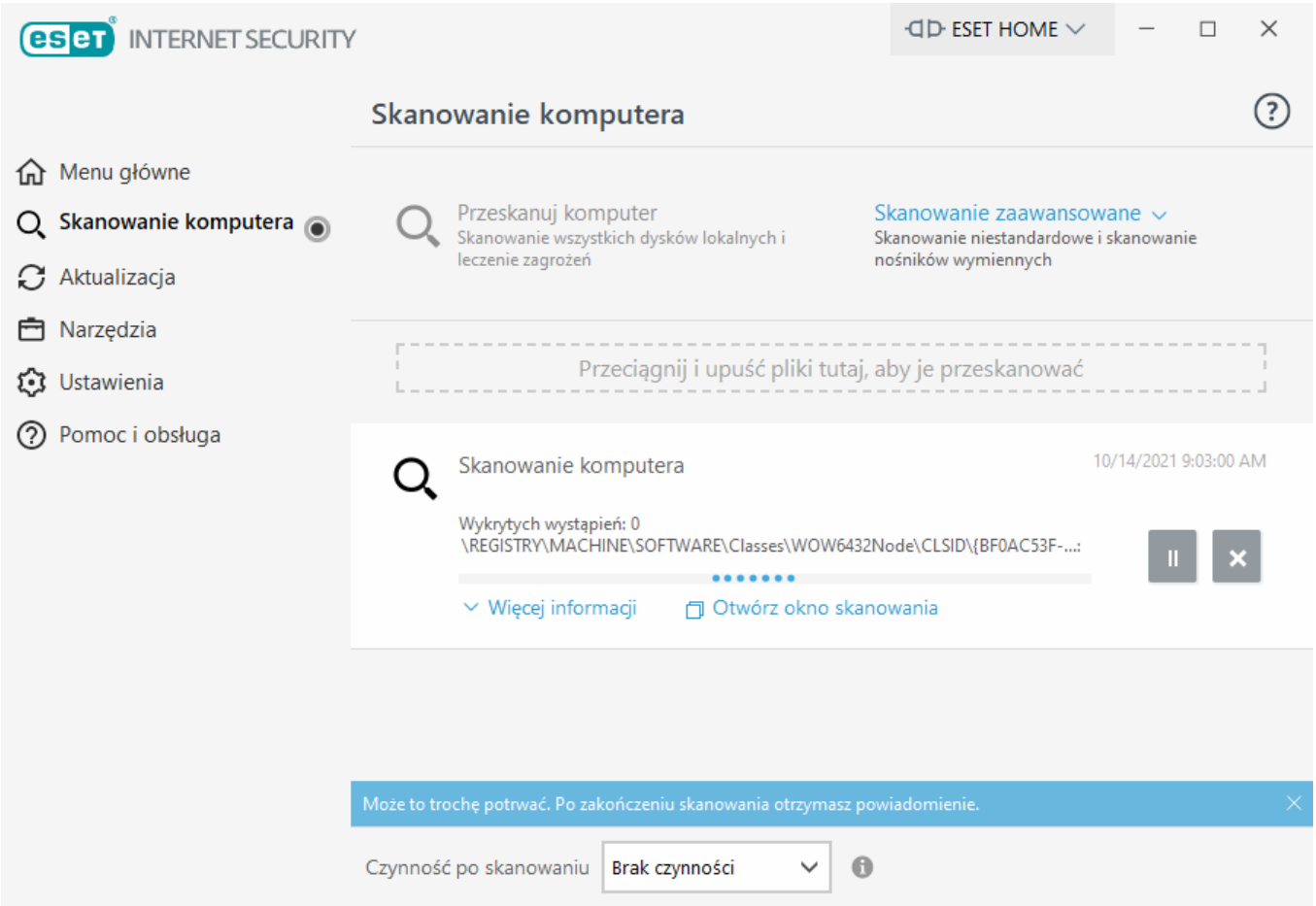
Filtr wyłączeń umożliwia wyłączenie określonych plików lub folderów z przesyłania próbek. Wymienione pliki nigdy nie będą wysyłane do analizy w laboratorium firmy ESET, nawet jeśli będą zawierały podejrzany kod. Popularne typy plików są wyłączone domyślnie (np. .doc).

Ta funkcja przydaje się do wyłączenia plików, które mogą zawierać poufne informacje, takie jak dokumenty lub arkusze kalkulacyjne.

Aby wykluczyć pliki pobrane z download.domain.com, kliknij pozycję **Ustawienia zaawansowane** > **Silnik detekcji** > **Ochrona oparta na chmurze** > **Przesyłanie próbek** > **Wykluczenia** i dodaj wykluczenie *download.domain.com*.

Skanowanie komputera

Skaner na żądanie jest ważnym składnikiem ochrony antywirusowej. Służy on do badania plików i folderów na komputerze. Z punktu widzenia bezpieczeństwa ważne jest, aby skanowanie komputera było przeprowadzane regularnie w ramach rutynowych działań związanych z bezpieczeństwem, a nie tylko w przypadku podejrzenia infekcji. Zalecane jest regularne przeprowadzanie dokładnego skanowania komputera w celu wykrycia obecności wirusów, które nie zostają znalezione przez funkcję Ochrona systemu plików w czasie rzeczywistym podczas zapisywania ich na dysku. Mogłoby się tak zdarzyć, gdyby Ochrona systemu plików w czasie rzeczywistym była wyłączona w danym momencie, silnik detekcji był nieaktualny lub gdyby plik nie został rozpoznany jako wirus podczas zapisywania go na dysku.



Dostępne są dwa typy operacji **Skanowanie komputera**. **Skanowanie komputera** umożliwia szybkie skanowanie systemu bez określania parametrów skanowania. **Skanowanie niestandardowe** (w menu Skanowanie zaawansowane) umożliwia wybranie jednego ze wstępnie zdefiniowanych profili skanowania zaprojektowanych do skanowania określonych lokalizacji oraz określenie obiektów skanowania.

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

Domyślnie program ESET Internet Security podejmuje próby automatycznego wyleczenia lub usunięcia wykryć wykrytych podczas skanowania komputera. W niektórych przypadkach, jeśli nie można wykonać żadnej akcji, zostanie wyświetlony interaktywny alert umożliwiający wybór sposobu leczenia (np. usuń lub zignoruj). Aby zmienić poziom leczenia i uzyskać bardziej szczegółowe informacje, zobacz Leczenie. Aby przejrzeć poprzednie skany, zobacz Pliki dziennika.

Skanowanie komputera

Typ **Skanowanie komputera** umożliwia szybkie uruchomienie skanowania komputera i wyleczenie zainfekowanych plików bez konieczności podejmowania dodatkowych działań przez użytkownika. Zaletą typu **Skanowanie komputera** jest łatwość obsługi i brak konieczności szczegółowej konfiguracji skanowania. W ramach skanowania sprawdzane są wszystkie pliki na dyskach lokalnych, 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.

Można też używać funkcji **skanowania przez przeciąganie i upuszczanie** do ręcznego skanowania pliku lub folderu. W tym celu należy kliknąć plik lub folder i przesunąć wskaźnik do zaznaczonego obszaru, przytrzymując wciśnięty przycisk myszy, a następnie zwolnić przycisk myszy. Spowoduje to przeniesienie aplikacji na pierwszy plan.

W obszarze **Skanowanie zaawansowane** dostępne są następujące opcje skanowania:

Skanowanie niestandardowe

Skanowanie niestandardowe umożliwia użytkownikowi określenie parametrów skanowania, takich jak skanowane obiekty i metody. 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.

Skanowanie nośników wymiennych

Opcja ta, podobnie jak opcja **Skanowanie komputera**, umożliwia szybkie uruchamianie skanowania nośników wymiennych (takich jak CD/DVD/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 **Dyski przenośne** z menu rozwijanego **Skanowane obiekty**, a następnie klikając opcję **Skanuj**.

Powtórz ostatnie skanowanie

Umożliwia szybkie uruchomienie wcześniejszego skanowania przy użyciu tych samych ustawień co poprzednio.

Menu rozwijane**Czynność po skanowaniu** umożliwia wybranie czynności, która będzie przeprowadzona automatycznie po zakończeniu skanowania:

- **Brak czynności** — po ukończeniu skanowania nie zostanie wykonana żadna czynność.
- **Wyłącz** — po ukończeniu skanowania komputer zostanie wyłączony.

• **Uruchom ponownie** — zamknięcie wszystkich otwartych programów i ponowne uruchomienie komputera po ukończeniu skanowania.

• **Uruchom ponownie w razie potrzeby** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.

• **Wymuś ponowne uruchomienie** — wymusza zamknięcie wszystkich otwartych programów bez oczekiwania na interakcję użytkownika i ponownie uruchamia komputer po zakończeniu skanowania.

• **W razie potrzeby wymuś ponowne uruchomienie** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.

• **Uśpij** — zapisanie sesji i przełączenie komputera w tryb obniżonego poboru energii, z którego szybko można wznowić pracę.

• **Hibernacja** — wszystkie procesy uruchomione w pamięci RAM zostają przeniesione do specjalnego pliku na dysku twardym. Komputer wyłącza się, ale po kolejnym uruchomieniu wznawia pracę od poprzedniego stanu.

Tryb uśpienia lub **Hibernacja** są dostępne w zależności od ustawień zasilania i trybu uśpienia komputera lub możliwości technicznych komputera czy laptopa. Należy pamiętać, że komputer w trybie uśpienia nadal działa. Wciąż są uruchomione podstawowe funkcje i komputer nadal zużywa energię, będąc na zasilaniu akumulatorowym. Aby ograniczyć zużycie baterii, na przykład po opuszczeniu biura, zalecane jest skorzystanie z opcji Hibernacja.

Wybrana czynność rozpocznie się po zakończeniu wszystkich uruchomionych skanowań. W przypadku wybrania opcji **Wyłącz** lub **Uruchom ponownie**, na 30 sekund przed automatycznym wyłączeniem zostanie wyświetlone okno dialogowe z potwierdzeniem (kliknij **Anuluj**, aby zrezygnować z wybranej czynności).

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

Program uruchamiający skanowanie niestandardowe

Opcji Skanowanie niestandardowe można używać do skanowania pamięci operacyjnej, sieci lub określonych części dysku. W tym celu należy kliknąć kolejno opcje **Skanowanie zaawansowane** > **Skanowanie niestandardowe** a zaznaczyć żądane obiekty w strukturze folderów (drzewa).

Możesz wybrać profil z menu rozwijanego **Profil** do skanowania określonych celów. Profilem domyślnym jest **Skanowanie inteligentne**. Istnieją trzy dodatkowe uprzednio zdefiniowane profile skanowania **Dokładne skanowanie**, **Skanowanie menu kontekstowego** oraz **Skanowanie komputera**. W tych profilach skanowania stosowane są różne parametry technologii ThreatSense. Dostępne opcje opisano w sekcji **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Skanowanie na żądanie** > Parametry technologii ThreatSense.

Struktura folderu (drzewa) również zawiera określone obiekty docelowe skanowania.

• **Pamięć operacyjna** — skanuje wszystkie procesy i dane aktualnie używane przez pamięć operacyjną.

• **Sektory rozruchowe/UEFI** — skanuje sektory rozruchowe i UEFI pod kątem obecności złośliwego

oprogramowania. Przeczytaj więcej o skanerze UEFI w słowniczku.

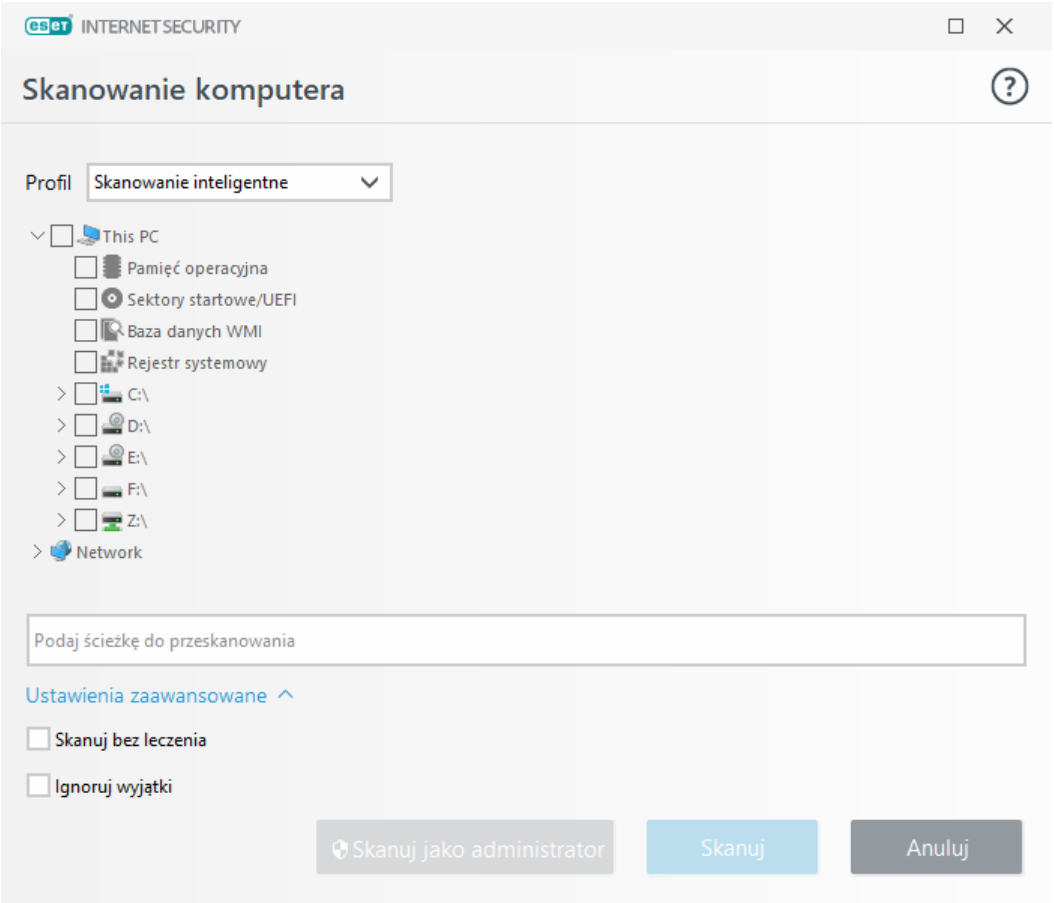
• **Baza danych WMI** — skanuje całą bazę danych Windows Management Instrumentation WMI, wszystkie przestrzenie nazw, wszystkie wystąpienia klas i wszystkie właściwości. Wyszukuje odwołania do zainfekowanych plików lub szkodliwego oprogramowania osadzonego jako dane.

• **Rejestr systemowy** — skanuje cały rejestr systemowy, wszystkie klucze i podklucze. Wyszukuje odwołania do zainfekowanych plików lub szkodliwego oprogramowania osadzonego jako dane. Podczas czyszczenia wykrytych obiektów w rejestrze pozostawiane są odwołania, co zapobiega utracie ważnych informacji.

Aby szybko przejść do obiektu skanowania (pliku lub folderu), wpisz jego ścieżkę w polu tekstowym poniżej struktury drzewa. W ścieżce rozróżniana jest wielkość liter. Aby uwzględnić obiekt skanowania w procesie skanowaniu, zaznacz jego pole wyboru w strukturze drzewa.

Planowanie cotygodniowego skanowania komputera

Aby zaplanować regularnie wykonywane zadanie, zapoznaj się z rozdziałem Planowanie cotygodniowego skanowania komputera.



Parametry czyszczenia dla danego skanowania można skonfigurować po kliknięciu kolejno pozycji **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Skanowanie na żądanie** > **Parametry ThreatSense** > **Czyszczenie**. W celu uruchomienia skanowania bez działań związanych z czyszczeniem należy wybrać opcję **Skanuj bez czyszczenia** w **Ustawieniach zaawansowanych**. Historia skanowania jest zapisywana w dzienniku skanowania.

Gdy wybrana jest opcja **Ignoruj wyjątki**, pliki o rozszerzeniach, które wcześniej zostały wyłączone ze skanowania, także zostaną przeskanowane.

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

niestandardowych.

Opcja **Skanuj jako administrator** umożliwia przeprowadzenie skanowania z uprawnieniami administratora. Tej opcji należy użyć, jeśli obecny użytkownik nie ma uprawnień dostępu do plików, które mają być skanowane. Ten przycisk jest niedostępny, jeśli aktualny użytkownik nie może wywoływać operacji kontroli konta użytkownika (UAC) jako administrator.

> Po ukończeniu skanowania można wyświetlić dziennik skanowania komputera, klikając opcję Wyświetl dziennik.

Postęp skanowania

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

> Jest całkowicie normalne, że nie można przeskanować niektórych plików, na przykład plików zabezpieczonych hasłem lub plików używanych przez system na prawach wyłączności (zwykle dotyczy to pliku *pagefile.sys* i pewnych plików dziennika). Więcej informacji zawiera ten artykuł z bazy wiedzy.

> Planowanie cotygodniowego skanowania komputera
> Aby zaplanować regularnie wykonywane zadanie, zapoznaj się z rozdziałem Planowanie cotygodniowego skanowania komputera.

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.

Znaleziono zagrożenia — łączna liczba skanowanych plików, znalezionych zagrożeń i zagrożeń wyleczonych podczas skanowania.

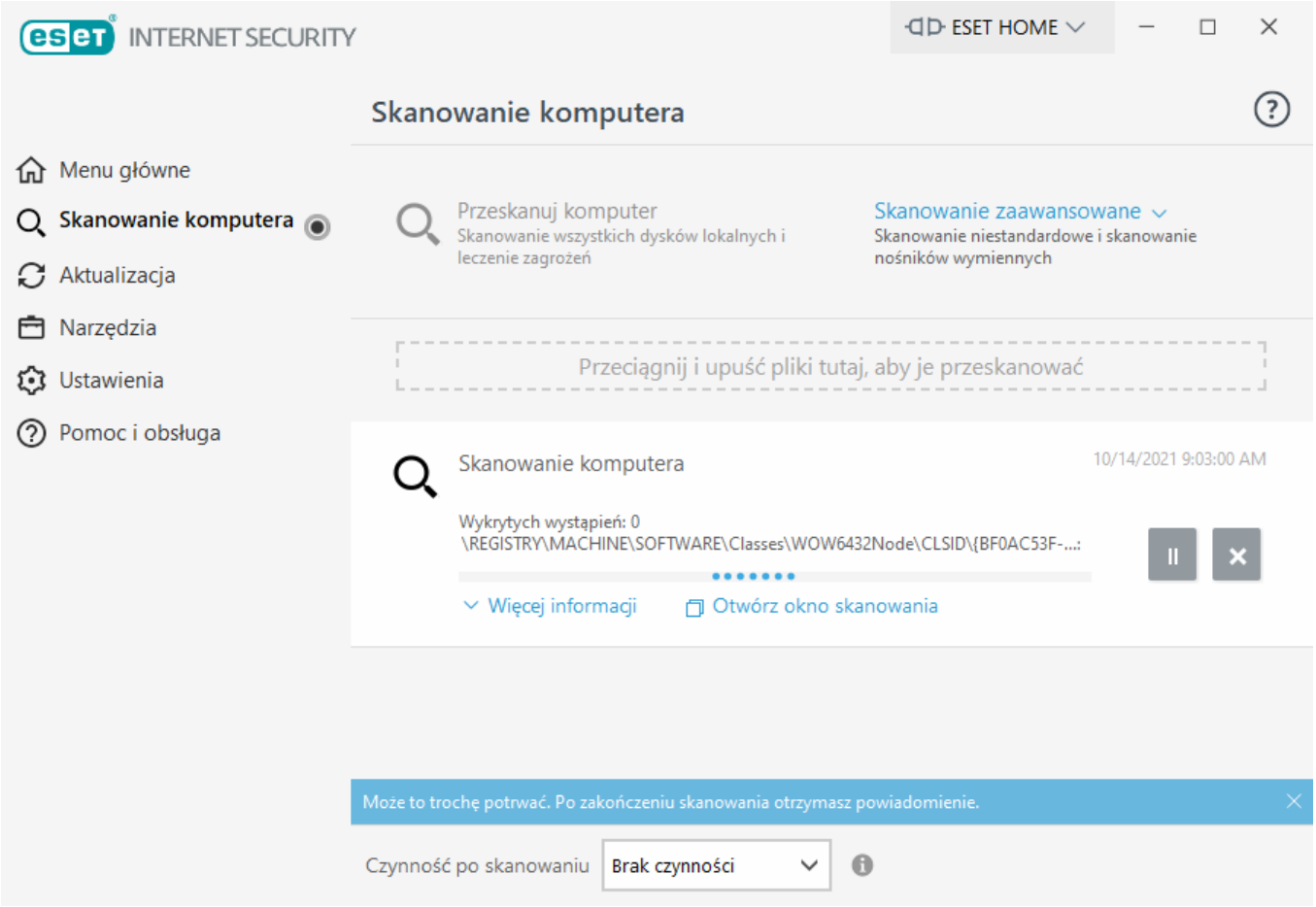
Pauza — umożliwia wstrzymanie skanowania.

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.

> Kliknij ikonę szkła powiększającego lub strzałki, aby wyświetlić szczegóły na temat aktualnego skanowania. Możesz uruchomić dodatkowe skanowanie w tle, klikając **Przeskanuj komputer** lub **Skanowanie zaawansowane** > **Własne ustawienia skanowania**.



Menu rozwijane**Czynność po skanowaniu** umożliwia wybranie czynności, która będzie przeprowadzona automatycznie po zakończeniu skanowania:

- **Brak czynności** — po ukończeniu skanowania nie zostanie wykonana żadna czynność.
- **Wyłącz** — po ukończeniu skanowania komputer zostanie wyłączony.
- **Uruchom ponownie** — zamknięcie wszystkich otwartych programów i ponowne uruchomienie komputera po ukończeniu skanowania.
- **Uruchom ponownie w razie potrzeby** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.
- **Wymuś ponowne uruchomienie** — wymusza zamknięcie wszystkich otwartych programów bez oczekiwania na interakcję użytkownika i ponownie uruchamia komputer po zakończeniu skanowania.
- **W razie potrzeby wymuś ponowne uruchomienie** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.
- **Uśpij** — zapisanie sesji i przełączenie komputera w tryb obniżonego poboru energii, z którego szybko można wznowić pracę.
- **Hibernacja** — wszystkie procesy uruchomione w pamięci RAM zostają przeniesione do specjalnego pliku na dysku twardym. Komputer wyłącza się, ale po kolejnym uruchomieniu wznawia pracę od poprzedniego stanu.

Tryb uśpienia lub **Hibernacja** są dostępne w zależności od ustawień zasilania i trybu uśpienia komputera lub możliwości technicznych komputera czy laptopa. Należy pamiętać, że komputer w trybie uśpienia nadal działa. Wciąż są uruchomione podstawowe funkcje i komputer nadal zużywa energię, będąc na zasilaniu akumulatorowym. Aby ograniczyć zużycie baterii, na przykład po opuszczeniu biura, zalecane jest skorzystanie z opcji Hibernacja.

Wybrana czynność rozpocznie się po zakończeniu wszystkich uruchomionych skanowań. W przypadku wybrania opcji **Wyłącz** lub **Uruchom ponownie**, na 30 sekund przed automatycznym wyłączeniem zostanie wyświetlone okno dialogowe z potwierdzeniem (kliknij **Anuluj**, aby zrezygnować z wybranej czynności).

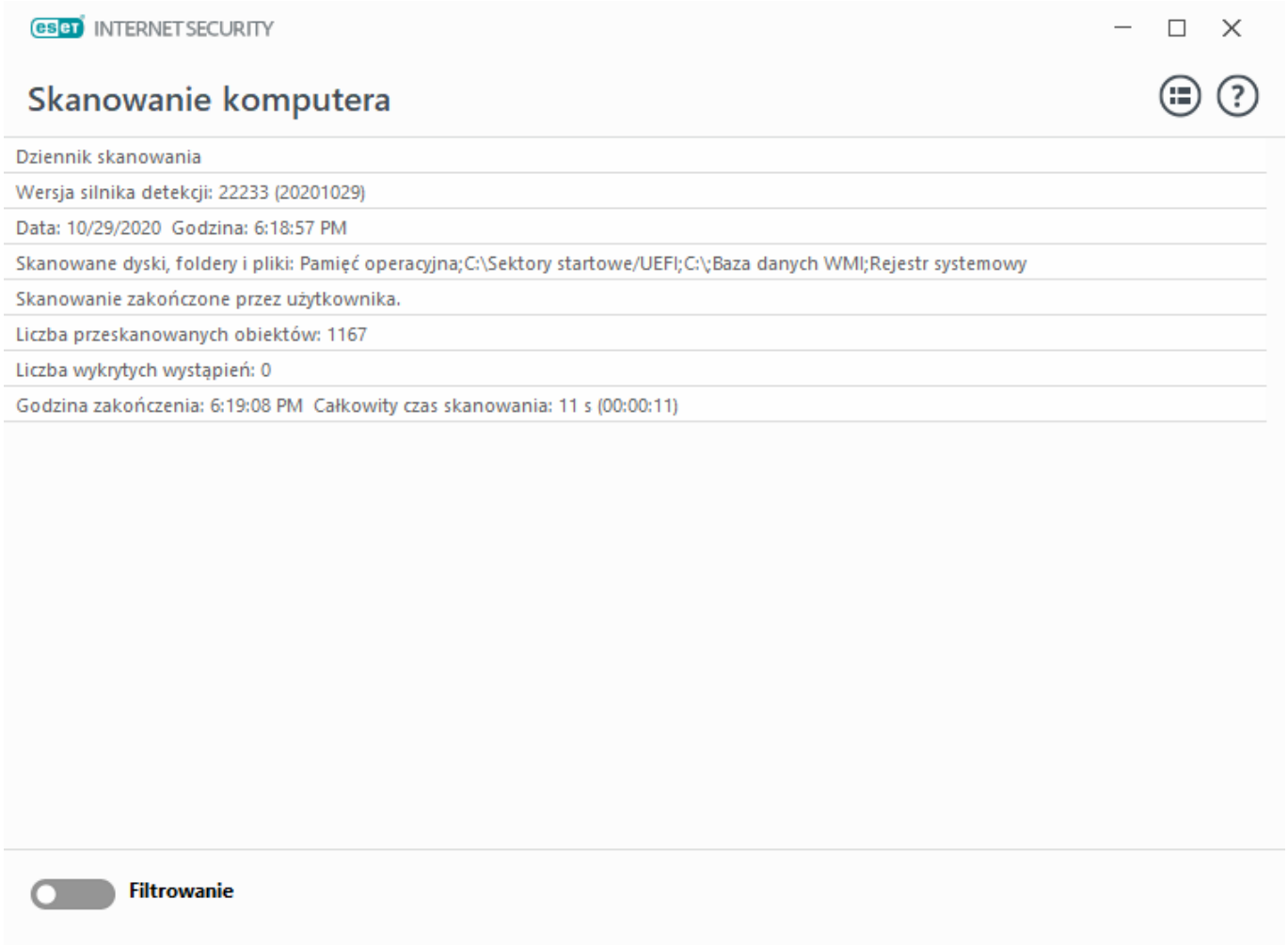
Dziennik skanowania komputera

Po zakończeniu skanowania zostanie otwarty dziennik skanowania komputera zawierający wszystkie istotne informacje dotyczące danego skanowania. Dziennik zawiera następujące informacje:

- Wersja silnika detekcji
- Data i godzina rozpoczęcia
- Lista przeskanowanych dysków, folderów i plików
- Nazwa planowanego skanowania (tylko planowane skanowanie)
- Stan skanowania
- Liczba przeskanowanych obiektów
- Liczba wykrytych potencjalnych zagrożeń
- Godzina zakończenia
- Całkowity czas skanowania

Nowe uruchomienie zaplanowanego zadania skanowania komputera jest pomijane, jeśli to samo zaplanowane zadanie, które zostało włączone wcześniej, jest nadal w toku. W przypadku pominięcia zaplanowanego zadania skanowania utworzony zostanie dziennik skanowania komputera z wpisem 0 zeskanowanych obiektów, a **skanowanie nie rozpoczęło się, ponieważ poprzednie skanowanie było nadal w toku**.

Aby sprawdzić poprzednie dzienniki skanowania, w głównym oknie programu należy kliknąć opcję **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**. Z menu rozwijanego wybierz opcję **Skanowanie komputera** i kliknij dwukrotnie odpowiedni rekord.



> Więcej informacji na temat rekordów „nie można otworzyć”, „błąd otwarcia” i/lub „uszkodzonego archiwum” można znaleźć w artykule bazy wiedzy firmy ESET.

Kliknij ikonę suwaka **Filtrowanie**, aby otworzyć okno Filtrowanie dziennika, w którym możesz zdefiniować własne kryteria wyszukiwania. Aby zobaczyć menu kontekstowe, kliknij właściwy wpis w dzienniku prawym przyciskiem myszy:

Czynność	Wykorzystanie
Filtruj same rekordy	Filtrowanie dziennika zostanie włączone. W dzienniku widoczne będą tylko rekordy tego samego typu jak zaznaczony.
Filtr	Ta opcja powoduje otwarcie okna Filtrowanie dziennika i umożliwia zdefiniowanie kryteriów filtrowania określonych wpisów w dzienniku. Skrót: `Ctrl+Shift+F`
Włącz filtr	Ustawienia filtru zostaną włączone. Jeśli filtr aktywowano po raz pierwszy, konieczne jest zdefiniowanie ustawień. Zostanie otworzone okno Filtrowanie dziennika.
Wyłącz filtr	Wyłącza filtr (ten sam efekt jak kliknięcie przełącznika na dole).
Kopiuj	Kopiuje zaznaczone rekordy do schowka. Skrót: `Ctrl+C`
Kopiuj wszystko	Kopiuje wszystkie rekordy w oknie.
Eksportuj	Eksportuje zaznaczone rekordy zapisane w schowku do pliku XML.
Eksportuj wszystko	Eksportuje wszystkie rekordy w oknie do pliku XML.
Opis wykrycia	Otwiera Encyklopedię zagrożeń firmy ESET, która zawiera szczegółowe informacje o zagrożeniach i objawach wyróżnionej infiltracji.

Skanowania w poszukiwaniu szkodliwego oprogramowania

Sekcja **Skanowania w poszukiwaniu szkodliwego oprogramowania** jest dostępna w menu **Ustawienia zaawansowane** (F5) po kliknięciu opcji **Silnik detekcji** > **Skanowania w poszukiwaniu szkodliwego oprogramowania** i obejmuje opcje wyboru parametrów skanowania. Sekcja ta zawiera następujące elementy:

Wybrany profil — określony zestaw parametrów stosowanych przez skaner na żądanie. W celu utworzenia nowego profilu należy kliknąć opcję **Edytuj** obok pozycji **Lista profili**. Więcej informacji zawiera artykuł Profile skanowania.

Skanowane obiekty — jeśli przeskanowany ma być wyłącznie określony obiekt docelowy, można kliknąć opcję **Edytuj** obok pozycji **Skanowane obiekty** i wybrać opcję z menu rozwijanego lub wybrać określone obiekty w strukturze (drzewie) folderów. Więcej informacji zawiera artykuł Skanowane obiekty.

Parametry technologii **ThreatSense** — w tej sekcji znajdują się ustawienia zaawansowane, takie jak rozszerzenia plików, które mają być sprawdzane, stosowane metody wykrywania itd. Kliknięcie umożliwia otwarcie karty z zaawansowanymi opcjami skanera.

Skanowanie w trakcie bezczynności

Skanowanie w trakcie bezczynności można włączyć w obszarze **Ustawienia zaawansowane**, wybierając kolejno **Silnik detekcji** > **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Skanowanie w trakcie bezczynności**.

Skanowanie w trakcie bezczynności

W celu włączenia tej funkcji należy przesunąć suwak obok pozycji **Włącz skanowanie w trakcie bezczynności**. Gdy komputer będzie w stanie bezczynności, na wszystkich dyskach lokalnych będzie wykonywane skanowanie w trybie cichym.

Domyślnie skanowanie w trakcie bezczynności nie pracuje, gdy komputer (notebook) jest zasilany z baterii. Można zmienić to ustawienie, przesuwając suwak obok opcji **Uruchom nawet jeśli komputer jest zasilany z baterii** w Ustawieniach zaawansowanych.

Przesuń suwak obok pozycji **Włącz zapisywanie w dzienniku** w ustawieniach zaawansowanych, aby rejestrować dane wyjściowe skanowania komputera w sekcji Pliki dziennika (w głównym oknie programu należy kliknąć **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**, a następnie wybrać pozycję **Skanowanie komputera** z menu rozwijanego **Dziennik**).

Wykrywanie stanu bezczynności

Pełną listę warunków, które muszą zostać spełnione w celu uruchomienia skanera w trybie bezczynności, można znaleźć w artykule poświęconym elementom wyzwalającym wykrywanie stanu bezczynności.

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

Profile skanowania

Istnieją 4 wstępnie zdefiniowane profile skanowania w ESET Internet Security:

- **Skanowanie inteligentne** – Jest to podstawowy zaawansowany profil skanowania. Skanowanie inteligentne korzysta z technologii Smart Optimization wykluczającej pliki oznaczone w poprzednim skanowaniu jako czyste, które dodatkowo nie zostały zmodyfikowane od czasu poprzedniego skanowania. Pozwala to skrócić czas skanowania z minimalnym wpływem na bezpieczeństwo systemu.

- **Skanowanie z poziomu skrótu w menu kontekstowym** – Możesz rozpocząć skanowanie na żądanie dowolnego pliku z menu kontekstowego. Profil skanowania menu kontekstowego umożliwia zdefiniowanie konfiguracji skanowania, która będzie używana podczas tego rodzaju skanowania.

- **Skanowanie dokładne** – Profil skanowania dokładnego domyślnie nie korzysta z funkcji Inteligentna optymalizacja, więc podczas używania tego profilu żadne pliki nie są wyłączane ze skanowania.

- **Skanowanie komputera** – Jest to domyślny profil używany w standardowym skanowaniu komputera.

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, otwórz okno Ustawienia zaawansowane (F5) i kliknij kolejno pozycje **Silnik detekcji** > **Skanowanie szkodliwego oprogramowania** > **Skanowanie na żądanie** > **Lista profili**. W oknie **Menedżer profili** wyświetlane jest menu rozwijane **Wybrany profil** z listą istniejących już profili skanowania oraz opcja umożliwiająca utworzenie nowego profilu. 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.

> Załóżmy, że chcesz utworzyć własny profil skanowania, a żądana konfiguracja częściowo pokrywa się z konfiguracją **Skanowanie komputera**, jednak nie chcesz skanować programów spakowanych ani potencjalnie niebezpiecznych aplikacji, za to chcesz zastosować ustawienie **Zawsze naprawiaj wykrycie**. 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.

Skanowane obiekty

W menu rozwijanym **Skanowane obiekty** można wybrać wstępnie zdefiniowane obiekty do skanowania:

- **Zgodnie z ustawieniami profilu** — powoduje wybranie obiektów określonych w wybranym profilu skanowania.
- **Dyski przenośne** — 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.

- **Wybór niestandardowy** — anuluje wszystkie poprzednie wybory.

Struktura folderu (drzewa) również zawiera określone obiekty docelowe skanowania.

- **Pamięć operacyjna** — skanuje wszystkie procesy i dane aktualnie używane przez pamięć operacyjną.
- **Sektory rozruchowe/UEFI** — skanuje sektory rozruchowe i UEFI pod kątem obecności złośliwego oprogramowania. Przeczytaj więcej o skanerze UEFI w słowniczku.
- **Baza danych WMI** — skanuje całą bazę danych Windows Management Instrumentation WMI, wszystkie przestrzenie nazw, wszystkie wystąpienia klas i wszystkie właściwości. Wyszukuje odwołania do zainfekowanych plików lub szkodliwego oprogramowania osadzonego jako dane.
- **Rejestr systemowy** — skanuje cały rejestr systemowy, wszystkie klucze i podklucze. Wyszukuje odwołania do zainfekowanych plików lub szkodliwego oprogramowania osadzonego jako dane. Podczas czyszczenia wykrytych obiektów w rejestrze pozostawiane są odwołania, co zapobiega utracie ważnych informacji.

Aby szybko przejść do obiektu skanowania (pliku lub folderu), wpisz jego ścieżkę w polu tekstowym poniżej struktury drzewa. W ścieżce rozróżniana jest wielkość liter. Aby uwzględnić obiekt skanowania w procesie skanowaniu, zaznacz jego pole wyboru w strukturze drzewa.

Kontrola dostępu do urządzeń

ESET Internet Security udostępnia funkcje automatycznej kontroli korzystania z urządzeń (CD, DVD, USB/...). Przy użyciu tego modułu można 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)
- Dysk CD/DVD
- Drukarka USB
- FireWire Pamięć masowa
- Bluetooth Urządzenie
- Czytnik kart inteligentnych
- Urządzenie do tworzenia obrazów
- Modem
- LPT/COM port
- Urządzenie przenośne
- Urządzenia dowolnego typu

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

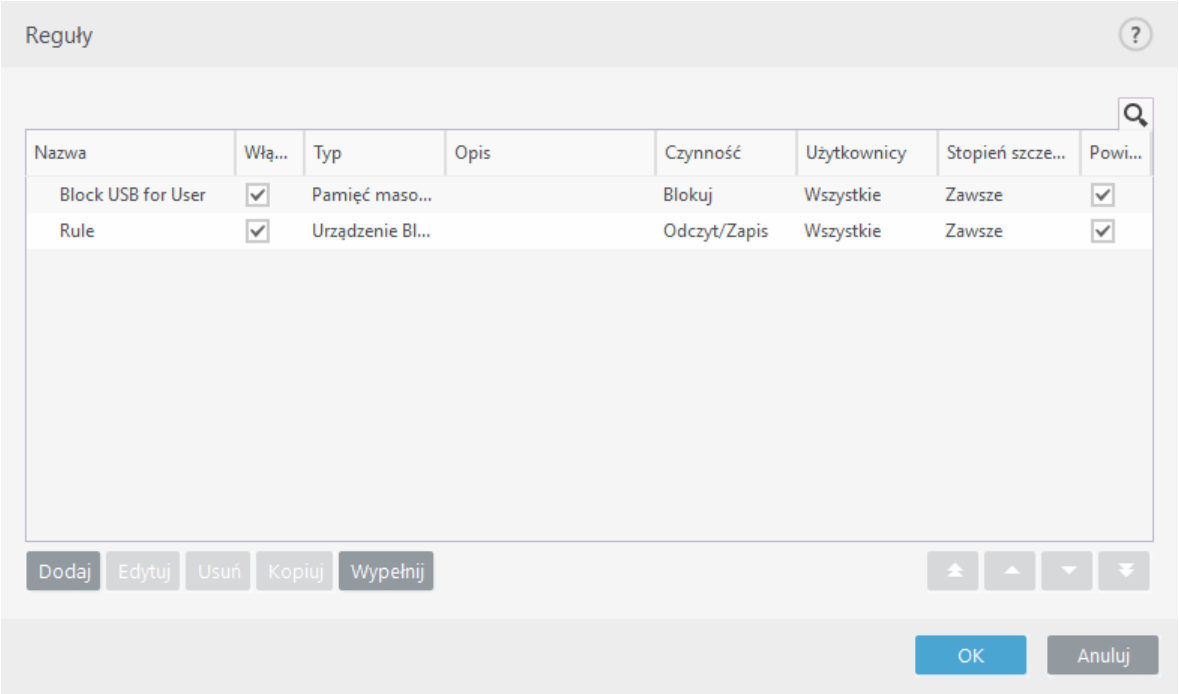
Przesuń suwak obok opcji **Włącz kontrolę dostępu do urządzeń**, aby aktywować funkcję kontroli dostępu do urządzeń w programie ESET Internet Security. Aby zmiana została zastosowana, należy uruchomić komputer ponownie. Po włączeniu kontroli dostępu do urządzeń zostaną aktywowane **reguły**, co umożliwi otwarcie okna Edytor reguł.

Możliwe jest tworzenie wielu grup urządzeń, w odniesieniu do których obowiązują różne reguły. Można też utworzyć tylko jedną grupę urządzeń, do której stosowana będzie reguła związana z czynnością **Odczyt/Zapis** lub **Tylko do odczytu**. Zapewnia to blokowanie podłączanych do komputera nierozpoznanych urządzeń przy użyciu funkcji Kontrola dostępu do urządzeń.

W przypadku podłączenia urządzenia blokowanego przez istniejącą regułę wyświetlane jest okno powiadomienia, a dostęp do urządzenia nie jest możliwy.

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 dla danych użytkowników lub grup użytkowników w oparciu o dodatkowe parametry urządzeń określane 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. Zobacz też Dodawanie reguł kontroli dostępu do urządzeń.

Kliknięcie przycisku **Dodaj** lub **Edytuj** umożliwia zarządzanie regułą. Kliknięcie przycisku **Kopiuj** umożliwia utworzenie nowej reguły ze wstępnie zdefiniowanymi opcjami pochodzącymi z innej wybranej reguły. Ciągi XML wyświetlane po kliknięciu danej reguły można kopiować do schowka, aby pomóc administratorom systemu w eksportowaniu/importowaniu tych danych oraz ich stosowaniu.

Naciśnięcie i przytrzymanie klawisza **CTRL** podczas klikania kolejnych reguł pozwala wybrać większą ich liczbę w celu wykonywania czynności na wszystkich wybranych regułach — na przykład ich usunięcia bądź przeniesienia w górę lub w dół listy. 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.

Sprawdzanie odbywa się według reguł posortowanych według priorytetu, przy czym ważniejsze reguły umieszczone są na górze.

Wpisy dziennika można wyświetlić w oknie głównym programu ESET Internet Security, wybierając kolejno opcje **Narzędzia**. > **Więcej narzędzi** > **Pliki dziennika**.

W dzienniku kontroli dostępu do urządzeń rejestrowane są wszystkie zdarzenia, w przypadku których uruchamiana jest funkcja kontroli dostępu do urządzeń.

Wykryte urządzenia

Użycie przycisku **Wypełnij** umożliwia przegląd wszystkich podłączonych obecnie urządzeń oraz informacji obejmujących: typ urządzenia, producenta urządzenia, model i numer seryjny (jeśli są dostępne).

Wybierz urządzenie z listy Wykryte urządzenia i kliknij przycisk **OK**, aby dodać regułę sterowania urządzeniem ze wstępnie zdefiniowanymi informacjami (wszystkie ustawienia można dostosować).

Urządzenia w trybie niskiego poboru mocy (uśpienia) są oznaczone ikoną ostrzeżenia . Aby włączyć przycisk **OK** i dodać regułę dla tego urządzenia:

- Podłącz ponownie urządzenie
- Użyj urządzenia (na przykład uruchom aplikację Aparat w systemie Windows, aby wybudzić kamerę internetową)

Grupy urządzeń

⚠ Urządzenie podłączone do komputera może stanowić zagrożenie bezpieczeństwa.

Okno Grupy urządzeń jest podzielone na dwie części. W prawej części okna znajduje się lista urządzeń należących do danej grupy, a w części lewej znajdują się utworzone grupy. Grupę, która ma zostać wyświetlona w prawym okienku należy wybrać z listy urządzeń.

Po otwarciu okna Grupy urządzeń i wybraniu grupy można dodawać urządzenia do listy lub usuwać je z niej. Innym sposobem dodawania urządzeń do grup jest zaimportowanie ich z pliku. Można również kliknąć przycisk **Wypełnij**, co umożliwi wyświetlenie listy wszystkich podłączonych do komputera urządzeń w oknie **Wykryte urządzenia**. Należy wybrać urządzenia z wyświetlonej listy i dodać je do grupy, klikając przycisk **OK**.

Elementy sterujące

Dodaj — można dodać grupę, wprowadzając jej nazwę, lub można dodać urządzenie do istniejącej grupy (opcjonalnie można wprowadzić szczegóły, takie jak nazwa dostawcy, model oraz numer seryjny), w zależności od tego, w której części okna znajduje się kliknięty przycisk.

Edytuj — ta opcja umożliwia zmianę nazwy wybranej grupy lub zmianę parametrów urządzenia (dostawcy, modelu, numeru seryjnego).

Usuń — powoduje usunięcie wybranej grupy lub urządzenia zależnie od tego, w której części okna znajduje się kliknięty przycisk.

Importuj — umożliwia zaimportowanie listy urządzeń z pliku tekstowego. Jest przy tym wymagane, aby dane w pliku miały prawidłowy format:

- Wpis o każdym urządzeniu musi być umieszczony w nowym wierszu.
- Dla każdego urządzenia musi być podany **Dostawca**, **Model** i **Numer seryjny**, oddzielone od siebie przecinkami.

Oto przykład zawartości pliku tekstowego:

```
Kingston,DT 101 G2,001CCE0DGRFC0371
04081-0009432,USB2.0 HD WebCam,20090101
```

Eksportuj — eksportuje listę urządzeń do pliku.

Użycie przycisku **Wypełnij** umożliwia przegląd wszystkich podłączonych obecnie urządzeń oraz informacji obejmujących: typ urządzenia, producenta urządzenia, model i numer seryjny (jeśli są dostępne).

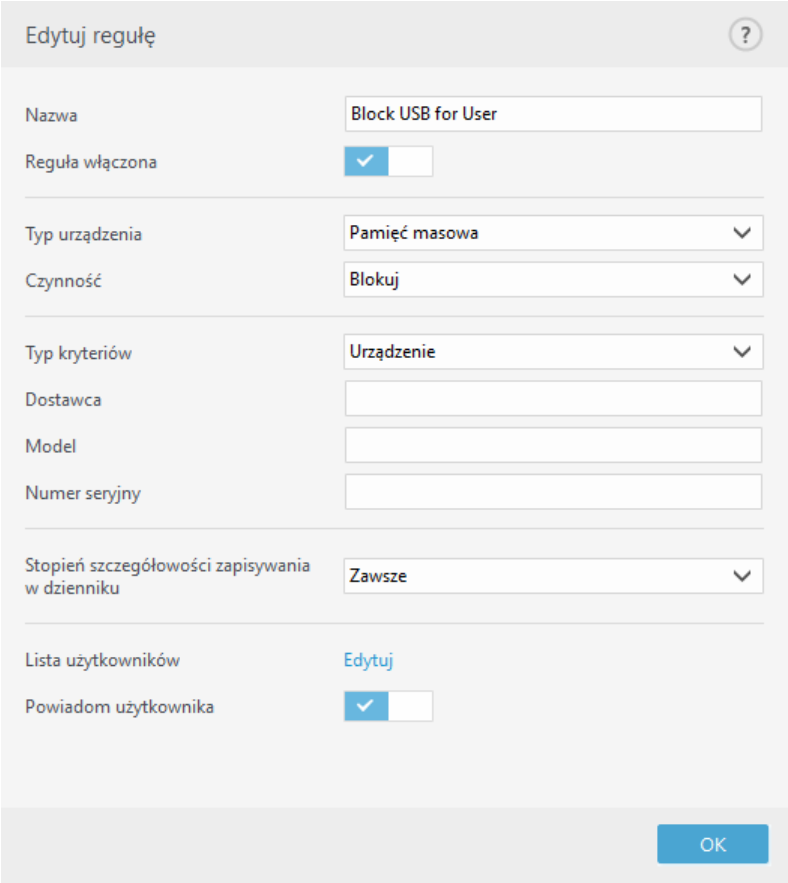
Po zakończeniu dostosowywania należy kliknąć przycisk **OK**. Opuszczenie okna **Grupy urządzeń** bez zapisywania zmian umożliwia przycisk **Anuluj**.

Możliwe jest tworzenie wielu grup urządzeń, w odniesieniu do których obowiązują różne reguły. Można też utworzyć tylko jedną grupę urządzeń, do której stosowana będzie reguła związana z czynnością **Odczyt/Zapis** lub **Tylko do odczytu**. Zapewnia to blokowanie podłączanych do komputera nierozpoznanych urządzeń przy użyciu funkcji Kontrola dostępu do urządzeń.

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

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 polu **Nazwa** należy wprowadzić opis reguły ułatwiający jej identyfikację. Przesunięcie suwaka 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 w przypadku urządzeń Bluetooth, dlatego można tylko zezwolić na dostęp do tych Bluetooth urządzeń, blokować dostęp lub wyświetlać ostrzeżenie).

Typ kryteriów

Wybierz 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 ID 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 CD.

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 (*, ?).

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 zapisywania w dzienniku

ESET Internet Security zapisuje wszystkie ważne zdarzenia w pliku dziennika, który można wyświetlić bezpośrednio z poziomu menu głównego. Kliknij kolejno pozycje **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**, a następnie wybierz opcję **Kontrola dostępu do urządzeń** z menu rozwijanego **Dziennik**.

- **Zawsze** — rejestrowanie wszystkich zdarzeń.
- **Diagnostyka** — zapisywane są informacje potrzebne do ulepszenia konfiguracji programu.
- **Informacje** — rejestrowanie komunikatów informacyjnych, w tym powiadomień o pomyślnych aktualizacjach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenie** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Brak** — w dziennikach nie są zapisywane żadne informacje.

Lista użytkowników

Reguły mogą ograniczać się do wybranych użytkowników lub grup użytkowników poprzez dodanie ich do listy użytkowników, wybierając **Edytuj** obok **Lista użytkowników**.

- **Dodaj** — umożliwia otwarcie okna dialogowego **Typy obiektów: Użytkownicy lub Grupy**, w którym można

wybrać pożądanych użytkowników.

- **Usuń**— umożliwia usunięcie wybranego użytkownika z filtru.

Ograniczenia list użytkowników

Nie można zdefiniować listy użytkowników dla reguł z określonymi typami urządzeń:

- Drukarka USB:
- Urządzenie Bluetooth
- Czytnik kart inteligentnych
- Urządzenie do tworzenia obrazów
- Modem
- Port LPT/COM

Powiadom użytkownika — w przypadku podłączania urządzenia zablokowanego przez istniejącą regułę zostanie wyświetlone powiadomienie.

Ochrona kamery internetowej

Ochrona kamery internetowej informuje o procesach i aplikacjach uzyskujących dostęp do kamery internetowej komputera. Próba uzyskania dostępu do kamery podjęta przez aplikację spowoduje wyświetlenie okna z powiadomieniem. Można **zezwolić** na dostęp lub go **zablokować**. Kolor okna alertu zależy od reputacji aplikacji.

Opcje konfiguracji ochrony kamery internetowej można modyfikować w obszarze **Ustawienia zaawansowane** (F5) > **Kontrola dostępu do urządzeń** > **Ochrona kamery internetowej**.

Aby aktywować funkcję Ochrona kamery internetowej w programie ESET Internet Security, przesuń suwak obok pozycji **Włącz ochronę kamery internetowej**.

Po włączeniu ochrony kamery internetowej **reguły** stają się aktywne, co pozwoli na otwarcie okna Edytora reguł.

Aby wyłączyć alerty dla aplikacji z obecną regułą, które zostały zmodyfikowane, ale nadal mają prawidłowy podpis cyfrowy (na przykład aktualizację aplikacji), przesuń suwak obok pozycji **Wyłącz alerty dostępu do kamery internetowej dla zmodyfikowanych aplikacji**.

Edytor reguł ochrony kamery internetowej

W tym oknie wyświetlane są istniejące reguły i można w nim kontrolować aplikacje oraz procesu uzyskujące dostęp do kamery internetowej komputera na podstawie podejmowanych przez użytkownika czynności.

Dostępne są następujące czynności:

- **Włącz dostęp**
- **Blokuj dostęp**

- **Zapytaj** (pyta użytkownika o zgodę za każdym razem, gdy aplikacja próbuje uzyskać dostęp do kamery internetowej)

Usuń zaznaczenie pola wyboru w kolumnie **Powiadom**, aby zatrzymać wyświetlanie powiadomień, gdy aplikacja uzyskuje dostęp do kamery internetowej.

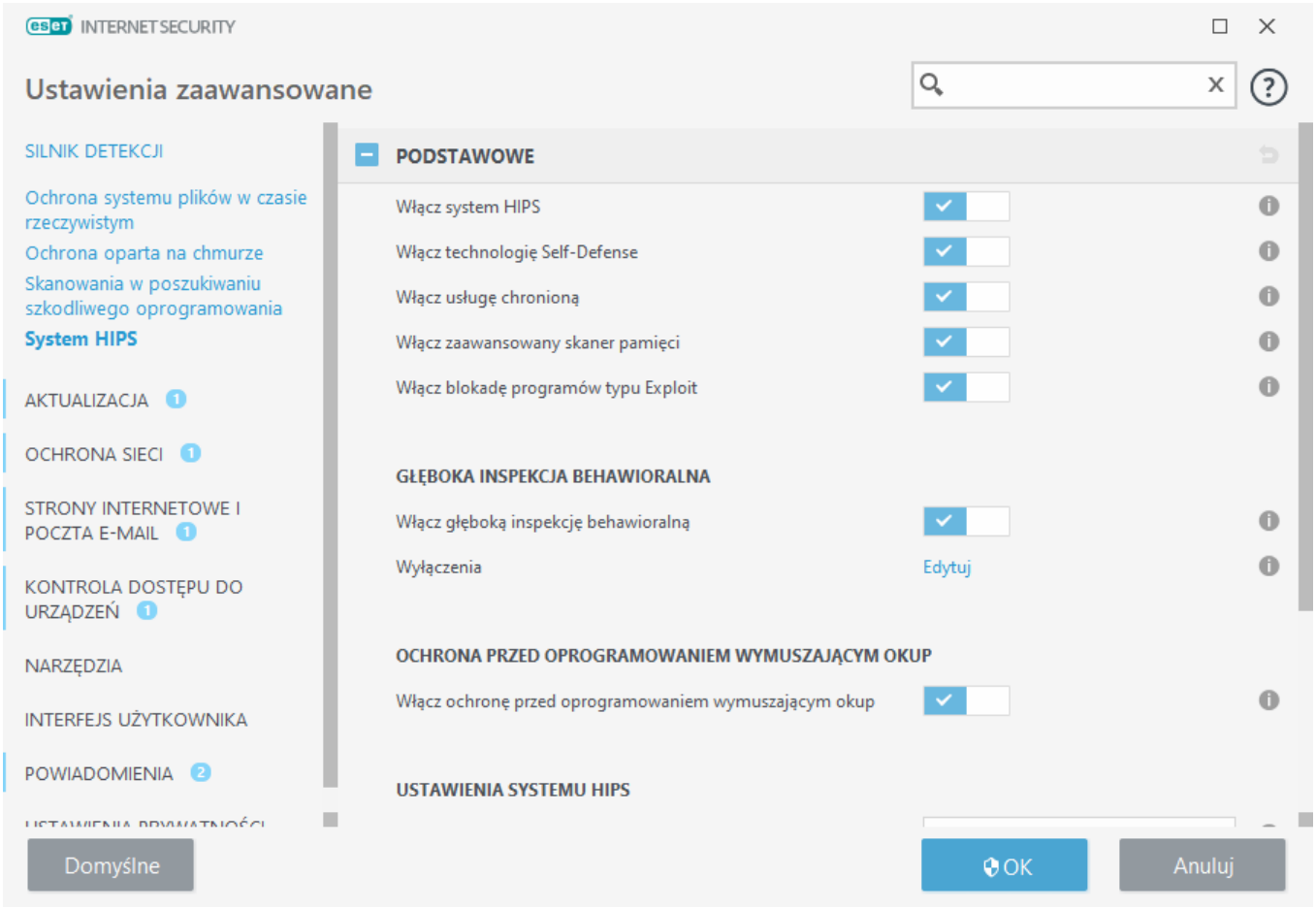
Ilustrowane instrukcje
Jak tworzyć i edytować reguły kamery internetowej w programie ESET Internet Security.

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 (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.

Ustawienia systemu HIPS można znaleźć w obszarze **Ustawienia zaawansowane**(F5) > **Silnik detekcji** > **System HIPS** > **Podstawowe**. Stan systemu HIPS (włączony/wyłączony) widoczny jest w oknie głównym programu ESET Internet Security w obszarze **Ustawienia** > **Ochrona komputera**.



Podstawowe

Włącz system HIPS — w programie ESET Internet Security system HIPS jest domyślnie włączony. Wyłączenie go

spowoduje dezaktywację pozostałych funkcji systemu HIPS, takich jak Blokada programów typu Exploit.

Włącz technologię Self-Defense — program ESET Internet Security ma wbudowaną technologię **Self-Defense**, która stanowi element systemu HIPS i zapobiega uszkodzeniu lub wyłączeniu ochrony antywirusowej oraz antyspyware przez szkodliwe oprogramowanie. Technologia Self-Defense chroni przed modyfikacją najważniejsze procesy systemowe i procesy oprogramowania ESET, klucze rejestru oraz pliki.

Włącz usługę chronioną – włącza ochronę usługi ESET (ekrn.exe). Po włączeniu usługa jest uruchamiana jako chroniony proces systemu Windows w celu ochrony przed atakami szkodliwego oprogramowania. Ta opcja jest dostępna w systemie Windows 8.1 i lub nowszy.

Włącz 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 takim 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.

Włącz blokadę programów typu Exploit — ta opcja ma na celu wzmocnienie ochrony typów aplikacji będących często celami ataków, 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.

Głęboka inspekcja behawioralna

Włącz głęboką inspekcję behawioralną — kolejna warstwa ochrony w ramach funkcji HIPS. To rozszerzenie HIPS analizuje zachowanie wszystkich programów działających na komputerze i ostrzega, jeśli to zachowanie jest szkodliwe.

Wyłączenia systemu HIPS z głębokiej inspekcji behawioralnej pozwalają wykluczyć z analizy wybrane procesy. Aby zapewnić skanowanie wszystkich procesów pod kątem zagrożeń, zaleca się tworzenie wyłączeń tylko wtedy, gdy jest to absolutnie konieczne.

Ochrona przed oprogramowaniem wymuszającym okup

Włącz ochronę przed oprogramowaniem wymuszającym okup — kolejna warstwa ochrony będąca elementem systemu HIPS. Aby ochrona przed oprogramowaniem wymuszającym okup mogła działać, należy włączyć system reputacji ESET LiveGrid®. Dowiedz się więcej na temat ochrony tego typu.

Ustawienia HIPS

Tryb filtrowania może działać w jednym z następujących trybów:

Tryb filtrowania	Opis
Tryb automatyczny	dozwolone są wszystkie operacje z wyjątkiem operacji zablokowanych przez wstępnie zdefiniowane reguły chroniące komputer.
Tryb inteligentny	użytkownik będzie powiadamiany wyłącznie o szczególnie podejrzanych zdarzeniach.
Tryb interaktywny	Użytkownik jest monitowany o potwierdzenie operacji.
Tryb oparty na regułach	blokuje wszystkie operacje niezdefiniowane przez określoną regułę, która na nie zezwala.

Tryb filtrowania	Opis
Tryb uczenia się	Operacje są włączane, a po każdej operacji tworzona jest reguła. Reguły utworzone w tym trybie można przeglądać w oknie edytora **reguł systemu HIPS**. Mają one niższy priorytet niż reguły utworzone ręcznie i reguły utworzone w trybie automatycznym. Po wybraniu **trybu uczenia się** z menu rozwijanego **trybu filtrowania** udostępnione zostanie ustawienie **Termin zakończenia trybu 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 ustawiany po zakończeniu trybu uczenia się — umożliwia wybranie trybu filtrowania, który będzie stosowany po zakończeniu trybu uczenia się. Po zakończeniu tego trybu opcja **Zapytaj użytkownika** będzie wymagać uprawnień administracyjnych, aby wprowadzić zmiany w trybie filtrowania systemu HIPS.

System HIPS monitoruje zdarzenia w systemie operacyjnym i reaguje na nie na podstawie reguł podobnych do reguł używanych przez zaporę. Kliknięcie opcji **Edytuj** obok pozycji **Reguły** powoduje otwarcie okna edytora **reguł systemu HIPS**. W oknie zarządzania regułami systemu HIPS można dodawać, edytować oraz usuwać reguły. Więcej informacji na temat tworzenia reguł i operacji systemu HIPS zawiera artykuł Edytowanie reguły HIPS.

Okno interaktywne systemu HIPS

Okno powiadomień systemu HIPS 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.

Reguły utworzone w oknie powiadomień są traktowane tak samo jak reguły utworzone ręcznie. Reguła utworzona z poziomu okna powiadomień może być ogólniejsza niż reguła, która spowodowała otwarcie tego okna dialogowego. Oznacza to, że po utworzeniu reguły w oknie dialogowym ta sama operacja może spowodować otwarcie tego samego okna. Więcej informacji zawiera artykuł Priorytet reguł systemu HIPS.

Jeśli czynnością domyślną ustawioną dla danej reguły jest **Pytaj za każdym razem**, 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.

Opcja **Zapamiętaj do zamknięcia aplikacji** powoduje stosowanie czynności (**Zezwól/Odmów**) do czasu zmiany reguł lub trybu filtrowania, aktualizacji modułu systemu HIPS lub ponownego uruchomienia systemu. Po wystąpieniu dowolnej z tych trzech czynności reguły zostają tymczasowe usunięte.

Opcja **Utwórz regułę i zapamiętaj na stałe** spowoduje utworzenie nowej reguły systemu HIPS, którą później będzie można zmienić w sekcji Zarządzanie regułami systemu HIPS (wymaga uprawnień administracyjnych).

Kliknięcie przycisku **Szczegóły** u dołu pozwala sprawdzić, jaka aplikacja wyzwoliła daną operację, jaka jest reputacja pliku lub jakiej operacji dotyczy pytanie o zezwolenie bądź odmowę.

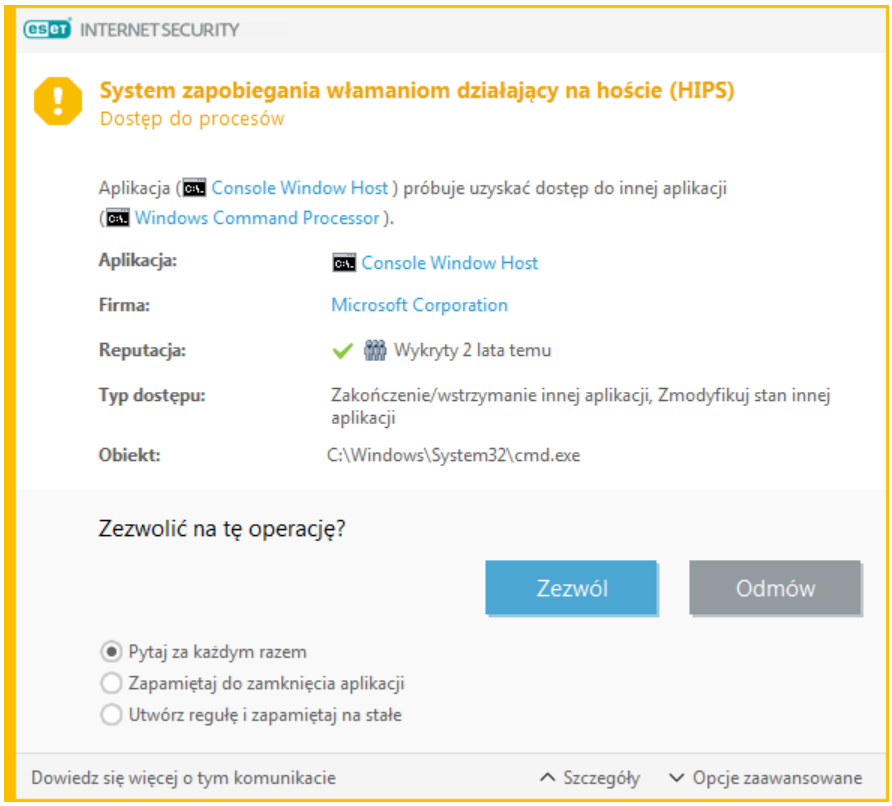
Aby otworzyć ustawienia dotyczące bardziej szczegółowych parametrów reguł, należy kliknąć pozycję **Opcje zaawansowane**. W przypadku wybrania opcji **Utwórz regułę i zapamiętaj na stałe** dostępne będą poniższe opcje:

- **Utwórz regułę obowiązującą tylko dla tej aplikacji** — zaznaczenie tego pola wyboru spowoduje utworzenie reguły dla wszystkich aplikacji źródłowych.
- **Tylko dla operacji** — pozwala wybrać operacje dotyczące plików/aplikacji/rejestru dla reguły. Zobacz opisy

wszystkich operacji systemu HIPS.

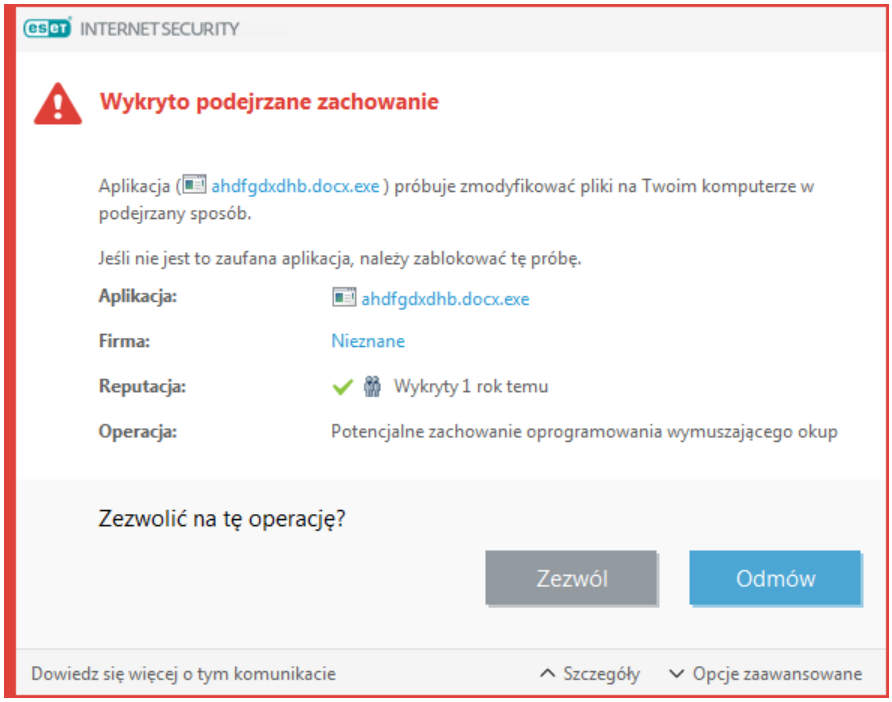
- **Tylko dla elementu docelowego** — pozwala wybrać elementy docelowe dotyczące plików/aplikacji/rejestru dla reguły.

> **Ciągłe powiadomienia systemu HIPS?**
> Aby nie dostawać cały czas kolejnych powiadomień, należy zmienić tryb filtrowania na **Tryb automatyczny** w obszarze **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **System HIPS** > **Podstawowe**.



Wykryto potencjalne zachowanie oprogramowania wymuszającego okup

To okno interaktywne jest wyświetlane w przypadku wykrycia potencjalnego zachowania oprogramowania wymuszającego okup. Można wybrać opcję **Odmów** lub **Zezwól**.



Kliknięcie pozycji **Szczegóły** umożliwia wyświetlenie szczegółów parametrów wykrywania. Korzystając z okna dialogowego, można **przesłać plik do analizy** lub **wyłączyć go z wykrywania**.

Aby można było zapewnić prawidłowe działanie funkcji Ochrona przed oprogramowaniem wymuszającym okup, funkcja ESET LiveGrid® musi być włączona.

Zarządzanie regułami systemu HIPS

Lista zdefiniowanych przez użytkownika lub dodanych automatycznie reguł z systemu HIPS. Bardziej szczegółowe informacje o tworzeniu reguł i działaniu systemu HIPS można znaleźć w rozdziale Ustawienia reguł systemu HIPS. Zobacz też: Ogólna zasada działania systemu HIPS.

Kolumny

Reguła — nazwa reguły podana przez użytkownika lub wybrana automatycznie.

Włączona — przesuń suwak w pozycję wyłączenia, jeśli chcesz pozostawić regułę na liście, ale nie chcesz jej używać.

Czynność — określona przez regułę czynność (**Zezwól**, **Blokuj** lub **Pytaj**), która ma zostać wykonana, gdy spełnione są warunki.

Źródła — reguła będzie stosowana tylko, jeśli zdarzenie zostanie spowodowane przez wymienione aplikacje.

Obiekty docelowe — reguła będzie stosowana tylko, gdy dana operacja będzie związana z określonym plikiem, aplikacją lub wpisem rejestru.

Stopień szczegółowości zapisywania w dzienniku — uruchomienie tej opcji spowoduje, że informacje o regule będą zapisywane w dzienniku systemu HIPS.

Powiadom — po wywołaniu zdarzenia w prawym dolnym rogu ekranu zostanie wyświetlone małe wyskakujące

okno.

Elementy sterujące

Dodaj — umożliwia utworzenie nowej reguły.

Edytuj — pozwala edytować zaznaczone elementy.

Usuń — służy do usuwania zaznaczonych elementów.

Priorytet reguł systemu HIPS

Nie są dostępne opcje umożliwiające dostosowanie poziomu priorytetu reguł systemu HIPS przy użyciu przycisków W górę/W dół (jak w przypadku reguł zapory, które reguły są wykonywane kolejno od góry do dołu).

- Wszystkie tworzone reguły mają taki sam priorytet
- Im bardziej szczegółowa jest reguła, tym wyższy ma priorytet (np. reguła dotycząca konkretnej aplikacji ma wyższy priorytet niż reguła dotycząca wszystkich aplikacji)
- W systemie HIPS istnieją reguły wewnętrzne o wyższym priorytecie, które nie są dostępne dla użytkownika (np. nie można zastąpić reguł zdefiniowanych przez technologię Self-Defense)
- Reguła mogąca spowodować zatrzymanie działania systemu operacyjnego nie zostanie zastosowana (będzie miała najniższy priorytet)

Edytowanie reguły HIPS

Najpierw zobacz artykuł Zarządzanie regułami systemu HIPS.

Nazwa reguły — nazwa reguły podana przez użytkownika lub wybrana automatycznie.

Czynność — określona czynność (**Zezwól**, **Blokuj** lub **Pytaj**), która ma zostać wykonana, gdy spełnione są warunki.

Operacje dotyczące — należy wybrać typ operacji, do której stosowana będzie reguła. Reguła będzie stosowana tylko w przypadku podanego typu operacji i wybranego elementu.

Włączona — przesuń suwak w pozycję wyłączenia, jeśli chcesz pozostawić regułę na liście, ale nie chcesz jej używać.

Stopień szczegółowości zapisywania w dzienniku — uruchomienie tej opcji spowoduje, że informacje o regule będą zapisywane w dzienniku systemu HIPS.

Powiadom użytkownika — po wywołaniu zdarzenia w prawym dolnym rogu ekranu zostanie wyświetlone małe wyskakujące okno.

Reguła składa się z części, które opisują warunki powodujące jej wywołanie:

Aplikacje źródłowe— reguła będzie stosowana tylko, jeśli zdarzenie zostanie spowodowane przez wymienione aplikacje. W celu dodania nowych plików należy wybrać z menu rozwijanego opcję **Określone aplikacje** i kliknąć opcję **Dodaj**. Aby dodać wszystkie aplikacje, można wybrać z menu rozwijanego opcję **Wszystkie aplikacje**.

Pliki docelowe — reguła będzie stosowana tylko wtedy, gdy operacja będzie dotyczyła określonego elementu docelowego. W celu dodania nowych plików lub folderów należy wybrać z menu rozwijanego opcję **Określone pliki** i kliknąć przycisk **Dodaj**. W celu dodania wszystkich aplikacji można wybrać z menu rozwijanego opcję **Wszystkie pliki**.

Wpisy rejestru — reguła będzie stosowana tylko wtedy, gdy operacja będzie dotyczyła określonego elementu docelowego. W celu dodania nowych plików lub folderów należy wybrać z menu rozwijanego opcję **Określone aplikacje** i kliknąć przycisk **Dodaj**. W celu dodania wszystkich aplikacji można wybrać z menu rozwijanego opcję **Wszystkie aplikacje**.

Wpisy rejestru — reguła będzie stosowana tylko wtedy, gdy operacja będzie dotyczyła określonego elementu docelowego. W celu wybrania klucza w rejestrze należy wybrać z menu rozwijanego opcję **Określone wpisy** i kliknąć przycisk **Dodaj**, aby wpisać go ręcznie. Można też kliknąć opcję **Otwórz edytor rejestru**, aby wybrać klucz z rejestru. Można także wyprać z menu rozwijanego opcję **Wszystkie wpisy**, aby dodać wszystkie aplikacje.

> Niektórych operacji dotyczących określonych reguł wstępnie zdefiniowanych w systemie HIPS nie można blokować i są one domyślnie dozwolone. Ponadto nie wszystkie operacje systemowe są monitorowane przez moduł HIPS. System HIPS monitoruje operacje, które można uznać za niebezpieczne.

Opisy ważnych operacji:

Operacje na plikach

- **Usunięcie pliku** — aplikacja monituje o zezwolenie na usunięcie pliku docelowego.
- **Zapis do pliku** — aplikacja monituje o zezwolenie na zapis do pliku docelowego.
- **Bezpośredni dostęp do dysku** — aplikacja próbuje dokonywać odczytu z dysku lub zapisu na dysku w niestandardowy sposób omijający standardowe procedury systemu Windows. Może to spowodować modyfikacje plików bez zastosowania odpowiednich reguł. Ta operacja może być spowodowana przez szkodliwe oprogramowanie próbujące uniknąć wykrycia, program do tworzenia kopii zapasowych próbujący wykonać dokładną kopię dysku lub program do zarządzania partycjami próbujący zmienić układ woluminów dyskowych.
- **Instalacja globalnego punktu zaczepienia** — wskazuje na wywołanie funkcji SetWindowsHookEx z biblioteki MSDN.
- **Ładowanie sterownika** — instalowanie i ładowanie sterowników w systemie.

Operacje na aplikacjach

- **Debugowanie innej aplikacji** — dołączenie debugera do procesu. Podczas debugowania aplikacji można odczytać i zmodyfikować wiele szczegółów związanych z jej działaniem oraz uzyskać dostęp do jej danych.
- **Przechwytywanie zdarzeń z innej aplikacji** — aplikacja źródłowa próbuje przechwycić zdarzenia skierowane do określonej aplikacji (na przykład program rejestrujący znaki wprowadzane na klawiaturze próbuje przechwycić zdarzenia przeglądarki internetowej).
- **Zakończenie/wstrzymanie innej aplikacji** — zawieszenie, wznowienie lub zakończenie procesu (dostęp można uzyskać bezpośrednio z Eksploratora procesów lub okienka Procesy).

• **Uruchomienie nowej aplikacji** — uruchamianie nowych aplikacji lub procesów.

• **Modyfikacja stanu innej aplikacji** — aplikacja źródłowa próbuje dokonać zapisu w pamięci aplikacji docelowych lub uruchomić kod w ich imieniu. Ta funkcja może być przydatna do zapewnienia ochrony ważnej aplikacji przez skonfigurowanie tej aplikacji jako docelowej w regule blokującej korzystanie z tej operacji.

Nie można przechwytywać operacji procesów w 64-bitowej wersji systemu Windows XP.

Operacje na rejestrze

• **Zmiana ustawień uruchamiania** — dowolne zmiany w ustawieniach określających, które aplikacje będą uruchamiane podczas uruchamiania systemu Windows. Można je znaleźć, przeszukując na przykład klucz Run w rejestrze systemu Windows.

• **Usunięcie z rejestru** — usunięcie klucza rejestru lub jego wartości.

• **Zmiana nazwy klucza rejestru** — zmiana nazw kluczy rejestru.

• **Modyfikacja rejestru** — tworzenie nowych wartości kluczy rejestru, zmienianie istniejących wartości, przenoszenie danych w drzewie bazy danych lub ustawianie praw użytkowników lub grup do kluczy rejestru.

Podając obiekt docelowy, można stosować symbole wieloznaczne z pewnymi ograniczeniami. W ścieżkach rejestru można zamiast konkretnego klucza stosować znak * (gwiazdka). Na przykład ścieżka *HKEY_USERS*\software* może oznaczać *HKEY_USER\.default\software*, ale nie *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*.
*HKEY_LOCAL_MACHINE\system\ControlSet** nie jest dozwoloną ścieżką klucza rejestru. Ścieżka klucza rejestru zakończona znakami * oznacza „ta ścieżka lub dowolna ścieżka na dowolnym poziomie po tym symbolu”. Jest to jedyny sposób stosowania symboli wieloznacznych w przypadku ścieżek plików. Najpierw sprawdzana jest konkretna część ścieżki, a następnie ścieżka odpowiadająca symbolowi wieloznacznemu (*).

W przypadku utworzenia bardzo ogólnej reguły, zostanie wyświetlone ostrzeżenie dotyczące tego typu reguł.

W poniższym przykładzie pokazano, jak ograniczyć niepożądane działanie konkretnej aplikacji:

1. Nadaj nazwę regule i w menu rozwijanym **Czynność** wybierz polecenie **Blokuj** (lub **Zapytaj**, jeśli chcesz podjąć decyzję później).

2. Przesuń suwak obok pozycji **Powiadom użytkownika**, aby powiadomienie było wyświetlane zawsze po zastosowaniu reguły.

3. Wybierz co najmniej jedną operację w sekcji **Operacje dotyczące**, której będzie dotyczyć reguła.

4. Kliknij przycisk **Dalej**.

5. W oknie **Aplikacje źródłowe** z menu rozwijanego wybierz opcję **Określone aplikacje**, aby zastosować nową regułę do wszystkich aplikacji próbujących wykonać dowolną z wybranych operacji dotyczących podanych aplikacji.

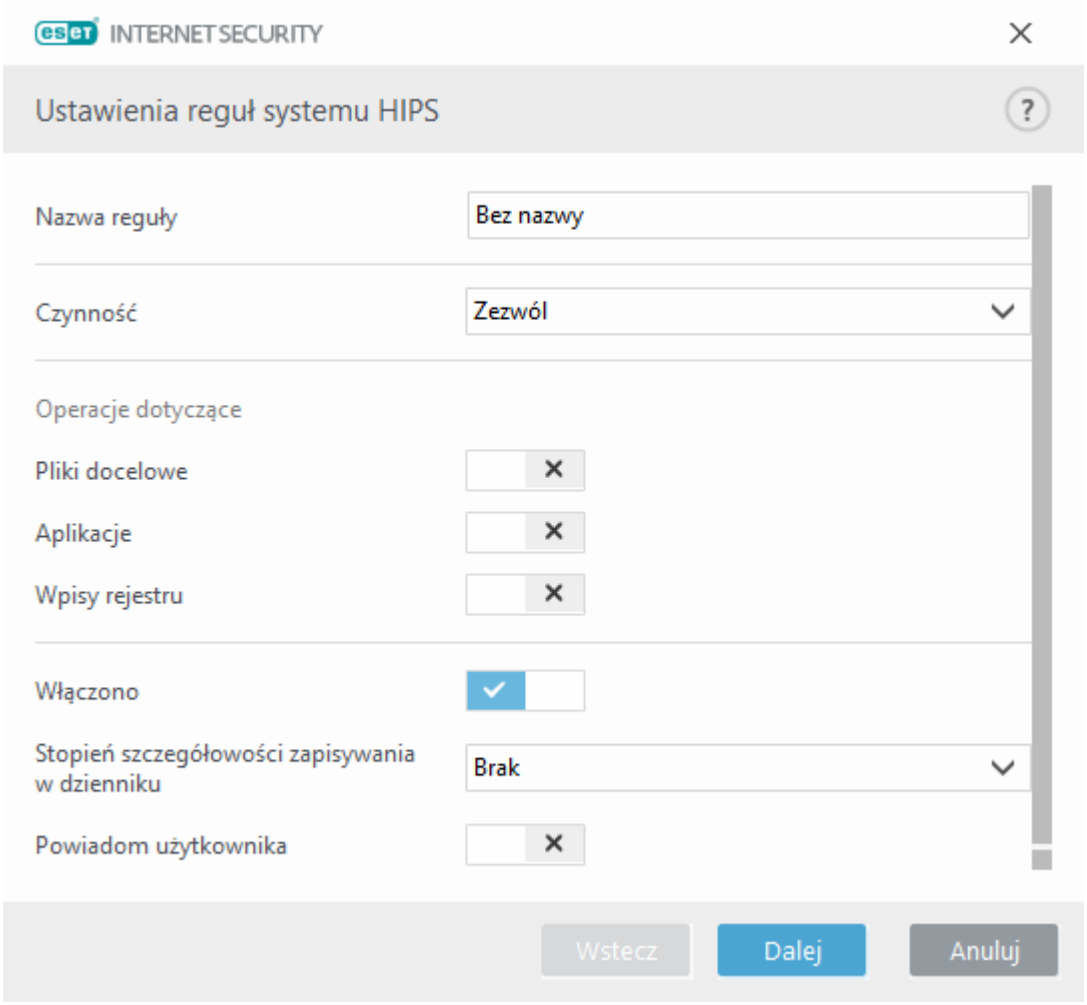
6. Kliknij przycisk **Dodaj**, a następnie kliknij pozycję **...**, wybierz ścieżkę do określonej aplikacji i naciśnij przycisk

OK. W razie potrzeby dodaj więcej aplikacji.
Przykład: *C:\Program Files (x86)\Untrusted application\application.exe*

7. Wybierz operację **Zapis do pliku**.

8. Z menu rozwijanego wybierz opcję **Wszystkie pliki**. Spowoduje to zablokowanie wszelkich prób zapisu w dowolnych plikach przez aplikacje wybrane w poprzednim punkcie.

9. Kliknij przycisk **Zakończ**, aby zapisać nową regułę.



Dodawanie ścieżki aplikacji/rejestru dla systemu HIPS

Kliknięcie opcji **...** umożliwia wybranie ścieżki do pliku aplikacji. Wybranie folderu spowoduje uwzględnienie wszystkich znajdujących się w nim aplikacji.

Opcja **Otwórz edytor rejestru** służy do uruchamiania edytora rejestru systemu Windows (regedit). Podczas dodawania ścieżki rejestru należy podać właściwą lokalizację w polu **Wartość**.

Przykładowe ścieżki pliku i rejestru:

- *C:\Program Files\Internet Explorer\iexplore.exe*
- *HKEY_LOCAL_MACHINE\system\ControlSet*

Ustawienia zaawansowane systemu HIPS

Poniższe opcje są przydatne podczas debugowania i analizowania działania aplikacji:

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

Rejestruj wszystkie zablokowane operacje — wszystkie zablokowane operacje zostaną zapisane w dzienniku systemu HIPS. Tej funkcji należy używać tylko w przypadku rozwiązywania problemów lub na żądanie pomocy technicznej firmy ESET, ponieważ może to wygenerować ogromny plik dziennika i spowolnić działanie komputera.

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.

Sterowniki, które mogą być ładowane

Sterowniki wyszczególnione na tej liście mogą być ładowane zawsze, niezależnie od trybu filtrowania HIPS, chyba że zostaną wyraźnie zablokowane przez regułę ustaloną przez użytkownika.

Dodaj — umożliwia dodanie nowego sterownika.

Edytuj — umożliwia edytowanie wybranego sterownika.

Usuń — umożliwia usunięcie sterownika z listy.

Resetuj — powoduje ponowne załadowanie zestawu sterowników systemowych.

Jeśli sterowniki dodane przez użytkownika ręcznie nie mają być uwzględniane, należy kliknąć opcję **Resetuj**. Ta opcja może być przydatna, gdy użytkownik dodał kilka sterowników i nie chce usuwać ich z listy ręcznie.

Tryb gier

Tryb gier to funkcja przeznaczona dla użytkowników, którzy wymagają niczym niezakłócanego dostępu do swojego oprogramowania, chcą zablokować wszelkie wyskakujące okienka i zależy im na zmniejszeniu obciążenia procesora (CPU). Tryb gier może być również wykorzystywany podczas prezentacji, które nie mogą być przerywane działaniem programu antywirusowego. Po włączeniu tej funkcji wszystkie wyskakujące okienka zostaną wyłączone i zostanie całkowicie zatrzymane działanie harmonogramu. Ochrona systemu pozostanie aktywna w tle, ale nie będzie wymagać interwencji użytkownika.

Możesz włączyć lub wyłączyć tryb gier w głównym oknie programu, wybierając **Ustawienia** > **Ochrona komputera**, a następnie klikając lub obok pozycji **Tryb gier**. Włączenie trybu gier 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 gier jest aktywny** wyświetlanego na pomarańczowo.

Włączenie opcji **Włącz tryb gier automatycznie przy uruchamianiu aplikacji w trybie pełnoekranowym** w obszarze **Ustawienia zaawansowane** (F5) > **Narzędzia** > **Tryb gier** umożliwia włączanie trybu gier przy każdym uruchomieniu aplikacji pełnoekranowej i wyłączanie tego trybu po zakończeniu działania takiej aplikacji.

Włączenie opcji **Automatycznie wyłącz tryb gier po** umożliwia zdefiniowanie czasu, po którym tryb gier jest automatycznie wyłączany.

> Jeśli zapora działa w trybie interaktywnym i jest włączony tryb gier, 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 gier interakcja z użytkownikiem jest wyłączona. Aby zezwolić na komunikację, należy zdefiniować regułę komunikacji dla każdej aplikacji, w przypadku której może wystąpić ten problem, lub użyć innego trybu filtrowania w zaporze. Należy pamiętać, że jeśli przy włączonym trybie gier zostanie otwarta strona internetowa lub aplikacja mogąca stanowić zagrożenie bezpieczeństwa, jej ewentualnemu zablokowaniu nie będzie towarzyszyć żaden komunikat ani ostrzeżenie, ponieważ interakcja ze strony użytkownika jest wyłączona.

Skanowanie przy uruchamianiu

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

Opcje skanowania podczas uruchamiania systemu są częścią zadania zaplanowanego **Sprawdzanie plików wykonywanych przy uruchamianiu systemu**. Aby zmodyfikować ustawienia, należy wybrać kolejno opcje **Narzędzia** > **Więcej narzędzi** > **Harmonogram**, kliknąć opcję **Automatyczne sprawdzanie plików przy uruchamianiu** , a następnie wybrać opcję **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.

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 **Skanuj obiekt docelowy** można określić dokładność skanowania plików używanych 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 ustalane dla każdej grupy powyżej. Jeśli wybierzesz niższą głębokość skanowania dla plików uruchamianych podczas rozruchu systemu, nieprzeskanowane pliki zostaną przeskanowane po otwarciu lub wykonaniu.

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.

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.

W celu aktywowania ochrony dokumentów otwórz okno **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Skanowanie w poszukiwaniu szkodliwego oprogramowania** > **Ochrona dokumentów** i kliknij suwak obok opcji **Włącz ochronę dokumentów**.

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

Wyłączenia

Wyłączenia pozwalają wykluczyć wybrane obiekty z silnika detekcji. Aby zapewnić skanowanie wszystkich obiektów, 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.

Pliki i foldery wyłączone ze skanowania pozwalają wykluczyć ze skanowania określone pliki i foldery. Ta opcja jest przydatna, jeśli trzeba wyłączyć ze skanowania konkretne elementy na poziomie plików — np. w aplikacjach dla graczy lub w przypadku niezwykłego zachowania systemu czy też chęci zwiększenia wydajności.

Zaawansowana konfiguracja wyłączeń umożliwia wykluczenie obiektów z wykrycia przy użyciu nazwy wykrycia, ścieżki lub skrótu. Nie polega natomiast na wyłączaniu plików i folderów ze skanowania, jak to ma miejsce w przypadku opcji Pliki i foldery wyłączone ze skanowania. Zaawansowana konfiguracja wyłączeń powoduje wyłączanie obiektów, tylko jeśli zostaną wykryte przez silnik detekcji, a na liście wyłączeń będzie obecna odpowiednia reguła.

Nie należy tego mylić z innymi typami wyłączeń:

- Wyłączenia procesów — ze skanowania są wyłączone wszystkie operacje na plikach związane z procesami wyłączonej aplikacji (może być to wymagane w celu przyspieszenia tworzenia kopii zapasowej i poprawienia dostępności usług).
- Wyłączenia rozszerzeń plików
- Wyłączenia systemu HIPS
- Filtr wyłączeń w ramach ochrony opartej na chmurze

Pliki i foldery wyłączone ze skanowania

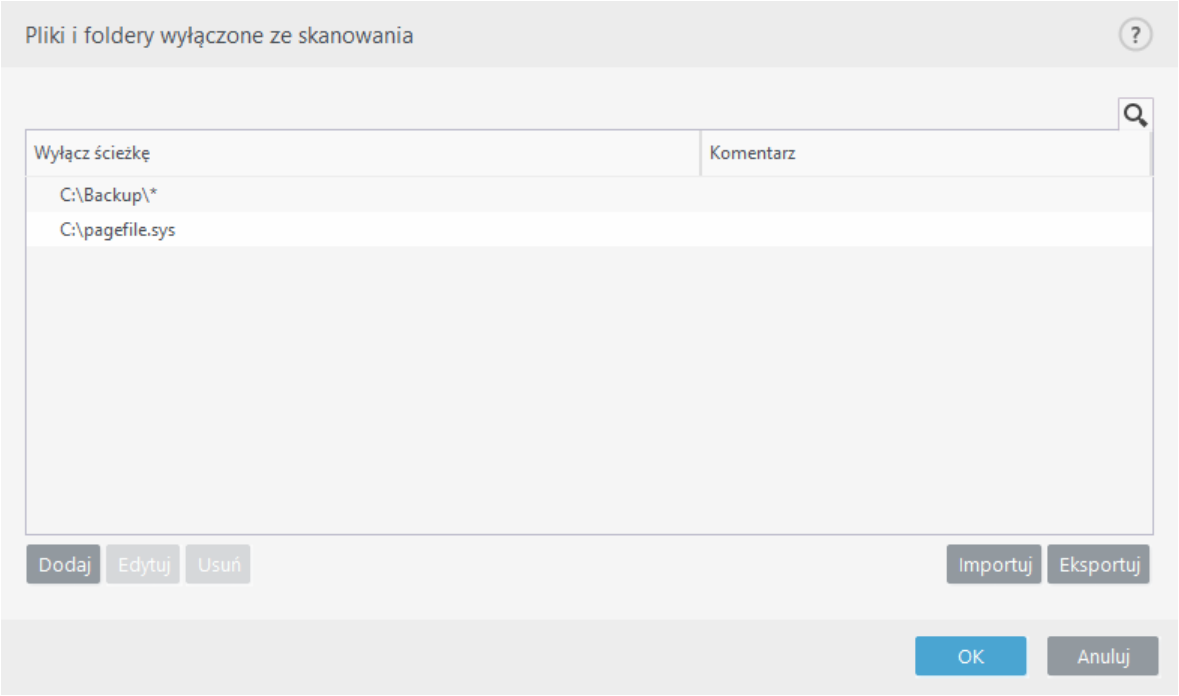
Ta opcja umożliwia wyłączenie ze skanowania określonych plików i folderów.

Aby zapewnić skanowanie wszystkich obiektów pod kątem zagrożeń, zaleca się tworzenie wyłączeń tylko wtedy, gdy jest to absolutnie konieczne. Istnieją jednak sytuacje, w których może być konieczne wykluczenie obiektu, na przykład dużych baz danych, które spowolniłyby pracę komputera podczas skanowania, lub w przypadku oprogramowania, które powoduje konflikt ze skanowaniem.

Aby dodać do listy wyłączeń pliki i foldery, które mają zostać wyłączone ze skanowania, należy wybrać kolejno **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Wyłączenia** > **Pliki i foldery wyłączone ze skanowania** > **Edytuj**.

> Należy pamiętać, że zaawansowana konfiguracja wyłączeń, wyłączenia rozszerzeń plików, wyłączenia systemu HIPS i wyłączenia procesów to różne zagadnienia.

Aby wyłączyć obiekt (ścieżkę: plik lub folder) ze skanowania, należy kliknąć przycisk **Dodaj** i wprowadzić odpowiednią ścieżkę lub wybrać obiekt w strukturze drzewa.



Zagrożenie w pliku nie zostanie wykryte przez moduł **Ochrona systemu plików w czasie rzeczywistym** ani moduł **Skanowania komputera**, jeśli plik spełnia kryteria wykluczenia ze skanowania.

Elementy sterujące

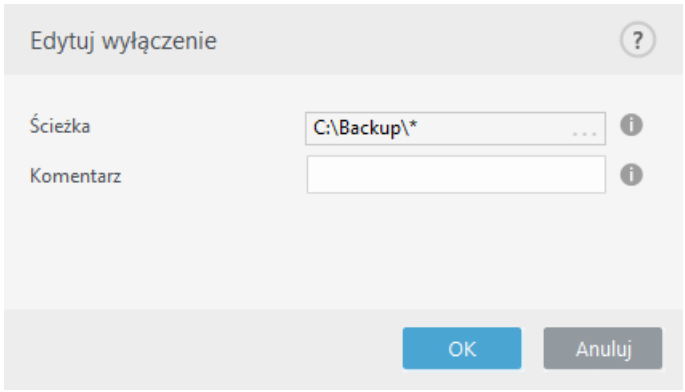
- **Dodaj** — pozwala dodać obiekty, które mają być pomijane podczas wykrywania.
- **Edytuj** — pozwala edytować zaznaczone elementy.
- **Usuń** — służy do usuwania zaznaczonych elementów (CTRL + kliknięcie pozwala zaznaczyć wiele elementów).

Dodawanie i edytowanie wyłączeń dotyczących wydajności

W tym oknie dialogowym można wyłączyć określoną ścieżkę (plik lub katalog) na danym komputerze.

Wybieranie lub ręczne wpisywanie ścieżki

Aby wybrać odpowiednią ścieżkę, należy kliknąć symbol **...** w polu **Ścieżka**.
W przypadku ręcznego podawania ścieżki warto skorzystać z przykładów formatów wyłączeń przedstawionych poniżej.



Aby wyłączyć grupę plików, można użyć symboli wieloznacznych. Znak zapytania (*?*) reprezentuje jeden znak, a gwiazdka (***) reprezentuje ciąg złożony z dowolnej liczby znaków (w tym ciąg pusty).

Format wyłączeń ze skanowania

• Aby wyłączyć ze skanowania wszystkie pliki z danego folderu lub podfolderu, należy wpisać ścieżkę do tego folderu i zastosować maskę *

• 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 brakujące lub nieznane znaki)

Przykłady:

• *C:\Tools** — na końcu ścieżki należy umieścić ukośnik wsteczny (\) i gwiazdkę (*), aby wskazać, że wyłączenie ma obejmować całą zawartość folderu (pliki i podfoldery).

• *C:\Tools*.** — taki zapis spowoduje działanie takie samo, jak w przypadku *C:\Tools**

• *C:\Tools* — folder *Tools* nie zostanie wyłączony. Dla skanera *Tools* może być także nazwą pliku.

• *C:\Tools*.dat* — taki zapis spowoduje wyłączenie plików .dat w folderze *Tools*.

• *C:\Tools\sg.dat* — ten zapis spowoduje wyłączenie tego konkretnego pliku znajdującego się w podanej ścieżce.

Zmienne systemowe w wyłączeniach

Definiując wyłączenia ze skanowania, można używać zmiennych systemowych, takich jak %PROGRAMFILES%.

- Aby wyłączyć ze skanowania folder Program Files za pomocą tej zmiennej systemowej, podczas dodawania folderu do wyłączeń należy użyć następującej ścieżki: *%PROGRAMFILES%** (pamiętając o dodaniu ukośnika wstecznego i gwiazdki na końcu ścieżki).
- Aby wyłączyć ze skanowania wszystkie pliki i foldery z podkatalogu *%PROGRAMFILES%*, należy użyć ścieżki *%PROGRAMFILES%\wyłączony_katalog**

Rozwiń listę obsługiwanych zmiennych systemowych

W ścieżce wyłączenia można używać następujących zmiennych:

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

Nie są obsługiwane zmienne systemowe specyficzne dla użytkownika (np. *%TEMP%* lub *%USERPROFILE%*) ani zmienne środowiskowe (np. *%PATH%*).

Symbole wieloznaczne wewnątrz ścieżki nie są obsługiwane

Używanie symboli wieloznacznych w środku ścieżki (na przykład *C:\Tools*\Data\file.dat*) może działać prawidłowo, ale nie jest oficjalnie obsługiwane dla plików i folderów wyłączonych ze skanowania z uwagi na wydajność. Zobacz następujący artykuł bazy wiedzy, aby uzyskać więcej informacji.

W przypadku zaawansowanej konfiguracji wyłączeń nie ma ograniczeń dotyczących używania symboli wieloznacznych w środku ścieżki.

Kolejność wyłączeń

- Nie ma opcji umożliwiających dostosowanie poziomu priorytetu wyłączeń przy użyciu przycisków W górę/W dół (jak w przypadku reguł zapory, które reguły są wykonywane kolejno od góry do dołu).
- Kiedy skaner napotka pierwszą regułę, która ma zastosowanie, druga reguła mająca zastosowanie nie zostanie już uwzględniona.
- Im mniej jest reguł, tym szybsze jest skanowanie.
- Nie należy tworzyć reguł równoległych.

Format ścieżki wyłączenia

Aby wyłączyć grupę plików, można użyć symboli wieloznacznych. Znak zapytania (*?*) reprezentuje jeden znak, a gwiazdka (***) reprezentuje ciąg złożony z dowolnej liczby znaków (w tym ciąg pusty).

Format wyłączeń ze skanowania

• Aby wyłączyć ze skanowania wszystkie pliki z danego folderu lub podfolderu, należy wpisać ścieżkę do tego folderu i zastosować maskę *

• 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 brakujące lub nieznane znaki)

Przykłady:

• *C:\Tools** — na końcu ścieżki należy umieścić ukośnik wsteczny (\) i gwiazdkę (*), aby wskazać, że wyłączenie ma obejmować całą zawartość folderu (pliki i podfoldery).

• *C:\Tools*.** — taki zapis spowoduje działanie takie samo, jak w przypadku *C:\Tools**

• *C:\Tools* — folder *Tools* nie zostanie wyłączony. Dla skanera *Tools* może być także nazwą pliku.

• *C:\Tools*.dat* — taki zapis spowoduje wyłączenie plików .dat w folderze *Tools*.

• *C:\Tools\sg.dat* — ten zapis spowoduje wyłączenie tego konkretnego pliku znajdującego się w podanej ścieżce.

Zmienne systemowe w wyłączeniach

Definiując wyłączenia ze skanowania, można używać zmiennych systemowych, takich jak %PROGRAMFILES%.

• Aby wyłączyć ze skanowania folder Program Files za pomocą tej zmiennej systemowej, podczas dodawania folderu do wyłączeń należy użyć następującej ścieżki: *%PROGRAMFILES%** (pamiętając o dodaniu ukośnika wstecznego i gwiazdki na końcu ścieżki).

• Aby wyłączyć ze skanowania wszystkie pliki i foldery z podkatalogu *%PROGRAMFILES%*, należy użyć ścieżki *%PROGRAMFILES%\wyłączony_katalog**

Rozwiń listę obsługiwanych zmiennych systemowych

W ścieżce wyłączenia można używać następujących zmiennych:

• *%ALLUSERSPROFILE%*
• *%COMMONPROGRAMFILES%*
• *%COMMONPROGRAMFILES(X86)%*
• *%COMSPEC%*
• *%PROGRAMFILES%*
• *%PROGRAMFILES(X86)%*
• *%SystemDrive%*
• *%SystemRoot%*
• *%WINDIR%*
• *%PUBLIC%*

Nie są obsługiwane zmienne systemowe specyficzne dla użytkownika (np. *%TEMP%* lub *%USERPROFILE%*) ani zmienne środowiskowe (np. *%PATH%*).

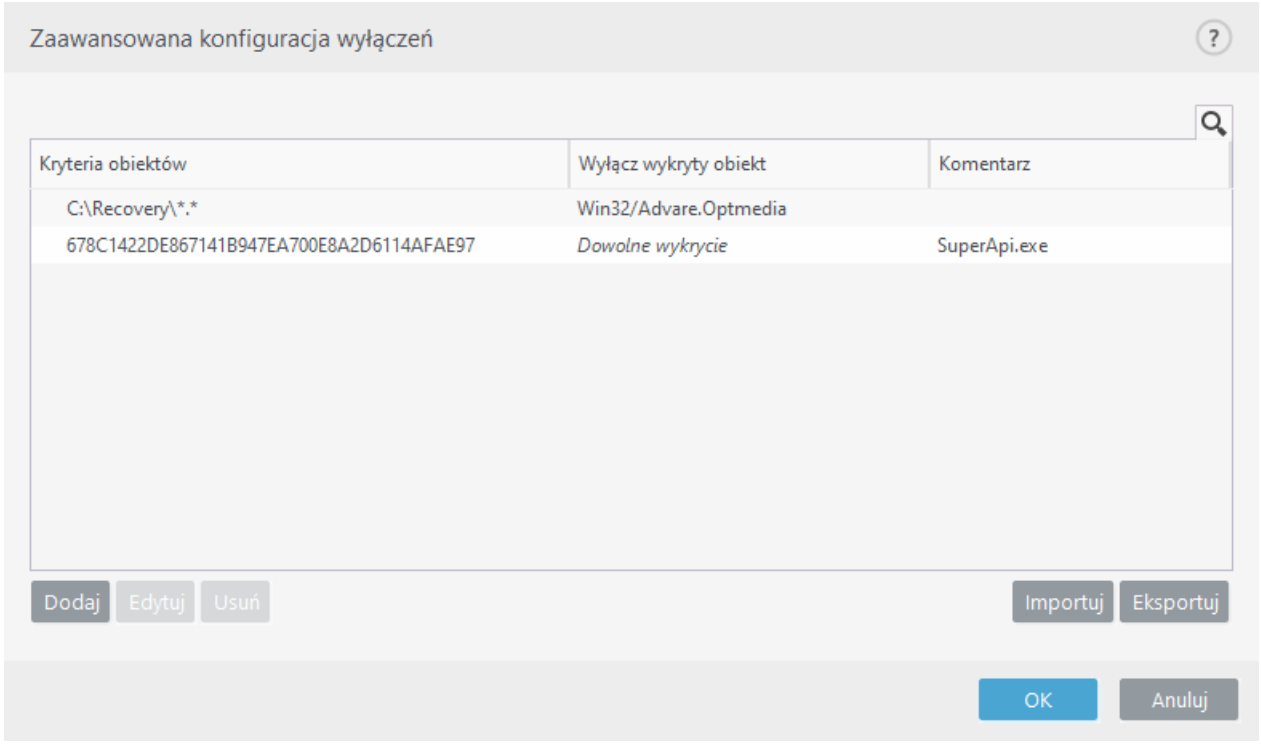
Zaawansowana konfiguracja wyłączeń

Zaawansowana konfiguracja wyłączeń umożliwia wyłączenie obiektów z wykrycia dzięki filtrowaniu nazwy wyłączenia, ścieżki do obiektu lub jego skrótu.

Na czym polega zaawansowana konfiguracja wyłączeń

Zaawansowana konfiguracja wyłączeń nie polega na wyłączaniu plików i folderów ze skanowania, jak to ma miejsce w przypadku opcji Pliki i foldery wyłączone ze skanowania. Zaawansowana konfiguracja wyłączeń powoduje wyłączanie obiektów, tylko jeśli zostaną wykryte przez silnik detekcji, a na liście wyłączeń będzie obecna odpowiednia reguła.

Za przykład (patrz pierwszy wiersz na poniższym obrazie) może posłużyć sytuacja, w której obiekt zostanie zidentyfikowany jako Win32/Adware.Optmedia, a wykryty plik to *C:\Recovery\file.exe*. W drugim wierszu każdy plik, który ma odpowiedni skrót SHA-1, zawsze będzie wyłączany bez względu na to, jaka jest nazwa wykrycia.



Aby wszystkie zagrożenia były wykrywane, zalecamy stosowanie zaawansowanej konfiguracji wyłączeń tylko wtedy, gdy jest to bezwzględnie konieczne.

Aby dodać pliki i foldery do listy wyłączeń, należy wybrać kolejno **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Wyłączenia** > **Zaawansowana konfiguracja wyłączeń** > **Edytuj**.

Należy pamiętać, że pliki i foldery wyłączone ze skanowania, wyłączenia rozszerzeń plików, wyłączenia systemu HIPS i wyłączenia procesów to różne zagadnienia.

Aby wyłączyć obiekt (według jego nazwy wyłączenia lub skrótu) z poziomu silnika detekcji, należy kliknąć przycisk **Dodaj**.

W przypadku Potencjalnie niepożądanych aplikacji i Potencjalnie niebezpiecznych aplikacji można również utworzyć wykluczenie przez jego nazwę wykrycia:

- W oknie alertu informującym o wykryciu (kliknij pozycję **Pokaż opcje zaawansowane,** a następnie wybierz pozycję **Wyłącz z wykrywania**).
- Z menu kontekstowego Pliki dziennika wybierz Kreator tworzenia zaawansowanej konfiguracji wyłączeń.
- Klikając **Narzędzia** > **Więcej narzędzi** > **Kwarantanna**, klikając prawym przyciskiem myszy plik poddany kwarantannie i wybierając z menu kontekstowego opcję **Przywróć i wyłącz ze skanowania**.

Zaawansowana konfiguracja wyłączeń — kryteria dotyczące obiektów

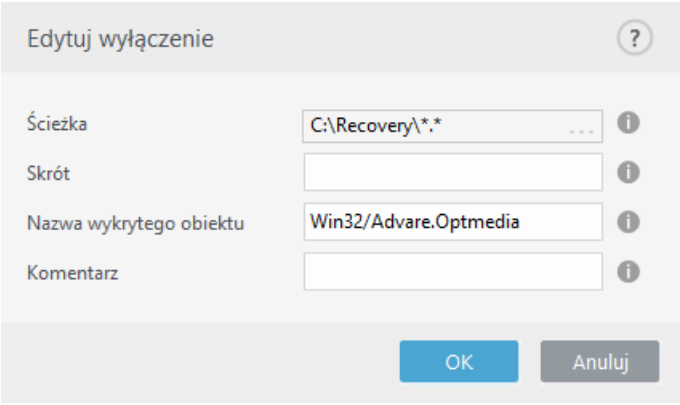
- **Ścieżka** — zaawansowaną konfigurację wyłączeń można ograniczyć do określonej ścieżki.
- **Nazwa wykrycia** — gdy obok wykluczonego pliku widać nazwę wykrycia, oznacza to, że plik będzie pomijany tylko przy wyszukiwaniu danego zagrożenia, a nie całkowicie. Jeśli później plik zostanie zarażony innym szkodliwym oprogramowaniem, moduł antywirusowy to wykryje.
- **Skrót** — wyłącza plik na podstawie określonego skrótu SHA-1 bez względu na typ, lokalizację, nazwę i rozszerzenie pliku.

Dodawanie i edytowanie wyłączeń wykryć

Wyłącz wykryty obiekt

Należy podać funkcjonującą w oprogramowaniu ESET prawidłową nazwę wykrycia. Aby znaleźć prawidłową nazwę, należy przejść do obszaru Pliki dziennika, a następnie wybrać z menu rozwijanego Pliki dziennika pozycję **Wykrycia**. Jest to przydatne w przypadku fałszywego alarmu dotyczącego próbki w programie ESET Internet Security. Wyłączenia dotyczące prawdziwych infekcji stanowią niebezpieczną praktykę. Należy wyłączyć tylko odpowiednie pliki/katalogi, klikając przycisk **...** w polu **Maska ścieżki** i/lub zrobić to tylko na określony czas. Wyłączenia dotyczą także potencjalnie niepożądanych aplikacji, potencjalnie niebezpiecznych aplikacji i podejrzanych aplikacji.

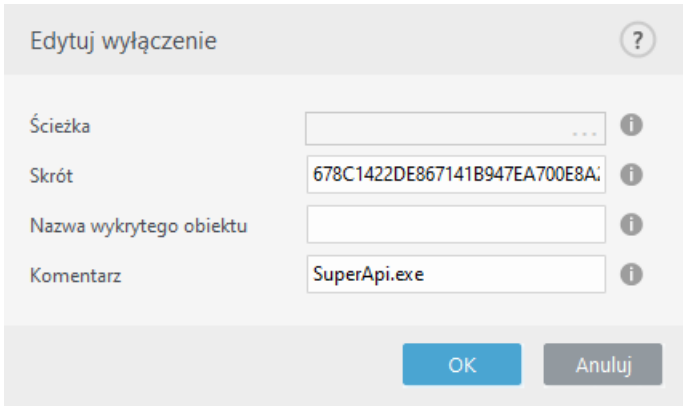
Zobacz też Format ścieżki wyłączenia.



Zobacz też przykład zaawansowanej konfiguracji wyłączeń poniżej.

Wyłącz skrót

Wyłącza plik na podstawie określonego skrótu SHA-1 bez względu na typ, lokalizację, nazwę i rozszerzenie pliku.



Wyłączenia według nazwy wykrycia

Aby wyłączyć określone wykrycie, należy wpisać jego prawidłową nazwę:
Win32/Adware.Optmedia
Dodając wyłączenie dotyczące wykrycia w oknie alertu w programie ESET Internet Security, można użyć następującego formatu:
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

Elementy sterujące

- **Dodaj** — pozwala dodać obiekty, które mają być pomijane podczas wykrywania.
- **Edytuj** — pozwala edytować zaznaczone elementy.
- **Usuń** — służy do usuwania zaznaczonych elementów (CTRL + kliknięcie pozwala zaznaczyć wiele elementów).

Kreator tworzenia zaawansowanej konfiguracji wyłączeń

Zaawansowaną konfigurację wyłączeń można utworzyć za pomocą menu kontekstowego Pliki dziennika (ta opcja nie jest dostępna w przypadku wykryć szkodliwego oprogramowania):

1. W głównym oknie programu kliknij opcję **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**.
2. Następnie należy kliknąć prawym przyciskiem myszy wykrycie w obszarze **Dziennik wykryć**.
3. Następnie należy kliknąć opcję **Utwórz wyłączenie**.

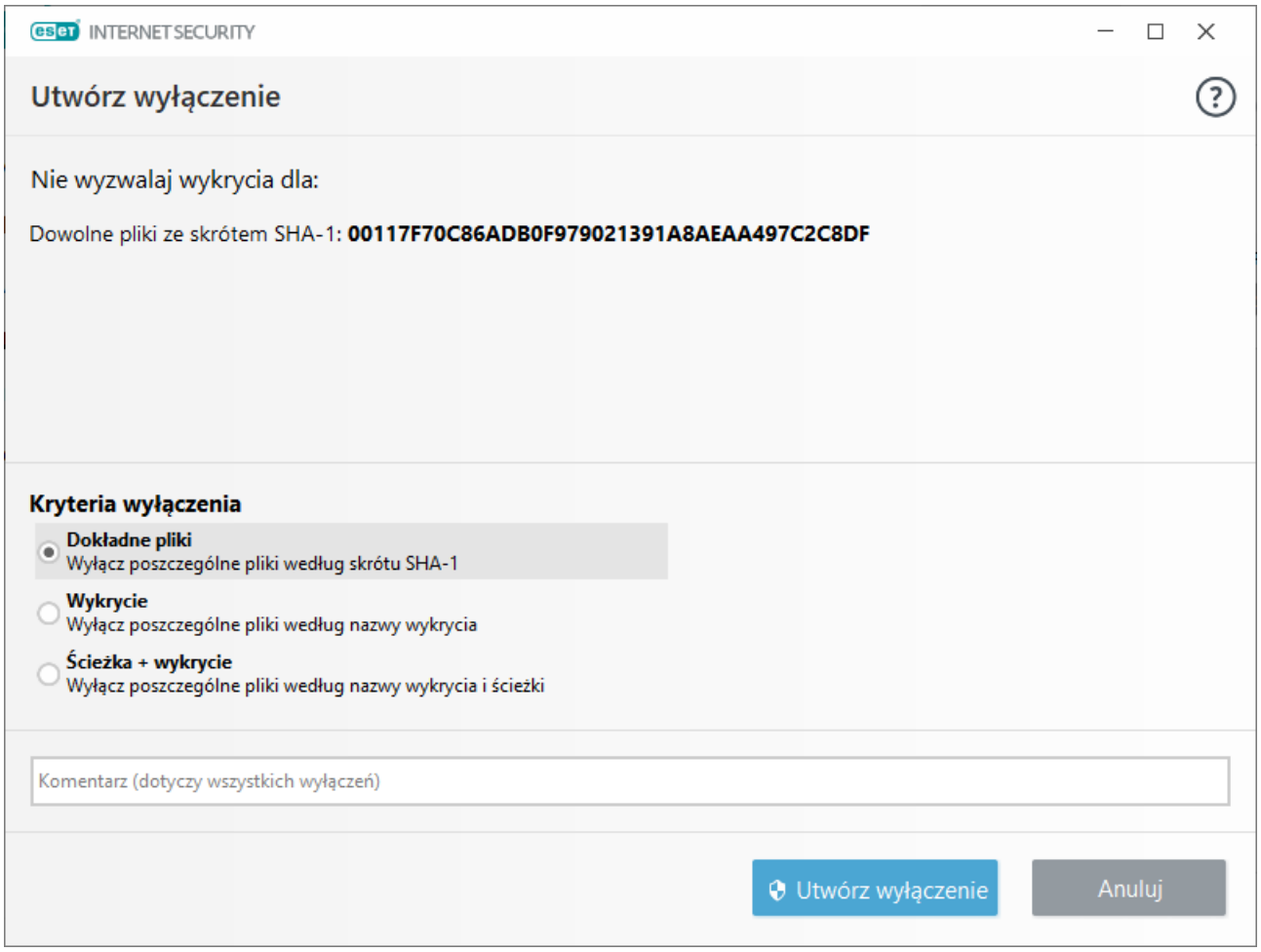
Aby wyłączyć co najmniej jedno wykrycie z uwzględnieniem ustawień **Kryteria wyłączenia**, należy kliknąć opcję **Zmień kryteria**:

- **Dokładne pliki** — wyłącza poszczególne pliki według skrótu SHA-1.
- **Wykrycie** — wyłącza poszczególne pliki według nazwy wykrycia.

• **Ścieżka + wykrycie** — wyłącza poszczególne pliki według nazwy wykrycia i ścieżki z uwzględnieniem nazwy pliku (np. *file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*).

Zalecana opcja jest wstępnie wybrana i zależy od typu wykrycia.

Przed kliknięciem opcji **Utwórz wyłączenie** można dodać **Komentarz**.



Wyłączenia systemu HIPS

Wyłączenia umożliwiają wyłączenie określonych procesów z głębokiej inspekcji behawioralnej systemu HIPS.

Aby edytować wyłączenia systemu HIPS, przejdź do pozycji **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **System HIPS** > **Podstawowe** > **Wyłączenia** > **Edycja**.

Należy pamiętać, że wyłączenia rozszerzeń plików, zaawansowana konfiguracja wyłączeń, pliki i foldery wyłączone ze skanowania oraz wyłączenia procesów to różne zagadnienia.

Aby wyłączyć obiekt, należy kliknąć przycisk **Dodaj** i wprowadzić ścieżkę do obiektu lub wybrać obiekt w strukturze drzewa. Można też edytować i usuwać wybrane wpisy.

Parametry 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. Aparat skanowania może kontrolować kilka strumieni danych jednocześnie, co zwiększa do maksimum skuteczność i wskaźnik wykrywalności. Ponadto technologia ThreatSense skutecznie 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 opcję **Parametry technologii ThreatSense** 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 zagrożeń atakujących pamięć operacyjną komputera.

Sektory startowe/UEFI — umożliwia skanowanie sektorów startowych w poszukiwaniu szkodliwego oprogramowania w głównym rekordzie rozruchowym. Więcej informacji na temat interfejsu UEFI można znaleźć

w słowniczku.

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 (SFX) to archiwa, które rozpakowują się same.

Programy pakujące w czasie wykonywania — 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 nie istniało lub nie było znane w chwili pobierania poprzedniej wersji silnika detekcji. Wadą może być ryzyko (niewielkie) wystąpienia tzw. fałszywych alarmów.

Zaawansowana heurystyka/sygnatury DNA — 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 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).

Leczenie

Ustawienia leczenia określają sposób działania programu ESET Internet Security podczas prób leczenia obiektów. Istnieją 4 poziomy leczenia:

Parametry ThreatSense mają następujące poziomy korygowania (tj. czyszczenia).

Naprawa w produkcie ESET Internet Security

Poziom leczenia	Opis
Zawsze naprawiaj wykrycie	Podjęcie próby naprawy podczas leczenia obiektów bez interwencji użytkownika. W niektórych rzadkich przypadkach (np. plików systemowych), jeśli nie można naprawić wykrycia, zgłoszony obiekt pozostanie w pierwotnej lokalizacji.
Napraw wykrycie, jeśli to bezpieczne — w przeciwnym razie pozostaw	Podjęcie próby naprawy podczas leczenia obiektów bez interwencji użytkownika. W niektórych przypadkach (np. plików systemowych lub archiwów zawierających zarówno czyste, jak i zainfekowane pliki), kiedy zagrożenia nie można naprawić, obiekt pozostanie w pierwotnej lokalizacji.

Poziom leczenia	Opis
Napraw wykrycie, jeśli to bezpieczne — w przeciwnym razie spytaj	Podjęcie próby naprawienia wykrytego zagrożenia podczas leczenia obiektów. W niektórych przypadkach, jeśli nie można wykonać żadnej akcji, użytkownikowi zostanie wyświetlony alert interaktywny umożliwiający wybór czynności zaradczej (np. usunięcia lub zignorowania). To ustawienie jest zalecane w większości przypadków.
Zawsze pytaj użytkownika	Użytkownik końcowy widzi interaktywne okno podczas leczenia obiektów i musi wybrać akcję naprawczą (na przykład usunąć lub zignorować). Ten poziom jest przeznaczony dla bardziej zaawansowanych użytkowników, którzy wiedzą, jakie kroki należy podjąć w przypadku wykrycia.

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 — dziennik skanowania będzie obejmować informacje o wszystkich skanowanych plikach w archiwach samorozpakowujących (nawet o tych niezainfekowanych). Może to spowodować wygenerowanie dużej ilości danych w dzienniku skanowania oraz zwiększenie rozmiaru pliku dziennika skanowania.

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 plików w obiekcie kontenera (np. w archiwum RAR/ZIP lub w wiadomości e-mail z wieloma załącznikami). To ustawienie nie dotyczy samodzielnych plików. Jeśli czas podany przez użytkownika w tym polu upłynie, skanowanie zostanie zatrzymane przy najbliższej okazji, bez względu na to, czy przeskanowano wszystkie pliki w obiekcie kontenera.
W przypadku archiwów z dużymi plikami skanowanie może zostać zatrzymane dopiero po wyodrębnieniu pliku z archiwum (np. zmienna zdefiniowana przez użytkownika to 3 sekundy, a wyodrębnianie pliku trwa 5 sekund). Po upłynięciu tego czasu pozostałe pliki w archiwum nie zostaną przeskanowane.
Aby skrócić czas skanowania, w tym w przypadku większych archiwów, skorzystaj z opcji **Maksymalny rozmiar obiektu** i **Maksymalny rozmiar pliku w archiwum** (niezalecane ze względu na możliwe zagrożenia bezpieczeństwa).
Wartość domyślna: bez ograniczeń.

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 maksymalna: **3 GB**.

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

Lista rozszerzeń plików wyłączonych ze skanowania

Wykluczone rozszerzenia plików są częścią parametrów ThreatSense. Aby skonfigurować wykluczone rozszerzenia plików, kliknij **Parametry ThreatSense** w oknie Ustawienia zaawansowane dla dowolnego modułu korzystającego z technologii ThreatSense.

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.

> Należy pamiętać, że wyłączenia procesów, wyłączenia systemu HIPS i wyłączenia plików/folderów to różne zagadnienia.

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`.

Aby dodać nowe rozszerzenie do listy, kliknij przycisk **Dodaj**. Wpisz rozszerzenie w pustym polu (np. tmp) i kliknij przycisk **OK**. Gdy wybrano opcję **Wprowadź wiele wartości**, można dodać wiele rozszerzeń plików oddzielonych wierszami, przecinkami lub średnikami (na przykład jako separator wybierz z menu rozwijanego pozycję **Średnik** i wpisz `edb;eml;tmp`).
Można użyć symbolu specjalnego znaku zapytania (?). Znak zapytania oznacza dowolny symbol (na przykład `?db`).

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.

Dodatkowe parametry ThreatSense

Aby edytować te ustawienia, przejdź do pozycji **Ustawienia zaawansowane** (F5) > **Silnik detekcji** > **Ochrona systemu plików w czasie rzeczywistym** > **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. Z tego powodu program sprawdza te pliki przy użyciu dodatkowych parametrów skanowania. Program ESET Internet Security używa zaawansowanej heurystyki, która może wykryć nowe zagrożenia przed opublikowaniem aktualizacji silnika detekcji wraz z metodami skanowania opartymi na sygnaturach.

Poza nowo utworzonymi plikami skanowanie obejmuje również **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 usunąć zaznaczenie opcji **Domyślne ustawienia skanowania archiwów**.

Dodatkowe parametry ThreatSense dla wykonywanych plików

Zaawansowana heurystyka podczas wykonywania pliku — domyślnie zaawansowana heurystyka jest stosowana podczas wykonywania plików. Gdy ta opcja jest włączona, zalecamy pozostawienie włączonych opcji inteligentnej optymalizacji oraz systemu ESET LiveGrid® w celu ograniczenia wpływu na wydajność systemu.

Zaawansowana heurystyka podczas wykonywania plików z nośników wymiennych — zaawansowana heurystyka służy do emulowania kodu w środowisku wirtualnym oraz do oceny działania kodu przed zezwoleniem na jego uruchomienie z nośników wymiennych.

Ochrona internetowa

Aby skonfigurować ochronę dostępu do stron internetowych i poczty e-mail, kliknij opcję **Ochrona w Internecie** w oknie **Ustawienia**. Z tego miejsca można uzyskać dostęp do bardziej szczegółowych ustawień programu.

Aby wstrzymać lub wyłączyć poszczególne moduły ochrony, kliknij ikonę suwaka .

Wyłączenie modułów ochrony może obniżyć poziom ochrony komputera.



Kliknij ikonę koła zębatego, aby otworzyć stronę internetową / e-mail / ochronę przed phishingiemoraz ochrony przed spamem w Ustawieniach zaawansowanych.

Obsługa komunikacji przez Internet jest standardową funkcją komputerów osobistych. Niestety, Internet stał się głównym medium używanym do rozpowszechniania 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(S) oraz IMAP(S). Dzięki zastosowaniu wtyczki do programu poczty e-mail, program ESET Internet Security umożliwia kontrolowanie całości komunikacji obsługiwanej przez program poczty e-mail.

Moduł Ochrona przed spamem filtruje niepożądane wiadomości e-mail.

W przypadku **ochrony przed spamem** kliknij ikonę koła zębatego i wybierz jedną z następujących opcji:

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

- **Lista adresów użytkownika** (jeśli jest włączona) — otwiera się okno dialogowe, w którym można dodawać, edytować lub usuwać adresy w celu zdefiniowania reguł antyspamowych. Reguły podane na tej liście będą miały zastosowanie do bieżącego użytkownika.

- **Globalna lista adresów** (jeśli jest włączona) — otwiera się okno dialogowe, w którym można dodawać, edytować lub usuwać adresy w celu zdefiniowania reguł antyspamowych. Reguły podane na tej liście będą miały zastosowanie do wszystkich użytkowników.

Ochrona przed atakami typu „phishing" pozwala na blokowanie stron internetowych znanych z dystrybuowania

ataków typu „phishing”. Zdecydowanie zalecamy pozostawienie opcji ochrony przed atakami typu „phishing” włączonej.

Filtrowanie protokołów

Ochrona antywirusowa protokołów aplikacji jest realizowana z wykorzystaniem technologii skanowania ThreatSense, w której połączono wszystkie zaawansowane metody wykrywania szkodliwego oprogramowania. Filtrowanie protokołów odbywa się automatycznie niezależnie od przeglądarki internetowej i programu poczty e-mail. Aby zmodyfikować ustawienia komunikacji szyfrowanej (SSL/TLS), należy wybrać kolejno opcje **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **SSL/TLS**.

Włącz filtrowanie zawartości protokołów aplikacji — przy użyciu tej opcji można wyłączyć filtrowanie protokołów. Należy pamiętać, że opcja ta ma wpływ na wiele komponentów programu ESET Internet Security (ochrona dostępu do stron internetowych, ochrona protokołów poczty e-mail, ochrona przed atakami typu „phishing”, kontrola rodzicielska), 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 ona przydatna, gdy filtrowanie protokołów powoduje problemy ze zgodnością.

Dodaje (na przykład *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsieć — podsieć (grupa komputerów) zdefiniowana przez adres IP i maskę (na przykład: *2002:c0a8:6301:1::1/64*).

Przykład wyłączonych adresów IP

Adresy IPv4 i maska:

- *192.168.0.10* — umożliwia dodanie adresu IP określonego komputera, do którego ma być stosowana reguła .
- *192.168.0.1* do *192.168.0.99* — umożliwia wprowadzenie początkowego i końcowego adresu IP w celu określenia zakresu adresów IP (wielu komputerów), do których ma być stosowana reguła.
- Podsieć (grupa komputerów) zdefiniowana przez adres IP i maskę. Na przykład *255.255.255.0* to maska sieci dla prefiksu *192.168.1.0/24* wyznaczająca zakres adresów od *192.168.1.1* do 192.168.1.254.

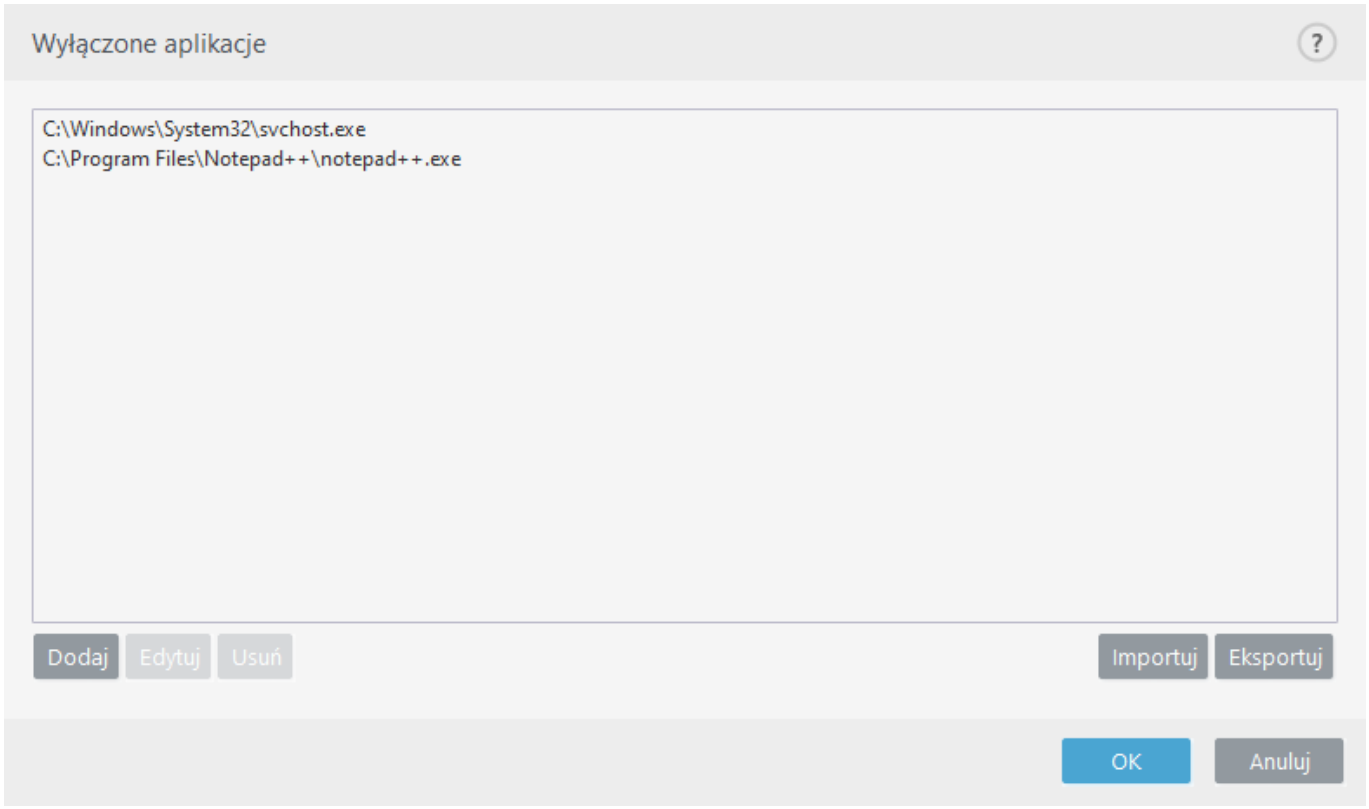
Adresy IPv6 i maska:

- *2001:718:1c01:16:214:22ff:fec9:ca5* — adres IPv6 określonego komputera, do którego ma być stosowana reguła
- *2002:c0a8:6301:1::1/64* — adres IPv6 z 64-bitowym prefiksem, co wyznacza zakres adresów od *2002:c0a8:6301:0001:0000:0000:0000:0000 do 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

Aplikacje wyłączone

Aby wykluczyć z filtrowania zawartości komunikację prowadzoną przez określone aplikacje korzystające z sieci, należy zaznaczyć je na liście. Komunikacja prowadzona przez te aplikacje za pośrednictwem protokołów HTTP, POP3 oraz IMAP nie będzie sprawdzana pod kątem obecności zagrożeń. Stosowanie tej opcji jest zalecane tylko w przypadku aplikacji, które działają nieprawidłowo, gdy ich komunikacja jest sprawdzana.

Działające aplikacje i usługi będą tu dostępne automatycznie. Kliknij **Dodaj** , aby ręcznie dodać aplikację, jeśli brakuje jej na liście filtrowania protokołów.



Wyłączone adresy IP

Pozycje na liście 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.

Kliknij opcję **Dodaj**, aby wyłączyć adres IP / zakres adresów / podsieć zdalnego punktu spoza listy filtrowania protokołów.

Kliknij **Usuń**, aby usunąć wybrane pozycje z listy.



Dodaj adres IPv4

Te opcje umożliwiają dodawanie adresów IP/zakresu adresów/podsieci punktów zdalnych, do których ma mieć zastosowanie dana reguła. Protokół Internet Protocol w wersji 4 to wersja starsza, ale wciąż najpowszechniej używana.

Pojedynczy adres — umożliwia dodanie adresu IP określonego komputera, do którego ma być stosowana reguła (na przykład *192.168.0.10*).

Zakres adresów — umożliwia wprowadzenie początkowego i końcowego adresu IP w celu określenia zakresu adresów IP (wielu komputerów), do których ma być stosowana reguła (na przykład od *192.168.0.1* do *192.168.0.99*).

Podsieć — podsieć (grupa komputerów) zdefiniowana przez adres IP i maskę.

Na przykład *255.255.255.0* to maska sieci dla prefiksu *192.168.1.0/24* wyznaczająca zakres adresów od *192.168.1.1* do 192.168.1.254.

Dodaj adres IPv6

Ta opcja pozwala na dodanie adresu IPv6/maski podsieci zdalnego punktu, do którego ma mieć zastosowanie reguła. Jest to najnowsza wersja protokołu Internet Protocol, która zastąpi starszą wersję 4.

Pojedynczy adres — umożliwia dodanie adresu IP określonego komputera, do którego ma być stosowana reguła (na przykład *2001:718:1c01:16:214:22ff:fec9:ca5*).

Podsieć — podsieć (grupa komputerów) zdefiniowana przez adres IP i maskę (na przykład: *2002:c0a8:6301:1::1/64*).

SSL/TLS

Program ESET Internet Security umożliwia sprawdzanie komunikacji z zastosowaniem protokołu SSL pod kątem zagrożeń. W przypadku sprawdzania komunikacji chronionej protokołem SSL można stosować różne tryby filtrowania 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 filtrowania	Opis
Tryb automatyczny	Domyślny tryb skanowania uwzględnia tylko odpowiednie aplikacje, takie jak przeglądarki internetowe i programy poczty e-mail. Można zastąpić tryb domyślny, wybierając aplikacje, których komunikacja ma być skanowana.
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 lub aplikacji, które zostaną wyłączone ze skanowania.

Tryb filtrowania	Opis
Tryb reguł	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 jest dozwolona, a jej treść jest filtrowana.

Lista aplikacji, dla których przeprowadzane jest filtrowanie protokołu SSL/TLS — umożliwia dostosowanie zachowania programu ESET Internet Security do określonych aplikacji.

Lista znanych certyfikatów — umożliwia dostosowanie sposobu działania programu ESET Internet Security do określonych certyfikatów SSL.

Nie uwzględniaj połączeń z zaufanymi domenami — gdy ta opcja jest włączona, komunikacja z zaufanymi domenami jest wyłączona ze sprawdzania. Stopień zaufania domeny jest określany przez wbudowaną białą listę.

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

Certyfikat główny

Dodaj certyfikat główny do znanych przeglądarek — aby w przeglądarkach internetowych lub programach poczty e-mail komunikacja przy użyciu protokołu SSL przebiegała prawidłowo, konieczne jest dodanie certyfikatu głównego firmy ESET do listy znanych certyfikatów głównych (wydawców). Gdy ta opcja jest włączona, program ESET Internet Security automatycznie doda certyfikat ESET SSL Filter CA do znanych przeglądarek (np. Opera). W przypadku przeglądarek korzystających z systemowego magazynu certyfikacji certyfikat jest dodawany automatycznie. Na przykład w konfiguracji przeglądarki Firefox automatycznie zakłada się, że główne urzędy certyfikacji w magazynie systemowym są zaufane.

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 poziomu zaufania dla certyfikatu — 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), zostaje 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 uszkodzony — oznacza to, że certyfikat został nieprawidłowo podpisany lub jest uszkodzony. W takim przypadku firma ESET zaleca pozostawienie włączonego **blokowania komunikacji używającej certyfikatu.** Jeśli wybrano opcję **Zapytaj o ważność certyfikatu**, użytkownik jest monitowany o wybranie akcji do podjęcia po ustanowieniu zaszyfrowanej komunikacji.

Przykłady z ilustracjami

Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:

- Powiadomienia dotyczące certyfikatów w produktach ESET do systemu Windows przeznaczonych dla użytkowników domowych
- „Zaszyfrowany ruch sieciowy: niezaufany certyfikat" podczas wyświetlania stron internetowych pojawia się komunikat

Certyfikaty

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). **Dodaj certyfikat główny do znanych przeglądarek** powinno być zaznaczone. 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.

W niektórych przypadkach certyfikat nie może zostać zweryfikowany za pomocą magazynu zaufanych głównych urzędów certyfikacji (np. VeriSign). Oznacza to, że został on podpisany samodzielnie przez jakąś osobę (np. przez administratora serwera internetowego lub małej firmy) i uważanie go za zaufany certyfikat nie musi się wiązać 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. Pojawi się okno dialogowe wyboru czynności, w którym można oznaczyć dany certyfikat jako zaufany lub wyłączony. Jeśli certyfikat nie występuje na liście zaufanych głównych urzędów certyfikacji (TRCA), okno to jest czerwone. Jeśli certyfikat występuje na liście zaufanych głównych urzędów certyfikacji, okno to jest zielone.

Można zaznaczyć pole wyboru **Blokuj komunikację używającą certyfikatu**, aby zawsze przerywać szyfrowane połączenie z witryną, która korzysta z niezweryfikowanego certyfikatu.

Jeśli dany certyfikat jest niepoprawny lub uszkodzony, oznacza to, że wygasła jego ważność lub został nieprawidłowo podpisany samodzielnie. W takim przypadku zalecamy zablokowanie korzystającej z niego komunikacji.

Zaszyfrowany ruch sieciowy

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 Internet 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**. Jeśli certyfikat nie znajduje się w Trusted Root Certification Authorities store (TRCA), zostanie uznany za niezaufany.

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 Internet Security musi **ignorować** ruch sieciowy, by umożliwić dalsze działanie aplikacji.

> **Przykłady z ilustracjami**
> Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:
> • Powiadomienia dotyczące certyfikatów w produktach ESET do systemu Windows przeznaczonych dla użytkowników domowych
> • „Zaszyfrowany ruch sieciowy: niezaufany certyfikat" podczas wyświetlania stron internetowych pojawia się komunikat

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

Lista znanych certyfikatów

Lista znanych certyfikatów może posłużyć do dostosowania zachowania programu ESET Internet 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 to służy do identyfikacji podmiotu związanego z kluczem publicznym przechowywanym w polu podmiotu klucza publicznego.

Dostęp — w celu **zezwolenia** lub **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 — należy dodać nowy certyfikat i skonfigurować w nim ustawienia dotyczące dostępu oraz opcji skanowania.

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

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

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

Lista aplikacji, dla których przeprowadzane jest filtrowanie protokołu SSL/TLS

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

Okno **Lista aplikacji, dla których przeprowadzane jest filtrowanie protokołu SSL/TLS** obejmuje następujące elementy:

Kolumny

Aplikacje — wybierz plik wykonywalny z drzewa katalogów, kliknij opcję **...** albo wpisz ścieżkę ręcznie.

Czynność skanowania — wybranie opcji **Skanuj** lub **Ignoruj** umożliwia skanowanie lub ignorowanie komunikacji. 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 — umożliwia dodanie filtrowanej aplikacji.

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

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

Importuj/**Eksportuj** — importowanie aplikacji z pliku lub zapisywanie bieżącej listy aplikacji do pliku.

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

Ochrona programów poczty e-mail

Zobacz Integracja ESET Internet Security z programem poczty e-mail, aby przeprowadzić konfigurację integracji.

Ustawienia programu poczty e-mail można znaleźć w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Programy poczty e-mail**.

Programy poczty e-mail

Włącz ochronę poczty e-mail poprzez wtyczki klientów — po wyłączeniu tej opcji ochrona poczty e-mail poprzez wtyczki klientów zostaje wyłączona.

Skanowane wiadomości

Wybierz wiadomości e-mail do skanowania:

- **Wiadomości odbierane**
- **Wiadomości wysyłane**
- **Wiadomości przeczytane**
- **Zmodyfikowana wiadomość e-mail**

> Zalecamy pozostawienie włączonej opcji **Włącz ochronę poczty e-mail poprzez wtyczki klientów**. Nawet gdy integracja nie jest włączona lub nie działa, komunikacja za pośrednictwem poczty e-mail jest nadal chroniona przez funkcję filtrowanie protokołów (IMAP/IMAPS i POP3/POP3S).

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 (czynność domyślna) — zainfekowane wiadomości będą automatycznie przenoszone do wskazanego folderu.

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

Integracja z programami poczty e-mail

Integracja ESET Internet Security z klientem poczty e-mail zwiększa poziom aktywnej ochrony przed złośliwym kodem w wiadomościach e-mail. Jeśli dany program poczty e-mail jest obsługiwany, można włączyć funkcję integracji w programie ESET Internet Security. Po jej aktywowaniu pasek narzędzi programu ESET Internet Security jest wstawiany bezpośrednio do programu poczty e-mail, umożliwiając skuteczniejszą ochronę poczty. Ustawienia integracji można znaleźć w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Programy 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.

W razie spowolnienia działania systemu podczas odbierania wiadomości e-mail wyłącz opcję **Optymalizacja obsługi załączników** i **Zaawansowane przetwarzanie dotyczące programu poczty e-mail**.

Pasek narzędzi programu Microsoft Outlook

Ochrona programu Microsoft Outlook działa na zasadzie wtyczki. Po zainstalowaniu oprogramowania ESET Internet Security ten pasek narzędzi zawierający opcje ochrony antywirusoweji antyspamowej jest dodawany do programu Microsoft Outlook:

Spam — umożliwia oznaczanie wybranych wiadomości jako spam. Po wprowadzeniu takiego oznaczenia do centralnego serwera przechowującego sygnatury spamu jest wysyłana sygnatura wiadomości. Jeśli serwer otrzyma więcej podobnych sygnatur od wielu użytkowników, dana wiadomość będzie w przyszłości uznawana za spam.

Pożądana wiadomość — umożliwia oznaczanie wybranych wiadomości jako „pożądane”.

Adres spamu (czarna lista, lista adresów nadawców spamu) — umożliwia dodanie nowego adresu nadawcy do czarnej listy. Wszystkie wiadomości otrzymywane od nadawców z tej listy będą automatycznie klasyfikowane jako spam.

Należy uważać na spoofing — technikę polegającą na fałszowaniu adresu nadawcy wiadomości w celu nakłonienia odbiorców do jej przeczytania i zareagowania na jej treść.

Adres zaufany (biała lista, lista zaufanych adresów) — umożliwia dodanie nowego adresu nadawcy do białej listy. Wszystkie wiadomości otrzymywane z adresów umieszczonych na białej liście nie będą nigdy automatycznie klasyfikowane jako spam.

ESET Internet Security – Kliknij dwukrotnie ikonę, aby otworzyć główne okno ESET Internet Security.

Ponowne skanowanie wiadomości — umożliwia ręczne rozpoczęcie sprawdzania poczty e-mail. Można określać wiadomości do sprawdzenia oraz włączać ponowne skanowanie odebranej poczty e-mail. Więcej informacji można znaleźć w części Ochrona programów poczty e-mail.

Ustawienia skanera — umożliwia wyświetlenie opcji ustawień funkcji Ochrona programów poczty e-mail

Ustawienia ochrony przed spamem — umożliwia wyświetlenie opcji ustawień funkcji Ochrona przed spamem.

Książki adresowe — powoduje otwarcie okna modułu ochrony przed spamem, w którym można uzyskać dostęp do list adresów wyłączonych, zaufanych i wysyłających spam.

Pasek narzędzi do programów Outlook Express i Windows Mail

Moduł ochrony przed spamem w programach Outlook Express i Windows Mail działa jako wtyczka. Po zainstalowaniu oprogramowania ESET Internet Security ten pasek narzędzi zawierający opcje ochrony antywirusoweji antyspamowej jest dodawany do programu Outlook Express lub Windows Mail:

Spam — umożliwia oznaczanie wybranych wiadomości jako spam. Po wprowadzeniu takiego oznaczenia do centralnego serwera przechowującego sygnatury spamu jest wysyłana sygnatura wiadomości. Jeśli serwer otrzyma więcej podobnych sygnatur od wielu użytkowników, dana wiadomość będzie w przyszłości uznawana za spam.

Pożądana wiadomość — umożliwia oznaczanie wybranych wiadomości jako „pożądane”.

Adres spamu — umożliwia dodanie nowego adresu nadawcy do cczarnej listy. Wszystkie wiadomości otrzymywane od nadawców z tej listy będą automatycznie klasyfikowane jako spam.

Należy uważać na spoofing — technikę polegającą na fałszowaniu adresu nadawcy wiadomości w celu nakłonienia odbiorców do jej przeczytania i zareagowania na jej treść.

Adres zaufany — umożliwia dodanie nowego adresu nadawcy do białej listy. Wszystkie wiadomości otrzymywane z adresów umieszczonych na białej liście nie będą nigdy automatycznie klasyfikowane jako spam.

ESET Internet Security – Kliknij dwukrotnie ikonę, aby otworzyć główne okno ESET Internet Security.

Ponowne skanowanie wiadomości — umożliwia ręczne rozpoczęcie sprawdzania poczty e-mail. Można określać wiadomości do sprawdzenia oraz włączać ponowne skanowanie odebranej poczty e-mail. Więcej informacji można znaleźć w części Ochrona programów poczty e-mail.

Ustawienia skanera — umożliwia wyświetlenie opcji ustawień funkcji Ochrona programów poczty e-mail

Ustawienia ochrony przed spamem — umożliwia wyświetlenie opcji ustawień funkcji Ochrona przed spamem.

Interfejs użytkownika

Dostosuj wygląd — umożliwia modyfikowanie wyglądu paska narzędzi danego programu poczty e-mail. Aby dostosować wygląd niezależnie od parametrów programu poczty e-mail, należy usunąć zaznaczenie tej opcji.

Pokaż tekst — powoduje wyświetlanie opisów ikon.

Tekst po prawej stronie — powoduje przesunięcie opisów opcji spod ikon na ich prawą stronę.

Duże ikony — powoduje wyświetlanie dużych ikon opcji menu.

Okno dialogowe potwierdzenia

Wyświetlanie tego powiadomienia ma na celu sprawdzenie, czy użytkownik faktycznie chce wykonać daną czynność, co powinno wyeliminować możliwość pomyłki.

W tym oknie dialogowym można również wyłączać potwierdzenia.

Ponowne skanowanie wiadomości

Za pośrednictwem zintegrowanego z programami poczty e-mail paska narzędzi programu ESET Internet Security można skonfigurować wiele opcji sprawdzania wiadomości e-mail. Opcja **Ponowne skanowanie wiadomości** oferuje dwa tryby skanowania:

Wszystkie wiadomości w bieżącym folderze — skanowane są wszystkie wiadomości w obecnie wyświetlanym folderze.

Tylko wybrane wiadomości — skanowane są tylko wiadomości zaznaczone przez użytkownika.

Zaznaczenie pola wyboru **Przeskanuj ponownie już skanowane wiadomości** umożliwia przeprowadzenie ponownego skanowania wiadomości, które zostały już przeskanowane.

Protokoły poczty e-mail

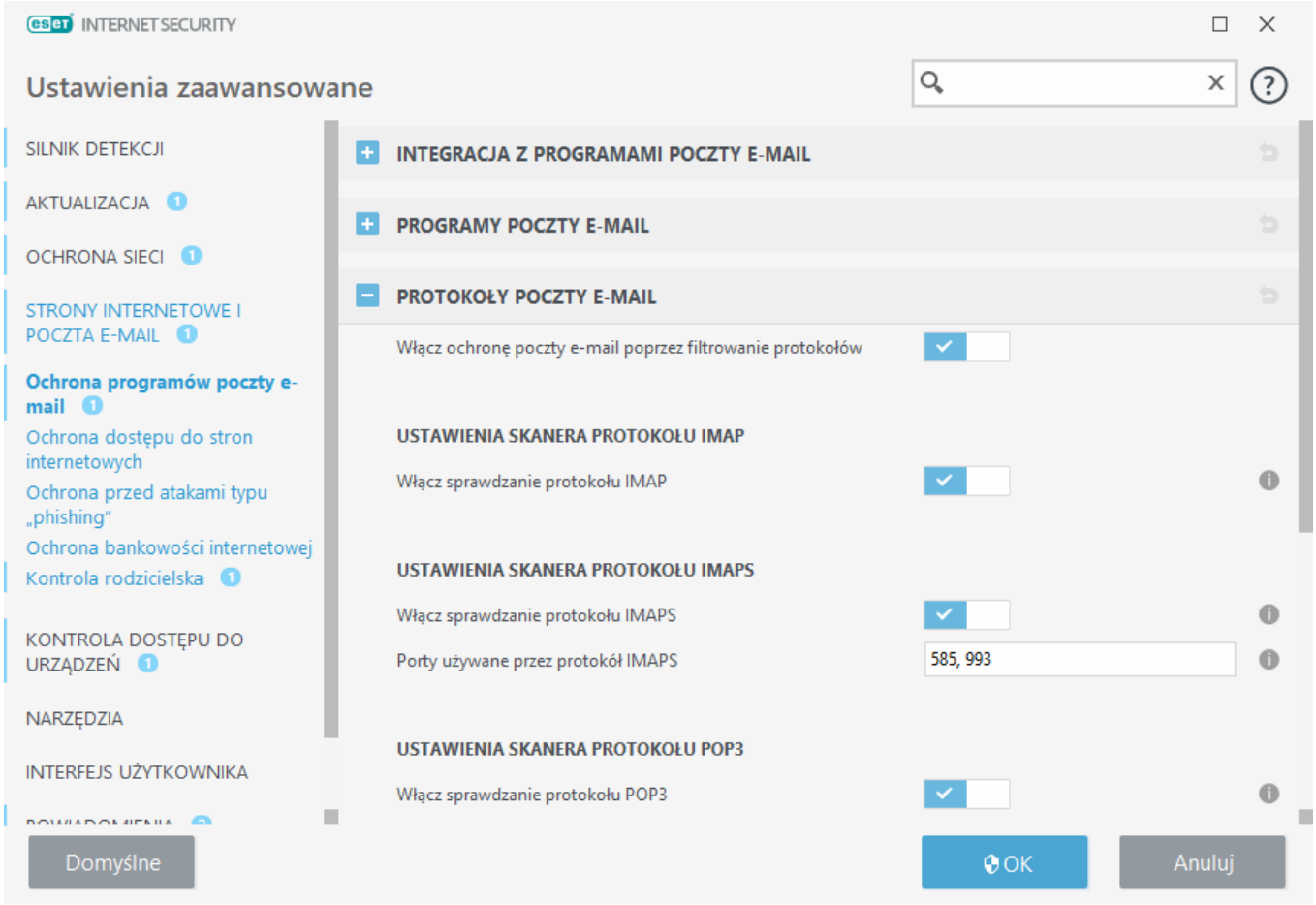
Protokoły IMAP i POP3 to najbardziej rozpowszechnione protokoły używane do obsługi komunikacji przychodzącej w programach poczty e-mail. IMAP (Internet Message Access Protocol) to kolejny protokół internetowy do odbierania poczty e-mail. IMAP ma pod pewnymi względami przewagę nad protokołem POP3, np. wiele klientów może być podłączonych równocześnie do tej samej skrzynki pocztowej przy zachowaniu informacji o stanie wiadomości (czy została ona przeczytana, usunięta albo czy udzielono już na nią odpowiedzi). Moduł ochrony udostępniający tę opcję jest automatycznie inicjowany po uruchomieniu komputera i jest aktywny w pamięci.

Program ESET Internet 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. Domyślnie skanowana jest cała komunikacja realizowana za pomocą protokołów POP3 i IMAP niezależnie od domyślnych numerów portów POP3/IMAP.
Protokół IMAP nie jest skanowany. Ale komunikacja z serwerem Microsoft Exchange może być skanowana przez moduł integracji w programach poczty e-mail (np. Microsoft Outlook).

Zalecamy pozostawienie włączonej opcji **Włącz ochronę poczty e-mail przez filtrowanie protokołów**. Aby skonfigurować sprawdzanie protokołów IMAP/IMAPS i POP3/POP3S, przejdź do menu **Ustawienia zaawansowane** > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Protokoły poczty e-mail**.

Program ESET Internet Security obsługuje również skanowanie protokołów IMAPS (585, 993) i POP3S (995), korzystających z szyfrowanego kanału przy przesyłaniu danych pomiędzy serwerem a klientem. Program ESET Internet 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. W razie potrzeby można dodać pozostałe porty komunikacyjne. Numery portów muszą być oddzielone przecinkami.

Komunikacja szyfrowana będzie skanowana domyślnie. Aby wyświetlić ustawienia skanera, otwórz stronę Ustawienia zaawansowane > **Strony internetowe i poczta e-mail** > **SSL/TLS**.



Filtr protokołów POP3 i POP3S

Protokół POP3 jest najpopularniejszym protokołem używanym do odbioru poczty e-mail w programach poczty e-mail. Program ESET Internet Security udostępnia ochronę tego protokołu bez względu na używany program poczty e-mail.

Moduł ochrony udostępniający tę opcję jest automatycznie inicjowany po uruchomieniu komputera i jest aktywny w pamięci. Aby moduł funkcjonował prawidłowo, należy się upewnić, że jest włączony — sprawdzanie protokołu POP3 odbywa się automatycznie bez konieczności zmiany konfiguracji programu poczty e-mail. Domyślnie skanowana jest cała komunikacja prowadzona przez port 110, ale w razie potrzeby skanowaniem można objąć również inne porty komunikacyjne. Numery portów muszą być oddzielone przecinkami.

Komunikacja szyfrowana będzie skanowana domyślnie. Aby wyświetlić ustawienia skanera, otwórz stronę Ustawienia zaawansowane > **Strony internetowe i poczta e-mail** > SSL/TLS.

W tej sekcji można skonfigurować sprawdzanie protokołów POP3 i POP3S.

Włącz sprawdzanie protokołu POP3 — zaznaczenie tej opcji powoduje włączenie skanowania całego ruchu obsługiwanego przez protokół POP3 pod kątem szkodliwego oprogramowania.

Porty używane przez protokół POP3 — lista portów używanych przez protokół POP3 (domyślnie jest to port 110).

Program ESET Internet Security obsługuje również sprawdzanie protokołu POP3S. W przypadku tego typu komunikacji informacje między serwerem a klientem przesyłane są przez szyfrowany kanał. Program ESET Internet Security sprawdza połączenia, używając metod szyfrowania SSL (Secure Socket Layer) i TLS (Transport Layer Security).

Nie używaj funkcji sprawdzania protokołu POP3S — szyfrowana komunikacja nie będzie sprawdzana.

Użyj funkcji sprawdzania protokołu POP3S dla wybranych portów — sprawdzanie protokołu POP3S będzie dotyczyło tylko portów zdefiniowanych w polu **Porty używane przez protokół POP3S**.

Porty używane przez protokół POP3S — lista portów protokołu POP3S do sprawdzenia (domyślnie jest to port 995).

Tagi 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**.

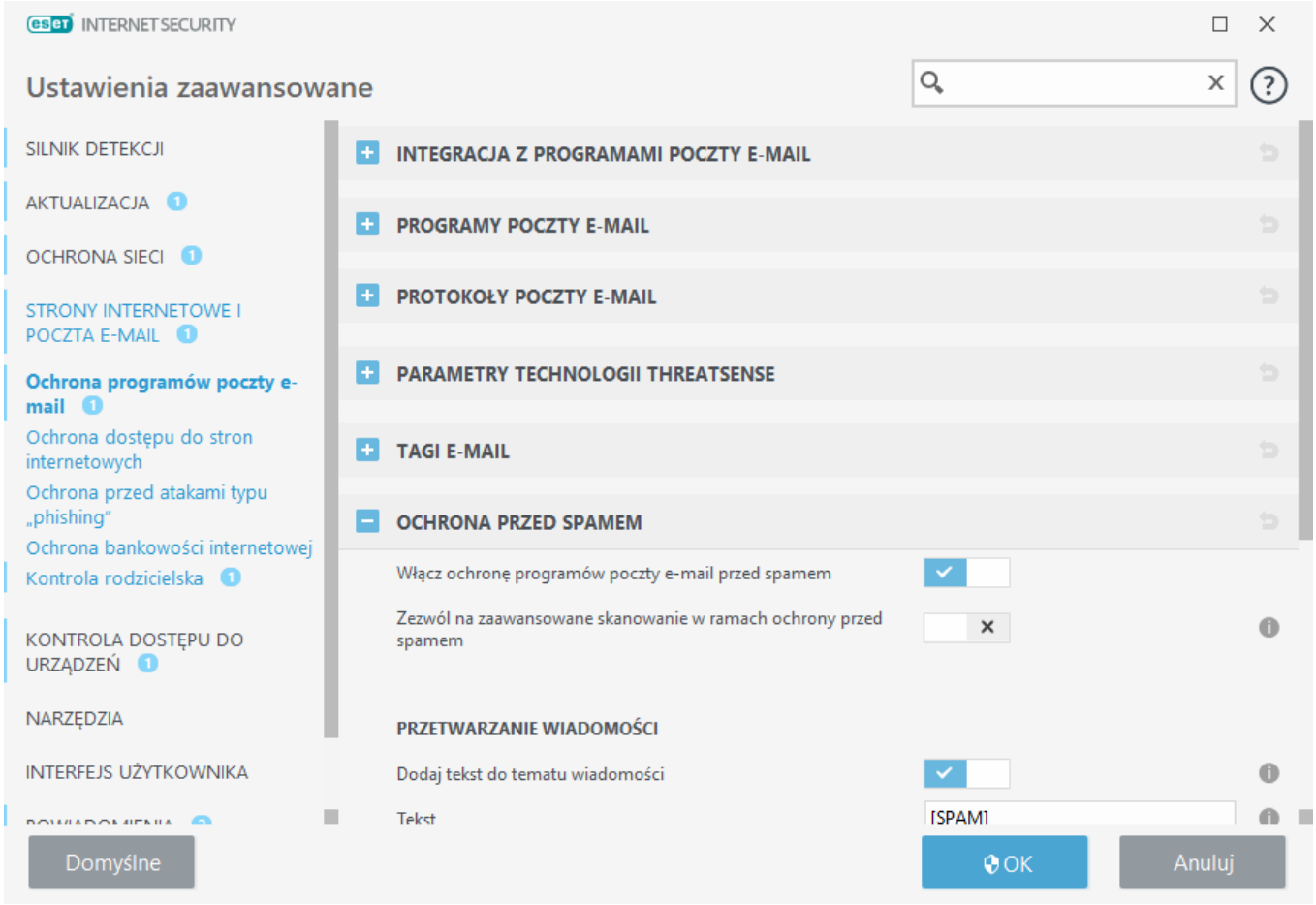
Po sprawdzeniu wiadomości e-mail może do niej zostać dołączone powiadomienie o wynikach skanowania. Do wyboru są następujące opcje: **Oznacz otrzymaną i przeczytaną wiadomość e-mail** oraz **Oznacz wysyłaną wiadomość e-mail**. Należy pamiętać, że w rzadkich przypadkach takie powiadomienia mogą być pomijane 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 są następujące opcje:

- **Nigdy** — powiadomienia nie będą dodawane.
- **W przypadku wykrycia** — tylko wiadomości zawierające szkodliwe oprogramowanie zostaną oznaczone jako sprawdzone (ustawienie domyślne).
- **Do wszystkich wiadomości e-mail po zeskanowaniu** — program będzie dołączać powiadomienia do wszystkich przeskanowanych wiadomości e-mail.

Komunikat dołączany do tematu wykrytej wiadomości e-mail — edytowanie tego szablonu pozwala zmodyfikować format przedrostka tematu zainfekowanej wiadomości e-mail. Korzystając z tej funkcji, można zastąpić temat wiadomości „Witaj” następującym formatem: „[wykryto %NAZWAOBIEKTU%] Witaj”. Zmienna %DETECTIONNAME% zawiera nazwę wykrytego obiektu.

Ochrona przed spamem

Niepożądana poczta e-mail — spam — to jeden z najpoważniejszych problemów komunikacji elektronicznej. Spam stanowi obecnie aż 30% wszystkich wysyłanych wiadomości e-mail. Ochrona przed spamem służy jako rozwiązanie zabezpieczające przed tym problemem. Połączenie kilku metod zabezpieczania poczty e-mail umożliwiło modułowi ochrony przed spamem zapewnienie bezpieczeństwa skrzynek pocztowych. Aby skonfigurować ochronę przed spamem, otwórz **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Ochrona przed spamem**.



Jedną z istotnych zasad stosowanych w celu wykrywania spamu jest identyfikacja niepożądanej poczty e-mail na podstawie wstępnie zdefiniowanych zaufanych adresów (dopuszczonych) i adresów kojarzonych ze spamem (zablokowanych).

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.

Włącz 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 przed spamem w programie ESET Internet Security umożliwia skonfigurowanie różnych parametrów wiadomości.

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 Internet Security z menu kontekstowego użytkownik może wybrać jedną z dostępnych opcji.

Użyj folderu — umożliwia wskazanie niestandardowego folderu, do którego mają trafiać po wykryciu zainfekowane wiadomości e-mail.

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 — aparat antyspamowy programu ESET Internet Security przypisuje każdej przeskanowanej wiadomości wynik spamu. Wiadomość zostanie zarejestrowana w dzienniku ochrony przed spamem (Główne okno programu > **Narzędzia** > **Więcej narzędzi** > **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.

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 skonfigurować je jednocześnie.

ESET Internet Security umożliwia ochronę przed spamem w programach Microsoft Outlook, Outlook Express, Windows Mail i Windows Live Mail.

Wynik przetwarzania adresów

Podczas dodawania nowych adresów lub zmiany akcji podjętej dla adresu e-mail, produkt ESET Internet Security wyświetla komunikaty z powiadomieniami. Zawartość powiadomień różni się w zależności od czynności, którą chce wykonać użytkownik.

Zaznaczenie pola wyboru **Nie pytaj ponownie** spowoduje, że od następnego razu dana czynność będzie wykonywana automatycznie, bez wyświetlania komunikatu.

Listy adresów antyspamowych

Funkcja ochrony przed spamem w programie ESET Internet Security umożliwia konfigurowanie różnych parametrów dotyczących książek adresowych.

Włącz listę adresów użytkownika — włącz tę opcję, aby aktywować listę adresów użytkownika.

Lista adresów użytkownika — lista adresów e-mail, na której można dodawać, edytować lub usuwać adresy, aby zdefiniować reguły antyspamowe. Reguły podane na tej liście będą miały zastosowanie do bieżącego użytkownika.

Włącz globalną listę adresów — włącz tę opcję, aby aktywować globalną listę adresów wspólną dla wszystkich użytkowników na tym urządzeniu.

Globalna lista adresów — lista adresów e-mail, na której można dodawać, edytować lub usuwać adresy, aby zdefiniować reguły antyspamowe. Reguły podane na tej liście będą miały zastosowanie do wszystkich użytkowników.

Automatycznie zezwalaj i dodawaj do listy adresów użytkownika

Adresy z książki adresowej traktuj jako zaufane – Adresy z Twojej listy kontaktów będą traktowane jako zaufane, bez konieczności dodawania ich do listy adresów użytkownika.

Dodaj adresy odbiorców z wiadomości wysyłanych — umożliwia dodawanie adresów odbiorców z wysyłanych wiadomości do listy adresów użytkownika z oznaczeniem dozwolone.

Dodaj adresy z wiadomości z klasyfikacją zmienioną na pożądane — umożliwia dodawanie adresów nadawców z wiadomości, w których przypadku zmieniono klasyfikację na wiadomości Pożądane do listy adresów użytkownika z oznaczeniem dozwolone.

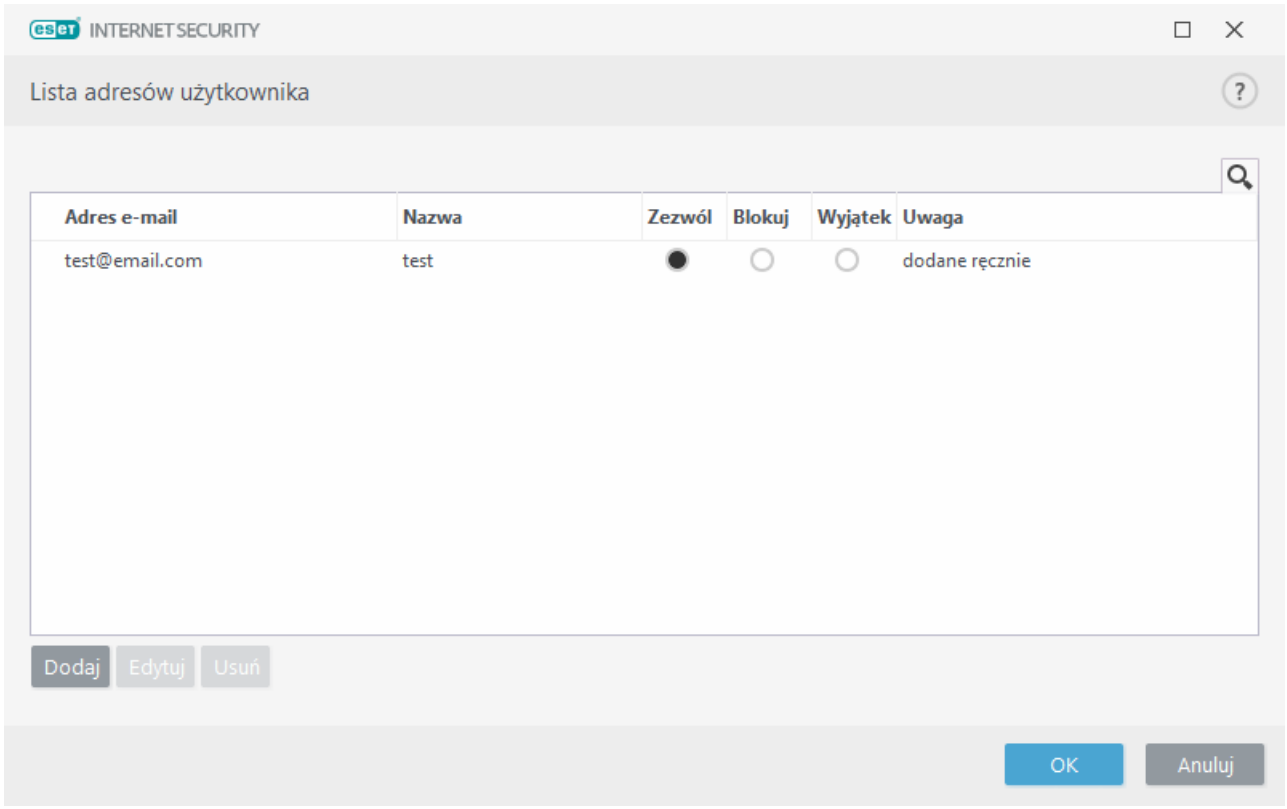
Automatycznie dodaj do listy adresów użytkownika jako wyjątek

Dodaj adresy z własnych kont — umożliwia dodawanie adresów z istniejących kont pocztowych w programie poczty e-mail do listy adresów użytkownika z oznaczeniem wyjątek.

Listy adresów

W celu zapewnienia ochrony przed niechcianymi wiadomościami e-mail, ESET Internet Security umożliwia klasyfikowanie adresów e-mail na listach adresów.

Aby edytować listy adresów, otwórz **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona programów poczty e-mail** > **Listy adresów antyspamowych** i kliknij **Edytuj** obok **Lista adresów użytkownika** lub **Globalna lista adresów**.



Kolumny

Adres e-mail – Adres, którego dotyczy reguła.

Nazwa – Nazwa reguły niestandardowej.

Zezwalaj/Blokuj/Wyjątek — przyciski opcji służące do określania, którą czynność należy wykonać dla danego adresu e-mail (kliknij przycisk opcji w preferowanej kolumnie, aby szybko zmienić czynność):

- **Zezwalaj** – Adresy, które są uważane za bezpieczne i od których chcesz otrzymywać wiadomości.
- **Blokuj** — adresy, które są uważane za niebezpieczne/spam i od których nie chcesz otrzymywać wiadomości.
- **Wyjątek** – Adresy, które są zawsze sprawdzane pod kątem spamu i które mogą być sfałszowane metodą spoofingu i wykorzystane do wysyłania spamu.

Uwaga — informacje o sposobie utworzenia reguły oraz wskazanie, czy dotyczy całej domeny / domen niższego poziomu.

Zarządzanie adresami

- **Dodaj** — kliknij, aby dodać regułę dla nowego adresu.
- **Edytuj** — wybierz i kliknij, aby edytować istniejącą regułę.
- **Usuń** — zaznacz i kliknij, aby usunąć regułę z listy adresów.

Dodawanie/edytowanie adresu

W tym oknie można dodać lub edytować adres na liście adresów antyspamowych oraz skonfigurować podjęte działania:

Adres e-mail — adres, do którego będzie miała zastosowanie reguła.

Nazwa — nazwa reguły niestandardowej.

Czynność — czynność, którą należy wykonać, jeśli adres e-mail kontaktu jest zgodny z adresem podanym w polu **Adres e-mail**:

- **Zezwalaj** — adresy, które są uważane za bezpieczne i od których chcesz otrzymywać wiadomości.
- **Blokuj** — adresy, które są uważane za niebezpieczne/spam i od których nie chcesz otrzymywać wiadomości.
- **Wyjątek** — adresy, które są zawsze sprawdzane pod kątem spamu i które mogą być sfałszowane metodą spoofingu i wykorzystane do wysyłania spamu.

Cała domena — zaznaczenie tej opcji powoduje zastosowanie reguły do całej domeny, do której należy dany kontakt (nie tylko do adresu podanego w polu **Adres e-mail**, ale do wszystkich adresów e-mail w domenie *address.info*).

Domeny niższego poziomu — zaznaczenie tej opcji powoduje zastosowanie reguły do domen niższego poziomu, do których należy dany kontakt (*address.info* to domena, a *my.address.info* to domena podrzędna).

Ochrona dostępu do stron internetowych

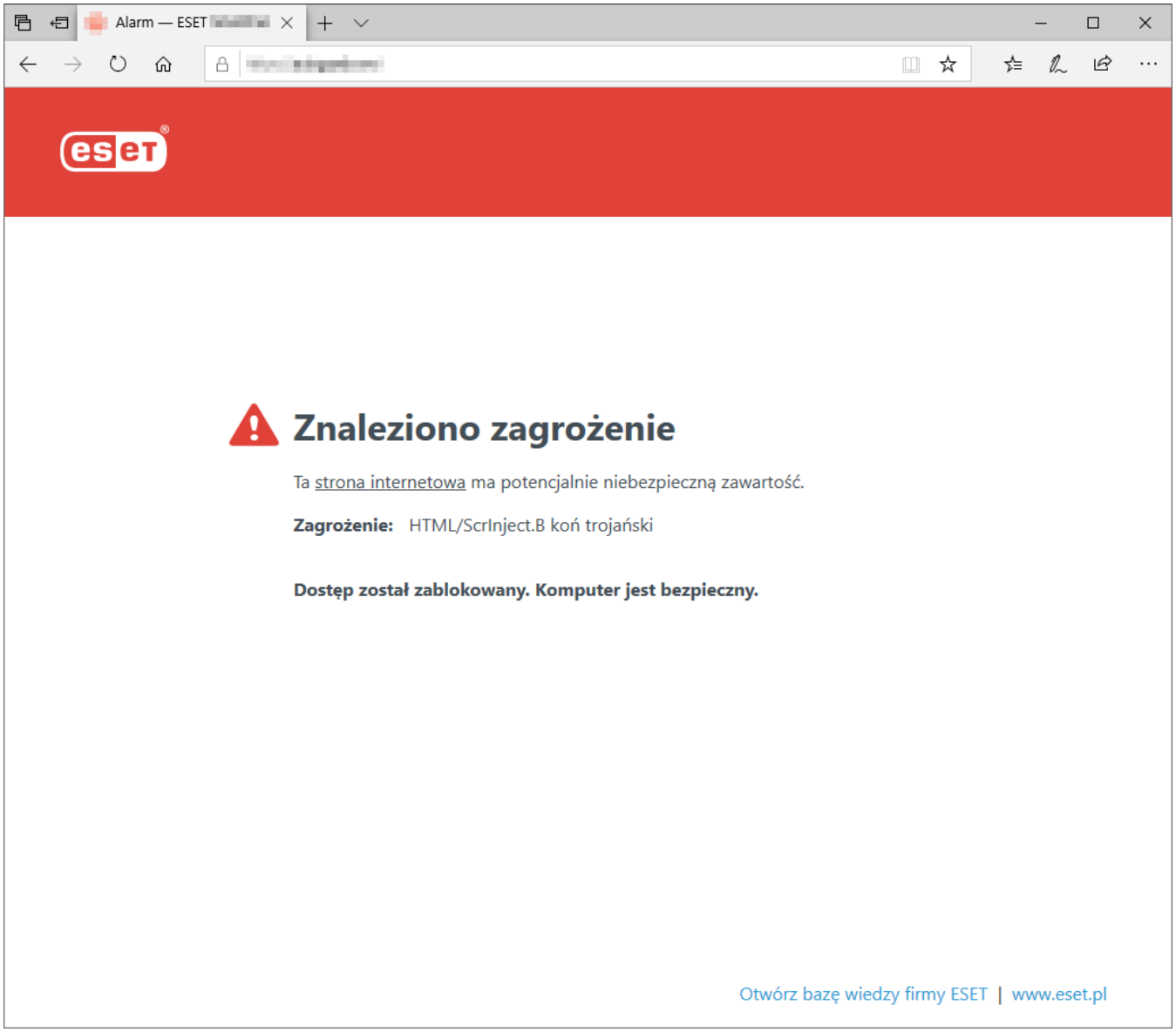
Zapewnianie połączenia z Internetem jest standardową funkcją komputera osobistego. Niestety komunikacja internetowa stała się głównym sposobem przenoszenia szkodliwego kodu. Ochrona dostępu do stron internetowych polega na monitorowaniu realizowanej między przeglądarkami internetowymi i zdalnymi serwerami 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, wybierając kolejno opcje **Ustawienia** > **Ochrona internetowa** > **Ochrona dostępu do stron internetowych**.



Jeśli witryna internetowa jest zablokowana, funkcja Ochrona dostępu do stron internetowych spowoduje wyświetlenie w przeglądarce następującego komunikatu:



Ilustrowane instrukcje

Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:

- Wyłączanie bezpiecznej strony internetowej z blokowania przez ochronę dostępu do stron internetowych
- Blokowanie witryny internetowej przy użyciu programu ESET Internet Security

---

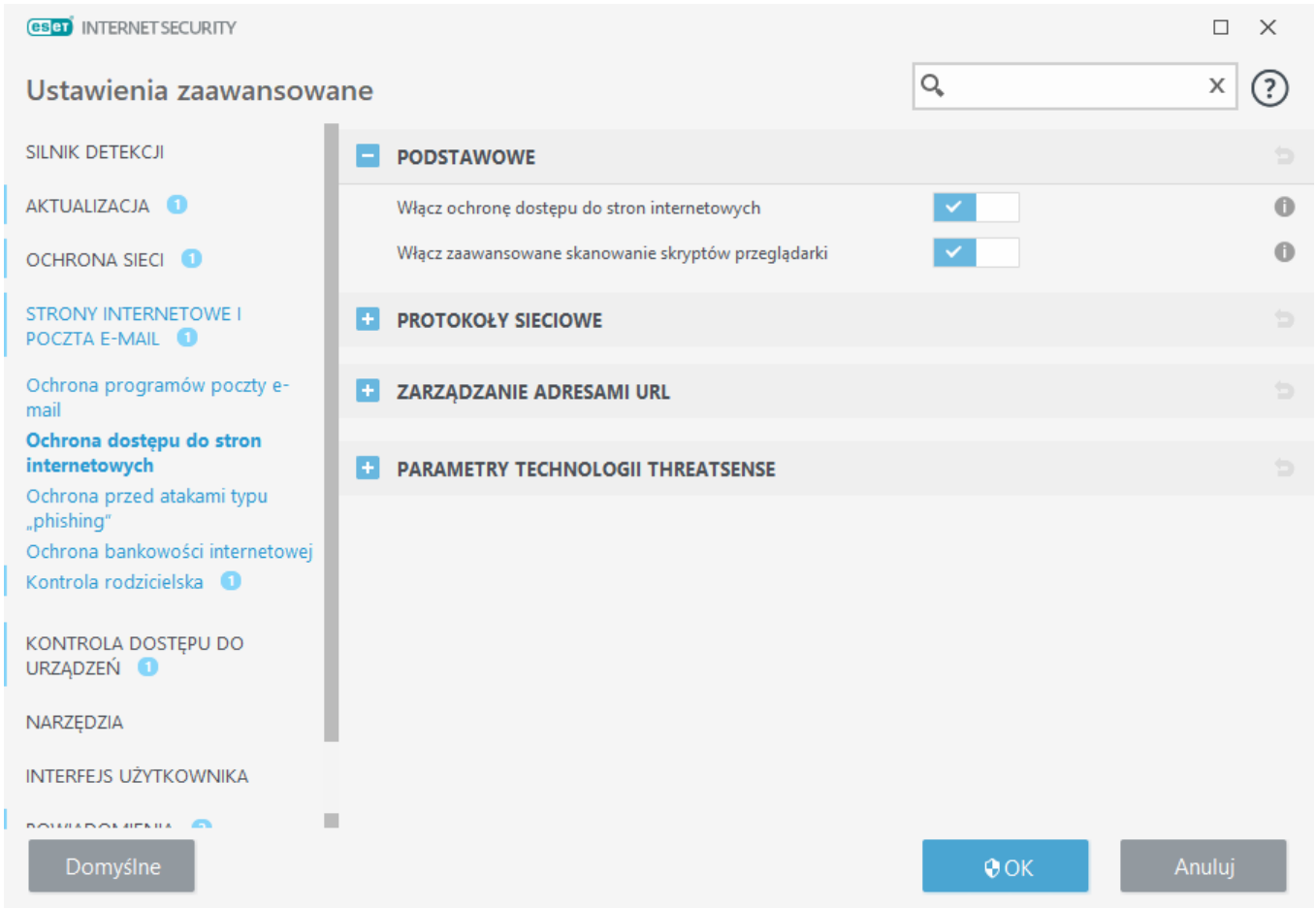
W obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona dostępu do stron internetowych** dostępne są następujące opcje:

Podstawowa — aby włączyć lub wyłączyć tę funkcję w obszarze Ustawienia zaawansowane.

Protokoły sieciowe — umożliwia skonfigurowanie monitorowania protokołów standardowych, które są używane w większości przeglądarek internetowych.

Zarządzanie adresami URL — umożliwia wskazanie adresów URL, 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.



Ustawienia zaawansowane ochrony dostępu do stron internetowych

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

Włącz ochronę dostępu do stron internetowych — gdy ta opcja jest wyłączona, ochrona dostępu do stron internetowych i ochrona przed atakami typu „phishing" nie jest włączana. Ta opcja jest dostępna tylko wówczas, gdy włączone jest filtrowanie protokołu SSL/TLS.

Włącz zaawansowane skanowanie skryptów przeglądarki — gdy ta opcja jest włączona, wszystkie programy JavaScript wykonywane w przeglądarkach internetowych są sprawdzane przy użyciu silnika detekcji.

Zdecydowanie zaleca się, aby ochrona dostępu do stron internetowych była włączona.

Protokoły sieciowe

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

Ustawienia skanera protokołu HTTP

Ruch sieciowy HTTP jest monitorowany zawsze na wszystkich portach i w przypadku wszystkich aplikacji.

Ustawienia skanera protokołu HTTPS

Program ESET Internet 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 Internet Security sprawdza połączenia, używając protokołów SSL (Secure Socket Layer) i TLS (Transport Layer Security). W programie skanowany jest wyłącznie ruch w portach (443, 0-65535) zdefiniowanych w obszarze **Porty używane przez protokół HTTPS**, niezależnie od wersji systemu operacyjnego.

Komunikacja szyfrowana będzie skanowana domyślnie. Aby wyświetlić ustawienia skanera, otwórz stronę Ustawienia zaawansowane > **Strony internetowe i poczta e-mail** > **SSL/TLS**.

Zarządzanie adresami URL

W sekcji Zarządzanie adresami URL można wskazać adresy HTTP, które mają być blokowane, dozwolone lub wyłączone ze skanowania treści.

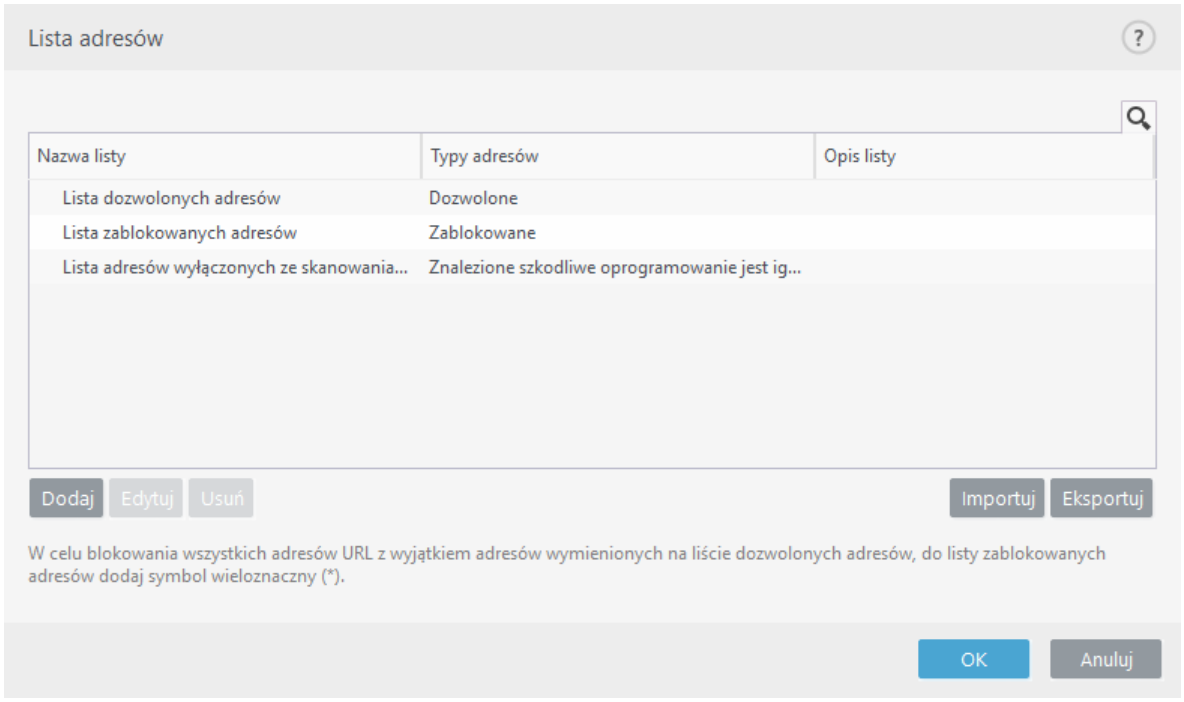
Jeśli oprócz filtrowania stron internetowych HTTP mają być również filtrowane adresy HTTPS, należy wybrać opcję Włącz filtrowanie protokołu SSL/TSL. W przeciwnym razie dodane zostaną tylko domeny HTTPS, które już były odwiedzane, a nie pełny adres URL.

Witryny internetowe wyszczególnione w wykazie **Lista zablokowanych adresów** nie będą dostępne, chyba że zostaną również uwzględnione w zestawieniu **Lista dozwolonych adresów**. Witryny internetowe z wykazu **Lista adresów wyłączonych ze skanowania treści** nie są poddawane skanowaniu w poszukiwaniu szkodliwego kodu w momencie uzyskiwania do nich dostępu.

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

Na listach nie można używać symboli specjalnych: * (gwiazdka) oraz ? (znak zapytania). Gwiazdka zastępuje dowolny ciąg znaków, a znak zapytania — dowolny symbol. Szczególną ostrożność należy zachować podczas określania adresów wyłączonych, ponieważ lista powinna zawierać wyłącznie zaufane i bezpieczne adresy. 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 wybrać opcję **Aktywna lista**. Aby otrzymywać powiadomienia podczas wprowadzania adresu z bieżącej listy, należy wybrać opcję **Powiadom o zastosowaniu**.

> **Zaufane domeny**
> Adresy nie będą filtrowane, jeśli włączono ustawienie **Strony internetowe i poczta e-mail** > **SSL/TLS** > **Nie uwzględniaj połączeń z zaufanymi domenami** i domena jest uznawana za zaufaną.



Elementy sterujące

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, a druga lista może obejmować własną czarną listę użytkownika. Ułatwia to uaktualnianie listy zewnętrznej bez ingerowania w listę użytkownika.

Edytuj — umożliwia modyfikację istniejących list. Ta opcja służy do dodawania i usuwania adresów.

Usuń — umożliwia usuwanie istniejących list. Opcja dostępna wyłącznie w przypadku list utworzony przy użyciu opcji **Dodaj** — niedostępna dla list domyślnych.

Lista adresów URL

W tej sekcji można określić listę adresów HTTP, które będą blokowane, dozwolone lub wyłączone ze sprawdzania.

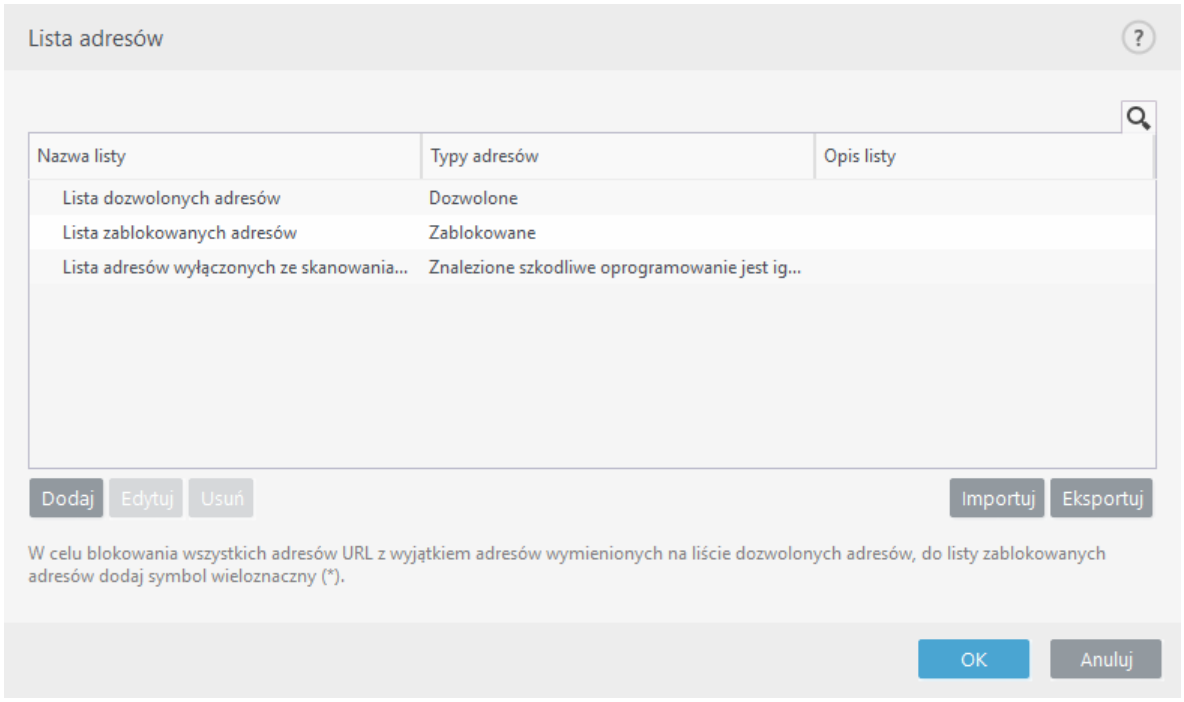
Domyślnie dostępne są trzy następujące listy:

- **Lista adresów wyłączonych ze skanowania treści** — dla żadnego z adresów dodanych do tej listy nie będzie wykonywane sprawdzanie w poszukiwaniu szkodliwego kodu.

- **Lista dozwolonych adresów** — jeśli włączona jest opcja Zezwól na dostęp tylko do adresów HTTP z listy dozwolonych adresów, a lista zablokowanych adresów zawiera wpis * (wszystko), użytkownik będzie mógł uzyskać dostęp tylko do adresów zawartych na tej pierwszej liście. Adresy na tej liście są dozwolone nawet wówczas, gdy zawarte są również na liście zablokowanych adresów.

- **Lista zablokowanych adresów** — użytkownik nie będzie miał dostępu do adresów określonych na tej liście, chyba że występują one również na liście dozwolonych adresów.

Aby utworzyć nową listę, kliknij przycisk **Dodaj**. Aby usunąć wybrane listy, kliknij przycisk **Usuń**.



Ilustrowane instrukcje

Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:

- Wyłączanie bezpiecznej strony internetowej z blokowania przez ochronę dostępu do stron internetowych
- Blokowanie witryny internetowej za pomocą produktów ESET do systemu Windows przeznaczonych dla użytkowników domowych

Więcej informacji można znaleźć w sekcjiZarządzanie adresami URL.

Tworzenie nowej listy adresów URL

W tej sekcji można określić listę adresów/masek URL, które będą blokowane, dozwolone lub wyłączone ze sprawdzania.

Podczas tworzenia nowej listy można skonfigurować następujące opcje:

Typ listy adresów — dostępne są trzy typy list:

- **Wyłączone ze sprawdzania** — dla żadnego z adresów dodanych do tej listy nie będzie wykonywane sprawdzanie w poszukiwaniu złośliwego kodu.

- **Zablokowane** — użytkownik nie będzie miał dostępu do adresów określonych na tej liście.

- **Dozwolone** — jeśli jest włączona opcja Zezwól na dostęp tylko do adresów HTTP z listy dozwolonych adresów, a lista zablokowanych adresów zawiera wpis * (wszystko), użytkownik będzie mógł uzyskać dostęp tylko do adresów zawartych na tej pierwszej liście. Adresy na tej liście są dozwolone nawet wówczas, gdy odpowiadają również wpisowi na liście zablokowanych adresów.

Nazwa listy — umożliwia nadanie nazwy liście. To pole będzie nieaktywne podczas edytowania jednej z trzech wstępnie zdefiniowanych list.

Opis listy — umożliwia wpisanie krótkiego opisu listy (opcjonalnie). To pole będzie nieaktywne podczas edytowania jednej z trzech wstępnie zdefiniowanych list.

Aby uaktywnić listę, należy wybrać opcję **Lista aktywnych** obok tej listy. Aby otrzymywać powiadomienia o każdym użyciu danej listy przy ocenie odwiedzanej strony HTTP, należy wybrać opcję **Powiadom o zastosowaniu**. Powiadomienie zostanie na przykład wysłane w przypadku zablokowania lub udostępnienia strony internetowej figurującej na liście zablokowanych lub dozwolonych adresów. W powiadomieniu znajdzie się nazwa listy, na której wyszczególniona jest dana strona internetowa.

Elementy sterujące

Dodaj — umożliwia dodanie do listy nowego adresu URL (można wprowadzić wiele wartości oddzielonych separatorem).

Edytuj — modyfikowanie adresów figurujących na liście. Jest to możliwe wyłącznie w przypadku adresów utworzonych przy użyciu opcji **Dodaj**.

Usuń — usuwanie adresów figurujących na liście. Jest to możliwe wyłącznie w przypadku adresów utworzonych przy użyciu opcji **Dodaj**.

Importuj — importowanie pliku zawierającego adresy URL (wartości muszą być oddzielone podziałami wiersza, na przykład w formacie *.txt z kodowaniem UTF-8).

Jak dodać maskę adresu URL

Przed wprowadzeniem odpowiedniego adresu lub maski domeny należy zapoznać się z instrukcjami zawartymi w tym oknie dialogowym.

Program ESET Internet Security pozwala użytkownikowi na blokowanie dostępu do określonych witryn internetowych i zapobieganie wyświetleniu ich zawartości w przeglądarce. Pozwala również określić, które adresy mają być wyłączone ze skanowania. Jeśli pełna nazwa serwera zdalnego jest nieznana lub użytkownik chce wskazać grupę serwerów, może użyć znaków (maski). Maski obejmują symbole wieloznaczne, takie jak ? oraz *:

- znak ? zastępuje jeden symbol
- znak * zastępuje dowolny ciąg znaków.

Na przykład zapis *.c?m blokuje wszystkie adresy, których ostatnia część zaczyna się od litery c, a kończy na literze m. Środkowy znak jest dowolny — może to zatem być adres .com, .cam itp.

Znaki „*.” na początku nazwy domeny są traktowane szczególnie. Po pierwsze symbol wieloznaczny „*” nie zastępuje w tym przypadku znaku ukośnika („/”). Pozwala to uniknąć pominięcia maski. Na przykład maska **.domena.com* nie odpowiada adresowi *http://dowolnadomena.com/anypath#.domena.com* (taki przyrostek może zostać dodany do dowolnego adresu URL bez wpływu na pobieranie). Po drugie, znaki „*.” zastępują również w tym szczególnym przypadku pusty ciąg. Dzięki temu przy użyciu jednej maski można uwzględnić całą domenę, wraz z wszelkimi domenami podrzędnymi. Na przykład maska **.domena.com* odpowiada również adresowi *http://domena.com*. Użycie maski **domena.com* byłoby nieprawidłowe, ponieważ uwzględniałaby ona również adres *http://innadomena.com*.

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

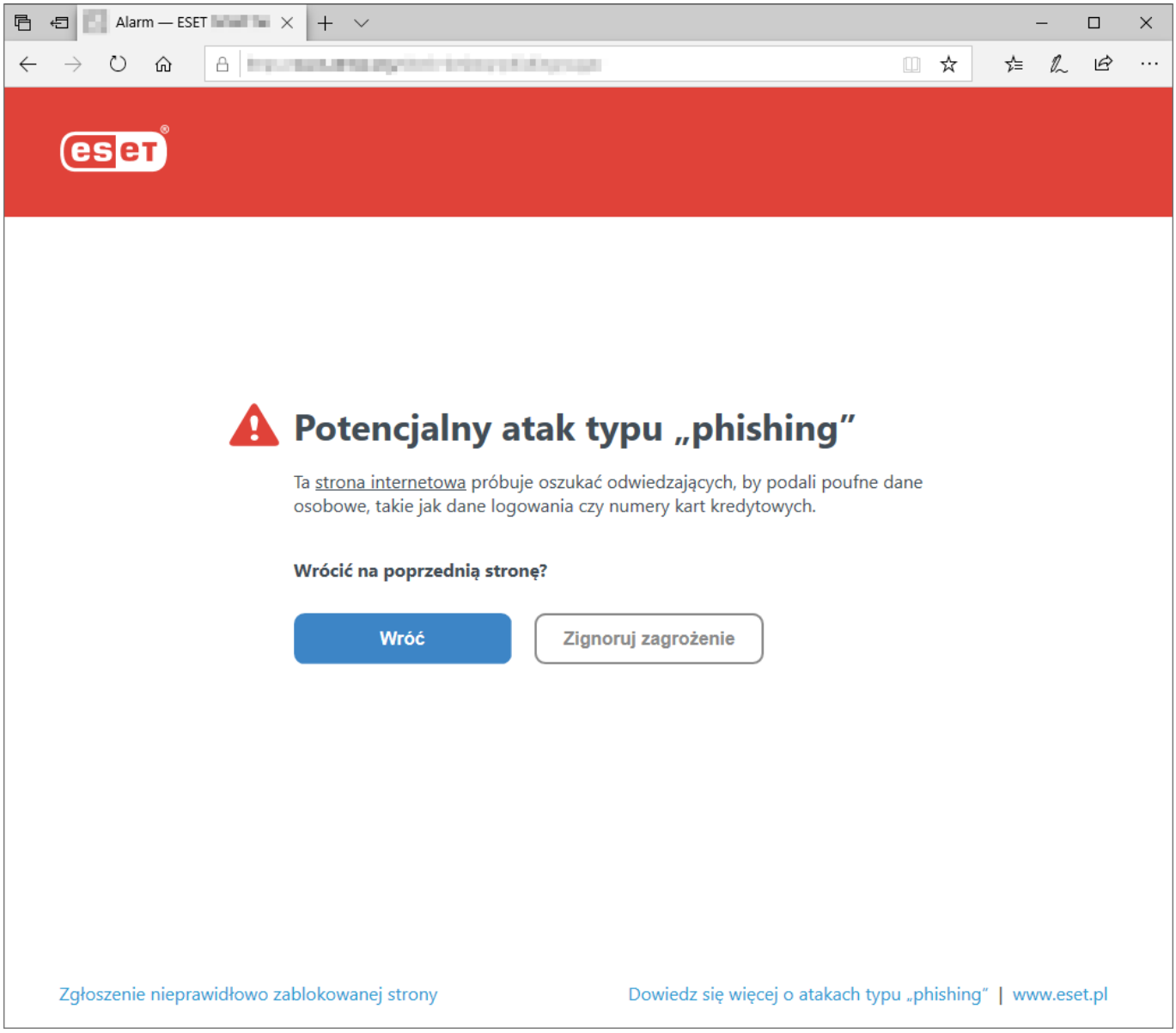
działaniach znajduje się w słowniczku. Program ESET Internet Security chroni komputer przed atakami typu „phishing”, blokując strony internetowe znane z rozpowszechniania takich treści.

Zdecydowanie zalecamy włączenie ochrony przed atakami typu „phishing” w programie ESET Internet 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 Internet 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 **Zignoruj zagrożenie**(niezalecane).



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** > **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.

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 nieprawidłowo blokowaną stronę.

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.).

Ochrona sieci

Konfigurację ochrony sieci można znaleźć w okienku **Konfiguracja** w obszarze **Ochrona sieci**.

Aby wstrzymać lub wyłączyć poszczególne moduły ochrony, kliknij ikonę suwaka .

Wyłączenie modułów ochrony może obniżyć poziom ochrony komputera.



Zapora — tutaj można dostosować tryb filtrowania zapory ESET. Aby wyświetlić bardziej precyzyjne ustawienia, kliknij ikonę koła zębatego i wybierz opcję **Konfiguruj** widoczną obok opcji **Zapora** lub naciśnij klawisz **F5** w celu otwarcia obszaru Ustawienia zaawansowane.

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

Wstrzymaj zaporę (zezwól na cały ruch) — to przeciwieństwo blokowania całego ruchu sieciowego. Wybranie tej opcji oznacza wyłączenie filtrowania przez zaporę 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**.

Blokuj cały ruch — wszystkie połączenia przychodzące i wychodzące będą blokowane przez zaporę. 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**.

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.

Ochrona przed atakami z sieci (IDS) — umożliwia analizowanie zawartości w ruchu sieciowym i ochronę przed atakami z sieci. Każdy ruch uznany za szkodliwy zostanie zablokowany. Jeśli użytkownik połączy się z niezabezpieczoną siecią bezprzewodową lub z siecią o słabej ochronie, program ESET Internet Security poinformuje o tym.

Ochrona przed botnetami — szybkie i precyzyjne wykrywanie szkodliwego oprogramowania w systemie.

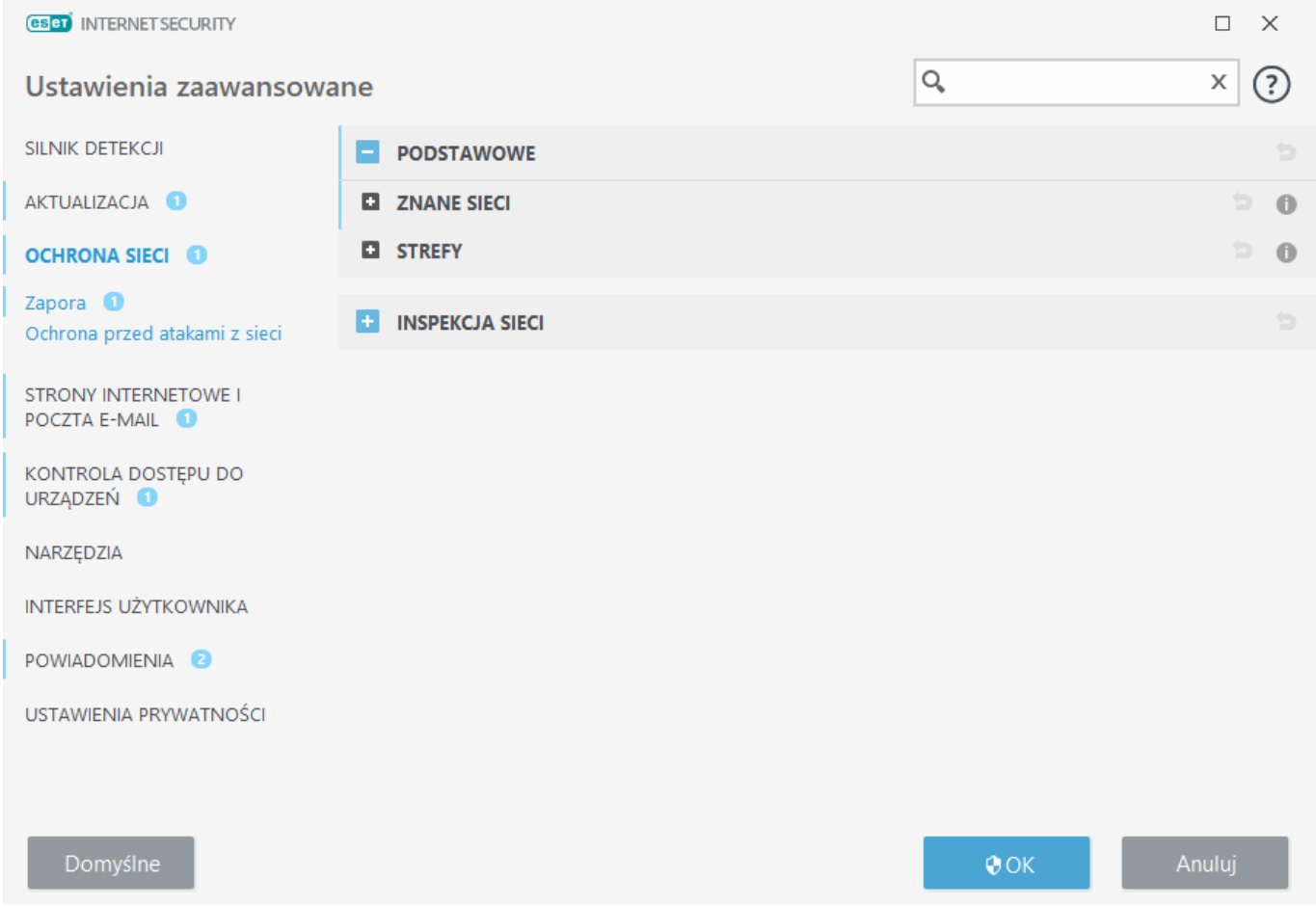
Połączone sieci — umożliwia wyświetlenie sieci, z którymi mają połączenie karty sieciowe. Po kliknięciu łącza pod nazwą sieci pojawi się wyskakujące okno, w którym można skonfigurować sieć jako zaufaną.

Tymczasowa czarna lista adresów IP— umożliwia wyświetlenie listy 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 F1.

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

Ustawienia zaawansowane dotyczące ochrony sieci

W oknie głównym programu kliknij **Ustawienia** > **Ustawienia zaawansowane (F5)** > **Ochrona sieci**.



Podstawowe

Znane sieci

Więcej informacji zawiera sekcja Znane sieci.

Strefy

Strefa reprezentuje zbiór adresów sieciowych, które tworzą jedną grupę logiczną. Aby wyświetlić więcej

informacji, zobacz Strefy ustawień.

Inspekcja sieci

Włącz Inspekcję sieci

Inspekcja sieci pomaga identyfikować luki w zabezpieczeniach sieci domowej, takie jak otwarte porty lub słabe hasło do routera. Zawiera również listę podłączonych urządzeń podzielonych na kategorie według typu.

Powiadamiaj o nowo wykrytych urządzeniach sieciowych

powiadamianie o wykryciu nowego urządzenia w sieci.

Znane sieci

W przypadku korzystania z komputera, który często łączy się z sieciami niezaufanymi lub sieciami innymi niż zaufana (sieć domowa lub biurowa), zalecamy weryfikację wiarygodności nowej sieci, z którą chcesz się połączyć. Po zdefiniowaniu sieci ESET Internet Security może rozpoznać zaufaną (domową lub biurową) sieć, korzystając z parametrów skonfigurowanych w **Dane identyfikacyjne sieci**. Komputery często łączą się z sieciami, których adres IP jest podobny do adresów sieci zaufanych. W takim przypadku ESET Internet Security może uznać nieznaną sieć za zaufaną (domową lub biurową). Zalecamy korzystanie z **Weryfikacji sieci** w celu uniknięcia podobnych sytuacji. Ustawienia znanych sieci można znaleźć, wybierając **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Podstawowe** > **Znane sieci**.

W przypadku połączenia karty sieciowej z siecią lub zmiany ustawień sieci ESET Internet Security przeskanuje listę znanych sieci w poszukiwaniu sieci odpowiadającej nowej. Jeśli **Identyfikacja sieci** oraz **Weryfikacja sieci** (opcjonalne) pasują, sieć zostanie oznaczona w interfejsie jako podłączona. W przypadku braku wyników w ustawieniach identyfikacji sieci zostanie utworzona nowa sieć w celu jej identyfikacji w chwili kolejnego połączenia. Domyślnie nowe połączenie z siecią korzysta z ochrony zdefiniowanej w ustawieniach systemu Windows. Pojawi się okno dialogowe **Wykryto nowe połączenie z siecią**, w którym należy wybrać rodzaj ochrony **Sieć zaufana**, **Sieć niezaufana** lub **Użyj ustawienia systemu Windows**. W przypadku połączenia karty sieciowej ze znaną siecią lub siecią oznaczoną jako **zaufana sieć**, lokalne podsieci dla danej karty zostaną dodane do zaufanych.

Typ ochrony nowych sieci — spośród dostępnych opcji: Opcje **Użyj ustawienia systemu Windows**, **Zapytaj użytkownika** lub **Oznacz jako zaufana** są używane domyślnie dla nowej sieci.

W sekcji **Znane sieci** można skonfigurować nazwę sieci, dane identyfikacyjne sieci, typ zabezpieczeń itp. Aby przejść do Edytora znanych sieci, kliknij pozycję **Edytuj**.

> W przypadku wybrania opcji **Użyj ustawienia systemu Windows** nie zostanie wyświetlone okno dialogowe, a sieć, z którą połączony jest użytkownik, zostanie automatycznie oznaczona zgodnie z ustawieniami systemu Windows. W związku z tym niektóre funkcje (na przykład udostępnianie plików oraz pulpit zdalny) staną się dostępne w nowych sieciach.

Edytor znanych sieci

Znane sieci można konfigurować ręcznie w obszarze **Ustawienia zaawansowane** > **Ochrona sieci** > **Podstawowe** > **Znane sieci** po kliknięciu pozycji **Edytuj**.

Kolumny

Nazwa — nazwa znanej sieci.

Typ zabezpieczeń — wskazuje, czy ustawienie wybrane dla sieci to **zaufana**, **niezaufana** lub **użyj ustawienia systemu Windows**.

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

Profil aktualizacji — umożliwia stosowanie utworzonego profilu aktualizacji po połączeniu z tą siecią.

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

W tym miejscu można podać **nazwę sieci** oraz wybrać **typ zabezpieczeń** (zaufana, niezaufana lub użyj ustawienia systemu Windows) dla sieci. Z menu rozwijanego **Profil zapory** należy wybrać profil dla danej sieci. Jeśli sieć korzysta z typu zabezpieczenia **sieć zaufana**, wszystkie bezpośrednio połączone z nią 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).

Ostrzegaj o słabym szyfrowaniu sieci Wi-Fi — program ESET Internet Security informuje o nawiązaniu połączenia z niechronioną siecią bezprzewodową lub siecią ze słabą ochroną.

Profil zapory — wybierz profil zapory używany podczas połączenia z tą siecią.

Aktualizuj profil — wybierz profil aktualizacji używany podczas połączenia z tą siecią.

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

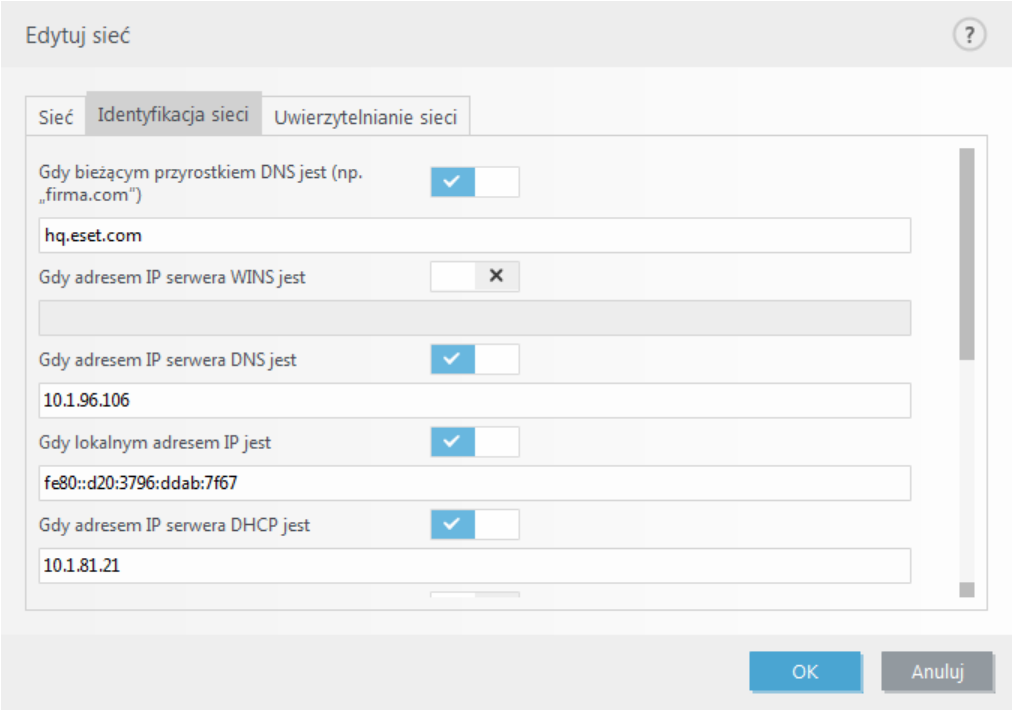
- **Identyfikacja sieci** — wszystkie podane parametry muszą być zgodne z parametrami aktywnego połączenia.

- **Uwierzytelnianie sieci** — w przypadku wybrania serwera uwierzytelniającego musi dojść do pomyślnego

uwierzytelnienia przy użyciu serwera uwierzytelniania ESET.

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.



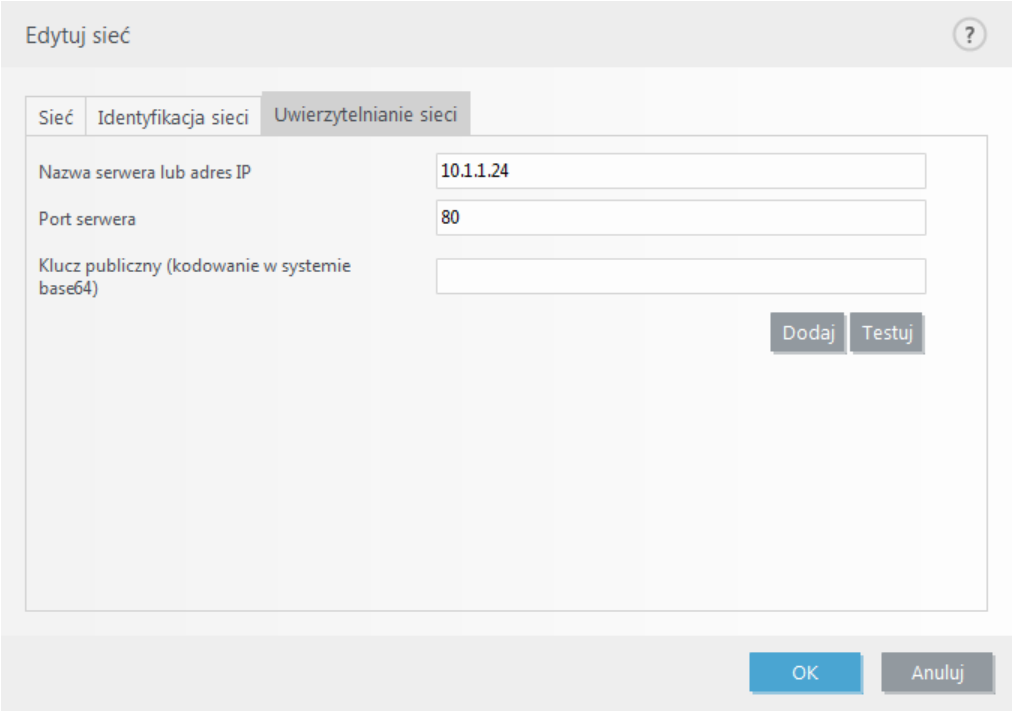
Uwierzytelnianie sieci

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.

Należy pobrać aplikację serwera uwierzytelniania ESET.

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.

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 strefy 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 strefy w trakcie konfigurowania strefy w ustawieniach zapory.

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

Konfigurowanie stref

Strefa to zestaw adresów sieciowych tworzących jedną grupę logiczną adresów IP. Jest przydatna, gdy użytkownik chce wykorzystać ten sam zestaw adresów w licznych regułach. Każdemu adresowi w danej grupie przypisywane są podobne reguły, określone centralnie dla całej grupy. Jednym z przykładów takiej grupy jest **strefa zaufana**. Strefa zaufana to grupa adresów sieciowych uznanych za całkowicie godne zaufania, które nie są w żaden sposób blokowane przez zaporę.

Aby dodać strefę zaufaną:

1. Otwórz **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Podstawowe** > **Strefy**.
2. Kliknij **Edytuj** obok pozycji **Strefy**.
3. Kliknij **Dodaj**, wpisz **nazwę** i **opis** strefy i wpisz zdalny adres IP w polu **Zdalny adres komputera (IPv4/IPv6, zakres, maska)**.
4. Kliknij przycisk **OK**.

Więcej informacji zawiera sekcja Strefy zapory.

Strefy zapory

Więcej informacji na temat stref można znaleźć w częściKonfigurowanie stref .

Kolumny

Nazwa — nazwa grupy komputerów zdalnych.

Adresy IP — zdalne adresy IP należące do strefy.

Elementy sterujące

Po **dodaniu** lub **zmodyfikowaniu** strefy dostępne są te pola:

Nazwa — nazwa grupy komputerów zdalnych.

Opis — ogólny opis grupy.

Adres zdalnego komputera (IPv4, IPv6, zakres, maska) — umożliwia dodanie zdalnego adresu, zakresu adresów lub podsieci.

Usuń — umożliwia usunięcie strefy z listy.

Należy pamiętać, że nie można usunąć wstępnie zdefiniowanych stref.

Zapora

Zapora kontroluje cały przychodzący i wychodzący ruch sieciowy komputera. Jej działanie polega na zezwalaniu na pojedyncze połączenia sieciowe lub ich odmawianiu na podstawie określonych reguł filtrowania. Zapora zapewnia ochronę przed atakami z komputerów zdalnych i umożliwia blokowanie niektórych potencjalnie niebezpiecznych usług.

Podstawowe

Włącz zaporę

zalecamy pozostawienie tej opcji włączonej w celu zapewnienia ochrony systemu. Gdy zapora jest włączona, ruch sieciowy jest skanowany w obu kierunkach.

Oceniaj także reguły zapory systemu Windows

W trybie automatycznym przepuszczaj także ruch przychodzący, na który zezwalają reguły zapory systemu Windows, o ile nie blokują go reguły programu ESET.

Tryb filtrowania

Zachowanie zapory zmienia się w zależności od trybu filtrowania. Tryby filtrowania mają również wpływ na wymagany poziom interakcji użytkownika.

Dostępne są następujące tryby filtrowania zapory programu ESET Internet Security:

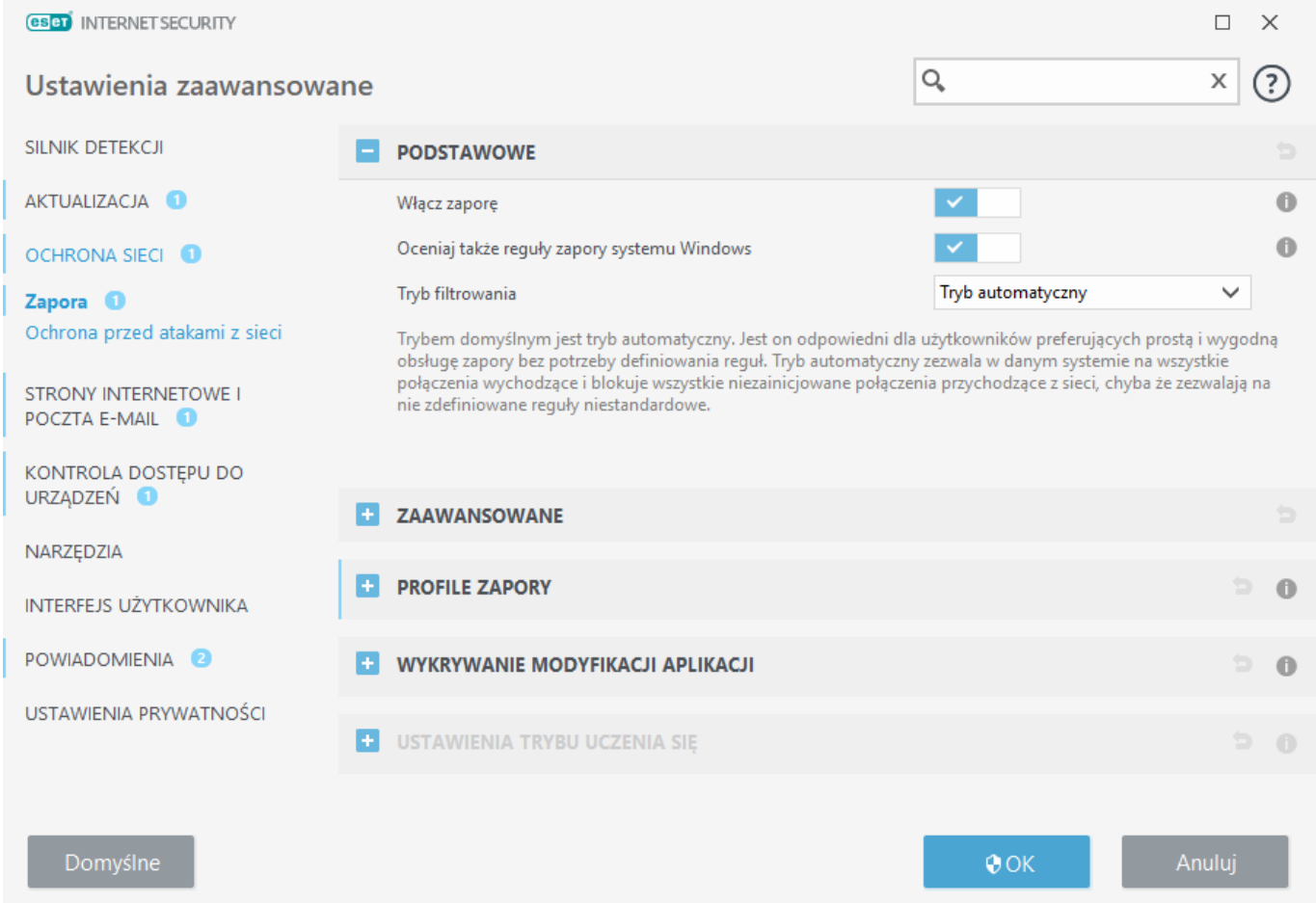
Tryb filtrowania	Opis
Tryb automatyczny	Tryb domyślny. Ten tryb jest odpowiedni dla użytkowników preferujących prostą i wygodną obsługę zapory bez potrzeby definiowania reguł. Można tworzyć niestandardowe, definiowane przez użytkownika reguły, lecz w **trybie automatycznym** nie jest to wymagane. Tryb automatyczny zezwala na cały ruch wychodzący na danym komputerze i blokuje większość ruchu przychodzącego (z wyjątkiem ruchu ze strefy zaufanej, zgodnie z zezwoleniami ustawionymi w sekcji IDS i opcje zaawansowane/Dozwolone usługi oraz odpowiedzi na ostatnią komunikację wychodzącą).
Tryb interaktywny	umożliwia tworzenie niestandardowych konfiguracji zapory. Po wykryciu połączenia, którego nie dotyczą żadne istniejące reguły, zostanie wyświetlone okno dialogowe informujące o nieznanym połączeniu. Okno to umożliwia zezwolenie na komunikację lub odmowę, a podjęta decyzja może zostać zapisana jako nowa reguła zapory. 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.

Tryb filtrowania	Opis
Tryb uczenia się	Automatycznie tworzy oraz zapisuje reguły. Ten tryb jest najodpowiedniejszy w przypadku początkowej konfiguracji zapory, jednak nie powinien pozostawać włączony przez dłuższy czas. Interakcja ze strony użytkownika nie jest wymagana, ponieważ program ESET Internet Security zapisuje reguły zgodnie ze wstępnie zdefiniowanymi parametrami. W celu uniknięcia zagrożeń bezpieczeństwa tryb uczenia się powinien być używany tylko, dopóki nie zostaną utworzone wszystkie reguły dla niezbędnych połączeń.

Zaawansowane

Reguły

W sekcji ustawień reguł można obejrzeć wszystkie reguły stosowane względem ruchu generowanego przez poszczególne aplikacje w ramach stref zaufanych i Internetu.



Gdy komputer zostanie zaatakowany przez botnet, można utworzyć regułę IDS. Regułę można modyfikować w obszarze **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Ochrona przed atakami z sieci** > **Reguły IDS** przez kliknięcie pozycji **Edytuj**.

Dozwolone usługi

Skonfiguruj dostęp do typowych usług sieciowych uruchomionych na komputerze. Więcej informacji można w sekcji Dozwolone usługi.

Profile zapory

Profile zapory umożliwiają dostosowanie działania zapory ESET Internet Security, pozwalając określić różne zestawy reguł na potrzeby różnych sytuacji.

Wykrywanie modyfikacji aplikacji

Funkcja wykrywania modyfikacji aplikacji wyświetla powiadomienia, gdy zmodyfikowane aplikacje z istniejącą regułą zapory próbują nawiązać połączenie.

Profile zapory

Profile umożliwiają sterowanie działaniem zapory programu ESET Internet Security. Podczas tworzenia lub edytowania reguły zapory 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 aktywnego profilu. Aby z łatwością modyfikować sposób działania zapory, można utworzyć wiele profili z różnymi regułami przypisanymi do kart sieciowych lub 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) > **Ochrona sieci** > **Znane sieci** > **Edytuj** 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 kartę sieciową, kliknąć opcję **Edytuj** obok pozycji **Profile przypisane do kart sieciowych**, przeprowadzić edycję wybranej karty sieciowej i wybrać profil z menu rozwijanego **Domyślny profil zapory**.

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

Okno dialogowe — Edytuj profile zapory sieciowej

Tutaj znajdują się opcje dotyczące profilu, takie jak **Dodaj**, **Edytuj** czy **Usuń**. Aby można było użyć opcji **Edytuj** lub **Usuń** w stosunku do profilu, musi on zostać wybrany z listy w oknie **Profilezapory**.

Więcej informacji zawiera temat Profile zapory.

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

Elementy sterujące

Dodaj — umożliwia dodanie nowej karty sieciowej.

Edytuj — pozwala edytować istniejące karty sieciowe.

Usuń — wybierz kartę sieciową, a następnie kliknij opcję **Usuń** w celu usunięcia karty sieciowej z listy.

OK/Anuluj — aby zapisać zmiany, należy kliknąć przycisk **OK**. Aby zamknąć opcję bez wprowadzania zmian, należy kliknąć opcję **Anuluj**.

Konfigurowanie i używanie reguł

Reguły stanowią zestaw warunków używanych do odpowiedniego testowania wszystkich połączeń sieciowych i wszystkich działań przypisanych do tych warunków. Za pomocą reguł zapory 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** > **Zaawansowane**. Część wstępnie zdefiniowanych reguł jest powiązana z polami wyboru **dozwolonych usług** (IDS i opcje zaawansowane).

Inaczej niż w poprzedniej wersji programu ESET Internet 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. W połączeniach wychodzących jest odwrotnie — system lokalny kontaktuje się z komputerem zdalnym.

W przypadku wykrycia nowego, nieznanego połączenia należy dokładnie rozważyć, czy zezwolić na to połączenie, czy je odrzucić. Niepożądane, niezabezpieczone lub całkowicie nieznane połączenia stanowią zagrożenie dla systemu. Gdy takie połączenie zostanie nawiązane, zalecamy zwrócenie szczególnej uwagi na komputer zdalny i aplikację, które próbują połączyć się z komputerem użytkownika. Wiele ataków polega na próbie pozyskania i

wysłania prywatnych danych lub pobraniu niebezpiecznych aplikacji na stacje robocze hosta. Zapora umożliwia użytkownikowi wykrycie i przerwanie takich połączeń.

Lista reguł zapory

Lista reguł zapory jest dostępna w obszarze **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Zapora** > **Zaawansowane** po kliknięciu opcji **Edytuj** widocznej obok opcji **Reguły**.

Kolumny

Nazwa — nazwa reguły.

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

Protokół — Internet protokół, którego dotyczy reguła.

Profil — wskazuje profil zapory, którego dotyczy reguła.

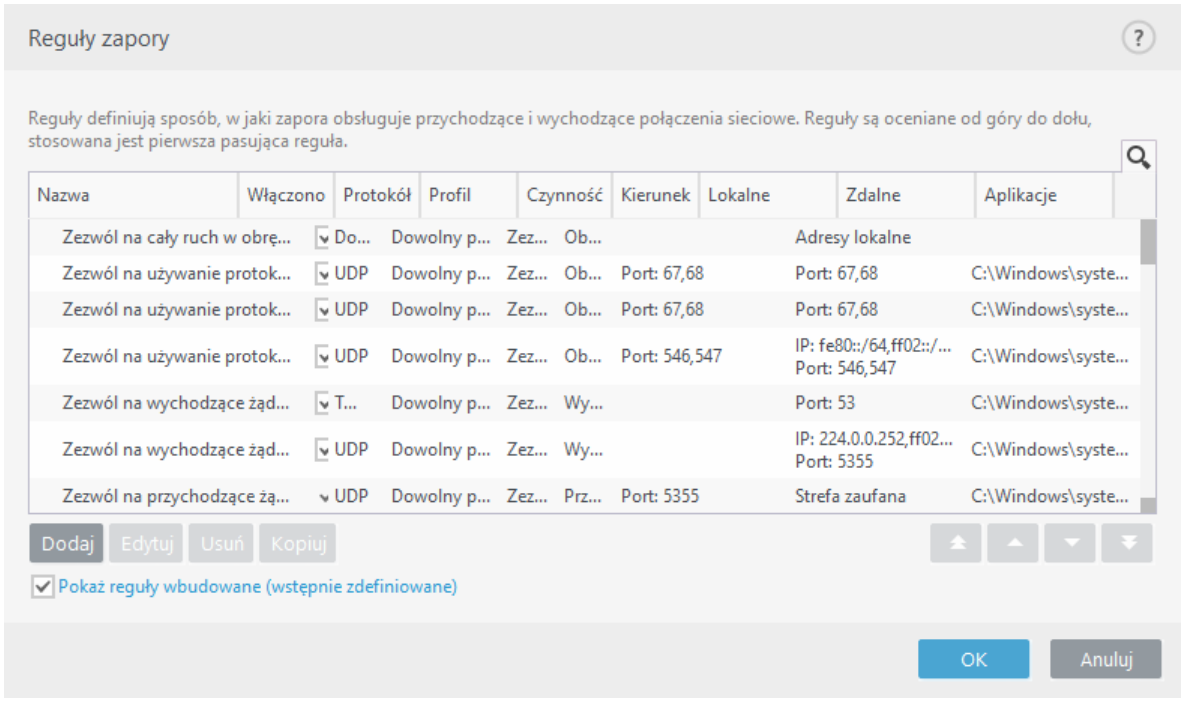
Czynność — wskazuje stan komunikacji (blokuj/zezwalaj/pytaj).

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

Lokalny — zdalny adres/zakres/podsieć IPv4 lub IPv6 i port komputera lokalnego.

Zdalny — zdalny adres/zakres/podsieć IPv4 lub IPv6 i port komputera zdalnego.

Aplikacja — aplikacja, której dotyczy reguła.



Elementy sterujące

Dodaj — umożliwia utworzenie nowej reguły.

Edytuj — umożliwia zmodyfikowanie istniejącej reguły.

Usuń — umożliwia usunięcie istniejącej reguły.

Kopiuj — umożliwia utworzenie kopii wybranej reguły.

Pokaż reguły wbudowane (wstępnie zdefiniowane) — reguły wstępnie zdefiniowane w programie ESET Internet 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).

Kliknij ikonę wyszukiwania w prawym górnym rogu, aby wyszukać reguły według nazwy, protokołu lub portu.

Dodawanie lub edytowanie reguł zapory

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.

Ilustrowane instrukcje

Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:

- Otwieranie lub zamykanie (zezwalanie lub blokowanie) określonego portu w zaporze ESET
- Tworzenie reguły zapory z plików dziennika programu ESET Internet Security

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.

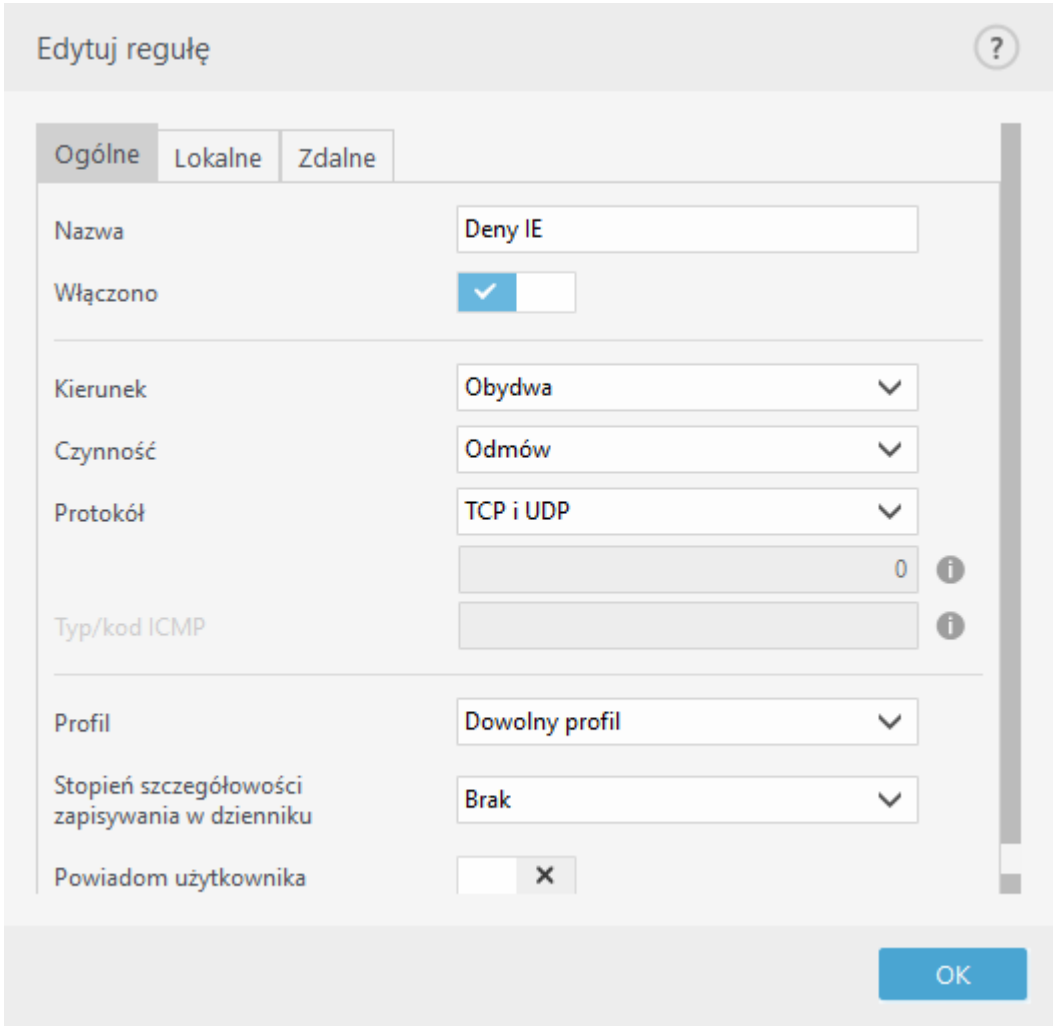
Protokół określa używany w regule protokół transmisji. Z menu rozwijanego wybierz protokół, który ma zostać

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 **Profil**.

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



Utworzymy nową regułę umożliwiającą przeglądarce internetowej Firefox uzyskiwanie dostępu do programu Internet / stron internetowych w sieci lokalnej. W tym przykładzie należy skonfigurować następujące elementy:
1.Na karcie **Ogólne** należy włączyć połączenia wychodzące korzystające z protokołów TCP i UDP.
2.Kliknij kartę **Lokalne**.
3.Wybierz ścieżkę do pliku używanej przeglądarki internetowej, klikając opcję **...** (na przykład *C:\Program Files\Firefox\Firefox.exe*). NIE należy wprowadzać nazwy aplikacji.
4.Na karcie **Zdalne** włącz porty o numerach 80 i 443, jeśli chcesz zezwolić na standardowe przeglądanie Internetu.

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

Reguła zapory — lokalna

Należy wprowadzić nazwę lokalnej aplikacji i określić porty lokalne, do których reguła ma zastosowanie.

Port — numery portów lokalnych. Jeśli nie zostanie wprowadzony żaden numer, reguła będzie stosowana do wszystkich portów. Można dodać pojedynczy port komunikacyjny lub zakres takich portów.

Adres IP — umożliwia dodanie zdalnych adresów, zakresu adresów lub podsieci, w odniesieniu do których stosowana jest reguła. Jeśli nie zostania wprowadzona żadna wartość, reguła będzie stosowana do całej komunikacji.

Strefy — lista dodanych stref.

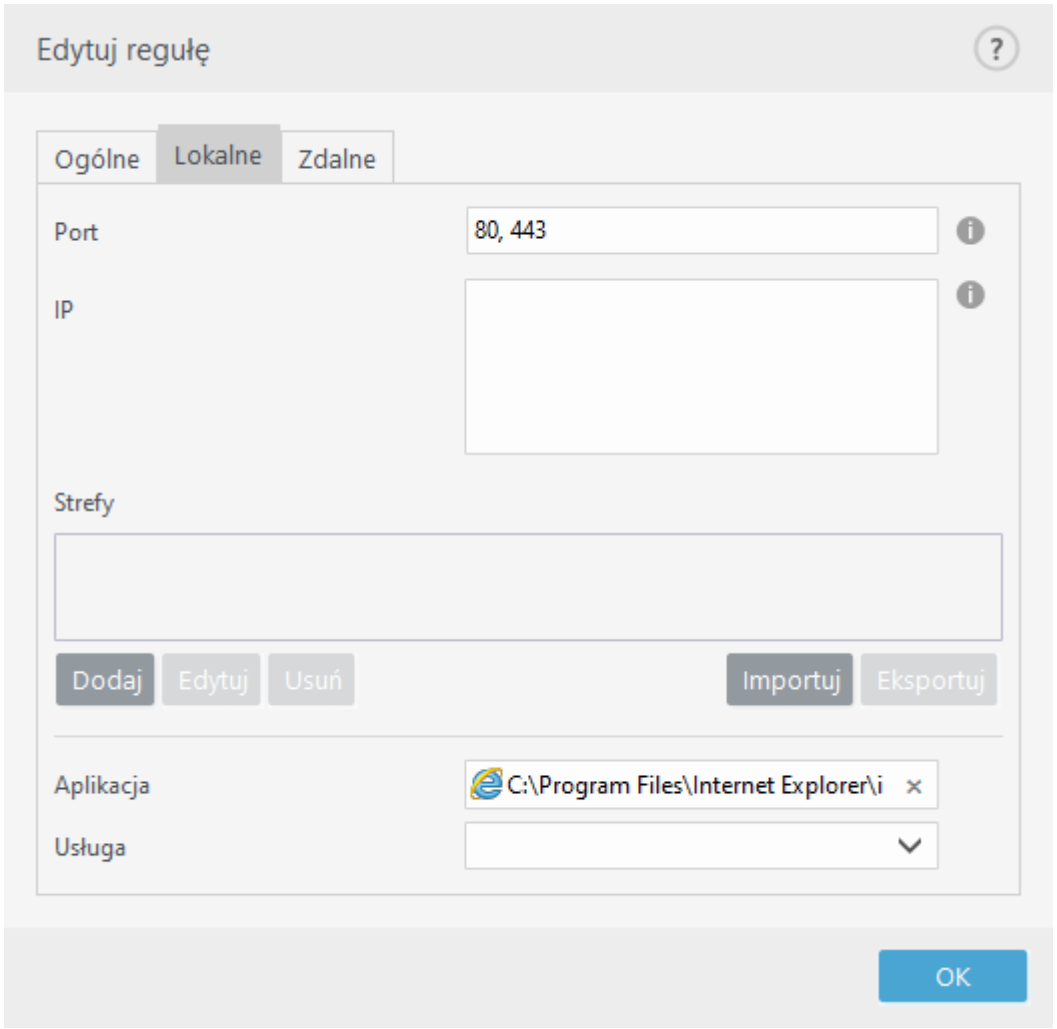
Dodaj — umożliwia dodanie utworzonej strefy z menu rozwijanego. Strefę można utworzyć na karcie Ustawienia strefy.

Usuń— umożliwia usunięcie stref z listy.

Aplikacja — nazwa aplikacji, do której jest stosowana reguła. Należy dodać lokalizację aplikacji, do której stosowana będzie reguła.

Usługa — w tym menu rozwijanym dostępne są usługi systemowe.

> W menu rozwijanym można utworzyć dla kopii dystrybucyjnej regułę, która umożliwi aktualizację przez port 2221 przy użyciu dostępnej w menu rozwijanym usługi EHttpSrv służącej do komunikacji.



Reguła zapory — zdalna

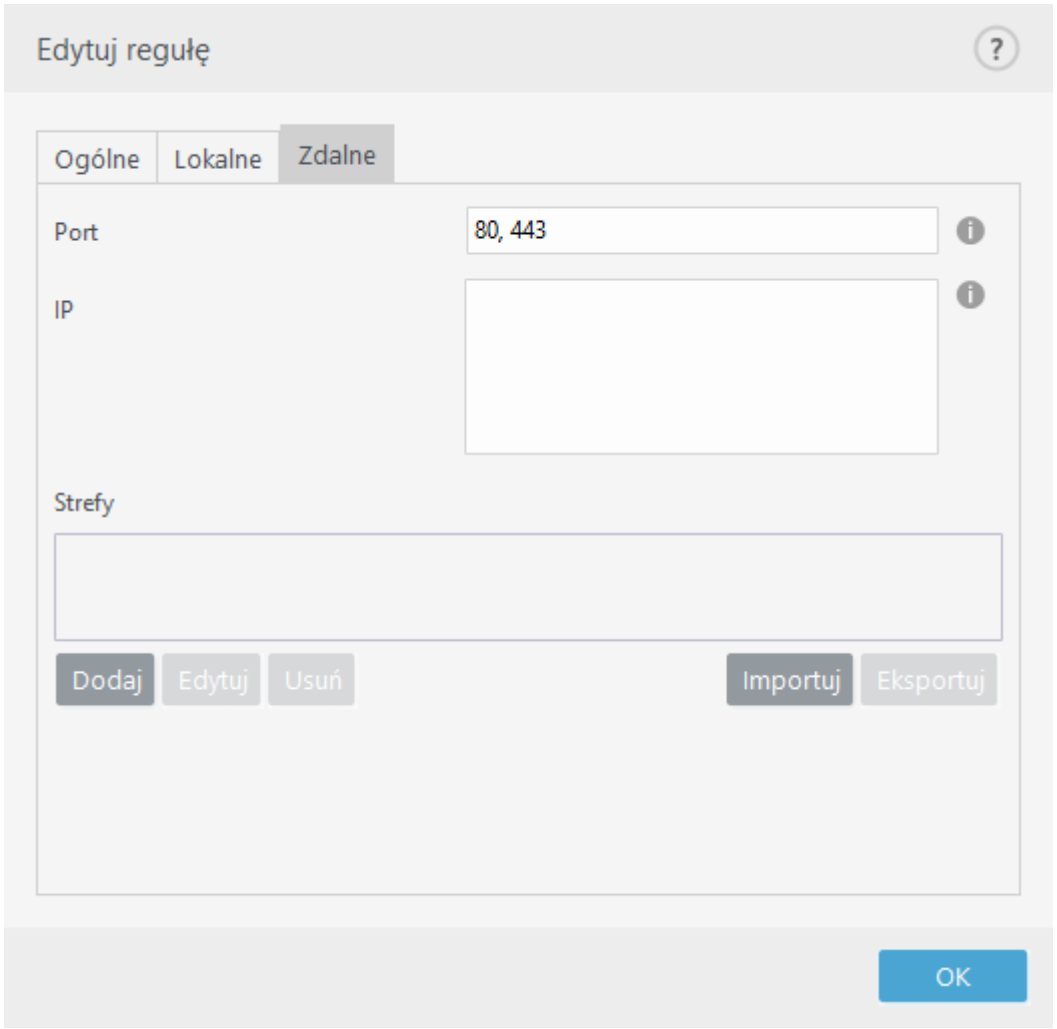
Port — numery portów zdalnych. Jeśli nie zostanie wprowadzony żaden numer, reguła będzie stosowana do wszystkich portów. Można dodać pojedynczy port komunikacyjny lub zakres takich portów.

Adres IP — umożliwia dodanie zdalnego adresu, zakresu adresów lub podsieci. Jest to adres, zakres adresów, podsieć lub strefa zdalna, do których ma mieć zastosowanie dana reguła. Jeśli nie zostanie wprowadzona żadna wartość, reguła będzie stosowana do całej komunikacji.

Strefy — lista dodanych stref.

Dodaj — umożliwia dodanie strefy poprzez wybranie jej z menu rozwijanego. Strefę można utworzyć na karcie Ustawienia strefy.

Usuń— umożliwia usunięcie stref z listy.



Wykrywanie modyfikacji aplikacji

Funkcja wykrywania modyfikacji aplikacji wyświetla powiadomienia, gdy zmodyfikowane aplikacje, dla których istnieje reguła zapory, próbują nawiązać połączenie. Modyfikacja aplikacji polega na tymczasowym lub trwałym zastąpieniu oryginalnej aplikacji inną aplikacją przy użyciu innego pliku wykonywalnego (chroni przed naruszeniami reguł zapory).

Należy pamiętać, że funkcja ta ogólnie nie służy do wykrywania modyfikacji w aplikacjach. Celem korzystania z niej jest unikanie naruszeń istniejących reguł zapory i monitorowane są wyłącznie aplikacje, dla których istnieją określone reguły zapory.

Włącz wykrywanie modyfikacji aplikacji — jeśli ta opcja jest zaznaczona, program sprawdza, czy aplikacje nie zostały w jakiś sposób zmienione (zaktualizowane, zainfekowane itp.). Gdy zmodyfikowana aplikacja spróbuje nawiązać połączenie, użytkownik zostanie o tym powiadomiony przez zaporę.

Zezwalaj na modyfikowanie aplikacji podpisanych (zaufanych) — brak powiadomienia, gdy aplikacja ma tę samą prawidłową sygnaturę cyfrową przed modyfikacją oraz po modyfikacji.

Lista aplikacji wyłączonych ze wykrycia — w oknie tym można dodawać lub usuwać poszczególne aplikacje, dla których dozwolone są modyfikacje bez powiadamiania.

Lista aplikacji wyłączonych z wykrywania

Zapora w programie ESET Internet Security wykrywa zmiany w aplikacjach, dla których istnieją reguły (zobacz sekcję Wykrywanie modyfikacji aplikacji).

W przypadku niektórych aplikacji używanie tej funkcji w celu wyłączenia ich ze sprawdzania przez zaporę może być niepożądane.

Dodaj — otwiera okno, w którym można wybrać aplikację, aby dodać ją do listy aplikacji wykluczonych z wykrywania modyfikacji. Można wybrać pozycję z listy uruchomionych aplikacji z otwartą komunikacją sieciową z istniejącą regułą zapory lub dodać określoną aplikację.

Edytuj — otwiera okno, w którym można wybrać lokalizację aplikacji, która znajduje się na liście aplikacji wykluczonych z wykrywania modyfikacji. Można wybrać pozycję z listy uruchomionych aplikacji z otwartą komunikacją sieciową z istniejącą regułą zapory lub ręcznie zmienić lokalizację.

Usuń — umożliwia usuwanie pozycji z listy aplikacji wykluczonych z wykrywania modyfikacji.

Ustawienia trybu 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 Internet Security zapisuje reguły zgodnie ze wstępnie zdefiniowanymi parametrami.

Stosowanie tego trybu może wystawić system na ryzyko i jest zalecane tylko przy wstępnej konfiguracji zapory.

Wybierz pozycję **Tryb uczenia się** z menu rozwijanego w obszarze **Ustawienia zaawansowane** (F5) > **Zapora** > **Podstawowe** > **Tryb filtrowania**, aby uaktywnić **Opcje trybu uczenia**. Sekcja ta zawiera następujące elementy:

> ⚠ Działając w trybie uczenia się, zapora nie filtruje komunikacji. Wszystkie połączenia przychodzące i wychodzące są dozwolone. W tym trybie komputer nie jest w pełni chroniony przez zaporę.

Tryb ustawiany po zakończeniu trybu uczenia się — określa tryb filtrowania, który zapora ESET Internet Security przywróci po zakończeniu okresu trybu uczenia się. Więcej informacji na temat trybów filtrowania. Po zakończeniu tego trybu opcja **Zapytaj użytkownika** będzie wymagać uprawnień administracyjnych, aby wprowadzić zmiany w trybie filtrowania zapory.

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 do 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.

Ochrona przed atakami z sieci (IDS)

Ochrona przed atakami z sieci (IDS) usprawnia wykrywanie luk zabezpieczeniach w zakresie znanych słabych punktów. Dowiedz się więcej o ochronie przed atakami z sieci w słowniczku.

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. Więcej informacji na temat ochrony przed botnetami można znaleźć w słowniczku.

Reguły IDS — W ramach tej opcji można skonfigurować zaawansowane opcje filtrowania służące do wykrywania różnych typów ataków i luk w zabezpieczeniach, które mogą być wykorzystane do uszkodzenia komputera.

> **Ilustrowane instrukcje**
>
> Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:
>
> - Wyłączanie adresu IP z IDS w programie ESET Internet Security

Wszystkie ważne zdarzenia wykryte przez ochronę sieci są zapisywane w pliku dziennika. Więcej informacji można znaleźć w dzienniku ochrony sieci.

Ochrona przed atakami brute force

Ochrona przed atakami typu brute force blokuje ataki polegające na odgadywaniu haseł dla usług RDP i SMB. Atak brute-force to metoda odkrywania ukierunkowanego hasła poprzez systematyczne wypróbowywanie wszystkich kombinacji liter, cyfr i symboli. Aby skonfigurować ochronę przed atakami Brute-force, w głównym oknie programu kliknij **opcję Ustawienia** > **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Ochrona przed atakami w sieci** > **Ochrona przed atakami Brute-force**.

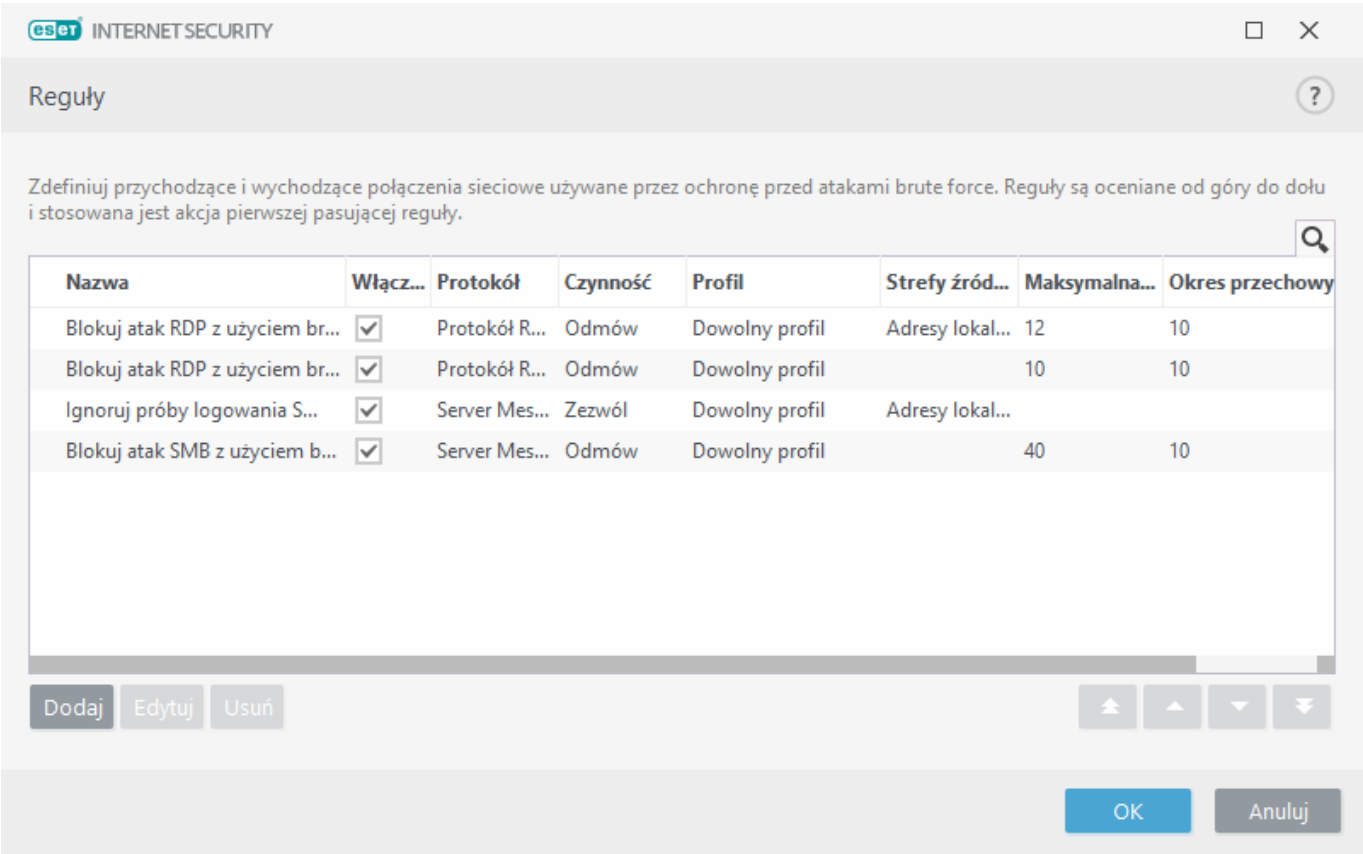
Włącz ochronę przed atakami typu brute force — ESET Internet Security sprawdza zawartość ruchu sieciowego i blokuje próby ataków zgadywania haseł.

Reguły – reguły ochrony przed atakami brute force umożliwiają tworzenie, edytowanie i wyświetlanie reguł dla przychodzących i wychodzących połączeń sieciowych. Więcej informacji zawiera rozdział Reguły.

Reguły

Reguły ochrony przed atakami typu brute force umożliwiają tworzenie, edytowanie i wyświetlanie reguł dla przychodzących i wychodzących połączeń sieciowych. Wstępnie zdefiniowanych reguł nie można edytować ani usuwać.

Zarządzanie regułami ochrony przed atakami brute force



Dodaj — umożliwia utworzenie nowej reguły.

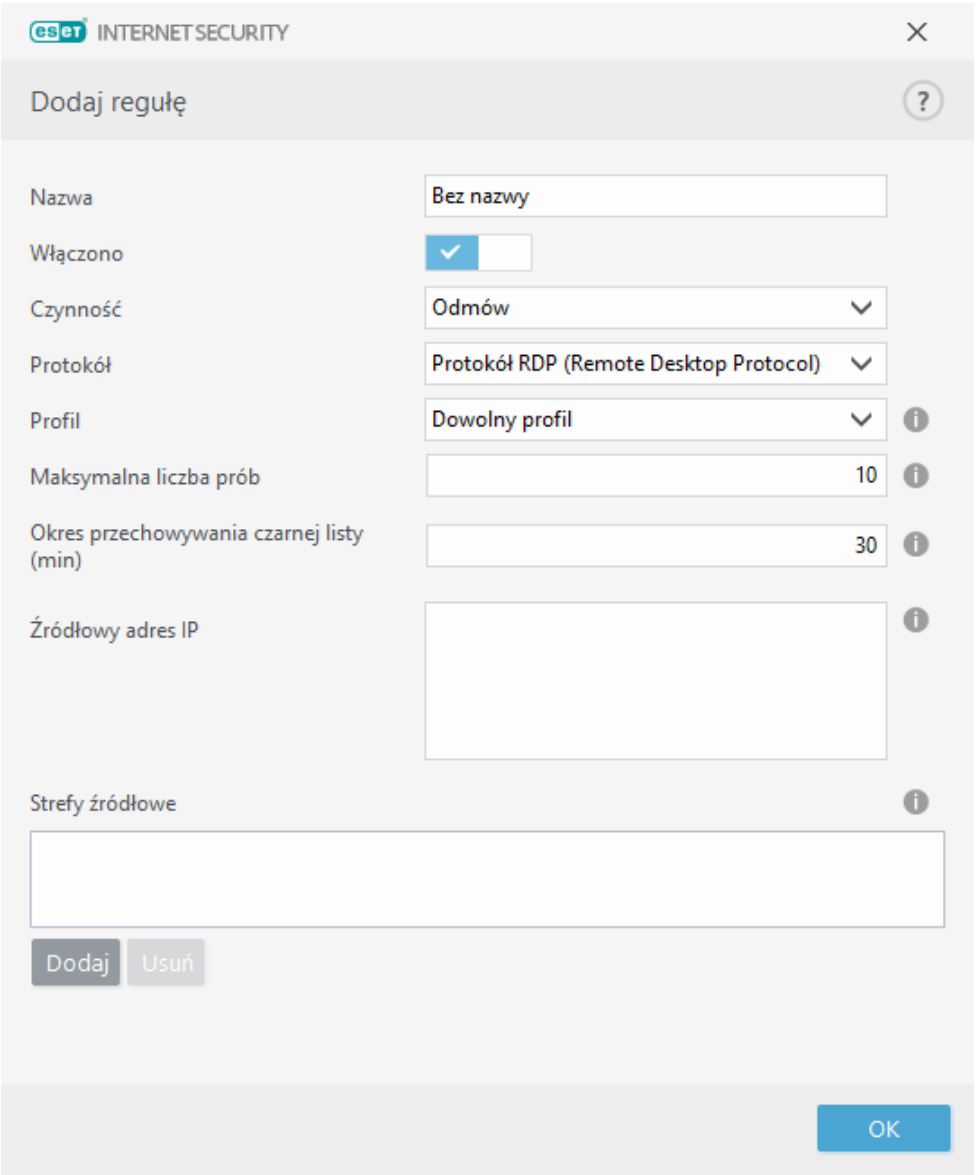
Edytuj — umożliwia zmodyfikowanie istniejącej reguły.

Usuń — umożliwia usunięcie istniejącej reguły z listy reguł.

 **Góra/Góra/Dół/Dół** — dostosuj poziom priorytetu reguł.

W celu zapewnienia możliwie najlepszej ochrony, stosowana jest reguła blokowania z najniższą wartością **Maksymalna liczba prób**, gdy do warunków wykrycia pasuje wiele reguł blokowania, nawet jeśli reguła znajduje się niżej na liście Reguł.

Edytor reguł



Nazwa — nazwa reguły.

Włączona — przesuń suwak w pozycję wyłączenia, jeśli chcesz pozostawić regułę na liście, ale nie chcesz jej używać.

Akcja — wybierz opcję **Odmów** lub **Zezwól na** połączenie, jeśli ustawienia reguły są spełnione.

Protokół — protokół komunikacyjny, który ma zostać sprawdzony przez regułę.

Profil — reguły własne można ustawiać i stosować dla poszczególnych profili.

Maksymalna liczba prób – Maksymalna dozwolona liczba prób powtórzenia ataku do momentu zablokowania adresu IP i dodania go do czarnej listy.

Okres przechowywania czarnej listy (min) — ustawia czas wygaśnięcia adresu z czarnej listy. Domyślny czas zliczania liczby prób wynosi 30 minut.

Źródłowy adres IP — lista adresów IP / zakresów / podsieci. W przypadku wielu adresów należy oddzielić je przecinkami.

Strefy źródłowe — umożliwia dodanie w tym miejscu wstępnie zdefiniowanej lub utworzonej strefy z zakresem adresów IP, klikając przycisk **Dodaj**.

IDS reguły

W niektórych sytuacjach usługa Intrusion Detection Service (IDS) może potraktować komunikację między routerami lub innymi wewnętrznymi urządzeniami sieciowymi jako potencjalny atak. Bezpieczny adres można dodać do listy adresów wykluczonych ze strefy IDS, co pozwoli pominąć usługę IDS.

> **Ilustrowane instrukcje**
> Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:
> - Wyłączanie adresu IP z IDS w programie ESET Internet Security

Kolumny

- **Wykrywanie** — typ wykrywania.

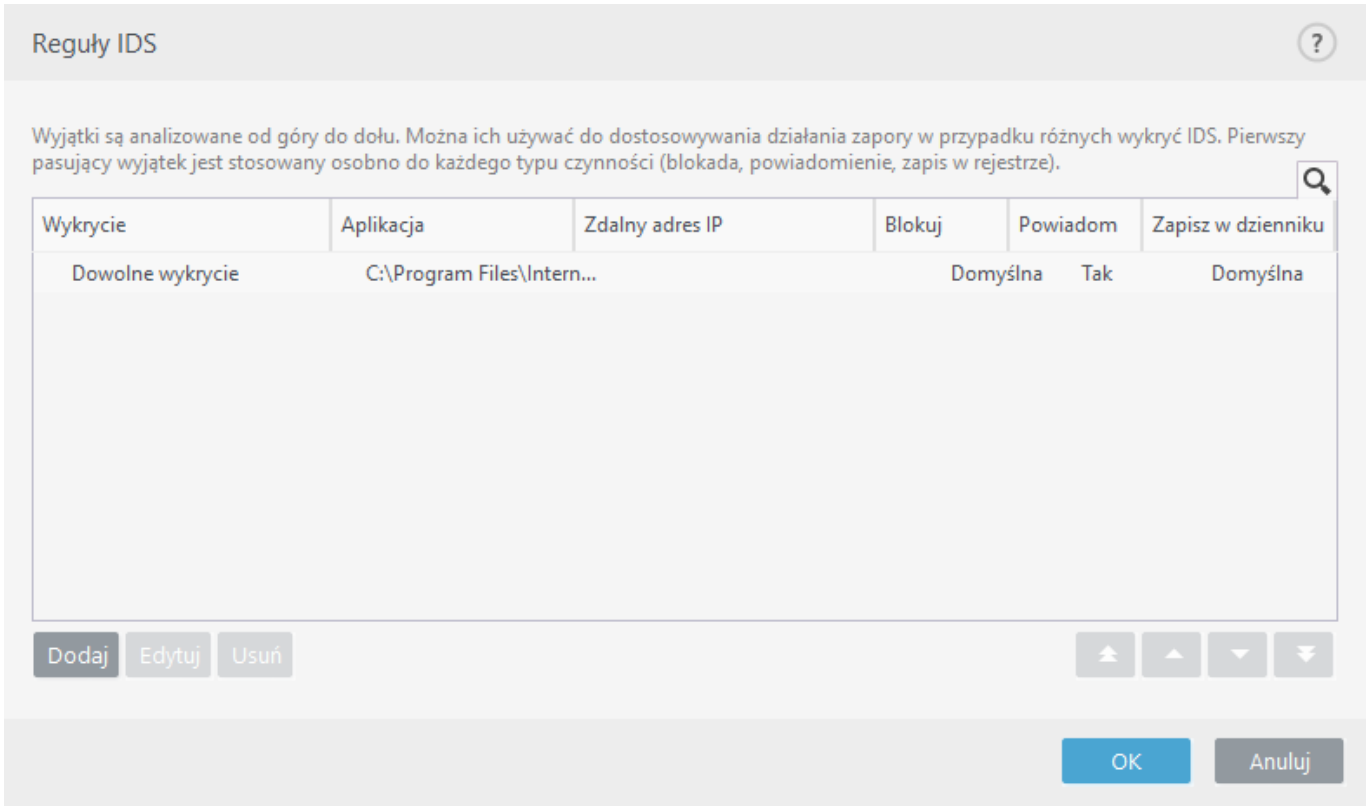
- **Aplikacja** — należy wybrać ścieżkę do pliku aplikacji objętej wyjątkiem, klikając pozycję ... (np. C:\Program Files\Firefox\Firefox.exe). NIE należy wprowadzać nazwy aplikacji.

- **Zdalny adres IP** — lista zdalnych adresów/zakresów/podsieci IPv4 lub IPv6. Adresy muszą być oddzielone przecinkami.

- **Blokuj** — każdemu procesowi systemu odpowiada domyślne działanie oraz przypisana czynność (blokuj lub zezwalaj). Aby zmienić domyślne działanie podejmowane w odniesieniu do programu ESET Internet Security, można wybrać z menu rozwijanego blokowanie lub zezwalanie.

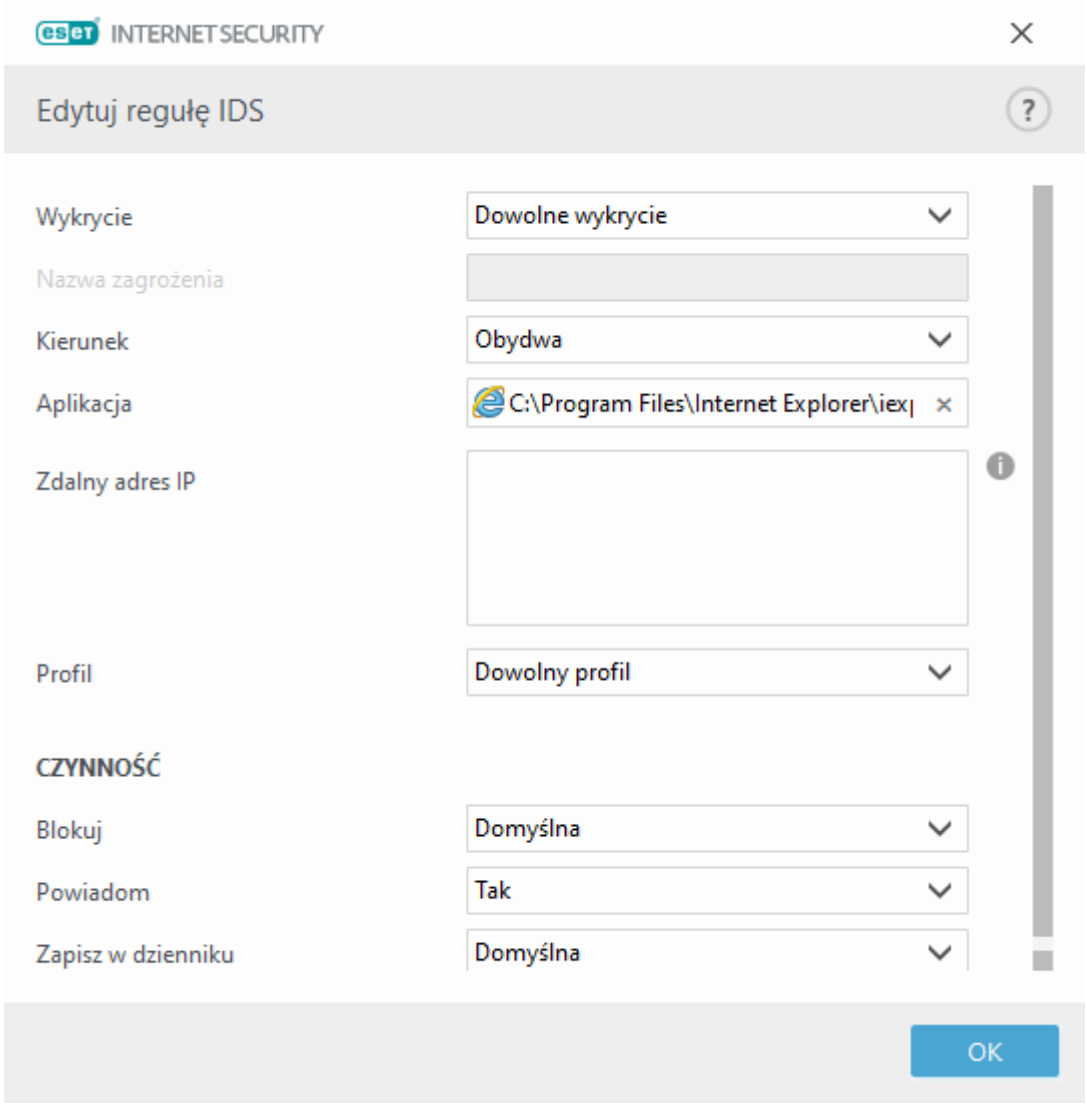
- **Powiadom** — należy zdecydować, czy Powiadomienia na pulpicie mają być wyświetlane na komputerze. Do wyboru są opcje **Domyślnie**/**Tak**/**Nie**.

- **Zapisz w dzienniku** — umożliwia zapisywanie zdarzeń w plikach dziennika programu ESET Internet Security. Do wyboru są opcje **Domyślnie**/**Tak**/**Nie**.



Zarządzanie regułami IDS

- **Dodaj** — kliknij, aby utworzyć nową regułę IDS.
- **Edytuj** — kliknij, aby edytować regułę IDS.
- **Usuń** — tę opcję należy zaznaczyć i kliknąć w celu usunięcia regułę z listy reguł IDS.
- **Na początek/W górę/W dół/Na koniec** — te opcje umożliwiają dostosowywanie priorytetów reguł (reguły są klasyfikowane kolejno od góry do dołu).



Jeśli chcesz, aby po każdym wystąpieniu zdarzenia następowało wyświetlenie powiadomienia i utworzenie wpisu w dzienniku:
1.Kliknij opcję **Dodaj**, aby dodać nową regułę IDS.
2.Z menu rozwijanego **Wykrywanie** wybierz konkretne wykrywanie.
✓ 3.Wybierz ścieżkę aplikacji, klikając opcję **...**, aby zastosować powiadomienie do tej aplikacji.
4.Pozostaw wartość **Domyślne** w menu rozwijanym **Blokuj**. Spowoduje to zastosowanie domyślnego działania programu ESET Internet Security.
5.W menu rozwijanych **Powiadom** i **Dziennik** ustaw wartości **Tak**.
6.Kliknij przycisk **OK**, aby zapisać powiadomienie.

Jeśli nie chcesz, aby było wyświetlane cykliczne powiadomienie sygnalizowane **Wykryciem** dotyczącym zdarzenia, którego nie uważasz za zagrożenie:
1.Kliknij opcję **Dodaj**, aby dodać nową regułę IDS.
2.Z menu rozwijanego **Wykrywanie** wybierz konkretne wykrywanie, na przykład **Sesja SMB bez rozszerzeń zabezpieczeń** lub **Wykryto atak ze skanowaniem portów TCP**.
✓ 3.Wybierz opcję **Przychodzące** z menu rozwijanego kierunku, jeśli dotyczy to komunikacji przychodzącej.
4.W menu rozwijanym **Powiadom** wybierz opcję **Nie**.
5.W menu rozwijanym **Dziennik** wybierz opcję **Tak**.
6.Pozostaw pole **Aplikacja** puste.
7.Jeśli komunikacja nie pochodzi z konkretnego adresu IP, pozostaw pole **Zdalny adres IP** puste.
8.Kliknij przycisk **OK**, aby zapisać powiadomienie.

Blokowanie podejrzanego zagrożenia

Taka sytuacja może mieć miejsce wówczas, gdy aplikacja działająca na komputerze użytkownika spróbuje przesłać szkodliwą komunikację do innego komputera w sieci, wykorzystując przy tym lukę w zabezpieczeniach lub w systemie zostanie wykryta próba skanowania portów.

Zagrożenie — nazwa zagrożenia.

Adres zdalny — zdalny adres IP.

Zezwalaj — utworzenie reguły usługi Intrusion Detection Service (IDS) ze wstępnie zdefiniowanym brakiem czynności w każdym z typów czynności (blokowanie, powiadamianie, zapisanie w dzienniku).

Blokuj dalej— powoduje zablokowanie wykrytego zagrożenia. Aby utworzyć regułę usługi IDS dla danego zagrożenia, należy zaznaczyć pole wyboru **Nie powiadamiaj mnie ponownie**, co spowoduje dodanie reguły bez żadnego powiadomienia ani zapisu w dzienniku.

> Informacje widoczne w tym oknie powiadomienia mogą się różnić w zależności od rodzaju wykrytego zagrożenia.
> Więcej informacji na temat zagrożeń i innych związanych z nimi terminów można znaleźć w artykułach Typy ataków zdalnych oraz Typy wykrytych zagrożeń.
> Aby rozwiązać problem ze zdarzeniem **Duplikaty adresów IP w sieci**, zapoznaj się z artykułem bazy wiedzy firmy ESET.

Rozwiązywanie problemów z ochroną sieci

Ten kreator ułatwia rozwiązywanie problemów z komunikacją spowodowanych działaniem zapory ESET. Z menu rozwijanego wybierz okres, w którym komunikacja była zablokowana. Lista Niedawno zablokowana komunikacja zawiera informacje o typie aplikacji lub urządzenia, reputacji i łącznej liczbie aplikacji i urządzeń zablokowanych w tym okresie. Aby uzyskać więcej informacji na temat zablokowanej komunikacji, kliknij opcję **Szczegóły**. Następnym krokiem jest odblokowanie aplikacji lub urządzenia, w przypadku którego występują problemy z łącznością.

Kliknij opcję **Odblokuj**, aby odblokować wcześniej zablokowaną komunikację. Jeśli nadal będą występować problemy z aplikacją lub urządzenie nie będzie działać zgodnie z oczekiwaniami, kliknij opcję **Aplikacja nadal nie działa**, aby zezwolić na całą komunikację wcześniej zablokowaną w przypadku tego urządzenia. Jeśli problem będzie nadal występował, uruchom ponownie komputer.

Kliknij **Pokaż zmiany,** aby wyświetlić reguły utworzone przez kreatora. Reguły utworzone przez kreator można też wyświetlić, klikając kolejno opcje **Ustawienia zaawansowane** > **Ochrona sieci** > **Zapora** > **Zaawansowane** > **Reguły**.

Kliknij **Odblokuj inne** , aby rozpocząć rozwiązywanie problemów z komunikacją w przypadku innego urządzenia lub innej aplikacji.

Dozwolone usługi i opcje zaawansowane

Opcje zaawansowane w sekcjach Zapora sieciowa i Ochrona przed atakami z sieci umożliwiają skonfigurowanie dostępu do niektórych usług uruchomionych na komputerze ze strefy zaufanej.

Można włączyć lub wyłączyć wykrywanie kilku typów ataków i exploitów, które mogą uszkodzić komputer.

W niektórych przypadkach użytkownik nie otrzyma powiadomienia o zablokowaniu komunikacji w związku z zagrożeniem. Instrukcje wyświetlania całej zablokowanej komunikacji w dzienniku zapory można znaleźć w sekcji Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika.

Dostępność poszczególnych opcji w tym oknie może być różna w zależności od typu lub wersji produktu ESET i modułu zapory, a także wersji systemu operacyjnego.

Dozwolone usługi

Ustawienia z tej grupy mają na celu uproszczenie konfiguracji dostępu do usług tego komputera ze strefy zaufanej. Wiele z nich służy do włączania/wyłączania zdefiniowanych wstępnie reguł zapory. Dozwolone usługi można edytować, otwierając **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Zapora** > **Zaawansowane** > **Dozwolone usługi**.

- **Zezwól na udostępnianie plików i drukarek w strefie zaufanej** — umożliwia komputerom zdalnym ze strefy zaufanej korzystanie z udostępnionych plików i drukarek.

- **Zezwól na używanie protokołu UPNP dla usług systemowych w strefie zaufanej** — pozwala na przychodzenie i wychodzenie żądań protokołów UPnP dla usług systemowych. UPnP (Universal Plug and Play znany również jako Microsoft Network Discovery) jest używany w Windows Vista i nowszych systemach operacyjnych.

- **Zezwól na połączenie przychodzące RPC w strefie zaufanej** — pozwala połączeniom TCP ze strefy zaufanej na uzyskiwanie dostępu do usług MS RPC Portmapper i RPC/DCOM.

- **Zezwól na używanie pulpitu zdalnego w strefie zaufanej** — zezwala na połączenia za pośrednictwem protokołu RDP i pozwala komputerom ze strefy zaufanej uzyskiwać dostęp do komputera użytkownika (za pośrednictwem programu, który wykorzystuje RDP, np. Podłączanie pulpitu zdalnego).

- **Włącz logowanie do grup typu multicast za pośrednictwem protokołu IGMP** — zezwala na wysyłanie i odbieranie strumieni typu multicast IGMP i UDP, na przykład przesyłanie strumienia wideo wygenerowanego przez programy korzystające z protokołu IGMP (Internet Group Management Protocol).

- **Włącz komunikację dla zmostkowanych połączeń** — zaznaczenie tej opcji zapobiega przerywaniu połączeń mostkowych. Sieci mostkowe łączą maszynę wirtualną z siecią przy użyciu karty Ethernet komputera-hosta. W przypadku korzystania z sieci mostkowej maszyna wirtualna może uzyskać dostęp do innych urządzeń przez sieć i odwrotnie, tak jakby była komputerem fizycznym w sieci.

- **Zezwól na automatyczne używanie Protokołu odnajdywania usług sieci Web (WSD) dla usług systemowych w strefie zaufanej** — zezwala na obsługę przychodzących żądań usługi Web Services Discovery ze stref zaufanych przez zaporę. WSD jest protokołem używanym do lokalizowania usług w sieci lokalnej.

- **Zezwól na rozwiązywanie adresów typu multicast w strefie zaufanej (LLMNR)** — LLMNR (Link-local Multicast Name Resolution) to protokół pakietowy DNS, który umożliwia hostom protokołu IPv4 i IPv6

rozpoznawanie nazw hostów podłączonych do tego samego łącza lokalnego bez odwoływania się do serwera DNS czy do konfiguracji klienta DNS. Ta opcja zezwala na przychodzące żądania strumieni multicast systemu DNS ze strefy zaufanej przez zaporę.

- **Obsługa grupy domowej systemu Windows** — umożliwia obsługę grupy domowej systemu operacyjnego Windows 7 i nowszych. Grupa domowa pozwala na udostępnianie plików i drukarek w sieci domowej. Aby ją skonfigurować, należy kliknąć kolejno opcje **Start** > **Panel sterowania** > **Sieć i Internet** > **Grupa domowa**.

Wykrywanie włamań

Wykrywanie włamań monitoruje komunikację sieciową urządzenia pod kątem szkodliwej aktywności. Można edytować te ustawienia, otwierając **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Ochrona przed atakami sieciowymi** > **Opcje zaawansowane** > **Wykrywanie włamań**.

- **ProtokółSMB** — wykrywanie i blokowanie różnego rodzaju problemów z zabezpieczeniami w protokole SMB.

- **Protokół RPC** — wykrywa i blokuje różne identyfikatory CVE w zdalnym systemie wywołania procedur opracowanym dla środowiska Distributed Computing Environment (DCE).

- **Protokół RDP** — wykrywa i blokuje różne identyfikatory CVE w protokole RDP (patrz wyżej).

- **Wykrywanie ataku z preparowaniem pakietów ARP** — wykrywanie ataków z preparowaniem pakietów ARP spowodowanych przez atak typu man-in-the-middle lub „węszeniem” przy przełączniku sieciowym. Protokół ARP (Address Resolution Protocol) jest używany przez aplikację sieciową lub urządzenie do ustalenia adresu Ethernet.

- **Wykrywanie ataku ze skanowaniem portów TCP/UDP** — wykrywa ataki z użyciem oprogramowania do skanowania portów, służącego do badania hosta pod kątem otwartych portów poprzez wysyłanie żądań programów do adresów portów. Celem tych działań jest znalezienie aktywnych portów i wykorzystanie luk w zabezpieczeniach usługi. Więcej informacji na temat ataków tego typu można znaleźć w słowniczku.

- **Blokowanie niebezpiecznych adresów po wykryciu ataku** — adresy IP, które zostały wykryte jako źródło ataków są dodawane do czarnej listy w celu zablokowania połączenia przez podany okres.

- **Wyświetl powiadomienie po wykryciu ataku** — umożliwia włączenie wyświetlania powiadomień na pasku zadań w prawym dolnym rogu ekranu.

- **Wyświetlaj także powiadomienia po wykryciu ataku przychodzącego na luki zabezpieczeń** — w przypadku wykrycia ataków na luki w zabezpieczeniach lub prób uzyskania w ten sposób dostępu do systemu wyświetlane są powiadomienia.

Sprawdzanie pakietów

Typ analizy pakietów, który filtruje dane przesyłane za pośrednictwem sieci. Można edytować te ustawienia, otwierając **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Ochrona przed atakami sieciowymi** > **Opcje zaawansowane** > **Inspekcja pakietów**.

- **Zezwól w protokole SMB na połączenia przychodzące do udziałów administracyjnych** — udziały administracyjne (admin shares) to domyślne udziały sieciowe, które współdzielą partycje dysku twardego (*C$*, *D$*, ...) w systemie razem z folderem systemowym (*ADMIN$*). Wyłączenie połączenia z udziałami administracyjnymi może osłabić wiele zagrożeń. Na przykład, robak Conficker przeprowadza ataki słownikowe w celu podłączenia do udziałów administracyjnych.

- **Odmów starym (nieobsługiwanym) dialektom protokołuSMB** — odmowa sesji SMB z nieaktualnym dialektem SMB, który nie jest obsługiwany przez IDS. Nowoczesne systemy Windows obsługują nieaktualne dialekty SMB ze względu na zgodność wsteczną z wcześniejszymi systemami operacyjnymi, np. Windows 95. Atakujący może użyć nieaktualnego dialektu w sesji SMB w celu uniknięcia kontroli ruchu. Należy odrzucić nieaktualne dialekty SMB, jeżeli komputer nie współdzieli plików (ogólnie komunikacji SMB) z komputerem, na którym zainstalowano wcześniejszą wersję Windows.

- **Odmów zabezpieczeniom protokołu SMB bez rozszerzeń zabezpieczeń** — rozszerzone zabezpieczenia mogą zostać użyte podczas negocjacji sesji SMB w celu zapewnienia bezpieczniejszego mechanizmu uwierzytelniania niż uwierzytelnianie LAN Manager Challenge/Response (LM). Schemat LM jest traktowany jako słaby i nie zaleca się korzystania z niego.

- **Odmów otwierania plików wykonywalnych na serwerze poza strefą zaufaną w protokole SMB** — odrzuca połączenie podczas próby uruchomienia pliku wykonywalnego (.exe, .dll itp.) z folderu udostępnionego na serwerze, który nie należy do strefy zaufanej w zaporze. Należy pamiętać, że kopiowanie plików wykonywalnych z zaufanych źródeł może być uzasadnione. Należy pamiętać, że kopiowanie wykonywalnych plików z zaufanych źródeł może być dozwolone, jednak to wykrywanie powinno zmniejszyć zagrożenia związane z niechcianym otwarciem pliku na serwerze ze złośliwym oprogramowaniem (na przykład poprzez kliknięcie przez użytkownika odnośnika do współdzielonego pliku wykonywalnego ze złośliwym oprogramowaniem).

- **Odmów uwierzytelniania NTLM w protokole SMB przy nawiązywaniu połączenia z serwerem w strefie zaufanej / spoza strefy zaufanej** — protokoły, które wykorzystują schematy uwierzytelniające NTLM (obie wersje) są celem ataków związanych z przekazywaniem poświadczeń (znanych jako metoda SMB Relay w przypadku protokołu SMB). Odmowa uwierzytelniania NTLM przy nawiązywaniu połączenia z serwerem spoza strefy zaufanej zmniejsza zagrożenia związane z przekazywaniem poświadczeń przez serwer ze złośliwym oprogramowaniem spoza strefy zaufanej. W podobny sposób można odmówić uwierzytelniania NTLM w przypadku serwerów ze strefy zaufanej.

- **Zezwól na komunikację z usługą Menedżer konta zabezpieczeń** — więcej informacji na temat tej usługi można znaleźć tutaj: [MS–SAMR].

- **Zezwól na komunikację z usługą Urząd zabezpieczeń lokalnych** — więcej informacji na temat tej usługi można znaleźć tutaj: [MS-LSAD] i [MS-LSAT].

- **Zezwól na komunikację z usługą Rejestr zdalny** — więcej informacji na temat tej usługi można znaleźć tutaj: [MS–RRP].

- **Zezwól na komunikację z usługą Services Control Manager** — więcej informacji na temat tej usługi można znaleźć tutaj: [MS–SCMR].

- **Zezwól na komunikację z Usługą serwera** — więcej informacji na temat tej usługi można znaleźć tutaj: [MS–SRVS].

- **Zezwól na komunikację z innymi usługami** — inne usługi MSRPC.

Połączone sieci

To zaznaczenie pokazuje sieci, z którymi są podłączone karty sieciowe. Opcja **Połączone sieci** znajduje się w menu głównym, w obszarze **Ustawienia** > **Ochrona sieci**. Po kliknięciu łącza pod nazwą sieci jest wyświetlany monit o wybranie typu ochrony dla sieci, z którą jest połączona karta sieciowa.

Istnieją dwa tryby ochrony sieci, które można wybrać w oknie konfigurowania ochrony sieci:

- **Tak** — w przypadku sieci zaufanej (sieci domowej lub biurowej). Komputer i udostępnione pliki przechowywane na komputerze są widoczne dla innych użytkowników sieci, a zasoby systemowe są dostępne dla innych użytkowników w sieci. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do bezpiecznej sieci lokalnej.

- **Nie** — w przypadku sieci niezaufanej (sieci publicznej). Pliki i foldery w systemie nie są udostępniane innym użytkownikom w sieci ani nie są widoczne, a udostępnianie zasobów systemowych jest dezaktywowane. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do sieci bezprzewodowych.

Kliknij ikonę koła zębatego obok sieci, aby wybrać jedną z następujących opcji (w przypadku sieci niezaufanych dostępna jest tylko opcja **Edytuj sieć**):

- **Edytuj sieć** — otwiera się edytor sieci.

- **Skanuj sieć za pomocą Inspekcji sieci** — otwiera się Inspekcja sieci w celu uruchomienia skanowania sieci.

- **Oznacz jako „Moja sieć”** — do sieci dodawany jest tag „Moja sieć”. Ten tag będzie wyświetlany obok sieci w całym produkcie ESET Internet Security, umożliwiając lepszą identyfikację i przegląd zabezpieczeń.

- **Usuń oznaczenie „Moja sieć”** — tag Moja sieć jest usuwany. Opcja ta jest dostępna tylko wtedy, gdy sieć jest oznakowana.

Aby wyświetlić poszczególne karty sieciowe wraz z przypisanymi do nich profilami zapory oraz strefami zaufanymi, kliknij pozycję **Karty sieciowe**. Szczegółowe informacje można znaleźć w sekcji Karty sieciowe.

Karty sieciowe

Okno kart sieciowych wyświetla następujące informacje dotyczące kart sieciowych:

- Nazwa karty sieciowej i typ połączenia (przewodowe, wirtualne itp.)

- Adres IP wraz z adresem MAC

- Połączona sieć (pokazuje tag Moja sieć)

- Adres IP strefy zaufanej wraz z podsiecią

- Aktywny profil (patrz Profile przypisane do kart sieciowych)

Czarna lista tymczasowa adresów IP

Aby wyświetlić adresy IP, które zostały wykryte jako źródła ataków i dodane do czarnej listy w celu zablokowania połączenia przez określony czas, w programie ESET Internet Security należy przejść do obszaru **Ustawienia** > **Ochrona sieci** > **Czarna lista tymczasowa adresów IP**. Tymczasowa blokada adresów obowiązuje przez godzinę.

Kolumny

Adres IP — umożliwia wyświetlenie zablokowanego adresu IP.

Powód blokady — umożliwia wyświetlenie typu ataku powstrzymanego z adresu (na przykład ataku skanowania portów TCP).

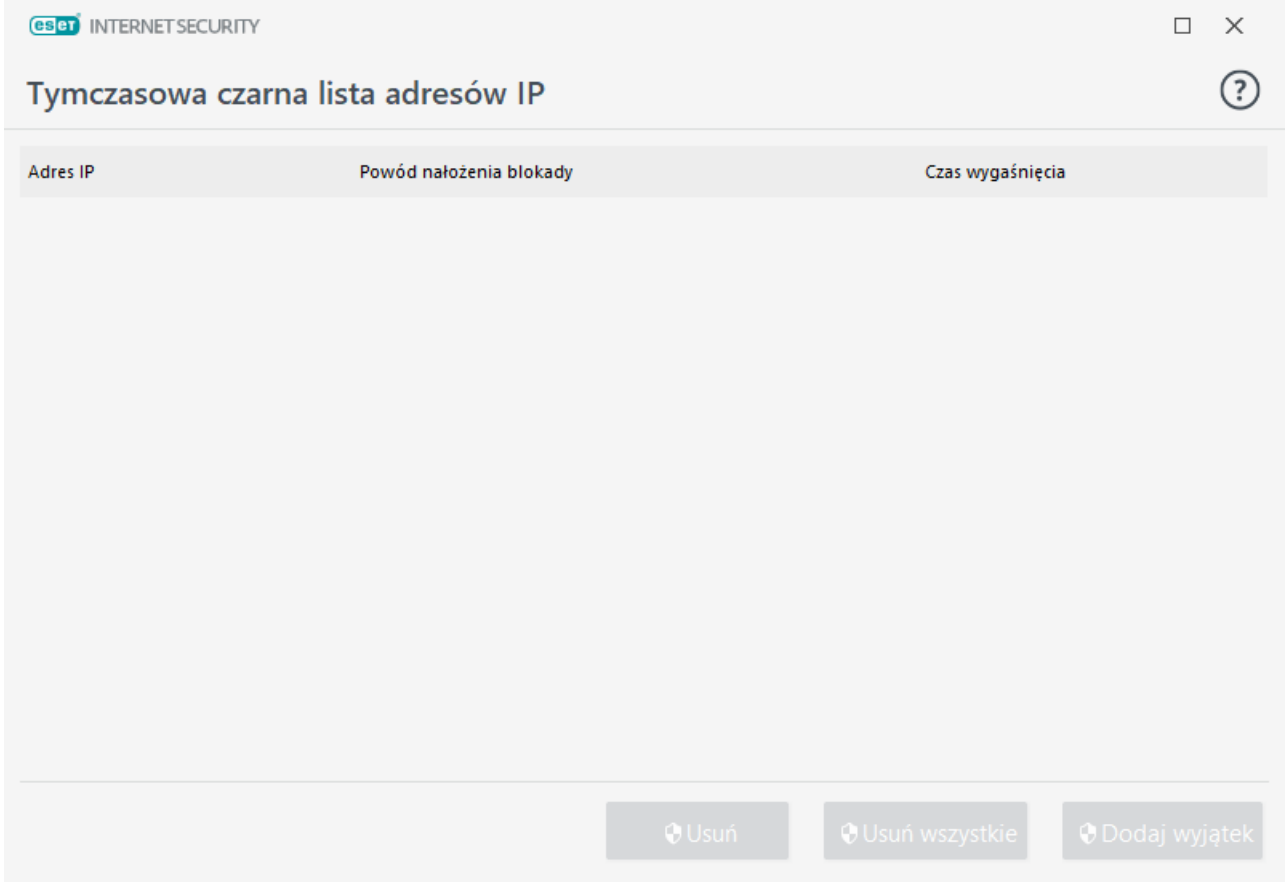
Limit czasu — pokazuje godzinę i datę, kiedy adres zostanie usunięty z czarnej listy.

Elementy sterujące

Usuń — umożliwia przedterminowe usunięcie adresu z czarnej listy.

Usuń wszystkie — umożliwia natychmiastowe usunięcie wszystkich adresów z czarnej listy.

Dodaj wyjątek — umożliwia dodanie wyjątku zapory do filtrowania IDS.



Dziennik ochrony sieci

Ochrona sieci ESET Internet Security zapisuje wszystkie ważne wydarzenia w dzienniku, do którego dostęp jest możliwy bezpośrednio z menu. Kliknij **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**, a następnie wybrać pozycję **Ochrona sieci** z menu rozwijanego **Dziennik**.

Pliki dziennika mogą posłużyć wykrywaniu błędów oraz ujawnianiu wtargnięć do systemu. Dziennik ochrony sieci ESET zawiera następujące informacje:

- data i godzina wystąpienia zdarzenia;

- nazwa zdarzenia;
- obiekt źródłowy;
- docelowy adres sieciowy;
- sieciowy protokół komunikacyjny;
- zastosowana reguła lub nazwa robaka, jeśli został zidentyfikowany;
- aplikacja, której dotyczy zdarzenie;
- użytkownik.

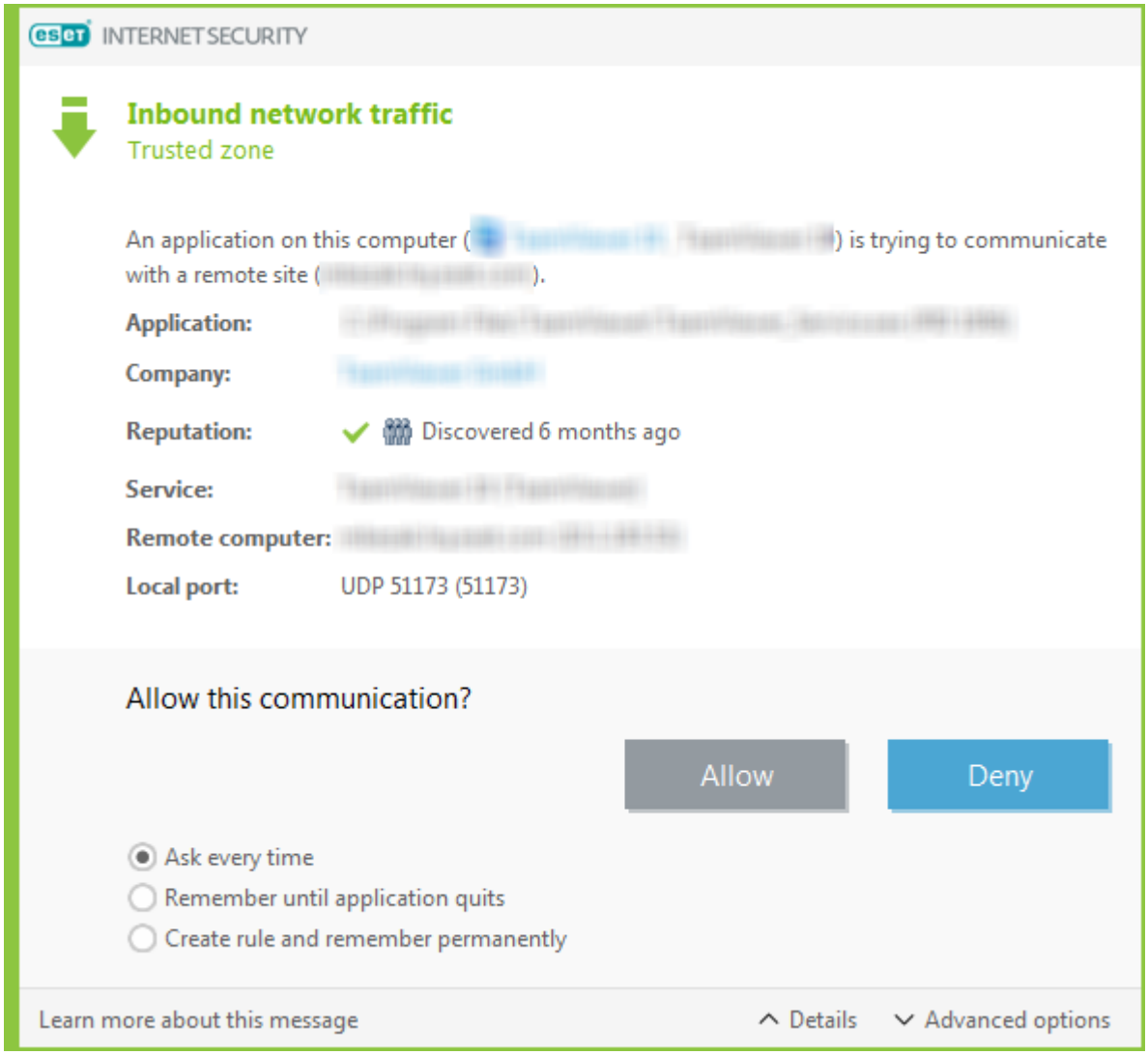
Dokładna analiza tych danych może pomóc w wykryciu prób złamania zabezpieczeń systemu. Wiele innych czynników wskazuje na potencjalne zagrożenia bezpieczeństwa i pozwala na zminimalizowanie ich skutków: częste połączenia z nieznanych lokalizacji, wielokrotne próby nawiązania połączenia, połączenia nawiązywane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

> **Wykorzystanie luki w zabezpieczeniach**
> Komunikat wykorzystania luki w zabezpieczeniach jest rejestrowany, nawet jeśli dana luka jest już załatana, ponieważ próba wykorzystania jest wykrywana i blokowana na poziomie sieci, zanim dojdzie do rzeczywistego wykorzystania.

Ustanawianie połączenia — wykrywanie

Zapora wykrywa każde nowo utworzone połączenie sieciowe. Aktywny tryb zapory określa, jakie działania są realizowane dla nowej reguły. Jeśli aktywowano opcję **Tryb automatyczny** lub **Tryb oparty na regułach**, zapora będzie wykonywać wstępnie zdefiniowane 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. Możesz wybrać opcję **Zezwalaj** lub **Odmów** (blokuj) połączenie. 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 **Utwórz regułę i zapamiętaj na stałe** oraz zapisać czynność jako nową regułę dla zapory. Jeśli zapora wykryje w przyszłości to samo połączenie, zostanie zastosowana istniejąca już reguła bez wymogu interakcji ze strony użytkownika.



Podczas tworzenia nowych reguł należy zezwalać tylko na połączenia, które są bezpieczne. Jeśli wszystkie połączenia są dozwolone, zapora nie spełnia swojego zadania. Oto ważne parametry połączeń:

Aplikacja — lokalizacja pliku wykonywalnego i identyfikator procesu. Nie zezwalaj na połączenia z nieznanymi aplikacjami i procesami.

Firma — nazwa wydawcy aplikacji. Kliknij tekst, aby wyświetlić certyfikat zabezpieczeń dla firmy.

Reputacja — poziom ryzyka połączenia. Połączeniom przypisywane są poziomy ryzyka: Bezpieczny (zielony), Nieznany (pomarańczowy) lub Ryzykowny (czerwony), przy użyciu wielu reguł heurystycznych, które badają specyfikację każdego połączenia, liczbę użytkowników i czas wykrywania. Te informacje są zbierane przez technologię ESET LiveGrid®.

Usługa — nazwa usługi, jeśli aplikacja jest usługą systemu Windows.

Komputer zdalny — adres urządzenia zdalnego. Należy zezwalać na połączenia tylko z zaufanymi i znanymi adresami.

Port zdalny — port komunikacyjny. W zwykłych warunkach powinna być dozwolona komunikacja za pośrednictwem typowych portów (np. ruch internetowy — port numer 80.443).

Wirusy często używają połączeń internetowych i ukrytych, co ułatwia im infekowanie systemów zdalnych. Jeśli reguły są prawidłowo skonfigurowane, zapora staje się użytecznym narzędziem ochrony przed wieloma próbami

ataku prowadzonymi przy użyciu szkodliwego kodu.

Rozwiązywanie problemów z zaporą ESET

Jeśli na komputerze z zainstalowanym programem ESET Internet Security pojawią się problemy z łącznością, można na kilka sposobów sprawdzić, czy powoduje je zapora ESET. Co więcej, zapora ESET może być przydatna w tworzeniu nowych reguł lub wyjątków w celu rozwiązania problemów z łącznością.

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

- Kreator rozwiązywania problemów
- Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika
- Tworzenie wyjątków na podstawie powiadomień zapory
- Zaawansowane funkcje dziennika dotyczące ochrony sieci
- Rozwiązywanie problemów z filtrowaniem protokołów

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** > **Ochrona sieci**.

Zapisywanie w dzienniku i tworzenie reguł oraz wyjątków na podstawie dziennika

Zapora ESET domyślnie nie zapisuje w dzienniku wszystkich zablokowanych połączeń. Aby wyświetlić elementy zablokowane przez Ochronę sieci, włącz zapisywanie w dzienniku w obszarze **Ustawienia zaawansowane**, wybierając kolejno opcje **Narzędzia** > **Diagnostyka** > **Zaawansowane zapisywanie w dzienniku** > **Włącz zaawansowane funkcje dziennika Ochrony sieci**. Jeśli w dzienniku znajduje się element, który nie powinien być blokowany przez zaporę, można dla tego elementu utworzyć regułę lub regułę IDS, klikając go prawym przyciskiem myszy i wybierając pozycję **Nie blokuj w przyszłości podobnych zdarzeń**. Należy pamiętać, że dziennik 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.

> Aby zobaczyć kolejność, w jakiej Ochrona sieci blokowała określone połączenia, należy skorzystać z zapisywania w dzienniku. Tworzenie reguł na podstawie dziennika umożliwia również tworzenie reguł dokładnie odpowiadających wymaganiom użytkownika.

Utwórz regułę z dziennika

W nowej wersji programu ESET Internet Security możliwe jest tworzenie reguł na podstawie dziennika. W menu głównym kliknij opcję **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**. Z menu rozwijanego wybierz opcję **Zapora**, 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 Internet Security należy skonfigurować następujące ustawienia:

1. W obszarze **Diagnostyka** w menu **Ustawienia zaawansowane** (F5) > **Narzędzia** > **Pliki dziennika** należy ustawić minimalną szczegółowość zapisów w dzienniku.

2. Włącz opcję **Wyświetlaj także powiadomienia po wykryciu ataku przychodzącego na luki zabezpieczeń** po wybraniu kolejno opcji **Ustawienia zaawansowane** (F5) > **Ochrona sieci** > **Ochrona przed atakami z sieci** > **Opcje zaawansowane** > **Wykrywanie włamań**.

Tworzenie wyjątków na podstawie powiadomień zapory

Gdy zapora ESET wykryje szkodliwe działanie sieci, zostanie wyświetlone okno powiadomień zawierające opis zdarzenia. Powiadomienie to zawiera łącze, za pomocą którego można dowiedzieć się więcej o zdarzeniu i w razie potrzeby skonfigurować regułę dla tego zdarzenia.

> 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 ESET, można utworzyć wyjątek bezpośrednio z powiadomienia.

Zaawansowane zapisywanie w dzienniku dotyczące ochrony sieci

Celem tej funkcji jest zapewnienie bardziej kompleksowych dzienników dla wsparcia technicznego ESET. Korzystaj z tej funkcji wyłącznie, gdy zostaniesz o to poproszony przez wsparcie techniczne ESET, ponieważ może ona wygenerować ogromny plik, mogący spowolnić Twój komputer.

1. Przejdź do **Ustawienia zaawansowane** > **Narzędzia** > **Diagnostyka** i kliknij **Włącz zaawansowane zapisywanie w dzienniku dotyczące ochrony sieci**.

2. Spróbuj odtworzyć napotkany problem.

3. Wyłącz zaawansowane zapisywanie w dzienniku dotyczące ochrony sieci.

4. Plik PCAP utworzony przez zaawansowane zapisywanie w dzienniku można znaleźć w tej samej lokalizacji, w której diagnostyka generuje jest zrzut pamięci: *C:\ProgramData\ESET\ESET Security\Diagnostics*

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 Internet 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).

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.

> Przeczytaj artykuł w bazie wiedzy, aby dowiedzieć się, jak zarządzać filtrowaniem protokołów/SSL/TSL w produkcie ESET do systemu Windows przeznaczonym dla użytkowników domowych.

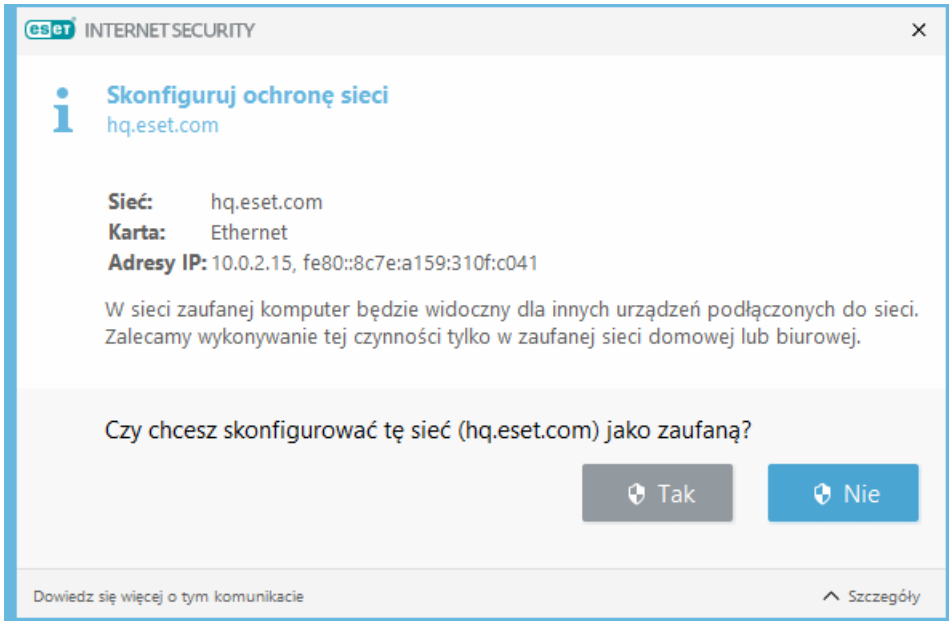
Wykrycie nowej sieci

Domyślnie ESET Internet Security używa ustawień systemu Windows po wykryciu nowej sieci. Aby wyświetlić okno dialogowe po wykryciu nowej sieci, zmień typ ochrony nowych sieci, aby zapytać użytkownika w sieciach znanych. Następnie, w przypadku wykrycia połączenia z nową siecią, użytkownik może wybrać poziom ochrony. To ustawienie będzie miało zastosowanie do połączeń ze wszystkimi komputerami zdalnymi w danej sieci.

Istnieją dwa tryby ochrony sieci, które można wybrać w oknie konfigurowania ochrony sieci:

- **Tak** — w przypadku sieci zaufanej (sieci domowej lub biurowej). Komputer i udostępnione pliki przechowywane na komputerze są widoczne dla innych użytkowników sieci, a zasoby systemowe są dostępne dla innych użytkowników w sieci. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do bezpiecznej sieci lokalnej.

- **Nie** — w przypadku sieci niezaufanej (sieci publicznej). Pliki i foldery w systemie nie są udostępniane innym użytkownikom w sieci ani nie są widoczne, a udostępnianie zasobów systemowych jest dezaktywowane. Zalecamy używanie tego ustawienia podczas uzyskiwania dostępu do sieci bezprzewodowych.



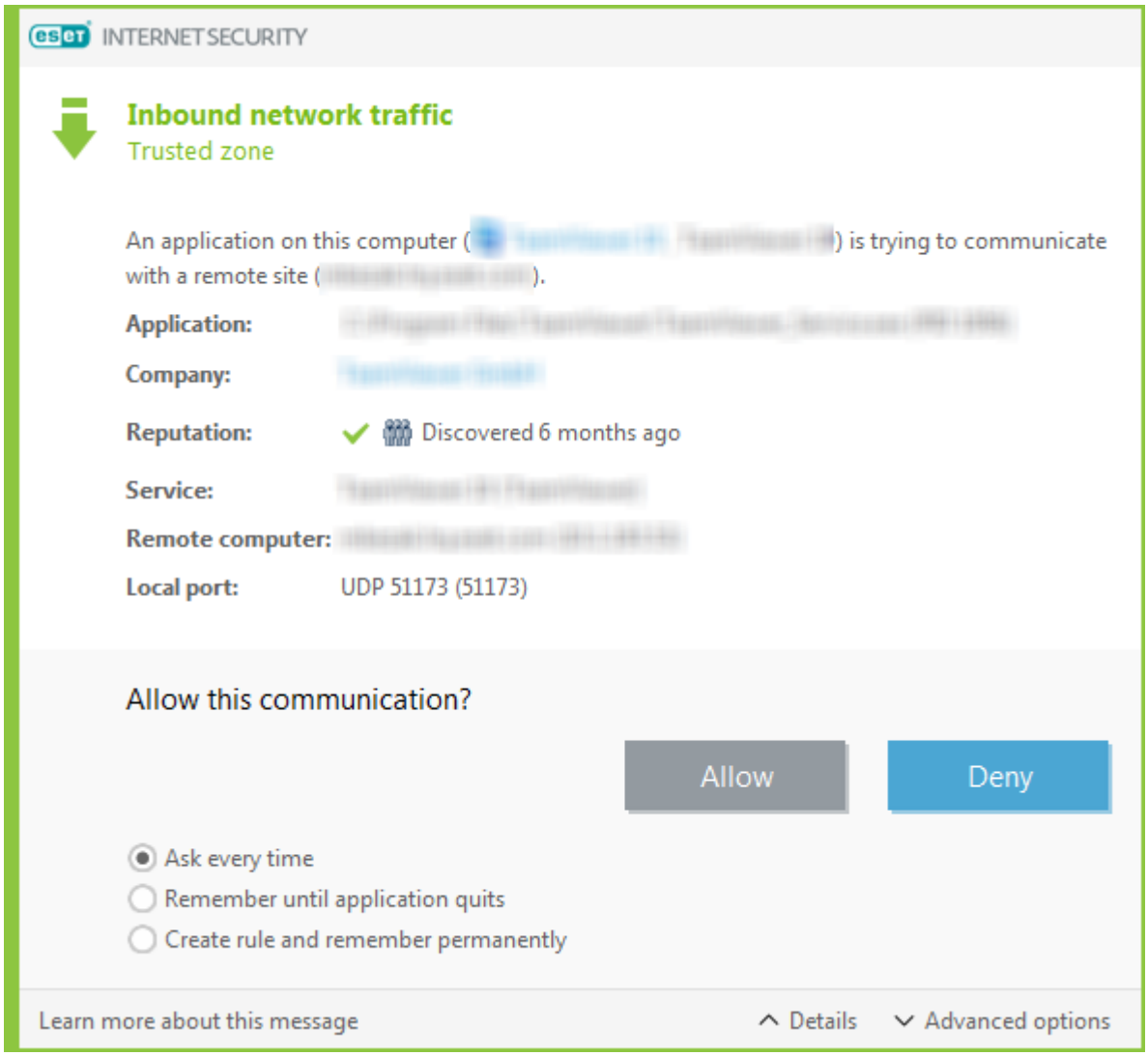
Jeśli sieć jest ustawiona jako zaufana, bezpośrednio połączone podsieci są automatycznie uznawane za zaufane.

Zmiana aplikacji

Zapora wykryła modyfikację aplikacji używanej do nawiązywania połączeń wychodzących z komputera. Istnieje możliwość, że aplikacja została po prostu zaktualizowana do nowszej wersji. Z drugiej strony modyfikacja mogła być spowodowana przez szkodliwe oprogramowanie. Jeśli użytkownik nie wie o żadnej uzasadnionej modyfikacji, zaleca się odmowę komunikacji i przeskanowanie komputera przy użyciu najnowszej bazy sygnatur wirusów.

Zaufana komunikacja przychodząca

Przykład połączenia przychodzącego w ramach strefy zaufanej:
Komputer zdalny ze strefy zaufanej próbuje nawiązać komunikację z aplikacją uruchomioną na komputerze lokalnym.



Aplikacja — aplikacja, z którą kontaktuje się komputer zdalny.

Firma — wydawca aplikacji.

Reputacja — reputacja aplikacji uzyskana przez technologię ESET LiveGrid®.

Usługa — nazwa usługi obecnie działającej na komputerze.

Komputer zdalny — komputer zdalny próbujący nawiązać połączenie z aplikacją uruchomioną na komputerze lokalnym.

Port lokalny — port używany do komunikacji.

Pytaj za każdym razem — jeśli czynnością domyślną ustawioną dla reguły jest **Pytaj**, po każdym uruchomieniu tej reguły wyświetlane jest okno dialogowe.

Zapamiętaj do zamknięcia aplikacji — program ESET Internet Security zapamiętuje daną czynność do następnego ponownego uruchomienia.

Utwórz regułę i zapamiętaj na stałe — zaznaczenie tej opcji przed zezwoleniem lub odmówieniem zgody na komunikację spowoduje, że program ESET Internet Security zapamięta wybraną czynność i zastosuje ją, gdy w przyszłości komputer zdalny znów podejmie próbę skontaktowania się z tą aplikacją.

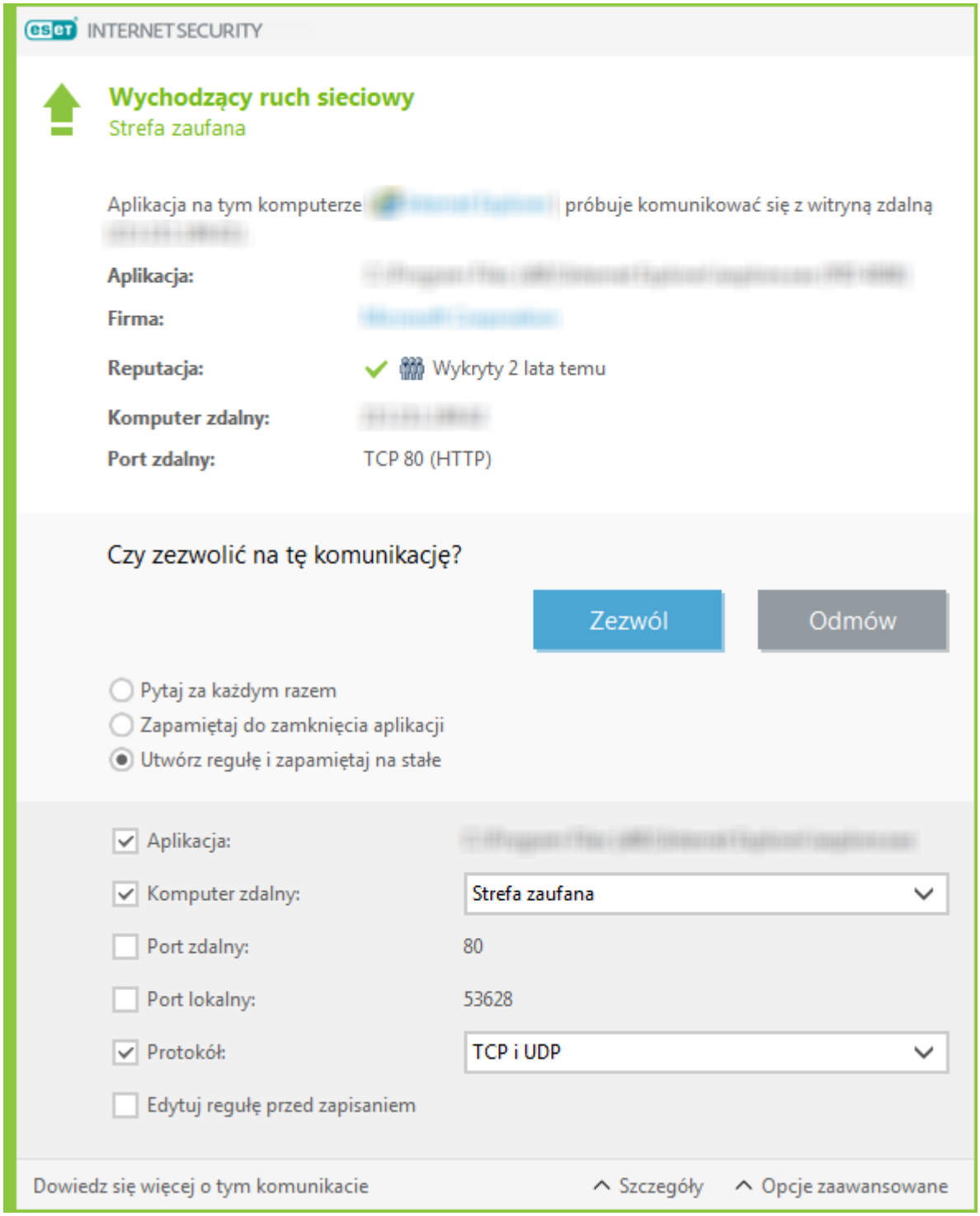
Zezwól — zezwolenie na połączenia przychodzące.

Odmów — odmowa zezwolenia na połączenia przychodzące.

Opcje zaawansowane — umożliwia dostosowanie właściwości reguły.

Zaufana komunikacja wychodząca

Przykład połączenia wychodzącego w ramach strefy zaufanej:
Lokalna aplikacja próbuje ustanowić połączenie z innym komputerem z sieci lokalnej lub z innej sieci znajdującej się w strefie zaufanej.



Aplikacja — aplikacja, z którą kontaktuje się komputer zdalny.

Firma — wydawca aplikacji.

Reputacja — reputacja aplikacji uzyskana przez technologię ESET LiveGrid®.

Usługa — nazwa usługi obecnie działającej na komputerze.

Komputer zdalny — komputer zdalny próbujący nawiązać połączenie z aplikacją uruchomioną na komputerze lokalnym.

Port lokalny — port używany do komunikacji.

Pytaj za każdym razem — jeśli czynnością domyślną ustawioną dla reguły jest **Pytaj**, po każdym uruchomieniu tej reguły wyświetlane jest okno dialogowe.

Zapamiętaj do zamknięcia aplikacji — program ESET Internet Security zapamiętuje daną czynność do następnego ponownego uruchomienia.

Utwórz regułę i zapamiętaj na stałe — zaznaczenie tej opcji przed zezwoleniem lub odmówieniem zgody na komunikację spowoduje, że program ESET Internet Security zapamięta wybraną czynność i zastosuje ją, gdy w przyszłości komputer zdalny znów podejmie próbę skontaktowania się z tą aplikacją.

Zezwól — zezwolenie na połączenia przychodzące.

Odmów — odmowa zezwolenia na połączenia przychodzące.

Opcje zaawansowane — umożliwia dostosowanie właściwości reguły.

Komunikacja przychodząca

Przykład przychodzącego połączenia internetowego:
Komputer zdalny próbuje nawiązać komunikację z aplikacją uruchomioną na komputerze lokalnym.

Aplikacja — aplikacja, z którą kontaktuje się komputer zdalny.

Firma — wydawca aplikacji.

Reputacja — reputacja aplikacji uzyskana przez technologię ESET LiveGrid®.

Usługa — nazwa usługi obecnie działającej na komputerze.

Komputer zdalny — komputer zdalny próbujący nawiązać połączenie z aplikacją uruchomioną na komputerze lokalnym.

Port lokalny — port używany do komunikacji.

Pytaj za każdym razem — jeśli czynnością domyślną ustawioną dla reguły jest **Pytaj**, po każdym uruchomieniu tej reguły wyświetlane jest okno dialogowe.

Zapamiętaj do zamknięcia aplikacji — program ESET Internet Security zapamiętuje daną czynność do następnego ponownego uruchomienia.

Utwórz regułę i zapamiętaj na stałe — zaznaczenie tej opcji przed zezwoleniem lub odmówieniem zgody na komunikację spowoduje, że program ESET Internet Security zapamięta wybraną czynność i zastosuje ją, gdy w przyszłości komputer zdalny znów podejmie próbę skontaktowania się z tą aplikacją.

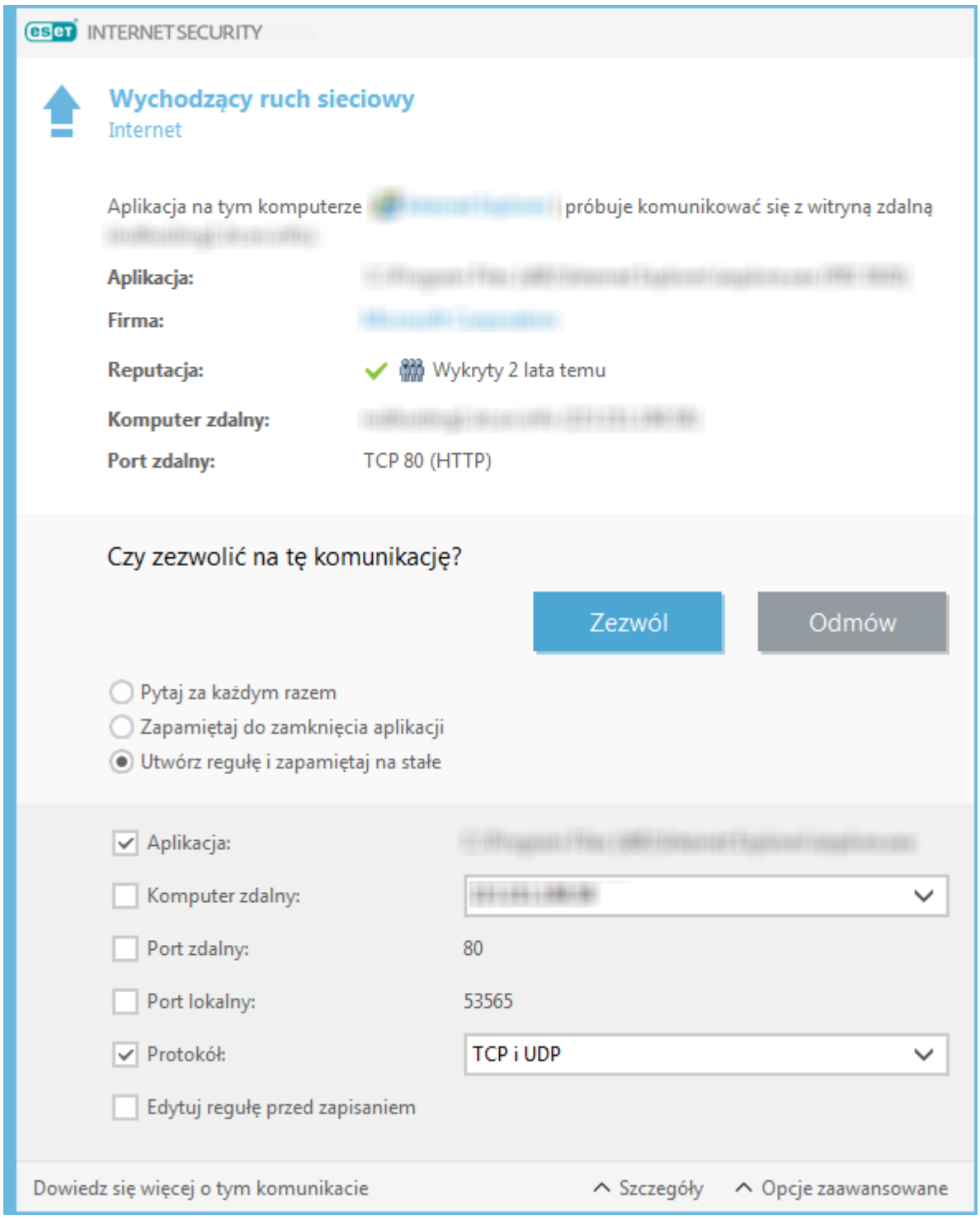
Zezwól — zezwolenie na połączenia przychodzące.

Odmów — odmowa zezwolenia na połączenia przychodzące.

Opcje zaawansowane — umożliwia dostosowanie właściwości reguły.

Komunikacja wychodząca

Przykład wychodzącego połączenia internetowego:
Lokalna aplikacja próbuje nawiązać połączenie z Internetem.



Aplikacja — aplikacja, z którą kontaktuje się komputer zdalny.

Firma — wydawca aplikacji.

Reputacja — reputacja aplikacji uzyskana przez technologię ESET LiveGrid®.

Usługa — nazwa usługi obecnie działającej na komputerze.

Komputer zdalny — komputer zdalny próbujący nawiązać połączenie z aplikacją uruchomioną na komputerze lokalnym.

Port lokalny — port używany do komunikacji.

Pytaj za każdym razem — jeśli czynnością domyślną ustawioną dla reguły jest **Pytaj**, po każdym uruchomieniu tej reguły wyświetlane jest okno dialogowe.

Zapamiętaj do zamknięcia aplikacji — program ESET Internet Security zapamiętuje daną czynność do następnego ponownego uruchomienia.

Utwórz regułę i zapamiętaj na stałe — zaznaczenie tej opcji przed zezwoleniem lub odmówieniem zgody na komunikację spowoduje, że program ESET Internet Security zapamięta wybraną czynność i zastosuje ją, gdy w przyszłości komputer zdalny znów podejmie próbę skontaktowania się z tą aplikacją.

Zezwól — zezwolenie na połączenia przychodzące.

Odmów — odmowa zezwolenia na połączenia przychodzące.

Opcje zaawansowane — umożliwia dostosowanie właściwości reguły.

Ustawienia widoku połączeń

Kliknięcie połączenia prawym przyciskiem myszy powoduje wyświetlenie dodatkowych opcji:

Rozpoznaj 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 localhost.

Szybkość odświeżania — wybierz częstotliwość odświeżania aktywnych połączeń.

Odśwież teraz — powoduje zaktualizowanie okna **Połączenia sieciowe**.

Narzędzia zabezpieczające

Ustawienia **Narzędzi zabezpieczających** umożliwiają skonfigurowanie następujących modułów:

- **Ochrona bankowości internetowej** — zapewnia dodatkową warstwę ochrony przeglądarki zaprojektowaną w celu ochrony danych finansowych podczas przeprowadzania transakcji przez Internet. Włącz funkcję **Zabezpiecz wszystkie przeglądarki**, aby uruchamiać wszystkie obsługiwane przeglądarki internetowe w trybie bezpiecznym. Aby uzyskać więcej informacji, zobacz Ochrona bankowości

internetowej.

• **Kontrola rodzicielska** — moduł Kontrola rodzicielska chroni dzieci, blokując nieodpowiednie lub szkodliwe treści w Internecie.

• **Anti-Theft** — włącz funkcję Anti-Theft, aby chronić komputer w przypadku zgubienia lub kradzieży.

Ochrona bankowości internetowej

Ochrona bankowości internetowej to dodatkowa warstwa zabezpieczeń, mających zapewnić ochronę danych finansowych podczas przeprowadzania transakcji przez Internet.

W większości przypadków zabezpieczona przeglądarka z funkcją ochrony bankowości internetowej jest uruchamiana w domyślnej przeglądarce po przejściu do znanej witryny bankowości internetowej.

Wybierz jedną z następujących opcji konfiguracji zachowania zabezpieczonej przeglądarki:

• **Zabezpiecz wszystkie przeglądarki** — jeśli ta opcja jest włączona, wszystkie obsługiwane przeglądarki internetowe uruchamiają się w trybie bezpiecznym. Pozwala to na przeglądanie Internetu, dostęp do bankowości internetowej, a także zakupy i transakcje online w jednym oknie zabezpieczonej przeglądarki bez przekierowania.

• **Przekierowanie stron internetowych** (domyślne) — strony internetowe z listy chronionych stron internetowych i wewnętrznej listy banków internetowych są przekierowywane do zabezpieczonej przeglądarki. Można wybrać, która przeglądarka (standardowa czy zabezpieczona) zostanie otwarta.

• Wyłączenie obu poprzednich opcji — aby uzyskać dostęp do zabezpieczonej przeglądarki w ESET Internet Security, kliknij pozycję **Narzędzia** > **Ochrona bankowości internetowej** lub kliknij ikonę pulpitu **Ochrona bankowości internetowej**. Przeglądarka wybrana jako domyślna w systemie Windows uruchamia się w trybie bezpiecznym.

Aby skonfigurować zachowanie zabezpieczonej przeglądarki, zobacz Ustawienia zaawansowane ochrony bankowości internetowej. Aby włączyć funkcję Zabezpiecz wszystkie przeglądarki w ESET Internet Security, kliknij **Ustawienia** > **Narzędzia zabezpieczające** i przesuń suwak **Zabezpiecz wszystkie przeglądarki** w pozycję włączoną.

Zabezpieczone przeglądanie Internetu wymaga stosowania zaszyfrowanej komunikacji HTTPS. Następujące przeglądarki obsługują usługę ochrony bankowości internetowej:

• Internet Explorer 8.0.0.0+

• Microsoft Edge 83.0.0.0+

• Google Chrome 64.0.0.0+

• Firefox 24.0.0.0+

Więcej informacji na temat funkcji ochrony bankowości internetowej zawierają poniższe artykuły z bazy wiedzy firmy ESET (dostępne w języku angielskim i kilku innych językach):

• Jak używać funkcji ochrony bankowości internetowej ESET?

• Włączanie lub wyłączanie ochrony bankowości internetowej ESET dla określonej witryny

- Wstrzymywanie lub wyłączanie funkcji ochrony bankowości internetowej w produktach ESET do systemu Windows dla użytkowników domowych
- Ochrona bankowości internetowej ESET — typowe błędy
- Słowniczek ESET | Ochrona bankowości internetowej

Ustawienia zaawansowane ochrony bankowości internetowej

Ustawienia te są dostępne w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona bankowości internetowej**.

Podstawowe

Włącz ochronę bankowości internetowej — po włączeniu opcji Ochrona bankowości internetowej lista chronionych stron internetowych stanie się aktywna i będzie można edytować listę Chronionych stron internetowych.

Ochrona przeglądarek

Zabezpiecz wszystkie przeglądarki — włącz tę opcję, aby uruchamiać wszystkie obsługiwane przeglądarki internetowe w trybie bezpiecznym.

Tryb instalacji rozszerzenia — z menu rozwijanego można wybrać, które rozszerzenia będą mogły być zainstalowane w przeglądarce zabezpieczonej przez firmę ESET: Zmiana trybu instalacji rozszerzenia nie wpływa na rozszerzenia przeglądarki zainstalowane wcześniej:

- **Niezbędne rozszerzenia** — tylko najistotniejsze rozszerzenia opracowane przez konkretnego producenta przeglądarki.
- **Wszystkie rozszerzenia** — wszystkie rozszerzenia obsługiwane przez określoną przeglądarkę.

Przekierowanie stron internetowych

Włącz przekierowanie chronionych stron internetowych — jeśli to ustawienie zostanie włączone, strony internetowe z listy chronionych stron internetowych i wewnętrznej listy banków internetowych będą przekierowywane do zabezpieczonej przeglądarki.

Chronione strony internetowe — lista stron internetowych, dla których można wybrać otwieraną przeglądarkę (normalna czy zabezpieczona). Gdy zabezpieczone przeglądanie jest aktywne, w ramce przeglądarki widoczne jest logo firmy ESET. Jeśli chcesz edytować tę listę, zobacz Chronione strony internetowe.

Przeglądarka zabezpieczona

Włącz zaawansowaną ochronę pamięci — jeśli to ustawienie zostanie włączone, pamięć zabezpieczonej przeglądarki będzie chroniona przed jej sprawdzaniem przez inne procesy.

Włącz ochronę klawiatury — po włączeniu informacje wprowadzane za pośrednictwem klawiatury do bezpiecznej przeglądarki będą ukrywane przed innymi aplikacjami. Zapewnia to większą ochronę przed programami rejestrującymi znaki wprowadzane na klawiaturze.

Zielona ramka przeglądarki — jeśli jest wyłączona, powiadomienie informacyjne w przeglądarce i zielona ramka wokół przeglądarki zostaną wyświetlone na krótko podczas uruchamiania przeglądarki, a następnie znikną.

Chronione strony internetowe

ESET Internet Security zawierają wbudowaną listę predefiniowanych stron internetowych, które wyzwalają uruchomienie bezpiecznej przeglądarki. W konfiguracji programu można dodać stronę internetową lub edytować listę stron internetowych.

Lista **Chronione strony internetowe** może być wyświetlana i edytowana w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Ochrona bankowości internetowej** > **Podstawowe** > **Chronione strony internetowe** > **Edytuj**. Okno składa się z:

Kolumny

Strona internetowa — chroniona strona internetowa.

Przeglądarka zabezpieczona — podczas zabezpieczonego przeglądania przy obramowaniu przeglądarki wyświetlane jest logo ESET.

Zadaj pytanie — gdy włączona jest ta opcja, podczas przeglądania strony internetowej jest wyświetlane okno dialogowe z opcjami przeglądania przez całą sesję zabezpieczonego przeglądania. Program ESET Internet Security może zapamiętać czynność użytkownika. Można też wykonać ją ręcznie.

Normalna przeglądarka — wybranie tej opcji umożliwia kontynuowanie przeprowadzania transakcji bankowych bez dodatkowego zabezpieczenia.

Elementy sterujące

Dodaj — pozwala dodać stronę internetową do listy znanych stron internetowych.

Edytuj — pozwala edytować zaznaczone elementy.

Usuń — służy do usuwania zaznaczonych elementów.

Importuj/Eksportuj — umożliwia eksportowanie listy chronionych stron internetowych i importowanie jej na nowe urządzenie.

Powiadomienie w przeglądarce

Przeglądarka zabezpieczona informuje o swoim aktualnym stanie poprzez powiadomienia w przeglądarce i kolor ramki przeglądarki.

Powiadomienia w przeglądarce są wyświetlane na karcie po prawej stronie.



Aby rozwinąć powiadomienie w przeglądarce, kliknij ikonę ESET. Aby zminimalizować powiadomienie, kliknij tekst powiadomienia. Aby odrzucić powiadomienie, kliknij ikonę zamykania.

Powiadomienie w przeglądarce

Typ powiadomienia	Stan
Powiadomienie informacyjne i zielona ramka przeglądarki	Zapewniona jest maksymalna ochrona, a powiadomienie w przeglądarce jest domyślnie zminimalizowane. Rozwiń powiadomienie w przeglądarce, aby wyświetlić opcje konfiguracji: • **Ukryj zieloną ramkę przeglądarki** — zaznacz pole wyboru, aby ukryć zieloną ramkę wokół przeglądarki po odrzuceniu powiadomienia. Możesz wyłączyć informacyjne powiadomienie w przeglądarce i zieloną ramkę wokół przeglądarki na stałe na ekranie Ochrona bankowości internetowej w Ustawieniach zaawansowanych. • **Ustawienia** — otwiera ustawienia narzędzi zabezpieczających.
Ostrzeżenie i pomarańczowa ramka przeglądarki	Przeglądarka zabezpieczona wymaga Twojej uwagi w przypadku niekrytycznego problemu. Aby uzyskać więcej informacji na temat problemu lub rozwiązania, postępuj zgodnie z instrukcjami podanymi w powiadomieniu w przeglądarce.
Alert zabezpieczeń i czerwona ramka przeglądarki	Przeglądarka nie jest chroniona przez ESET Banking & Payment Protection. Uruchom ponownie przeglądarkę, aby upewnić się, że ochrona jest aktywna. Aby rozwiązać konflikt z plikami załadowanymi do przeglądarki, skontaktuj się z pomocą techniczną ESET, postępując zgodnie z instrukcjami zawartymi w naszym artykule bazy wiedzy.

Kontrola rodzicielska

W module Kontrola rodzicielska można skonfigurować ustawienia kontroli rodzicielskiej, czyli zautomatyzowanych narzędzi pomagających rodzicom chronić swoje dzieci i wprowadzać ograniczenia dostępu do urządzeń i usług. Celem tego mechanizmu jest uniemożliwienie dzieciom i młodym osobom dostępu do stron zawierających nieodpowiednie lub szkodliwe treści.

Kontrola rodzicielska umożliwia blokowanie stron internetowych, które mogą zawierać obraźliwe materiały. Ponadto można zablokować dostęp do ponad 40 wstępnie zdefiniowanych kategorii i ponad 140 podkategorii witryn internetowych.

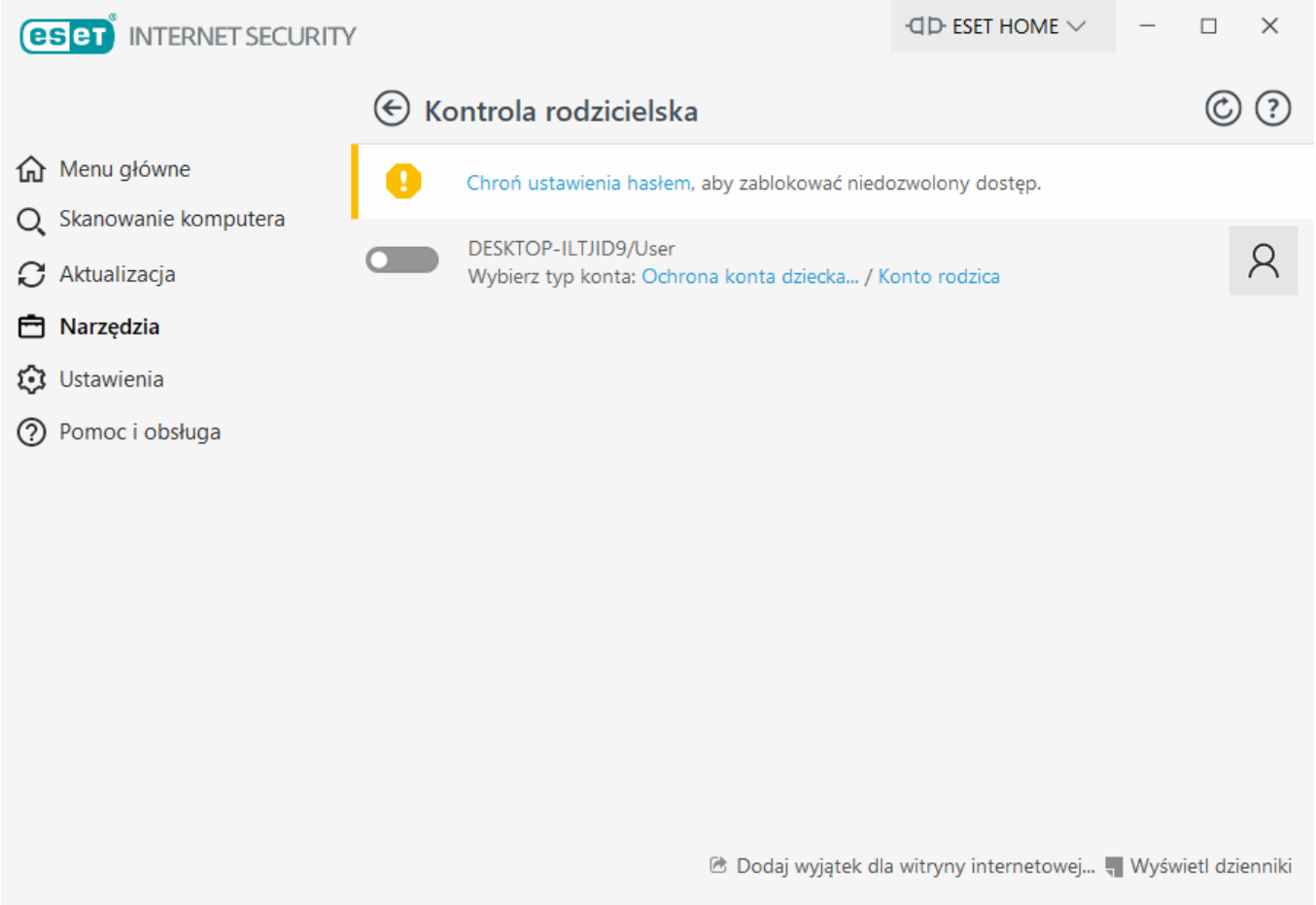
Aby aktywować kontrolę rodzicielską na określonym koncie użytkownika, należy wykonać poniższe kroki:

1. Domyślnie kontrola rodzicielska jest wyłączona w programie ESET Internet Security. Można ją włączyć na dwa sposoby:

   • Kliknij przełącznik po wybraniu kolejno opcji **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska** w głównym oknie programu i zmień stan opcji Kontrola rodzicielska na Włączona.

   • Naciśnij klawisz F5, aby przejść do drzewa **Ustawienia zaawansowane**, wybierz kolejno opcje **Strony internetowe i poczta e-mail** > **Kontrola rodzicielska**, a następnie przesuń suwak obok opcji **Włącz kontrolę rodzicielską**.

2. W głównym oknie programu kliknij kolejno opcje **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska**. Chociaż obok opcji **Kontrola rodzicielska** widnieje stan **Włączona**, należy skonfigurować kontrolę rodzicielską na danym koncie, klikając symbol strzałki, a w następnym oknie klikając pozycję **Chroń konto dziecka** lub **Konto rodzica**. W następnym oknie należy wprowadzić datę urodzenia, aby określić poziom dostępu i zalecane strony internetowe odpowiednie do wieku. Kontrola rodzicielska zostanie włączona na określonym koncie użytkownika. Aby dostosować kategorie, które mają być dozwolone lub zablokowane na karcie Kategorie, kliknij pozycję **Blokowana zawartość i ustawienia** pod nazwą konta. Aby zezwalać na niestandardowe witryny niepasujące do kategorii lub je blokować, kliknij kartę Wyjątki.



Po kliknięciu w głównym oknie programu ESET Internet Security kolejno opcji **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska** zostanie wyświetlone główne okno zawierające te elementy:

Konta użytkowników systemu Windows

Jeśli dla istniejącego konta została utworzona rola, zostanie ona w tym miejscu wyświetlona. Należy kliknąć przełącznik , aby wyświetlony został zielony znacznik obok pozycji Kontrola rodzicielska dla tego konta. Pod aktywnym kontem należy kliknąć pozycję Zablokowana zawartość i ustawienia, aby wyświetlić listę dozwolonych kategorii stron internetowych oraz zablokowanych i dozwolonych stron internetowych dla danego konta.

Aby utworzyć nowe konto (np. dla dziecka), należy wykonać następujące szczegółowe instrukcje dotyczące systemów Windows 7 i Windows Vista:
1.Otwórz sekcję **Konta użytkowników**, klikając przycisk **Start** (znajdujący się w lewym dolnym rogu pulpitu), a następnie klikając polecenie **Panel sterowania** i łącze **Konta użytkowników**.
2.Kliknij łącze **Zarządzaj kontem użytkownika**. Jeśli pojawi się monit o hasło administratora lub potwierdzenie, wpisz hasło lub potwierdź.
3.Kliknij opcję **Utwórz nowe konto**.
4.Wpisz nazwę, jaką chcesz nadać kontu użytkownika, kliknij typ konta, a następnie kliknij przycisk **Utwórz konto**.
5.Otwórz ponownie okienko Kontrola rodzicielska, klikając kolejno opcje **Ustawienia** > **Narzędzia zabezpieczające** w głównym oknie programu ESET Internet Security > **Kontrola rodzicielska**. Następnie kliknij symbol strzałki.

Zawartość dolnej części okna

Dodaj wyjątek dla witryny internetowej — w przypadku każdego konta rodzica można oddzielnie zezwalać na daną witrynę i blokować ją.

Wyświetl dzienniki — przy użyciu tej opcji można przejrzeć szczegółowy dziennik działań funkcji Kontrola rodzicielska (zablokowane strony, konto, dla którego strona była blokowana, kategoria itd.). Można też filtrować ten dziennik na podstawie własnych kryteriów, klikając opcję **Filtrowanie**.

Kontrola rodzicielska

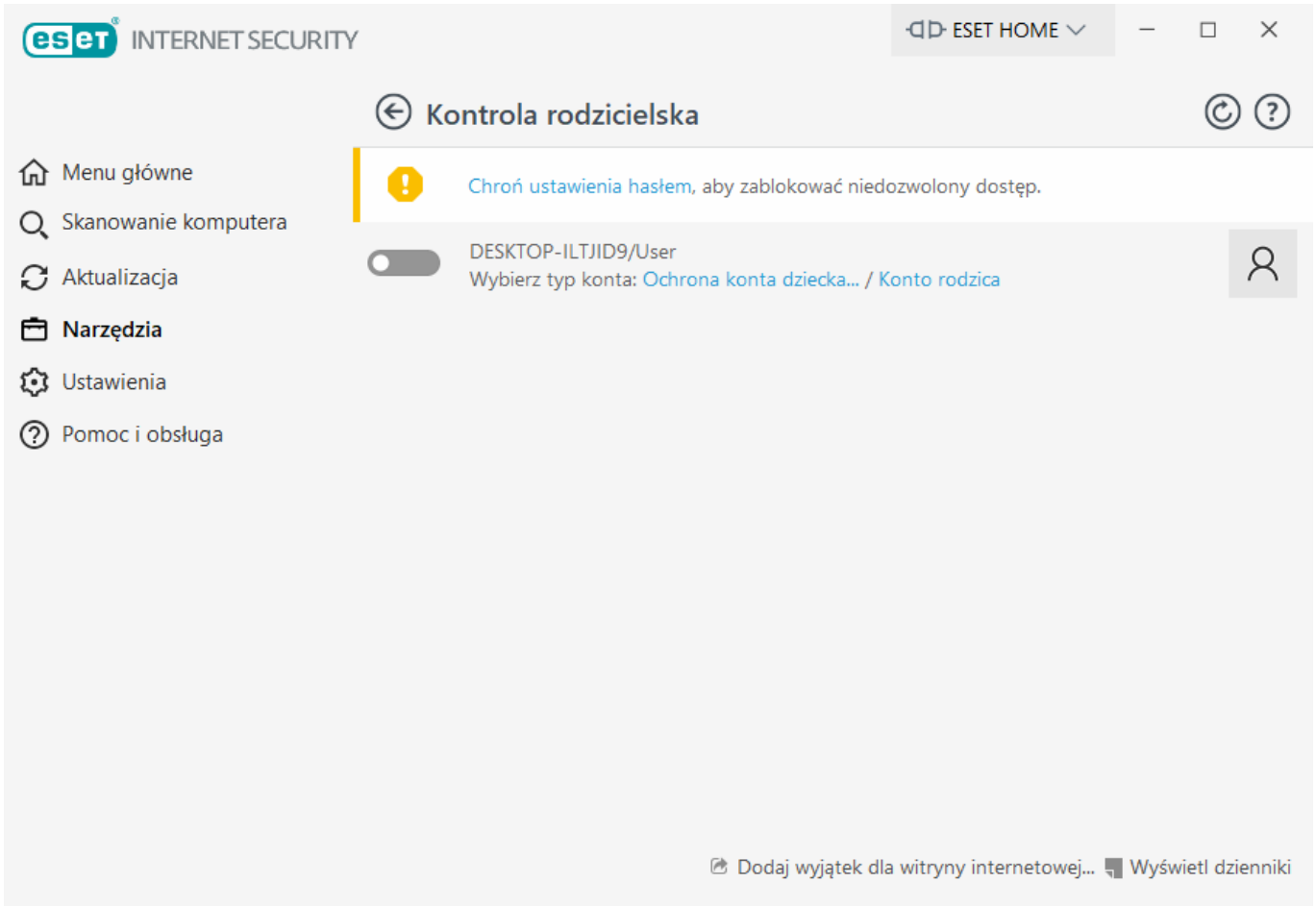
Po wyłączeniu funkcji kontroli rodzicielskiej zostanie wyświetlone okno **Wyłącz kontrolę rodzicielską**. W tym miejscu można ustawić przedział czasowy, w którym ochrona będzie wyłączona. Opcja następnie zostanie zmieniona na **Wstrzymana** lub **Wyłączona na stałe**.

Ważne jest, aby ustawienia oprogramowania ESET Internet Security były chronione hasłem. Hasło to można ustawić w sekcji Ustawienia dostępu. Jeśli hasło nie zostanie ustawione, pojawi się ostrzeżenie **Chroń wszystkie ustawienia przy użyciu hasła**, aby zapobiec nieautoryzowanym zmianom. Ograniczenia ustawione w sekcji Kontrola rodzicielska mają wpływ tylko na standardowe konta użytkownika. Administrator może ominąć każde ograniczenie, więc w jego przypadku nie mają one zastosowania.

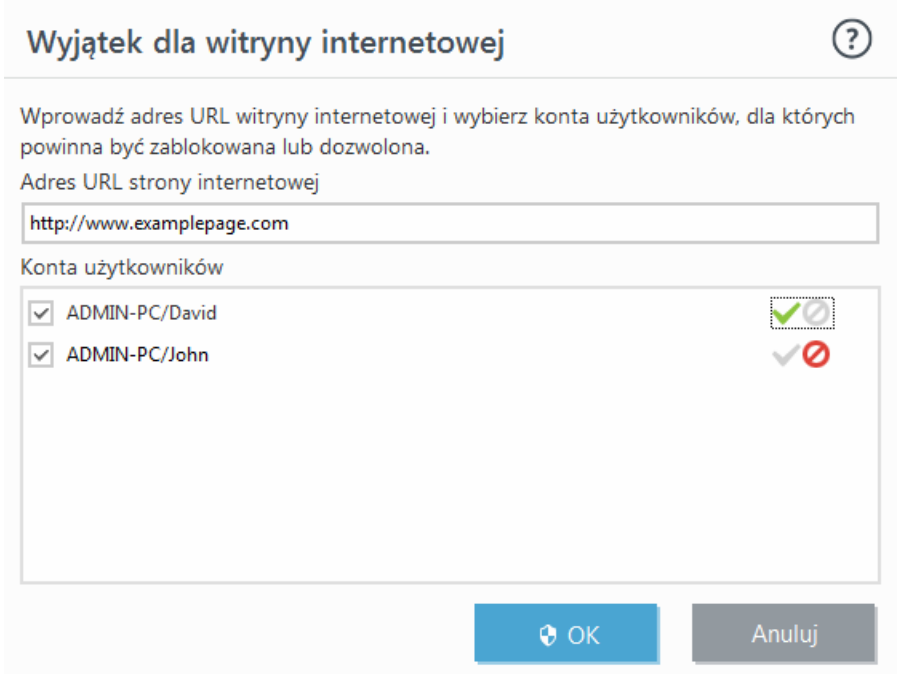
Kontrola rodzicielska wymaga do poprawnego działania włączenia funkcji filtrowania zawartości protokołów aplikacji, sprawdzania protokołu HTTP i zapory. Wszystkie te funkcje są domyślnie włączone.

Wyjątki dla witryny internetowej

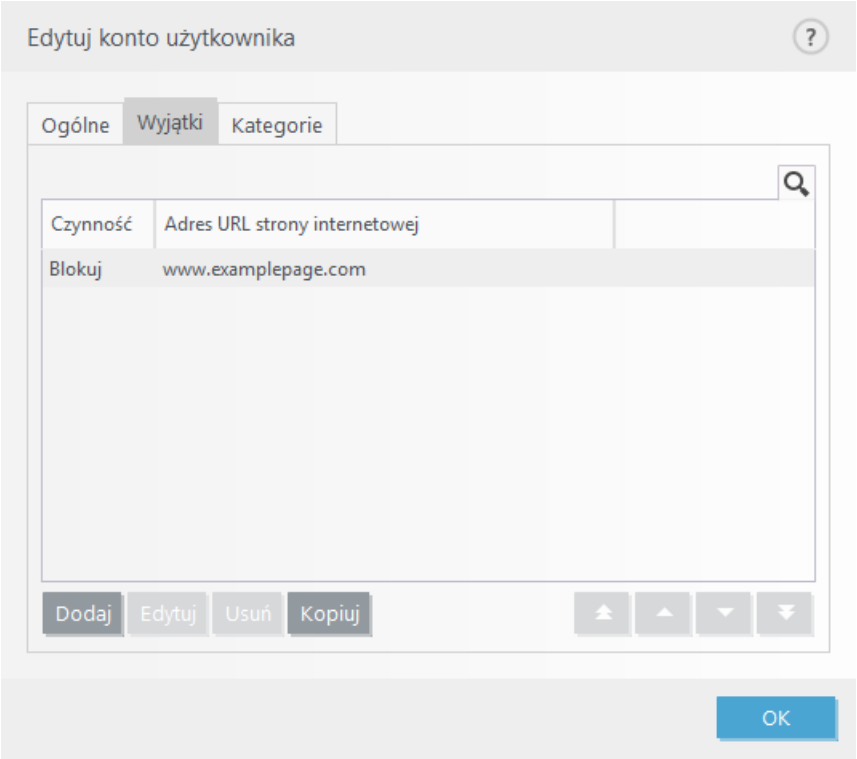
W celu dodania wyjątku dla witryny internetowej należy kliknąć kolejno pozycje **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska**, a następnie kliknąć opcję **Dodaj wyjątek dla witryny internetowej**.



Wprowadź adres URL w polu **Adres URL witryny**, wybierz ✔ (dozwolona) lub ⊘ (zablokowana) dla każdego z kont użytkownika, a następnie kliknij **OK** w celu dodania go do listy.



Aby usunąć adres URL z listy, należy kliknąć kolejno pozycje **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska**, a następnie **Blokowana zawartość i ustawienia** w odniesieniu do odpowiedniego konta użytkownika, kliknąć kartę **Wyjątek**, wybrać wyjątek i kliknąć opcję **Usuń**.



Na liście adresów URL nie można używać symboli specjalnych: * (gwiazdki) i ? (znaku zapytania). Na przykład adresy stron internetowych z wieloma domenami najwyższego poziomu należy wprowadzić ręcznie (*examplepage.com*, *examplepage.sk* itd.). W przypadku dodania domeny do listy cała zawartość umieszczona w tej domenie i wszystkich domenach podrzędnych (np. *sub.examplepage.com*) będzie zablokowana lub dozwolona zgodnie z wybraną przez użytkownika czynnością na podstawie adresu URL.

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

Konta użytkowników

Ustawienia te są dostępne w obszarze **Ustawienia zaawansowane** (F5) > **Strony internetowe i poczta e-mail** > **Kontrola rodzicielska** > **Konta użytkowników** > **Edytuj**.

W tej sekcji można powiązać konta użytkowników systemu Windows używane przez funkcję kontroli rodzicielskiej z poszczególnymi użytkownikami, aby ograniczyć tym użytkownikom dostęp do nieodpowiednich lub szkodliwych treści w Internecie.

Kolumny

Konto Windows — nazwa użytkownika.

Włączono — gdy ta opcja jest włączona, funkcje kontroli rodzicielskiej dla określonego konta użytkownika są aktywne.

Domena — nazwa domeny, do której należy użytkownik.

Data urodzenia — umożliwia określenie wieku użytkownika, do którego należy konto.

Elementy sterujące

Dodaj — powoduje wyświetlenie okna dialogowego Obsługa kont użytkowników.

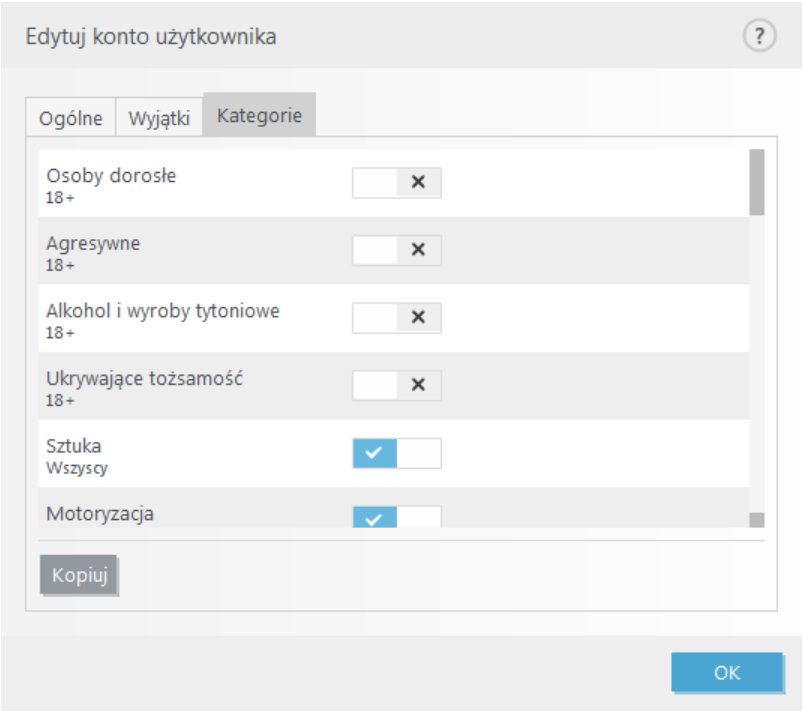
Edytuj — ta opcja umożliwia edycję zaznaczonych kont.

Usuń — umożliwia usunięcie wybranego konta.

Odśwież — jeśli dodano konto użytkownika, program ESET Internet Security może odświeżyć listę kont użytkowników bez ponownego otwierania okna.

Kategorie

Zaznacz pole wyboru w kolumnie **Włączone** obok kategorii, aby na nią zezwolić. Jeśli pole wyboru pozostanie puste, kategoria nie będzie dozwolona dla tego konta.



Poniżej podano niektóre przykłady kategorii (grup), których użytkownicy mogą nie znać:

• **Inne** — zazwyczaj prywatne (lokalne) adresy IP, na przykład w sieci intranet, 127.0.0.0/8, 192.168.0.0/16 itp. Po wystąpieniu 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 rodzicielskiej.

• **Niezaliczone do żadnej kategorii** — nieznane strony internetowe, które nie znalazły się jeszcze w bazie danych kontroli rodzicielskiej.

• **Dynamiczne** — strony internetowe, które przekierowują do innych stron w innych witrynach.

Obsługa kont użytkowników

W oknie dostępne są trzy karty:

Ogólne

Kliknij suwak obok pozycji **Włączone**, aby włączyć Kontrolę rodzicielską dla wybranego poniżej konta Windows.

Najpierw przy użyciu opcji **Wybierz** należy wybrać konto w systemie operacyjnym na komputerze. Ograniczenia ustawione w sekcji Kontrola rodzicielska mają wpływ tylko na standardowe konta w systemie Windows. Ograniczenia te nie dotyczą kont administratorów.

Jeśli konto jest używane przez rodzica, należy wybrać opcję **Konto rodzica**.

Należy wprowadzić **datę urodzenia dziecka** będącego użytkownikiem konta, aby określić jego poziom dostępu oraz reguły dostępu do stron z ograniczeniami wiekowymi.

Stopień szczegółowości zapisywania w dzienniku

ESET Internet Security zapisuje wszystkie ważne zdarzenia w pliku dziennika, który można wyświetlić bezpośrednio z poziomu menu głównego. Kliknij kolejno pozycje **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika**, a następnie wybierz opcję **Kontrola rodzicielska** z menu rozwijanego **Dziennik**.

- **Diagnostyka** — zapisywane są informacje potrzebne do ulepszenia konfiguracji programu.
- **Informacje** — umożliwia rejestrowanie komunikatów informacyjnych, w tym powiadomień o dopuszczonych i zablokowanych wyjątkach, oraz wszystkich rekordów wyższych kategorii.
- **Ostrzeżenie** — rejestrowanie błędów krytycznych oraz komunikatów ostrzegawczych.
- **Brak** — w dziennikach nie są zapisywane żadne informacje.

Wyjątki

Utworzenie wyjątku umożliwia zezwolenie użytkownikowi na dostęp do stron internetowych spoza listy wyjątków oraz zabronienie takiego dostępu. Jest to przydatne, jeśli potrzebna jest kontrola dostępu do konkretnych stron internetowych, a nie kategorii. Wyjątki utworzone dla danego konta mogą być kopiowane do innych kont i używane w odniesieniu do innych kont. Jest to przydatne, gdy trzeba utworzyć identyczne reguły dla dzieci w tym samym wieku.

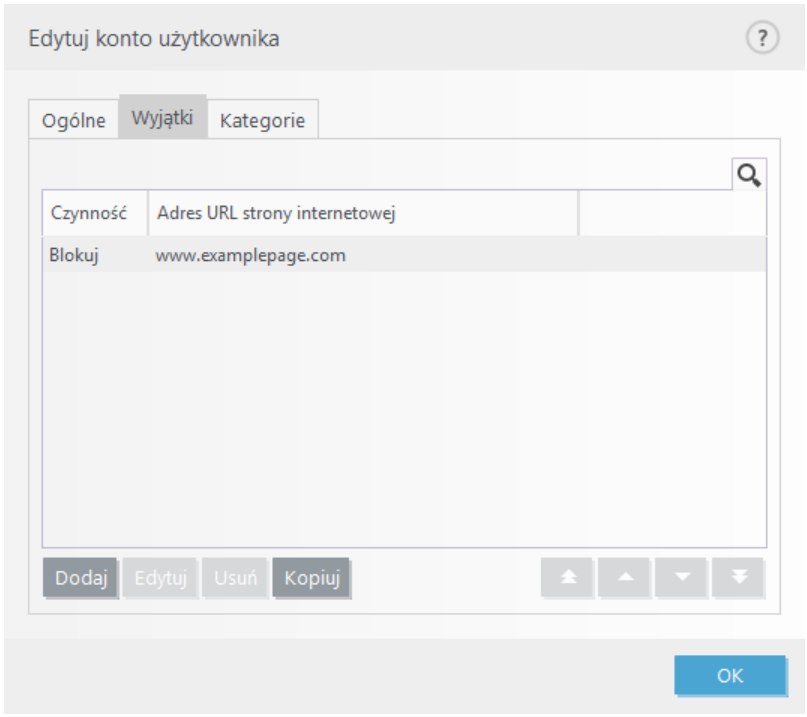
Należy kliknąć opcję **Dodaj** , aby utworzyć nowy wyjątek. W menu rozwijanym należy wybrać **czynność** (na przykład **Blokuj**), wpisać **adres URL strony internetowej**, do której ma mieć zastosowanie ten wyjątek, a następnie kliknąć przycisk **OK**. Wyjątek zostanie dodany do listy istniejących wyjątków wraz z widocznym stanem.

Dodaj — umożliwia utworzenie nowego wyjątku.

Edytuj — umożliwia edycję opcji **Adres URL strony internetowej** lub **czynność** na potrzeby wybranego wyjątku.

Usuń — umożliwia usunięcie zaznaczonego wyjątku.

Kopiuj — w menu rozwijanym należy wybrać użytkownika, od którego ma zostać skopiowany tworzony wyjątek.

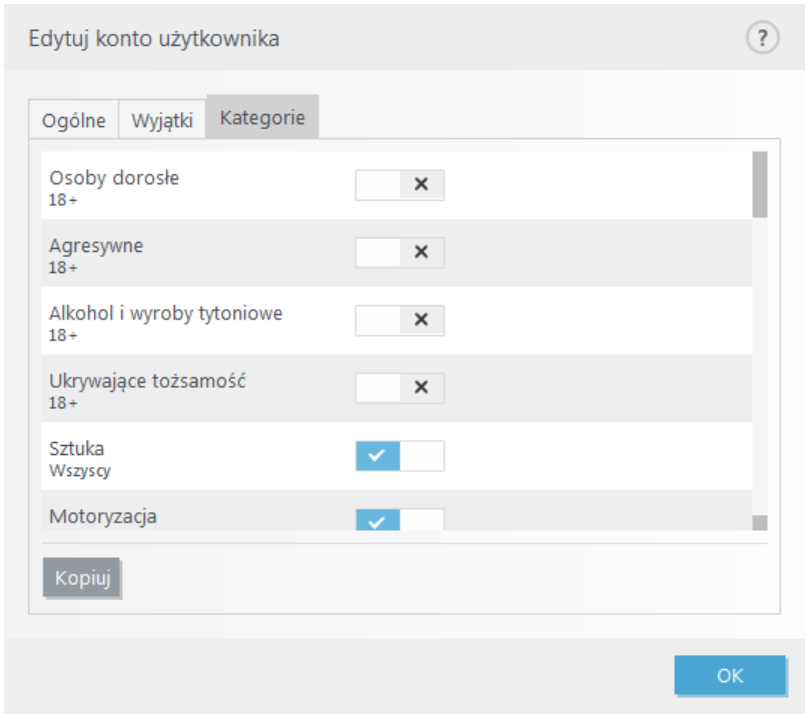


Skonfigurowane wyjątki mają wyższy priorytet w stosunku do kategorii określonych dla wybranych kont. Jeśli na przykład dla konta zablokowano kategorię **Aktualności**, ale dodano wyjątek zezwalający na dostęp do określonej strony internetowej z wiadomościami, użytkownik korzystający z tego konta ma dostęp do tej strony. Wprowadzone w tym miejscu zmiany można wyświetlać w sekcji Wyjątki.

Kategorie

W sekcji **Kategorie** można wybrać dla każdego konta ogólne kategorie stron internetowych, które mają być zablokowane lub dozwolone. Zaznaczenie pola wyboru obok kategorii powoduje zezwolenie na nią. Jeśli pole zostanie niezaznaczone, kategoria nie będzie dozwolona dla tego konta.

Kopiuj — umożliwia skopiowanie listy zablokowanych i dozwolonych kategorii z istniejącego zmodyfikowanego konta.



Skopiuj wyjątki z ustawień użytkownika

W menu rozwijanym należy wybrać użytkownika, od którego ma zostać skopiowany wyjątek.

Skopiuj kategorie z konta

Umożliwia skopiowanie listy zablokowanych i dozwolonych kategorii ze zmodyfikowanego uprzednio konta.

Włącz kontrolę rodzicielską

Opcja **Włącz kontrolę rodzicielską** integruje Kontrolę rodzicielską z programem ESET Internet Security. Sekcja Kontrola rodzicielska w oknie głównym w obszarze **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska** zostanie wyświetlona.

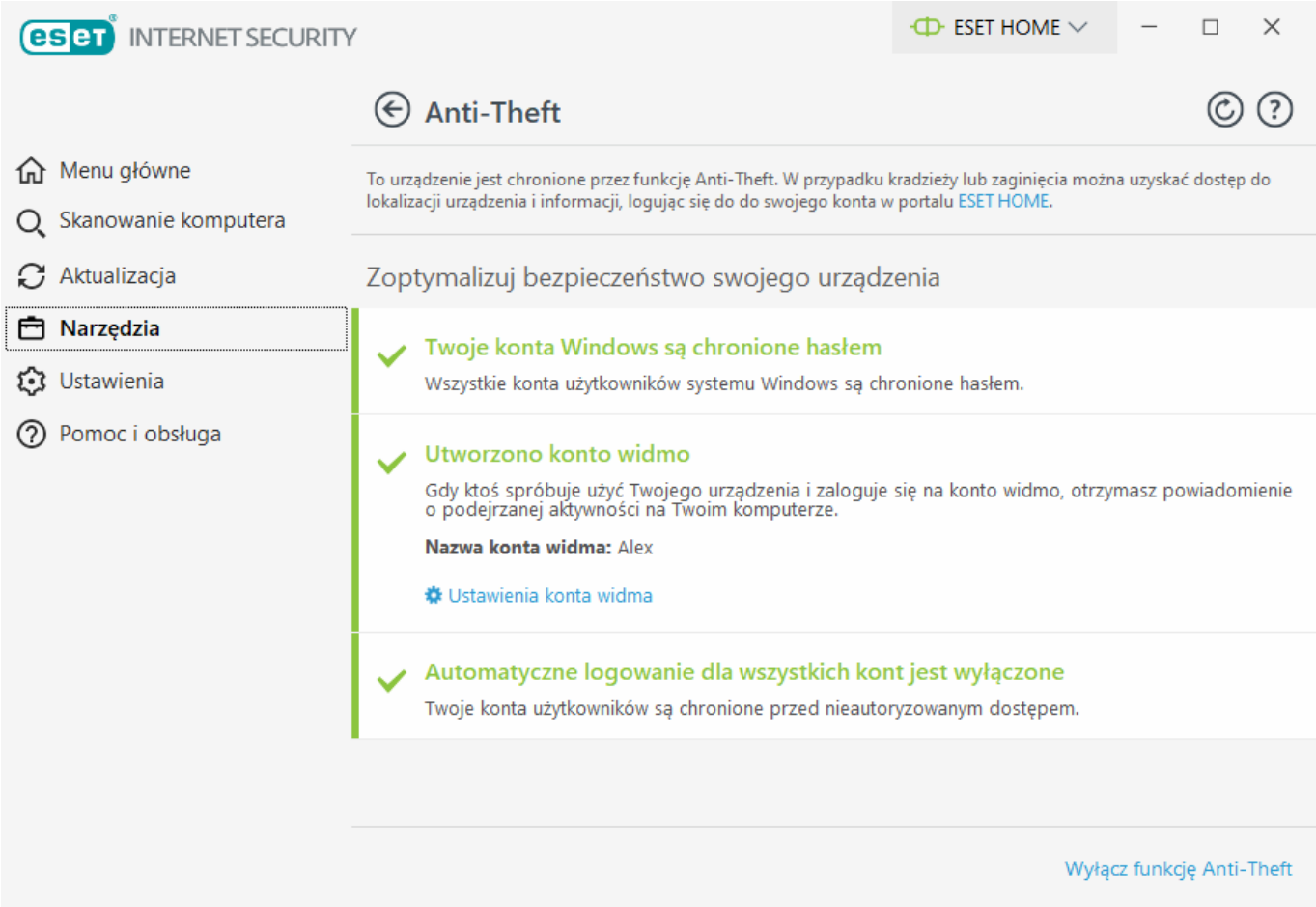
Anti-Theft

Urządzenia osobiste są ciągle narażone na zgubienie lub kradzież podczas naszych codziennych podróży z domu do pracy lub innych miejsc publicznych. Anti-Theft to funkcja, która zwiększa bezpieczeństwo na poziomie użytkownika w przypadku zgubienia lub kradzieży urządzenia. Anti-Theft umożliwi monitorowanie działań wykonywanych na urządzeniu oraz śledzenie brakującego urządzenia z wykorzystaniem lokalizacji na podstawie adresu w ESET HOME. Dzięki temu odzyskasz urządzenie i ochronisz swoje dane osobowe.

Dzięki zastosowaniu nowoczesnych technologii (np. wyszukiwania lokalizacji geograficznej adresu IP, rejestrowania zdjęć za pomocą kamery internetowej, ochrony kont użytkowników i monitorowania urządzenia) funkcja Anti-Theft może pomóc zarówno właścicielowi, jak i organom ścigania w zlokalizowaniu komputera lub urządzenia w przypadku jego zgubienia lub kradzieży. W ESET HOME możesz zobaczyć, jaka aktywność jest wykonywana na komputerze lub urządzeniu.

Aby dowiedzieć się więcej na ten temat Anti-Theft w ESET HOME, zapoznaj się z ESET HOME Pomocą online.

Po włączeniu Anti-Theft możesz zoptymalizować bezpieczeństwo urządzenia w głównym oknie programu > **Narzędzia** > **Anti-Theft**.



Opcje optymalizacji

Nie utworzono konta widma

Utworzenie konta widmo zwiększa szansę na zlokalizowanie zgubionego lub skradzionego urządzenia. Jeśli oznaczysz urządzenie jako zaginione, Anti-Theft zablokuje dostęp do aktywnych kont użytkownika w celu ochrony danych poufnych. Ewentualne próby korzystania z urządzenia będą ograniczone do konta widmo. Konto widmo to konto gościa z ograniczonymi uprawnieniami. Jest ono używane jako konto domyślne do momentu, gdy urządzenie zostanie oznaczone jako odzyskane — dzięki temu nie ma możliwości zalogowania się na inne konta użytkownika lub uzyskania dostępu do danych użytkownika.

Każda próba zalogowania się do konta widmo, gdy komputer jest w normalnym stanie, zostanie zgłoszona w wiadomości e-mail z informacją o podejrzanej aktywności na komputerze. Po otrzymaniu powiadomienia e-mail można zdecydować, czy komputer ma zostać oznaczony jako zaginiony.

Aby utworzyć konto widmo, kliknij **Utwórz konto widmo**, wpisz **nazwę konta widma** w polu tekstowym i kliknij **Utwórz**.

Po utworzeniu konta widmo kliknij **Ustawienia konta widma**, aby zmienić nazwę lub usunąć konto.

Ochrona hasłem kont Windows

Twoje konto użytkownika nie jest chronione hasłem. To ostrzeżenie zostanie wyświetlone, jeśli co najmniej jedno konto użytkownika nie jest chronione hasłem. Aby rozwiązać ten problem, należy utworzyć na komputerze hasło dla wszystkich użytkowników (z wyjątkiem **konta widma**).

Aby utworzyć hasło do konta użytkownika, kliknij **Zarządzaj kontami Windows** i zmień hasło lub postępuj zgodnie z poniższymi instrukcjami:

1. Naciśnij klawisze CTRL+Alt+Delete na klawiaturze.
2. Kliknij **Zmień hasło**.
3. Zostaw pole **Stare hasło** puste.
4. Wpisz hasło w polach **Nowe hasło** i **Potwierdź hasło**, a następnie naciśnij klawisz **Enter**.

Automatyczne logowanie do kont Windows

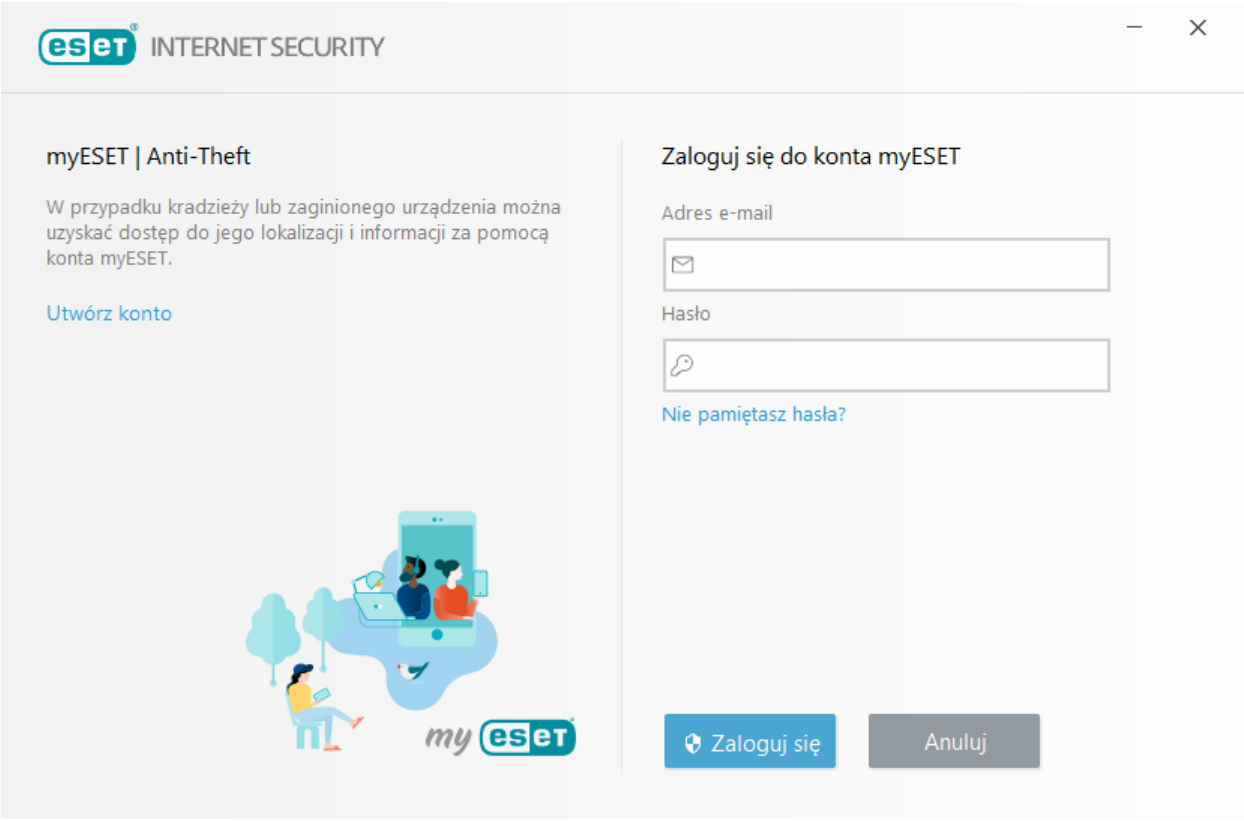
Twoje konto użytkownika ma włączone automatyczne logowanie. W związku z tym Twoje konto nie jest chronione przed nieautoryzowanym dostępem. To ostrzeżenie zostanie wyświetlone, jeśli na co najmniej jednym koncie użytkownika włączono automatyczne logowanie. Aby rozwiązać ten problem, kliknij opcję **Wyłącz automatyczne logowanie**.

Automatyczne logowanie do konta widma

Automatyczne logowanie jest aktywne dla **konta widmo** na Twoim urządzeniu. Gdy urządzenie pracuje w normalnym stanie, nie zalecamy korzystania z automatycznego logowania, ponieważ może to powodować problemy z dostępem do rzeczywistego konta użytkownika lub wysyłać fałszywe alarmy o zaginięciu komputera. Aby rozwiązać ten problem, kliknij opcję **Wyłącz automatyczne logowanie**.

Zaloguj się na swoje konto ESET HOME.

Aby włączyć/wyłączyć Anti-Theft i uzyskać dostęp do lokalizacji urządzenia i informacji o nim w ESET HOME, zaloguj się na swoje konto ESET HOME.



Dostępnych jest kilka metod logowania się na konto ESET HOME:

- **Użyj swojego adresu e-mail i hasła ESET HOME** — wpisz **adres e-mail** i **hasło** użyte do utworzenia konta ESET HOME, a następnie kliknij przycisk **Zaloguj się**.

- **Użyj swojego konta Google /AppleID** – kliknij **Kontynuuj za pomocą konta Google** lub **Kontynuuj przy użyciu Apple** i zaloguj się na odpowiednie konto. Po pomyślnym zalogowaniu zostaniesz przekierowany na stronę internetową potwierdzenia ESET HOME. Aby kontynuować, przejdź z powrotem do okna produktu ESET. Aby uzyskać więcej informacji na temat konta Google /loginu AppleID, zapoznaj się z instrukcjami na stronie pomocy online ESET HOME.

- **Zeskanuj kod QR —** kliknij opcję **Skanuj kod QR**, aby wyświetlić kod QR. Otwórz aplikację mobilną ESET HOME i zeskanuj kod QR lub skieruj aparat urządzenia na kod QR. Aby uzyskać więcej informacji, zobacz instrukcje w Pomocy online ESET HOME.

Logowanie nie powiodło się — częste błędy.

Jeśli nie posiadasz konta ESET HOME, kliknij **Utwórz konto**, aby się zarejestrować, lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.
Jeśli nie pamiętasz hasła, kliknij **Nie pamiętam hasła** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie lub skorzystaj z instrukcji w sekcji pomocy programu ESET HOME.

Anti-Theft nie obsługuje systemu Microsoft Windows Home Server.

Konfiguracja nazwy urządzenia

Pole **Nazwa urządzenia** zawiera nazwę komputera (urządzenia), która będzie wyświetlana jako identyfikator ESET HOME na wszystkich serwerach. Nazwa komputera jest używana domyślnie. Wpisz nazwę urządzenia lub użyj nazwy domyślnej i kliknij przycisk **Kontynuuj**.

Anti-Theft włączono/wyłączono

To okno zawiera komunikat potwierdzający włączenie/wyłączenie Anti-Theft:

- Włączono — urządzenie jest teraz chronione przez program Anti-Theft, a jego zabezpieczeniami można zarządzać zdalnie w portalu ESET HOME, korzystając z konta.

- Wyłączono — program Anti-Theft jest wyłączony na tym urządzeniu, a wszystkie dane związane z <%ESET_ANTTHEFT%> tego urządzenia są usuwane z portalu ESET HOME.

Dodawanie nowego urządzenia nie powiodło się

Podczas aktywacji produktu Anti-Theft wystąpił błąd.

Najczęstsze scenariusze to:

- Błąd logowania do ESET HOME

- Brak połączenia z Internetem (lub Internet w danej chwili nie działa)

Jeśli nie możesz rozwiązać problemu, skontaktuj się z działem pomocy technicznej firmy ESET.

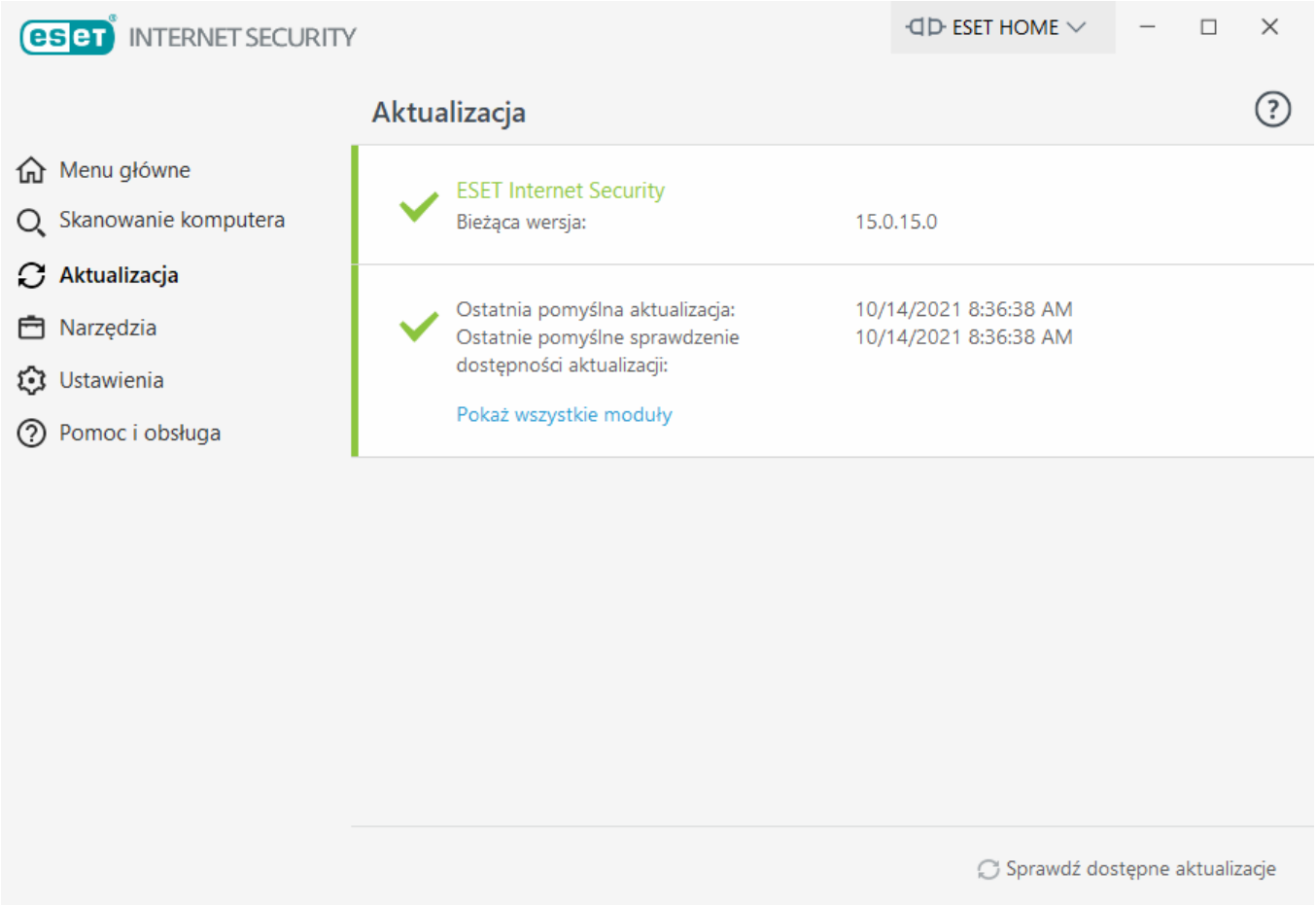
Aktualizowanie programu

Regularne aktualizowanie programu ESET Internet Security to najlepszy sposób na zapewnienie najwyższego poziomu bezpieczeństwa komputera. Moduł aktualizacji zapewnia aktualność modułów programu i komponentów systemu.

Klikając przycisk **Aktualizacja** w głównym oknie programu, można wyświetlić bieżący stan aktualizacji, w tym datę i godzinę ostatniej pomyślnej aktualizacji, oraz ustalić, czy w danej chwili należy przeprowadzić aktualizację.

Oprócz aktualizacji automatycznych można kliknąć przycisk **Sprawdź aktualizacje**, aby przejść do ręcznej aktualizacji. Regularna aktualizacja modułów programu oraz komponentów stanowi istotny element kompleksowej ochrony przed szkodliwym kodem. Należy zwrócić uwagę na konfigurację modułów produktu i działanie funkcji aktualizacji. Aby można było otrzymywać aktualizacje, należy aktywować produkt przy użyciu klucza licencyjnego. Jeśli klucz licencyjny nie został wpisany podczas instalacji, trzeba to zrobić w celu aktywowania programu podczas aktualizacji na potrzeby dostępu do serwerów aktualizacji ESET.

> Klucz licencyjny jest wysyłany w wiadomości e-mail przez firmę ESET po zakupie programu ESET Internet Security.



Bieżąca wersja — umożliwia wyświetlenie numeru zainstalowanej bieżącej wersji produktu.

Ostatnia pomyślna aktualizacja — wyświetla datę ostatniej udanej aktualizacji. Jeśli nie jest wyświetlona niedawna data, moduły produktu mogą być nieaktualne.

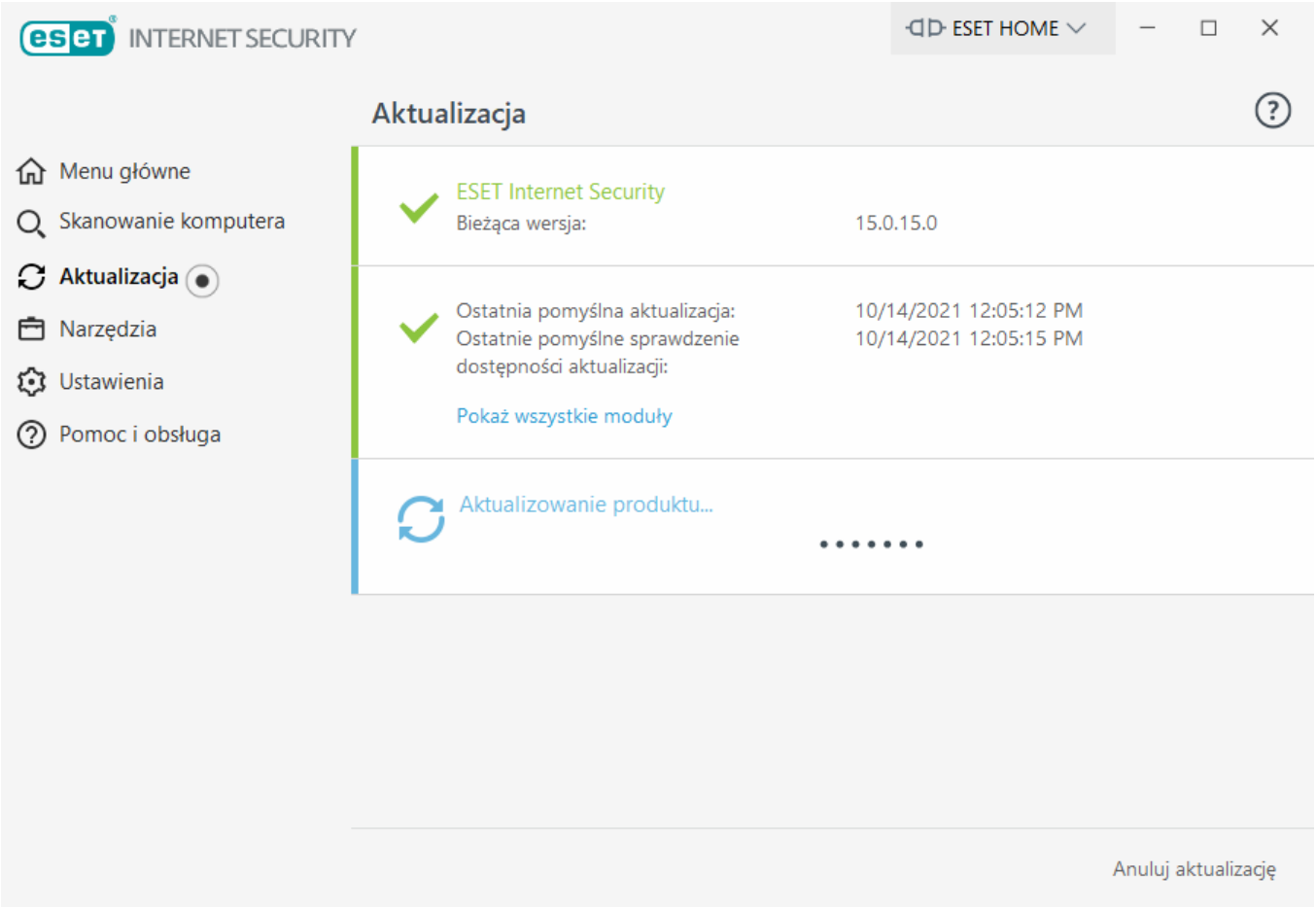
Ostatnie pomyślne sprawdzenie dostępności aktualizacji — wyświetla datę ostatniego udanego sprawdzenia dostępności aktualizacji.

Pokaż wszystkie moduły — wyświetla listę zainstalowanych modułów programu.

Kliknij przycisk **Sprawdzanie dostępnych aktualizacji**, aby wykryć ostatnią dostępną wersję ESET Internet Security.

Procedura aktualizacji

Po kliknięciu opcji **Sprawdź dostępne aktualizacje** rozpocznie się pobieranie. W jego trakcie jest wyświetlany pasek postępu i czas pozostały do końca pobierania. Aby przerwać aktualizację, należy kliknąć przycisk **Anuluj aktualizację**.



W normalnych warunkach w oknie **Aktualizacja** widoczny jest zielony znacznik sygnalizujący aktualność programu. Jeżeli nie jest on widoczny, oznacza to, że program jest nieaktualny i bardziej podatny na infekcje. Należy wówczas jak najszybciej zaktualizować moduły programu.

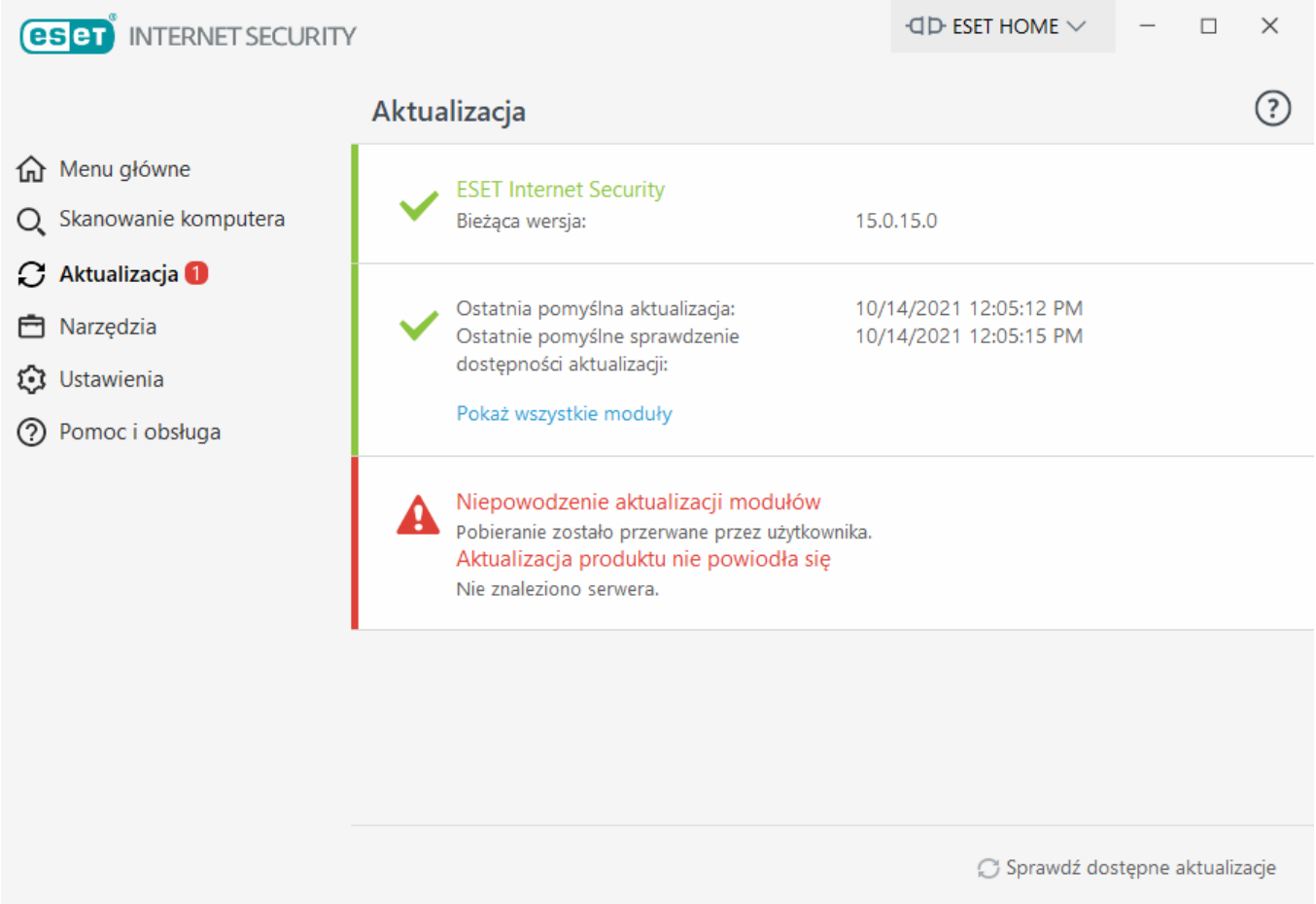
Nieudana aktualizacja

Jeżeli pojawi się komunikat o nieudanej aktualizacji modułów, przyczyną mogą być następujące problemy:

1. **Nieprawidłowa licencja** — licencja używana do aktywacji programu jest nieprawidłowa lub wygasła. W

głównym oknie programu kliknij pozycję **Pomoc i obsługa** > **Zmień licencję**, a następnie wprowadź nowy klucz licencyjny.

2. **Wystąpił błąd podczas pobierania plików aktualizacji** — możliwa 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).



Po pomyślnej aktualizacji programu ESET Internet Security do nowszej wersji zalecamy ponowne uruchomienie komputera, aby zapewnić prawidłową aktualizację wszystkich modułów programu. Po zwykłych aktualizacjach modułów nie jest wymagane ponowne uruchomienie komputera.

Więcej informacji można znaleźć w artykule Rozwiązywanie problemów związanych z komunikatem „Aktualizacja modułów nie powiodła się”.

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.

Podstawowe

Jeżeli nie ustawiono określonego profilu aktualizacji w sekcji **Ustawienia zaawansowane** > **Zapora** > **Znane sieci**,

aktualnie używany profil aktualizacji jest wyświetlany w menu rozwijanym **Wybierz domyślny profil aktualizacji**.

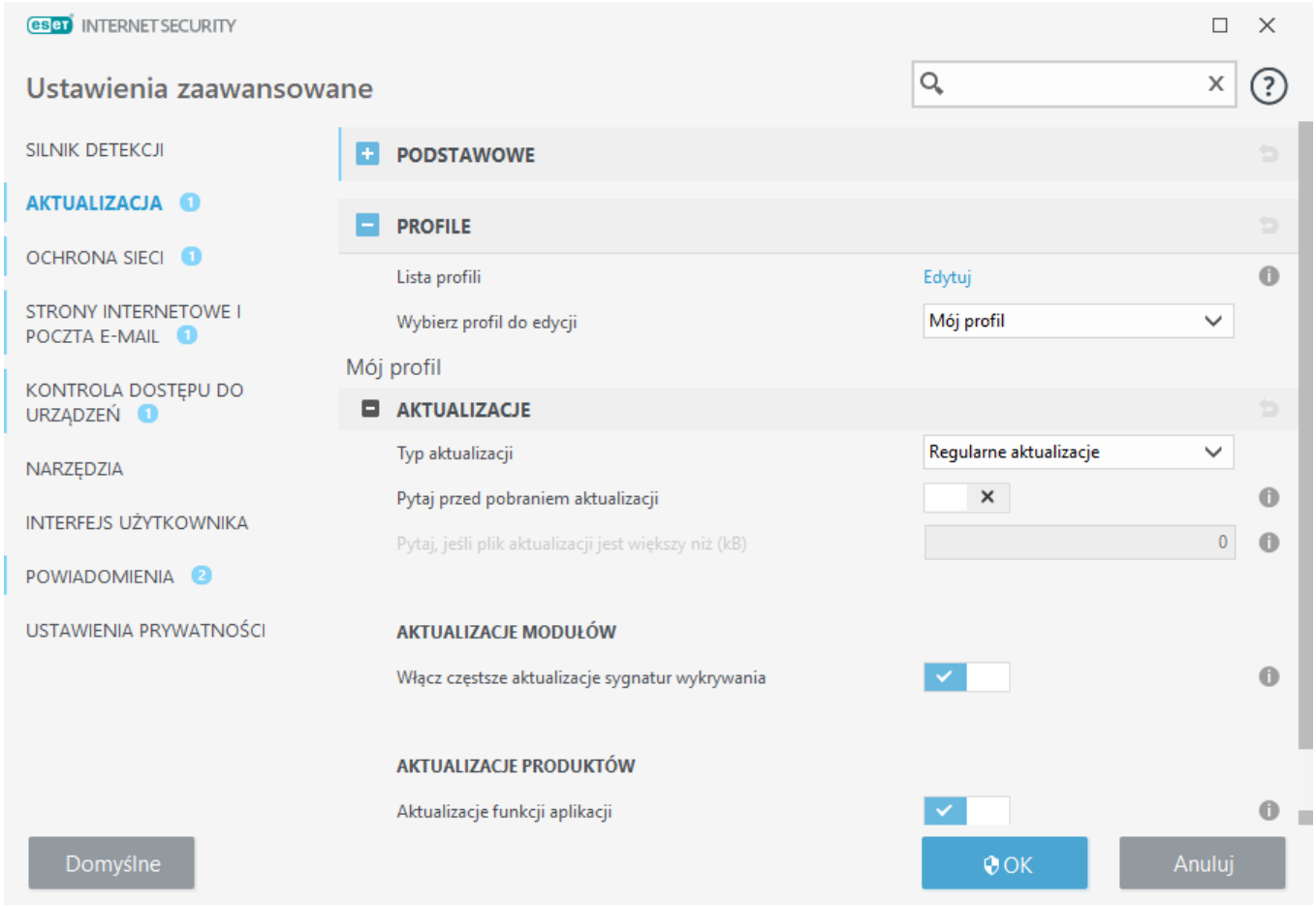
Informacje dotyczące tworzenia nowego profilu można znaleźć w części Profile aktualizacji.

Automatyczne przełączanie profilu — umożliwia zmianę profilu dla określonej sieci.

Jeśli przy próbie pobrania aktualizacji silnika detekcji lub modułów wystąpią trudności, kliknij opcję **Wyczyść** w celu usunięcia tymczasowych plików aktualizacji lub wyczyszczenia pamięci podręcznej.

Cofanie aktualizacji modułów

W razie podejrzeń, że nowa aktualizacja silnika detekcji i/lub modułów programu może być niestabilna lub uszkodzona, można wycofać zmiany i wrócić do poprzedniej wersji oraz wyłączyć aktualizacje na określony czas.



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).

Profile

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 **Wybierz profil do edycji** jest wyświetlany 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**.

Aktualizacje

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.

Pytaj przed pobraniem aktualizacji — program będzie wyświetlać powiadomienie, w którym można zaakceptować lub odrzucić pobieranie pliku aktualizacji.

Pytaj, jeśli plik aktualizacji jest większy niż (kB) — jeśli rozmiar pliku aktualizacji przekroczy podaną wartość, w programie zostanie wyświetlone powiadomienie. Jeśli rozmiar plik aktualizacji zostanie ustawiony na 0kB, okno potwierdzenia będzie wyświetlane każdorazowo.

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 gier powoduje wyłączenie wszystkich powiadomień.

Aktualizacje modułów

Włącz częstsze aktualizacje sygnatur detekcji — sygnatury detekcji będą aktualizowane w krótszych odstępach. Wyłączenie tego ustawienia może negatywnie wpłynąć na wskaźnik wykrywalności.

Aktualizacje produktów

Aktualizacje funkcji aplikacji — automatyczne instalowanie nowych wersji programu ESET Internet Security.

Opcje połączenia

Aby używać serwera proxy do pobierania aktualizacji, zobacz sekcję Opcje połączenia.

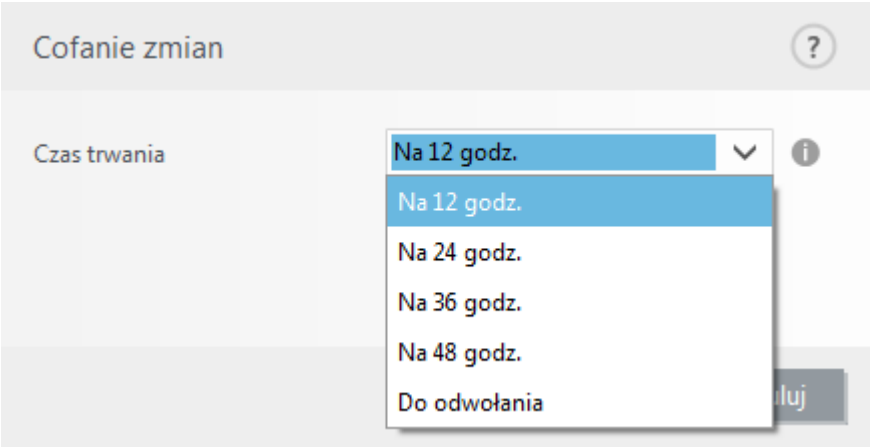
Cofanie aktualizacji

W razie podejrzeń, że nowa aktualizacja silnika detekcji 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.

ESET Internet Security zapisuje migawki silnika detekcji i modułów programu przeznaczone do użycia z funkcją cofania zmian. Aby tworzyć migawki bazy danych wirusów, należy pozostawić włączony przełącznik opcji **Utwórz migawki modułów**. Gdy opcja ta jest włączona, pierwsza migawka tworzona jest przy pierwszej aktualizacji. Następna po 48 godzinach. Pole **Liczba kopii przechowywanych lokalnie**określa liczbę przechowywanych migawek silnika detekcji.

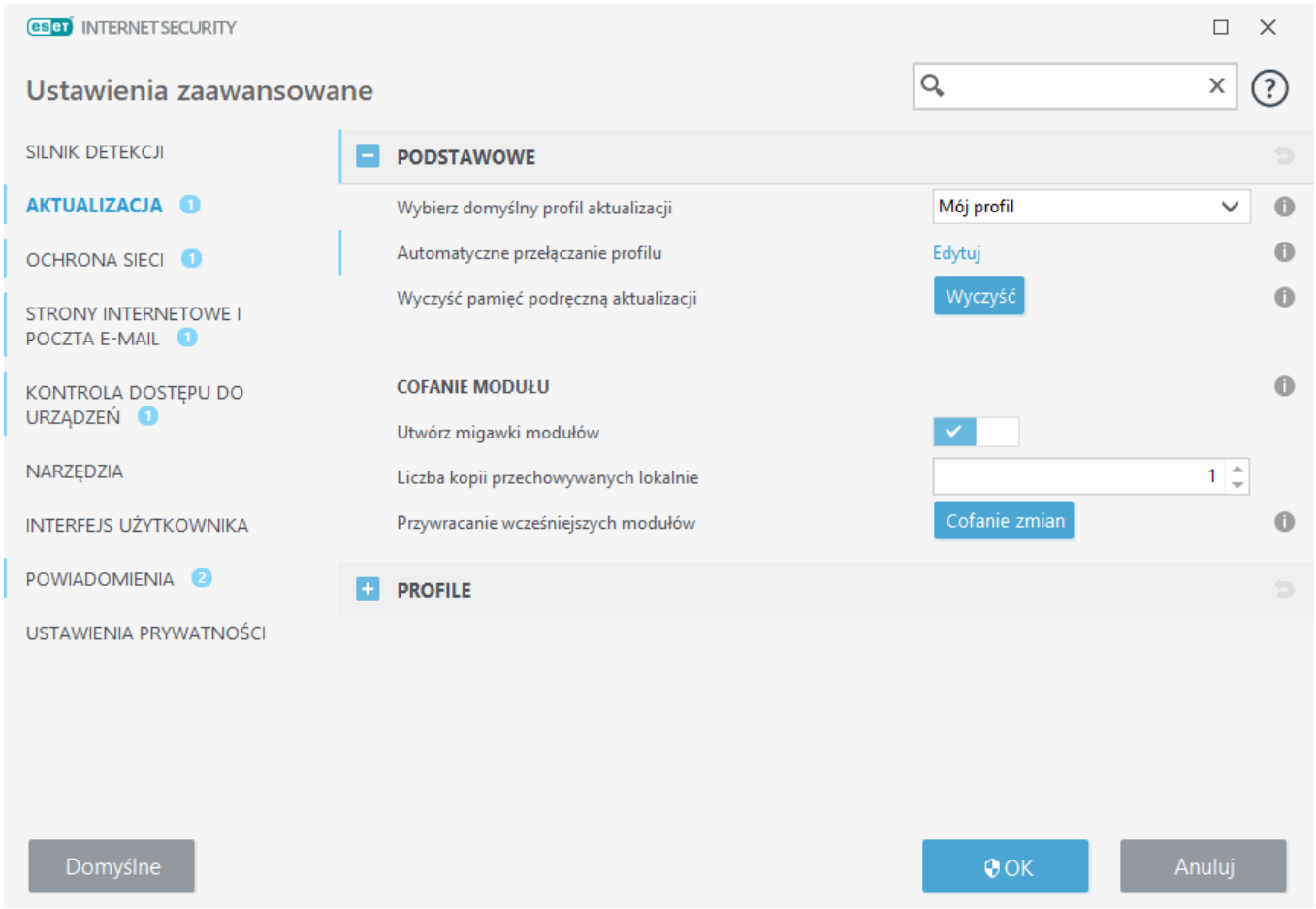
Po osiągnięciu maksymalnej ilości migawek (na przykład trzy), najstarsza migawka jest zastępowana nową migawką co 48 godzin. ESET Internet Security potrafi przywrócić wersję aparatu wykrywania i aktualizacji modułu programu do najstarszej migawki.

Po kliknięciu opcji **Cofanie zmian** (**Ustawienia zaawansowane** (F5) > **Aktualizacja** > **Podstawowe**) z menu rozwijanego **Czas trwania** należy wybrać okres, w którym aktualizacje silnika detekcji i modułów programu będą wstrzymane.



Wybranie opcji **Do odwołania** umożliwia odroczenie regularnych aktualizacji na czas nieokreślony do czasu ręcznego przywrócenia funkcji aktualizacji. ESET nie zaleca wyboru tej opcji, ponieważ wiąże się ona z potencjalnym zagrożeniem bezpieczeństwa.

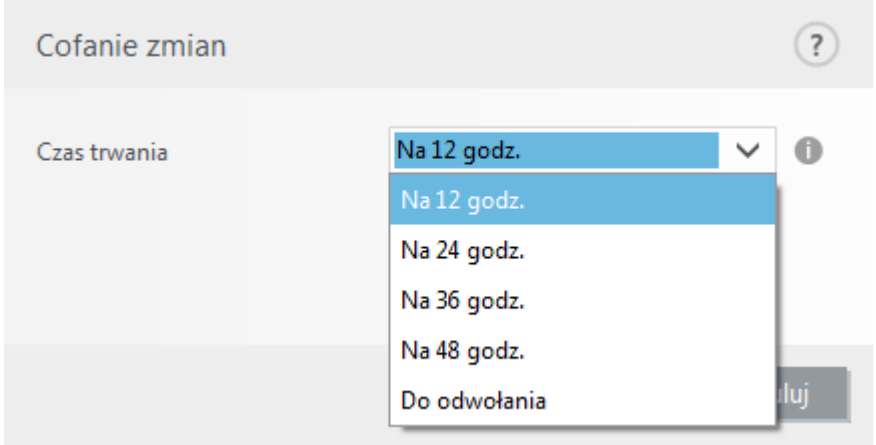
Jeśli funkcja wycofywania zmian zostanie uruchomiona, przycisk **Cofnij zmiany** zmieni się w przycisk **Zezwalaj na aktualizacje**. W przedziale czasowym wybranym z menu rozwijanego **Zawieś aktualizacje** nie będą dozwolone żadne aktualizacje. Silnik detekcji jest przywracany do najstarszej dostępnej wersji i zapisywany w postaci migawki w systemie plików lokalnego komputera.



Przyjmijmy, że numer 22700 oznacza najnowszą wersję silnika detekcji. Wersje 22698 i 22696 są przechowywane jako migawki silnika detekcji. Należy zauważyć, że wersja 22697 nie jest dostępna, ponieważ komputer był wyłączony i zanim zdążył pobrać wersję 22697, została już udostępniona nowsza aktualizacja. Jeśli w polu **Liczba kopii przechowywanych lokalnie** ustawiono wartość 2, to po kliknięciu przycisku **Cofanie zmian** zostanie przywrócona wersja silnika detekcji (i modułów programu) numer 22696. Ten proces może trochę potrwać. To, czy wersja silnika detekcji została przywrócona, można sprawdzić w głównym oknie programu w sekcji Aktualizacja.

Interwał czasu wycofywania

Po kliknięciu opcji **Cofanie zmian** (**Ustawienia zaawansowane** (F5) > **Aktualizacja** > **Podstawowe**) z menu rozwijanego **Czas trwania** należy wybrać okres, w którym aktualizacje silnika detekcji i modułów programu będą wstrzymane.



Wybranie opcji **Do odwołania** umożliwia odroczenie regularnych aktualizacji na czas nieokreślony do czasu ręcznego przywrócenia funkcji aktualizacji. ESET nie zaleca wyboru tej opcji, ponieważ wiąże się ona z potencjalnym zagrożeniem bezpieczeństwa.

Aktualizacje produktów

Sekcja **Aktualizacje produktów** umożliwia automatyczne instalowanie nowych aktualizacji funkcji, gdy są dostępne.

Aktualizacje funkcji aplikacji wprowadzają nowe funkcje lub zmieniają te, które są znane z poprzednich wersji. Może ona być wykonywana automatycznie, bez interwencji użytkownika. Istnieje też możliwość powiadamiania użytkownika o aktualizacjach. Po zainstalowaniu aktualizacji funkcji aplikacji może być wymagane ponowne uruchomienie komputera.

Aktualizacje funkcji aplikacji — gdy ta opcja jest włączona, aktualizacje funkcji aplikacji będą przeprowadzane automatycznie.

Opcje połączenia

Aby przejść do opcji konfiguracji serwera proxy dla danego profilu aktualizacji, kliknij pozycję **Aktualizacja** w drzewie **Ustawienia zaawansowane** (F5), a następnie kliknij kolejno pozycje **Profile** > **Aktualizacje** > **Opcje połączenia**. Kliknij menu rozwijane **Tryb proxy** i wybierz jedną spośród trzech następujących opcji:

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

Wybranie 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 Internet Security nie używać serwera proxy.

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

- Do aktualizacji programu ESET Internet Security używany jest inny serwer niż ten, który zdefiniowano w obszarze **Narzędzia** > **Serwer proxy**. W tej konfiguracji w razie potrzeby należy podać następujące informacje dotyczące nowego serwera: adres **serwera proxy**, **port** komunikacyjny (domyślnie 3128) oraz **nazwę użytkownika** i **hasło**.

- Ustawienia serwera proxy nie są konfigurowane na poziomie globalnym, ale program ESET Internet Security będzie łączyć się z serwerem proxy w celu pobrania aktualizacji.
- Komputer jest podłączony do Internetu za pośrednictwem serwera proxy. Podczas instalacji programu ustawienia są pobierane z opcji programu Internet Explorer, jeśli jednak ulegną później zmianie (np. użytkownik zmieni dostawcę Internetu), należy upewnić się, że ustawienia serwera proxy podane 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**.

Użyj połączenia bezpośredniego, jeśli serwer proxy jest niedostępny — niedostępny serwer proxy będzie pomijany podczas aktualizacji.

> Pola **Nazwa użytkownika** oraz **Hasło** w tej części dotyczą serwera proxy. Pola te należy wypełnić tylko wtedy, gdy uzyskanie dostępu do serwera proxy wymaga podania nazwy użytkownika i hasła. Pola te należy wypełnić tylko wtedy, gdy uzyskanie dostępu do serwera proxy wymaga podania nazwy użytkownika i hasła i gdy wiadomo, że w celu uzyskania dostępu do Internetu niezbędne jest podanie hasła do serwera proxy.

Tworzenie zadań aktualizacji

Aktualizacje można uruchamiać ręcznie, klikając opcję **Sprawdź dostępne aktualizacje** w oknie głównym wyświetlanym po kliknięciu opcji **Aktualizacja** w menu głównym.

Inną możliwością jest wykonywanie aktualizacji jako zaplanowanych zadań. Aby skonfigurować zaplanowane zadanie, kliknij kolejno opcje **Narzędzia** > **Więcej narzędzi** > **Harmonogram**. Domyślnie w programie ESET Internet 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.

Okno dialogowe — Wymagane uruchomienie ponowne

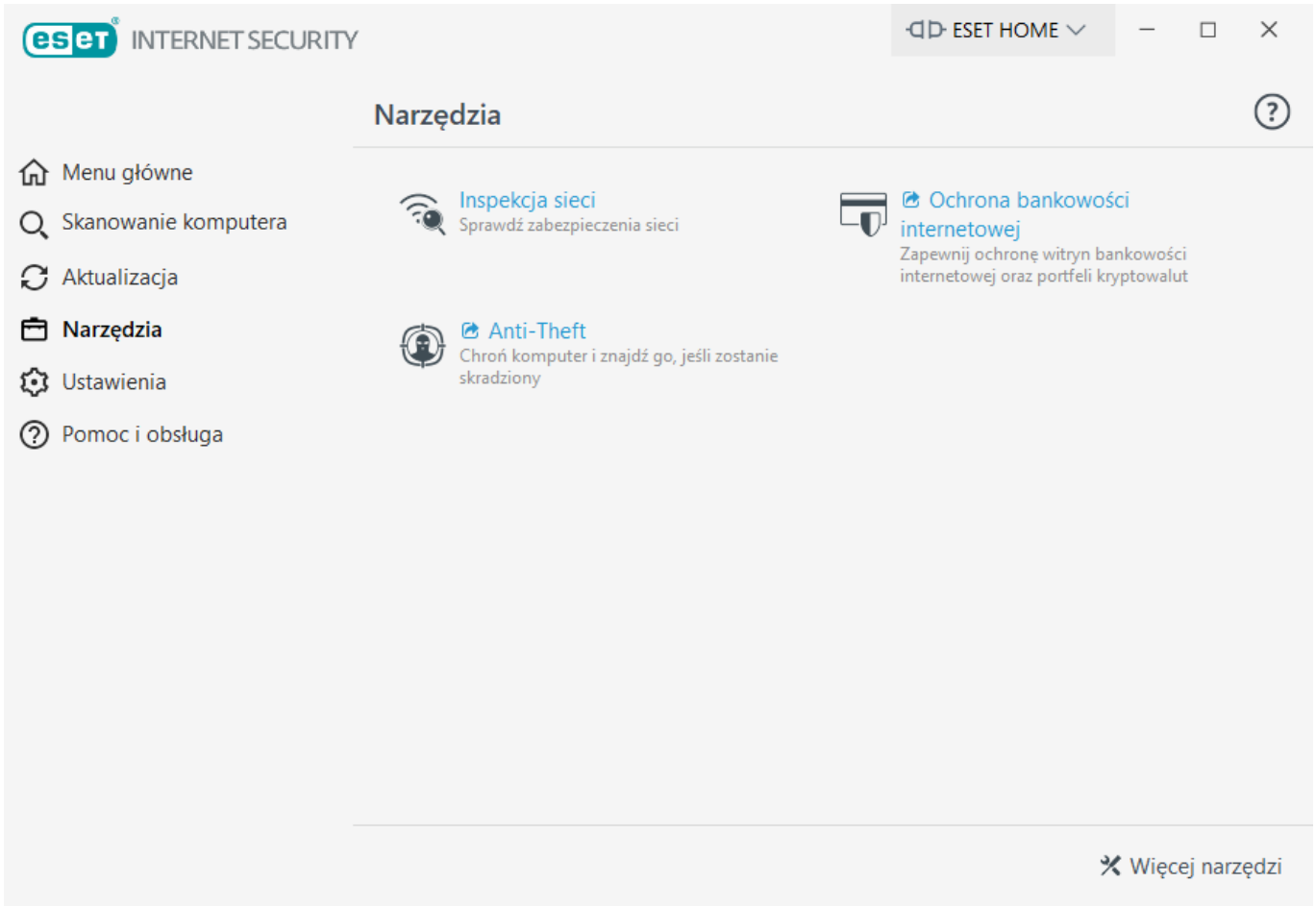
Ponowne uruchomienie komputera jest wymagane po zaktualizowaniu programu ESET Internet Security do nowej wersji. Nowe wersje produktu ESET Internet Security są wydawane w celu wdrożenia ulepszeń lub rozwiązania problemów, których automatyczne aktualizacje modułów programu nie mogą rozwiązać.

Nową wersję ESET Internet Security można zainstalować automatycznie na podstawie ustawień aktualizacji programu lub ręcznie, pobierając i instalując nowszą wersję już zainstalowanego programu.

Kliknij przycisk **Uruchom ponownie teraz**, aby ponownie uruchomić komputer. Jeśli planujesz ponowne uruchomienie komputera w późniejszym czasie, kliknij przycisk **Przypomnij mi później**. Później możesz ponownie uruchomić komputer ręcznie z sekcji **Strona główna** w głównym oknie programu.

Narzędzia

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



Inspekcja sieci — obniżenie ryzyka wystąpienia problemów z zabezpieczeniami podczas korzystania z sieci. Aby uzyskać więcej informacji, zobacz Inspekcja sieci.

Ochrona bankowości internetowej — program ESET Internet Security chroni numery kart kredytowych i inne poufne dane osobowe podczas korzystania z bankowości elektronicznej oraz stron do dokonywania płatności program. Zostanie uruchomiona zabezpieczona przeglądarka, aby zapewnić bezpieczniejsze środowisko dla transakcji bankowych.

Anti-Theft — lokalizuje utracone urządzenie (zgubione lub skradzione) i ułatwia jego odnalezienie.

W celu wyświetlenia innych narzędzi do ochrony komputera (np. Kwarantanna) należy kliknąć pozycję Więcej narzędzi.

Inspekcja sieci

Inspekcja sieci ułatwia wykrywanie luk w zabezpieczeniach sieci zaufanej (sieci domowej lub biurowej), na przykład otwarte porty lub słabe hasła routera. Ta funkcja oferuje również łatwo dostępną listę połączonych urządzeń, na której są one uszeregowane według typów (np. drukarka, router, urządzenie mobilne), dzięki czemu można sprawdzić urządzenia połączone z siecią domową (np. konsola do gier, urządzenia IoT lub inne urządzenia do obsługi domu inteligentnego).

Inspekcja sieci pomaga rozpoznać luki w zabezpieczeniach routera i podnosi poziom ochrony po podłączeniu do sieci.

Inspekcja sieci nie zmienia konfiguracji routera za użytkownika. Zmiany należy wprowadzić samodzielnie w służącym do tego interfejsie routera. Routery domowe mogą być bardzo podatne na działanie szkodliwego oprogramowania używanego do przeprowadzania ataków typu „rozproszona odmowa usługi” (DDoS). Jeśli domyślne hasło nie zostało zmienione, hakerzy mogą je łatwo odgadnąć, a następnie zalogować się do routera i zmienić jego konfigurację lub zaatakować sieć.

Zdecydowanie zalecamy utworzenie silnego i długiego hasła, które zawiera cyfry, symbole i duże litery. Aby hasło było trudniejsze do złamania, użyj różnych typów znaków.

Jeśli sieć, z którą się łączysz, jest skonfigurowana jako zaufana, możesz oznaczyć ją jako „Moja sieć”. Kliknij **Oznacz jako „Moja sieć”**, aby dodać do sieci tag Moja sieć. Ten tag będzie wyświetlany obok sieci w całym produkcie ESET Internet Security, umożliwiając lepszą identyfikację i przegląd zabezpieczeń. Kliknij **Usuń oznaczenie jako „Moja sieć”**, aby usunąć tag.

Każde urządzenie podłączone do sieci jest wyświetlane w widoku listy z podstawowymi informacjami. Kliknij określone urządzenie, aby je edytować lub wyświetlić szczegółowe informacje o urządzeniu.

Przy użyciu menu rozwijanego **Sieci** w widoku sieci można filtrować urządzenia na podstawie następujących kryteriów:

- Urządzenia podłączone do określonej sieci
- Urządzenia połączone ze **wszystkimi sieciami**
- Urządzenia bez kategorii

Aby wyświetlić wszystkie połączone z siecią urządzenia w widoku sonara, kliknij ikonę sonara . W celu wyświetlenia podstawowych informacji o urządzeniu, takich jak nazwa sieci oraz data ostatniego połączenia, należy przesunąć wskaźnik na jego ikonę.

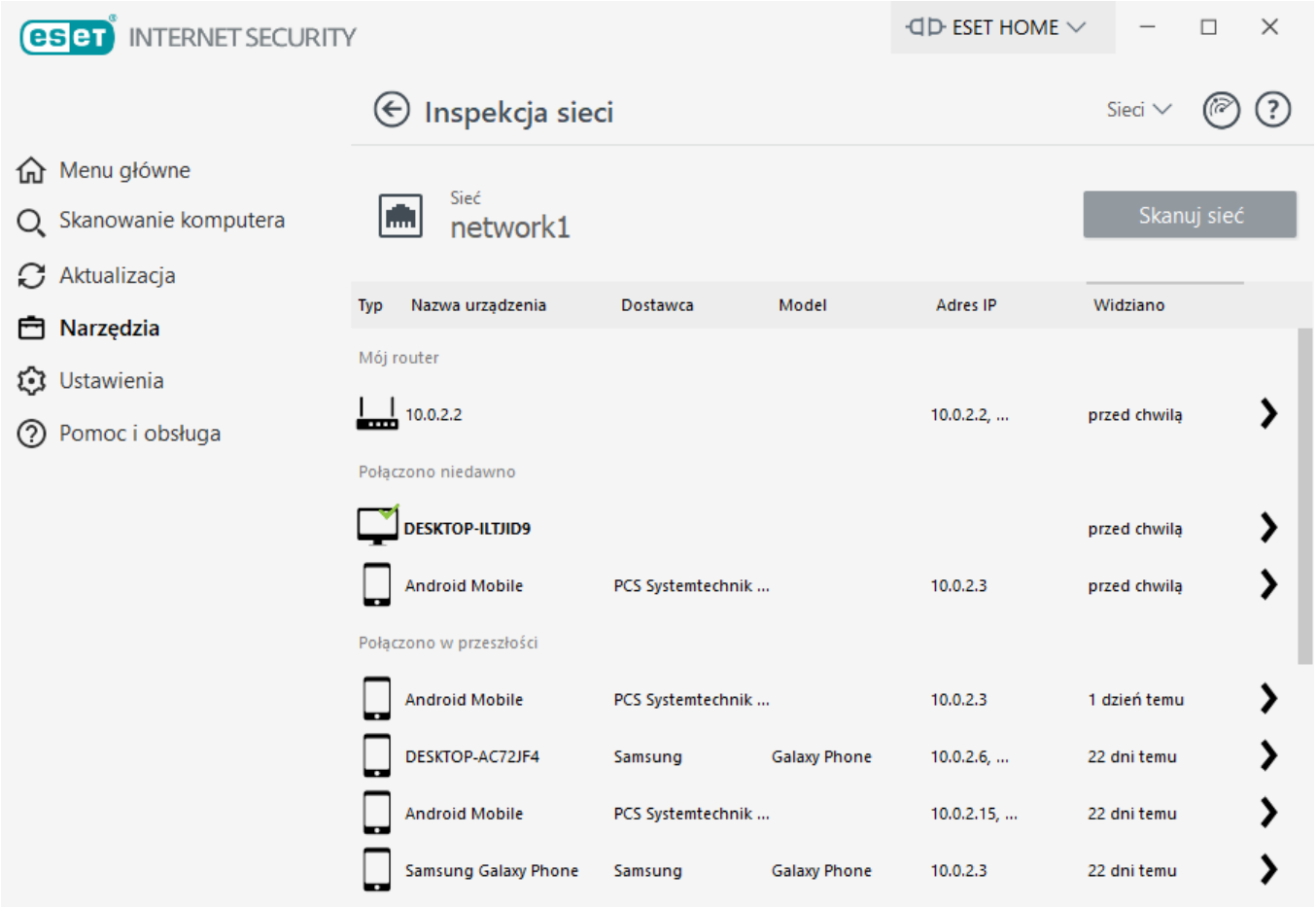
Kliknięcie tej ikony umożliwia edytowanie urządzenia lub wyświetlenie szczegółowych informacji o urządzeniu. Ostatnio podłączone urządzenia są wyświetlane bliżej routera, aby można było je łatwiej zauważyć.

Kliknij opcję **Skanuj sieć**, aby ręcznie wykonać skanowanie sieci, z którą masz nawiązane połączenie. Opcja **Skanuj sieci** jest dostępne tylko dla sieci zaufanej. Zobacz Znane sieci, aby przejrzeć lub edytować ustawienia sieci.

Dostępne są następujące opcje skanowania:

- Skanuj wszystko
- Skanuj tylko router
- Skanuj tylko urządzenia

Skanowanie sieci należy wykonywać wyłącznie w sieci zaufanej! Przeprowadzanie skanowania w sieciach niezaufanych może wiązać się z potencjalnymi zagrożeniami.



Po ukończeniu skanowania zostanie wyświetlone powiadomienie z łączem do podstawowych informacji o urządzeniu. Będzie też można dwukrotnie kliknąć podejrzane urządzenie w widoku listy lub sonara. Kliknij pozycję **Rozwiąż problem**, aby wyświetlić ostatnio zablokowaną komunikację. Więcej informacji o rozwiązywaniu problemów z zaporą.

Moduł Inspekcji sieci wyświetla dwa rodzaje powiadomień:

- **Nowe urządzenie połączone z siecią** — powiadomienie to jest wyświetlane, jeśli nieznane dotąd urządzenie połączy się z siecią, gdy połączony jest użytkownik.

- **Znaleziono nowe urządzenia sieciowe** — powiadomienie to jest wyświetlane, jeśli użytkownik ponownie nawiąże połączenie z siecią zaufaną, w której jest obecne nieznane wcześniej urządzenie.

Oba rodzaje powiadomień informują o tym, że nieautoryzowane urządzenie próbuje nawiązać połączenie z siecią domową. Kliknij **wyświetl urządzenie**, aby wyświetlić szczegóły.

Co oznaczają ikony na urządzeniach w oknie Inspekcja sieci?

	Żółta ikona gwiazdki wskazuje urządzenia, które są nowe w sieci lub wykryte przez system ESET po raz pierwszy.
	Żółta ikona ostrzeżenia wskazuje, że mogą występować luki w zabezpieczeniach routera. Kliknij ikonę w produkcie, aby uzyskać bardziej szczegółowe informacje na temat problemu.
	Czerwona ikona ostrzeżenia wskazuje, że występują luki w zabezpieczeniach routera i może on być zainfekowany. Kliknij ikonę w produkcie, aby uzyskać bardziej szczegółowe informacje na temat problemu.



Niebieska ikona wskazuje, że produkt ESET ma dodatkowe informacje na temat routera, ale sytuacja nie wymaga natychmiastowej uwagi, ponieważ nie ma zagrożeń bezpieczeństwa. Kliknij ikonę w produkcie, aby uzyskać bardziej szczegółowe informacje.

Urządzenie sieciowe w Inspekcji sieci

W tym obszarze można znaleźć szczegółowe informacje na urządzenia, m.in. następujące:

- Nazwa urządzenia
- Typ urządzenia
- Ostatnio widziano
- Nazwa sieci
- Adres IP
- Adres MAC
- System operacyjny

Ikona ołówka wskazuje, że można zmodyfikować nazwę lub typ.

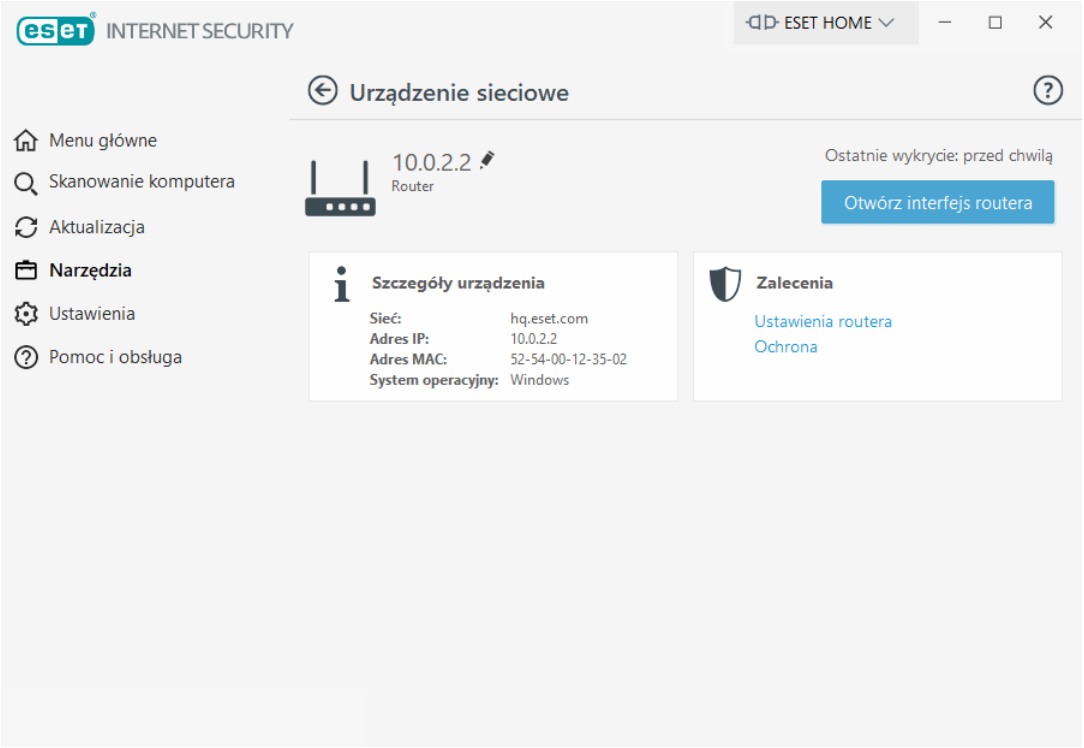
Usuń z historii — usuń urządzenie z listy urządzeń. Ta opcja jest dostępna tylko dla urządzeń, które nie są obecnie podłączone do sieci.

W przypadku każdego typu urządzenia dostępne są następujące czynności:

Router

Ustawienia routera — dostęp do ustawień routera można uzyskać przez interfejs sieciowy, aplikację mobilną lub klikając opcję **Otwórz interfejs routera**. Jeśli masz router zapewniony przez dostawcę usług internetowych, w celu rozwiązania wykrytych problemów związanych z bezpieczeństwem konieczny może być kontakt z działem pomocy technicznej dostawcy usług internetowych lub producentem routera. Zawsze przestrzegaj zasad dotyczących bezpieczeństwa opisanych w podręczniku użytkownika routera.

Ochrona – Aby chronić router i sieć przed cyberatakami, postępuj zgodnie z następującymi podstawowymi zaleceniami.

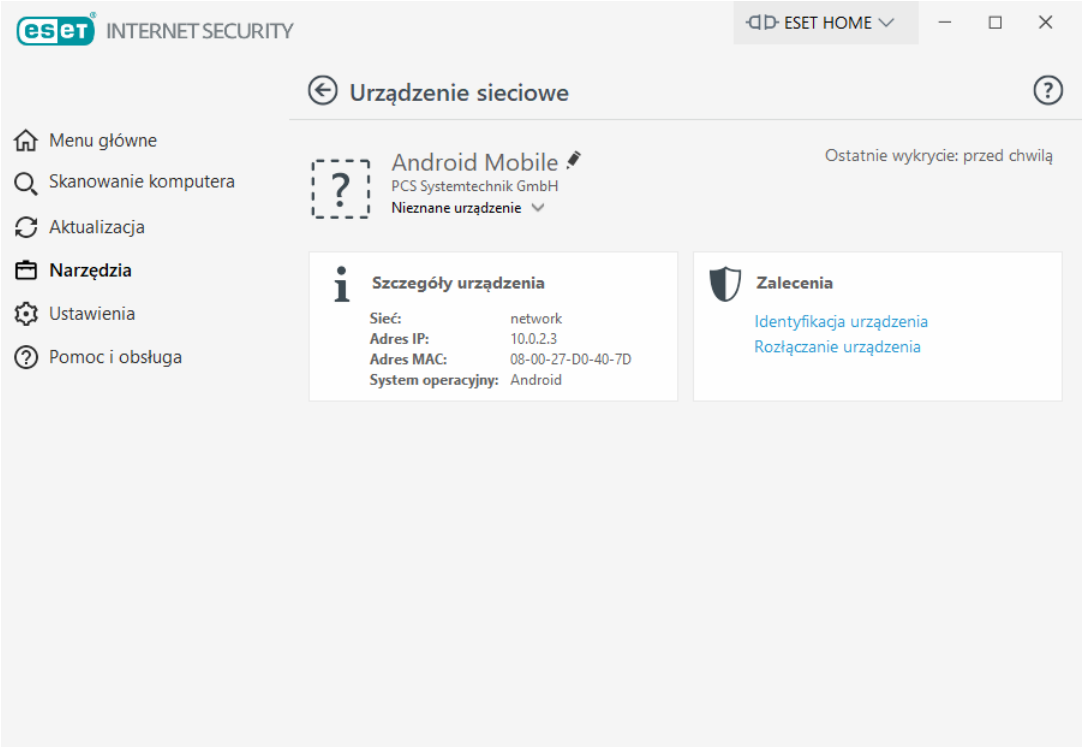


Urządzenie sieciowe

Identyfikacja urządzenia — jeśli nie masz pewności co do danego urządzenia połączonego z siecią, sprawdź nazwę sprzedawcy lub producenta widoczną pod nazwą urządzenia. Pomoże ona rozpoznać rodzaj urządzenia. Możesz zmienić nazwę urządzenia, aby ułatwić jego identyfikację w przyszłości.

Rozłączanie urządzenia — jeśli nie masz pewności, czy połączone urządzenie jest bezpieczne dla Twojej sieci lub Twoich urządzeń, zablokuj dostęp urządzenia do sieci z poziomu ustawień routera lub zmień hasło do sieci.

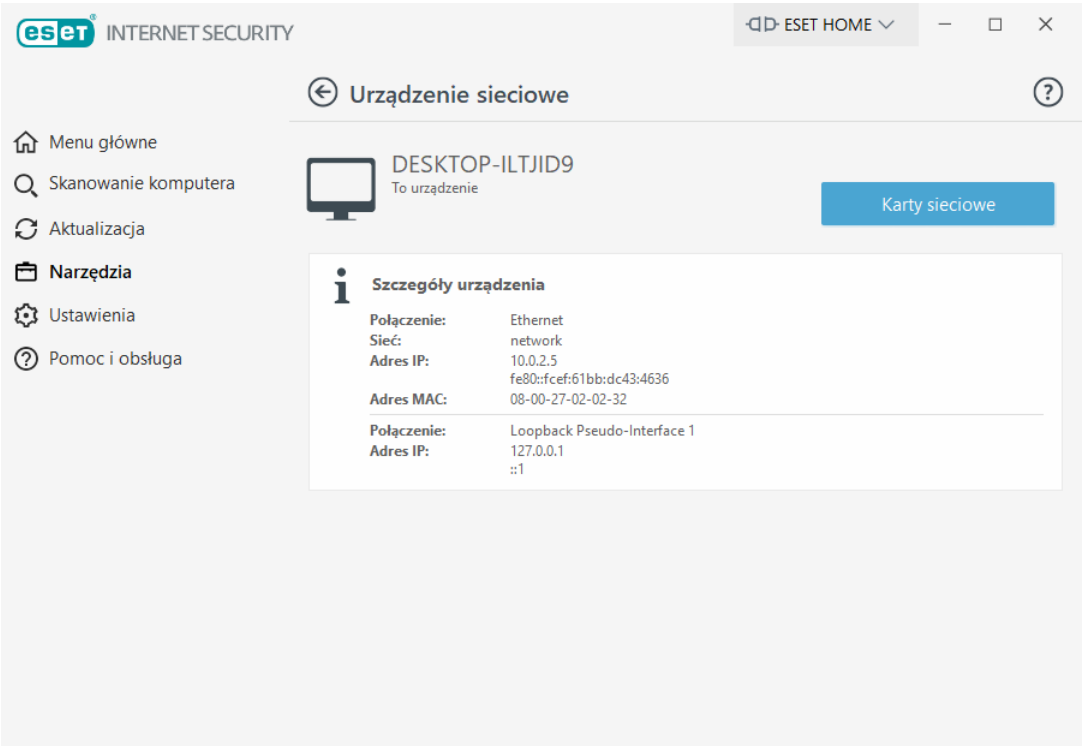
Ochrona — aby chronić urządzenie przed atakami i szkodliwym oprogramowaniem, zainstaluj na urządzeniu rozwiązanie zabezpieczające przed cyberatakami i dbaj o to, żeby system operacyjny i zainstalowane oprogramowanie zawsze były aktualne. Aby zachować ochronę, nie łącz się z niezabezpieczonymi sieciami Wi-Fi.



To urządzenie

To urządzenie reprezentuje Twój komputer w sieci.

Karty sieciowe — tu widoczne są informacje o kartach sieciowych.



Powiadomienia | Inspekcja sieci

Poniżej znajduje się kilka powiadomień, które mogą zostać wyświetlone, gdy program ESET Internet Security wykryje problem dotyczący luki w zabezpieczeniach routera. Każde powiadomienie zawiera krótki opis i zapewnia rozwiązanie lub kroki do wykonania w celu zminimalizowania ryzyka dotyczącego luki w zabezpieczeniach routera. Jeśli nie czujesz się komfortowo przy wprowadzaniu zmian w routerze, zalecamy skontaktowanie się z producentem routera albo dostawcą usług internetowych.

Wykryto potencjalną lukę w zabezpieczeniach
W routerze mogą występować znane luki w zabezpieczeniach, które mogą ułatwić przeprowadzenie ataku i mogą zostać wykorzystane. Zaktualizuj oprogramowanie układowe routera.

Wykryto lukę w zabezpieczeniach
W routerze występują znane luki w zabezpieczeniach, które ułatwiają przeprowadzanie ataków i mogą zostać wykorzystane. Zaktualizuj oprogramowanie układowe routera.

Znaleziono zagrożenie.
Router jest zainfekowany szkodliwym oprogramowaniem. Uruchom router ponownie i powtórz skanowanie.

Słabe hasło do routera
Hasło do routera jest słabe i ktoś może je z łatwością odgadnąć. Zmień hasło w routerze.

Szkodliwe przekierowanie w sieci
Ruch internetowy jest przekierowywany do szkodliwych stron internetowych. Może to oznaczać, że router został zaatakowany. Zmień ustawienie serwera DNS w routerze.

Otwarte usługi sieciowe
Na routerze są uruchomione usługi sieciowe, które mogą zostać wykorzystane przez inne osoby. Może być ze względu na nieprawidłową konfigurację lub zaatakowany router. Sprawdź konfigurację routera.

Otwarte usługi sieciowe o charakterze poufnym
Na routerze są uruchomione usługi sieciowe o charakterze poufnym, które mogą zostać wykorzystane przez inne osoby. Może być ze względu na nieprawidłową konfigurację lub zaatakowany router. Sprawdź konfigurację routera.

Nieaktualne oprogramowanie układowe
Oprogramowanie układowe w routerze jest nieaktualne i może zawierać luki w zabezpieczeniach. Zaktualizuj oprogramowanie układowe routera.

Szkodliwe ustawienie routera
Używany serwer DNS ma szkodliwy charakter i może przekierowywać użytkowników do niebezpiecznych stron internetowych. Może to oznaczać, że router został zaatakowany. Zmień ustawienie serwera DNS w routerze.

Usługi sieciowe
Na routerze są uruchomione powszechnie używane usługi sieciowe. Są one wymagane w sieci i prawdopodobnie bezpieczne. Sprawdź konfigurację routera.

Narzędzia w programie ESET Internet Security

Menu **Narzędzia** zawiera moduły, które upraszczają administrowanie programem i udostępniają dodatkowe opcje dla użytkowników zaawansowanych. Narzędzia te są widoczne dopiero po kliknięciu pozycji **Więcej narzędzi** w prawym dolnym rogu.

To menu zawiera następujące narzędzia:

Pliki dziennika

Raport zabezpieczeń

Uruchomione procesy (jeśli usługa ESET LiveGrid® jest włączona w programie ESET Internet Security)

Połączenia sieciowe (jeśli zapora jest włączona w programie ESET Internet Security)

ESET SysInspector

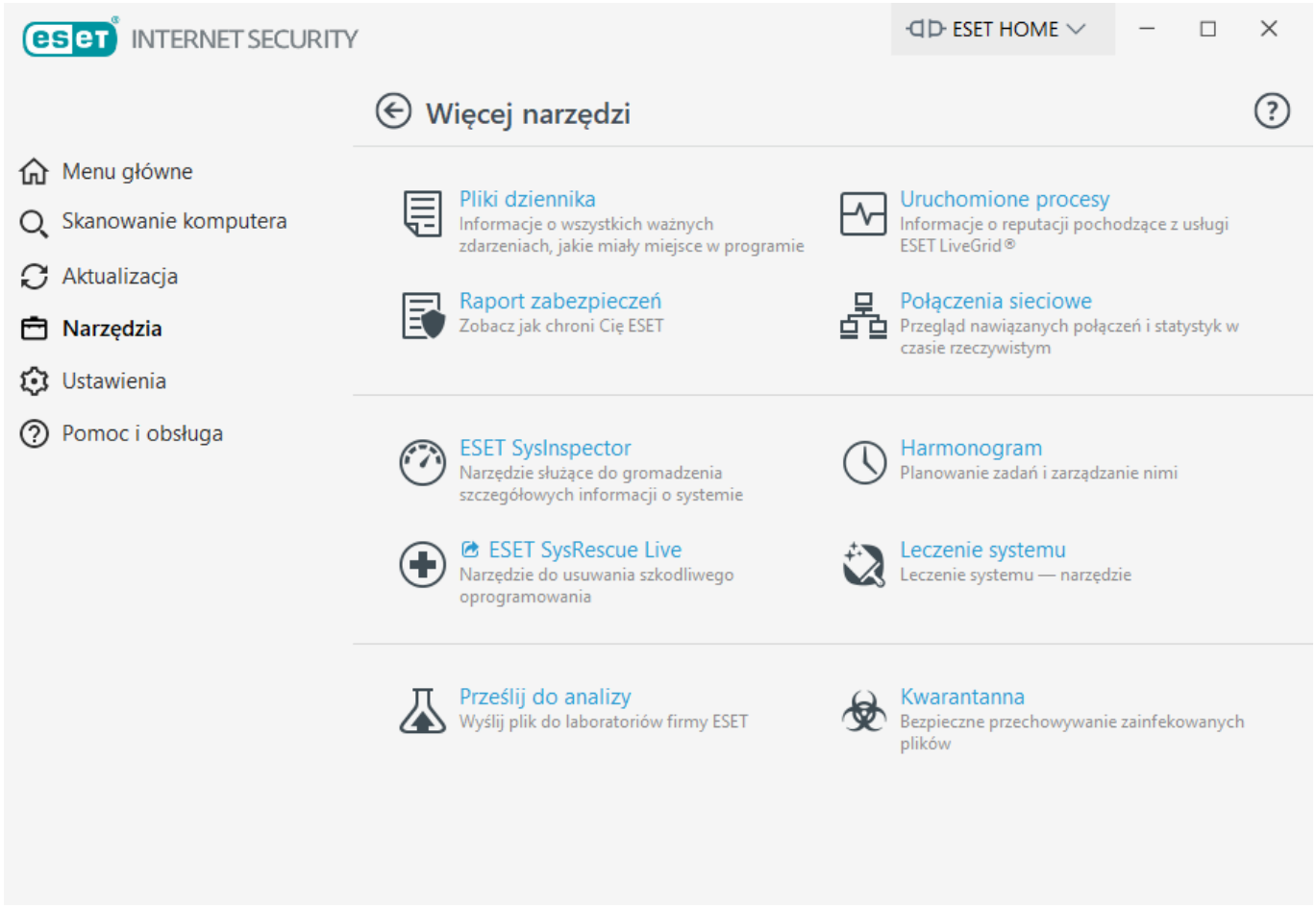
ESET SysRescue Live — kliknięcie tej pozycji powoduje przekierowanie do witryny narzędzia ESET SysRescue Live, skąd można pobrać obraz .iso dysku CD/DVD narzędzia ESET SysRescue Live.

Harmonogram

Leczenie systemu — narzędzie ułatwiające przywracanie komputera do użytecznego stanu po jego wyleczeniu z zagrożenia.

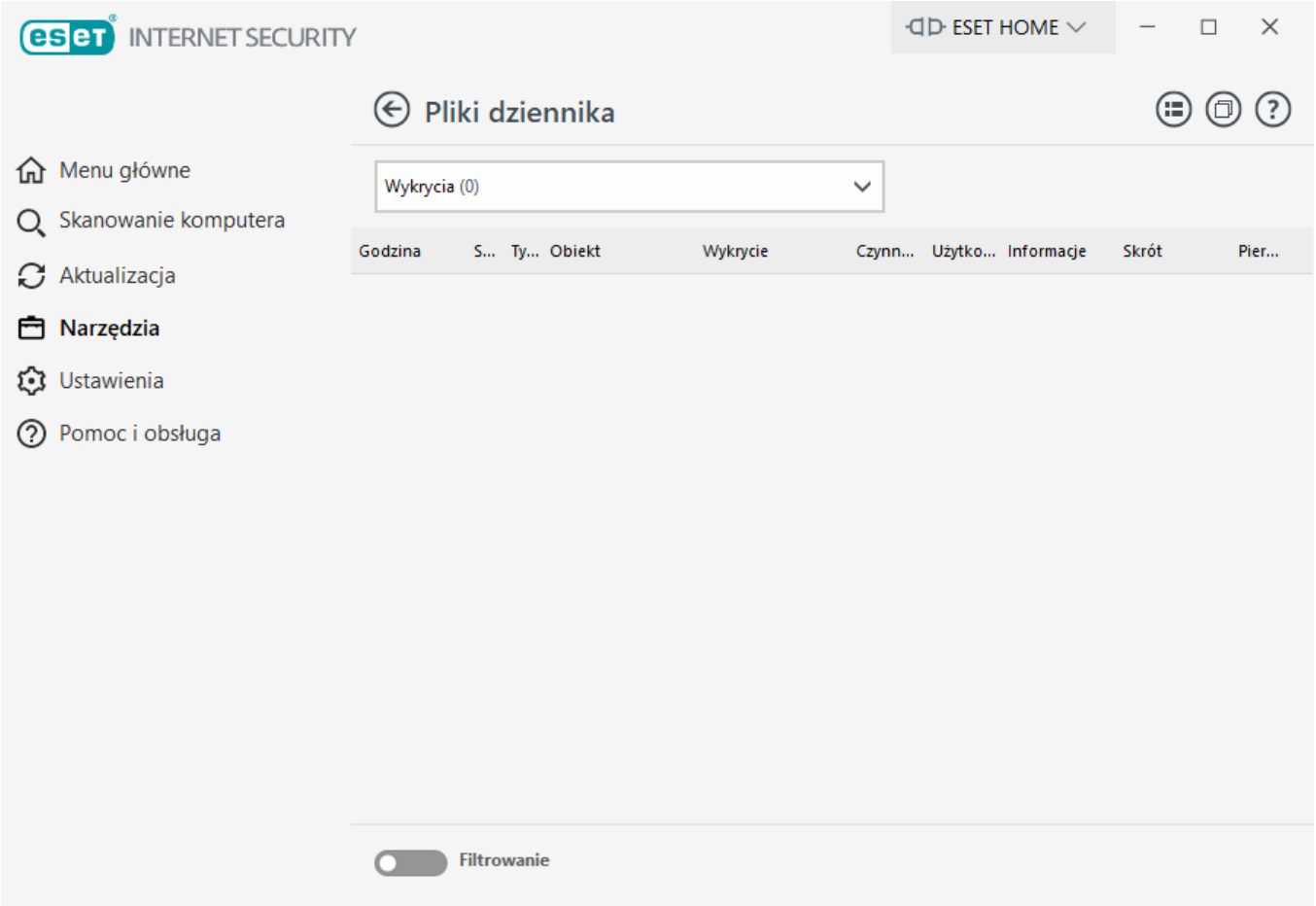
Prześlij do analizy — umożliwia przesłanie podejrzanego pliku do analizy w laboratorium firmy ESET (dostępność tej opcji zależy od konfiguracji rozwiązania ESET LiveGrid®).

Kwarantanna



Pliki dziennika

Pliki dziennika zawierają informacje o wszystkich ważnych zdarzeniach, jakie miały miejsce, oraz przegląd wykrytych zagrożeń. Informacje zapisywane w dzienniku są bardzo ważne i przydatne podczas analizy systemu, wykrywania zagrożeń i rozwiązywania 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 Internet Security można bezpośrednio wyświetlać wiadomości tekstowe oraz wyświetlać i archiwizować dzienniki.



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

- **Wykrycia** — ten dziennik zawiera szczegółowe informacje na temat zagrożeń i infekcji wykrytych przez program ESET Internet Security. Zawiera on między innymi: datę i godzinę wykrycia, typ skanera, tym obiektu, lokalizację obiektu, nazwę wykrytego obiektu, podjęte działanie, nazwę użytkownika zalogowanego w czasie wykrycia infekcji, skrót oraz pierwsze wystąpienie. Nieusunięte infekcje są zawsze oznaczone czerwonym tekstem na jasnoczerwonym tle. Usunięte infekcje są oznaczone żółtym tekstem na białym tle. Nieoczyszczone i potencjalnie niebezpieczne lub niepożądane aplikacje są oznaczone żółtym tekstem na białym tle.

- **Zdarzenia** — wszystkie ważne działania wykonywane przez program ESET Internet Security są zapisywane w dzienniku zdarzeń. Dziennik zdarzeń zawiera informacje na temat zdarzeń i błędów, które wystąpiły w programie. Jest przeznaczony do 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 są wyświetlane wyniki wszystkich ukończonych operacji 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 systemu HIPS, które zostały zaznaczone do rejestrowania. Pozycje dziennika zawierają informacje o aplikacji, która wywołała operację, wyniku (zezwolenie lub zablokowanie reguły) oraz nazwie reguły.

• **Ochrona sieci** — dziennik ochrony sieci wyświetla wszystkie ataki zdalne wykryte przez zaporę, ochronę przed atakami z sieci (IDS) oraz Botnet. W tym miejscu znajdziesz informacje na temat wszystkich ataków na Twój komputer. Kolumna Zdarzenia wyświetla listę wszystkich wykrytych ataków. Kolumna Źródła zawiera dodatkowe informacje na temat źródła ataku. Kolumna Protokół zawiera informacje na temat protokołu komunikacyjnego użytego do przeprowadzenia ataku. Analiza dziennika ochrony sieci może pomóc w wykryciu prób infiltracji systemu w odpowiednim czasie, zapobiegając nieautoryzowanemu dostępowi do systemu. W celu uzyskania dodatkowych informacji zobacz IDS i ustawienia zaawansowane.

• **Filtrowane witryny internetowe** — ta lista jest przydatna do przeglądania listy witryn zablokowanych przez funkcje Ochrona dostępu do stron internetowych lub Kontrola rodzicielska. 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 rodzicielska** — umożliwia wyświetlenie stron internetowych zablokowanych i dozwolonych przez funkcję Kontrola rodzicielska. Kolumny Typ dopasowania i Wartości dopasowania informują, w jaki sposób 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. 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).

• **Ochrona kamery internetowej** — zawiera zapisy dotyczące aplikacji blokowanych przez funkcję Ochrona kamery internetowej.

Zaznacz treść dziennika i naciśnij klawisze **CTRL + C**, aby skopiować ją do schowka. W celu zaznaczenia większej liczby wpisów należy przytrzymać klawisz **CTRL** lub **SHIFT**.

Kliknij symbol **Filtrowanie** powoduje otwarcie okna Filtrowanie dziennika, w którym można zdefiniować kryteria filtrowania.

Kliknięcie rekordu prawym przyciskiem myszy umożliwia otwarcie 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** — po kliknięciu tej opcji w oknie Filtrowanie dziennika można zdefiniować kryteria filtrowania określonych wpisów w dzienniku.

• **Włącz filtr** — umożliwia aktywację ustawień filtra.

• **Wyłącz filtr** — umożliwia wyczyszczenie wszystkich ustawień filtrowania (opisanych powyżej).

• **Kopiuj/Kopiuj wszystko** — kopiuje informacje o wybranych rekordach w oknie.

• **Usuń/Usuń wszystko** — umożliwia usunięcie wybranych rekordów albo wszystkich wyświetlanych rekordów. Konieczne jest posiadanie uprawnień administratora.

• **Eksportuj/Eksportuj wszystko** — eksportuje informacje o wybranych lub wszystkich rekordach w formacie XML.

• **Znajdź/Znajdź następny/Znajdź poprzedni** — po kliknięciu tej opcji można zdefiniować kryteria filtrowania, aby wyróżnić określony wpis za pomocą okna filtrowania dziennika.

• **Opis wykrycia** — otwiera Encyklopedię zagrożeń firmy ESET, która zawiera szczegółowe informacje o zagrożeniach i objawach zarejestrowanej infiltracji.

• **Utwórz wyłączenie** — umożliwia utworzenie zaawansowanej konfiguracji wyłączeń przy użyciu kreatora (opcja niedostępna w przypadku wykryć dotyczących szkodliwego oprogramowania).

Filtrowanie dziennika

Kliknij **Filtrowanie** w obszarze **Narzędzia** > **Więcej narzędzi** > **Pliki dziennika** w celu zdefiniowania kryteriów filtrowania.

Funkcja filtrowania dziennika ułatwia znajdowanie szukanych informacji, szczególnie w przypadku istnienia wielu rekordów. Umożliwia ona zawężenie zakresu rekordów dziennika, na przykład podczas wyszukiwania konkretnego typu zdarzenia, stanu lub przedziału czasu. Rekordy dziennika można filtrować, określając pewne opcje wyszukiwania. W oknie Pliki dziennika pojawią się tylko rekordy spełniające kryteria zdefiniowane w opcjach.

W polu **Znajdź tekst** należy wpisać szukane słowo kluczowe. Menu rozwijane **Wyszukaj w kolumnach** pozwala doprecyzować wyszukiwanie. W menu rozwijanym **Typy rekordów dziennika** należy wybrać co najmniej jeden rekord. W polu **Okres** można wybrać przedział czasu, z którego mają zostać wyświetlone wyniki. Dostępne są też dodatkowe opcje wyszukiwania, takie jak **Tylko całe wyrazy** czy **Uwzględniaj wielkość liter**.

Znajdź tekst

W tym polu należy wpisać ciąg (wyraz lub część wyrazu). W wynikach zostaną pokazane tylko rekordy zawierające ten ciąg. Pozostałe rekordy zostaną pominięte.

Wyszukaj w kolumnach

W tym polu należy wybrać kolumny, które zostaną uwzględnione w wyszukiwaniu. Można wybrać jedną lub więcej kolumn.

Typy rekordów

W tym polu należy wybrać co najmniej jeden typ rekordów dziennika z menu rozwijanego:

• **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszania 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

Przedział czasu

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

• **Nieokreślony** (domyślnie) — przeszukiwanie całego dziennika, bez ograniczenia do konkretnego przedziału czasu.

• **Ostatni dzień**

• **Ostatni tydzień**

• **Ostatni miesiąc**

• **Okres** — umożliwia określenie konkretnego przedziału czasu („Od” i „Do”) i uwzględnienie tylko rekordów zawartych w tym przedziale.

Tylko całe wyrazy

Zaznaczenie tego pola spowoduje wyszukiwanie całych wyrazów w celu zawężenia wyników.

Uwzględniaj wielkość liter

Tę opcję należy zaznaczyć, jeśli filtrowanie ma uwzględniać pisownię wielkimi i małymi literami. Po skonfigurowaniu opcji filtrowania/wyszukiwania należy kliknąć przycisk **OK**, aby wyświetlić odfiltrowane rekordy dziennika, lub przycisk **Znajdź**, aby rozpocząć wyszukiwanie. Pliki dziennika są przeszukiwane od góry do dołu, począwszy od bieżącej pozycji (czyli zaznaczonego rekordu). Wyszukiwanie trwa do momentu znalezienia pierwszego pasującego rekordu. Naciśnięcie klawisza **F3** spowoduje wyszukanie następnego rekordu, a kliknięcie prawym przyciskiem myszy i wybranie polecenia **Znajdź** pozwoli doprecyzować opcje wyszukiwania.

Konfiguracja dzienników

Dostęp do konfiguracji dzienników programu ESET Internet Security można uzyskać z poziomu jego okna głównego. Należy kliknąć kolejno **Ustawienia** > **Ustawienia zaawansowane** > **Narzędzia** > **Pliki dziennika**. W sekcji dzienników można określić sposób zarządzania dziennikami. W celu oszczędzania miejsca na dysku twardym program automatycznie usuwa starsze dzienniki. Można określić następujące opcje plików dziennika:

Minimalna szczegółowość zapisów w dzienniku — umożliwia określenie minimalnego poziomu szczegółowości zdarzeń rejestrowanych w dzienniku.

• **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszania 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. błędu uruchomienia ochrony antywirusowej, zaporyitp.).

Wszystkie blokowane połączenia są rejestrowane, gdy wybrany jest poziom szczegółowości Diagnostyka.

Wpisy dziennika starsze niż liczba dni podana w polu **Automatycznie usuwaj rekordy starsze niż (dni)** będą usuwane automatycznie.

Automatycznie optymalizuj pliki dzienników — zaznaczenie tej opcji powoduje automatyczną defragmentację plików dziennika po przekroczeniu stopnia fragmentacji określonego w polu **Jeśli liczba nieużywanych rekordów przekracza (%)**.

Kliknij przycisk **Optymalizuj**, aby rozpocząć defragmentację plików dziennika. Wszystkie puste wpisy dzienników są usuwane, co wpływa na wzrost wydajności i szybkości przetwarzania dziennika. Poprawę można zaobserwować zwłaszcza w przypadku dzienników zawierających dużą liczbę wpisów.

Opcja **Włącz protokół tekstowy** umożliwia zapisywanie dzienników w plikach innego formatu osobno od plików dziennika:

• **Katalog docelowy** — katalog, w którym będą zapisywane pliki dzienników (dotyczy wyłącznie plików tekstowych/CSV). Każdej sekcji dziennika odpowiada osobny plik o wstępnie zdefiniowanej nazwie (np. virlog.txt to plik odpowiadający sekcji plików dziennika **Wykrycia**, jeśli wybrany format zapisu dzienników to zwykły tekst).

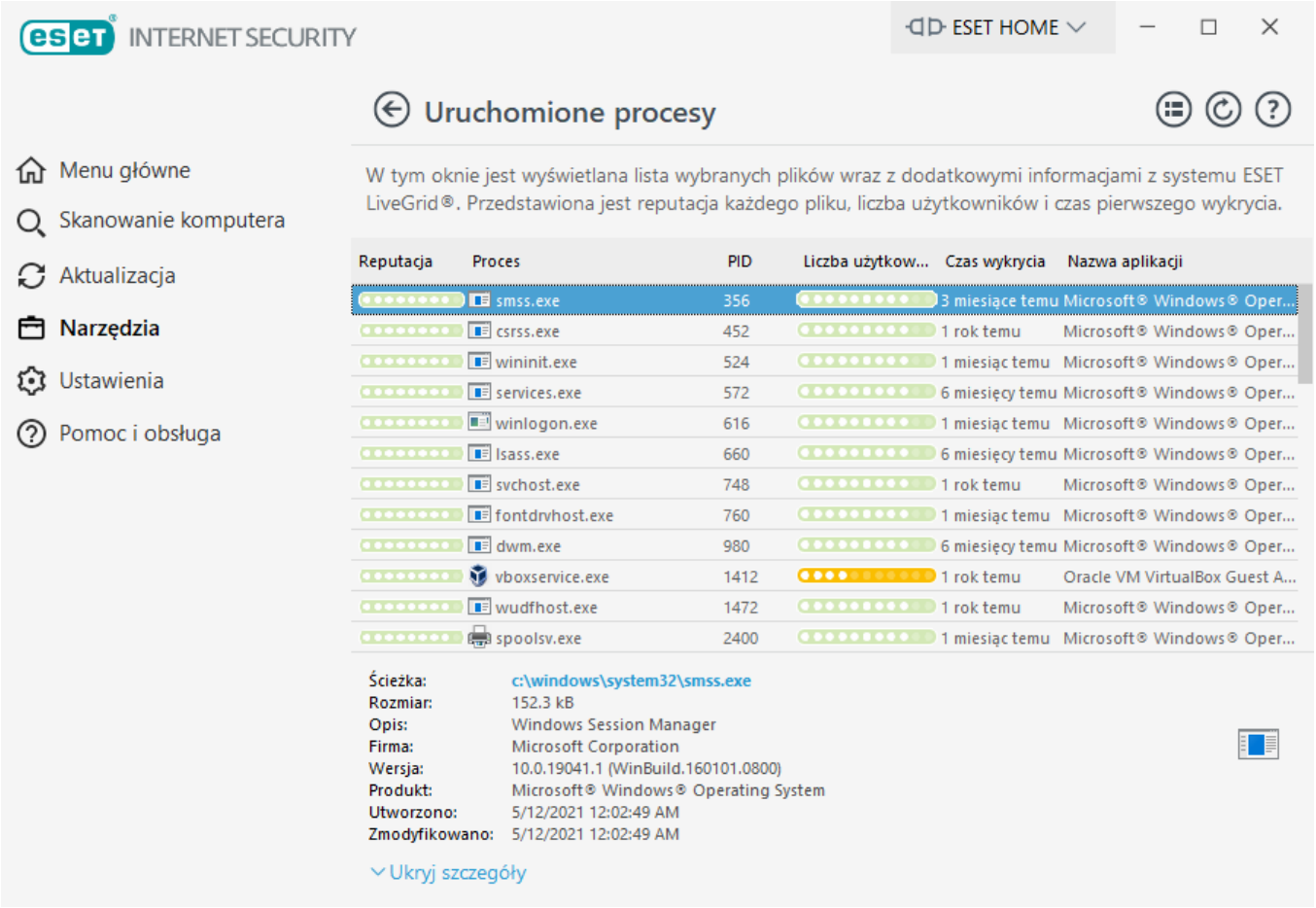
• **Typ** — po wybraniu formatu pliku **Tekst** dzienniki będą zapisywane w postaci pliku tekstowego, a dane będą rozdzielane tabulatorami. Dotyczy to też formatu pliku **CSV** — wartości rozdzielanych przecinkami. W przypadku wybrania opcji **Zdarzenie** zamiast w pliku dzienniki będą zapisywane w dzienniku zdarzeń systemu Windows (można go wyświetlić w obszarze Podgląd zdarzeń w Panelu sterowania).

• **Usuń wszystkie pliki dzienników** — powoduje usunięcie wszystkich zapisanych dzienników aktualnie wybranych w menu rozwijanym **Typ**. Po pomyślnym usunięciu dzienników wyświetlane jest powiadomienie.

Aby szybciej rozwiązać problemy firma ESET może czasem prosić użytkowników o przekazanie dzienników zapisanych na ich komputerach. Narzędzie ESET Log Collector ułatwia użytkownikom gromadzenie niezbędnych informacji. Więcej informacji na temat narzędzia ESET Log Collector można znaleźć w artykule bazy wiedzy ESET.

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 Internet Security dostarcza szczegółowych informacji o uruchomionych procesach i chroni użytkowników dzięki zastosowaniu technologii ESET LiveGrid®.



Reputacja — w większości przypadków ESET Internet Security i technologia ESET LiveGrid® przypisują obiektom (plikom, procesom, kluczom rejestru itd.) poziomy ryzyka, używając do tego wielu reguł heurystyki. W wyniku pozyskanej heurystycznie wiedzy obiektom przypisywany jest poziom 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.

Znane aplikacje oznaczone jako Czyste (kolor zielony) na pewno nie są zainfekowane (są na białej liście) i zostaną wyłączone ze skanowania.

PID — numer identyfikacyjny procesu, który może być używany jako parametr w wywołaniach różnych funkcji, np. przy dostosowywaniu priorytetu procesu.

Liczba użytkowników — liczba użytkowników korzystających z danej aplikacji. Te informacje są zbierane przez technologię ESET LiveGrid®.

Czas wykrycia — okres od wykrycia aplikacji przez technologię ESET LiveGrid®.

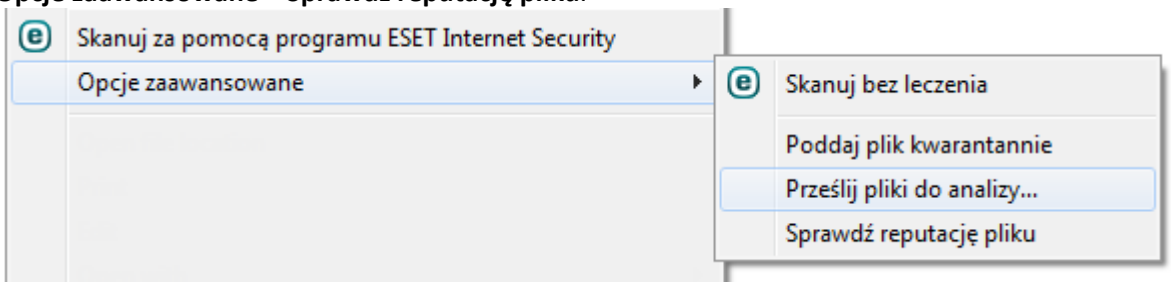
Aplikacja oznaczona jako Nieznana (kolor pomarańczowy)niekoniecznie jest szkodliwym oprogramowaniem. Zwykle jest to po prostu nowa aplikacja. W przypadku braku pewności co do bezpieczeństwa pliku można przesłać plik do analizy w laboratorium firmy ESET. Jeśli okaże się, że jest to szkodliwa aplikacja, możliwość jej wykrycia zostanie dodana do jednej z przyszłych aktualizacji.

Nazwa aplikacji — nazwa programu lub procesu.

Kliknięcie aplikacji umożliwia wyświetlenie następujących informacji szczegółowych na jej temat:

- **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 modyfikacji** — data i godzina utworzenia lub modyfikacji.

Można również sprawdzać reputację plików, które nie zachowują się jak uruchomione programy lub procesy. W tym celu kliknij plik prawym przyciskiem myszy w eksploratorze plików i wybierz kolejno pozycje **Opcje zaawansowane** > **Sprawdź reputację pliku**.



Raport zabezpieczeń

Funkcja ta umożliwia zapoznanie się z przeglądem statystyk w następujących kategoriach:

- **Zablokowane strony internetowe** — wyświetla liczbę zablokowanych stron internetowych (adresy URL dodane do czarnej listy ze względu na potencjalnie niepożądane aplikacje, ataki typu „phishing” albo złamane zabezpieczenia routera, adresu IP lub certyfikatu).
- **Wykryte zainfekowane obiekty poczty e-mail** — wyświetla wykrytą liczbę zainfekowanych obiektów poczty e-mail.
- **Zablokowane strony internetowe w ramach kontroli rodzicielskiej** — wyświetla liczbę stron internetowych zablokowanych w ramach kontroli rodzicielskiej.
- **Wykryte potencjalnie niepożądane aplikacje** — wyświetla liczbę potencjalnie niepożądanych aplikacji.
- **Wykryte wiadomości e-mail będące spamem** — wyświetla liczbę wykrytych wiadomości e-mail będących spamem.
- **Zablokowany dostęp do kamery internetowej** — wyświetla liczbę zablokowanych prób uzyskania dostępu do kamery internetowej.
- **Zastosowano ochronę dostępu do bankowości internetowej** — wyświetla liczbę zdarzeń bezpiecznego uzyskania dostępu do witryn internetowych za pomocą funkcji Ochrona bankowości internetowej.

- **Sprawdzone dokumenty** — wyświetla liczbę przeskanowanych dokumentów.
- **Przeskanowane aplikacje** — wyświetla liczbę przeskanowanych obiektów wykonywalnych.
- **Sprawdzone inne obiekty** — wyświetla liczbę innych przeskanowanych obiektów.
- **Przeskanowane obiekty stron internetowych** — wyświetla liczbę przeskanowanych obiektów stron internetowych.
- **Przeskanowane obiekty poczty e-mail** — wyświetla liczbę przeskanowanych obiektów poczty e-mail.

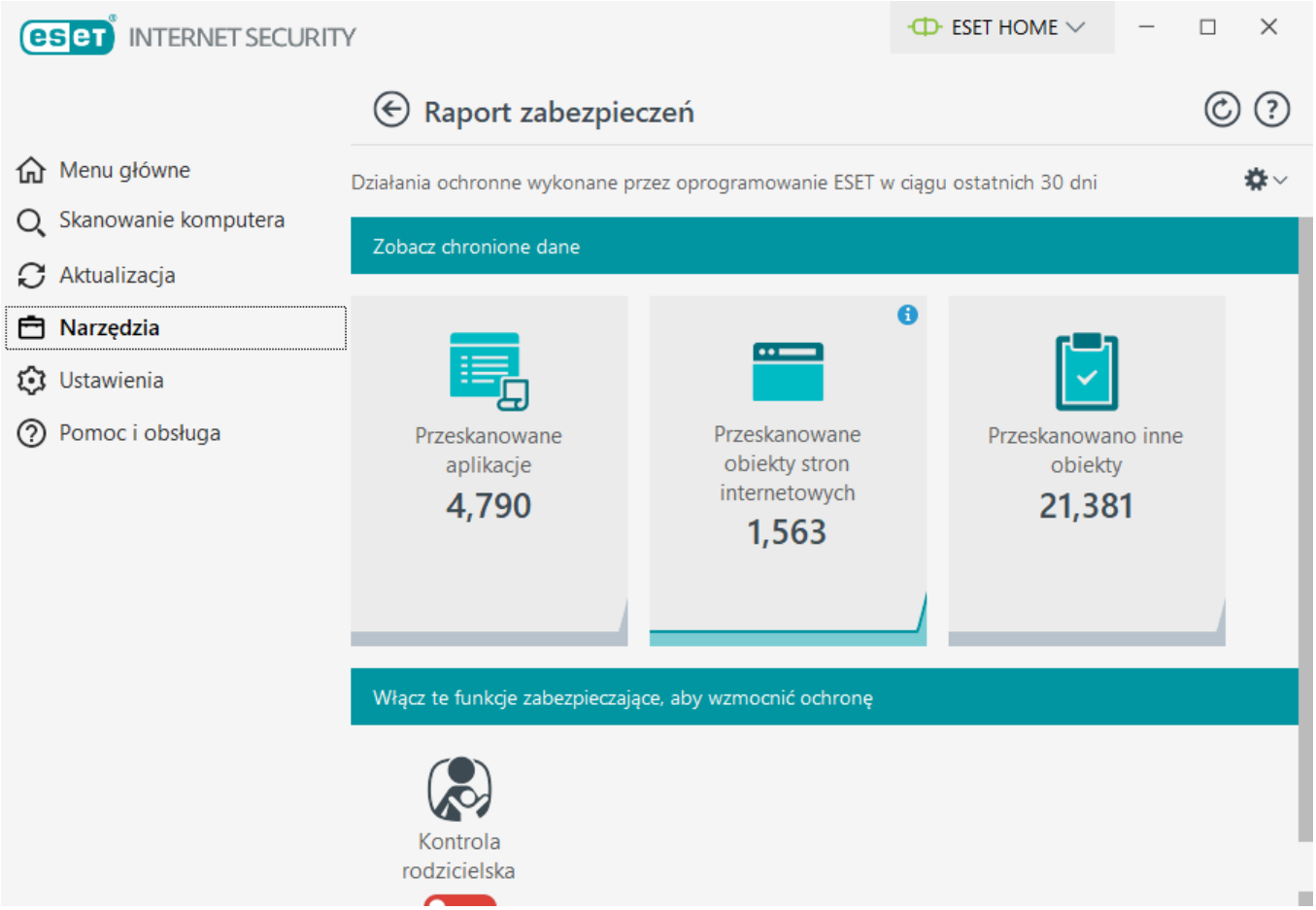
Kolejność powyższych kategorii zależy od powiązanych z nimi wartości liczbowych, przy czym na samej górze znajdują się wartości najwyższe. Kategorie, których wartość wynosi zero, nie są wyświetlane. Aby rozwinąć i wyświetlić ukryte kategorie, należy kliknąć przycisk **Pokaż więcej**.

Ostatnia część raportu zabezpieczeń umożliwia aktywowanie następujących funkcji:

- Kontrola rodzicielska
- Anti-Theft

Po włączeniu funkcji nie będzie ona wyświetlana jako niedziałająca w raporcie zabezpieczeń.

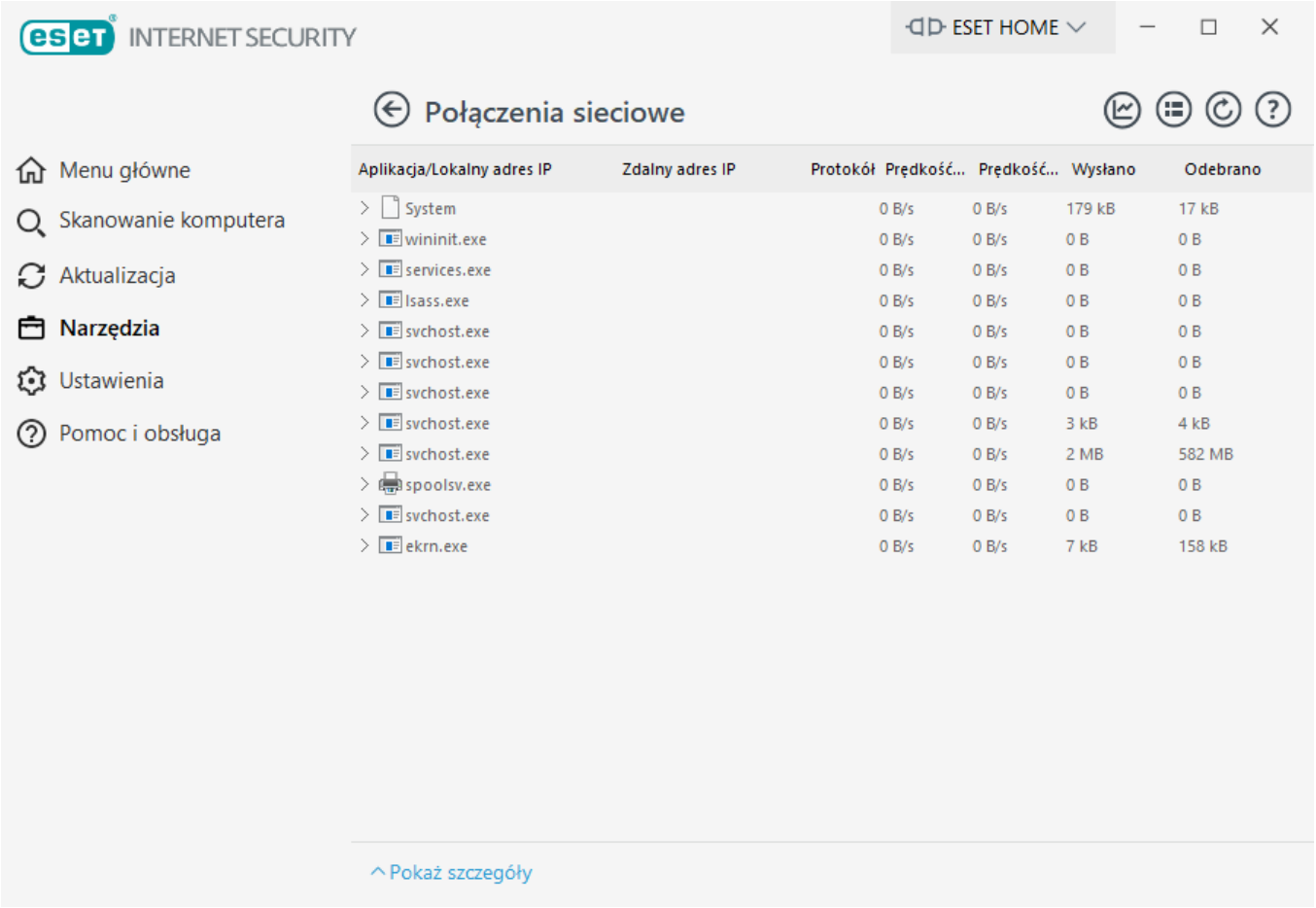
Kliknięcie symbolu koła zębatego znajdującego się w prawym górnym rogu pozwala **włączyć/wyłączyć powiadomienia o raportach zabezpieczeń** lub wybrać, czy wyświetlane dane powinny pochodzić z okresu ostatnich 30 dni, czy też od momentu aktywacji produktu. Jeśli produkt ESET Internet Security został zainstalowany maksymalnie 30 dni temu, wówczas można wybrać jedynie liczbę dni od momentu instalacji. Okres 30 dni jest ustawiony domyślnie.



Opcja **Resetuj dane** spowoduje wyczyszczenie wszystkich statystyk i usunięcie istniejących danych z raportu zabezpieczeń. Czynność ta musi zostać potwierdzona z wyjątkiem sytuacji, w której opcja **Pytaj przed resetowaniem statystyk** w obszarze **Ustawienia zaawansowane** > **Powiadomienia** > **Interaktywne alerty** > **Komunikaty wymagające potwierdzeń** > **Edytuj** nie jest zaznaczona.

Połączenia sieciowe

W sekcji Połączenia sieciowe wyświetlana jest lista aktywnych i oczekujących połączeń. Dzięki temu łatwiej jest kontrolować wszystkie aplikacje nawiązujące połączenia wychodzące.



Kliknij ikonę wykresu, aby otworzyć okno Aktywność sieciowa.

W pierwszym wierszu jest wyświetlana nazwa aplikacji i szybkość transmisji danych. Aby zobaczyć listę połączeń nawiązanych przez aplikację (i inne szczegółowe informacje), należy kliknąć **>**.

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.

Kliknięcie połączenia prawym przyciskiem myszy powoduje wyświetlenie dodatkowych opcji:

Rozpoznaj 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 localhost.

Szybkość odświeżania — wybierz częstotliwość odświeżania aktywnych połączeń.

Odśwież teraz — powoduje zaktualizowanie okna **Połączenia sieciowe**.

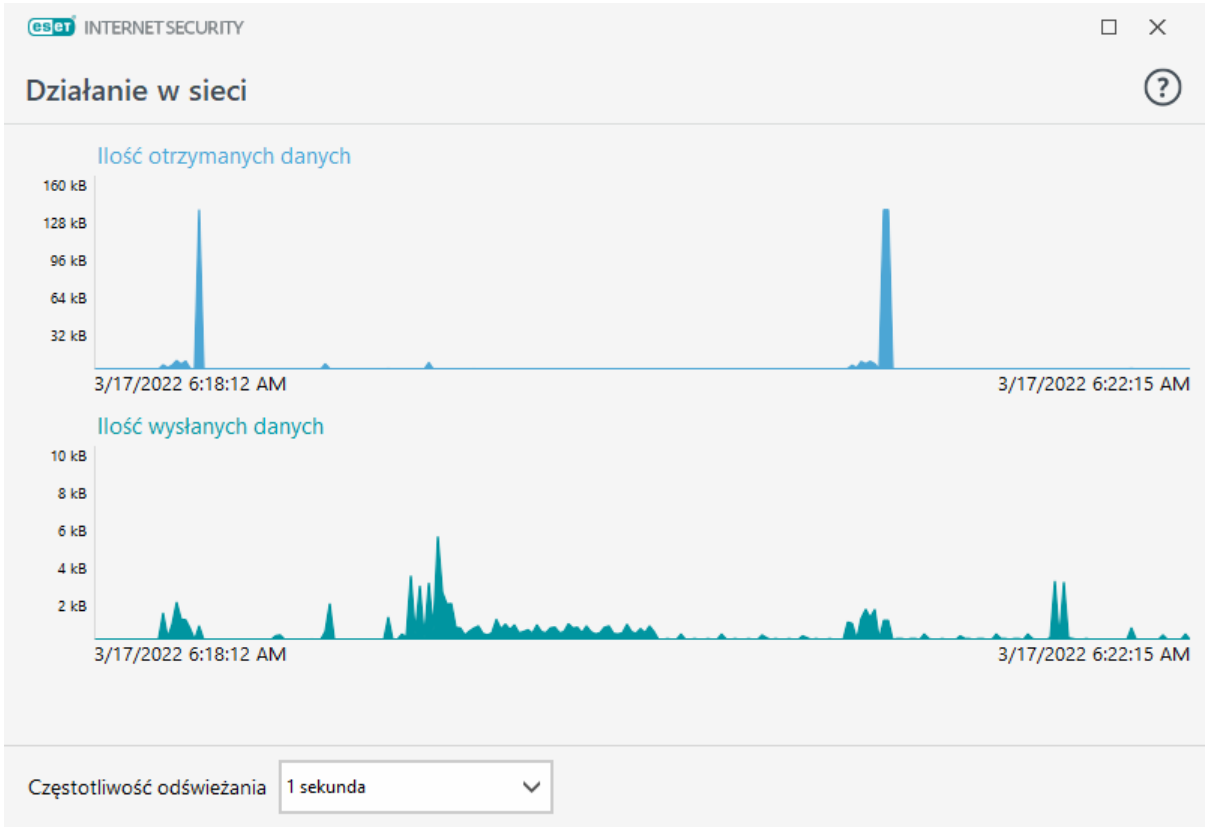
Kolejne opcje są dostępne tylko po kliknięciu aplikacji lub procesu, a nie aktywnego połączenia:

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 Konfigurowanie i używanie reguł.

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 Konfigurowanie i używanie reguł.

Działanie w sieci

Aby wyświetlić bieżącą **aktywność sieciową** w formie wykresu, kliknij **Narzędzia** > **Więcej narzędzi** > **Połączenia sieciowe** i kliknij ikonę wykresu. Na dole wykresu znajduje się oś czasu, która rejestruje aktywność sieciową w czasie rzeczywistym na podstawie wybranego przedziału czasu. Aby zmienić przedział czasu, wybierz odpowiednią wartość z menu rozwijanego **Częstotliwość odświeżania**.



Dostępne są następujące opcje:

- **1 sekunda** — wykres jest odświeżany co sekundę, a oś czasu odpowiada ostatnim 4 minutom.
- **1 minuta (ostatnie 24 godziny)** — wykres jest odświeżany co minutę, a oś czasu odpowiada ostatnim 24 godzinom.
- **1 godzina (ostatni miesiąc)** — wykres jest odświeżany co godzinę, a oś czasu odpowiada ostatniemu miesiącowi.

Oś pionowa wykresu reprezentuje ilość odebranych lub wysłanych danych. Najedź kursorem myszy na wykres, aby zobaczyć dokładną ilość odebranych/wysłanych danych w określonym czasie.

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. Aby dowiedzieć się, jak korzystać z programu ESET SysInspector, przejdź do Pomocy online ESET SysInspector.

W oknie ESET SysInspector wyświetlane są następujące informacje o dziennikach:

- **Godzina** — godzina utworzenia dziennika.
- **Komentarz** — krótki komentarz.
- **Użytkownik** — nazwa użytkownika, który utworzył dziennik.
- **Stan** — stan procesu tworzenia dziennika.

Dostępne są następujące czynności:

- **Pokaż** — otwiera się wybrane logowanie do ESET SysInspector. 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. Poczekaj, aż zostanie wygenerowany ESET SysInspector (stan **utworzono**) przed próbą uzyskania dostępu do dziennika.
- **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. Poczekaj, aż zostanie wygenerowany ESET SysInspector (stan **utworzono**) przed próbą uzyskania dostępu do dziennika.

• **Usuń** — powoduje usunięcie wybranych dzienników z listy.

• **Usuń wszystko** — powoduje usunięcie wszystkich dzienników.

• **Eksportuj** — umożliwia wyeksportowanie dziennika do pliku .xml lub skompresowanego pliku .xml. Dziennik zostanie wyeksportowany do C:\ProgramData\ESET\ESET Security\SysInspector.

Harmonogram

Harmonogram służy do zarządzania zaplanowanymi zadaniami i uruchamiania ich ze wstępnie zdefiniowaną konfiguracją.

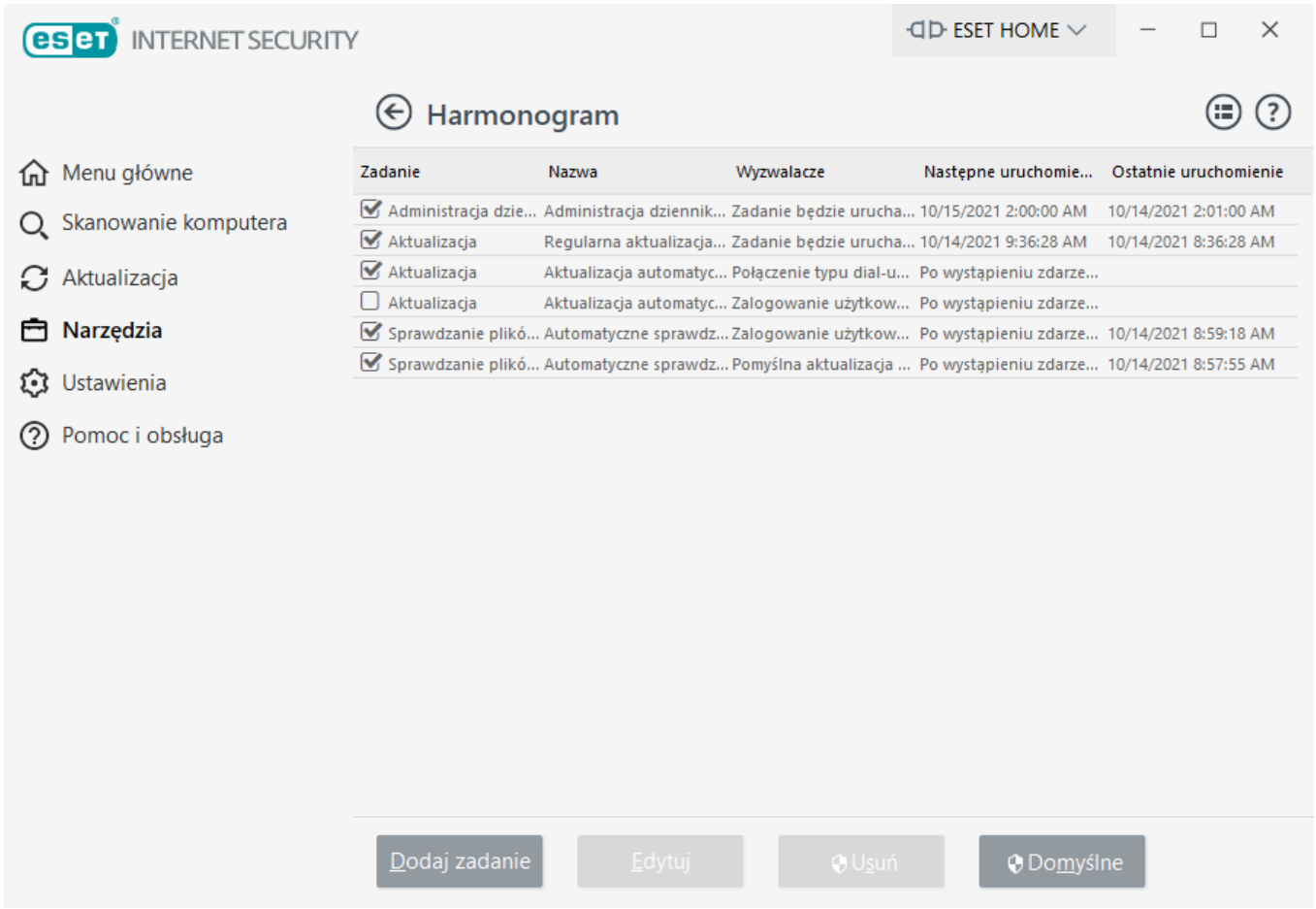
Harmonogram jest dostępny z poziomu głównego okna programu ESET Internet Security po kliknięciu opcji **Narzędzia** > **Więcej narzędzi** > **Harmonogram**. Okno **Harmonogram** zawiera listę wszystkich zaplanowanych zadań oraz ich skonfigurowane właściwości, takie jak wstępnie zdefiniowany dzień, godzina i używany profil skanowania.

Okno Harmonogram umożliwia planowanie następujących zadań: aktualizowanie modułów, zadania skanowania, 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. Listę zaplanowanych zadań można przywrócić do ustawień domyślnych i usunąć wszystkie zmiany, klikając pozycję **Domyślne**. 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 silnika detekcji)

Aby zmodyfikować konfigurację istniejącego zaplanowanego zadania (zarówno domyślnego, jak i zdefiniowanego przez użytkownika), kliknij prawym przyciskiem myszy zadanie i wybierz pozycję **Edytuj** lub wybierz zadanie, które chcesz zmodyfikować, 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 migawki stanu 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 przypadku każdego komponentu.

   • **Skanowanie komputera na żądanie** — umożliwia skanowanie plików i folderów na komputerze.

   • **Aktualizacja** — umożliwia zaplanowanie zadania aktualizacji modułów.

4. Aby aktywować zadanie, kliknij suwak obok pozycji **Włączono** (można to zrobić później poprzez zaznaczenie lub odznaczenie pola wyboru na liście zaplanowanych zadań), kliknij **Dalej** i wybierz jedną z opcji określających

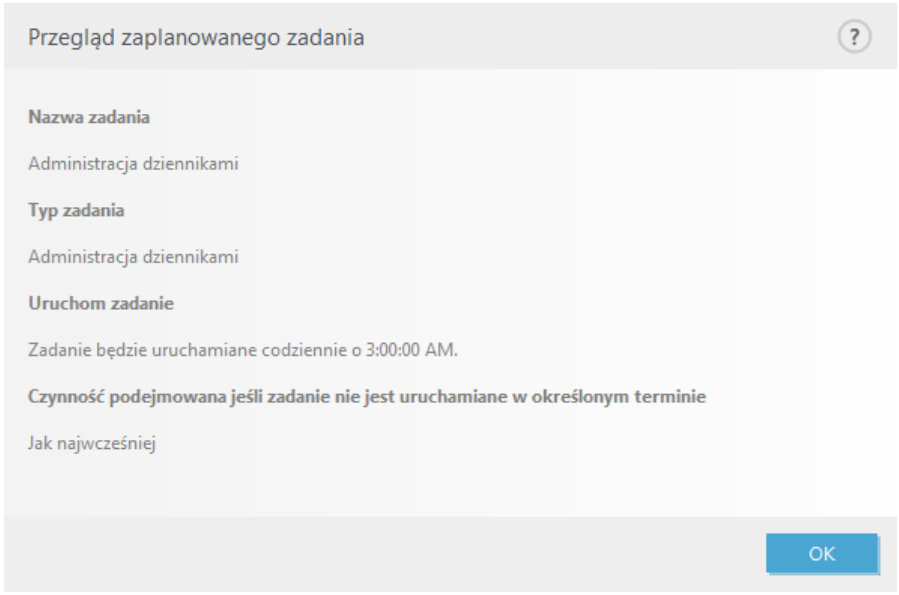
częstotliwość jego wykonywania:

- **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, jeśli czas od ostatniego uruchomienia przekroczy (liczbę godzin)** — wskazuje czas, jaki upłynął od pierwszego pominiętego uruchomienia zadania. Jeśli ten czas zostanie przekroczony, zadanie zostanie natychmiast uruchomione. Ustaw czas za pomocą pokrętła poniżej.

Zaplanowane zadanie można przejrzeć po kliknięciu go prawym przyciskiem i wybraniu opcji **Pokaż szczegóły zadania**.



Opcje planowanego skanowania

W tym oknie można określić opcje zaawansowane dla zaplanowanego zadania skanowania komputera.

Aby uruchomić skanowanie bez akcji czyszczenia, kliknij **Ustawienia zaawansowane** i wybierz **Skanuj bez czyszczenia**. Historia skanowania jest zapisywana w dzienniku skanowania.

Gdy wybrana jest opcja **Ignoruj wyjątki**, pliki o rozszerzeniach, które wcześniej zostały wyłączone ze skanowania, także zostaną przeskanowane.

Można skonfigurować czynność wykonywaną automatycznie po ukończeniu skanowania. Opcje dostępne są w menu rozwijanym:

- **Brak czynności** — po ukończeniu skanowania nie zostanie wykonana żadna czynność.
- **Wyłącz** — po ukończeniu skanowania komputer zostanie wyłączony.
- **Uruchom ponownie** — zamknięcie wszystkich otwartych programów i ponowne uruchomienie komputera po ukończeniu skanowania.
- **Uruchom ponownie w razie potrzeby** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.
- **Wymuś ponowne uruchomienie** — wymusza zamknięcie wszystkich otwartych programów bez oczekiwania na interakcję użytkownika i ponownie uruchamia komputer po zakończeniu skanowania.
- **W razie potrzeby wymuś ponowne uruchomienie** — komputer uruchamia się ponownie, jeśli jest to konieczne w celu zakończenia leczenia wykrytych zagrożeń.
- **Uśpij** — zapisanie sesji i przełączenie komputera w tryb obniżonego poboru energii, z którego szybko można wznowić pracę.
- **Hibernacja** — wszystkie procesy uruchomione w pamięci RAM zostają przeniesione do specjalnego pliku na dysku twardym. Komputer wyłącza się, ale po kolejnym uruchomieniu wznawia pracę od poprzedniego stanu.

> **Tryb uśpienia** lub **Hibernacja** są dostępne w zależności od ustawień zasilania i trybu uśpienia komputera lub możliwości technicznych komputera czy laptopa. Należy pamiętać, że komputer w trybie uśpienia nadal działa. Wciąż są uruchomione podstawowe funkcje i komputer nadal zużywa energię, będąc na zasilaniu akumulatorowym. Aby ograniczyć zużycie baterii, na przykład po opuszczeniu biura, zalecane jest skorzystanie z opcji Hibernacja.

Aby uniemożliwić nieupoważnionym użytkownikom zatrzymywanie czynności wykonywanych po skanowaniu, należy wybrać opcję **Użytkownik nie może anulować skanu**.

Aby umożliwić użytkownikom z ograniczeniami wstrzymywanie skanowania komputera na określony czas, należy wybrać opcję **Użytkownik może wstrzymać skanowanie na (min)**.

Zobacz także Postęp skanowania.

Przegląd zaplanowanego zadania

To okno dialogowe przedstawia szczegółowe informacje dotyczące wybranego zaplanowanego zadania. Aby je otworzyć, należy dwukrotnie kliknąć niestandardowe zadanie lub kliknąć prawym przyciskiem myszy niestandardowe zaplanowane zadanie, a następnie kliknąć pozycję **Pokaż szczegóły zadania**.

Szczegóły zadania

Wpisz **nazwę zadania**, wybierz jedną z opcji **Typ zadania**, a następnie kliknij przycisk **Dalej**:

- **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 w programie ESET SysInspector, gromadząc szczegółowe informacje dotyczące komponentów systemu (na przykład sterowników i aplikacji) wraz z oceną poziomu ryzyka w przypadku każdego komponentu.
- **Skanowanie komputera na żądanie** — umożliwia skanowanie plików i folderów na komputerze.
- **Aktualizacja** — umożliwia zaplanowanie zadania aktualizacji modułów.

Częstotliwość wykonywania zadania

Zadanie będzie wykonywane wielokrotnie, co określony czas. Należy wybrać jedną z dostępnych opcji częstotliwości:

- **Raz** — zadanie zostanie wykonane tylko raz w wyznaczonym dniu o ustalonej godzinie.
- **Wielokrotnie** — zadanie będzie wykonywane z określonym interwałem (podanym w godzinach).
- **Codziennie** — zadanie będzie wykonywane każdego dnia o określonej godzinie.
- **Co tydzień** — zadanie będzie wykonywane raz lub kilka razy w tygodniu, w wybrane dni o ustalonej godzinie.
- **Po wystąpieniu zdarzenia** — zadanie będzie wykonywane po wystąpieniu określonego zdarzenia.

Pomiń zadanie, gdy komputer jest zasilany z baterii — zadanie nie zostanie uruchomione, gdy w momencie jego planowego uruchomienia komputer będzie działać na zasilaniu akumulatorowym. Dotyczy to również komputerów pracujących przy zasilaniu awaryjnym (UPS).

Czas zadania - Raz

Wykonanie zadania — zadanie zostanie uruchomione tylko raz, w określonym dniu i o określonej godzinie.

Czas zadania - Codziennie

Zadanie będzie wykonywane każdego dnia o określonej godzinie.

Czas zadania - Co tydzień

Zadanie będzie wielokrotnie uruchamiane co tydzień w wybranym dniu i godzinie.

Czas zadania — zdarzenie wyzwalane

Zadanie zostanie wykonane po wystąpieniu jednego z następujących zdarzeń:

- **Każde uruchomienie komputera**
- **Pierwsze uruchomienie komputera każdego dnia**
- **Nawiązanie połączenia modemowego z Internetem/wirtualną siecią prywatną**
- **Pomyślna aktualizacja modułu**
- **Pomyślna aktualizacja produktu**
- **Zalogowanie użytkownika**
- **Wykrycie zagrożenia**

Tworząc harmonogram zadań wykonywanych po wystąpieniu określonego zdarzenia, można określić minimalny odstęp czasowy między dwoma kolejnymi wykonaniami danego zadania. Na przykład, jeśli użytkownik loguje się na komputerze kilka razy dziennie, może wybrać odstęp 24-godzinny, aby dane zadanie było wykonywane tylko po pierwszym zalogowaniu danego dnia, a potem dopiero w następnym dniu.

Pominięte zadanie

Zadanie może zostać pominięte, gdy komputer działa na zasilaniu akumulatorowym lub gdy jest wyłączony. Spośród poniższych opcji należy wybrać termin uruchomienia pominiętego zadania, a następnie kliknąć **Dalej**:

- **W następnym zaplanowanym terminie** — zadanie zostanie uruchomione w następnym zaplanowanym terminie, jeśli komputer będzie włączony.
- **Jak najwcześniej** — zadanie zostanie uruchomione po włączeniu komputera.
- **Natychmiast, jeśli czas od ostatniego zaplanowanego uruchomienia przekracza (liczba godzin)** — wskazuje czas, jaki upłynął od pierwszego pominiętego uruchomienia zadania. Jeśli ten czas zostanie przekroczony, zadanie zostanie natychmiast uruchomione.

Natychmiast, jeśli czas od ostatniego zaplanowanego uruchomienia przekracza (godz.) – przykłady

Przykładowe zadanie jest ustawione tak, aby było uruchamiane wielokrotnie co godzinę. Opcja **Natychmiast, jeśli czas od ostatniego zaplanowanego uruchomienia przekracza (liczba godzin)** jest zaznaczona, a przekroczony czas jest ustawiony na dwie godziny. Zadanie zostanie uruchomione o godzinie 13:00, a po zakończeniu komputer przejdzie w tryb uśpienia:

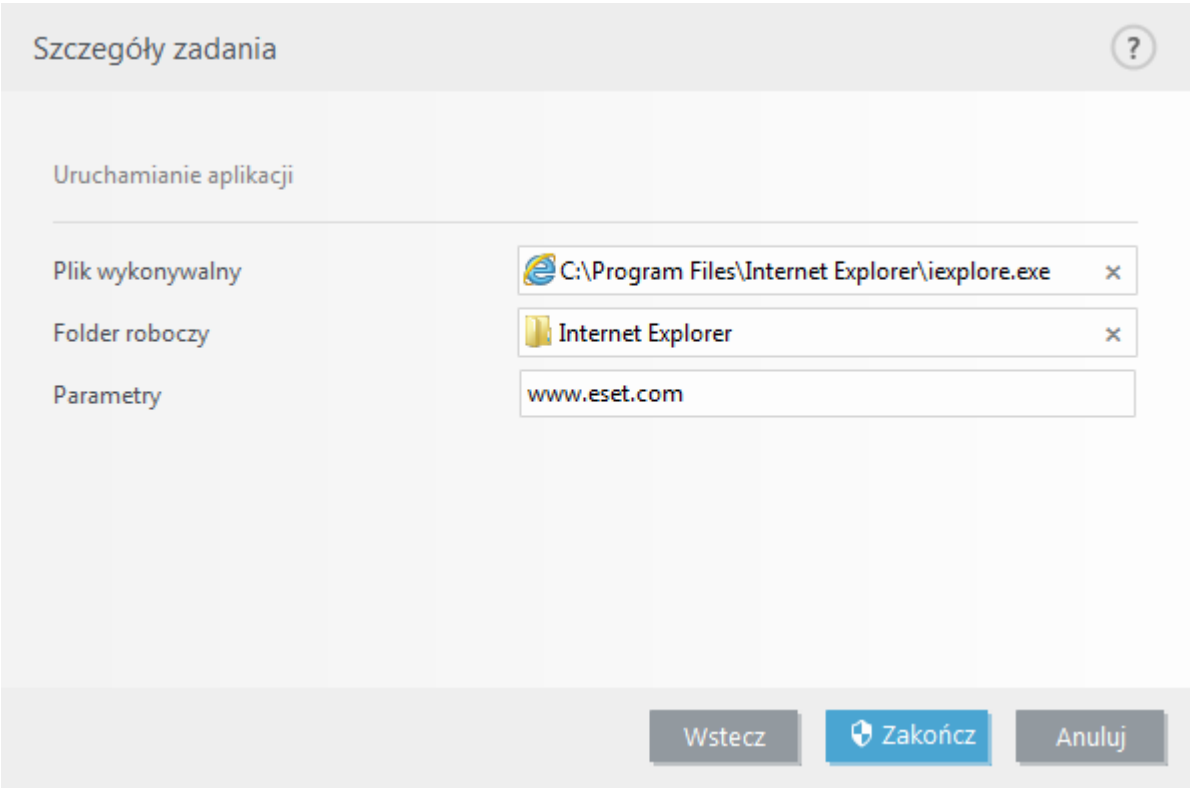
- Komputer wzbudza się o 15:30. Uruchomienie zadania pominięto po raz pierwszy o godzinie 14:00. Od godziny 14:00 minęło zaledwie 1,5 godziny, więc zadanie zostanie uruchomione o godzinie 16:00.
- Komputer wzbudza się o 16:30. Uruchomienie zadania pominięto po raz pierwszy o godzinie 14:00. Od godziny 14:00 minęły dwie i pół godziny, więc zadanie zostanie uruchomione natychmiast.

Szczegóły zadania — Aktualizacja

Aby aktualizować program przy użyciu dwóch serwerów aktualizacji, konieczne jest utworzenie dwóch różnych profili aktualizacji. Jeśli nie powiedzie się pobranie plików aktualizacji przy użyciu pierwszego profilu, program automatycznie przełączy się na użycie drugiego z nich. Takie rozwiązanie jest odpowiednie na przykład dla notebooków, które zwykle korzystają z serwera aktualizacji w sieci lokalnej, ale ich właściciele często łączą się z Internetem poprzez inne sieci. Jeśli w takiej sytuacji próba aktualizacji przy użyciu pierwszego profilu nie powiedzie się, automatycznie zostanie użyty drugi profil w celu pobrania plików aktualizacji z serwerów aktualizacji firmy ESET.

Szczegóły zadania - Uruchom aplikację

Dzięki temu zadaniu można zaplanować uruchomienie aplikacji zewnętrznej.



Plik wykonywalny — wybierz plik wykonywalny z drzewa katalogów, kliknij opcję **...** albo wpisz ścieżkę ręcznie.

Folder roboczy — podaj folder roboczy aplikacji. Wszystkie pliki tymczasowe tworzone przez aplikację wskazaną w

polu **Plik wykonywalny** będą zapisywane w tym katalogu.

Parametry — podaj parametry wiersza polecenia dla aplikacji (opcjonalnie).

Aby zatwierdzić zadanie, kliknij przycisk **Zakończ**.

Leczenie systemu

Leczenie systemu to narzędzie ułatwiające przywracanie komputera do użytecznego stanu po jego wyleczeniu z zagrożenia. Szkodliwe oprogramowanie może wyłączyć narzędzia systemowe, takie jak Edytor rejestru, Menedżer zadań czy Aktualizacje systemu Windows. Funkcja Leczenie systemu umożliwia przywracanie domyślnych wartości i ustawień danego systemu jednym kliknięciem.

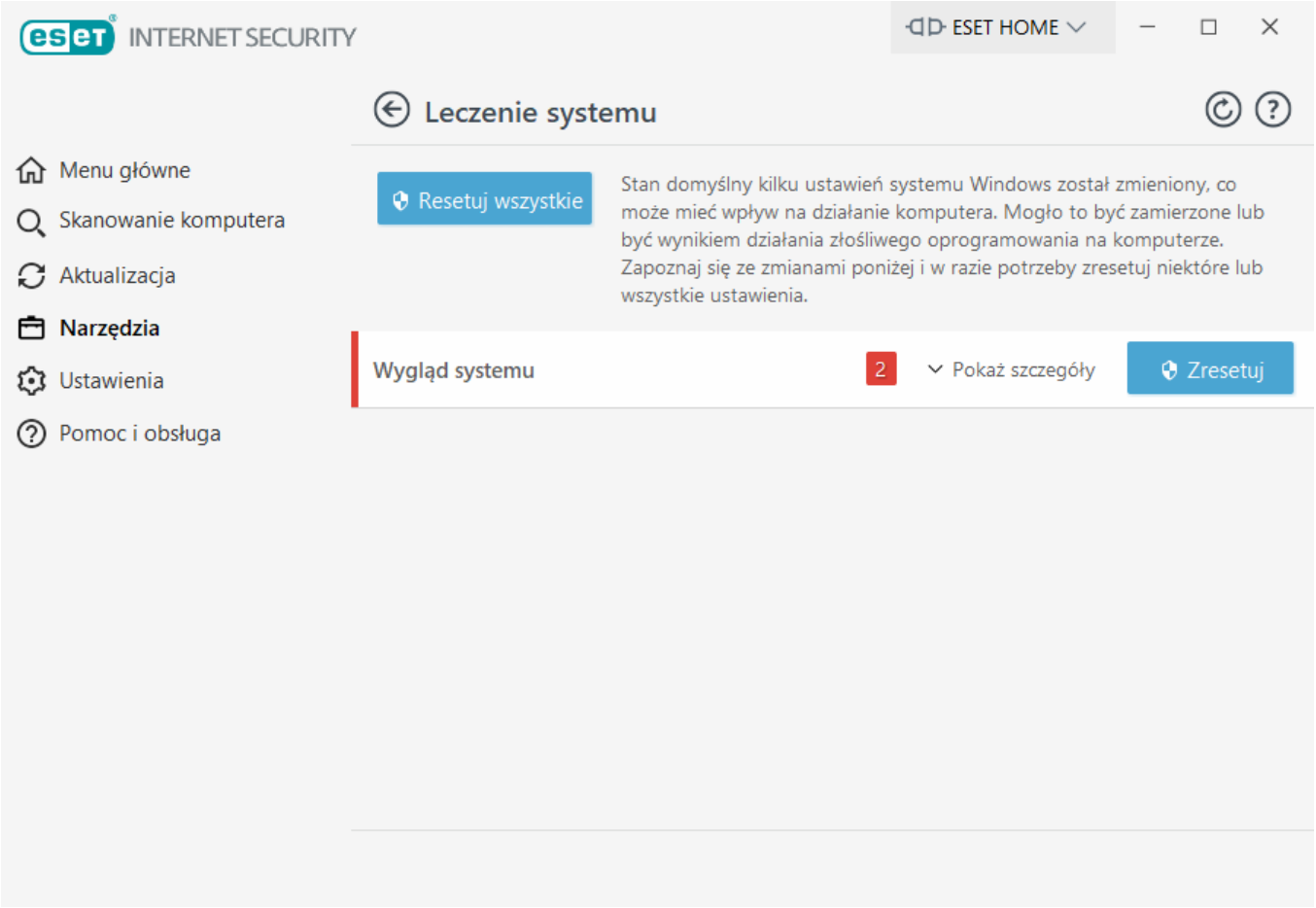
Leczenie systemu zgłasza problemy z pięciu kategorii ustawień:

- **Ustawienia zabezpieczeń**: zmiany w ustawieniach, które mogą zwiększyć podatność komputera na zagrożenia, na przykład w ustawieniach funkcji Windows Update.
- **Ustawienia systemu**: zmiany w ustawieniach systemu, które mogą zmienić działanie komputera, na przykład w ustawieniach skojarzeń plików.
- **Wygląd systemu**: ustawienia zmieniające wygląd systemu, na przykład ustawienia tapety pulpitu.
- **Wyłączone funkcje**: ważne funkcje i aplikacje, które mogą być wyłączone.
- **Przywracanie systemu Windows**: ustawienia funkcji Przywracanie systemu Windows, które umożliwiają przywracanie systemu do poprzedniego stanu

Narzędzie Leczenie systemu może być używane w następujących przypadkach:

- Znalezienie zagrożenia
- Kliknięcie przez użytkownika opcji **Zresetuj**

Można przejrzeć zmiany i w razie potrzeby zresetować ustawienia.



Narzędzia Leczenie systemu może używać tylko użytkownik z uprawnieniami administratora.

ESET SysRescue Live

ESET SysRescue Live to bezpłatne narzędzie umożliwiające tworzenie rozruchowego dysku ratunkowego CD/DVD lub USB. Przy użyciu nośnika ratunkowego można uruchomić zainfekowany komputer, przeskanować go pod kątem szkodliwego oprogramowania i wyleczyć zainfekowane pliki.

Główną zaletą narzędzia ESET SysRescue Live jest to, że działa niezależnie od systemu operacyjnego komputera, a jednocześnie ma bezpośredni dostęp do dysku i systemu plików. Umożliwia to usunięcie zagrożeń, których nie można usunąć w normalnych warunkach, na przykład podczas działania systemu operacyjnego.

- Pomoc online dotycząca usługi ESET SysRescue Live

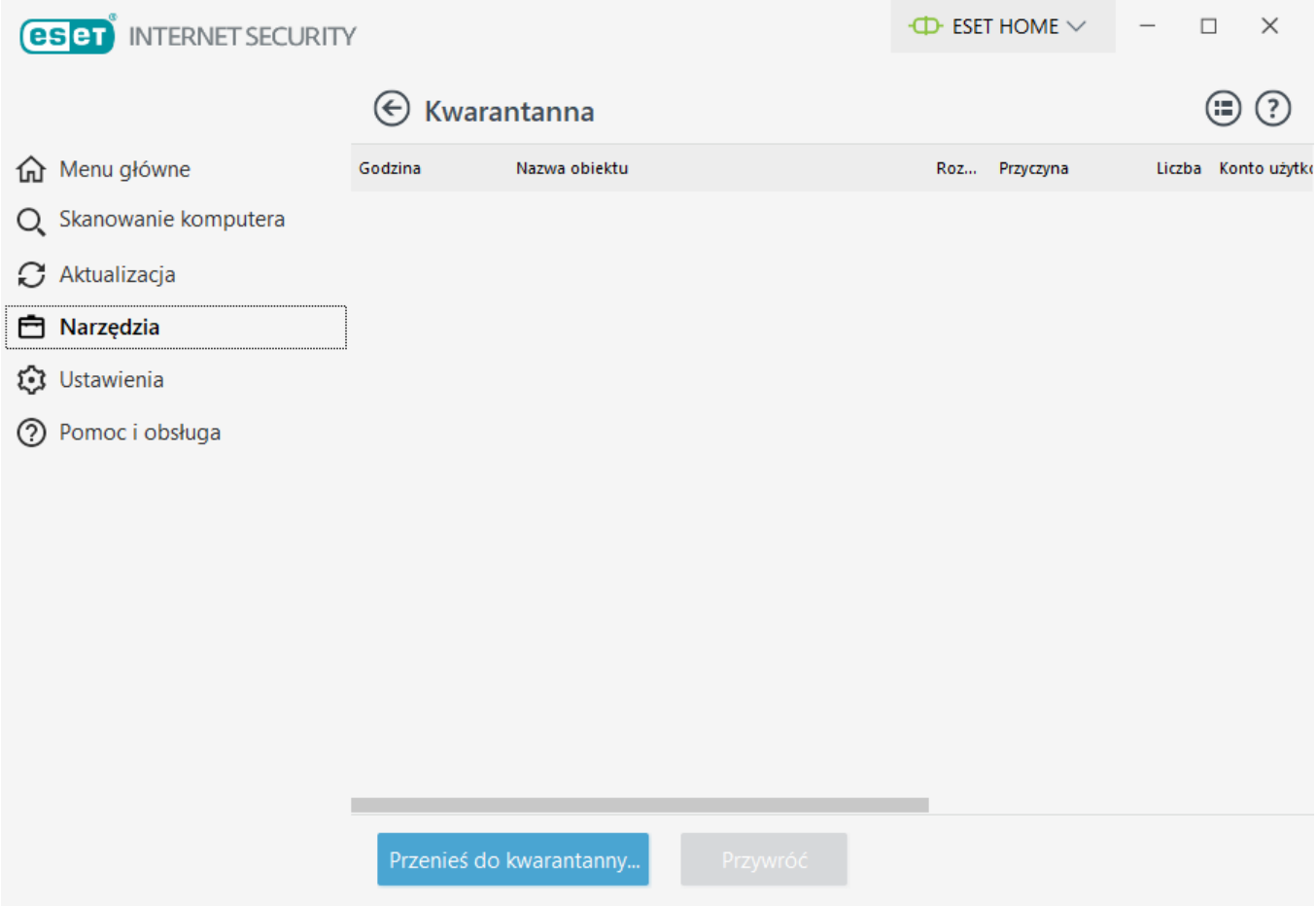
Kwarantanna

Głównym zadaniem funkcji kwarantanny jest bezpieczne przechowywanie zgłoszonych obiektów (takich jak szkodliwe oprogramowanie, zainfekowane pliki lub potencjalnie niepożądane aplikacje).

Kwarantanna jest dostępna z poziomu głównego okna programu ESET Internet Security po kliknięciu opcji **Narzędzia** > **Więcej narzędzi** > **Kwarantanna**.

Pliki przechowywane w folderze kwarantanny można przeglądać w tabeli zawierającej następujące informacje:

- Data i godzina poddania kwarantannie
- Ścieżka do pierwotnej lokalizacji pliku
- Rozmiar pliku w bajtach
- Powód (np. obiekt dodany przez użytkownika)
- Liczba wykrytych obiektów (na przykład zduplikowane wykrycia tego samego pliku lub archiwum zawierające wiele przypadków infekcji)



Poddawanie plików kwarantannie

Program ESET Internet Security automatycznie poddaje kwarantannie usunięte pliki (jeśli ta opcja nie została anulowana w oknie alertu).

Dodatkowe pliki powinny zostać poddane kwarantannie w następujących przypadkach:

a.Jeśli nie można ich wyleczyć

b.Jeśli ich usunięcie nie jest bezpieczne lub wskazane

c.Jeśli są one fałszywie wykrywane przez program ESET Internet Security

d.Jeśli plik zachowuje się podejrzanie, ale nie jest wykrywany przez skaner

Aby poddać plik kwarantannie, można skorzystać z różnych opcji:

a.Ręcznie przeciągnij i upuść plik do kwarantanny, klikając go i przesuwając wskaźnik do zaznaczonego obszaru, przytrzymując jednocześnie naciśnięty przycisk myszy, a następnie zwolnij przycisk myszy. Spowoduje to przeniesienie aplikacji na pierwszy plan.

b.Kliknij plik prawym przyciskiem myszy > kliknij **Opcje zaawansowane** > **Poddaj plik kwarantannie**.

c.Kliknij pozycję **Przenieś do kwarantanny** w oknie **Kwarantanna**.

d.Możesz też skorzystać z menu kontekstowego: kliknij prawym przyciskiem myszy okno **Kwarantanna** i wybierz pozycję **Kwarantanna**.

Przywracanie plików z kwarantanny

Pliki poddane kwarantannie można również przywrócić do ich pierwotnej lokalizacji:

- Umożliwia to funkcja **Przywróć**, dostępna w menu kontekstowym otwieranym po kliknięciu prawym przyciskiem myszy danego pliku w obszarze Kwarantanna.

- Jeśli plik jest oznaczony jako potencjalnie niepożądana aplikacja, włączona jest opcja **Przywróć i wyłącz ze skanowania**. Zobacz też: Wyłączenia.

- Menu kontekstowe zawiera także opcję **Przywróć do**, która umożliwia przywrócenie pliku do lokalizacji innej niż ta, z której został usunięty.

- Funkcja przywracania nie jest dostępna w niektórych przypadkach, na przykład gdy pliki znajdują się w udziale sieciowym tylko do odczytu.

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. Usunięte elementy są usuwane na stałe z urządzenia i kwarantanny.

Przesyłanie pliku z kwarantanny

Jeśli poddano kwarantannie podejrzany plik, który nie został wykryty przez program, lub jeśli plik został błędnie oceniony jako zarażony (np. w wyniku analizy heurystycznej kodu), a następnie poddany kwarantannie, należy wysłać próbkę do analizy w laboratorium firmy ESET. Aby przesłać plik, należy kliknąć go prawym przyciskiem myszy i z menu kontekstowego wybrać polecenie **Prześlij do analizy**.

Opis wykrycia

Kliknij prawym przyciskiem myszy element i wybierz **Opis wykrycia,** aby otworzyć Encyklopedię zagrożeń firmy ESET, która zawiera szczegółowe informacje o zagrożeniach i objawach zarejestrowanej infiltracji.

Ilustrowane instrukcje

Następujące artykuły z bazy wiedzy ESET mogą być dostępne tylko w języku angielskim:

- Przywracanie pliku poddanego kwarantannie w programie ESET Internet Security
- Usuwanie pliku poddanego kwarantannie w programie ESET Internet Security
- Produkt ESET powiadomił mnie o wykryciu zagrożenia — co mam zrobić?

Niepowodzenie kwarantanny

Powody sprawiające, że niektórych plików nie można poddać kwarantannie:

- **Nie posiadasz uprawnień do odczytu** — oznacza to, że nie możesz wyświetlić zawartości pliku.
- **Nie posiadasz uprawnień do zapisu** — oznacza to, że nie możesz modyfikować zawartości pliku, a więc dodawać nowej zawartości lub usuwać istniejącej.
- **Plik, który próbujesz poddać kwarantannie, jest zbyt duży** — musisz zmniejszyć rozmiar pliku.

Po wyświetleniu komunikatu o błędzie „Niepowodzenie kwarantanny” kliknij **Więcej informacji**. Pojawi się okno zawierające listę błędów kwarantanny oraz nazwę pliku i przyczynę, dlaczego plik nie może zostać poddany kwarantannie.

Serwer proxy

W dużych sieciach LAN 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 Internet 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 Internet Security. Wprowadzone w tym miejscu parametry będą używane przez wszystkie moduły, które wymagają połączenia internetowego.

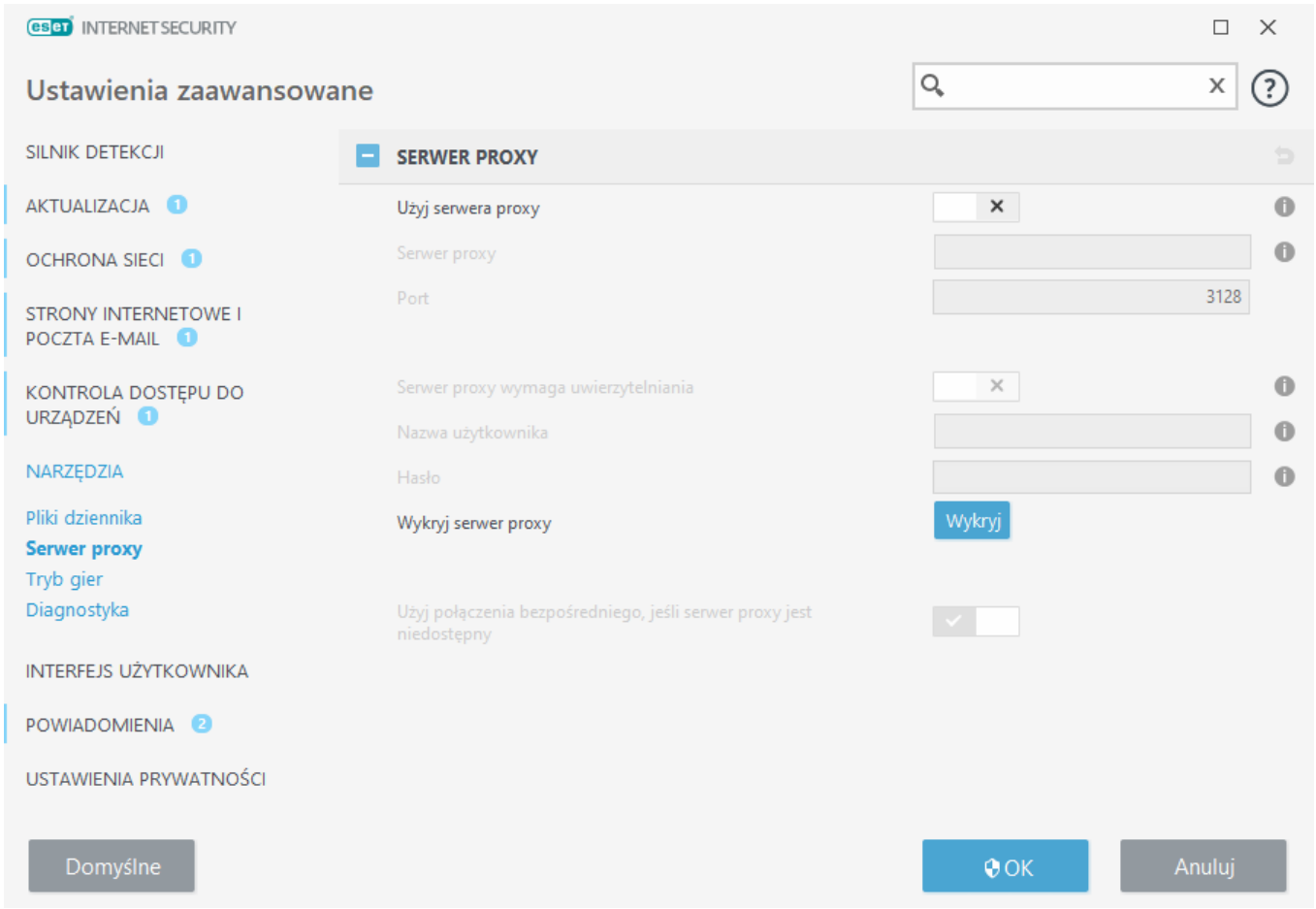
Aby określić ustawienia serwera proxy na tym poziomie, zaznacz pozycję **Użyj serwera proxy**, a następnie wprowadź adres serwera proxy w polu **Serwer proxy** oraz jego numer portu — w polu **Port**.

Jeśli komunikacja z serwerem proxy wymaga uwierzytelniania, wybierz opcję **Serwer proxy wymaga uwierzytelniania** i w odpowiednich polach wprowadź **nazwę użytkownika** i **hasło**. Kliknij opcję **Wykryj serwer proxy**, aby włączyć automatyczne wykrywanie i wprowadzanie ustawień serwera proxy. Zostaną skopiowane parametry określone w opcjach internetowych przeglądarki Internet Explorer lub Google Chrome.

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

Użyj połączenia bezpośredniego, jeśli serwer proxy jest niedostępny — jeśli w produkcie ESET Internet Security skonfigurowano nawiązywanie połączenia się za pomocą serwera proxy, ale serwer proxy jest niedostępny, produkt ESET Internet Security pominie go i będzie się łączyć bezpośrednio z serwerami firmy ESET.

Ustawienia serwera proxy można również skonfigurować w obszarze Ustawienia zaawansowane (**Ustawienia zaawansowane** > **Aktualizacja** > **Profile** > **Aktualizacje** > **Opcje połączenia**, wybierając opcję **Połączenie przez serwer proxy** z menu rozwijanego **Tryb proxy**). To ustawienie ma zastosowanie do danego profilu aktualizacji i jest zalecane w przypadku komputerów przenośnych, które często pobierają aktualizacje sygnatur wirusów z lokalizacji zdalnych. Więcej informacji na temat tego ustawienia można znaleźć w sekcji Zaawansowane ustawienia aktualizacji.



Wybieranie próbki do analizy

Jeżeli znajdziesz podejrzany plik na komputerze lub podejrzaną witrynę w Internecie, możesz je przesłać do analizy w laboratorium firmy ESET (dostępność tej opcji zależy od konfiguracji rozwiązania ESET LiveGrid®).

Zanim prześlesz próbki do firmy ESET

Nie przesyłaj próbki, jeżeli nie spełnia co najmniej jednego z następujących kryteriów:

- Próbka nie jest w ogóle wykrywana przez produkt ESET.
- Plik jest błędnie wykrywany jako zagrożenie.
- Nie akceptujemy plików osobistych jako próbek (w celu przeskanowania pod kątem szkodliwego oprogramowania przez ESET). Laboratorium ESET nie skanuje plików użytkowników na żądanie.
- Wpisz opisowy temat wiadomości i podaj jak najwięcej informacji na temat podejrzanego pliku (może to być np. zrzut ekranu lub adres witryny internetowej, z której został on pobrany).

Próbkę do analizy (plik lub witrynę) można przesłać do ESET jedną z następujących metod:

1. Użyj formularza przesyłania próbki dostępnego w produkcie. Aby go znaleźć, wybierz pozycje **Narzędzia** > **Więcej narzędzi** > **Prześlij plik do analizy**. Maksymalny dopuszczany rozmiar próbki wynosi 256 MB.

2. Plik można też przesłać pocztą e-mail. W tym celu należy go skompresować za pomocą programu WinRAR/WinZIP, szyfrując archiwum przy użyciu hasła „infected”. Tak przygotowane archiwum należy wysłać na adres samples@eset.com.

3. Informacje o zgłaszaniu spamu, fałszywych alarmów spamowych lub witryn internetowych zakwalifikowanych nieprawidłowo przez moduł Kontrola rodzicielska zawiera artykuł bazy wiedzy ESET.

W formularzu **Wybieranie próbki do analizy** wybierz opis z menu rozwijanego **Powód przesyłania pliku**, który najlepiej odpowiada celowi wiadomości:

- Podejrzany plik
- Podejrzana witryna (witryna internetowa, która jest zainfekowana przez szkodliwe oprogramowanie),
- Fałszywy alarm - witryna
- Plik z fałszywym alarmem (plik, który został wykryty jako zainfekowany, ale zainfekowany nie był),
- 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 dodatkowych informacji. Może on zostać wykorzystany w celu nawiązania kontaktu, jeśli analiza wymaga dodatkowych informacji. Wprowadzenie adresu kontaktowego jest opcjonalne. Aby pozostawić to pole puste, wybierz pozycję **Prześlij anonimowo**.

> **ESET może nie odpowiedzieć na zgłoszenie**
> Jeśli nie są wymagane dodatkowe informacje, firma ESET nie odpowiada na zgłoszenia. Nasze serwery codziennie odbierają dziesiątki tysięcy plików, dlatego nie da się odpowiedzieć każdemu nadawcy. Jeśli okaże się, że próbka jest szkodliwą aplikacją lub witryną internetową, możliwość jej wykrycia zostanie dodana do jednej z przyszłych aktualizacji produktu ESET.

Wybieranie próbki do analizy — podejrzany plik

Obserwowane oznaki i objawy zarażenia szkodliwym oprogramowaniem — należy wprowadzić opis zachowania podejrzanego pliku na komputerze.

Pochodzenie pliku (adres URL lub dostawca)— należy podać pochodzenie (źródło) pliku i okoliczności jego napotkania.

Uwagi oraz informacje dodatkowe — można tu wprowadzić dodatkowe informacje lub opisy, które pomogą podczas przetwarzania identyfikacji podejrzanego pliku.

> Wymagany jest tylko pierwszy parametr — **Obserwowane oznaki i objawy zarażenia szkodliwym oprogramowaniem**, ale podanie informacji dodatkowych znacznie ułatwi naszym laboratoriom identyfikację i przetwarzanie próbek.

Wybieranie próbki do analizy — podejrzana witryna

Należy wybrać jedną z pozycji rozwijanego menu **Nieprawidłowości występujące na witrynie**:

- **Zainfekowana** — witryna internetowa, która zawiera wirusy lub inne złośliwe oprogramowanie rozprowadzane za pośrednictwem różnych metod.
- **Ataki typu „phishing”** — działania takie są podejmowane z myślą o uzyskaniu dostępu do prywatnych danych, np. numerów kont bankowych, kodów PIN itp. Więcej informacji na temat ataków tego typu można

znaleźć w słowniczku.

- **Fałszywa** — fałszywa lub nieuczciwa witryna internetowa, stworzona z myślą o szybkim zysku.
- Wybierz **Inne**, jeżeli powyższe opcje nie dotyczące witryny, którą zamierzasz przesłać.

Uwagi i informacje dodatkowe — można tu wprowadzić dodatkowe informacje lub opisy, które pomogą w procesie analizowania podejrzanej witryny internetowej.

Wybieranie próbki do analizy — plik z fałszywym alarmem

Zachęcamy użytkowników do przysyłania plików, które zostały wykryte jako infekcja, ale nie są zainfekowane, w celu udoskonalenia naszych aparatów antywirusowych i antyspyware oraz pomagania w ochronie innych użytkowników. Fałszywe alarmy mogą wystąpić, gdy plik ma taki sam wzorzec jak ten, który znajduje się w silniku detekcji.

Nazwa i wersja aplikacji — nazwa programu i jego wersja (np. numer, alias lub nazwa kodowa).

Pochodzenie pliku (adres URL lub dostawca) — należy podać pochodzenie (źródło) pliku i okoliczności jego napotkania.

Przeznaczenie aplikacji — ogólny opis aplikacji, jej typ (np. przeglądarka internetowa, odtwarzacz multimedialny) i zakres funkcji.

Uwagi i informacje dodatkowe — można tu wprowadzić dodatkowe informacje lub opisy, które pomogą w przetwarzaniu podejrzanego pliku.

> Trzy pierwsze parametry są wymagane do identyfikacji legalnego oprogramowania i odróżnienia go od szkodliwego kodu. Podanie dodatkowych informacji wydatnie pomoże naszym laboratoriom w identyfikacji i przetwarzaniu przesłanych próbek.

Wybieranie próbki do analizy — witryna z fałszywym alarmem

Zachęcamy użytkowników do przysyłania adresów witryn internetowych, które zostały wykryte jako infekcja, oszustwo lub ataki typu „phishing”, ale nimi nie są. Fałszywe alarmy mogą wystąpić, gdy plik ma taki sam wzorzec jak ten, który znajduje się w silniku detekcji. Prosimy o dostarczanie takich witryn internetowych, ponieważ pozwala to na doskonalenie działania naszego aparatu antywirusowego i ochrony przed atakami typu „phishing” oraz pomaga zapewnić ochronę innym użytkownikom.

Uwagi i informacje dodatkowe — można tu wprowadzić dodatkowe informacje lub opisy, które pomogą w przetwarzaniu podejrzanej witryny internetowej.

Wybieranie próbki do analizy — inne

Z tego formularza należy skorzystać, jeśli danego pliku nie można zaliczyć ani do kategorii **Podejrzany plik**, ani do kategorii **Fałszywy alarm**.

Powód przesyłania pliku — należy podać szczegółowy opis pliku i powód jego przesłania.

Aktualizacja systemu Microsoft Windows®

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 Internet 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.

Okno dialogowe – Aktualizacje systemu

Jeżeli będą dostępne aktualizacje do systemu operacyjnego, zostanie wyświetlone powiadomienie w oknie głównym programu ESET Internet Security. Kliknij pozycję **Więcej informacji**, aby otworzyć okno Aktualizacje systemu.

W oknie aktualizacji systemu znajduje się lista dostępnych aktualizacji gotowych do pobrania i zainstalowania. Typ aktualizacji jest wyświetlany obok jej nazwy.

Kliknij dwukrotnie dowolny wiersz aktualizacji, aby wyświetlić okno Informacje o aktualizacjach zawierające dodatkowe informacje.

Aby rozpocząć pobieranie i instalowanie aktualizacji systemu operacyjnego, należy kliknąć opcję **Uruchom aktualizację systemu**.

Informacje o aktualizacjach

Informacje o aktualizacjach systemu Windows. W oknie wyświetlane są nazwa i numer aktualizacji oraz priorytet i opis problemu usuwanego dzięki aktualizacji.

Interfejs użytkownika

Aby skonfigurować zachowanie graficznego interfejsu użytkownika (GUI) programu, w głównym oknie programu kliknij przycisk **Ustawienia** > **Ustawienia zaawansowane** (F5) > **Interfejs użytkownika**.

Wygląd i efekty wizualne programu można dostosować na ekranie Elementy interfejsu użytkownika w sekcji Ustawień zaawansowanych.

Aby zapewnić maksymalne bezpieczeństwo oprogramowania zabezpieczającego, można zapobiec wprowadzaniu w nim wszelkich nieupoważnionych zmian, chroniąc ustawienia hasłem przy użyciu narzędzia Ustawienia dostępu.

> Aby skonfigurować zachowanie powiadomień systemowych, alertów wykrywania i stanów aplikacji, zobacz sekcję Powiadomienia.

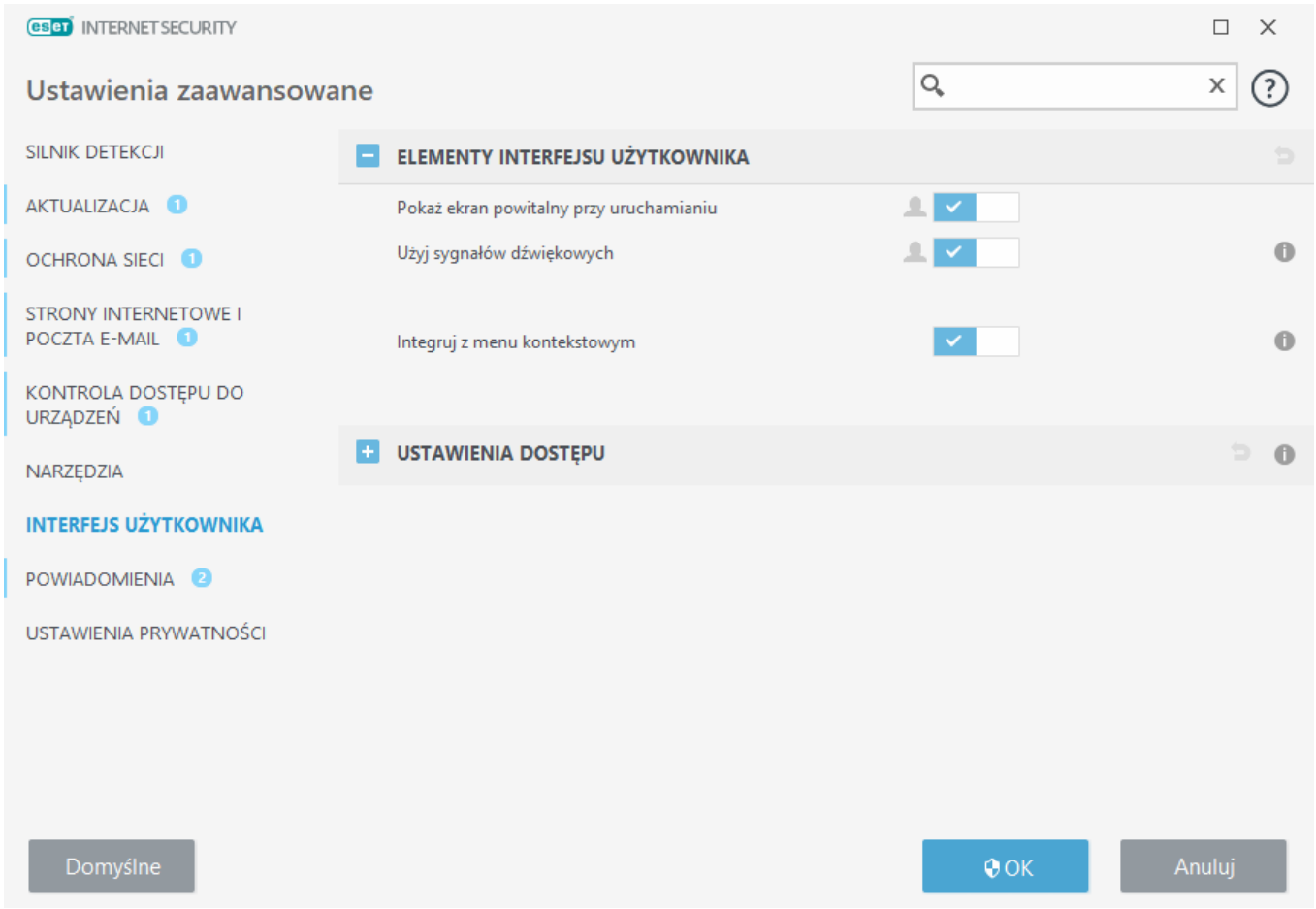
Elementy interfejsu użytkownika

Opcje konfiguracji interfejsu użytkownika w programie ESET Internet Security umożliwiają dostosowanie środowiska pracy do potrzeb użytkownika. Te opcje konfiguracji są dostępne po wybraniu kolejno pozycji **Ustawienia zaawansowane** (F5) > **Interfejs użytkownika** > **Elementy interfejsu użytkownika**.

Aby wyłączyć ekran powitalny programu ESET Internet Security, należy usunąć zaznaczenie opcji **Pokaż ekran powitalny przy uruchamianiu**.

Używaj sygnału dźwiękowego — ESET Internet Security odtwarza dźwięk po wystąpieniu ważnego zdarzenia podczas skanowania, np. po wykryciu zagrożenia lub po zakończeniu skanowania.

Integruj z menu kontekstowym — włącza integrację elementów sterujących programu ESET Internet Security z menu kontekstowym.



Ustawienia dostępu

Ustawienia programu ESET Internet Security stanowią kluczowy element polityki bezpieczeństwa. Nieupoważnione modyfikacje mogą stanowić potencjalne zagrożenie dla stabilności i ochrony systemu. Aby zapobiec nieautoryzowanemu wprowadzaniu zmian, parametry ustawień programu ESET Internet Security oraz proces dezinstalacji można chronić za pomocą hasła.

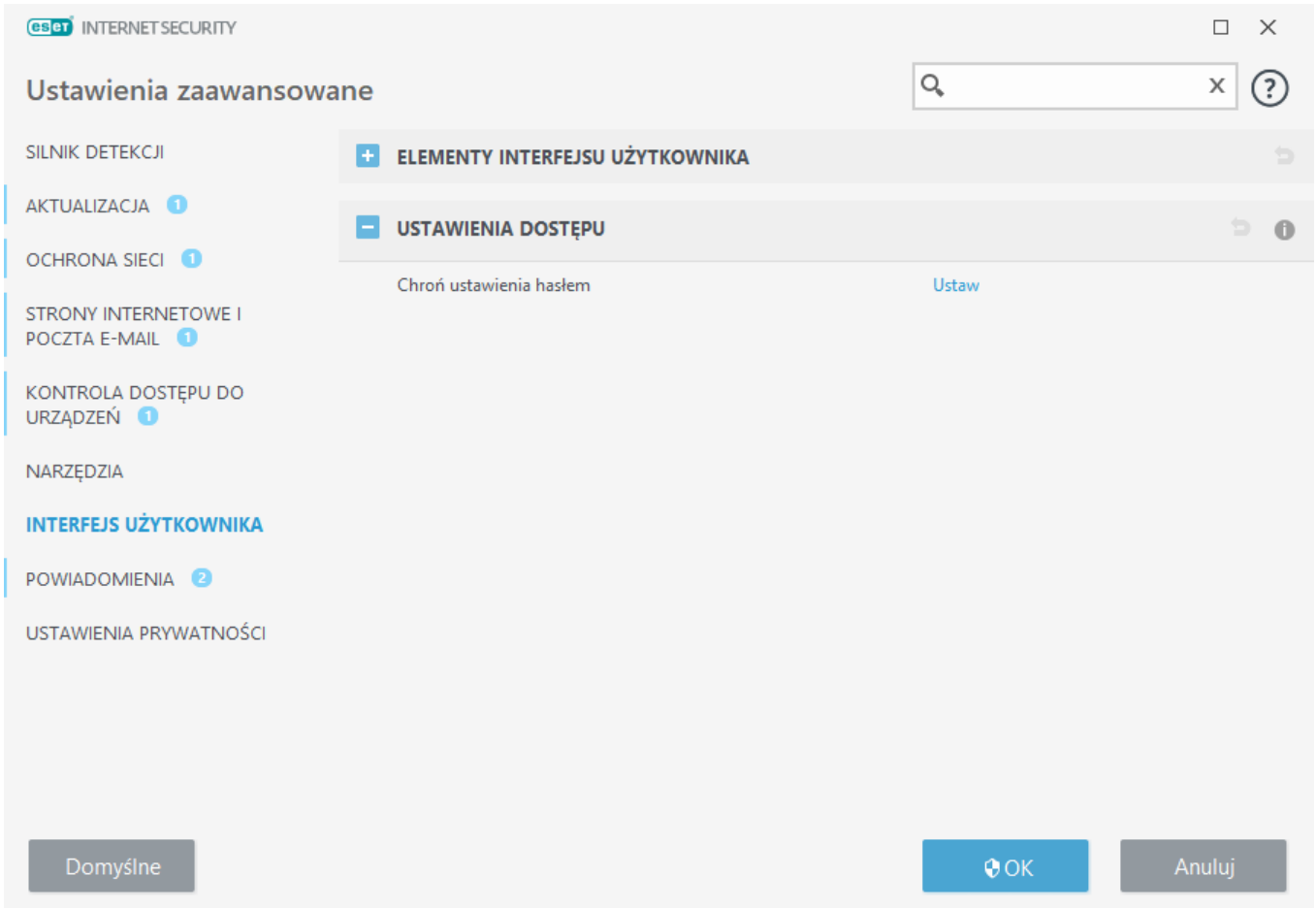
Aby ustawić hasło do ochrony parametrów ustawień i dezinstalacji ESET Internet Security, kliknij pozycję **Ustaw** obok ustawienia **Chroń ustawienia hasłem**.

Podczas uzyskiwania dostępu do chronionego hasłem obszaru Ustawienia zaawansowane wyświetli się okno, w którym należy wpisać hasło. Jeśli użytkownik nie pamięta hasła lub je utracił, powinien kliknąć znajdującą się pod spodem opcję **Przywróć hasło** i wprowadzić adres e-mail podany podczas rejestracji licencji. Firma ESET wyśle do użytkownika wiadomość e-mail z kodem weryfikacyjnym i instrukcją zresetowania hasła.

- Odblokowywanie obszaru Ustawienia zaawansowane

Aby zmienić hasło, kliknij pozycję **Zmień hasło** obok pozycji **Chroń ustawienia hasłem**.

Aby usunąć hasło, kliknij pozycję **Usuń** obok pozycji **Chroń ustawienia hasłem**.



Hasło do ustawień zaawansowanych

Aby zabezpieczyć parametry ustawień zaawansowanych programu ESET Internet Security przed nieautoryzowaną modyfikacją, należy ustawić nowe hasło.

Aby zmienić bieżące hasło:

1. Wpisz stare hasło w polu **Stare hasło**.
2. Wpisz nowe hasło w polach **Nowe hasło** i **Potwierdź hasło**.
3. Kliknij przycisk **OK**.

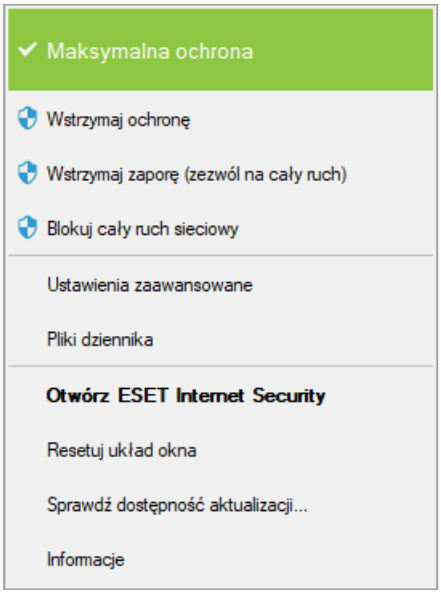
To hasło będzie wymagane podczas modyfikowania ustawień programu ESET Internet Security w przyszłości.

Jeżeli nie pamiętasz hasła, dostęp do ustawień zaawansowanych można przywrócić przy użyciu metody „Przywróć hasło”.

Aby odzyskać utracony klucz licencyjny ESET, sprawdzić datę wygaśnięcia licencji lub inne informacje na temat licencji produktu ESET Internet Security, zapoznaj się z naszym artykułem bazy wiedzy.

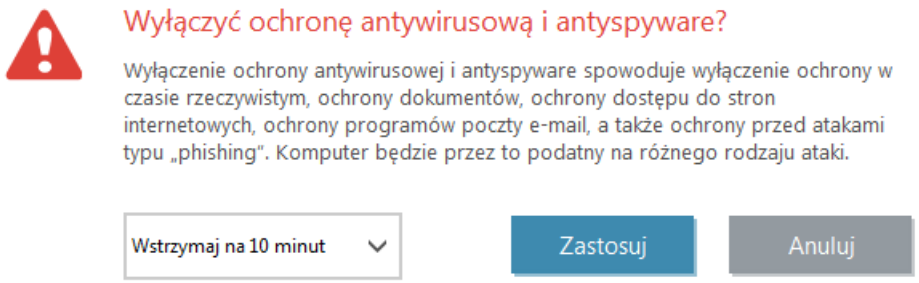
Ikona na pasku zadań

Dostęp do części najważniejszych opcji konfiguracji oraz funkcji można uzyskać po kliknięciu prawym przyciskiem myszy ikony na pasku zadań .



Wstrzymaj ochronę — powoduje wyświetlenie okna dialogowego potwierdzenia, które umożliwia wyłączenie silnika detekcji chroniącego przed złośliwymi atakami na system przez kontrolowanie komunikacji dotyczącej plików, stron internetowych i poczty e-mail.

Menu rozwijane **Przedział czasowy** pozwala wybrać okres, w trakcie którego ochrona 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**. Można je otworzyć również w inny sposób: naciskając klawisz F5 lub klikając kolejno opcje **Ustawienia** > **Ustawienia zaawansowane**.

Pliki dziennika — pliki dziennika zawierają informacje o ważnych zdarzeniach, jakie miały miejsce w programie, oraz udostępniają zestawienie wykrytych zagrożeń.

Otwórz program ESET Internet Security — powoduje otwarcie głównego okna programu ESET Internet Security z poziomu ikony na pasku zadań.

Zresetuj układ okien — umożliwia przywrócenie domyślnych wymiarów i położenia okna programu ESET Internet Security.

Sprawdź dostępne aktualizacje — umożliwia uruchomienie aktualizacji silnika detekcji (wcześniejsza nazwa to baza 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 Internet Security i zainstalowanych modułach programu. Można tu również znaleźć datę wygaśnięcia licencji oraz informacje na temat systemu operacyjnego i zasobów systemowych.

Obsługa czytnika ekranu

Produktu ESET Internet Security można używać razem z czytnikami ekranu, aby umożliwić użytkownikom programu ESET z zaburzeniami wzroku poruszanie się po produkcie lub skonfigurowanie ustawień. Obsługiwane są następujące czytniki ekranu (JAWS, NVDA, Narrator).

Aby upewnić się, że oprogramowanie czytnika ekranu może poprawnie uzyskać dostęp do interfejsu graficznego programu ESET Internet Security, postępuj zgodnie z instrukcjami zawartymi w naszym artykule Bazy wiedzy.

Pomoc i obsługa

Program ESET Internet Security udostępnia narzędzia i informacje ułatwiające rozwiązywanie problemów, które można napotkać.

Licencja

- **Rozwiązywanie problemów z licencjami** — kliknij to łącze, aby znaleźć rozwiązania problemów z aktywacją lub zmianą licencji.
- **Zmień licencję**— powoduje otwarcie okna aktywacji, gdzie można aktywować produkt. Jeśli urządzenie jest połączone z kontem ESET HOME, wybierz licencję z konta ESET HOME lub dodaj nową.

Zainstalowany produkt

- **Nowości** — kliknij tę opcję, aby otworzyć okno informacyjne o nowych i ulepszonych funkcjach.
- **Informacje o programie ESET Internet Security** — informacje na temat danego egzemplarza programu ESET Internet Security.
- **Rozwiązywanie problemów z produktem** — kliknij to łącze, aby znaleźć rozwiązania najczęściej występujących problemów.
- **Zmień produkt** — po kliknięciu tego łącza można sprawdzić, czy przy użyciu bieżącej licencji program ESET Internet Security można zmienić na inną linię produktów.

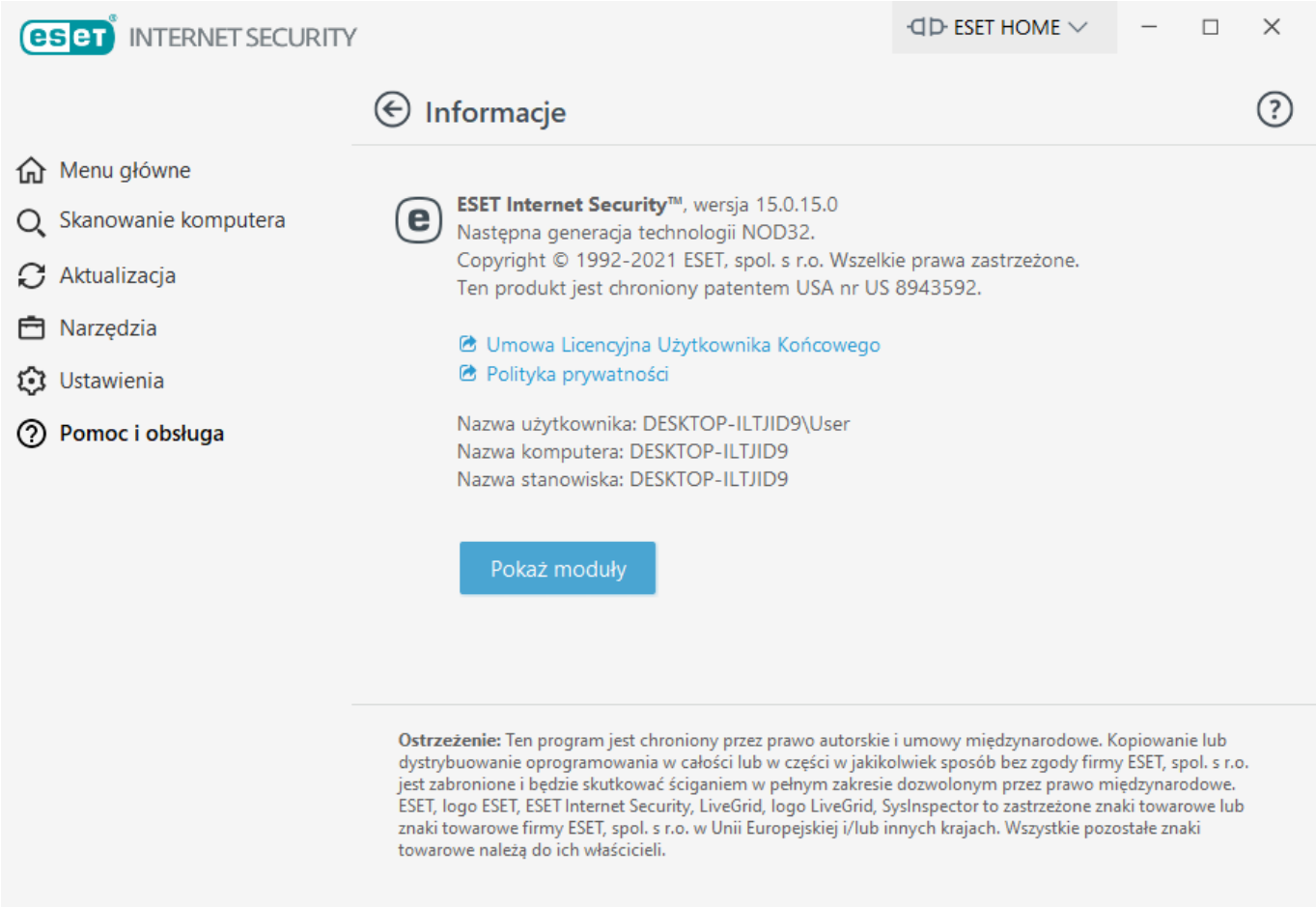
Strona Pomocy — kliknięcie tego łącza powoduje otwarcie stron pomocy programu ESET Internet Security.

Pomoc techniczna

— Baza wiedzy zawiera odpowiedzi na często zadawane pytania oraz zalecane rozwiązania różnych problemów. Dzięki regularnym aktualizacjom przez specjalistów z firmy ESET baza wiedzy jest bardzo skutecznym narzędziem do rozwiązywania różnych problemów.

Informacje o programie ESET Internet Security

To okno zawiera szczegółowe informacje o zainstalowanej wersji ESET Internet Security i komputerze.



Kliknij przycisk **Pokaż moduły**, aby wyświetlić informacje o liście załadowanych modułów programu.

- Informacje o modułach można skopiować do schowka, klikając opcję **Kopiuj**. Może to być przydatne podczas rozwiązywania problemów lub podczas kontaktowania się z pomocą techniczną.

- Kliknij opcję **Silnik detekcji** w oknie Moduły, aby otworzyć radar ESET Virus, który zawiera informacje o każdej wersji silnika detekcji programu ESET.

Aktualności ESET

W tym oknie program ESET Internet Security regularnie wyświetla aktualności firmy ESET.

komunikaty w ramach produktu to wiadomości związane z firmą ESET oraz inne informacje przeznaczone dla użytkowników. Wysyłanie wiadomości marketingowych wymaga zgody użytkownika. W związku z tym wiadomości marketingowe nie są wysyłane do użytkownika domyślnie (wyświetlany jest znak zapytania). Włączenie tej opcji oznacza zgodę na otrzymywanie wiadomości marketingowych od firmy ESET. Jeżeli nie chcesz **otrzymywać materiałów marketingowych od firmy ESET**, wyłącz tę opcję.

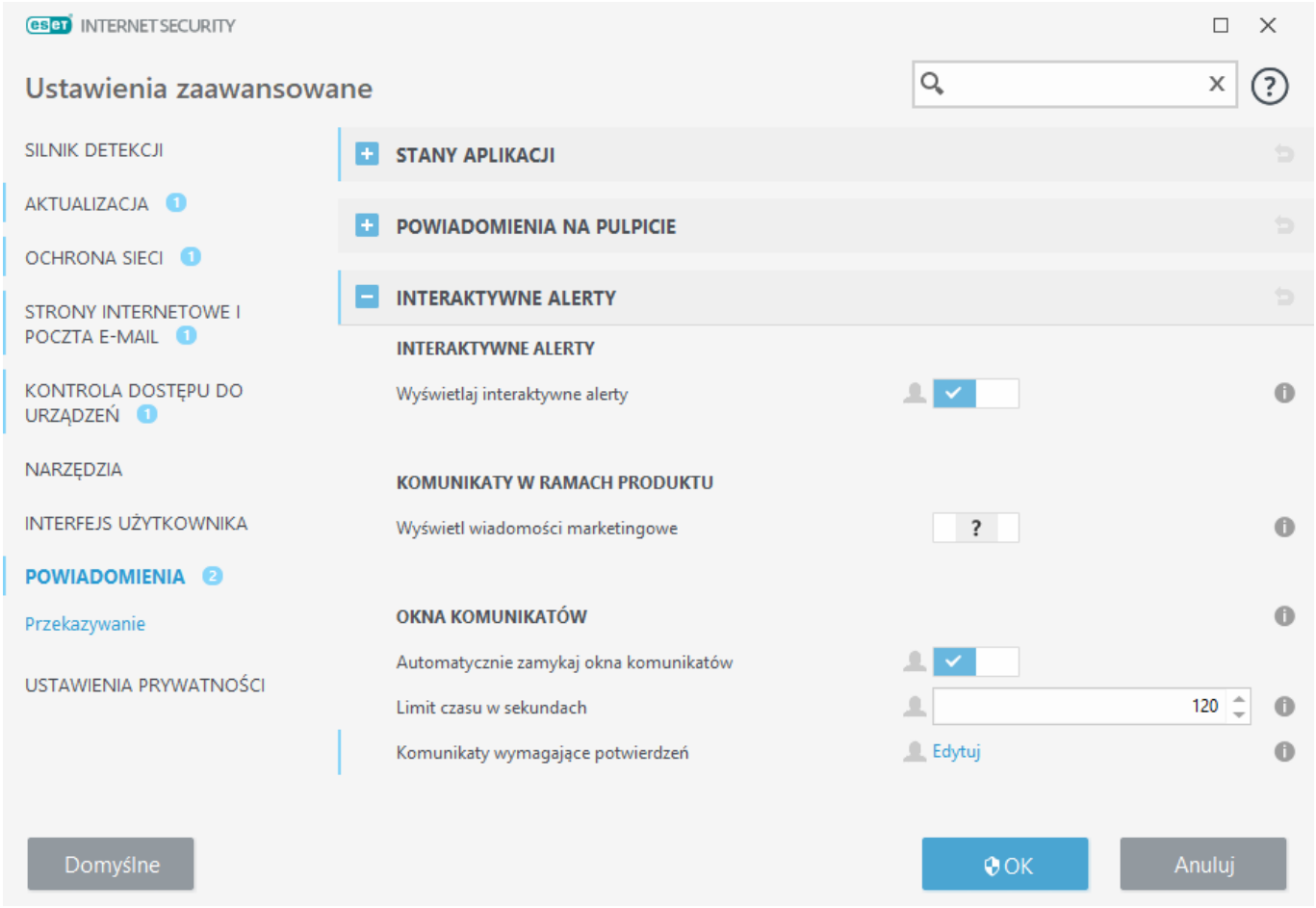
Aby włączyć lub wyłączyć otrzymywanie wiadomości marketingowych w wyskakującym oknie, postępuj zgodnie z poniższymi instrukcjami.

1. Otwórz główne okno produktu ESET.

2. Naciśnij klawisz **F5**, by uzyskać dostęp do menu **Ustawienia zaawansowane**.

3. Kliknij **Powiadomienia** > **Interaktywne alerty**.

4. Skonfiguruj opcję **Wyświetl wiadomości marketingowe**.



Przesyłanie danych konfiguracji systemu

Aby zapewnić użytkownikom pomoc w jak najszybszy i jak najprecyzyjniejszy sposób, firma ESET wymaga podania informacji dotyczących konfiguracji programu ESET Internet Security, szczegółowych informacji dotyczących systemu oraz uruchomionych procesów (plik dziennika programu ESET SysInspector) oraz danych rejestru. Te dane zostaną wykorzystane przez firmę ESET wyłącznie w celu zapewnienia klientowi pomocy technicznej.

Wraz z formularzem internetowym do firmy ESET zostaną przesłane także dane konfiguracyjne systemu. Aby zapamiętać tę czynność w ramach tego procesu, zaznacz opcję **Zawsze przesyłaj te informacje**. Aby przesłać formularz bez przesyłania jakichkolwiek danych, kliknij opcję **Nie przesyłaj informacji**. Można wówczas skontaktować się z działem pomocy technicznej firmy ESET przy użyciu formularza internetowego.

To ustawienie można również skonfigurować w obszarze **Ustawienia zaawansowane** > **Narzędzia** > **Diagnostyka** > Pomoc techniczna.

Jeśli użytkownik zdecydował się przesłać dane systemowe, konieczne jest wypełnienie i przesłanie formularza internetowego, gdyż w przeciwnym razie nie zostanie utworzony bilet i dane systemowe zostaną utracone.

Pomoc techniczna

W głównym oknie programu kliknij pozycję **Pomoc i obsługa** > **Pomoc techniczna**.

Kontakt z działem pomocy technicznej

Poproś o pomoc techniczną — jeśli nie możesz znaleźć odpowiedzi na problem, możesz użyć tego formularza dostępnego w witrynie firmy ESET, aby szybko skontaktować się z działem pomocy technicznej firmy ESET. W zależności od ustawień przed wypełnieniem formularza internetowego może zostać wyświetlone okno umożliwiające przesłanie danych konfiguracji systemu.

Dostarcz informacje działowi pomocy technicznej

Szczegóły dla działu pomocy technicznej — gdy zostanie wyświetlony monit, można skopiować i wysłać informacje do działu pomocy technicznej firmy ESET (na przykład informacje o licencji, nazwie i wersji produktu, systemie operacyjnym i informacje na temat komputera).

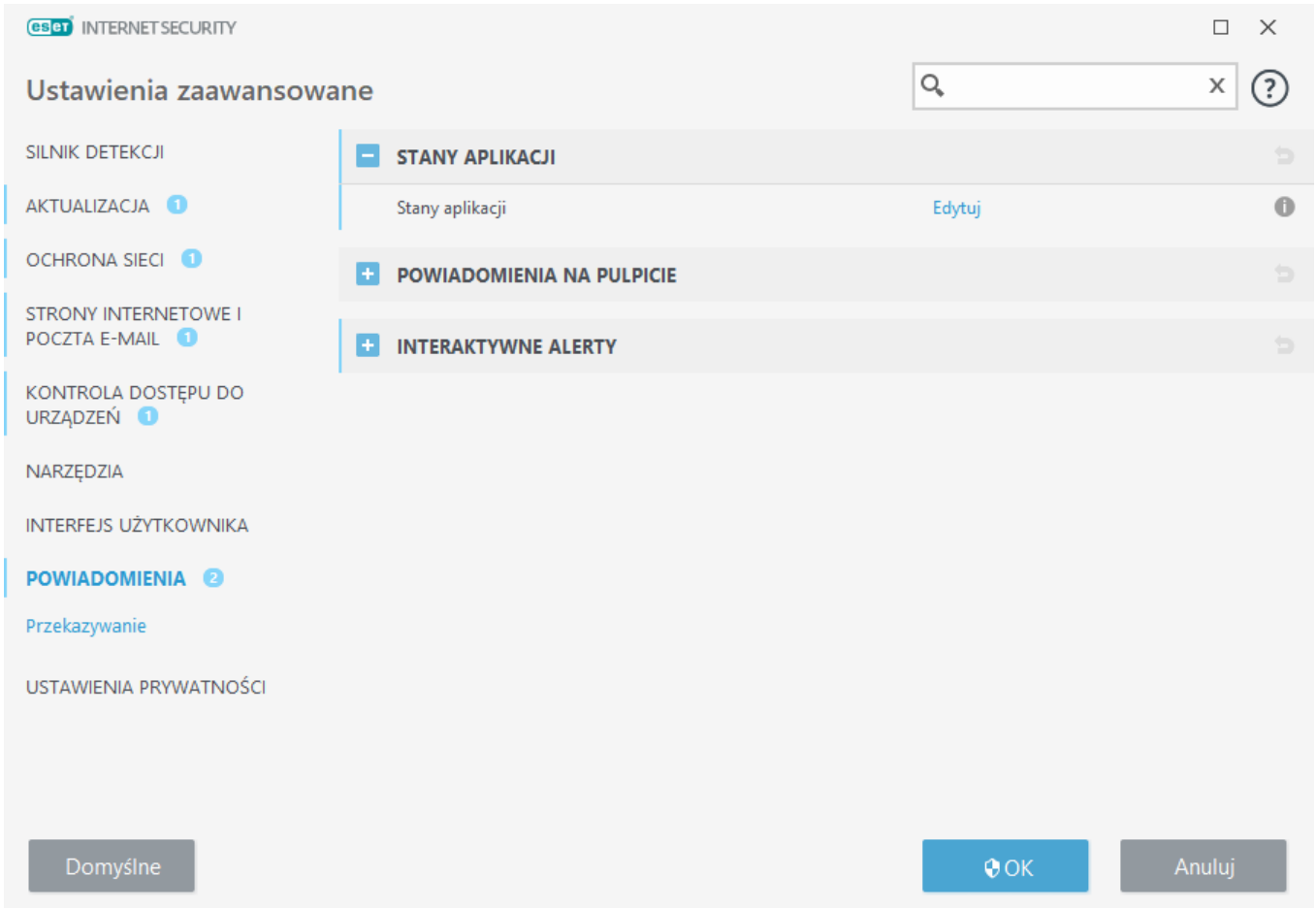
ESET Log Collector — łącze do artykułu bazy wiedzy firmy ESET z narzędziem ESET Log Collector, które automatycznie gromadzi informacje i dzienniki z komputera, aby usprawnić rozwiązywanie problemów. Więcej informacji zawiera instrukcja obsługi online narzędzia ESET Log Collector.

Kliknij pozycję **Włącz zaawansowane zapisywanie w dzienniku**, aby utworzyć zaawansowane dzienniki wszystkich funkcji, co pomoże programistom w diagnozowaniu i rozwiązywaniu problemów. Minimalna szczegółowość zapisów w dzienniku jest ustawiona na poziomie **Diagnostycznym**. Zaawansowane zapisywanie w dzienniku zostanie wyłączone po dwóch godzinach, chyba że zatrzyma się je wcześniej, klikając pozycję **Zatrzymaj zaawansowane zapisywanie w dzienniku**. Po utworzeniu wszystkich dzienników zostanie wyświetlone okno z powiadomieniem umożliwiające bezpośredni dostęp do folderu diagnostycznego z utworzonymi dziennikami.

Powiadomienia

Aby zarządzać powiadomieniami programu ESET Internet Security, otwórz **Ustawienia zaawansowane** (F5) > **Powiadomienia**. Można skonfigurować następujące typy powiadomień:

- Statusy aplikacji — Powiadomienia wyświetlane w sekcji głównej głównego okna programu.
- Powiadomienia na pulpicie — małe wyskakujące okienka obok systemowego paska zadań.
- Alerty interaktywne — okna alertów i okna komunikatów wymagające interakcji z użytkownikiem.
- Przekazywanie (powiadomienia e-mail)— powiadomienia e-mail są wysyłane na podany adres e-mail.



Stany aplikacji

Statusy aplikacji — kliknij przycisk **Edytuj**, aby wybrać, które stany aplikacji będą wyświetlane w sekcji głównej głównego okna programu.

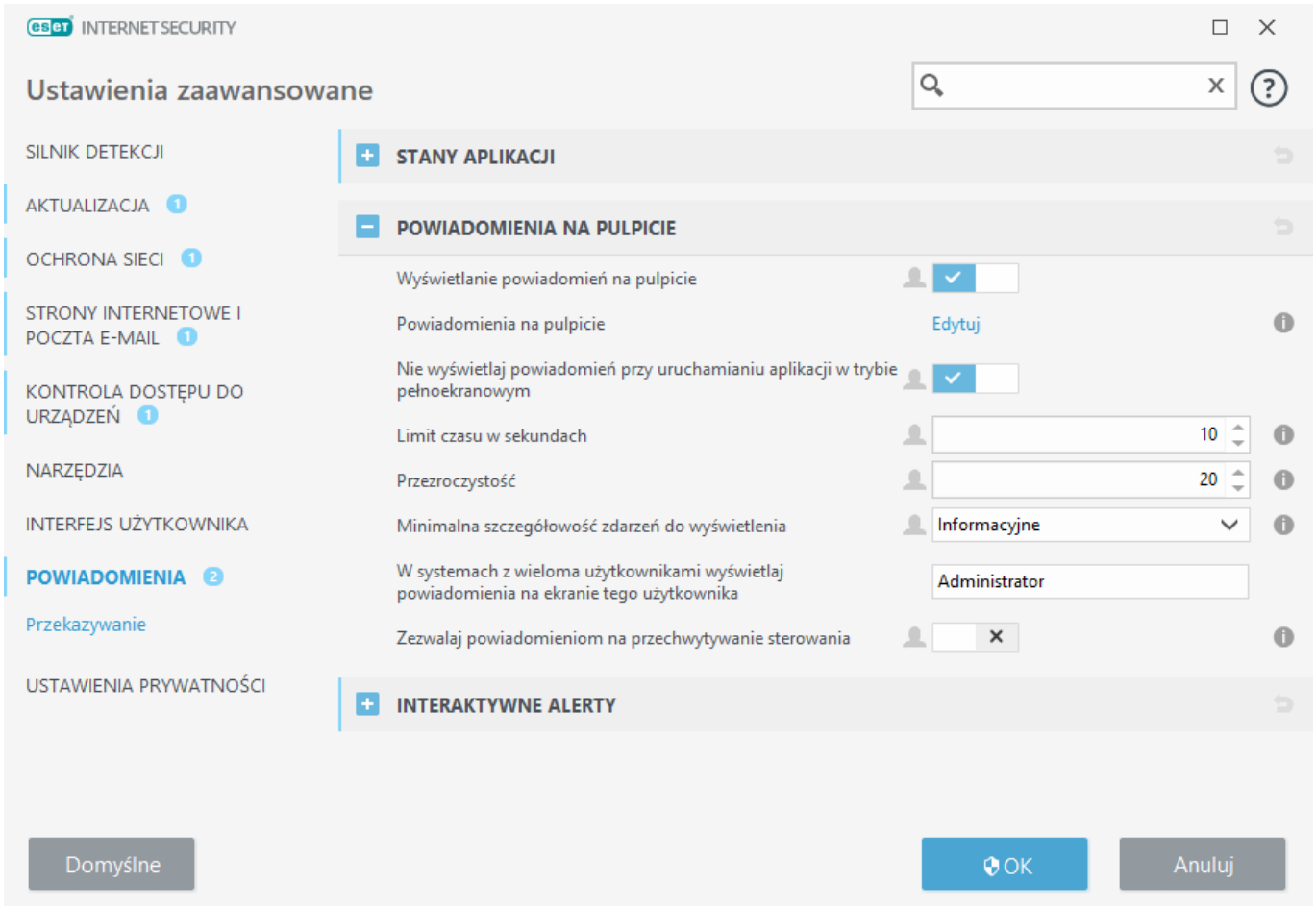
Okno dialogowe — Stany aplikacji

W tym oknie dialogowym można wybrać, które stany aplikacji będą wyświetlane. Na przykład po wstrzymaniu ochrony antywirusowej i antyspyware lub włączeniu trybu gier.

Stan aplikacji zostanie również wyświetlony, jeśli produkt nie został aktywowany lub licencja wygasła.

Powiadomienia na pulpicie

Powiadomienia na pulpicie znajdują się w małym, wyskakującym okienku wyświetlanym obok paska zadań systemu. Domyślnie jest ono widoczne przez 10 sekund, a następnie powoli zanika. Powiadomienia zawierają informacje o pomyślnych aktualizacjach produktu, połączeniu z nowymi urządzeniami, ukończeniu skanowania antywirusowego lub znalezieniu nowego zagrożenia.



Wyświetlaj powiadomienia na pulpicie — zalecamy włączenie tej opcji, aby produkt mógł informować o wystąpieniu nowego zdarzenia.

Powiadomienia na pulpicie — kliknij **Edytuj**, aby włączyć lub wyłączyć wybrane Powiadomienia na pulpicie.

Nie wyświetlaj powiadomień przy uruchamianiu aplikacji w trybie pełnoekranowym — pomijaj wszystkie nieinteraktywne powiadomienia podczas uruchamiania aplikacji w trybie pełnoekranowym.

Limit czasu w sekundach — ustaw czas widoczności powiadomień. Wartość musi wynosić od 3 do 30 sekund.

Przezroczystość — ustaw procent przezroczystości powiadomień. Obsługiwany zakres wynosi od 0 (brak przezroczystości) do 80 (bardzo wysoka przezroczystość).

Minimalna szczegółowość zdarzeń do wyświetlenia — ustaw początkowy poziom ważności powiadomienia, które będzie wyświetlane. Z menu rozwijanego wybierz jedną z następujących opcji:

- **Diagnostyczne** — wyświetla informacje potrzebne do ulepszania konfiguracji programu, a także wszystkich rekordów wyższych kategorii.
- **Informacyjne** — wyświetla komunikaty informacyjne, takie jak niestandardowe zdarzenia sieciowe, w tym powiadomienia o pomyślnych aktualizacjach, a także wszystkie rekordy wyższych kategorii.
- **Ostrzeżenia** — wyświetla komunikaty ostrzegawcze, błędy i błędy krytyczne (na przykład program Antistealth nie działa poprawnie lub aktualizacja nie powiodła się).
- **Błędy** — wyświetla błędy (na przykład nie uruchomiono ochrony dokumentów) i błędy krytyczne.

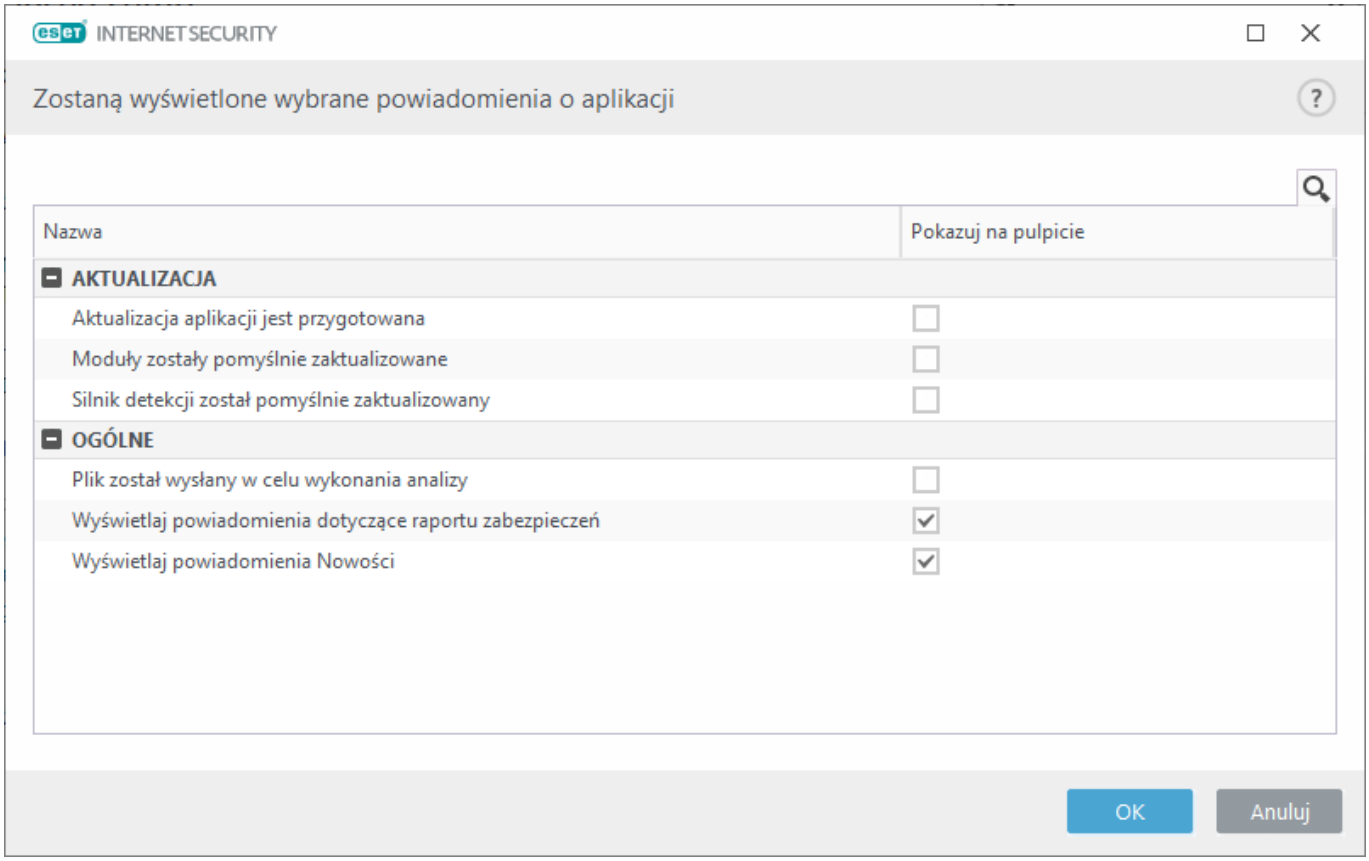
- **Krytyczne** — wyświetla tylko błędy krytyczne (np. błąd uruchomienia ochrony antywirusowej lub zainfekowanie systemu).

W systemach z wieloma użytkownikami wyświetlaj powiadomienia na ekranie następującego użytkownika — umożliwia wyświetlanie powiadomień na pulpicie tylko wybranemu kontu. Na przykład jeśli posiadasz konto Administratora, wpisz pełną nazwę konta i otrzymuj powiadomienia o nowych zdarzeniach dotyczących produktu. Tylko jedno konto użytkownika może otrzymywać powiadomienia na pulpicie.

Zezwalaj na ustawianie ostrości na powiadomieniu — umożliwia ustawianie ostrości na powiadomieniu; powiadomienia są dostępne w menu **ALT + Tab.**

Lista powiadomień na pulpicie

Aby dostosować widoczność powiadomień na pulpicie (wyświetlanych w prawym dolnym rogu ekranu), otwórz **Ustawienia zaawansowane** (F5) > **Powiadomienia** > **Powiadomienia na pulpicie**. Kliknij przycisk **Edytuj** obok pozycji **Powiadomienia na pulpicie** i zaznacz odpowiednie pole wyboru **Pokaż**.



Ogólne

Wyświetlaj powiadomienia dotyczące raportu zabezpieczeń — otrzymuj powiadomienie o wygenerowaniu nowego raportu zabezpieczeń.

Wyświetlaj powiadomienia o nowościach — otrzymuj powiadomienia o nowych i usprawnionych funkcjach najnowszej wersji produktu.

Plik został wysłany w celu wykonania analizy — otrzymuj powiadomienie za każdym razem, gdy ESET Internet Security wysyła plik do analizy.

Aktualizacja

Aktualizacja aplikacji jest przygotowana — otrzymuj powiadomienie, gdy dostępna jest aktualizacja do nowej wersji ESET Internet Security.

Silnik detekcji został pomyślnie zaktualizowany — otrzymuj powiadomienie o aktualizacji modułów silnika detekcji produktu.

Moduły zostały pomyślnie zaktualizowane — otrzymuj powiadomienie o aktualizacji składników programu.

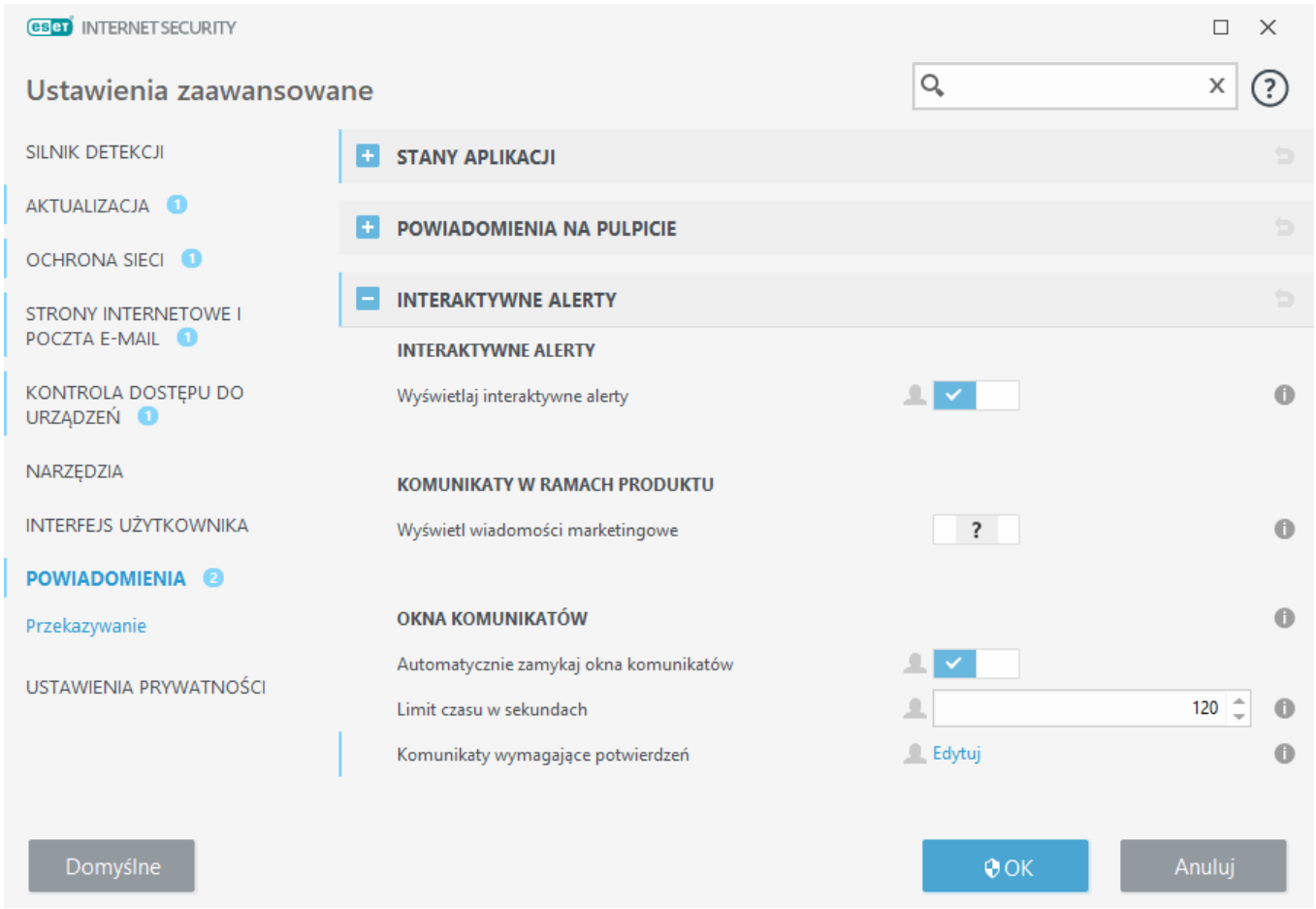
Aby skonfigurować ogólne ustawienia powiadomień na pulpicie, na przykład czas wyświetlania powiadomienia lub minimalną szczegółowość zdarzeń do wyświetlenia, przejdź do sekcji Powiadomienia na pulpicie w obszarze **Ustawienia zaawansowane** (F5) > **Powiadomienia**.

Interaktywne alerty

Szukasz informacju o typowych alertach i powiadomieniach?

- Znaleziono zagrożenie.
- Adres został zablokowany
- Produkt nie został aktywowany
- Zmiana na produkt o większej ilości funkcjonalności
- Zmień na produkt o ograniczonej ilości funkcji
- Aktualizacja jest dostępna
- Informacje dotyczące aktualizacji nie są spójne
- Rozwiązywanie problemów związanych z komunikatem „Aktualizacja modułów nie powiodła się”
- Rozwiązywanie problemów z aktualizacjami modułów
- Zablokowane zagrożenie sieciowe
- Certyfikat witryny został odwołany

Alerty interaktywne w sekcji **Powiadomienia o ustawieniach zaawansowanych** (F5) > umożliwia skonfigurowanie sposobu obsługi okien komunikatów i interaktywnych alertów dotyczących wykrycia, w których użytkownik musi podjąć decyzję (na przykład o potencjalnej witrynie wyłudzającej informacje) w programie ESET Internet Security.



Interaktywne alerty

Wyłączenie opcji **Wyświetlaj interaktywne alerty** spowoduje ukrycie wszystkich okien alertów i jest zalecane jedynie w specyficznych sytuacjach. ESET zaleca pozostawienie ustawienia domyślnego tej opcji (włączona).

Komunikaty w ramach produktu

komunikaty w ramach produktu to wiadomości związane z firmą ESET oraz inne informacje przeznaczone dla użytkowników. Wysyłanie wiadomości marketingowych wymaga zgody użytkownika. W związku z tym wiadomości marketingowe nie są wysyłane do użytkownika domyślnie (wyświetlany jest znak zapytania). Włączenie tej opcji oznacza zgodę na otrzymywanie wiadomości marketingowych od firmy ESET. Jeżeli nie chcesz **otrzymywać materiałów marketingowych od firmy ESET**, wyłącz tę opcję.

Okna komunikatów

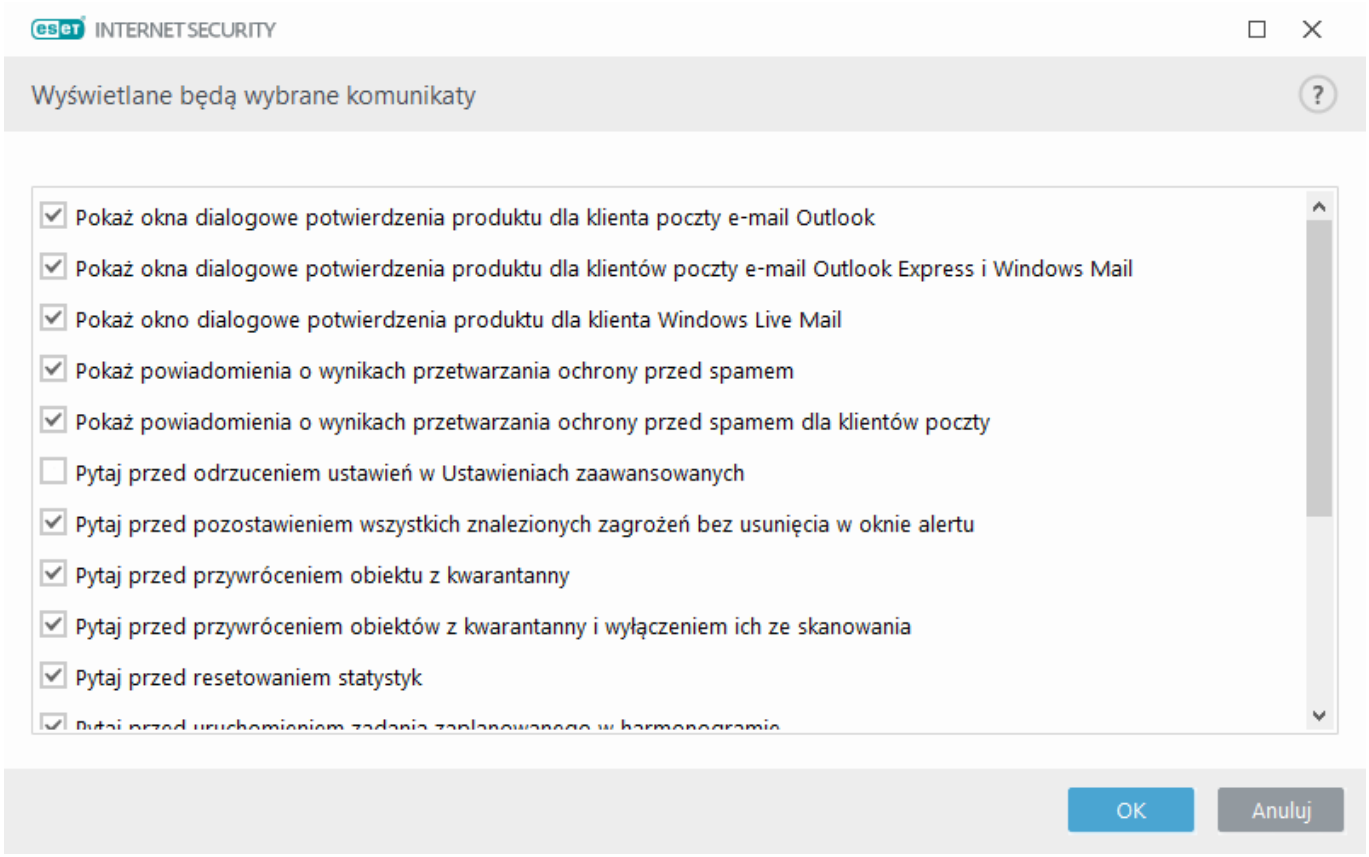
Aby wyskakujące okna były automatycznie zamykane po upływie określonego czasu, należy zaznaczyć opcję **Automatycznie zamykaj okna komunikatów**. Jeśli użytkownik nie zamknie okna alertu ręcznie, zostanie ono zamknięte automatycznie po upływie określonego czasu.

Limit czasu w sekundach — ustaw czas widoczności powiadomień. Wartość musi wynosić od 10 do 999 sekund.

Komunikaty potwierdzające — kliknij **Edytuj**, aby wyświetlić listy komunikatów wymagających potwierdzenia, z których można wybrać elementy do wyświetlenia.

Komunikaty wymagające potwierdzeń

Aby dostosować komunikaty wymagające potwierdzeń, przejdź do menu **Ustawienia zaawansowane** (F5) > **Powiadomienia** > **Interaktywne alerty** i kliknij opcję **Edytuj** obok pozycji **Komunikaty potwierdzające**.



To okno dialogowe wyświetla Komunikaty wymagające potwierdzeń, które program ESET Internet Security wyświetla przed wykonaniem każdego działania. Zaznacz lub odznacz pole wyboru obok każdego z komunikatów potwierdzeń, by go włączyć lub wyłączyć.

Dowiedz się więcej o konkretnej funkcji związanej z komunikatami potwierdzającymi:

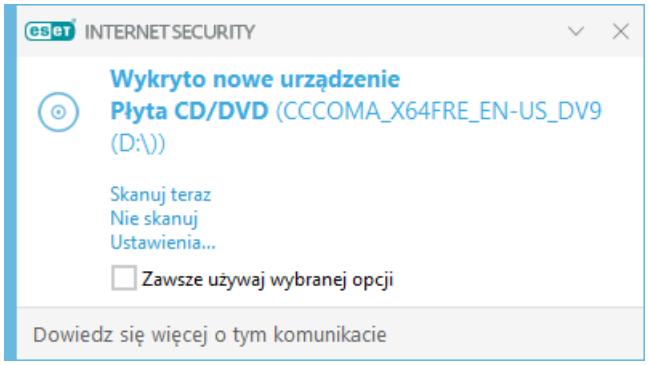
- Pytaj przed usunięciem zapiszu w dzienniku programu ESET SysInspector
- Pytaj przed usunięciem wszystkich dzienników programu ESET SysInspector
- Pytaj przed usunięciem obiektu z kwarantanny
- Pytaj przed odrzuceniem ustawień w Ustawieniach zaawansowanych
- Pytaj przed pozostawieniem wszystkich znalezionych zagrożeń bez usunięcia w oknie alertu
- Pytaj przed usunięciem zapiszu w dziennik
- Pytaj przed usunięciem zadania zaplanowanego w harmonogramie
- Pytaj przed usunięciem wszystkich rekordów dziennika
- Pytaj przed resetowaniem statystyk

- Pytaj przed przywróceniem obiektu z kwarantanny
- Pytaj przed przywróceniem obiektów z kwarantanny i wyłączeniem ich ze skanowania
- Pytaj przed uruchomieniem zadania zaplanowanego w harmonogramie
- Pokaż powiadomienia o wynikach przetwarzania ochrony przed spamem
- Pokaż powiadomienia o wynikach przetwarzania ochrony przed spamem dla klientów poczty
- Pokaż okna dialogowe potwierdzenia produktu dla klientów poczty e-mail Outlook Express i Windows Mail
- Pokaż okno dialogowe potwierdzenia produktu dla klienta Windows Live Mail
- Pokaż okna dialogowe potwierdzenia produktu dla klienta poczty e-mail Outlook

Nośniki wymienne

Program ESET Internet Security udostępnia funkcję automatycznego skanowania nośników wymiennych (CD, DVD, USB i innych) po ich włożeniu do komputera. Dzięki temu administrator komputera może uniemożliwić użytkownikom korzystanie z nośników wymiennych z niepożądaną zawartością.

Jeśli w ustawieniach programu ESET Internet Security włączono opcję **Pokaż opcje skanowania**, po włożeniu nośnika wymiennego pojawi się następujące okno dialogowe:



Opcje dostępne w tym oknie:

- **Skanuj teraz** — powoduje rozpoczęcie skanowania nośnika wymiennego.
- **Nie skanuj** — nośniki wymienne nie będą skanowane.
- **Ustawienia** — powoduje otwarcie sekcji **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 Internet 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.

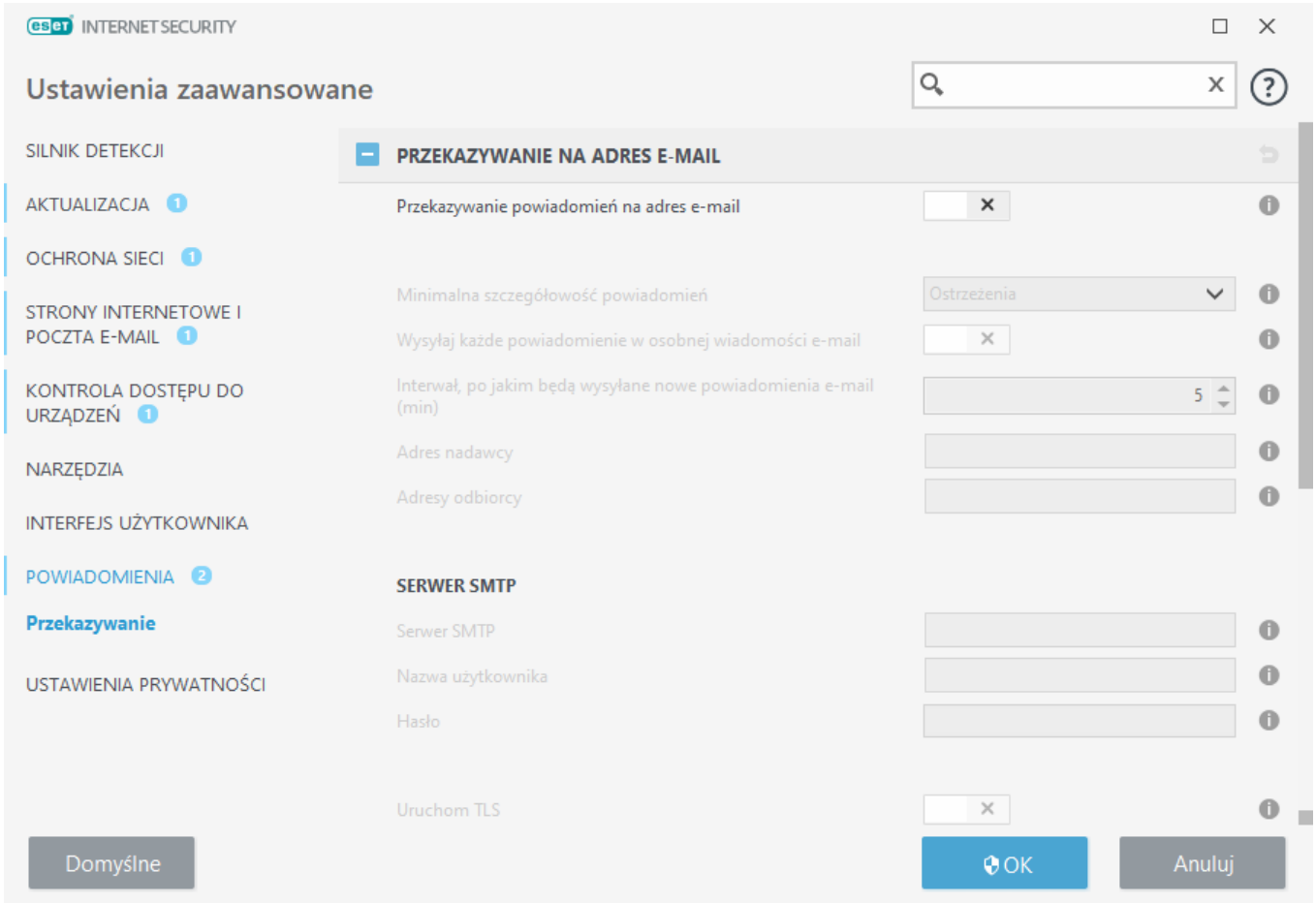
Aby zmienić ustawienia skanowania nośników wymiennych, otwórz Ustawienia zaawansowane (**F5**) > **Silnik detekcji** > **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Nośniki wymienne**.

Czynność do wykonania po włożeniu nośnika wymiennego — umożliwia wybór domyślnej czynności, która zostanie wykonana po włożeniu do komputera nośnika wymiennego (CD/DVD/USB). Wybierz czynność:

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

Przekazywanie

ESET Internet Security może automatycznie wysyłać e-maile z powiadomieniami, jeśli wystąpi zdarzenie o wybranym poziomie szczegółowości. Otwórz okno **Ustawienia zaawansowane** (F5) > **Powiadomienia** > **Przekazywanie powiadomień** > i włącz opcję **Przekazywanie powiadomień na adres e-mail**, aby aktywować powiadomienia e-mail.



Z menu rozwijanego **Minimalna szczegółowość powiadomień** można wybrać początkowy stopień ważności powiadomień, które będą wysyłane.

• **Diagnostyczne** — rejestrowanie informacji potrzebnych do ulepszania 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** — rejestruje tylko błędy krytyczne (na przykład „Błąd uruchomienia ochrony antywirusowej” lub „Znaleziono zagrożenie”).

Wysyłaj każde powiadomienie w osobnej wiadomości e-mail — po włączeniu tej opcji odbiorca będzie otrzymywał osobną wiadomość e-mail z każdym powiadomieniem. Może to spowodować odebranie znacznej liczby wiadomości e-mail w krótkim czasie.

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.

Adres nadawcy — w tym polu można określić adres nadawcy, który będzie wyświetlany w nagłówkach wiadomości e-mail z powiadomieniami.

Adresy odbiorców — w tym polu można określić adresy odbiorców, które będą wyświetlane w nagłówkach wiadomości e-mail z powiadomieniami. Można dodać wiele wartości. Używając średnika jako separatora.

Serwer SMTP

Serwer **SMTP** — serwer SMTP używany do wysyłania powiadomień (na przykład smtp.provider.com:587; wstępnie zdefiniowany port to 25).

> Serwery SMTP z szyfrowaniem TLS są obsługiwane przez program ESET Internet 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.

Uruchom TLS — Secure Alert i wiadomości z powiadomieniami przy użyciu szyfrowania TLS.

Testuj połączenie SMTP — na adres e-mail odbiorcy zostanie wysłana testowa wiadomość e-mail. Należy podać następujące informacje: serwer SMTP, nazwa użytkownika, hasło, adres nadawcy, adres odbiorcy.

Format wiadomości

Komunikacja między programem a zdalnym użytkownikiem lub administratorem systemu odbywa się za pomocą wiadomości e-mail lub powiadomień rozsyłanych w sieci LAN (za pośrednictwem usługi wiadomości błyskawicznych systemu Windows). **Domyślny format alertów i powiadomień** będzie w większości przypadków optymalny. Może się jednak zdarzyć, że konieczna będzie zmiana formatu wiadomości o zdarzeniu.

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. ESET nie zaleca wprowadzania zmian w tym zakresie tego formatu. W pewnych okolicznościach (takich jak korzystanie z automatycznego systemu przetwarzania poczty) zmiana formatu może być jednak konieczna.

Zestaw znaków — przekształca wiadomość e-mail na postać kodowaną znakami ANSI z uwzględnieniem ustawień regionalnych systemu Windows — na przykład windows-1250, Unicode (UTF-8), ACSII 7-bit lub japońskiego (ISO-2022-JP). W wyniku tych działań "á" zostanie zamienione na "a", a nieznane symbole na "?".

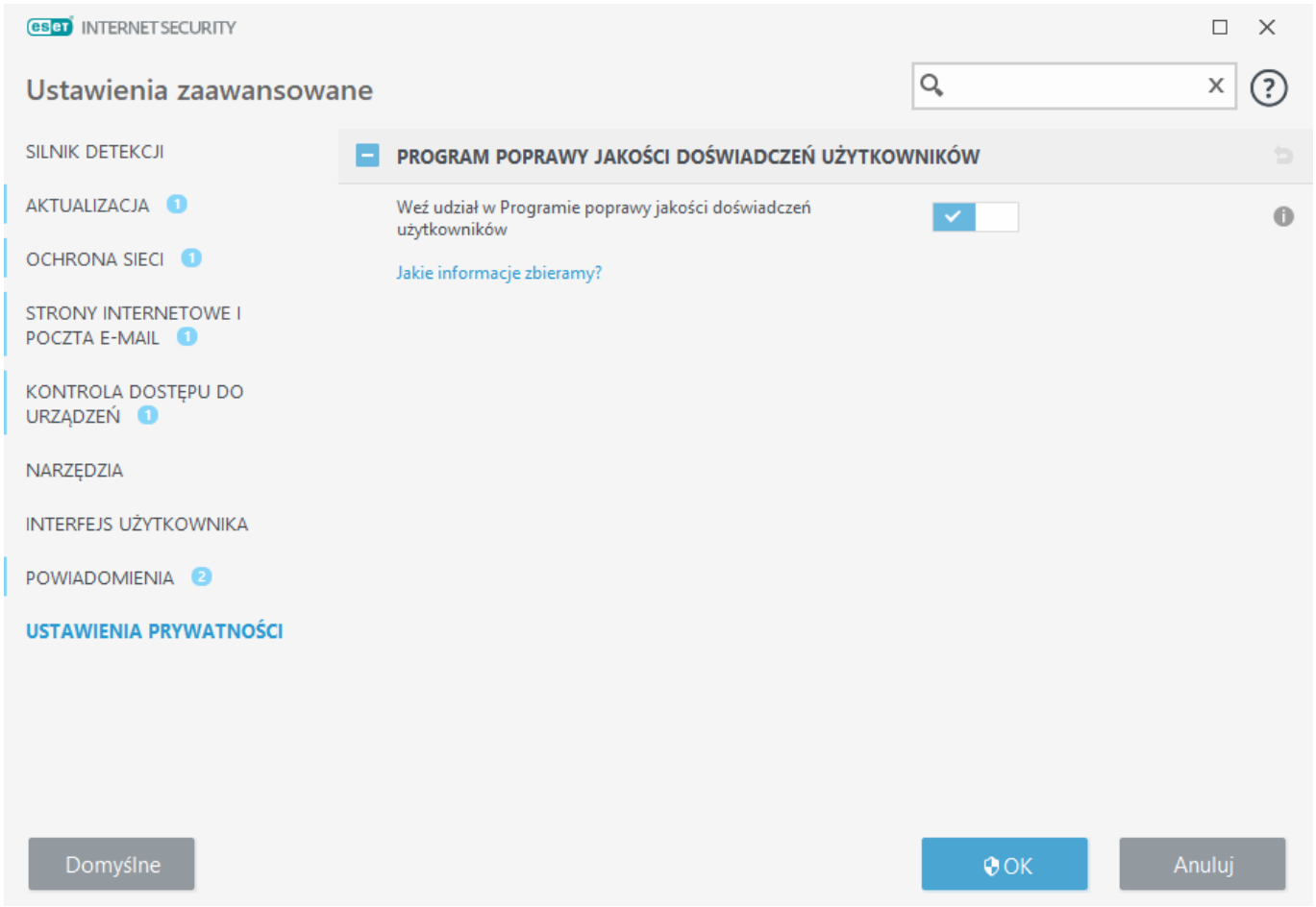
Użyj kodowania Quoted-printable — źródło wiadomości e-mail zostanie zakodowane w formacie Quoted-printable (QP), w którym są stosowane znaki ASCII oraz jest obsługiwane prawidłowe przekazywanie w wiadomościach e-mail specjalnych znaków narodowych w formacie 8-bitowym (ąćęłńóśźż).

- **%TimeStamp%** — data i godzina wystąpienia zdarzenia
- **%Scanner%** — moduł, którego dotyczy zdarzenie
- **%ComputerName%** — nazwa komputera, na którym wystąpił alert
- **%ProgramName%** — program, który wygenerował alert
- **%InfectedObject%** — nazwa zainfekowanego pliku, wiadomości itp.
- **%VirusName%** — identyfikacja infekcji
- **%Action%** — czynność wykonywana po wykryciu infekcji
- **%ErrorDescription%** — opis zdarzenia niezwiązanego z wirusem

Słowa kluczowe **%InfectedObject%** i **%VirusName%** są używane tylko w wiadomościach ostrzegających o zagrożeniach, a słowo kluczowe **%ErrorDescription%** — tylko w wiadomościach o zdarzeniach.

Ustawienia prywatności

W oknie głównym programu kliknij **Ustawienia** > **Ustawienia zaawansowane** (F5) > **Ustawienia prywatności**.



Program poprawy jakości doświadczeń użytkowników

Włącz suwak obok pozycji **Weź udział w Programie poprawy jakości doświadczeń użytkowników**, aby dołączyć do Programu poprawy jakości doświadczeń użytkowników. Dołączając, użytkownik przekazuje firmie ESET anonimowe informacje dotyczące korzystania z produktów firmy ESET. Zebrane dane pomogą nam poprawić Twoje wrażenia nigdy i nie będą udostępniane stronom trzecim. Jakie informacje zbieramy?

Profile

Menedżer profili jest używany w dwóch sekcjach programu ESET Internet Security: **Skanowanie komputera na żądanie** oraz **Aktualizacja**.

Skanowanie komputera

Istnieją 4 wstępnie zdefiniowane profile skanowania w ESET Internet Security:

- **Skanowanie inteligentne** – Jest to podstawowy zaawansowany profil skanowania. Skanowanie inteligentne korzysta z technologii Smart Optimization wykluczającej pliki oznaczone w poprzednim skanowaniu jako czyste, które dodatkowo nie zostały zmodyfikowane od czasu poprzedniego skanowania. Pozwala to skrócić czas skanowania z minimalnym wpływem na bezpieczeństwo systemu.

- **Skanowanie z poziomu skrótu w menu kontekstowym** – Możesz rozpocząć skanowanie na żądanie dowolnego pliku z menu kontekstowego. Profil skanowania menu kontekstowego umożliwia zdefiniowanie konfiguracji skanowania, która będzie używana podczas tego rodzaju skanowania.

- **Skanowanie dokładne** – Profil skanowania dokładnego domyślnie nie korzysta z funkcji Inteligentna optymalizacja, więc podczas używania tego profilu żadne pliki nie są wyłączane ze skanowania.

- **Skanowanie komputera** – Jest to domyślny profil używany w standardowym skanowaniu komputera.

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, otwórz okno Ustawienia zaawansowane (F5) i kliknij kolejno pozycje **Silnik detekcji** > **Skanowanie szkodliwego oprogramowania** > **Skanowanie na żądanie** > **Lista profili**. W oknie **Menedżer profili** wyświetlane jest menu rozwijane **Wybrany profil** z listą istniejących już profili skanowania oraz opcja umożliwiająca utworzenie nowego profilu. 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.

> Załóżmy, że chcesz utworzyć własny profil skanowania, a żądana konfiguracja częściowo pokrywa się z konfiguracją **Skanowanie komputera**, jednak nie chcesz skanować programów spakowanych ani potencjalnie niebezpiecznych aplikacji, za to chcesz zastosować ustawienie **Zawsze naprawiaj wykrycie**. 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.

Profil aktualizacji — obecnie używany profil aktualizacji. Aby go zmienić, należy wybrać inny profil z menu rozwijanego.

Lista profili — możliwość tworzenia nowych lub usuwania istniejących profili aktualizacji.

Skróty klawiszowe

Aby usprawnić nawigację w produkcie ESET Internet Security, można skorzystać z następujących skrótów klawiaturowych:

Skróty klawiaturowe	Czynność
F1	Otwieranie stron pomocy.
F5	Otwieranie ustawień zaawansowanych.
Strzałka w górę / Strzałka w dół	nawigacja w elementach menu rozwijanego

Skróty klawiaturowe	Czynność
TAB	przechodzenie do następnego elementu GUI w oknie
Shift+TAB	przechodzenie do poprzedniego elementu GUI w oknie
ESC	Zamykanie aktywnego okna dialogowego.
Ctrl+U	Wyświetlanie informacji o licencji ESET i komputerze (szczegółowe informacje dla działu pomocy technicznej).
Ctrl+R	Przywrócenie domyślnych wymiarów i położenia okna na ekranie
ALT + Strzałka w lewo	nawiguj do tyłu
ALT + Strzałka w prawo	nawiguj do przodu
ALT+Home	nawiguj do strony głównej

Do nawigacji można również używać przycisków myszy do tyłu lub do przodu.

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 ESET Internet Security problemów.

Należy kliknąć menu rozwijane dostępne obok pozycji **Typ zrzutu** i wybrać jedną z trzech dostępnych opcji:

- **Wyłącz** — wybranie tej opcji powoduje wyłączenie tej funkcji.

- **Mini** (domyślne) — 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.

Katalog docelowy — katalog, w którym po wystąpieniu awarii zostanie zapisany zrzut pamięci.

Otwórz folder diagnostyki — aby otworzyć ten katalog w nowym oknie *Eksploratora Windows*, kliknij przycisk **Otwórz**.

Utwórz zrzut diagnostyczny — aby utworzyć zrzut diagnostyczny w **katalogu docelowym**, kliknij opcję **Utwórz**.

Zaawansowane zapisywanie w dzienniku

Włącz zaawansowane zapisywanie w dzienniku dla wiadomości marketingowych — rejestruj wszystkie zdarzenia związane z wiadomościami marketingowymi w produkcie.

Włącz zaawansowane zapisywanie informacji w dziennikach dla aparatu Antispam — umożliwia rejestrowanie wszystkich zdarzeń występujących podczas skanowania pod kątem spamu. Może to pomóc programistom w diagnozowaniu i rozwiązywaniu problemów z aparatem ochrony przed spamem firmy ESET.

Włącz zaawansowane funkcje dziennika silnika Anti-theft — umożliwia rejestrowanie wszystkich zdarzeń funkcji Anti-Theft do celów diagnostyki i rozwiązywania problemów.

Włącz zaawansowane zapisywanie w dzienniku dla funkcji Ochrona bankowości internetowej — rejestruj wszystkie zdarzenia występujące w ochronie bankowości internetowej.

Włącz zaawansowane rejestrowanie przy skanowaniu komputera przy skanowaniu komputera — umożliwia rejestrowanie zdarzeń występujących podczas skanowania plików i folderów przez funkcję skanowania komputera.

Włącz zaawansowane rejestrowanie kontroli dostępu do urządzeń — umożliwia rejestrowanie wszystkich zdarzeń dotyczących kontroli dostępu do urządzeń. Może to pomóc programistom w diagnozowaniu i rozwiązywaniu problemów z kontrolą dostępu do urządzeń.

Włącz zaawansowane zapisywanie w dzienniku dla serwerów bezpośrednio w chmurze – rejestruj wszystkie zdarzenia występujące w ESET LiveGrid®. Może to pomóc programistom w diagnozowaniu i rozwiązywaniu problemów związanych z ESET LiveGrid®.

Włącz zaawansowane zapisywanie w dzienniku dla ochrony dokumentów — rejestruje wszystkie zdarzenia dotyczące funkcji Ochrona dokumentów, aby umożliwić diagnozowanie i rozwiązywanie problemów.

Włącz zaawansowane zapisywanie w dzienniku ochrony programów poczty e-mail — umożliwia rejestrowanie wszystkich zdarzeń w zakresie ochrony programów poczty e-mail i dodatku poczty e-mail, aby umożliwić diagnozowanie i rozwiązywanie problemów.

Włącz zaawansowane zapisywanie dotyczące jądra — rejestrowanie wszystkich zdarzeń występujących w jądrze ESET (ekrn).

Włącz zaawansowane rejestrowanie licencji — umożliwia rejestrowanie całej komunikacji produktu z serwerami aktywacji ESET lub ESET License Manager.

Włącz śledzenie pamięci – zapisuj wszystkie zdarzenia, które pomogą programistom zdiagnozować wycieki pamięci.

Włącz zaawansowane rejestrowanie ochrony sieci — umożliwia rejestrowanie wszystkich danych sieciowych przesyłanych przez zaporę w formacie PCAP. Pomaga to programistom w diagnozowaniu i rozwiązywaniu problemów z zaporą.

Włącz zaawansowane funkcje dziennika systemu operacyjnego — zapisuj dodatkowe informacje na temat systemu operacyjnego, na przykład dotyczące uruchomionych procesów, aktywności procesora i działania dysku. Mogą one pomóc programistom w diagnozowaniu i rozwiązywaniu problemów dotyczących produktów ESET działających w danym systemie operacyjnym.

Włącz zaawansowane funkcje dziennika kontroli rodzicielskiej — umożliwia rejestrowanie wszystkich zdarzeń dotyczących kontroli rodzicielskiej. Może to pomóc programistom w diagnozowaniu i rozwiązywaniu problemów z kontrolą rodzicielską.

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.

Włącz zaawansowane rejestrowanie wiadomości push — rejestruj wszystkie zdarzenia występujące podczas przesyłania wiadomości.

Włącz zaawansowane zapisywanie w dzienniku dla ochrony systemu plików w czasie rzeczywistym — umożliwia rejestrowanie zdarzeń występujących podczas skanowania plików i folderów przez funkcję Ochrona systemu plików w czasie rzeczywistym.

Włącz zaawansowane zapisywanie informacji w dziennikach dla aparatu aktualizacji — umożliwia rejestrowanie wszystkich zdarzeń występujących podczas procesu aktualizacji. Może to pomóc programistom w diagnozowaniu i rozwiązywaniu problemów związanych z aparatem aktualizacji.

Pliki dziennika znajdują się w pliku *C:\ProgramData\ESET\ESET Security\Diagnostics*.

Pomoc techniczna

Podczas kontaktowania się z pomocą techniczną firmy ESET z poziomu produktu ESET Internet Security można przesyłać dane konfiguracyjne systemu. Wybierz opcję **Zawsze przesyłaj** z menu rozwijanego **Przesyłanie danych konfiguracji systemu**, aby automatycznie przesłać dane, lub wybierz opcję **Zapytaj przed przesłaniem**, aby zostać zobaczyć monit o pozwolenie przed przesłaniem danych.

Import i eksport ustawień

Dostosowany plik konfiguracyjny .xml programu ESET Internet Security można importować i eksportować za pośrednictwem menu **Ustawienia**.

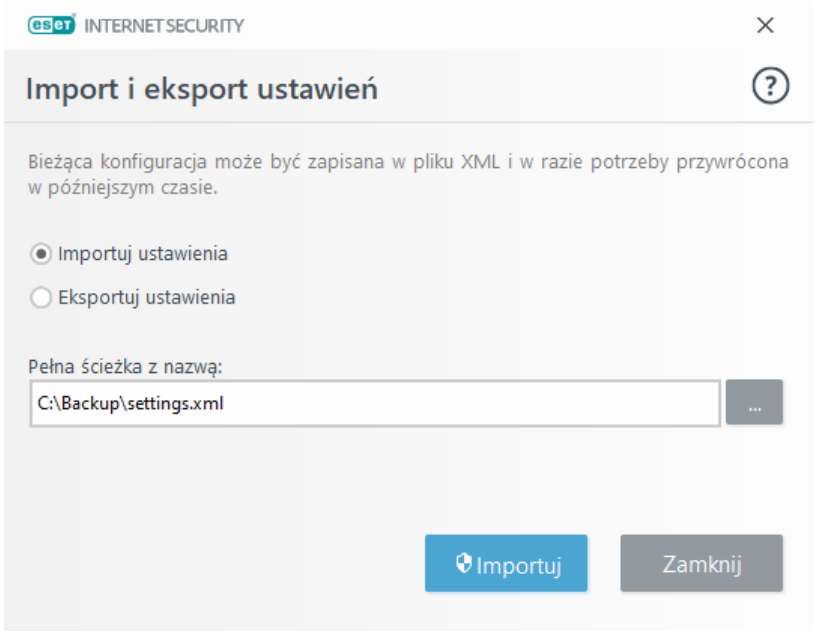
> **Ilustrowane instrukcje**
> Patrz Importowanie lub eksportowanie ustawień konfiguracyjnych ESET przy użyciu pliku .xml, aby wyświetlić ilustrowane instrukcje dostępne w języku angielskim i kilku innych językach.

Importowanie i eksportowanie plików konfiguracyjnych przydaje się, jeśli trzeba wykonać kopię zapasową bieżącej konfiguracji programu ESET Internet Security do użycia w późniejszym terminie. Funkcja eksportu ustawień jest również pomocna, gdy chcesz używać preferowanej konfiguracji na wielu komputerach. Ustawienia można łatwo przenieść, importując je z pliku .xml.

Aby zaimportować konfigurację, 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.

Aby wyeksportować konfigurację, w głównym oknie programu kliknij **Ustawienia** > **Importuj/eksportuj ustawienia**. Wybierz opcję **Eksportuj ustawienia** i wpisz pełną ścieżkę pliku z nazwą. Kliknij **...**, aby przejść do lokalizacji na komputerze w celu zapisania pliku konfiguracyjnego.

> Przy eksportowaniu ustawień może pojawić się błąd, jeśli nie masz wystarczających uprawnień do zapisania eksportowanego pliku w określonym katalogu.



Przywracanie wszystkich ustawień w bieżącej sekcji

Aby przywrócić wszystkim ustawieniom w bieżącej sekcji wartości domyślne zdefiniowane przez ESET, należy kliknąć zakrzywioną strzałkę .

Należy pamiętać, że w przypadku kliknięcia opcji **Przywróć domyślne** wszelkie wprowadzone zmiany zostaną utracone.

Przywróć zawartość tabel — po włączeniu tej opcji reguły, zadania oraz profile, które zostały dodane ręcznie lub automatycznie zostaną utracone.

Zobacz też Importowanie i eksportowanie ustawień.

Przywróć ustawienia domyślne

Aby przywrócić wszystkie ustawienia programu w każdym z modułów, należy kliknąć opcję **Domyślne** w obszarze **Ustawienia zaawansowane** (F5). Zostaną przywrócone wartości ustawień, które obowiązywały bezpośrednio po instalacji.

Zobacz też Importowanie i eksportowanie ustawień.

Błąd podczas zapisywania konfiguracji

Ten komunikat o błędzie informuje, że ustawienia nie zostały zapisane poprawnie z powodu błędu.

Zwykle oznacza on, że użytkownik, który próbował zmodyfikować parametry programu:

- ma niewystarczające uprawnienia dostępu lub nie ma niezbędnych uprawnień w systemie operacyjnym i nie może modyfikować plików konfiguracyjnych ani rejestru systemu.
  > W celu wprowadzenia odpowiednich modyfikacji musi zalogować się administrator systemu.

- włączył ostatnio tryb uczenia się w systemie HIPS lub zaporze i próbował zmodyfikować ustawienia

zaawansowane.
> Aby zapisać konfigurację i uniknąć konfliktów konfiguracji, zamknij obszar Ustawienia zaawansowane bez zapisywania i spróbuj ponownie wprowadzić wymagane zmiany.

Drugą najpopularniejszą przyczyną jest nieprawidłowe działanie programu lub jego uszkodzenie. Ten problem można rozwiązać, ponownie instalując program.

Skaner wiersza polecenia

Moduł antywirusowy programu ESET Internet Security można uruchomić z poziomu wiersza polecenia — ręcznie (polecenie „ecls”) lub za pomocą pliku wsadowego (bat).

Posługiwanie się skanerem ESET uruchamianym z wiersza poleceń:

```
ecls [OPTIONS..] FILES..
```

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=MASK	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-exclude=ROZSZERZENIA	Wyłącz ze skanowania ROZSZERZENIA plików oddzielone dwukropkami

/clean-mode=TRYB	używaj TRYBU leczenia zainfekowanych obiektów Dostępne są następujące opcje: • `none` (domyślne) — nie nastąpi automatyczne leczenie. • `standard` — 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

Kody zakończenia o wartości wyższej niż 100 oznaczają, że plik nie został przeskanowany i dlatego może być zainfekowany.

Funkcja poleceń ESET CMD

Ta funkcja pozwala używać zaawansowanych poleceń ecmd. Umożliwia ona eksportowanie i importowanie ustawień za pomocą wiersza polecenia (ecmd.exe). Dotychczas eksportowanie ustawień było możliwe tylko przy użyciu graficznego interfejsu użytkownika. Konfigurację programu ESET Internet Security można wyeksportować do pliku *.xml*.

Po włączeniu funkcji poleceń ESET CMD dostępne są dwie metody autoryzacji:

- **Brak** — brak autoryzacji. Nie zalecamy tej metody, ponieważ umożliwia ona importowanie niepodpisanych konfiguracji. Stanowi to potencjalne ryzyko.

- **Hasło do ustawień zaawansowanych** — hasło wymagane w celu zaimportowania konfiguracji z pliku .xml. Plik musi być podpisany (informacje o podpisywaniu plików konfiguracyjnych .xml znajdują się poniżej).

Przed zaimportowaniem nowej konfiguracji należy podać hasło określone w sekcji Ustawienia dostępu. Jeśli nie włączono ustawień dostępu, hasło nie jest zgodne lub plik konfiguracji .xml nie jest podpisany, konfiguracja nie zostanie zaimportowana.

Po włączeniu funkcji ESET CMD można importować i eksportować konfiguracje programu ESET Internet Security przy użyciu wiersza polecenia. Eksportowanie/importowanie można przeprowadzać ręcznie. Można też utworzyć skrypt automatyzujący te operacje.

Można też otworzyć wiersz polecenia systemu Windows (cmd) przy użyciu opcji **Uruchom jako administrator**. W przeciwnym razie zostanie wyświetlony komunikat **Error executing command**. Podczas eksportowania konfiguracji musi także istnieć folder docelowy. Polecenie eksportowania działa nawet przy wyłączonym ustawieniu ESET CMD.

Polecenie eksportowania ustawień:
`ecmd /getcfg c:\config\settings.xml`

Polecenie importowania ustawień:
`ecmd /setcfg c:\config\settings.xml`

Zaawansowane polecenia ecmd można uruchamiać tylko lokalnie.

Podpisywanie pliku konfiguracyjnego *.xml*:

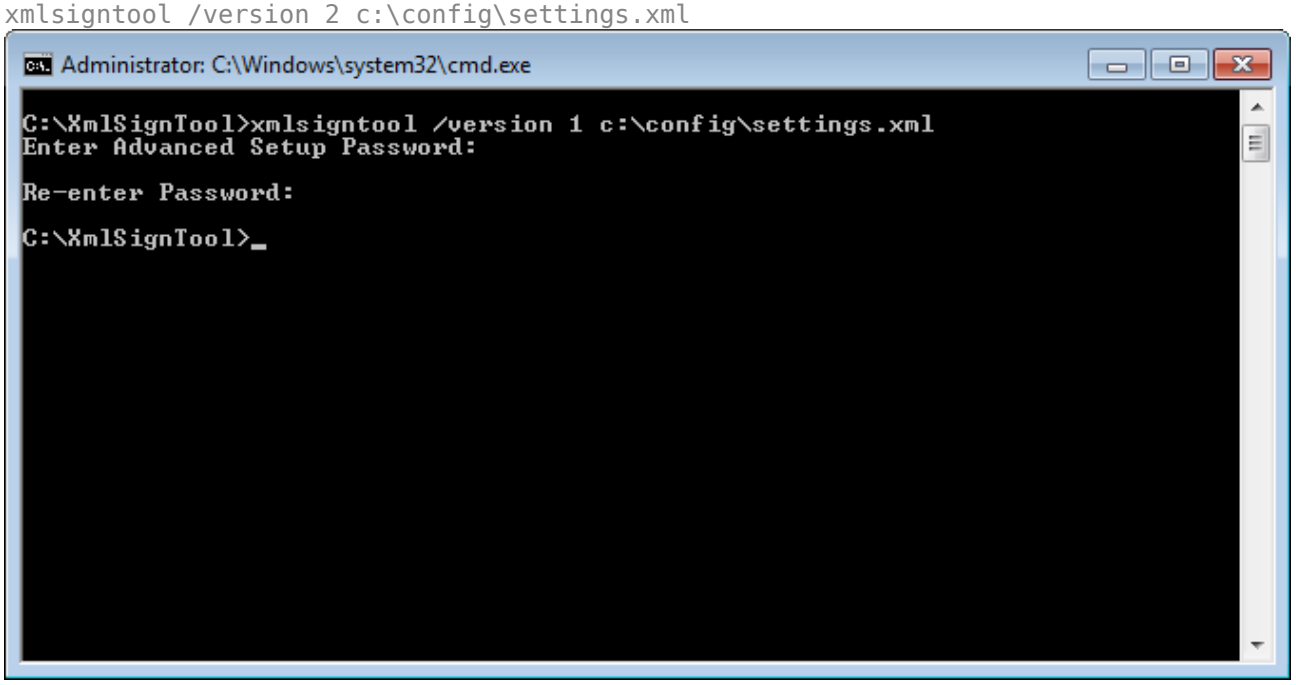
1. Pobierz plik wykonywalny narzędzia XmlSignTool.
2. Otwórz wiersz polecenia systemu Windows (cmd) przy użyciu opcji **Uruchom jako administrator**.
3. Przejdź do lokalizacji zapisywania pliku `xmlsigntool.exe`.
4. Wykonaj polecenie, aby podpisać plik konfiguracyjny *.xml*. Składnia: `xmlsigntool /version 1|2 <xml_file_path>`

Wartość parametru `/version` zależy od wersji produktu ESET Internet Security. W przypadku wersji programu ESET Internet Security wcześniejszych niż 11.1 użyj parametru `/version 1`. W przypadku aktualnej wersji programu ESET Internet Security użyj parametru `/version 2`.

5. Po wyświetleniu monitu przez narzędzie XmlSignTool wprowadź hasło z sekcji Ustawienia zaawansowane i je potwierdź. Po wykonaniu tych czynności plik konfiguracyjny *.xml* zostanie podpisany i będzie można go zaimportować w innym wystąpieniu programu ESET Internet Security za pomocą funkcji ESET CMD z użyciem metody autoryzacji hasłem.

Polecenie podpisania wyeksportowanego pliku konfiguracyjnego:

```
xmlsigntool /version 2 c:\config\settings.xml
```



Jeśli hasło z sekcji Ustawienia dostępu zostanie zmienione, a wymagane jest zaimportowanie konfiguracji podpisanej wcześniej przy użyciu starego hasła, należy ponownie podpisać plik konfiguracyjny *.xml* przy użyciu nowego hasła. Umożliwia to korzystanie ze starszych plików konfiguracyjnych bez konieczności eksportowania ich na inny komputer z programem ESET Internet Security przed zaimportowaniem.

Używanie funkcji poleceń ESET CMD bez metody autoryzacji nie jest zalecane, ponieważ umożliwi to zaimportowanie niepodpisanych konfiguracji. Należy ustawić hasło zapobiegające nieupoważnionym modyfikacjom przez użytkowników. W tym celu należy wybrać kolejno opcje **Ustawienia zaawansowane** > **Interfejs użytkownika** > **Ustawienia dostępu**.

Wykrywanie stanu bezczynności

Ustawienia wykrywania stanu bezczynności można skonfigurować w obszarze **Ustawienia zaawansowane** po wybraniu kolejno opcji **Silnik detekcji** > **Skanowania w poszukiwaniu szkodliwego oprogramowania** > **Skanowanie w trakcie bezczynności** > **Wykrywanie stanu bezczynności**. Te ustawienia określają element wyzwalający funkcję Skanowanie w trakcie bezczynności:

- **Wyłączony ekran lub wygaszacz ekranu**
- **Blokada komputera**
- **Wylogowanie użytkownika**

Użyj suwaków dla poszczególnych stanów, aby włączyć lub wyłączyć różne elementy wywołujące wykrywanie stanu bezczynności.

Często zadawane pytania

Poniżej omówiono niektóre często zadawane pytania oraz typowe problemy. Aby poznać sposób rozwiązania danego problemu, należy kliknąć jeden z poniższych tematów:

- Aktualizowanie programu ESET Internet Security
- Usuwanie wirusa z komputera
- Zezwalanie na komunikację określonej aplikacji
- Włączanie kontroli rodzicielskiej na koncie
- Tworzenie nowego zadania w harmonogramie
- Planowanie cotygodniowego zadania skanowania
- Jak usunąć błąd „Nie można przekierować ochrony bankowości internetowej do żądanej strony internetowej”
- Odblokowywanie obszaru Ustawienia zaawansowane
- Jak rozwiązać dezaktywację produktu z ESET HOME

Jeśli dany problem nie jest uwzględniony na liście powyżej, można spróbować wyszukać informacje o nim w pomocy online ESET Internet Security.

Jeśli rozwiązania problemu/odpowiedzi na pytanie nie można znaleźć w pomocy online ESET Internet Security, można spróbować przeszukać regularnie aktualizowaną internetową Bazę wiedzy firmy ESET. Poniżej znajdują się linki do najbardziej popularnych artykułów w bazie wiedzy:

- Jak odnowić licencję?
- Podczas instalowania produktu ESET pojawił się błąd aktywacyjny. Co to oznacza?
- Aktywowanie produktu ESET dla domu działającego w systemie Windows przy użyciu nazwy użytkownika, hasła lub klucza licencyjnego
- Odinstalowywanie lub ponowne instalowanie produktu ESET dla domu
- Otrzymałem wiadomość, że instalacja ESET zakończyła się przedwcześnie
- Co mam zrobić po odnowieniu licencji? (Użytkownicy domowi)
- Co mam zrobić, gdy zmienię adres e-mail?
- Przenoszenie produktu firmy ESET na nowy komputer lub urządzenie
- Jak uruchomić Windows w trybie awaryjnym lub trybie awaryjnym z obsługą sieci
- Wyłączanie bezpiecznej strony internetowej z blokowania
- Umożliwianie czytnikom ekranu dostępu do graficznego interfejsu użytkownika programów ESET

W razie potrzeby można się skontaktować z naszym działem pomocy technicznej, aby zadać pytania lub zgłosić problemy.

Aktualizowanie programu ESET Internet Security

Aktualizowanie programu ESET Internet Security może się odbywać ręcznie lub automatycznie. Aby uruchomić proces aktualizacji, kliknij przycisk **Aktualizuj** w głównym oknie programu, a następnie kliknij pozycję **Sprawdź dostępne aktualizacje**.

W ramach domyślnych ustawień instalacji jest tworzone zadanie aktualizacji automatycznej wykonywane co godzinę. Aby zmienić odstęp czasu między aktualizacjami, przejdź do opcji **Narzędzia** > **Harmonogram**.

Usuwanie wirusa z komputera

Jeśli komputer wykazuje symptomy zainfekowania 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 komputera**, aby rozpocząć skanowanie systemu.

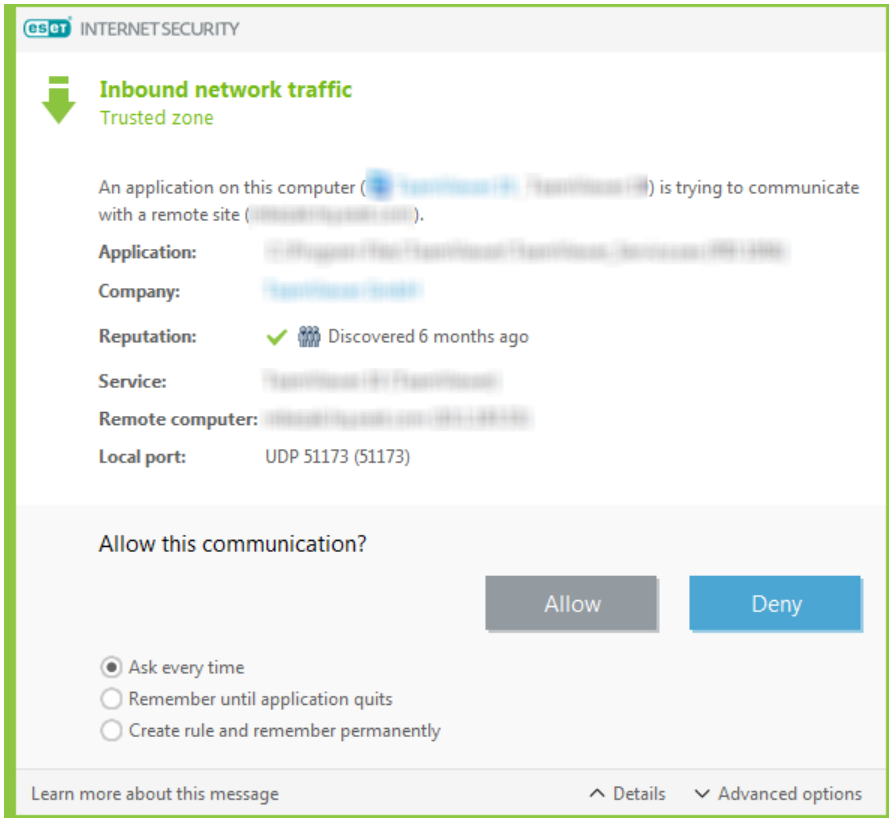
3. Po zakończeniu skanowania przejrzyj dziennik zawierający liczbę obiektów przeskanowanych, zainfekowanych i wyleczonych.

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.

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 Internet Security przy każdej próbie nawiązania połączenia, należy zaznaczyć pole wyboru **Utwórz regułę i zapamiętaj na stałe**.



Można utworzyć nowe reguły zapory dla aplikacji, zanim zostaną one wykryte przez ESET Internet Security. W oknie konfiguracji zapory otwórz główne okno programu > **Ustawienia** > **Ochrona sieci** > kliknij ikonę obok pozycji **Zapora** > **Konfiguruj**> **Zaawansowane** > **Reguły** > **Edytuj**.

Kliknij opcję **Dodaj**, a następnie na karcie **Ogólne** wprowadź 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.

Włączanie kontroli rodzicielskiej na koncie

Aby aktywować kontrolę rodzicielską na określonym koncie użytkownika, należy wykonać poniższe kroki:

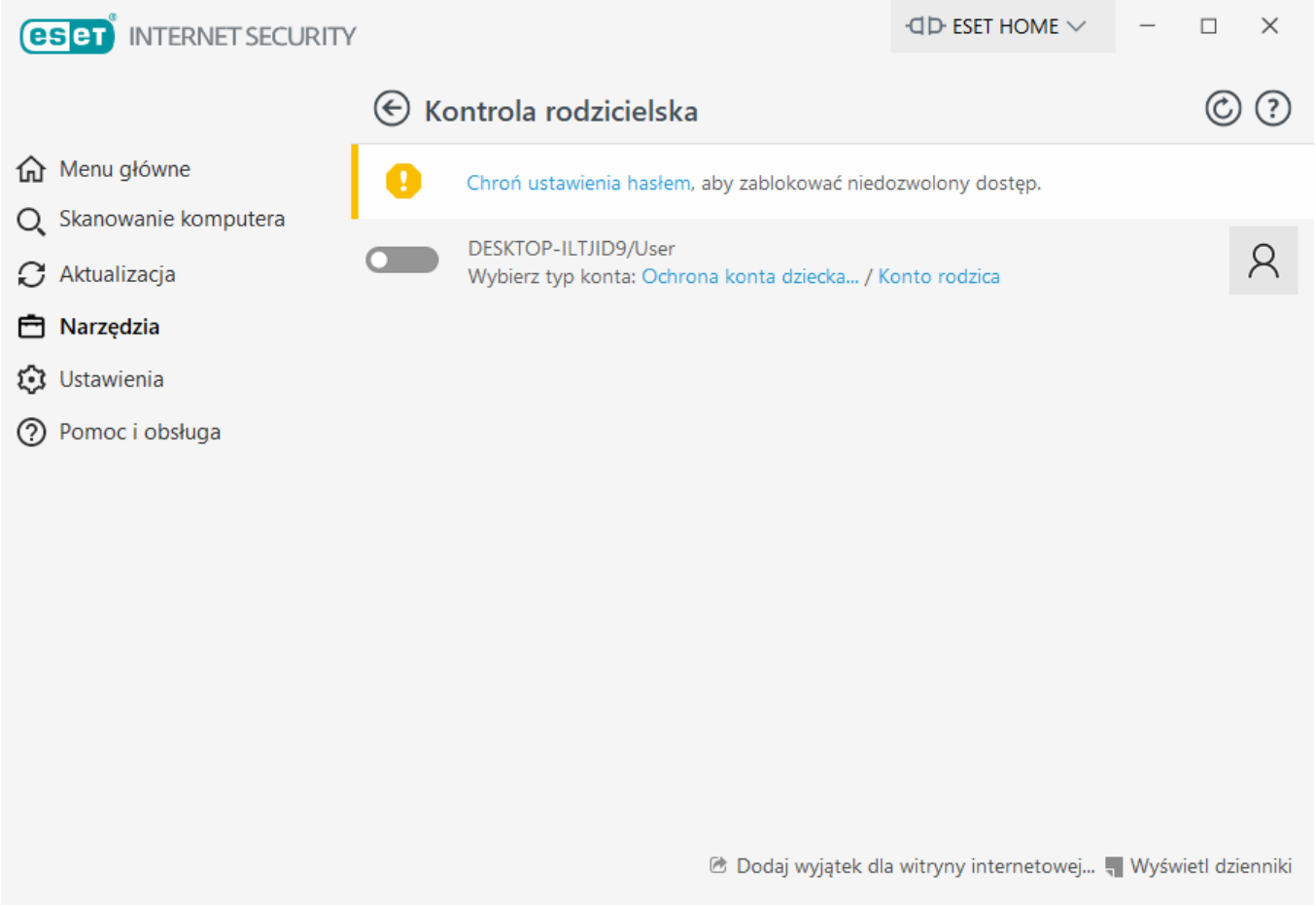
1. Domyślnie kontrola rodzicielska jest wyłączona w programie ESET Internet Security. Można ją włączyć na dwa sposoby:

   • Kliknij przełącznik po wybraniu kolejno opcji **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska** w głównym oknie programu i zmień stan opcji Kontrola rodzicielska na Włączona.

   • Naciśnij klawisz F5, aby przejść do drzewa **Ustawienia zaawansowane**, wybierz kolejno opcje **Strony internetowe i poczta e-mail** > **Kontrola rodzicielska**, a następnie przesuń suwak obok opcji **Włącz kontrolę rodzicielską**.

2. W głównym oknie programu kliknij kolejno opcje **Ustawienia** > **Narzędzia zabezpieczające** > **Kontrola rodzicielska**. Chociaż obok opcji **Kontrola rodzicielska** widnieje stan **Włączona**, należy skonfigurować kontrolę rodzicielską na danym koncie, klikając symbol strzałki, a w następnym oknie klikając pozycję **Chroń konto**

dziecka lub **Konto rodzica**. W następnym oknie należy wprowadzić datę urodzenia, aby określić poziom dostępu i zalecane strony internetowe odpowiednie do wieku. Kontrola rodzicielska zostanie włączona na określonym koncie użytkownika. Aby dostosować kategorie, które mają być dozwolone lub zablokowane na karcie Kategorie, kliknij pozycję **Blokowana zawartość i ustawienia** pod nazwą konta. Aby zezwalać na niestandardowe witryny niepasujące do kategorii lub je blokować, kliknij kartę Wyjątki.



Tworzenie nowego zadania w harmonogramie

Aby utworzyć nowe zadanie w obszarze **Narzędzia** > **Więcej narzędzi** > **Harmonogram**, należy kliknąć przycisk **Dodaj** lub kliknąć prawym przyciskiem myszy i z menu kontekstowego wybrać polecenie **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 w programie ESET SysInspector, gromadząc szczegółowe informacje dotyczące komponentów systemu (na przykład sterowników i aplikacji) wraz z oceną poziomu ryzyka w przypadku każdego komponentu.
- **Skanowanie komputera na żądanie** — umożliwia skanowanie plików i folderów na komputerze.

- **Aktualizacja** — umożliwia zaplanowanie zadania aktualizacji modułów.

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 (godz.)**)

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.

Planowanie cotygodniowego skanowania komputera

Aby zaplanować zadanie cykliczne, otwórz główne okno programu i kliknij opcję **Narzędzia** > **Więcej narzędzi** > **Harmonogram**. Poniżej przedstawiono krótką instrukcję planowania zadania, które umożliwia skanowanie dysków lokalnych co tydzień. Więcej szczegółowych instrukcji zawiera ten artykuł z bazy wiedzy.

Aby zaplanować zadanie skanowania:

1. Kliknij przycisk **Dodaj** znajdujący się w głównym oknie sekcji Harmonogram.
2. Wprowadź nazwę zadania i wybierz opcję **Skanowanie komputera na żądanie** z menu rozwijanego **Typ zadania**.
3. Jako częstotliwość zadań wybierz opcję **Co tydzień**.
4. Ustaw dzień i godzinę wykonania zadania.
5. Wybierz opcję **Wykonaj zadanie jak najszybciej**, aby wykonać zadanie później, gdyby zaplanowane wykonanie zadania nie odbyło się z jakiegoś powodu (np. w wyniku wyłączenia komputera).
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**.

Jak usunąć błąd „Nie można przekierować ochrony bankowości internetowej do żądanej strony internetowej”

> **Użyj opcji Zabezpiecz wszystkie przeglądarki zamiast przekierowywania witryny**
> Domyślnie zabezpieczona przeglądarka z funkcją ochrony bankowości internetowej jest uruchamiana w aktualnie używanej przeglądarce po odwiedzeniu znanej witryny bankowej. Zamiast przekierowywania witryny można użyć opcji Zabezpiecz wszystkie przeglądarki, aby uruchomić wszystkie obsługiwane przeglądarki w trybie bezpiecznym. Umożliwia to przeglądanie Internetu, dostęp do bankowości internetowej i dokonywanie transakcji online bez przekierowywania w jednym zabezpieczonym oknie przeglądarki.
> Aby użyć opcji Zabezpiecz wszystkie przeglądarki, otwórz główne okno programu, przejdź do pozycji **Ustawienia** > **Narzędzia zabezpieczające** i przesuń suwak obok pozycji **Zabezpiecz wszystkie przeglądarki**.

Aby rozwiązać problem z błędem przekierowania witryny, postępuj zgodnie z poniższymi instrukcjami:

> **Po wykonaniu każdego kroku sprawdź, czy Ochrona bankowości internetowej działa.**
> Jeżeli okno przeglądarki nadal nie działa, wykonaj następny krok, aż zacznie działać.

1. Uruchom ponownie komputer.

2. Sprawdź, czy używasz najnowszej wersji systemu operacyjnego Windows i ESET Internet Security: Zaktualizuj produkty ESET do systemu Windows dla użytkowników domowych do najnowszej wersji.

3. Być może występuje konflikt z oprogramowaniem zabezpieczającym, siecią VPN lub zaporą sieciową innej firmy. Tymczasowo wyłącz lub odinstaluj to oprogramowanie.

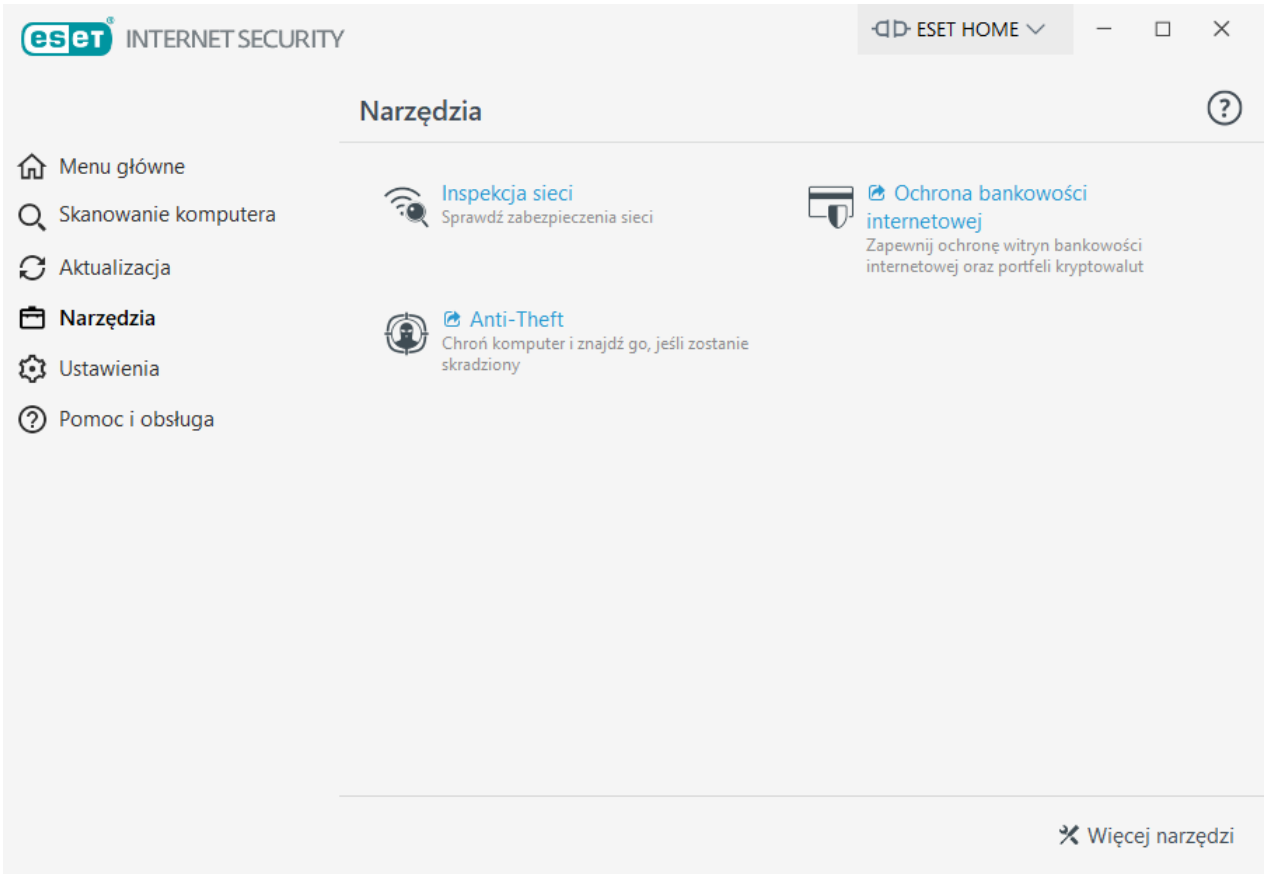
4. Wyłącz wszystkie rozszerzenia przeglądarki innych firm.

5. Wyczyść pamięć podręczną przeglądarki. Jak wyczyścić pamięć podręczną przeglądarki Firefox lub wyczyścić pamięć podręczną przeglądarki Google Chrome?

6. Sprawdź, czy domyślna przeglądarka nie została wyłączona w sekcji **Ustawienia zaawansowane** > **Strony internetowe i poczta e-mail** > **Filtrowanie protokołów** > **Wyłączone aplikacje**. Przejdź do Ustawień zaawansowanych.

7. Jeśli wersja produktu ESET nie została zmieniona na wyższą w poprzednich krokach, odinstaluj i zainstaluj ponownie produkt ESET. Po instalacji uruchom ponownie komputer.

8. Jeśli problem będzie się powtarzał, możesz włączyć opcję Zabezpiecz wszystkie przeglądarki lub uzyskać dostęp do zabezpieczonej przeglądarki w obszarze głównego okna programu > **Narzędzia** > **Ochrona bankowości internetowej**.



Ochrona bankowości internetowej to dodatkowa warstwa zabezpieczeń, mających zapewnić ochronę danych finansowych podczas przeprowadzania transakcji przez Internet.

W większości przypadków zabezpieczona przeglądarka z funkcją ochrony bankowości internetowej jest uruchamiana w domyślnej przeglądarce po przejściu do znanej witryny bankowości internetowej.

Wybierz jedną z następujących opcji konfiguracji zachowania zabezpieczonej przeglądarki:

- **Zabezpiecz wszystkie przeglądarki** — jeśli ta opcja jest włączona, wszystkie obsługiwane przeglądarki internetowe uruchamiają się w trybie bezpiecznym. Pozwala to na przeglądanie Internetu, dostęp do bankowości internetowej, a także zakupy i transakcje online w jednym oknie zabezpieczonej przeglądarki bez przekierowania.

- **Przekierowanie stron internetowych** (domyślne) — strony internetowe z listy chronionych stron internetowych i wewnętrznej listy banków internetowych są przekierowywane do zabezpieczonej przeglądarki. Można wybrać, która przeglądarka (standardowa czy zabezpieczona) zostanie otwarta.

- Wyłączenie obu poprzednich opcji — aby uzyskać dostęp do zabezpieczonej przeglądarki w ESET Internet Security, kliknij pozycję **Narzędzia** > **Ochrona bankowości internetowej** lub kliknij ikonę pulpitu **Ochrona bankowości internetowej**. Przeglądarka wybrana jako domyślna w systemie Windows uruchamia się w trybie bezpiecznym.

Aby skonfigurować zachowanie zabezpieczonej przeglądarki, zobacz Ustawienia zaawansowane ochrony bankowości internetowej. Aby włączyć funkcję Zabezpiecz wszystkie przeglądarki w ESET Internet Security, kliknij **Ustawienia** > **Narzędzia zabezpieczające** i przesuń suwak **Zabezpiecz wszystkie przeglądarki** w pozycję włączoną.

Zabezpieczone przeglądanie Internetu wymaga stosowania zaszyfrowanej komunikacji HTTPS. Następujące

przeglądarki obsługują usługę ochrony bankowości internetowej:

- Internet Explorer 8.0.0.0+
- Microsoft Edge 83.0.0.0+
- Google Chrome 64.0.0.0+
- Firefox 24.0.0.0+

Więcej informacji na temat funkcji ochrony bankowości internetowej zawierają poniższe artykuły z bazy wiedzy firmy ESET (dostępne w języku angielskim i kilku innych językach):

- Jak używać funkcji ochrony bankowości internetowej ESET?
- Włączanie lub wyłączanie ochrony bankowości internetowej ESET dla określonej witryny
- Wstrzymywanie lub wyłączanie funkcji ochrony bankowości internetowej w produktach ESET do systemu Windows dla użytkowników domowych
- Ochrona bankowości internetowej ESET — typowe błędy
- Słowniczek ESET | Ochrona bankowości internetowej

Jeśli nadal nie możesz rozwiązać tego problemu, wyślij e-mail do działu pomocy technicznej firmy ESET.

Odblokowywanie chronionego hasłem obszaru Ustawienia zaawansowane

Podczas uzyskiwania dostępu do chronionego hasłem obszaru Ustawienia zaawansowane wyświetli się okno, w którym należy wpisać hasło. Jeśli użytkownik nie pamięta hasła lub je utracił, powinien kliknąć opcję **Przywróć hasło** i wpisać adres e-mail podany podczas rejestracji licencji. Spowoduje to wysłanie przez ESET wiadomości e-mail z kodem weryfikacyjnym. Należy go wprowadzić, a następnie wpisać i potwierdzić nowe hasło. Kod weryfikacyjny jest ważny przez siedem dni.

Przywróć hasło za pomocą konta ESET HOME — użyj tej opcji, jeśli licencja użyta do aktywacji jest powiązana z Twoim kontem ESET HOME. Wpisz adres e-mail, którego używasz do logowania się na swoje konto ESET HOME.

Jeśli nie pamiętasz adresu e-mail lub masz trudności z przywróceniem hasła, kliknij opcję **Skontaktuj się z pomocą techniczną**. Nastąpi przekierowanie do witryny internetowej firmy ESET w celu skontaktowania się z naszym działem pomocy technicznej.

Wygeneruj kod dla działu pomocy technicznej — opcja ta generuje kod, który trzeba podać pracownikowi działu pomocy technicznej. Skopiuj kod podany przez dział pomocy technicznej i kliknij pozycję **Mam kod weryfikacyjny**. Wpisz kod weryfikacyjny, a następnie wpisz i potwierdź nowe hasło. Kod weryfikacyjny jest ważny przez siedem dni.

Więcej informacji można znaleźć w części Odblokowywanie hasła do ustawień w produktach ESET do systemu Windows dla użytkowników domowych.

Jak rozwiązać dezaktywację produktu z ESET HOME

Produkt nie został aktywowany

Ten komunikat o błędzie pojawia się, gdy właściciel licencji dezaktywuje użytkownika ESET Internet Security z portalu ESET HOME lub licencja udostępniona kontu ESET HOME nie jest już udostępniana. Aby rozwiązać ten problem:

- Kliknij **Aktywuj** i użyj jednej z metod aktywacji, aby aktywować ESET Internet Security.
- Skontaktuj się z właścicielem licencji, podając informacje, że licencja ESET Internet Security została dezaktywowana przez właściciela licencji lub nie jest już udostępniana. Właściciel może rozwiązać problem w portalu ESET HOME.

Produkt dezaktywowano, a urządzenie zostało odłączone

Ten komunikat o błędzie pojawia się po usunięciu urządzenia z konta ESET HOME. Aby rozwiązać ten problem:

- Kliknij **Aktywuj** i użyj jednej z metod aktywacji, aby aktywować ESET Internet Security.
- Skontaktuj się z właścicielem licencji, podając informacje, że ESET Internet Security został dezaktywowany, a urządzenie zostało odłączone od ESET HOME.
- Jeśli jesteś właścicielem licencji i nie wiesz o tych zmianach, przejrzyj Dziennik aktywności konta ESET HOME . Jeśli znajdziesz podejrzane działania, zmień hasło do konta ESET HOME i skontaktuj się z działem pomocy technicznej firmy ESET.

Produkt dezaktywowano, a urządzenie zostało odłączone

Ten komunikat o błędzie pojawia się po usunięciu urządzenia z konta ESET HOME. Aby rozwiązać ten problem:

- Kliknij **Aktywuj** i użyj jednej z metod aktywacji, aby aktywować ESET Internet Security.
- Skontaktuj się z właścicielem licencji, podając informacje, że ESET Internet Security został dezaktywowany, a urządzenie zostało odłączone od ESET HOME.
- Jeśli jesteś właścicielem licencji i nie wiesz o tych zmianach, przejrzyj Dziennik aktywności konta ESET HOME . Jeśli znajdziesz podejrzane działania, zmień hasło do konta ESET HOME i skontaktuj się z działem pomocy technicznej firmy ESET.

Produkt nie został aktywowany

Ten komunikat o błędzie pojawia się, gdy właściciel licencji dezaktywuje użytkownika ESET Internet Security z portalu ESET HOME lub licencja udostępniona kontu ESET HOME nie jest już udostępniana. Aby rozwiązać ten problem:

• Kliknij **Aktywuj** i użyj jednej z metod aktywacji, aby aktywować ESET Internet Security.

• Skontaktuj się z właścicielem licencji, podając informacje, że licencja ESET Internet Security została dezaktywowana przez właściciela licencji lub nie jest już udostępniana. Właściciel może rozwiązać problem w portalu ESET HOME.

Program poprawy jakości doświadczeń użytkowników

Uczestnicy Programu poprawy jakości doświadczeń użytkowników dostarczają firmie ESET anonimowych informacji dotyczących sposobu korzystania z jej produktów. Więcej informacji na temat przetwarzania danych zawiera nasza polityka prywatności.

Zgoda uczestnika

Udział w tym programie jest dobrowolny i wymaga zgody uczestnika. Po dołączeniu do programu uczestnictwo w nim ma charakter pasywny, co oznacza, że użytkownik nie musi podejmować żadnych dodatkowych działań. Zgodę na udział w programie można cofnąć w dowolnej chwili w ustawieniach produktu. Uniemożliwi nam to dalsze przetwarzanie anonimowych danych pozyskiwanych od użytkownika.

Zgodę na udział w programie można cofnąć w dowolnej chwili w ustawieniach produktu:

- Zmiana ustawień Programu poprawy jakości doświadczeń użytkowników w produktach ESET do systemu Windows przeznaczonych dla użytkowników domowych

Jakie rodzaje informacji zbieramy?

Dane dotyczące interakcji z produktem

Na podstawie tych informacji wiemy więcej o tym, jak są używane nasze produkty. Dzięki temu wiemy na przykład, które funkcje są wykorzystywane częściej, które ustawienia modyfikują użytkownicy lub ile czasu poświęcają oni na używanie produktu.

Dane dotyczące urządzeń

Te informacje zbieramy po to, by wiedzieć, gdzie i na jakich urządzeniach są używane nasze produkty. Są to z reguły takie dane, jak model urządzenia, kraj oraz wersja i nazwa systemu operacyjnego.

Dane dotyczące diagnostyki błędów

Zbieramy także informacje o błędach i awariach, na przykład o tym, jaki wystąpił błąd i jakie działania do niego doprowadziły.

Dlaczego zbieramy te informacje?

Te anonimowe informacje umożliwiają nam doskonalenie produktów dla naszych użytkowników. Pomagają nam one optymalnie dostosowywać produkty do potrzeb użytkowników, upraszczać ich obsługę i zapewniać ich bezawaryjne działanie.

Kto administruje tymi informacjami?

Wyłącznym administratorem danych zbieranych w ramach programu jest firma ESET, spol. s r.o. Danych tych nie udostępniamy osobom trzecim.

Umowa licencyjna użytkownika końcowego

Obowiązuje od 19 października 2021 r..

WAŻNE: Przed pobraniem, zainstalowaniem, skopiowaniem lub użyciem Oprogramowania należy się dokładnie zapoznać z poniższymi warunkami korzystania z produktu. **POBRANIE, ZAINSTALOWANIE, SKOPIOWANIE LUB UŻYCIE OPROGRAMOWANIA OZNACZA WYRAŻENIE ZGODY NA NINIEJSZE WARUNKI I AKCEPTACJĘ POLITYKI PRYWATNOŚCI.**

Umowę Licencyjną Użytkownika Końcowego

Niniejsza Umowa licencyjna użytkownika końcowego („Umową”), zawierana między spółką ESET, spol. s r. o., z siedzibą w Słowacji pod adresem Einsteinova 24, 85101 Bratislava, Slovak Republic, zarejestrowaną w Rejestrze Handlowym Sądu Rejonowego dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („firmą ESET” lub „Dostawcą”), a licencjobiorcą, który jest osobą fizyczną lub prawną („Licencjobiorcą” lub „Użytkownikiem końcowym”), uprawnia Licencjobiorcę do korzystania z Oprogramowania określonego w punkcie 1 niniejszej Umowy. Oprogramowanie określone w punkcie 1 niniejszej Umowy może znajdować się na nośniku danych albo zostać przesłane pocztą elektroniczną, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł na warunkach wyszczególnionych poniżej.

NINIEJSZA UMOWA DOTYCZY WYŁĄCZNIE OKREŚLENIA PRAW UŻYTKOWNIKA KOŃCOWEGO I NIE STANOWI UMOWY SPRZEDAŻY. Dostawca pozostaje właścicielem kopii Oprogramowania i nośnika fizycznego zawartego w opakowaniu z produktem, a także wszystkich innych kopii Oprogramowania, które Użytkownik końcowy może wykonać zgodnie z niniejszą Umową.

Kliknięcie opcji „Akceptuję” lub „Akceptuję...” w trakcie instalowania, pobierania, kopiowania lub używania Oprogramowania oznacza, że Licencjobiorca wyraża zgodę na warunki określone w niniejszej Umowie oraz akceptuje Politykę prywatności. Jeśli Licencjobiorca nie wyraża zgody na którykolwiek warunek określony w niniejszej Umowie i/lub Polityce prywatności, powinien niezwłocznie kliknąć opcję anulowania i przerwać instalację lub pobieranie albo zniszczyć Oprogramowanie, nośnik instalacyjny, dokumentację towarzyszącą Oprogramowaniu i dowód sprzedaży Oprogramowania bądź zwrócić je Dostawcy lub w miejscu zakupu Oprogramowania.

LICENCJOBIORCA PRZYJMUJE DO WIADOMOŚCI, ŻE KORZYSTANIE Z OPROGRAMOWANIA OZNACZA ZAPOZNANIE SIĘ Z NINIEJSZĄ UMOWĄ, ZROZUMIENIE WARUNKÓW W NIEJ OKREŚLONYCH ORAZ ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA.

1. **Oprogramowanie.** W niniejszej Umowie termin „Oprogramowanie” oznacza: (i) program komputerowy, do którego dołączono niniejszą Umowę, i wszystkie jego składniki; (ii) całą zawartość dysków, płyt CD-ROM i płyt DVD, wiadomości e-mail wraz z ich załącznikami oraz innych nośników, do których jest dołączona niniejsza Umowa, w tym Oprogramowanie w formie kodu obiektowego dostarczone na nośniku danych albo za pośrednictwem poczty elektronicznej lub Internetu; (iii) wszelkie powiązane drukowane materiały instruktażowe oraz wszelką inną dokumentację powiązaną z Oprogramowaniem, w tym przede wszystkim wszelkie opisy Oprogramowania, jego dane techniczne, wszelkie opisy jego właściwości lub działania, wszelkie opisy środowiska operacyjnego, w którym Oprogramowanie jest używane, instrukcje obsługi lub instalacji Oprogramowania oraz wszelkie opisy sposobu korzystania z Oprogramowania („Dokumentacją”); (iv) wszelkie ewentualne kopie

Oprogramowania, poprawki możliwych błędów Oprogramowania, dodatki do Oprogramowania, rozszerzenia Oprogramowania, zmodyfikowane wersje Oprogramowania oraz aktualizacje składników Oprogramowania, na które Dostawca udziela Licencjobiorcy licencji zgodnie z zapisami w punkcie 3 niniejszej Umowy. Oprogramowanie będzie dostarczane wyłącznie w postaci wykonywalnego kodu obiektowego.

2. **Instalacja, komputer i klucz licencyjny**. Oprogramowanie dostarczone na nośniku danych, otrzymane za pośrednictwem poczty elektronicznej, pobrane z Internetu, pobrane z serwerów Dostawcy lub uzyskane z innych źródeł musi zostać zainstalowane. Oprogramowanie należy zainstalować na prawidłowo skonfigurowanym komputerze, który spełnia minimalne wymagania określone w Dokumentacji. Procedurę instalacji również opisano w Dokumentacji. Na komputerze, na którym zostanie zainstalowane Oprogramowanie, nie można instalować sprzętu komputerowego ani programów komputerowych, które mogłyby niekorzystnie wpłynąć na Oprogramowanie. Komputer oznacza sprzęt, w tym między innymi komputery osobiste, laptopy, stacje robocze, palmtopy, smartfony, przenośne urządzenia elektroniczne lub inne urządzenia elektroniczne, dla których przeznaczone jest Oprogramowanie, na których zostanie zainstalowane i/lub będzie używane. Klucz licencyjny oznacza niepowtarzalny ciąg symboli, liter, cyfr i znaków specjalnych, dostarczony Użytkownikowi końcowemu w celu umożliwienia mu legalnego korzystania z Oprogramowania, jego określonych wersji lub rozszerzenia warunków Licencji zgodnie z niniejszą Umową.

3. **Licencja**. Dostawca udziela Licencjobiorcy praw określonych poniżej (w dalszej części nazywanych zbiorczo „Licencją"), jeśli Licencjobiorca zobowiązał się przestrzegać i przestrzega wszelkich warunków określonych w niniejszej Umowie:

a) **Instalacja i użycie.** Licencjobiorcy przysługują niewyłączne, nieprzenoszalne prawa do zainstalowania Oprogramowania na dysku twardym komputera lub na innym nośniku do trwałego przechowywania danych, do zainstalowania i przechowywania Oprogramowania w pamięci systemu komputerowego oraz do zaimplementowania, przechowywania i wyświetlania Oprogramowania.

b) **Postanowienia w sprawie liczby Licencji.** Prawo do korzystania z Oprogramowania w ramach jednej Licencji jest ograniczone do jednego Użytkownika końcowego. Jeden Użytkownik końcowy oznacza: (i) instalację Oprogramowania na jednym komputerze lub, jeśli liczba Licencji zależy od liczby skrzynek pocztowych, (ii) użytkownika komputera, który odbiera pocztę elektroniczną za pośrednictwem klienta poczty elektronicznej. Jeśli do klienta poczty elektronicznej dociera poczta elektroniczna, która jest następnie automatycznie dystrybuowana do innych użytkowników, liczbę Użytkowników końcowych stanowi liczba wszystkich użytkowników, do których jest dostarczana poczta. Jeśli serwer poczty pełni funkcję bramy pocztowej, liczba Użytkowników końcowych jest równa liczbie użytkowników serwera poczty, którzy są obsługiwani przez tę bramę. Jeśli jeden użytkownik odbiera pocztę przesyłaną na różne adresy e-mail (np. za pośrednictwem usługi aliasów), a liczba tych adresów jest nieokreślona i wiadomości nie są automatycznie dystrybuowane przez klienta poczty elektronicznej do większej liczby użytkowników, wymagana jest Licencja na jednego użytkownika komputera. Z jednej Licencji można korzystać każdorazowo tylko na jednym komputerze. Użytkownik końcowy może wprowadzić klucz licencyjny do Oprogramowania tylko w zakresie, w jakim przysługuje mu prawo do korzystania z Oprogramowania zgodnie z ograniczeniami wynikającymi z liczby Licencji przyznanych przez Dostawcę. Klucz licencyjny ma charakter poufny, Licencjobiorca nie może udostępniać Licencji stronom trzecim ani pozwalać im na używanie klucza licencyjnego, o ile nie dopuszcza tego niniejsza Umowa lub Dostawca. W przypadku naruszenia klucza licencyjnego należy bezzwłocznie powiadomić Dostawcę.

c) **Wersja Home/Business Edition.** Wersja Home Oprogramowania jest przeznaczona wyłącznie do używania w środowiskach prywatnych i/lub niekomercyjnych tylko na użytek domowy i rodzinny. W przypadku zamiaru zainstalowania i użycia Oprogramowania w środowisku komercyjnym, na serwerze poczty, w systemie przekazywania wiadomości e-mail lub w połączeniu z bramą pocztową bądź internetową wymagane jest nabycie wersji Business Edition Oprogramowania.

d) **Okres obowiązywania Licencji.** Prawo do korzystania z Oprogramowania jest ograniczone w czasie.

e) **Oprogramowanie dostarczone przez producenta urządzenia (OEM).** Prawo do korzystania z Oprogramowania, które zostało dostarczone przez producenta zakupionego urządzenia (OEM, Original Equipment Manufacturer), jest ograniczone do tego urządzenia. Prawa tego nie można przenosić na inne urządzenia.

f) **Oprogramowanie w wersji próbnej lub nieprzeznaczonej do obrotu handlowego.** Nie można pobierać opłat za korzystanie z Oprogramowania, które jest oznaczone napisem „Not for resale" lub „NFR" (Nie do sprzedaży) albo „TRIAL" (Wersja próbna). Oprogramowanie takie jest przeznaczone wyłącznie do prezentacji lub testowania jego funkcji.

g) **Wygaśnięcie Licencji.** Licencja wygasa automatycznie po upływie okresu jej obowiązywania. Jeśli Licencjobiorca naruszył którekolwiek z postanowień niniejszej Umowy, Dostawca jest uprawniony do rozwiązania niniejszej Umowy oraz do wykonania wszelkich innych praw i zastosowania wszelkich innych środków prawnych przysługujących mu w takiej sytuacji. W razie anulowania Licencji Licencjobiorca musi natychmiast usunąć lub zniszczyć Oprogramowanie i wszystkie jego kopie zapasowe lub zwrócić je na własny koszt do firmy ESET bądź w miejscu zakupu Oprogramowania. Po wygaśnięciu Licencji Dostawca jest też uprawniony do anulowania prawa Użytkownika końcowego do używania funkcji Oprogramowania, które wymagają połączenia z serwerami Dostawcy lub serwerami innych firm.

4. **Wymagania dotyczące funkcji gromadzących dane i połączenia z Internetem.** Aby Oprogramowanie działało poprawnie, wymagane jest stałe połączenie z Internetem oraz regularne połączenia z serwerami Dostawcy lub z serwerami innych firm, a gromadzenie potrzebnych danych powinno odbywać się zgodnie z obowiązującą Polityką prywatności. Połączenie z Internetem oraz gromadzenie potrzebnych danych są wymagane w przypadku następujących funkcji Oprogramowania:

a) **Aktualizacje Oprogramowania.** Dostawca jest uprawniony do wprowadzania aktualizacji w Oprogramowaniu (w dalszej części nazywanych „Aktualizacjami"), przy czym nie jest zobowiązany do ich wprowadzania. Funkcja Aktualizacji jest domyślnie włączona w ustawieniach standardowych Oprogramowania, dlatego Aktualizacje są instalowane automatycznie, o ile Użytkownik końcowy nie zmienił ustawienia automatycznego instalowania Aktualizacji. W celu przeprowadzania aktualizacji wymagana jest weryfikacja autentyczności Licencji, w tym informacji dotyczących komputera i/lub platformy, na której zostało zainstalowane Oprogramowanie, zgodnie z Polityką Prywatności.

Dostarczanie wszelkich Aktualizacji może podlegać Polityce końca okresu użytkowania ("Polityka EOL"), która jest dostępna na stronie stronie https://go.eset.com/eol_home. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą dostarczane żadne aktualizacje.

b) **Przekazywanie szkodliwego oprogramowania i informacji o komputerze do Dostawcy**. Oprogramowanie obejmuje funkcje, które gromadzą próbki wirusów komputerowych, innych szkodliwych programów komputerowych oraz podejrzanych, problematycznych, potencjalnie niepożądanych lub niebezpiecznych obiektów, takich jak pliki, adresy URL, pakiety IP oraz ramki Ethernet („Szkodliwe oprogramowanie"), po czym wysyłają je do Dostawcy. Wysyłane dane obejmują m.in. informacje o procesie instalacji, komputerze i/lub platformie, na której zainstalowano Oprogramowanie, a także informacje o działaniu i funkcjonalności Oprogramowania („Informacje"). Informacje oraz Szkodliwe oprogramowanie mogą obejmować dane Użytkownika końcowego (w tym jego dane osobowe pobrane losowo lub przypadkowo) lub dane innych użytkowników komputera, na którym zainstalowano Oprogramowanie, a także pliki uszkodzone przez Szkodliwe oprogramowanie wraz z powiązanymi z nimi metadanymi.

Informacje oraz Szkodliwe oprogramowanie mogą być gromadzone przy użyciu następujących funkcji Oprogramowania:

i. Funkcja systemu reputacji LiveGrid służy do gromadzenia i wysyłania do Dostawcy jednokierunkowych skrótów związanych ze Szkodliwym oprogramowaniem. Funkcję tę można włączyć w ustawieniach standardowych Oprogramowania.

ii. System informacji zwrotnych LiveGrid służy do gromadzenia i wysyłania do Dostawcy Szkodliwego oprogramowania wraz z powiązanymi metadanymi, a także Informacji. Funkcję tę może włączyć Użytkownik końcowy podczas procesu instalacji Oprogramowania.

Dostawca może wykorzystać otrzymane Informacje oraz Szkodliwe oprogramowanie tylko w celu analizy Szkodliwego oprogramowania, usprawnienia Oprogramowania i zweryfikowania autentyczności Licencji i jest zobowiązany do podjęcia stosownych środków gwarantujących zachowanie poufności Szkodliwego oprogramowania i Informacji. Włączenie tej funkcji Oprogramowania oznacza, że Dostawca może gromadzić i przetwarzać Szkodliwe oprogramowanie i Informacje zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Użytkownik może wyłączyć te funkcje w każdej chwili.

Na potrzeby niniejszej Umowy konieczne jest gromadzenie, przetwarzanie i przechowywanie danych umożliwiających Dostawcy identyfikację Licencjobiorcy zgodnie z Polityką prywatności. Licencjobiorca niniejszym zgadza się, aby Dostawca, korzystając z własnych środków, mógł sprawdzić, czy Licencjobiorca używa Oprogramowania zgodnie z postanowieniami niniejszej Umowy. Licencjobiorca zgadza się, że na potrzeby niniejszej Umowy konieczne jest przekazywanie jego danych podczas komunikacji pomiędzy Oprogramowaniem a systemami komputerowymi Dostawcy lub jego partnerów handlowych w ramach sieci dystrybucyjnej i wsparcia Dostawcy w celu zapewnienia funkcjonalności Oprogramowania i upoważnienia do używania Oprogramowania oraz ochrony praw Dostawcy.

Po zawarciu niniejszej Umowy Dostawca i każdy z jego partnerów handlowych, w ramach sieci dystrybucyjnej i wsparcia Dostawcy, będzie uprawniony do przekazywania, przetwarzania i przechowywania istotnych danych identyfikujących Licencjobiorcę w celach związanych z rozliczaniem opłat, wykonywaniem niniejszej Umowy i przekazywaniem powiadomień na komputerze Licencjobiorcy.

Szczegółowe informacje na temat ochrony prywatności, danych osobowych i praw Licencjobiorcy jako podmiotu danych dostępne są w Polityce prywatności w witrynie Dostawcy, bezpośrednio podczas procesu instalacji. Można do niej przejść także z poziomu sekcji pomocy w Oprogramowaniu.

5. **Wykonywanie praw Użytkownika końcowego**. Licencjobiorca może wykonywać swoje prawa wyłącznie osobiście lub za pośrednictwem swoich pracowników. Licencjobiorca może korzystać z Oprogramowania wyłącznie w celu zapewnienia ciągłości swojej działalności gospodarczej i w celu zabezpieczenia komputerów lub systemów komputerowych, na które uzyskał Licencję.

6. **Ograniczenie praw.** Licencjobiorca nie może kopiować, rozpowszechniać ani wyodrębniać składników Oprogramowania, jak również nie może tworzyć produktów na podstawie Oprogramowania (nie może wykonywać dzieł pochodnych). Korzystając z Oprogramowania, Licencjobiorca musi przestrzegać następujących ograniczeń:

a) Licencjobiorca może wykonać jedną kopię Oprogramowania na nośniku przeznaczonym do trwałego przechowywania danych i przechowywać tę kopię w charakterze archiwalnej kopii zapasowej, tj. nie może zainstalować ani użyć takiej kopii na żadnym komputerze. Wszelkie inne kopie Oprogramowania wykonane przez Licencjobiorcę stanowią naruszenie warunków określonych w niniejszej Umowie.

b) Licencjobiorca nie może używać, modyfikować, tłumaczyć ani odtwarzać Oprogramowania ani jego kopii w sposób inny niż wyszczególniony w niniejszej Umowie.

c) Licencjobiorca nie może sprzedawać Oprogramowania, udzielać na nie podlicencji, oddawać go w użytkowanie, wypożyczać go innym osobom ani pożyczać go od innych osób, a także nie może używać Oprogramowania w celu świadczenia usług o charakterze dochodowym.

d) Licencjobiorca nie może podejmować prób odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji ani w żaden inny sposób, chyba że pozwalają mu na to przepisy, które w

stosownym zakresie wyraźnie znoszą niniejsze postanowienie.

e) Licencjobiorca zobowiązuje się używać Oprogramowania w sposób zgodny z wszelkimi przepisami, które mają zastosowanie do Oprogramowania ze względu na właściwość terytorialną Licencjobiorcy, w tym między innymi ze stosownymi ograniczeniami dotyczącymi prawa autorskiego i innych praw własności intelektualnej.

f) Licencjobiorca zgadza się korzystać z Oprogramowania i jego funkcji w sposób, który nie ograniczy dostępu do tych usług innym Użytkownikom końcowym. Dostawca zastrzega sobie prawo do ograniczenia zakresu usług udostępnianych konkretnym Użytkownikom końcowym w celu zapewnienia możliwości korzystania z nich jak największej liczbie Użytkowników końcowych. Ograniczenie zakresu usług może również oznaczać całkowitą blokadę funkcji Oprogramowania oraz usunięcie Danych i informacji przechowywanych na serwerach Dostawcy lub zewnętrznego podmiotu związanych z wybranymi funkcjami Oprogramowania.

g) Licencjobiorca zobowiązuje się nie podejmować działań obejmujących korzystanie z klucza licencyjnego, niezgodnych z postanowieniami niniejszej Umowy lub prowadzących do przekazania klucza licencyjnego osobie nieuprawnionej do korzystania z Oprogramowania, takich jak przekazanie wykorzystanego lub niewykorzystanego klucza licencyjnego w dowolnej formie, a także nieautoryzowana reprodukcja lub dystrybucja zduplikowanych lub wygenerowanych kluczy licencyjnych albo korzystanie z Oprogramowania w wyniku wykorzystania klucza licencyjnego uzyskanego z innego źródła niż Dostawca.

7. **Prawo autorskie**. Oprogramowanie i wszystkie prawa z nim związane, w tym między innymi prawa własności i prawa własności intelektualnej do Oprogramowania, należą do firmy ESET i/lub jej licencjodawców. Prawa te gwarantują zapisy traktatów międzynarodowych oraz wszelkie właściwe przepisy ustawowe obowiązujące w kraju, w którym jest używane Oprogramowanie. Struktura Oprogramowania, sposób jego zorganizowania i kod w nim zawarty są cennymi tajemnicami handlowymi oraz informacjami poufnymi firmy ESET i/lub jej licencjodawców. Licencjobiorca nie może kopiować Oprogramowania poza okolicznościami opisanymi w punkcie 6(a). Wszelkie kopie utworzone przez Licencjobiorcę zgodnie z niniejszą Umową muszą zawierać te same informacje o prawie autorskim i innych prawach własności, które znajdują się w Oprogramowaniu. Licencjobiorca niniejszym przyjmuje do wiadomości, że w razie naruszenia postanowień niniejszej Umowy przez podjęcie próby odtworzenia kodu źródłowego Oprogramowania na drodze dekompilacji lub dezasemblacji albo w inny sposób prawa do wszelkich informacji uzyskanych przez Licencjobiorcę w wyniku podjęcia takiej próby zostaną uznane za automatycznie i nieodwołalnie przeniesione w całości na Dostawcę już w momencie powstania takich informacji i to niezależnie od praw przysługujących Dostawcy w związku z naruszeniem przez Licencjobiorcę warunków określonych w niniejszej Umowie.

8. **Zastrzeżenie praw**. Dostawca niniejszym zastrzega sobie wszelkie prawa do Oprogramowania, z wyjątkiem praw wyraźnie udzielonych Licencjobiorcy, występującemu w charakterze Użytkownika końcowego, na podstawie niniejszej Umowy.

9. **Różne wersje językowe, Oprogramowanie obsługujące wiele urządzeń i wiele kopii Oprogramowania**. Jeśli Oprogramowanie może obsługiwać wiele platform lub języków bądź jeśli Licencjobiorca uzyskał wiele kopii Oprogramowania, Oprogramowania można używać tylko na tych systemach komputerowych i w tych wersjach, na które Licencjobiorca uzyskał Licencje. Licencjobiorca nie może sprzedawać wersji ani kopii Oprogramowania, których nie używa, jak również nie może ich oddawać w użytkowanie, udzielać na nie podlicencji, wypożyczać ich ani przenosić do nich praw na inne osoby.

10. **Rozpoczęcie i zakończenie obowiązywania Umowy.** Niniejsza Umowa wchodzi w życie z datą wyrażenia przez Licencjobiorcę zgody na warunki określone w tej Umowie. Licencjobiorca może rozwiązać niniejszą Umowę w dowolnej chwili przez trwałe odinstalowanie i zniszczenie Oprogramowania, wszystkich jego kopii zapasowych i wszelkich powiązanych materiałów dostarczonych przez Dostawcę lub jego partnerów handlowych bądź przez zwrócenie tych produktów na własny koszt. Prawo Licencjobiorcy do korzystania z Oprogramowania i wszelkich jego funkcji może podlegać Polityce EOL. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, prawo Licencjobiorcy do korzystania z

Oprogramowania wygaśnie. Bez względu na powód rozwiązania niniejszej Umowy po zakończeniu jej obowiązywania nadal obowiązują postanowienia zawarte w punktach 7, 8, 11, 13, 19 i 21.

11. **OŚWIADCZENIA UŻYTKOWNIKA KOŃCOWEGO**. LICENCJOBIORCA (WYSTĘPUJĄCY W CHARAKTERZE UŻYTKOWNIKA KOŃCOWEGO) PRZYJMUJE OPROGRAMOWANIE W STANIE TAKIM, W JAKIM ZOSTAŁO MU ONO DOSTARCZONE, BEZ JAKICHKOLWIEK WYRAŹNYCH LUB DOROZUMIANYCH GWARANCJI, O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA. ANI WŁAŚCICIELE STOSOWNYCH PRAW AUTORSKICH NIE UDZIELAJĄ ŻADNYCH WYRAŹNYCH ANI DOROZUMIANYCH GWARANCJI, W TYM MIĘDZY INNYMI GWARANCJI PRZYDATNOŚCI HANDLOWEJ LUB PRZYDATNOŚCI DO OKREŚLONEGO CELU, JAK RÓWNIEŻ NIE GWARANTUJĄ, ŻE OPROGRAMOWANIE NIE BĘDZIE NARUSZAĆ PRAW PATENTOWYCH, PRAW AUTORSKICH, PRAW DO ZNAKÓW TOWAROWYCH ANI INNYCH PRAW OSÓB TRZECICH. ANI DOSTAWCA, ANI ŻADNA INNA OSOBA NIE GWARANTUJE, ŻE FUNKCJE OPROGRAMOWANIA SPEŁNIAJĄ WYMAGANIA LICENCJOBIORCY LUB ŻE DZIAŁANIE OPROGRAMOWANIA BĘDZIE NIEZAKŁÓCONE I POZBAWIONE BŁĘDÓW. LICENCJOBIORCA BIERZE NA SIEBIE WSZELKĄ ODPOWIEDZIALNOŚĆ I RYZYKO ZA DOBÓR OPROGRAMOWANIA ODPOWIEDNIEGO DO OSIĄGNIĘCIA CELÓW LICENCJOBIORCY ORAZ ZA PRZEPROWADZENIE INSTALACJI OPROGRAMOWANIA, ZA JEGO UŻYCIE I ZA WYNIKI TEGO UŻYCIA.

12. **Brak innych zobowiązań**. W niniejszej Umowie określono wszystkie zobowiązania Dostawcy i jego licencjodawców.

13. **OGRANICZENIE ODPOWIEDZIALNOŚCI**. O ILE PRAWO WŁAŚCIWE TEGO NIE ZABRANIA, ANI DOSTAWCA, ANI JEGO PRACOWNICY CZY LICENCJODAWCY NIE PONOSZĄ ŻADNEJ ODPOWIEDZIALNOŚCI ZA JAKIEKOLWIEK UTRATY ZYSKÓW, PRZYCHODÓW, ŹRÓDEŁ PRZYCHODÓW LUB DANYCH, SZKODY MAJĄTKOWE LUB OBRAŻENIA CIAŁA, ZAKŁÓCENIA DZIAŁALNOŚCI PRZEDSIĘBIORSTWA, UTRATY DANYCH HANDLOWYCH CZY JAKIEKOLWIEK SZKODY SZCZEGÓLNE, BEZPOŚREDNIE, POŚREDNIE, UBOCZNE, GOSPODARCZE, MORALNE LUB WYNIKOWE, JAK RÓWNIEŻ NIE BĘDĄ PONOSIĆ KOSZTÓW NABYCIA ZASTĘPCZYCH TOWARÓW LUB USŁUG ANI POKRYWAĆ RÓŻNIC MIĘDZY CENAMI KONTRAKTOWYMI A CENAMI TRANSAKCJI. ZASTRZEŻENIE OKREŚLONE W POWYŻSZYM ZDANIU MA ZASTOSOWANIE BEZ WZGLĘDU NA PRZYCZYNĘ POWSTANIA SZKODY I NA TO, CZY EWENTUALNE ROSZCZENIE ZOSTAŁO ZGŁOSZONE NA PODSTAWIE UMOWY, PRZEPISÓW O CZYNACH NIEDOZWOLONYCH, PRZEPISÓW DOTYCZĄCYCH ZANIEDBAŃ CZY NA JAKIEJKOLWIEK INNEJ PODSTAWIE ORAZ CZY ZOSTAŁO ONO ZGŁOSZONE W ZWIĄZKU Z INSTALACJĄ, UŻYCIEM CZY Z NIEMOŻNOŚCIĄ UŻYCIA OPROGRAMOWANIA. ZASTRZEŻENIE TO MA ZASTOSOWANIE TAKŻE WÓWCZAS, GDY DOSTAWCA LUB JEGO LICENCJODAWCY BĄDŹ PODMIOTY STOWARZYSZONE ZOSTALI POWIADOMIENI O MOŻLIWOŚCI WYSTĄPIENIA DANEJ SZKODY. W PRZYPADKU JURYSDYKCJI, KTÓRE NIE ZEZWALAJĄ NA WYŁĄCZENIE ODPOWIEDZIALNOŚCI ODSZKODOWAWCZEJ, LECZ DOPUSZCZAJĄ JEJ OGRANICZENIE, ODPOWIEDZIALNOŚĆ DOSTAWCY, JEGO PRACOWNIKÓW, LICENCJODAWCÓW LUB PODMIOTÓW STOWARZYSZONYCH JEST OGRANICZONA DO KWOTY ZAPŁACONEJ PRZEZ LICENCJOBIORCĘ ZA LICENCJE.

14. Jeśli którekolwiek postanowienie niniejszej Umowy jest sprzeczne z ustawowymi prawami konsumenckimi jakiejkolwiek osoby, postanowienie to nie może być interpretowane w sposób naruszający te prawa.

15. **Pomoc techniczna**. Usługi pomocy technicznej świadczą wedle własnego uznania i bez udzielania jakichkolwiek gwarancji firma ESET lub inne firmy, którym firma ESET zleca świadczenie takich usług. Gdy Oprogramowanie lub którakolwiek z jego funkcji osiągnie datę zakończenia okresu użytkowania określoną w Polityce EOL, nie będą świadczone żadne usługi pomocy technicznej. Przed skorzystaniem z usługi pomocy technicznej Użytkownik końcowy musi utworzyć kopię zapasową wszystkich istniejących danych, programów i aplikacji. Ani firma ESET, ani inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, nie mogą wziąć na siebie odpowiedzialności za uszkodzenie lub utratę danych, własności, oprogramowania lub urządzeń, jak również nie mogą odpowiadać za utratę zysków spowodowaną świadczeniem usług pomocy technicznej. Firma ESET i/lub inne firmy, którym firma ESET zleca świadczenie usług pomocy technicznej, zastrzegają sobie prawo do odmowy wykonania usługi, jeśli uznają, że nie mieści się ona w zakresie oferowanych usług pomocy technicznej. Firma ESET zastrzega sobie prawo do odmowy, wstrzymania lub zaprzestania świadczenia usług pomocy technicznej, jeśli uzna to za stosowne. Informacje dotyczące licencji, Informacje i inne dane zgodne z

Polityką prywatności mogą być wymagane na potrzeby świadczenia pomocy technicznej.

16. **Przeniesienie Licencji**. Jeśli odpowiednie postanowienia niniejszej Umowy tego nie zabraniają, Oprogramowanie można przenosić między poszczególnymi systemami komputerowymi. O ile nie jest to sprzeczne z warunkami określonymi w niniejszej Umowie, za zgodą Dostawcy Użytkownik końcowy może trwale przenieść Licencję i wszelkie prawa przysługujące mu na podstawie niniejszej Umowy na innego Użytkownika końcowego, pod warunkiem że (i) nie zachowa dla siebie żadnych kopii Oprogramowania; (ii) przeniesienie praw będzie bezpośrednie, tj. prawa zostaną przeniesione bezpośrednio na nowego Użytkownika końcowego; (iii) nowy Użytkownik końcowy przejmie na siebie wszystkie prawa i obowiązki wynikające z niniejszej Umowy, które miały dotąd zastosowanie do Użytkownika końcowego przenoszącego Licencję; (iv) nowy Użytkownik końcowy otrzyma od Użytkownika końcowego przenoszącego Licencję dokumentację, która umożliwi mu stwierdzenie zgodnie z zapisami w punkcie 17, czy Oprogramowanie jest oryginalne.

17. **Weryfikowanie oryginalności Oprogramowania.** Użytkownik końcowy może wykazać swoje uprawnienia do korzystania z Oprogramowania w jeden z poniższych sposobów: (i) na podstawie certyfikatu licencyjnego wystawionego przez Dostawcę lub inną firmę wskazaną przez Dostawcę; (ii) na podstawie pisemnej umowy licencyjnej, jeśli została ona zawarta; (iii) na podstawie wiadomości e-mail od Dostawcy z danymi dotyczącymi licencji (nazwą użytkownika i hasłem). Informacje dotyczące licencji oraz dane identyfikujące Użytkownika końcowego zgodne z Polityką prywatności mogą być wymagane w celu weryfikacji oryginalności Oprogramowania.

18. **Udzielanie Licencji organom władzy publicznej i rządowi USA**. Organy władzy publicznej, w tym rząd Stanów Zjednoczonych Ameryki Północnej, otrzymują Licencje na Oprogramowanie zgodnie z postanowieniami niniejszej Umowy, tj. z uwzględnieniem wszystkich praw i obowiązków określonych w niniejszej Umowie.

19. **Zgodność z przepisami o kontroli handlu**.

a) Licencjobiorca nie będzie, bezpośrednio ani pośrednio, eksportować, reeksportować, przekazywać lub w inny sposób udostępniać Oprogramowania jakiejkolwiek osobie, nie będzie używać go w jakikolwiek sposób, ani też nie będzie uczestniczyć w jakichkolwiek działaniach, które mogłyby spowodować, że firma ESET lub jej spółki holdingowe, spółki zależne oraz spółki zależne dowolnych z jej spółek holdingowych, jak również podmioty kontrolowane przez jej spółki holdingowe („Podmiotami stowarzyszonymi”), naruszyłyby przepisy o kontroli handlu, obejmujące:

i. wszelkie przepisy prawne, które kontrolują, ograniczają lub nakładają wymogi licencyjne na eksport, reeksport lub transfer towarów, oprogramowania, technologii lub usług, wydane lub przyjęte przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność

ii. wszelkie gospodarcze, finansowe (handlowe lub inne) sankcje, ograniczenia, embarga, zakazy importu lub eksportu, zakazy przekazywania funduszy lub aktywów bądź świadczenia usług, lub też równoważne środki nałożone przez jakikolwiek rząd, stan lub organ regulacyjny Stanów Zjednoczonych, Singapuru, Wielkiej Brytanii, Unii Europejskiej lub dowolnego z jej państw członkowskich, albo jakikolwiek kraj, w którym mają być wykonywane zobowiązania wynikające z Umowy lub w którym firma ESET lub dowolny z jej Podmiotów stowarzyszonych są zarejestrowane lub prowadzą działalność.

(Akty prawne, o których mowa w pkt i i ii powyżej, łącznie nazywane są „Przepisami dotyczącymi kontroli handlu").

b) Firma ESET ma prawo zawiesić swoje zobowiązania wynikające z niniejszych warunków lub wypowiedzieć je ze skutkiem natychmiastowym w następujących przypadkach:

i. Gdy firma ESET stwierdzi na podstawie stosownego uzasadnienia, że Użytkownik naruszył lub może naruszyć postanowienia punktu 19 a) Umowy.

ii. Gdy Użytkownik końcowy i/lub Oprogramowanie podlegają przepisom o kontroli handlu i w związku z tym firma ESET stwierdzi na podstawie stosownego uzasadnienia, że dalsze wykonywanie zobowiązań wynikających z Umowy mogłoby spowodować, że firma ESET lub jej Podmioty stowarzyszone naruszyłyby przepisy o kontroli handlu lub byłyby narażone na negatywne konsekwencje wynikające z tych przepisów.

c) Żadne z postanowień Umowy nie ma na celu ani nie powinno być interpretowane lub odczytywane jako nakłanianie bądź wymaganie od którejkolwiek ze stron działania lub powstrzymania się od działania (albo wyrażenia zgody na działanie lub powstrzymanie się od działania) w sposób niezgodny z obowiązującymi przepisami o kontroli handlu, zabroniony przez te przepisy lub podlegający karze w związku z tymi przepisami.

20. **Zawiadomienia**. Wszystkie zawiadomienia oraz zwroty Oprogramowania i Dokumentacji należy kierować na adres: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic, bez uszczerbku dla praw firmy ESET do komunikowania użytkownikowi wszelkich zmian w niniejszej Umowie, Polityce Prywatności, Polityce EOL oraz Dokumentacji zgodnie z punktem 22 niniejszej Umowy. Firma ESET może wysyłać wiadomości e-mail, powiadomienia w aplikacji za pośrednictwem Oprogramowania lub poprzez publikację komunikatów na naszej stronie internetowej. Użytkownik wyraża zgodę na otrzymywanie od firmy ESET informacji prawnych w formie elektronicznej, w tym wszelkich komunikatów dotyczących zmian Warunków, Warunków szczególnych lub Polityki Prywatności, wszelkich propozycji/akceptacji umowy lub zaproszeń do pertraktacji, powiadomień lub innych komunikatów prawnych. Taką komunikację elektroniczną uznaje się za otrzymaną na piśmie, chyba że obowiązujące przepisy prawa wyraźnie wymagają innej formy komunikacji.

21. **Prawo właściwe**. Niniejsza Umowa podlega przepisom prawnym obowiązującym w Słowacji i powinna być interpretowana zgodnie z tymi przepisami. Użytkownik końcowy i Dostawca niniejszym stwierdzają, że do niniejszej Umowy nie mają zastosowania przepisy dotyczące konfliktu praw ani Konwencja Organizacji Narodów Zjednoczonych o umowach międzynarodowej sprzedaży towarów. Licencjobiorca wyraźnie stwierdza, że wszelkie spory lub roszczenia względem Dostawcy wynikające z zawarcia niniejszej Umowy, jak również wszelkie spory lub roszczenia związane z użyciem Oprogramowania będą rozstrzygane przez Sąd Rejonowy dla okręgu Bratislava I. Licencjobiorca wyraźnie poddaje się jurysdykcji tego sądu.

22. **Postanowienia ogólne**. Uznanie któregokolwiek z postanowień niniejszej Umowy za nieważne lub niewykonalne nie wpływa na ważność innych postanowień niniejszej Umowy, które pozostają wówczas w mocy zgodnie z warunkami określonymi w niniejszej Umowie. Niniejsza Umowa została zawarta w języku angielskim. W przypadku sporządzenia tłumaczenia niniejszej Umowy dla wygody lub do innych celów oraz w przypadku rozbieżności pomiędzy wersjami językowymi niniejszej Umowy pierwszeństwo ma wersja angielska.

Firma ESET zastrzega sobie prawo do wprowadzania zmian w Oprogramowaniu oraz modyfikowania warunków niniejszej Umowy, Aneksów, Załączników, Polityki Prywatności, Polityki EOL oraz Dokumentacji lub dowolnej ich części w dowolnym czasie poprzez aktualizowanie odpowiednich dokumentów (i) w celu odzwierciedlenia zmian wprowadzonych w zakresie Oprogramowania oraz w sposobie prowadzenia działalności przez firmę ESET, (ii) ze względów prawnych, regulacyjnych lub bezpieczeństwa lub (iii) w celu zapobiegania nadużyciom lub szkodom. Licencjobiorca zostanie powiadomiony o wszelkich zmianach w niniejszej Umowie za pośrednictwem poczty e-mail, powiadomienia w aplikacji lub innych kanałów komunikacji elektronicznej. Jeśli Licencjobiorca nie zgadza się z proponowanymi zmianami w Umowie, może ją rozwiązać zgodnie z punktem 10 w ciągu 30 dni od otrzymania powiadomienia o zmianie. O ile Licencjobiorca nie wypowie Umowy w tym terminie, proponowane zmiany zostaną uznane za zaakceptowane i wejdą w życie wobec Licencjobiorcy od dnia otrzymania powiadomienia o zmianie.

Niniejsza Umowa stanowi całość porozumienia między Dostawcą a Licencjobiorcą w sprawie Oprogramowania i zastępuje wszelkie wcześniejsze oświadczenia, negocjacje, zobowiązania, wymiany zdań lub reklamy związane z Oprogramowaniem.

ANEKS DO UMOWY

Ocena zabezpieczeń urządzeń podłączonych do sieci. Dodatkowe zapisy dotyczące oceny zabezpieczeń urządzeń podłączonych do sieci brzmią następująco:

Oprogramowanie zawiera funkcję służącą do sprawdzania zabezpieczeń sieci lokalnej Użytkownika końcowego oraz zabezpieczeń urządzeń w sieci lokalnej. Funkcja ta wymaga podania nazwy sieci lokalnej i informacji na temat urządzeń w tej sieci, takich jak obecność, typ, nazwa, adres IP i adres MAC urządzenia w sieci lokalnej w połączeniu z informacjami o licencji. Informacje te obejmują także typ zabezpieczeń i typ szyfrowania sieci bezprzewodowej w przypadku routerów. Wspomniana funkcja może również przekazywać informacje dotyczące dostępności programowego rozwiązania zabezpieczającego na potrzeby ochrony urządzeń w sieci lokalnej.

Ochrona przed niewłaściwym wykorzystaniem danych. Dodatkowe zapisy dotyczące ochrony przed niewłaściwym wykorzystaniem danych brzmią następująco:

Oprogramowanie zawiera funkcję zapobiegającą utracie i niewłaściwemu wykorzystywaniu kluczowych danych wskutek kradzieży Komputera. Funkcja jest domyślnie wyłączona w ustawieniach Oprogramowania. W celu jej aktywacji należy utworzyć Konto ESET HOME, za pośrednictwem którego uruchamiany jest mechanizm gromadzenia danych, gdy komputer zostanie skradziony. W przypadku aktywacji tej funkcji Oprogramowania dane dotyczące ukradzionego komputera zostaną zebrane i wysłane Dostawcy. Mogą zawierać dane dotyczące lokalizacji sieci komputera, dane na temat treści wyświetlanych na ekranie komputera, dane na temat konfiguracji komputera i/lub dane zarejestrowane przez kamerę podłączoną do komputera (odtąd określane „Danymi"). Użytkownik końcowy ma prawo wykorzystywać Dane pozyskane przez tę funkcję i dostarczone za pośrednictwem Konta ESET HOME wyłącznie w celu usunięcia skutków kryzysowej sytuacji spowodowanej kradzieżą komputera. Wyłącznie na potrzeby tej funkcji Dostawca przetwarza Dane zgodnie z Polityką prywatności i obowiązującymi przepisami prawa. Dostawca zezwoli Użytkownikowi końcowemu na dostęp do Danych przez okres niezbędny do realizacji celu, dla którego Dane zostały pozyskane, jednak nie dłuższy niż okres przechowywania określony w Polityce prywatności. Użytkownik końcowy może stosować funkcję ochrony przed niewłaściwym wykorzystaniem danych wyłącznie na Komputerach i kontach, do których ma uprawniony dostęp. Każde zdarzenie nielegalnego użycia będzie zgłaszane właściwym władzom. Dostawca będzie przestrzegał obowiązujących przepisów prawa, a w przypadku niewłaściwego wykorzystania danych będzie wspierał działania uprawnionych organów. Użytkownik przyjmuje do wiadomości i potwierdza, że odpowiada za utrzymanie poufności hasła dostępu do swojego Konta ESET HOME i nie ujawni go żadnym osobom trzecim. Użytkownik końcowy odpowiada za wszelkie przypadki użycia funkcji ochrony przed niewłaściwym wykorzystaniem danych oraz Konta ESET HOME, bez względu na fakt, czy odbyło się to za jego zgodą czy nie. W razie naruszenia zabezpieczeń Konta ESET HOME należy natychmiast powiadomić Dostawcę. Dodatkowe zapisy dotyczące ochrony przed niewłaściwym wykorzystaniem danych mają zastosowanie wyłącznie do użytkowników końcowych produktów ESET Internet Security oraz ESET Smart Security Premium.

ESET Secure Data. Dodatkowe zapisy dotyczące funkcji ESET Secure Data brzmią następująco:

1. Definicje. W niniejszych dodatkowych zapisach dotyczących funkcji ESET Secure Data poniższe słowa mają następujące znaczenia:

a) „Informacje" wszelkie informacje lub dane zaszyfrowane lub odszyfrowane przy użyciu oprogramowania;

b) „Produkty"ESET Secure Dataoprogramowanie i dokumentacja.

c) „ESET Secure Data" oprogramowanie używane do szyfrowania i odszyfrowywania danych elektronicznych;

Wszystkie odniesienia do liczby mnogiej dotyczą również liczby pojedynczej, a wszystkie odniesienia do rodzaju męskiego dotyczą również rodzaju żeńskiego i nijakiego oraz odwrotnie. Słowa bez określonej definicji należy stosować zgodnie z definicjami określonymi w niniejszej Umowie.

2. Dodatkowa deklaracja Użytkownika końcowego. Licencjobiorca przyjmuje do wiadomości i potwierdza co następuje:

a) Do obowiązków Użytkownika końcowego należy ochrona, konserwacja i tworzenie kopii zapasowych informacji.

b) Użytkownik końcowy powinien wykonać pełną kopię zapasową wszystkich informacji i danych (w tym między innymi wszystkich kluczowych informacji i danych) posiadanych na komputerze przed zainstalowaniem Oprogramowania ESET Secure Data.

c) Obowiązkiem Licencjobiorcy jest przechowywanie kopii bezpieczeństwa wszelkich informacji używanych do konfiguracji oprogramowania ESET Secure Datai korzystania z niego, a także utworzenie na osobnym nośniku danych kopii zapasowych wszystkich kluczy szyfrowania, kodów licencyjnych, plików kluczy i innych wygenerowanych danych;

d) Użytkownik końcowy jest odpowiedzialny za korzystanie z Produktów. Dostawca nie ponosi odpowiedzialności za żadne straty, roszczenia ani szkody wynikłe z nieautoryzowanego bądź omyłkowego szyfrowania lub odszyfrowywania Informacji albo innych danych, niezależnie od tego, gdzie i w jaki sposób te informacje lub dane są przechowywane;

e) Choć Dostawca dołożył wszelkich odpowiednich starań, by zapewnić integralność i bezpieczeństwo oprogramowania ESET Secure Data, Produkty (wszystkie i każdy z osobna) nie mogą być wykorzystywane w żadnym z obszarów wymagających bezawaryjnego działania lub które stanowią potencjalne niebezpieczeństwo bądź zagrożenie, w tym między innymi w obiektach jądrowych, systemach nawigacji, kontroli i komunikacji ruchu lotniczego, systemach związanych z bronią i obronnością oraz systemach do podtrzymywania i monitorowania funkcji życiowych;

f) Do Użytkownika końcowego należy obowiązek upewnienia się, że poziom bezpieczeństwa i szyfrowania zapewniany przez produkty jest adekwatny do jego wymagań;

g) Licencjobiorca ponosi odpowiedzialność za użytkowanie Produktów (wszystkich i każdego z osobna), w tym między innymi za zapewnienie, że użytkowanie to jest zgodne ze wszystkimi przepisami prawa obowiązującymi w Republice Słowackiej lub w innym kraju czy regionie, gdzie Produkty są wykorzystywane. Licencjobiorca musi zagwarantować, że przed rozpoczęciem użytkowania produktów upewnił się, czy nie narusza to embarga jakiegokolwiek kraju (Republiki Słowackiej ani innego państwa);

h) Oprogramowanie ESET Secure Data może co pewien czas kontaktować się z serwerami Dostawcy w celu sprawdzenia informacji licencyjnych oraz dostępności poprawek, dodatków service pack i innych aktualizacji, które mogą poprawiać, podtrzymywać, modyfikować lub doskonalić działanie oprogramowania ESET Secure Data, a także może wysyłać ogólne informacje systemowe dotyczące jego działania, zgodnie z Polityką prywatności.

i) Dostawca nie ponosi żadnej odpowiedzialności za straty, szkody, wydatki i roszczenia wynikłe z utraty, kradzieży, nieprawidłowego użytkowania, awarii, uszkodzenia lub zniszczenia haseł, informacji dotyczących konfiguracji, kluczy szyfrowania, kodów aktywacyjnych licencji oraz innych danych generowanych lub przechowywanych podczas korzystania z oprogramowania.

Dodatkowe zapisy dotyczące ESET Secure Data mają zastosowanie wyłącznie do użytkowników końcowych programu ESET Smart Security Premium.

Password Manager Oprogramowanie. Dodatkowe zapisy dotyczące Oprogramowania Password Manager brzmią następująco:

1. Dodatkowa deklaracja Użytkownika końcowego. Licencjobiorca przyjmuje do wiadomości i potwierdza, że nie

może:

a) używać Oprogramowania Password Manager do zastosowań o znaczeniu krytycznym, od których może zależeć ludzkie życie lub mienie. Użytkownik końcowy rozumie, że Oprogramowanie Password Manager nie jest przeznaczone do takich celów i że jego awaria w takich przypadkach może prowadzić do śmierci, obrażeń ciała lub poważnych szkód majątkowych lub ekologicznych, za które Dostawca nie ponosi odpowiedzialności.

OPROGRAMOWANIE PASSWORD MANAGER NIE ZOSTAŁO ZAPROJEKTOWANE, NIE JEST LICENCJONOWANE ANI NIE JEST PRZEZNACZONE DO UŻYWANIA W ŚRODOWISKACH O WYSOKIM RYZYKU WYMAGAJĄCYCH BEZAWARYJNEGO DZIAŁANIA, W TYM MIĘDZY INNYMI DO PROJEKTOWANIA, BUDOWY, UTRZYMANIA ANI EKSPLOATACJI OBIEKTÓW NUKLEARNYCH, SYSTEMÓW NAWIGACJI I KOMUNIKACJI LOTNICZEJ, SYSTEMÓW KONTROLI RUCHU LOTNICZEGO, SYSTEMÓW PODTRZYMYWANIA ŻYCIA ANI SYSTEMÓW UZBROJENIA. DOSTAWCA NIE UDZIELA ŻADNEJ GWARANCJI, WYRAŻONEJ BEZPOŚREDNIO ANI DOROZUMIANEJ, W ODNIESIENIU DO PRZYDATNOŚCI PRODUKTU DO TAKICH CELÓW.

b) używać Oprogramowania Password Manager w sposób, który narusza niniejszą umowę lub przepisy prawa Republiki Słowackiej albo systemu prawnego Użytkownika końcowego. W szczególności Użytkownik końcowy nie może używać Oprogramowania Password Manager do prowadzenia ani promowania jakichkolwiek nielegalnych działań, w tym przesyłania danych lub zawartości szkodliwej oraz takiej, którą można wykorzystywać do jakichkolwiek działań nielegalnych, lub która w jakikolwiek sposób narusza przepisy prawa bądź prawa osób trzecich (w tym prawa własności intelektualnej). Ograniczenie to obejmuje m.in. wszelkie próby uzyskania dostępu do kont w Pamięci masowej (do celów niniejszych dodatkowych zapisów dotyczących Oprogramowania Password Manager „Pamięć masowa” oznacza miejsce w pamięci masowej zarządzane przez Dostawcę lub osobę trzecią w celu umożliwienia synchronizacji i tworzenia kopii zapasowych danych Użytkownika końcowego), a także do wszelkich kont i danych innych użytkowników Oprogramowania Password Manager oraz Pamięci masowej. Jeżeli Użytkownik końcowy naruszy którekolwiek z tych postanowień, Dostawca ma prawo natychmiast rozwiązać niniejszą umowę i obciążyć Użytkownika końcowego kosztami wszelkich niezbędnych środków naprawczych, a także podjąć niezbędne kroki, aby uniemożliwić dalsze korzystanie z Oprogramowania Password Manager bez możliwości zwrotu pieniędzy.

2. OGRANICZENIE ODPOWIEDZIALNOŚCI. OPROGRAMOWANIE PASSWORD MANAGER JEST DOSTARCZANE „W STANIE TAKIM, W JAKIM JEST”. NIE UDZIELA SIĘ ŻADNYCH GWARANCJI ANI RĘKOJMI — ZARÓWNO WYRAŻONYCH JAWNIE, JAK I DOROZUMIANYCH. UŻYTKOWNIK KOŃCOWY KORZYSTA Z TEGO OPROGRAMOWANIA NA WŁASNE RYZYKO. PRODUCENT NIE JEST ODPOWIEDZIALNY ZA UTRATĘ DANYCH, SZKODY, OGRANICZENIE DOSTĘPNOŚCI USŁUGI, W TYM WSZELKIE DANE WYSYŁANE PRZEZ OPROGRAMOWANIE PASSWORD MANAGER DO ZEWNĘTRZNEJ PAMIĘCI MASOWEJ W CELU SYNCHRONIZACJI I TWORZENIA KOPII ZAPASOWYCH DANYCH. SZYFROWANIE DANYCH PRZY UŻYCIU OPROGRAMOWANIA PASSWORD MANAGER NIE OZNACZA ŻADNEJ ODPOWIEDZIALNOŚCI DOSTAWCY W ODNIESIENIU DO BEZPIECZEŃSTWA TYCH DANYCH. UŻYTKOWNIK KOŃCOWY WYRAŹNIE ZGADZA SIĘ Z TYM, ŻE DANE UZYSKANE, UŻYWANE, SZYFROWANE, PRZECHOWYWANE, SYNCHRONIZOWANE LUB WYSYŁANE ZA POMOCĄ OPROGRAMOWANIA PASSWORD MANAGER RÓWNIEŻ MOGĄ BYĆ PRZECHOWYWANE NA SERWERACH OSÓB TRZECICH (DOTYCZY TO TYLKO KORZYSTANIA Z OPROGRAMOWANIA PASSWORD MANAGER Z WŁĄCZONYMI USŁUGAMI SYNCHRONIZACJI I TWORZENIA KOPII ZAPASOWYCH). JEŻELI DOSTAWCA WEDŁUG WŁASNEGO UZNANIA ZDECYDUJE SIĘ UŻYĆ PAMIĘCI MASOWEJ, WITRYNY INTERNETOWEJ, PORTALU INTERNETOWEGO, SERWERA LUB USŁUGI OSOBY TRZECIEJ, NIE PONOSI ON ODPOWIEDZIALNOŚCI ZA JAKOŚĆ, BEZPIECZEŃSTWO ANI DOSTĘPNOŚĆ TAKICH USŁUG OSOBY TRZECIEJ ORAZ NIE PONOSI ODPOWIEDZIALNOŚCI WZGLĘDEM UŻYTKOWNIKA KOŃCOWEGO ZA NARUSZENIA ZOBOWIĄZAŃ PRAWNYCH LUB UMOWNYCH PRZEZ OSOBĘ TRZECIĄ ANI ZA SZKODY, UTRATĘ ZYSKÓW, SZKODY FINANSOWE LUB NIEFINANSOWE ANI INNEGO RODZAJU STRATY PONIESIONE PODCZAS KORZYSTANIA Z TEGO OPROGRAMOWANIA. DOSTAWCA NIE PONOSI ODPOWIEDZIALNOŚCI ZA ZAWARTOŚĆ DANYCH UZYSKANYCH, UŻYWANYCH, SZYFROWANYCH, PRZECHOWYWANYCH, SYNCHRONIZOWANYCH LUB WYSYŁANYCH ZA POMOCĄ OPROGRAMOWANIA PASSWORD MANAGER ANI ZNAJDUJĄCYCH SIĘ W PAMIĘCI MASOWEJ. UŻYTKOWNIK KOŃCOWY PRZYJMUJE DO WIADOMOŚCI, ŻE DOSTAWCA NIE MA DOSTĘPU DO ZAWARTOŚCI

PRZECHOWYWANYCH DANYCH I NIE JEST W STANIE ICH MONITOROWAĆ ANI USUWAĆ ZAWARTOŚCI SZKODLIWEJ W ŚWIETLE PRAWA.

Dostawca jest właścicielem wszystkich praw do ulepszeń, udoskonaleń i poprawek związanych z Oprogramowaniem Password Manager („Ulepszeń"), nawet jeżeli takie Ulepszenia powstały na podstawie opinii, pomysłów lub propozycji zgłoszonych przez Użytkownika końcowego w jakiejkolwiek formie. Użytkownikowi końcowemu nie przysługuje prawo do żadnego wynagrodzenia, w tym honorariów, związanego z takimi Ulepszeniami.

PODMIOTY I LICENCJODAWCY DOSTAWCY NIE PONOSZĄ ODPOWIEDZIALNOŚCI WOBEC UŻYTKOWNIKA KOŃCOWEGO Z TYTUŁU WSZELKICH ROSZCZEŃ I ZOBOWIĄZAŃ WYNIKAJĄCYCH Z UŻYWANIA OPROGRAMOWANIA PASSWORD MANAGER PRZEZ UŻYTKOWNIKA KOŃCOWEGO LUB OSOBY TRZECIE, KORZYSTANIA LUB NIEKORZYSTANIA Z USŁUG JAKICHKOLWIEK FIRM MAKLERSKICH ANI ZE SPRZEDAŻY LUB KUPNA JAKICHKOLWIEK PAPIERÓW WARTOŚCIOWYCH NIEZALEŻNIE OD TEGO, CZY TAKIE ROSZCZENIA SĄ WNOSZONE NA PODSTAWIE JAKIEJKOLWIEK TEORII PRAWA CZY ZASAD SŁUSZNOŚCI.

PODMIOTY I LICENCJODAWCY DOSTAWCY NIE PONOSZĄ ODPOWIEDZIALNOŚCI ZA WSZELKIE BEZPOŚREDNIE, PRZYPADKOWE, SZCZEGÓLNE, POŚREDNIE LUB WTÓRNE SZKODY ZWIĄZANE Z JAKIMKOLWIEK OPROGRAMOWANIEM OSÓB TRZECICH, WSZELKIMI DANYMI, DO KTÓRYCH UŻYTKOWNIK KOŃCOWY UZYSKUJE DOSTĘP ZA POŚREDNICTWEM OPROGRAMOWANIA PASSWORD MANAGER, UŻYTKOWANIEM LUB NIEMOŻNOŚCIĄ UŻYTKOWANIA OPROGRAMOWANIA PASSWORD MANAGER BĄDŹ UZYSKIWANIA DO NIEGO DOSTĘPU, A TAKŻE WSZELKIMI DANYMI UDOSTĘPNIANYMI ZA POŚREDNICTWEM OPROGRAMOWANIA PASSWORD MANAGER ANI ZA TAKIE SZKODY Z NICH WYNIKAJĄCE NIEZALEŻNIE OD TEGO, CZY TAKIE ROSZCZENIA SĄ WNOSZONE NA PODSTAWIE JAKIEJKOLWIEK TEORII PRAWA CZY ZASAD SŁUSZNOŚCI. ODSZKODOWANIA WYKLUCZONE PRZEZ TĘ KLAUZULĘ OBEJMUJĄ MIĘDZY INNYMI ODSZKODOWANIA ZA UTRATĘ ZYSKÓW Z DZIAŁALNOŚCI GOSPODARCZEJ, OBRAŻENIA CIAŁA, USZKODZENIE MIENIA, ZAKŁÓCENIE DZIAŁALNOŚCI GOSPODARCZEJ, UTRATĘ TRANSAKCJI BIZNESOWYCH ORAZ UTRATĘ INFORMACJI OSOBISTYCH. PRZEPISY OBOWIĄZUJĄCE W NIEKTÓRYCH SYSTEMACH PRAWNYCH MOGĄ NIE ZEZWALAĆ NA OGRANICZENIE ODPOWIEDZIALNOŚCI ZA SZKODY PRZYPADKOWE LUB WTÓRNE, ZATEM POWYŻSZE OGRANICZENIE MOŻE NIE MIEĆ ZASTOSOWANIA W PRZYPADKU UŻYTKOWNIKA KOŃCOWEGO. W TAKICH PRZYPADKACH ODPOWIEDZIALNOŚĆ DOSTAWCY JEST OGRANICZONA DO MINIMALNEJ WYSOKOŚCI DOZWOLONEJ PRZEZ PRAWO WŁAŚCIWE.

INFORMACJE PRZEKAZYWANE ZA POŚREDNICTWEM OPROGRAMOWANIA PASSWORD MANAGER, W TYM NOTOWANIA GIEŁDOWE, ANALIZY, INFORMACJE RYNKOWE, WIADOMOŚCI I DANE FINANSOWE, MOGĄ BYĆ OPÓŹNIONE, NIEDOKŁADNE LUB ZAWIERAĆ BŁĘDY BĄDŹ POMINIĘCIA, A PODMIOTY I LICENCJODAWCY DOSTAWCY NIE PONOSZĄ ZA NIE ODPOWIEDZIALNOŚCI. DOSTAWCA MOŻE ZMIENIĆ DOWOLNY ASPEKT LUB FUNKCJĘ OPROGRAMOWANIA PASSWORD MANAGER, ZAKOŃCZYĆ ICH OFEROWANIE LUB UNIEMOŻLIWIĆ KORZYSTANIE Z DOWOLNYCH LUB WSZYSTKICH FUNKCJI BĄDŹ TECHNOLOGII W OPROGRAMOWANIU PASSWORD MANAGER W DOWOLNYM MOMENCIE I BEZ UPRZEDNIEGO POWIADOMIENIA UŻYTKOWNIKA KOŃCOWEGO.

JEŻELI POSTANOWIENIA W NINIEJSZYM ARTYKULE OKAŻĄ SIĘ NIEWAŻNE Z JAKIEGOKOLWIEK POWODU LUB DOSTAWCA ZOSTANIE UZNANY ZA ODPOWIEDZIALNEGO ZA STRATY, SZKODY ITP. PRZEZ OBOWIĄZUJĄCE PRZEPISY PRAWA, STRONY ZGADZAJĄ SIĘ CO DO TEGO, ŻE ODPOWIEDZIALNOŚĆ DOSTAWCY WOBEC UŻYTKOWNIKA JEST OGRANICZONA DO ŁĄCZNEJ KWOTY OPŁAT LICENCYJNYCH WNIESIONYCH PRZEZ UŻYTKOWNIKA KOŃCOWEGO.

UŻYTKOWNIK KOŃCOWY ZOBOWIĄZUJE SIĘ DO ZWOLNIENIA Z ODPOWIEDZIALNOŚCI, OBRONY I ZABEZPIECZENIA DOSTAWCY ORAZ JEGO PRACOWNIKÓW, PODMIOTY ZALEŻNE I STOWARZYSZONE, A TAKŻE PARTNERÓW REBRANDINGOWYCH I INNYCH WOBEC WSZELKICH ROSZCZEŃ, ZOBOWIĄZAŃ, ODSZKODOWAŃ, STRAT, KOSZTÓW, WYDATKÓW I OPŁAT, JAKIE PODMIOTY TE MOGĄ PONIEŚĆ WSKUTEK KORZYSTANIA PRZEZ UŻYTKOWNIKA KOŃCOWEGO Z OPROGRAMOWANIA PASSWORD MANAGER.

3. Dane w Oprogramowaniu Password Manager. Jeżeli Użytkownik końcowy celowo nie wybierze innej opcji, wszelkie wprowadzone przez niego dane, które są zapisywane w bazie danych Oprogramowania Password Manager, są przechowywane w formacie zaszyfrowanym na komputerze lub innym urządzeniu pamięci masowej zdefiniowanym przez Użytkownika końcowego. Użytkownik końcowy rozumie, że w przypadku usunięcia lub uszkodzenia jakiejkolwiek bazy danych Oprogramowania Password Manager bądź innych plików wszystkie zawarte w nich dane zostaną nieodwracalnie utracone, a Użytkownik końcowy rozumie i akceptuje ryzyko takiej utraty. To, że dane osobowe są przechowywane w zaszyfrowanym formacie na komputerze, nie oznacza, że takich informacji nie może wykraść lub nadużyć ktoś, kto odkryje hasło główne bądź uzyska dostęp do zdefiniowanego przez klienta urządzenia aktywującego do otwierania bazy danych. Użytkownik końcowy ponosi odpowiedzialność za zabezpieczanie wszelkich metod uzyskiwania dostępu do danych.

4. Przesyłanie danych osobowych do Dostawcy lub Pamięci Masowej. Jeżeli Użytkownik końcowy wybierze taką opcję i wyłącznie w celu zapewnienia terminowej synchronizacji oraz tworzenia kopii zapasowych danych, Oprogramowanie Password Manager przesyła dane osobowe z bazy danych oprogramowania Password Manager — hasła, dane logowania, konta i tożsamości — przez Internet do Pamięci Masowej. Dane są przesyłane wyłącznie w formie zaszyfrowanej. Używanie Oprogramowania Password Manager do wypełniania formularzy online hasłami, nazwami użytkownika lub innymi danymi może wymagać przesyłania tych informacji przez Internet do witryny określonej przez Użytkownika końcowego. Ta transmisja danych nie jest inicjowana przez oprogramowanie Password Manager i dlatego Dostawca nie ponosi odpowiedzialności za bezpieczeństwo takich interakcji z jakimikolwiek witrynami obsługiwanymi przez różnych dostawców. Wszelkich transakcji za pośrednictwem Internetu, niezależnie od tego, czy są powiązane z Oprogramowaniem Password Manager czy nie, Użytkownik końcowy dokonuje według własnego uznania i na własne ryzyko oraz ponosi wyłączną odpowiedzialność za uszkodzenie systemu komputerowego lub utratę danych na skutek pobierania lub wykorzystywania jakichkolwiek materiałów bądź usług. Aby zminimalizować ryzyko utraty cennych danych, Dostawca zaleca klientom okresowe wykonywanie kopii zapasowych bazy danych i innych ważnych plików na dyskach zewnętrznych. Dostawca nie jest w stanie zapewnić pomocy w odzyskaniu utraconych lub uszkodzonych danych. Jeżeli Dostawca świadczy usługi tworzenia kopii zapasowych plików baz danych na wypadek uszkodzenia lub usunięcia takich plików na komputerach użytkowników, taka usługa tworzenia kopii zapasowych jest oferowana bez żadnych gwarancji i rękojmi oraz nie pociąga za sobą żadnej odpowiedzialności Dostawcy względem Użytkownika końcowego.

Korzystanie z Oprogramowania Password Manager oznacza zgodę Użytkownika końcowego na to, że oprogramowanie może co pewien czas kontaktować się z serwerami Dostawcy w celu sprawdzenia informacji licencyjnych oraz dostępności poprawek, dodatków service pack i innych aktualizacji, które mogą poprawiać, podtrzymywać, modyfikować lub doskonalić działanie Oprogramowania Password Manager. Oprogramowanie Password Manager może wysyłać ogólne informacje systemowe związane ze swoim funkcjonowaniem w sposób zgodny z Polityką prywatności.

5. Instrukcja i informacje dotyczące odinstalowania. Wszelkie informacje z bazy danych, które Użytkownik końcowy chce zachować, należy wyeksportować przed odinstalowaniem Oprogramowania Password Manager.

Dodatkowe zapisy dotyczące Oprogramowania Password Manager mają zastosowanie wyłącznie do użytkowników końcowych programu ESET Smart Security Premium.

ESET LiveGuard. Dodatkowe zapisy dotyczące funkcji ESET LiveGuard brzmią następująco:

Oprogramowanie zawiera funkcję dodatkowej analizy plików przesłanych przez Użytkownika końcowego. Dostawca będzie wykorzystywał wyłącznie pliki przesłane przez Użytkownika końcowego i wyniki analizy zgodnie z Polityką Prywatności oraz odpowiednimi przepisami prawa.

Dodatkowe zapisy dotyczące ESET LiveGuard mają zastosowanie wyłącznie do użytkowników końcowych programu ESET Smart Security Premium.

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

Zasady ochrony prywatności

Jako administrator danych, firma ESET, spol. s r. o., z siedzibą pod adresem Einsteinova 24, 851 01 Bratislava, Slovak Republic, zarejestrowana w Rejestrze Handlowym prowadzonym przez Sąd Rejonowy dla okręgu Bratislava I, w sekcji Sro pod numerem 3586/B, numer w rejestrze przedsiębiorców: 31333532 („ESET" lub „My"), przykłada szczególną wagę do kwestii ochrony danych osobowych. Chcemy spełnić wymóg przejrzystości znormalizowany prawnie zgodnie z Ogólnym rozporządzeniem o ochronie danych UE („RODO"). W związku z tym publikujemy niniejszą Politykę prywatności wyłącznie w celu przekazania klientowi jako osobie, której dane dotyczą (dalej „Użytkownik końcowy" lub „Ty"), informacji na następujące tematy z obszaru ochrony danych osobowych:

- Podstawa prawna przetwarzania danych osobowych,
- Udostępnianie danych i poufność,
- Bezpieczeństwo danych,
- Prawa osoby, której dane dotyczą,
- Przetwarzanie danych osobowych
- Informacje kontaktowe.

Podstawa prawna przetwarzania danych osobowych

Firma ESET przetwarza dane wyłącznie w oparciu o kilka podstaw prawnych przewidzianych przepisami prawa dotyczącymi ochrony prywatności danych osobowych. Przetwarzanie danych osobowych przez firmę ESET jest niezbędne głównie do realizacji Umowę Licencyjną Użytkownika Końcowego („EULA") z Użytkownikiem końcowym (art. 6 ust. 1 lit. b ustawy RODO), która obejmuje dostarczanie produktów lub usług firmy ESET, chyba że wyraźnie zaznaczono inaczej, np.:

- Podstawa prawna dotycząca uzasadnionego interesu (art. 6 ust. 1 lit. f ustawy RODO), która umożliwia firmie ESET przetwarzanie danych oraz monitorowanie sposobu korzystania i zadowolenia z Usług przez użytkowników w celu zapewnienia najlepszej możliwej ochrony, wsparcia i doświadczenia. W świetle obowiązujących przepisów prawa działania marketingowe są uznawane za uzasadniony interes, dlatego firma ESET polega na nich w komunikacji marketingowej z klientami.

- Firma ESET może wymagać od Użytkownika zgody w określonych sytuacjach (art. 6 ust. 1 lit. a ustawy RODO), gdy taka podstawa prawna zostanie uznana za najodpowiedniejszą lub jeśli wymaga tego prawo.

- Przestrzeganie obowiązków prawnych (art. 6 ust. 1 lit. c ustawy RODO), np. określenie wymagań dotyczących komunikacji elektronicznej, fakturowania lub dokumentów rozliczeniowych.

Udostępnianie danych i poufność

Nie udostępniamy Twoich danych stronom trzecim. Jednakże ESET jest firmą działającą na całym świecie za pośrednictwem swoich spółek stowarzyszonych oraz partnerów będących częścią sieci sprzedaży, usług i pomocy technicznej. Przetwarzane przez firmę ESET informacje dotyczące licencji, rozliczeń i pomocy technicznej mogą być przesyłane między nami a naszymi partnerami oraz spółkami stowarzyszonymi z tytułu realizacji Umowy Licencyjnej Użytkownika Końcowego, na przykład świadczenia usług lub udzielania pomocy technicznej.

Firma ESET woli przetwarzać swoje dane w Unii Europejskiej (UE). Jednak w zależności od Twojej lokalizacji (w razie korzystania z naszych produktów i/lub usług poza UE) i/lub wybranej usługi może być konieczne przekazanie Twoich danych do kraju spoza UE. Na przykład korzystamy z usług stron trzecich w związku z przetwarzaniem w chmurze. W takich przypadkach starannie dobieramy naszych usługodawców i zapewniamy odpowiedni poziom ochrony danych za pomocą wymogów umownych oraz środków technicznych i organizacyjnych. Z reguły zawieramy standardowe klauzule umowne UE, w razie potrzeby uzupełniając je dodatkowymi przepisami umownymi.

W przypadku niektórych krajów spoza UE, takich jak Wielka Brytania i Szwajcaria, UE określiła już porównywalny poziom ochrony danych. Ze względu na ten porównywalny poziom ochrony danych przekazywanie danych do tych krajów nie wymaga żadnego specjalnego upoważnienia ani zgody.

Bezpieczeństwo danych

Firma ESET stosuje odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu zabezpieczeń odpowiedniego do zagrożeń. Dokładamy wszelkich starań, aby zapewnić nieprzerwaną poufność, integralność, dostępność i odporność systemów oraz usług związanych z przetwarzaniem danych. W przypadku naruszenia ochrony danych zagrażającego prawom i wolnościom Użytkownika końcowego jesteśmy jednak gotowi do powiadomienia o tym fakcie odpowiednich organów nadzorczych oraz osoby, których dane dotyczą.

Prawa osób, których dane dotyczą

Prawa każdego Użytkownika końcowego są ważne i chcemy poinformować, że wszyscy Użytkownicy końcowi (z dowolnego kraju UE oraz spoza UE) mają następujące prawa zagwarantowane przez firmę ESET. Aby skorzystać z praw osoby, której dane dotyczą, możesz skontaktować się z nami za pośrednictwem formularza pomocy technicznej lub poczty elektronicznej, wysyłając wiadomość na adres dpo@eset.sk. W celach identyfikacyjnych prosimy o podanie następujących informacji: Imię i nazwisko, adres e-mail oraz – jeśli jest dostępny – klucz licencyjny lub numer klienta oraz przynależność do firmy. Prosimy o powstrzymanie się od przesyłania nam jakichkolwiek innych danych osobowych, takich jak data urodzenia. Zwracamy uwagę, że aby móc przetworzyć Twoje zapytanie, a także w celach identyfikacyjnych, będziemy przetwarzać Twoje dane osobowe.

Prawo do wycofania zgody. Prawo do wycofania zgody obowiązuje wyłącznie w przypadku przetwarzania na podstawie udzielonej zgody. Jeśli przetwarzamy Twoje dane osobowe na podstawie Twojej zgody, masz prawo wycofać tę zgodę w dowolnym momencie bez podania przyczyn. Wycofanie zgody jest skuteczne tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jej wycofaniem.

Prawo do wyrażenia sprzeciwu. Prawo do wyrażenia sprzeciwu wobec przetwarzania danych obowiązuje wyłącznie w przypadku przetwarzania na podstawie uzasadnionego interesu firmy ESET lub strony trzeciej. Jeśli przetwarzamy Twoje dane osobowe w celu ochrony uzasadnionego interesu, będąc osobą, której dane dotyczą, masz prawo w dowolnym momencie sprzeciwić się uzasadnionemu interesowi wskazanemu przez nas i przetwarzaniu Twoich danych osobowych. Sprzeciw jest skuteczny tylko na przyszłość i nie wpływa na zgodność z prawem danych przetwarzanych przed jego wyrażeniem. Jeśli przetwarzamy Twoje dane osobowe w celach marketingu bezpośredniego, nie jest konieczne podawanie powodów Twojego sprzeciwu. Dotyczy to również profilowania, o ile jest ono związane z marketingiem bezpośrednim. We wszystkich innych przypadkach prosimy o krótkie poinformowanie nas o powodzie sprzeciwu wobec przetwarzania Twoich danych osobowych zgodnie z uzasadnionym interesem firmy ESET.

Należy pamiętać, że w niektórych przypadkach, pomimo wycofania zgody, jesteśmy uprawnieni do dalszego przetwarzania Danych osobowych na podstawie innej podstawy prawnej, na przykład w celu realizacji umowy.

Prawo do uzyskania dostępu. Jako osoba, której dane dotyczą, masz prawo do bezpłatnego uzyskania w dowolnym momencie informacji o Twoich danych przechowywanych przez firmę ESET.

Prawo do sprostowania. Jeśli nieumyślnie przetwarzamy Twoje nieprawidłowe dane osobowe, masz prawo do ich poprawienia.

Prawo do usunięcia danych i prawo do ograniczenia przetwarzania. Jako osoba, której dane dotyczą, masz prawo do zażądania usunięcia lub ograniczenia przetwarzania swoich danych osobowych. Jeśli przetwarzamy Twoje dane osobowe, na przykład na mocy wyrażonej przez Ciebie zgody, którą następnie wycofujesz, a nie istnieje żadna inna podstawa prawna, taka jak umowa, natychmiast usuwamy Twoje dane osobowe. Twoje dane osobowe zostaną również usunięte z końcem naszego okresu przechowywania, gdy tylko nie będą już potrzebne do określonych dla nich celów.

Jeśli wykorzystujemy Twoje dane osobowe wyłącznie do celów marketingu bezpośredniego i zdecydujesz się odwołać swoją zgodę lub sprzeciwisz się leżącemu u podstaw przetwarzania uzasadnionemu interesowi firmy ESET, ograniczymy przetwarzanie Twoich danych osobowych, umieszczając Twoje dane kontaktowe na naszej wewnętrznej czarnej liście, aby uniknąć niechcianego kontaktu. W innych przypadkach Twoje dane osobowe zostaną usunięte.

Należy pamiętać, że możemy być zobowiązani do przechowywania Twoich danych do czasu wygaśnięcia obowiązków przechowywania i okresów wymaganych przez ustawodawcę lub organy nadzorcze. Obowiązki i okresy przechowywania mogą również wynikać z ustawodawstwa słowackiego. Po ich upłynięciu właściwe dane zostaną rutynowo usunięte.

Prawo do przeniesienia danych. Z przyjemnością przekazujemy Użytkownikowi będącemu osobą, której dane dotyczą, jego dane osobowe przetwarzane przez firmę ESET w formacie xls.

Prawo do wniesienia skargi. Jako osoba, której dane dotyczą, masz prawo do wniesienia w dowolnym momencie skargi do organu nadzorczego. Firma ESET podlega prawu słowackiemu i obowiązują ją przepisy Unii Europejskiej o ochronie danych. Właściwym organem nadzorczym ds. danych jest Urząd Ochrony Danych Osobowych Republiki Słowackiej z siedzibą pod adresem Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Przetwarzanie danych osobowych

Usługi zaimplementowane w produkcie firmy ESET są przez nas świadczone zgodnie z postanowieniami Umowy EULA, ale niektóre z nich mogą wymagać szczególnej uwagi. Chcemy przekazać szczegółowe informacje na temat gromadzenia danych związanych ze świadczonymi przez nas usługami. Świadczymy różne usługi opisane w Umowie Licencyjnej Użytkownika Końcowego oraz w dokumentacja. Abyśmy mogli dostarczać nasze usługi, musimy gromadzić następujące informacje:

Dane licencyjne i rozliczeniowe. Imię i nazwisko, adres e-mail, klucz licencyjny i (w stosownych przypadkach) adres, przynależność do firmy i dane dotyczące płatności są gromadzone i przetwarzane przez firmę ESET w celu ułatwienia aktywacji licencji, dostarczenia klucza licencyjnego, przypomnień o wygaśnięciu, realizacji wniosków o pomoc techniczną, weryfikacji autentyczności licencji, świadczenia naszych usług oraz dostarczania innych powiadomień, w tym wiadomości marketingowych, zgodnie z obowiązującymi przepisami lub zgodą użytkownika. Firma ESET jest prawnie zobowiązana do przechowywania informacji rozliczeniowych przez okres 10 lat, jednak informacje licencyjne zostaną zanonimizowane nie później niż 12 miesięcy po wygaśnięciu licencji.

Aktualizacja i inne statystyki. Przetwarzane informacje obejmują informacje na temat procesu instalacji oraz komputera użytkownika końcowego (np. platformy, na której jest zainstalowany nasz produkt), a także informacje o działaniu i funkcjach naszych produktów, takie jak informacje o systemie operacyjnym, dane dotyczące sprzętu, identyfikatory instalacji, identyfikatory licencji, adres IP, adres MAC oraz ustawienia konfiguracji produktu. Są one przetwarzane do celów dostarczania aktualizacji usług oraz konserwacji, zapewniania bezpieczeństwa i ulepszania naszej infrastruktury.

Informacje te są przechowywane oddzielnie od informacji identyfikacyjnych wymaganych do celów licencjonowania i fakturowania, ponieważ nie wymagają identyfikacji Użytkownika końcowego. Okres przechowywania wynosi do 4 lat.

System reputacji ESET LiveGrid®. Skróty jednokierunkowe związane z infekcjami są przetwarzane na potrzeby systemu reputacji ESET LiveGrid®, który poprawia wydajność naszych rozwiązań do ochrony przed szkodliwym oprogramowaniem, porównując skanowane pliki z białą i czarną listą obiektów w chmurze. Użytkownik końcowy nie jest identyfikowany podczas tego procesu.

System informacji zwrotnych ESET LiveGrid®. Próbki podejrzanego kodu i metadanych używane przez system reputacji ESET LiveGrid®, które pozwalają produktom ESET reagować natychmiast na potrzeby użytkowników końcowych i zapewnić ochronę przed najnowszymi zagrożeniami. Korzystamy następujących danych otrzymanych od użytkowników końcowych

- Dane dotyczące infekcji, takie jak próbki potencjalnych wirusów i innych szkodliwych programów, a także podejrzane, potencjalnie niepożądane i potencjalnie niebezpieczne obiekty (np. pliki wykonywalne i wiadomości e-mail zgłoszone jako spam lub oznaczone przez nasz produkt);

- Informacje dotyczące korzystania z Internetu, takie jak adres IP, informacje geograficzne, pakiety IP, adresy URL i ramki sieci Ethernet;

- Pliki zrzutu awaryjnego i informacje w nich zawarte.

Nie mamy zamiaru gromadzić danych spoza tego zakresu, jednak czasami nie da się tego uniknąć. Przypadkowo zebrane dane mogą być zawarte w samym szkodliwym oprogramowaniu (i zebrane bez wiedzy i zgody użytkownika końcowego) lub mogą stanowić część nazwy pliku lub adresu URL. Nie zamierzamy wykorzystywać tych danych w naszych systemach ani przetwarzać ich w celu określonym w tej Polityce prywatności.

Wszystkie informacje uzyskane i przetwarzane za pośrednictwem systemu informacji zwrotnych ESET LiveGrid® są przeznaczone do użycia bez identyfikowania Użytkownika końcowego.

Ocena zabezpieczeń urządzeń podłączonych do sieci. Na potrzeby dostarczania funkcji oceny zabezpieczeń urządzeń podłączonych do sieci przetwarzamy nazwy sieci lokalnej i informacje na temat urządzeń w tej sieci, takie jak dane dotyczące obecności, typ, nazwa, adres IP i adres MAC urządzenia w sieci lokalnej w połączeniu z informacjami o licencji. Informacje te obejmują także typ zabezpieczeń i typ szyfrowania sieci bezprzewodowej w przypadku routerów. Informacje dotyczące licencji pozwalające na identyfikację Użytkownika końcowego będą anonimizowane nie później niż 12 miesięcy po wygaśnięciu licencji.

Pomoc techniczna. Aby zapewnić możliwość świadczenia pomocy technicznej lub pomocy innego rodzaju, mogą być wymagane dane kontaktowe i informacje dotyczące licencji przesyłane w zgłoszeniach do działu pomocy. W zależności od wybranego przez Użytkownika końcowego sposobu komunikacji możemy gromadzić następujące dane: adres e-mail, numer telefonu, informacje o licencji, szczegółowe informacje o produkcie oraz opis zgłoszenia do pomocy technicznej. W celu podniesienia jakości udzielanej pomocy technicznej możemy poprosić Użytkownika końcowego o dodatkowe informacje. Dane przetwarzane w celu świadczenia pomocy technicznej są przechowywane przez 4 lata.

Ochrona przed niewłaściwym wykorzystaniem danych. W przypadku utworzenia konta ESET HOME na stronie https://home.eset.com i aktywacji funkcji przez Użytkownika końcowego w związku z kradzieżą komputera zbierane i przetwarzane będą następujące informacje: dane lokalizacyjne, zrzuty ekranu, dane o konfiguracji komputera oraz dane rejestrowane przez kamerę komputera. Zgromadzone dane są przechowywane na naszych serwerach lub na serwerach naszych usługodawców przez okres 3 miesięcy.

Password Manager. W przypadku aktywowania funkcji Password Manager dane logowania są przechowywane w

zaszyfrowanej formie wyłącznie na komputerze lub innym urządzeniu Użytkownika. Jeśli Użytkownik aktywuje usługę synchronizacji, w celu jej świadczenia zaszyfrowane dane będą przechowywane na serwerach firmy ESET lub jej usługodawców. Do zaszyfrowanych danych nie będą mieli dostępu ani firma ESET, ani usługodawca. Tylko Użytkownik ma klucz do odszyfrowania takich danych. Dane zostaną usunięte po dezaktywacji funkcji.

ESET LiveGuard. Jeśli użytkownik zdecyduje się aktywować usługę ESET LiveGuard, wymaga ona przesłania przykładowych próbek, takich jak pliki wstępnie zdefiniowane i wybrane przez Użytkownika końcowego. Próbki wybrane do zdalnej analizy zostaną przesłane do usługi ESET, a wynik analizy zostanie odesłany z powrotem do komputera Użytkownika. Wszelkie podejrzane próbki są przetwarzane w taki sam sposób jak dane zbierane przez system informacji zwrotnych ESET LiveGrid®.

Program poprawy jakości doświadczeń użytkowników. Jeśli zdecydowałeś się aktywować Program poprawy jakości doświadczeń użytkowników , na podstawie Twojej zgody będą gromadzone i wykorzystywane anonimowe informacje telemetryczne dotyczące korzystania z naszych produktów.

Należy pamiętać, że jeśli osoba korzystająca z naszych produktów i usług nie jest Użytkownikiem końcowym, który zakupił produkt lub usługę i zawarł z nami Umowę Licencyjną Użytkownika Końcowego (np. pracownik Użytkownika końcowego, członek rodziny lub osoba w inny sposób upoważniona przez Użytkownika końcowego do korzystania z produktu lub usługi zgodnie z umową EULA), przetwarzanie danych odbywa się w uzasadnionym interesie firmy ESET w rozumieniu art. 6 ust. 1 lit. f ustawy RODO, aby umożliwić użytkownikowi upoważnionemu przez Użytkownika końcowego korzystanie z produktów i usług świadczonych przez nas zgodnie z Umową EULA.

Informacje kontaktowe

Jeżeli użytkownik chce skorzystać z prawa przysługującego mu jako osobie, której dane dotyczą, a także w przypadku pytań lub wątpliwości, użytkownik może przesłać do nas wiadomość na adres:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk