G Data Security 2015

Podręcznik użytkownika

ISBN 978-83-61624-20-2

G Data Software Sp. z o.o.
ul. 28 Lutego 2, 78-400 Szczecinek
tel. 094 3729 650
faks 094 3729 659
e-mail: biuro@gdata.pl
Raiffeisen Bank Polska S.A.
78 1750 1396 0000 0000 2014 8837

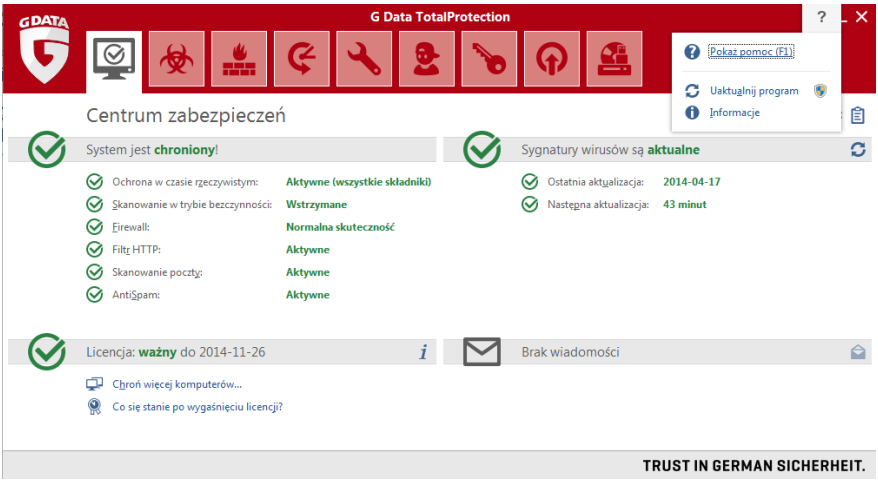
Wydanie pierwsze, kwiecień 2014

G Data Software Sp. z o.o.

Spis treści

1 Wstęp

Dziękujemy za zakupienie oprogramowania G Data i mamy nadzieję, że produkt w pełni spełni Twoje oczekiwania. Wszelkie zapytania, sugestie i zgłoszenia problemów prosimy kierować do Pomoc technicznej G Data.



Jeśli potrzebujesz informacji na temat konkretnej opcji, w każdej chwili możesz wcisnąć F1 aby otworzyć stronę pomocy odnoszącą się do bieżącego okna.

1.1 Pomoc techniczna

Masz problemy z zainstalowaniem programu? Program nie działa? Zgłoś problem do Pomocy technicznej G Data. Aby zgłosić problem do Pomocy technicznej, wyślij wiadomość z opisem problemu. Można również zgłosić problem telefonicznie.

Dobre przygotowanie do rozmowy przyspieszy proces udzielania pomocy i ułatwi kontakt z serwisantem.

- Przygotuje dane klienta (dane dostępu do aktualizacji, Numer rejestracyjny lub Numer klienta)
- Upewnij się, że oprogramowanie G Data Software jest zainstalowane na

komputerze

- Zgromadź informacje na temat sprzętu i innego oprogramowania zainstalowanego w komputerze
- Przygotuj kartkę i coś do pisania

e-mail: pomoc@gdata.pl

telefon: 94 3729 650

Odpowiedzi na większość pytań znajdziesz w podręczniku użytkownika lub w pliku pomocy. Warto zajrzeć też na stronę internetową G Data Software i przejrzeć najczęściej zadawane pytania na stronie: www.gdata.pl/pomoc.

1.2 Instalacja programu

Oprogramowanie G Data Software funkcjonuje prawidłowo na komputerach o następujących parametrach:

- System Windows 8.1, 8, 7 lub Vista (32/64-bit), od 1 GB RAM
- System Windows XP z dodatkiem SP 2 (tylko 32-bit), od 512 MB RAM

Jeśli jest to nowy komputer, lub masz pewność, że był wcześniej chroniony przez skuteczne oprogramowanie antywirusowe, odinstaluj bieżący program antywirusowy i przystąp do instalacji według poniższego opisu. Jeśli masz uzasadnione podejrzenie, że komputer mógł zostać zainfekowany, możesz przed instalacją wykonać skanowanie przy pomocy płyty startowej G Data. Szczegóły znajdziesz w rozdziale: Płyta startowa 114.

Krok 1. - Uruchomienie instalacji

Uruchom instalację jednym ze wskazanych sposobów, w zależności od nośnika, jakim dysponujesz:

- Płyta CD/DVD: Włóż płytę do napędu. Okno autostartu lub instalatora programu G Data otworzy się automatycznie.
- Plik pobrany z Internetu: Kliknij dwukrotnie plik instalacyjny pobrany z Internetu aby uruchomić instalację.

Wskazówka: Jeśli okno instalatora nie otwiera się automatycznie, istnieje

możliwość, że funkcja automatycznego uruchamiania nośników zewnętrznych systemu Windows jest wyłączona lub nieprawidłowo skonfigurowana.

- Jeśli zamiast okna startowego instalacji uruchomi się okno wyboru, wybierz polecenie Uruchom AUTOSTRT.EXE.

- Jeśli nie otwiera się żadne okno, uruchom Eksplorator Windows, kliknij ikonkę nośnika z programem i uruchom plik instalacyjny, np. setup.exe.

Krok 2. - Wersja językowa

Wybierz język instalacji programu G Data i kliknij przycisk **Dalej**. Domyślnie zaznaczony jest język systemu operacyjnego.

Krok 3. - Metoda instalacji

Kreator instalacji umożliwia wybranie instalacji standardowej lub instalacji użytkownika. Zalecamy wybranie opcji instalacji standardowej.

Inicjatywa G Data Malware Information: Specjaliści G Data Security Labs rozwijają mechanizmy chroniące Klientów G Data przed złośliwym oprogramowaniem. Skuteczność działania i szybkość tworzenia mechanizmów ochronnych zależy w dużej mierze od posiadanych informacji na temat złośliwego oprogramowania. Informacje na temat szkodliwych programów najlepiej pozyskiwać bezpośrednio z zaatakowanych lub zainfekowanych komputerów. Inicjatywa G Data Malware Information umożliwia przekazywanie informacji na temat zagrożeń. Dzięki przystąpieniu do Inicjatywy, możesz wspomóc zespół specjalistów G Data Security Labs wysyłając informacje o złośliwych programach atakujących Twój komputer. Twój udział w Inicjatywie G Data Malware Information wpłynie bezpośrednio na podniesienie jakości produktów oferowanych przez G Data Software.

Wskazówka: Instalacja użytkownika umożliwia ręczny wybór składników oprogramowania oraz wskazanie innego niż domyślny folderu instalacji.

Krok 4 - Warunki licencji

Przeczytaj i zatwierdź warunki licencji na użytkowanie programu.

Krok 5 - Instalacja użytkownika (opcjonalnie)

Po wybraniu opcji instalacji użytkownika pojawią się dwa okna umożliwiające wskazanie innego niż domyślny folderu instalacji oraz ręczny wybór składników oprogramowania do instalacji. Jeśli wybierzesz w

poprzednim oknie instalację standardową, te okna się nie pojawią.

- Użytkownika: Zaznacz lub usuń zaznaczenie przy wybranych składnikach programu. Zainstalowane zostaną tylko zaznaczone moduły (np. AntiVirus, AntiSpam itd.). Zestaw dostępnych składników zależy od wersji programu - G Data AntiVirus, G Data InternetSecurity lub G Data TotalProtection.

- Pełna: Zainstalowane zostaną wszystkie składniki.

- Minimalna: Zostanie zainstalowany tylko obowiązkowy składnik - AntiVirus.

Modyfikowanie zestawu składników: Po zakończeniu instalacji można zmodyfikować skład komponentów przez ponowne uruchomienie instalatora. Jeśli dysponujesz nowszą wersją instalacyjną programu, możesz uaktualnić zainstalowany produkt poprzez uruchomienie nowego instalatora bez potrzeby usuwania bieżącej wersji. W trakcie instalacji możesz również zmodyfikować zestaw składników programu.

Krok 6 - Wersja programu

Wybierz, czy chcesz skorzystać z pełnej, opłaconej wersji programu G Data, czy też chcesz wypróbować program korzystając z możliwości aktywacji wersji testowej.

Krok 7 - Aktywacja licencji

Podczas instalacji program zapyta o metodę aktywacji produktu. Program będzie aktualizował się przez Internet po dokonaniu aktywacji.

- **Nowy numer rejestracyjny:** Jeśli chcesz zarejestrować zakupiony numer rejestracyjny produktu G Data, wybierz tę opcję. Wypełnij formularz i kliknij przycisk **Zarejestruj**.

Po zarejestrowaniu dane dostępu do aktualizacji zostaną automatycznie wprowadzone do programu, a także wysłane na wskazany w formularzu adres e-mail.

- **Dane dostępu:** Jeśli Twój numer został wcześniej zarejestrowany, możesz od razu wprowadzić dane dostępu (użytkownik i hasło).

Wskazówka: Dane dostępu znajdziesz w wiadomości e-mail potwierdzającej rejestrację.

Jeśli nie masz danych w zasięgu ręki, lub nie masz dostępu do wiadomości z

potwierdzeniem rejestracji, kliknij przycisk Nie pamiętasz danych dostępu? Zostaniesz przeniesiony na stronę internetową umożliwiającą ponowne wysłanie danych dostępu po wpisaniu adresu e-mail wskazanego w procesie rejestracji. W razie problemów z odzyskaniem danych skontaktuj się z Pomocą techniczną 1.

- **Uaktywnię później:** Jeśli nie chcesz uaktywniać oprogramowania, lub chcesz to zrobić później, wybierz tę opcję. Produkt będzie w pełni funkcjonalny, ale nie będzie pobierał aktualizacji z Internetu. W celu uaktywnienia oprogramowania w późniejszym terminie, uruchom aktualizację. Program sam zaoferuje dostępne opcje aktywacji.

Krok 8 - Zakończenie instalacji

Po zakończeniu instalacji wymagane jest ponowne uruchomienia komputera. Kliknij przycisk **Zakończ** aby sfinalizować instalację. Jeśli nie chcesz uruchamiać komputera ponownie w tym momencie, usuń zaznaczenie z pola **Teraz wykonaj restart**.

2 Po instalacji

Okno interfejsu oprogramowania G Data możesz otworzyć klikając ikonę programu na pulpicie. Widok **Centrum zabezpieczeń** informuje o stanie poszczególnych modułów zabezpieczających. Szczegóły znajdziesz w rozdziale Centrum zabezpieczeń 6.

Oprócz okna interfejsu programu G Data Software, masz do dyspozycji kilka innych możliwości skorzystania z zainstalowanego oprogramowania:

Ikonka paska zadań: Ikona programu umożliwia szybki dostęp do niektórych opcji programu. W razie potrzeby wyświetla znak ostrzeżenia informujący o potrzebie ingerencji użytkownika lub przypominający o wyłączonych czasowo zabezpieczeniach. Więcej szczegółów w rozdziale: Ikonka paska zadań 116.

Niszczarka: Narzędzie umożliwiające bezpowrotne usuwanie plików. Aby zniszczyć plik, przeciągnij go nad ikonę Niszczarki i upuść. Możesz również skorzystać z menu kontekstowego prawego klawisza. Narzędzie jest dostępne tylko w pakietach zabezpieczeń G Data. Nie znajdziesz go w produkcie G Data AntiVirus.

Szybkie skanowanie
Znalazłeś na dysku podejrzany plik? Chcesz szybko przeskanować plik pobrany z Internetu lub folder? Nie musisz uruchamiać okna programu G Data Software. Kliknij dany plik lub folder prawym klawiszem myszki i wybierz polecenie Skanuj programem G Data AntiVirus.

Po zainstalowaniu programu komputer uruchamia się inaczej niż zwykle: Możliwe, że płyta z programem G Data nadal znajduje się w napędzie, i zamiast systemu Windows uruchamia się system operacyjny z płyty startowej. Aby uruchomić system Windows, wyjmij płytę z napędu.

3 Centrum zabezpieczeń

Po zainstalowaniu oprogramowania G Data Software ochrona komputera odbywa się całkowicie automatycznie. Uruchamianie Centrum zabezpieczeń jest niezbędne tylko w celu modyfikacji zaawansowanych ustawień programu.

Widok Centrum zabezpieczeń przedstawia stan poszczególnych składników ochrony w jednym oknie. Ikona poziomu zabezpieczeń informuje o stanie produktu.

Zielony kolor oznacza, że ustawienia zabezpieczeń są optymalne i system jest bezpieczny.

Czerwony kolor oznacza potencjalne zagrożenie dla systemu operacyjnego. Niezbędna jest natychmiastowa interwencja użytkownika.

Szary kolor oznacza, że dana funkcja nie została włączona.

Żółty kolor oznacza, że wskazana jest interwencja użytkownika.

Modyfikacji ustawień i funkcji możesz dokonać poprzez kliknięcie wybranej pozycji Centrum zabezpieczeń lub poprzez przycisk ustawień.

Pozostałe funkcje

Ustawienia 70: Ten przycisk otwiera okno ustawień dotyczących poszczególnych warstw ochrony.

Protokół 113: Otwiera listę wszystkich raportów z działań programu. Klikając nagłówki poszczególnych kolumn, możesz posortować je według czasu rozpoczęcia, rodzaju, tytułu lub statusu.

Ten przycisk znajdujący się w prawym, górnym rogu okna rozwija listę dodatkowych poleceń programu:

Pokaż pomoc: Otwiera plik pomocy programu G Data. Jeśli potrzebujesz informacji na temat konkretnej opcji, w każdej chwili możesz wcisnąć w konkretnym oknie klawisz F1.

Uaktualnij program: Jeśli dostępna jest aktualizacja plików programu G Data dla zainstalowanej wersji produktu, ten przycisk umożliwia jej pobranie i zainstalowanie.

Informacje: Kliknij aby wyświetlić szczegółowe informacje o zainstalowanej wersji oprogramowania.

3.1 Składniki ochrony

Centrum zabezpieczeń umożliwia szybkie modyfikowanie ustawień niektórych składników programu. Kliknij wiersz z nazwą składnika, aby rozwinąć listę dostępnych poleceń.

Ochrona w czasie rzeczywistym

Mechanizmy chroniące komputer w czasie rzeczywistym weryfikują na bieżąco działanie systemu operacyjnego badając każdą próbę zapisu lub odczytu dowolnego pliku. Pozwala to zablokować wszelkie próby uruchomienia złośliwego kodu lub dokonania manipulacji na plikach systemu operacyjnego. Ochrona powinna być stale włączona. Jest to kluczowy element zabezpieczający.

- **Wyłącz Strażnika:** Jeśli mimo wszystko chcesz wyłączyć ochronę w czasie rzeczywistym, możesz to zrobić uruchamiając to polecenie. Jeżeli zamierzasz w ten sposób wpłynąć na wydajność komputera, sprawdź przedtem koniecznie, czy nie pomaga wybranie profilu ustawień dla wolniejszych komputerów w oknie Skuteczność / Szybkość 71. Wyłączenie Strażnika na stałe jest zdecydowanie niezalecane.

- **Wyłącz kontrolę zachowania:** Kontrola zachowania to inteligenty moduł weryfikujący zachowanie aplikacji, co umożliwia wykrywanie

nieznanych zagrożeń niezależnie od sygnatur wirusów. Jest to moduł zwiększający skuteczność ochrony przed zagrożeniami.

- **Zaawansowane...:** To polecenie otwiera okno Ustawienia | AntiVirus | Ochrona w czasie rzeczywistym 74.

Ostatnie skanowanie w trybie bezczynności

Ten wiersz wyświetla informację o terminie wykonania ostatniego skanowania w trybie bezczynności. Kliknij wiersz aby wyświetlić listę dostępnych poleceń.

- **Skanuj komputer:** Polecenie uruchamia skanowanie wszystkich dysków lokalnych oraz obszarów systemowych. Skanowanie może spowodować wolniejsze działanie niektórych aplikacji. Szczegóły na temat skanowania znajdziesz w rozdziale Skanowanie 14.

- **Wywołaj skanowanie w trybie bezczynności:** Skanowanie w trybie bezczynności uruchamiane jest automatycznie i przebiega niezauważalnie w tle. Jest uruchamiane w momencie, kiedy komputer nie jest używany. Jeśli program zarejestruje aktywność systemu Windows lub użytkownika, skanowanie zostanie wstrzymane do ponownego przejścia w stan bezczynności. To polecenie pozwala na wymuszenie rozpoczęcia kolejnego skanowania w trybie bezczynności.

- **Wyłącz skanowanie w trybie bezczynności:** Jeśli nie chcesz aby Twój komputer był sukcesywnie skanowany w trakcie przerw w pracy, możesz wyłączyć całkowicie funkcję skanowania w tym trybie za pomocą tego polecenia (niezalecane).

Firewall

Firewall pełni funkcje zapory internetowej chroniącej komputery działające pod kontrolą systemu operacyjnego Windows przed nieautoryzowanym dostępem do danych oraz przed atakami hakerów działających w sieci lokalnej oraz w Internecie. Ten składnik dostępny jest w produktach G Data InternetSecurity oraz G Data TotalProtection. Kliknij wiersz aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

- **Wyłącz Firewall:** W razie potrzeby możesz wyłączyć zaporę połączeń na zadany okres czasu. W takim przypadku Twój komputer nadal będzie połączony z Internetem/siecią, ale połączenia nie będą chronione przed atakami (niezalecane)

- **Wyłącz autopilota:** Domyślnie program ma włączony tryb autopilota, dzięki czemu funkcjonuje bez potrzeby ingerencji użytkownika. Po

wyłączeniu trybu autopilota, zapora przełącza się w tryb ręczny, który wymaga potwierdzania reguł stosowania połączeń wychodzących dla aplikacji i serwisów. Program będzie wyświetlał zapytania w momencie uruchomienia każdego programu, który łączy się po raz pierwszy z Internetem w określony sposób. Wyłączenie autopilota nie jest zalecane.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | Firewall | Tryb automatyczny 102.

Filtr HTTP

Filtr automatycznie weryfikuje otwierane strony pod kątem złośliwych programów i wyłudzania informacji. Jeśli pobierana zawartość lub otwierana strona zostanie zakwalifikowana jako niebezpieczna, zagrożenie zostanie zgłoszone w postaci komunikatu, a strona nie otworzy się.

Jeśli spróbujesz pobrać niebezpieczny plik, program G Data zatrzyma proces pobierania przed rozpoczęciem zapisu w folderze tymczasowych plików internetowych. W przeglądarce pojawi się odpowiedni komunikat.

- **Wyłącz filtr stron HTTP:** Polecenie umożliwia wyłączenie ochrony przeglądarek. Może zaistnieć taka potrzeba, np. w przypadku pobierania dużych plików z zaufanych źródeł. Generalnie komputer jest chroniony przez inne warstwy ochrony pomimo wyłączenia ochrony w przeglądarce. Nie zalecamy jednak wyłączania filtra HTTP na stałe, ze względu na popularne ostatnio ataki stron wyłudzających informacje.

- **Zdefiniuj wyjątki:** W niektórych przypadkach, skanowanie HTTP może spowodować nieprawidłowe wyświetlanie danej strony Internetowej lub blokowanie usługi dostępnej przez stronę. Program umożliwia konfigurację wyjątków HTTP. Strony ustawione jako wyjątki nie są skanowane. Szczegóły na temat konfiguracji wyjątków HTTP znajdziesz w rozdziale: Wyjątki HTTP 84.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | AntiVirus | Filtrowanie HTTP 83.

Skanowanie poczty

Składnik chroniący korespondencję elektroniczną dba o to, aby do programów pocztowych nie przedostawały się zarażone wiadomości. Zapobiega również nieświadomemu wysyłaniu niebezpiecznych załączników.

- **Wyłącz ochronę poczty:** To polecenie powoduje wyłączenie mechanizmu filtrującego pocztę elektroniczną. Jeśli wyłączysz filtr poczty,

wiadomości nie będą skanowane. Wyłączenie ochrony poczty nie jest zalecane.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | AntiVirus | Skanowanie wiadomości 86.

Microsoft Office Outlook: W programie Microsoft Office Outlook skanowanie poczty realizowane jest dodatkowo przez specjalną wtyczkę. Wtyczka realizuje wszystkie czynności związane z ochroną, które oferuje standardowa ochrona protokołów POP3/IMAP/SMTP. Po zainstalowaniu programu znajdziesz w dodatkach i w menu aplikacji Microsoft Office Outlook poleceń umożliwiających skanowanie folderów z wiadomościami.

AntiSpam

Oferty, reklamy, niezamówione newslettery – ilość niechcianych wiadomości wzrasta nieuchronnie. Skrzynki odbiorcze momentalnie przepełniają się od nadmiaru nieprzydatnych wiadomości. Składnik AntiSpam doskonale chroni skrzynkę przed napływem spamu. Kombinacja nowoczesnych kryteriów rozpoznawania spamu zapobiega pomyłkom w odróżnianiu spamu od wiadomości marketingowych. Kliknij wiersz aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

- **Protokół: Spam...:** Ten przycisk otwiera okno z listą wiadomości zakwalifikowanych przez program jako spam. Poniżej znajdują się 4 przyciski umożliwiające zmianę kwalifikacji wiadomości, odświeżenie widoku lub usunięcie pozycji z listy. Zmodyfikowanie kwalifikacji wiadomości przyciskiem Na zaufaną listę... spowoduje, że wiadomości od nadawcy zaznaczonej wiadomości nie będą w przyszłości filtrowane i oznaczane jako niechciane.

- **Protokół: Wiadomości...:** Ten przycisk otwiera okno z listą maili zakwalifikowanych przez program jako zwykłe wiadomości. Poniżej znajdują się 4 przyciski umożliwiające zmianę kwalifikacji wiadomości, odświeżenie widoku lub usunięcie pozycji z listy. Zmodyfikowanie kwalifikacji wiadomości przyciskiem Na czarną listę... spowoduje, że wiadomości od nadawcy zaznaczonej wiadomości będą w przyszłości automatyczne oznaczane jako spam.

- **Edytuj dozwolone...:** Przycisk otwiera listę nadawców i domen, od których wiadomości nigdy nie będą traktowane jako spam. Okno umożliwia wprowadzanie nowych pozycji, modyfikowanie ich, a także usuwanie adresów/domen. Przyciski Import... i Eksport umożliwiają zapisanie listy w postaci pliku tekstowego, a także odczytanie adresów z przygotowanego wcześniej pliku i umieszczenie ich na liście. Pozycje w pliku (adresy lub domeny) powinny być ułożone jeden pod drugim.

- **Edytuj niedozwolone...:** Przycisk otwiera listę nadawców i domen, od których wiadomości zawsze będą traktowane jako spam. Okno umożliwia wprowadzanie nowych pozycji, modyfikowanie ich, a także usuwanie adresów/domen. Przyciski Import... i Eksport umożliwiają zapisanie listy w postaci pliku tekstowego, a także odczytanie adresów z przygotowanego wcześniej pliku i umieszczenie ich na liście. Pozycje w pliku (adresy lub domeny) powinny być ułożone jeden pod drugim.

- **Wyłącz filtr spamu:** Ten przycisk spowoduje wyłączenie filtra. Wiadomości nie będą wtedy filtrowane.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | AntiSpam | Filtr spamu 94.

Ostatnia aktualizacja

Ten wiersz wskazuje dokładny czas ostatniego przeprowadzenia aktualizacji sygnatur wirusów programu G Data. Jeśli wiersz wyróżniony jest czerwonym kolorem, przeprowadź jak najszybciej aktualizację sygnatur wirusów. Kliknij wiersz aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

- Uaktualnij sygnatury wirusów: Sygnatury wirusów są pobierane automatycznie w godzinnych odstępach. Kliknij to polecenie, jeśli chcesz wymusić natychmiastowe pobranie najnowszych sygnatur wirusów.

- Wyłącz automatyczne aktualizacje: Jeśli nie chcesz aby program automatycznie pobierał sygnatury wirusów, kliknij to polecenie. Wyłączenie automatu aktualizującego wzorce wirusów nie jest bezpieczne. Wyłączaj tę funkcję tylko w świadomie i w uzasadnionych przypadkach.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | AntiVirus | Aktualizacje 81.

Następna aktualizacja

Ten wiersz wskazuje termin następnej zaplanowanej aktualizacji sygnatur wirusów. Kliknij wiersz aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

- Uaktualnij sygnatury wirusów: Sygnatury wirusów są pobierane automatycznie w godzinnych odstępach. Kliknij to polecenie, jeśli chcesz wymusić natychmiastowe pobranie najnowszych sygnatur wirusów.

- Wyłącz automatyczne aktualizacje: Jeśli nie chcesz aby program

automatycznie pobierał sygnatury wirusów, kliknij to polecenie. Wyłączenie automatu aktualizującego wzorce wirusów nie jest bezpieczne. Wyłączaj tę funkcję tylko w świadomie i w uzasadnionych przypadkach.

- **Zaawansowane...:** Szczegóły znajdziesz w rozdziale Ustawienia | AntiVirus | Aktualizacje 81.

3.2 Licencja

W tej sekcji znajdziesz informację o czasie pozostałym do końca licencji na oprogramowanie G Data Software. Przed zakończeniem okresu licencyjnego otrzymasz automatyczne powiadomienie mailowe z propozycją wykupienia kontynuacji licencji przez internet.

Na niedługo przed upłynięciem licencji na korzystanie z programu, program wyświetli komunikat o nadchodzącym terminie upływu ważności licencji.

Jeżeli chcesz dokonać przedłużenia licencji przez sklep internetowy, kliknij dymek z komunikatem, a następnie przycisk **Zamów**.

Jeśli produkt nie został aktywowany podczas instalacji, w sekcji Licencja dostępny jest przycisk **Aktywuj licencję**. Pojawi się okno, które umożliwia wprowadzenie danych dostępu do aktualizacji lub zarejestrowanie nowej licencji.

Po dokonaniu aktywacji produktu, w sekcji Licencja dostępny jest przycisk **Chroń więcej komputerów...**. Kliknięcie przycisku otwiera stronę umożliwiającą zamówienie dodatkowych licencji w wygodny sposób.

3.3 Moduły programu

W zależności od zainstalowanej wersji programu do dyspozycji masz szereg ikon służących do przełączania między następującymi modułami programu:

Centrum zabezpieczeń 6: Twoje osobiste centrum zabezpieczeń. W tym widoku uzyskasz zestawienie informacji na temat stanu najważniejszych aspektów ochrony Twojego komputera.

Ochrona antywirusowa 14: Umożliwia ręczne uruchomienie

skanowania całego komputera lub poszczególnych elementów. Z tego miejsca możesz przejść do widoku Kwarantanny lub utworzyć nośnik startowy.

Firewall 18: Firewall pełni funkcje zapory internetowej chroniącej komputery działające pod kontrolą systemu operacyjnego Windows przed nieautoryzowanym dostępem do danych oraz przed atakami hakerów działających w sieci lokalnej oraz w Internecie. Ten składnik dostępny jest w produktach G Data InternetSecurity oraz G Data TotalProtection.

Backup 29: Kopie zapasowe danych zapisywane na dyskach przenośnych lub innych dyskach podłączonych do komputera to doskonała metoda na uniknięcie utraty danych na skutek awarii sprzętu lub np. kradzieży laptopa.

Tuner 44: Składnik Tuner umożliwia wygodną i prostą optymalizację ustawień komputera. Przypomina automatycznie o aktualizowaniu systemu Windows i aplikacji pakietu Microsoft Office, defragmentuje dyski twarde. Można zaplanować także automatyczne usuwanie plików tymczasowych, a także niepotrzebnych elementów z rejestru. Dzięki tym usprawnieniom system Windows zyska na wydajności i przejrzystości.

Kontrola rodzicielska 47: Moduł kontroli rodzicielskiej umożliwia ograniczenie użytkownikom dostępu do stron internetowych zawierających niepożądane treści, a także zarządzanie czasem dostępu do internetu oraz komputera.

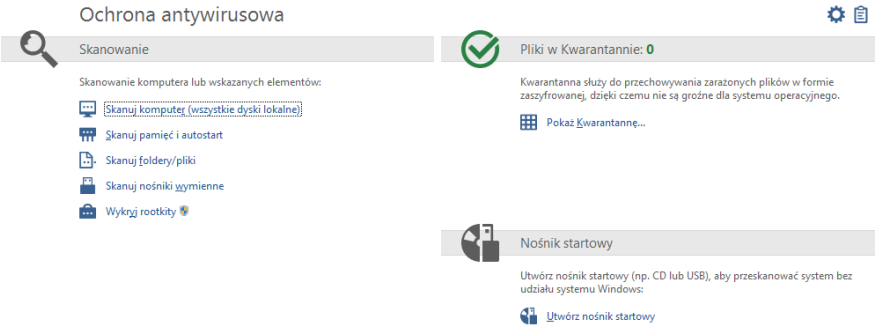
Sejf 57: Ten składnik pakietu umożliwia przechowywanie danych w wirtualnych sejfach. Można utworzyć dowolną ilość sejfów do których dostęp chroniony jest hasłem. Każdy sejf może mieć kilka różnych haseł dostępu na różnym poziomie uprawnień. Można przykładowo założyć hasło, które umożliwi jedynie odczyt danych z sejfu.

Autostart Manager 68: Moduł umożliwiający wybiórcze opóźnianie uruchamiania programów, które włączane są przy starcie systemu operacyjnego. Dzięki tej funkcji komputer może uruchamiać się szybciej i nie jest obciążony przy starcie.

Kontrola urządzeń 70: Umożliwia kontrolowanie dostępu do urządzeń podłączonych do komputera - napędy przenośne USB, stacje dyskietek, napędy optyczne.

4 Ochrona antywirusowa

Ten moduł programu G Data umożliwia ręczne uruchomienie skanowania całego komputera lub poszczególnych elementów. Z tego miejsca możesz przejść do widoku Kwarantanny lub utworzyć nośnik startowy.



Uwaga: Ręczne skanowanie komputera i nośników wymiennych jest uzupełniającym elementem ochrony. Podstawowe funkcje ochronne spełnia Strażnik oraz funkcja skanowania w trybie bezczynności. Dodatkowe skanowanie zalecane jest np. po wykryciu infekcji przez Strażnika.

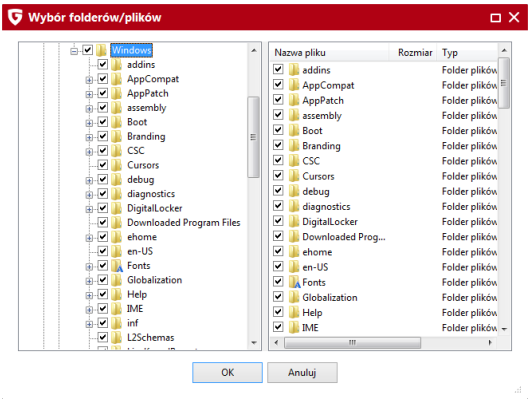
4.1 Skanowanie

Wybierz z listy rodzaj skanowania, który chcesz uruchomić ręcznie.

Skanuj komputer (wszystkie dyski lokalne): Polecenie uruchamia skanowanie wszystkich dysków lokalnych oraz obszarów systemowych. Szczegóły znajdziesz w rozdziale. Szczegóły znajdziesz w rozdziale Jak przeprowadzić skanowanie? 117.

Skanuj pamięć i autostart: Program sprawdzi pliki oraz biblioteki wszystkich bieżących procesów. Pozwoli to usunąć szkodliwe programy z pamięci (jeżeli nie od razu - zostaną wyeliminowane po kolejnym uruchomieniu komputera). W ten sposób zablokowana zostanie aktywność działających w systemie wirusów, bez potrzeby skanowania całego dysku. Proces ten trwa o wiele krócej niż gruntowne skanowanie całego dysku twardego.

Skanuj foldery/pliki: To polecenie umożliwia przeskanowanie wybranych napędów, folderów i plików. Kliknij wiersz aby otworzyć okno wyboru umożliwiające zaznaczenie elementów do przeskanowania.Po lewej stronie okna wyboru znajduje się drzewo folderów rozwijanych przyciskiem +. Skontrolowany zostanie każdy zaznaczony obiekt. Jeśli nie zaznaczysz wszystkich podkatalogów czy plików danego katalogu, wiersz będzie koloru szarego. Na czarno oznaczane są foldery skanowane w całości.



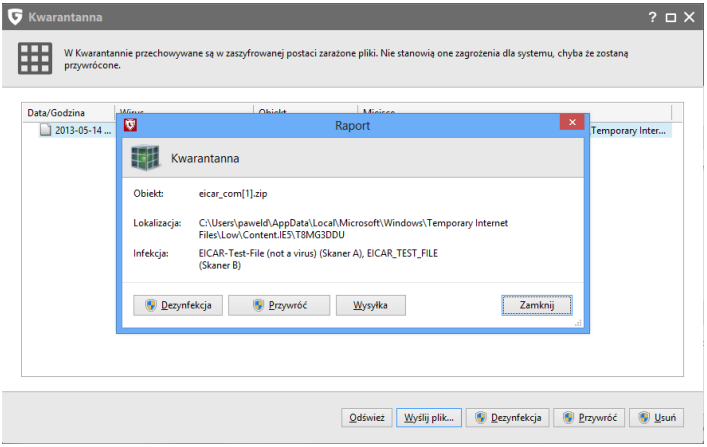
Skanuj nośniki wymienne: Ta funkcja służy do skanowania wymiennych napędów komputera, czyli płyt CD-ROM, DVD-ROM, dyskietek, kart pamięci Flash i pendrive'ów. Uruchomienie tej funkcji spowoduje przeskanowanie wszystkich nośników wymiennych widocznych w systemie. Pamiętaj, że programy nie mogą usuwać wirusów z nośników zabezpieczonych przed zapisem i płyt jednokrotnego zapisu. W przypadku wykrycia wirusa na takim nośniku, program może tylko sporządzić raport z wykrycia.

Wykryj rootkity: Użycie tego polecenia spowoduje uruchomienie narzędzia skanującego system na obecność rootkitów z pominięciem skanowania całego komputera.

4.2 Kwarantanna

Kwarantanna to zaszyfrowany folder, w którym program przechowuje bezpiecznie zarażone pliki. Nie stanowią one w tej postaci zagrożenia dla systemu. Decyzję, co zrobić z zarażonymi plikami, można w ten sposób odłożyć na później. Zaznacz wybrany plik w folderze Kwarantanny i zdecyduj, czy chcesz go zdezynfekować, przywrócić czy też usunąć.

Pokaż Kwarantannę: Kliknij to polecenie aby otworzyć okno Kwarantanny.



- **Odśwież:** Odświeża widok okna pobierając aktualne informacje z systemu operacyjnego.
- **Wyślij plik:** Istnieje możliwość przesłania zarażonego pliku z Kwarantanny do Ambulansu G Data. Możesz to zrobić, jeśli masz skonfigurowane konto e-mail w programie pocztowym.

  Specjaliści G Data Security Labs rozwijają mechanizmy chroniące Klientów G Data przed złośliwym oprogramowaniem. Skuteczność

działania i szybkość tworzenia mechanizmów ochronnych zależy w dużej mierze od posiadanych informacji na temat złośliwego oprogramowania. Informacje na temat szkodliwych programów najlepiej pozyskiwać bezpośrednio z zaatakowanych lub zainfekowanych komputerów. Inicjatywa G Data Malware Information umożliwia przekazywanie informacji na temat zagrożeń. Dzięki przystąpieniu do Inicjatywy, możesz wspomóc zespół specjalistów G Data Security Labs wysyłając informacje o złośliwych programach atakujących Twój komputer.

- **Dezynfekcja:** Jeżeli wirus nie zniszczył zarażonego pliku, program może usunąć kod wirusa i odzyskać dane w oryginalnej postaci. Odzyskane pliki przenoszone są automatyczne do folderu źródłowego.

- **Przywróć:** Czasem zachodzi konieczność przywrócenia pliku do pierwotnej lokalizacji, pomimo, że nie da się go zdezynfekować gdyż wirus uszkodził jego część. Jeżeli zajdzie potrzeba przywrócenia zarażonego pliku, zaleca się zachowanie wszelkich możliwych środków ostrożności (odłączenie komputera od sieci lokalnej/Internetu, sporządzenie kopii zapasowych ważnych, niezarażonych danych).

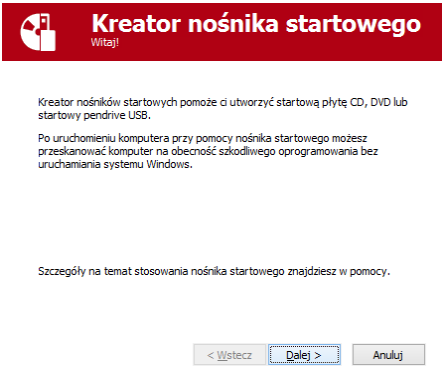
- **Usuń:** Jeżeli plik nie jest potrzebny, można go po prostu usunąć z Kwarantanny.

4.3 Nośnik startowy

Dzięki nośnikowi można przeprowadzić skanowanie lokalnych napędów, wykazujące ewentualną obecność wirusa lub rootkita na dysku lub w pamięci. Skanowanie odbywa się bez udziału systemu Windows.

Szczegóły dotyczące obsługi nośnika startowego znajdziesz w rozdziale Skanowanie nośnikiem startowym 114.

Aby utworzyć nośnik startowy kliknij polecenie **Utwórz nośnik startowy** i postępuj zgodnie ze wskazówkami. W trakcie tworzenia nośnika możesz uaktualnić sygnatury wirusów, aby utworzony nośnik rozpoznawał również najnowsze zagrożenia. Jako nośnik startowy możesz wykorzystać czystą płytę CD/DVD lub pendrive USB.



Przywracanie z kopii: Nośnik startowy umożliwia również przywrócenie partycji lub dysku, jeśli wcześniej sporządzona została kopia zapasowa (dostępne w pakiecie G Data TotalProtection).

5 Firewall

Firewall pełni funkcje zapory internetowej chroniącej komputery działające pod kontrolą systemu operacyjnego Windows przed nieautoryzowanym dostępem do danych oraz przed atakami hakerów działających w sieci lokalnej oraz w Internecie. Ten składnik dostępny jest w produktach G Data InternetSecurity oraz G Data TotalProtection. Kliknij wiersz aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

- Status 19: Ten widok wyświetla podstawowe informacje o stanie zapory.
- Sieci 20: Widok przedstawia zestawienie połączeń sieciowych i informuje o powiązaniach połączeń z zestawami reguł.
- Zestaw reguł 22: Lista gotowych zestawów reguł zapory.

Ustawienia 102: Ten przycisk otwiera okno globalnych ustawień zapory.

Protokół 113: Otwiera listę wszystkich raportów z działań zapory. Klikając nagłówki poszczególnych kolumn, możesz posortować raporty.

5.1 Status

Widok zawiera podstawowe informacje na temat aktualnego stanu zapory. Symbol ostrzeżenia oznacza, że ustawienia zapory wymagają interwencji użytkownika.

Przez kliknięcie danego wpisu można rozwinąć listę dostępnych poleceń.

- **Status:** Ten wiersz widoku Status informuje o zastosowanym trybie skuteczności zapory. Domyślnie zapora ma ustawioną normalną skuteczność działania.

- **Tryb:** Ten wiersz informuje o ustawionym trybie pracy zapory. Domyślnie włączony jest tryb Automatyczny (autopilot).

Tryb autopilota (zalecany): Zapora działa automatycznie i nie wymaga ingerencji użytkownika. Odpowiednie reguły dostępu są tworzone automatycznie.

Ręczne ustawianie reguł: Wyłączenie autopilota spowoduje, że zapora będzie wymagała od użytkownika potwierdzenia każdej tworzonej reguły dostępu do Internetu dla aplikacji lub usługi.

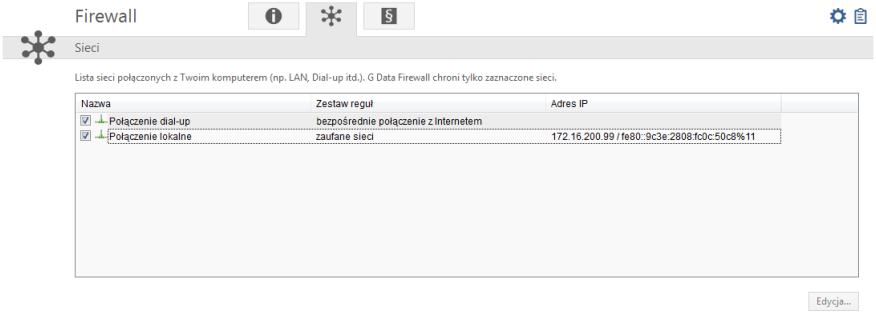
- **Sieci:** Zapora kontroluje wszystkie połączenia sieciowe komputera. Jeśli przynajmniej jedno połączenie nie jest niechronione, np. po ręcznym wyłączeniu ochrony połączenia, przy pozycji Sieci widoku Status pojawi się symbol ostrzegawczy.

- **Zablokowane ataki:** Jeżeli zapora zablokuje atak przeprowadzony z sieci lokalnej lub internetu, w wierszu Zarejestrowane ataki pojawi się odpowiednia adnotacja. Dwukrotne kliknięcie wiersza otworzy okno zawierające szczegóły na temat zablokowanych ataków.

- **Radar aplikacji:** Ta pozycja okna Status pokazuje ilość aplikacji zablokowanych automatycznie przez zaporę. Jeżeli przy pozycji Radar aplikacji pojawi się symbol ostrzeżenia, kliknij dwukrotnie wiersz Radar aplikacji aby otworzyć okno z listą zablokowanych programów. Aby odblokować dany program, zaznacz go i kliknij przycisk Zezwól.

5.2 Sieci

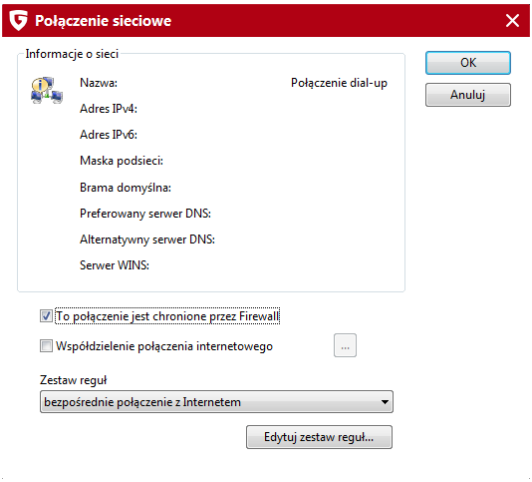
Widok przedstawia listę dostępnych połączeń sieciowych (np. LAN, WLAN, dial-up) Twojego komputera. Okno informuje również o zestawie reguł 22 stosowanym dla każdego połączenia oraz o adresach IP aktywnych połączeń.



Dwukrotne kliknięcie wiersza danego połączenia otwiera okno właściwości umożliwiające modyfikację ustawień zapory dla tego połączenia.

5.2.1 Właściwości połączenia

W oknie wyświetlone są szczegóły połączenia. Można tutaj również modyfikować ustawienia zapory dla wybranego połączenia sieciowego, a także uruchomić asystenta tworzenia reguł.



- **Informacje o sieci:** Szczegółowe informacje na temat danego połączenia: Adres IP (v4 oraz v6), Maska podsieci, Brama domyślna, Serwer DNS oraz Serwer WINS.

- **To połączenie jest chronione przez Firewall:** Wyłączenie tej opcji spowoduje wyłączenie zapory dla danego połączenia. Należy to robić tylko w uzasadnionych przypadkach.

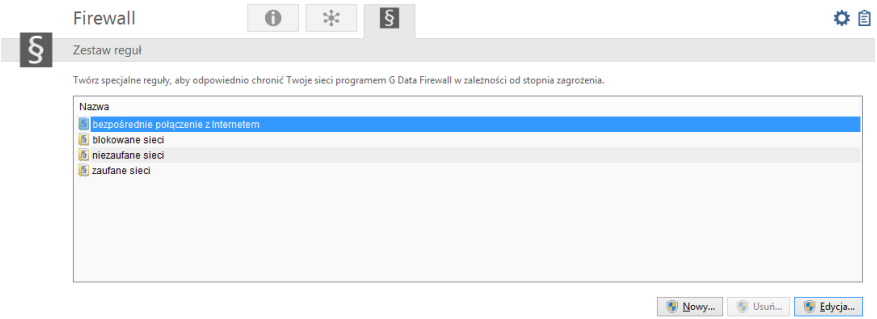
- **Współdzielenie połączenia internetowego:** W przypadku połączeń wdzwanianych istnieje możliwość udostępnienia połączenia internetowego innym sieciom. Opcja dostępna tylko dla połączeń dial-up.

- **Pozwól na automatyczną konfigurację (DHCP):** To ustawienie musi być włączone w sieciach dynamicznie przydzielających adresy IP poprzez serwer DHCP (Dynamic Host Configuration Protocol).

- **Zestaw reguł:** Możesz wybrać jeden z gotowych zestawów reguł z przewijanej listy, lub kliknąć przycisk **Edytuj zestaw reguł...** aby zmodyfikować zaawansowane ustawienia zaznaczonego na liście zestawu reguł. Szczegóły znajdziesz w rozdziale Zestaw reguł 22.

5.3 Zestaw reguł

Widok przedstawia listę predefiniowanych zestawów, gotowych do użycia po zainstalowaniu programu. Można modyfikować ustawienia istniejących zestawów reguł, lub tworzyć nowe zestawy dla specjalnych potrzeb.



Podstawowych czterech zestawów reguł dla sieci zaufanych, niezaufanych, blokowanych i bezpośredniego połączenia z Internetem nie da się usunąć. Zestawy reguł, które stworzysz sam, można będzie usunąć.

5.3.1 Modyfikacja i tworzenie zestawów reguł

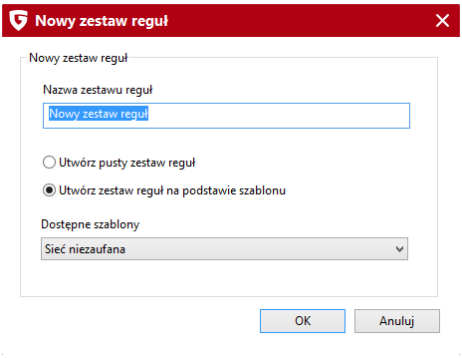
Do każdego połączenia można przyporządkować wybrany zestaw reguł. Poszczególne sieci mogą być chronione przez zaporę w konkretny sposób. Domowa sieć chroniona przez router wyposażony w sprzętową zaporę wymaga niższego poziomu zabezpieczeń niż komputer podłączony bezpośrednio do Internetu.

Zapora proponuje cztery gotowe zestawy reguł dla różnych typów sieci:

- **Bezpośrednie połączenia z Internetem:** Dla komputerów połączonych bezpośrednio z Internetem.
- **Niezaufane sieci:** Sieci otwarte, np. hot-spoty lub inne sieci publiczne o nieznanych ustawieniach.
- **Zaufane sieci:** Do zaufanych można zaliczyć np. prawidłowo zabezpieczone sieci domowe oraz korporacyjne.
- **Blokowane sieci:** Tego zestawu można użyć, jeśli połączenie komputera

z Internetem ma być czasowo lub trwale zablokowane. Ten zestaw reguł jest pusty, więc cały ruch połączeń objętych tym zestawem jest blokowany. Można udostępnić część usług lub aplikacji tego zestawu przez ręczne dodawanie reguł.

Za pomocą przycisku **Nowy**, możesz stworzyć własny zestaw reguł dla wybranej sieci. Wpisz nazwę dla tworzonego zestawu reguł i wybierz, czy chcesz utworzyć pusty zestaw reguł, czy skorzystać z jednego z dostępnych zestawów reguł.



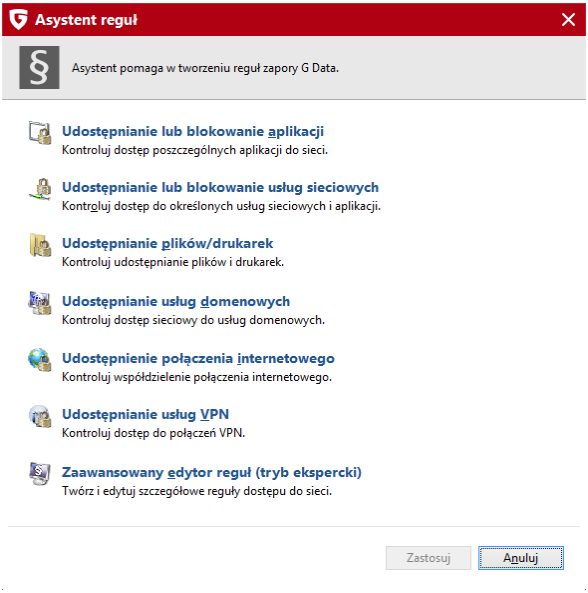
W widoku **Zestaw reguł**, pod nadaną przez użytkownika nazwą zestawu pojawi się nowy zestaw reguł. Po naciśnięciu przycisku **Edytuj** w zależności od ustawień, otworzy się **Asystent tworzenia reguł** lub **dialog zaawansowany** umożliwiający szczegółową konfigurację poszczególnych reguł.

Więcej na temat reguł i zestawów znajdziesz w rozdziałach Asystent tworzenia reguł 23 i Tryb zaawansowany 26.

Opis działania automatycznego generowania zapytań opisany jest w rozdziale Półautomatyczne tworzenie reguł 118.

5.3.1.1 Asystent tworzenia reguł

Przy jego pomocy możesz zdefiniować określone dodatkowe reguły danego zestawu reguł lub zmodyfikować istniejące reguły. Początkującym użytkownikom zalecamy stosowanie **Asystenta tworzenia reguł** do ręcznej konfiguracji zapory lub zdanie się na tryb autopilota. Za pośrednictwem **Asystenta tworzenia reguł** możesz zmienić jedną lub kilka reguł w wybranym zestawie.



W zależności od tego, który zestaw reguł został wybrany dla danej sieci, może mieć miejsce sytuacja, że jedna i ta sama aplikacja w zestawie reguł (np. dla niezaufanych sieci) będzie zablokowana, a w drugim zestawie reguł (np. dla sieci zaufanych) będzie mieć pełen dostęp. W ten sposób użytkownik jest w stanie ograniczyć np. przeglądarkę internetową przyporządkowując jej odpowiednio zróżnicowane reguły, aby mieć dostęp na strony znajdujące się na sieci wewnętrznej (np. domowej) ale blokować połączenie w sieci zewnętrznej.

Asystent tworzenia reguł umożliwia podjęcie następujących działań:

- **Udostępnianie lub blokowanie aplikacji:** Możesz wskazać program (plik) i zezwolić lub zablokować jej dostęp do sieci. W polu Kierunek połączenia wskazać czy wybrany program ma zostać zablokowany dla połączeń wychodzących, przychodzących czy w obydwu kierunkach. W ten sposób użytkownik zapory może np. uniemożliwić aplikacji do odtwarzania muzyki łączenie się ze zdalnym serwerem i pobieranie aktualizacji.

- **Udostępnianie lub blokowanie usług sieciowych:** Porty przekazują aplikacjom dane za pośrednictwem określonych protokołów. Przesyłanie danych ze stron internetowych odbywa się poprzez port 80, wysyłanie poczty elektronicznej przez port 25, odbieranie poczty elektronicznej

przez port 110 itd. W komputerze bez zapory wszystkie porty używane przez aplikacje są generalnie otwarte, chociaż zazwyczaj zwykli użytkownicy ich nie wykorzystują. Blokując jeden lub kilka portów, można w szybki sposób zamknąć luki bezpieczeństwa, które mogłyby być wykorzystane przez hakerów lub wirusy. Przy pomocy Asystenta tworzenia reguł można zablokować wszystkie lub tylko niektóre porty (np. tylko dla wybranych programów).

- **Udostępnianie plików/drukarek:** Umożliwia automatyczne utworzenie reguł niezbędnych do udostępniania i korzystania z udostępnionych zasobów sieciowych i drukarek.

- **Udostępnianie usług domenowych:** Domena umożliwia scentralizowane zarządzanie komputerami w sieci wyposażonej w kontroler domeny. Dlatego też dostęp do usług domen w sieciach niezaufanych powinien być z reguły zablokowany.

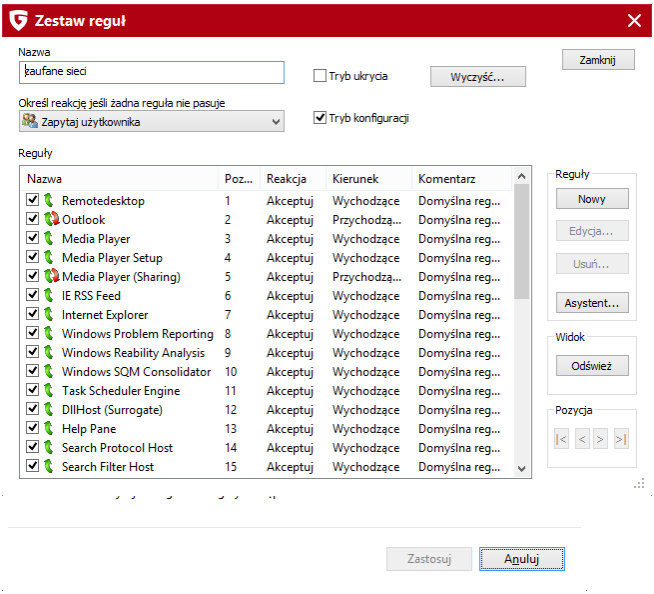
- **Udostępnianie połączenia internetowego:** Ta funkcjonalność dotyczy jedynie połączeń typu dialup (np. Neostrada, GPRS, UMTS itp.). Po udostępnieniu danego połączenia, konkretne komputery w sieci lokalnej również mogą z niego korzystać.

- **Udostępnianie usług VPN:** Umożliwia utworzenie reguł niezbędnych do prawidłowego działania połączeń zdalnych z sieciami prywatnymi.

- **Zaawansowany edytor reguł (tryb ekspercki):** W ten sposób użytkownik może przejść z trybu **Asystenta tworzenia reguł** do trybu zaawansowanego 26.

5.3.1.2 Tryb zaawansowany

W trybie zaawansowanym można skonfigurować reguły dla poszczególnych zestawów reguł. Tworzenie może przebiegać przy użyciu **Asystenta tworzenia reguł** lub ręcznie.



Dostępne są następujące ustawienia:

- **Nazwa:** Tu w zależności od potrzeb można zmieniać nazwę aktualnego zestawu reguł. Pod tą nazwą zestaw będzie wyświetlony w liście w widoku Zestaw reguł.

- **Tryb ukrycia:** W trybie ukrycia system nie odpowiada na zapytania wysyłane do komputera, w celu sprawdzenia dostępności portów. Utrudnia to hakerom uzyskanie informacji o systemie.

- **Określ reakcję, jeśli żadna reguła nie pasuje:** To pole określa reakcję na połączenie aplikacji, które nie jest regulowane przez żadną regułę.

- **Tryb konfiguracji:** Tryb konfiguracji przydatny jest w przypadku stosowania aplikacjach, które wykorzystują technikę kanałów zwrotnych (np. FTP, gry sieciowe). Aplikacje te łączą się ze zdalnym komputerem i

negocjują z nim kanał zwrotny, poprzez który zdalny komputer łączy się następnie ponownie z aplikacją użytkownika. Jeśli tryb konfiguracji jest aktywny, zapora rozpoznaje kanał zwrotny i udziela mu dostępu bez dodatkowych zapytań.

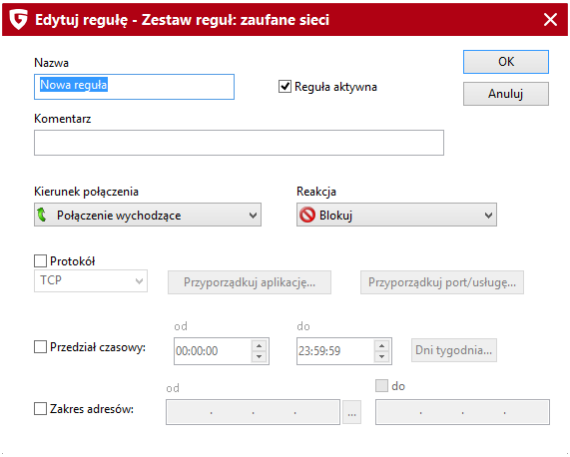
- **Szczegóły ICMP:** Internet Control Message Protocol (ICMP) to protokół internetowy umożliwiający przekazywanie informacji o błędach, pakietach testowych oraz o transferze danych. Pakiety ICMP mogą być wykorzystywane do inwigilowania komputera. Z tego powodu pakiety ICMP powinny być filtrowane przez zaporę.

Reguły

Lista zawiera wszystkie reguły stosowane w danym zestawie. Reguły umożliwiają blokowanie lub akceptowanie połączeń wywoływanych zdalnie i lokalnie przez usługi i aplikacje. Metody tworzenia reguł:

- Zastosowanie Asystenta tworzenia reguł 23.
- Ręcznie, poprzez kliknięcie przycisku **Nowy** w widoku trybu zaawansowanego 26.
- W oknie zapytania wyświetlanym automatycznie podczas próby nawiązania połączenia.

Kolejność reguł może mieć znaczenie. Może dojść np. do zablokowania usługi zaakceptowanej na poziomie portu przez regułę blokującą dostęp dla całego protokołu. Kolejność reguł można zmieniać poprzez przeciąganie ich nazw lub przy użyciu przycisków strzałek w sekcji **Pozycja**.



Okno **Edytuj regułę** zawiera następujące pola, przyciski i rozwijane listy umożliwiające utworzenie nowej lub zmodyfikowanie istniejącej reguły:

- **Nazwa:** W regułach predefiniowanych jest to nazwa aplikacji której dotyczy reguła. Nazwę można zmieniać i uzupełniać.
- **Reguła aktywna:** Można wyłączyć działanie reguły poprzez odznaczenie tego pola.
- **Komentarz:** Pole informuje w jaki sposób reguła została utworzona. Reguły predefiniowane oznaczone są komentarzem Domyślna reguła, natomiast w przypadku reguł tworzonych na podstawie zapytań w tej rubryce widnieje tekst Generowane poprzez zapytanie. Wprowadź własny komentarz dla reguł generowanych ręcznie.
- **Kierunek połączenia:** To ustawienie definiuje, czy chodzi w danym przypadku o regułę dla połączeń wychodzących, przychodzących czy dla obydwu rodzajów.
- **Reakcja:** To pole określa, czy reguła ma blokować, czy akceptować połączenia.
- **Protokół:** Wybór protokołu umożliwia zdefiniowanie ogólnej reguły dla całego protokołu, bez względu na aplikację, czy port.
- **Przedział czasowy:** Reguły mogą być także aktywne tylko w czasie określonym w tej sekcji. W ten sposób można ograniczyć dostęp konkretnych aplikacji do sieci np. tylko do czasu pracy.

- **Zakres adresów IP:** Reglamentacja dostępu do sieci staje się prostsza szczególnie w przypadku sieci z przydzielonymi stałymi adresami IP.

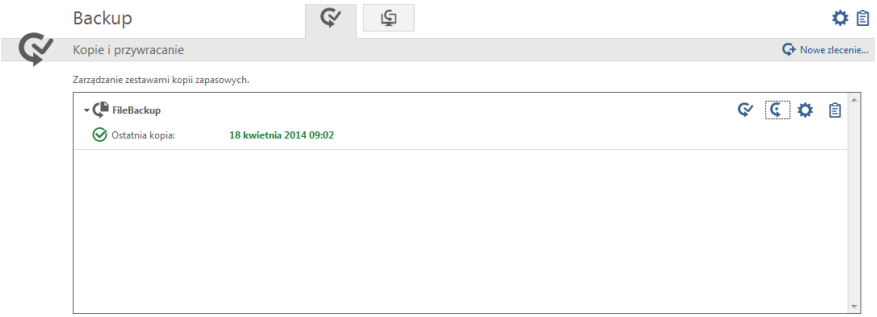
6 Backup

Kopie zapasowe danych zapisywane na dyskach przenośnych lub innych dyskach podłączonych do komputera to doskonała metoda na uniknięcie utraty danych na skutek awarii sprzętu lub np. kradzieży laptopa.

Moduł G Data Backup udostępnia dwa widoki - **Kopie i przywracanie** oraz **Funkcje**. Przełączanie między widokami możliwe jest poprzez klikanie ikon w pasku widoków.

6.1 Kopie i przywracanie

Widok umożliwia zarządzanie zleceniami kopii zapasowych. Z tego miejsca można tworzyć nowe zlecenia kopii, modyfikować je, a także przywracać dane.



Każde zlecenie kopii zapasowej umożliwia wykonywanie operacji na zleceniu za pomocą dostępnych przycisków:

Przywracanie: Jeśli zlecenie zostało wcześniej uruchomione, to polecenie umożliwia przywrócenie danych objętych zleceniem. Szczegóły znajdziesz w rozdziale Przywracanie z kopii 38.

Backup: To polecenie wymusza natychmiastowe uruchomienie

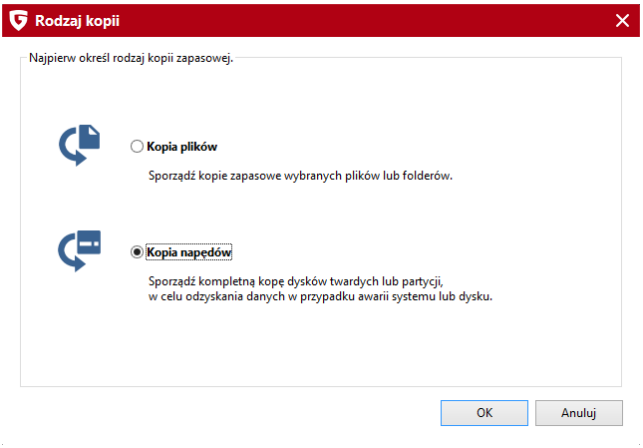
zlecenie kopii, niezależnie od harmonogramu.

Ustawienia: Ten przycisk otwiera okno ustawień danego zlecenia. Szczegóły znajdziesz w rozdziale Nowe zlecenie kopii 30 .

Protokół: To polecenie otwiera okno zawierającą listę działań wykonanych przez program w odniesieniu do danego zlecenia kopii. Rejestrowane są wszystkie ręczne i automatyczne uruchomienia zlecenia, a także błędy, np. dotyczące braku miejsca na nośniku docelowym kopii zapasowej.

6.1.1 Nowe zlecenie kopii

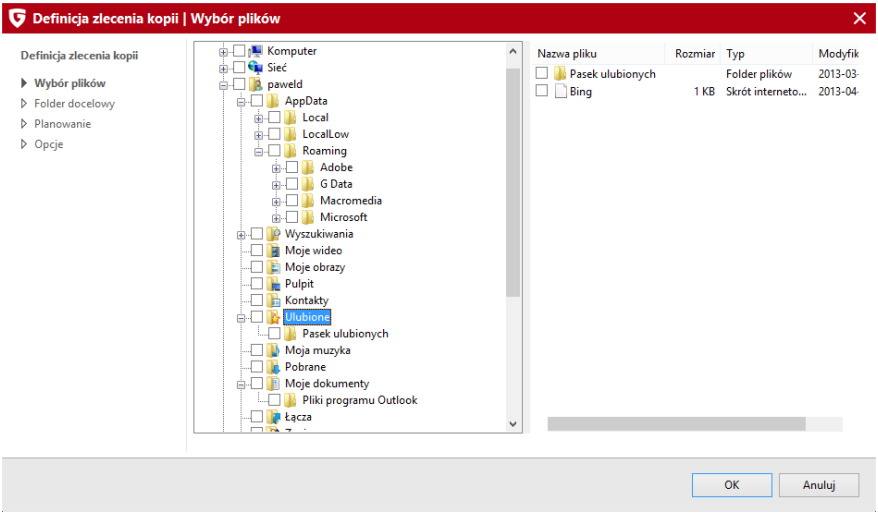
Kliknij przycisk **Nowe zlecenie**, aby utworzyć nowy wpis na liście zleceń kopii.



6.1.1.1 Wybór plików / partycji / dysków

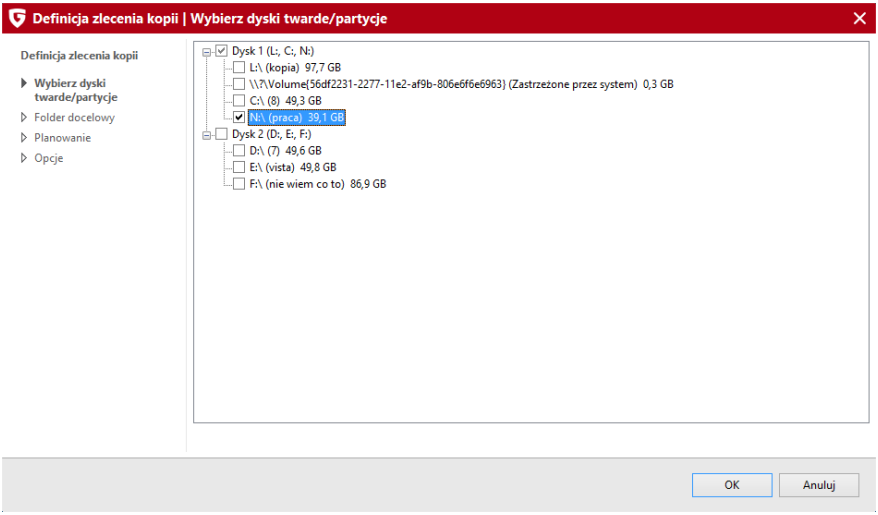
Pierwszym krokiem jest wybór rodzaju kopii zapasowej. Można kopiować wybrane pliki i foldery, lub też sporządzać kopie całych partycji i dysków twardych.

Kopia plików: W przypadku kopii plików i folderów ręcznie zaznacz foldery i pliki, które chcesz zabezpieczyć kopią zapasową.



Klikając znak (+) możesz rozwijać foldery w drzewku. Zaznacz foldery/pliki, które mają być uwzględniane przy wyszukiwaniu zadanych powyżej formatów plików. Na szaro zaznaczane są foldery, które nie są uwzględniane w całości (np. tylko niektóre podfoldery).

Kopia napędów: W przypadku wybrania kopii napędów zaznacz dyski twarde lub partycje, których kopie chcesz wykonywać.



6.1.1.2 Folder docelowy

Wskaż nośnik i folder docelowy dla kopii zapasowej. Jeżeli nośnika wymiennego (np. pendrive'a USB) nie ma na liście, podłącz go do komputera i kliknij przycisk **Odśwież**. Program umożliwia zapis kopii na różnych nośnikach wymiennych (np. pamięci USB, karty SD, zewnętrzne dyski twarde), na lokalnych dyskach twardych, w folderach sieciowych a także serwerach FTP.

Aby skorzystać z możliwości kopiowania danych na serwer FTP zaznacz opcję **Wyślij archiwum na serwer FTP**.

Najlepiej, żeby kopia była sporządzana na innym dysku lub innym nośniku niż znajdują się oryginalne dane. W przypadku awarii dysku można będzie wtedy dane odzyskać. Jeżeli kopia zostanie sporządzona na dysku, na którym znajdują się oryginały danych, w przypadku uszkodzenia lub utraty dysku, kopia również zostanie utracona.

Utwórz archiwum w chmurze: Wykorzystaj jeden z popularnych serwisów oferujących przechowywanie danych w chmurze - Microsoft Dropbox lub Google Drive. Załóż konto lub zaloguj się swoimi poświadczeniami do wybranego serwisu w celu powiązania usługi kopii zapasowych z chmurą.

Wskazówka: W przypadku wyboru opcji przechowywania kopii w chmurze, warto pamiętać o zaszyfrowaniu danych. Szyfrowanie można włączyć lub wyłączyć w oknie Opcji 35.

6.1.1.3 Planowanie

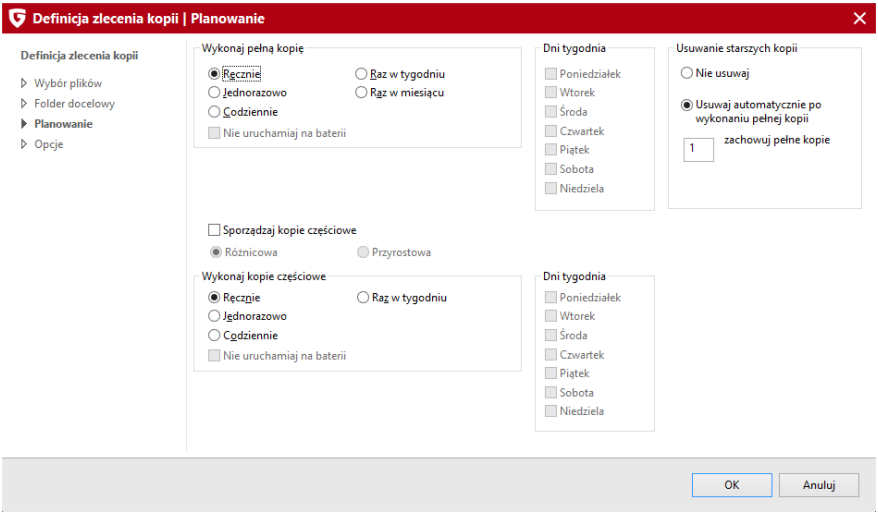
Widok umożliwia skonfigurowanie harmonogramu automatycznie wykonywanych kopii zapasowych. Ustawienie **Ręcznie** należy w tym celu zmienić na **Codziennie**, **Raz w tygodniu** lub **Raz w miesiącu**. Ustaw pożądaną częstotliwość wykonywania kopii korzystając z dostępnych ustawień.

Regularne sporządzane kopii pochłania dużo miejsca na nośniku docelowym. Jeżeli nie są Ci potrzebne wszystkie kopie zapasowe możesz ustawić opcję automatycznie usuwającą starsze kopie. Jeżeli chcesz przechowywać starsze kopie zapasowe, zalecane jest wprowadzenie ograniczenia ilości przechowywania pełnych kopii. Starsze kopie będą sukcesywnie zastępowane nowszymi, co pozwoli zaoszczędzić miejsce na dysku.

Ustawienie **Nie uruchamiaj na baterii** spowoduje, że zlecenia kopii będą wykonywane tylko podczas ładowania laptopa.

Wykonaj pełną kopię

Górny harmonogram określa częstotliwość wykonywania pełnych kopii zadanego obszaru danych.



Uwaga: Planowanie kopii zapasowych nie obejmie zleceń kopii zapisywanych na nośnikach CD-ROM/DVD-ROM, ponieważ w przypadku potrzeby zmiany nośnika niezbędna jest interwencja użytkownika.

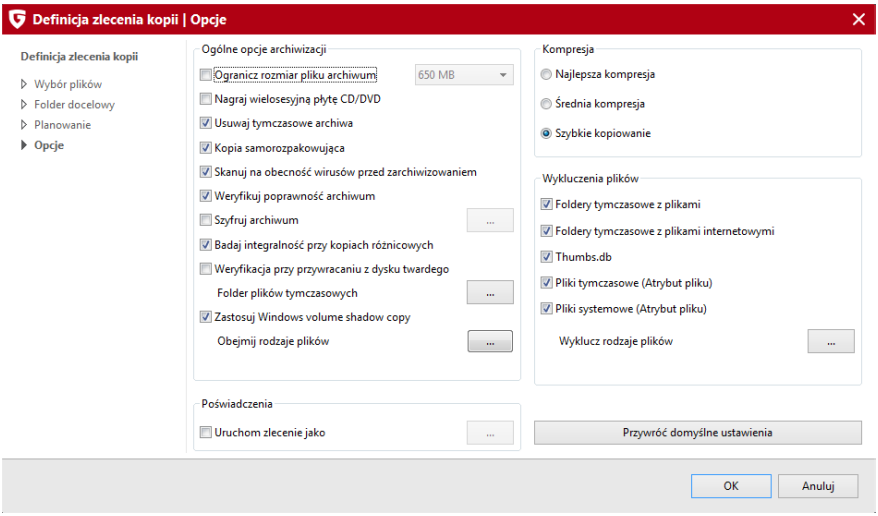
Tworzenie kopii częściowych przyspiesza proces kopiowania danych. Zamiast kopiować wszystkie dane, program porównuje je z gotową pełną kopią i tylko uzupełnia lub uaktualnia dane, których brakuje w kopii. W tym celu zaznacz opcję **Kopie częściowe**

Wykonuj kopie częściowe

Różnicowe / przyrostowe: Kopie różnicowe uzupełniają ostatnią pełną kopię o zmodyfikowane w międzyczasie dane. Ich stosowanie zmniejsza zapotrzebowanie na miejsce, w odróżnieniu od kopii pełnych. Kopia przyrostowa dodatkowo powoduje archiwizowanie danych zmodyfikowanych między kolejnymi kopiami częściowymi. Wadą tego rozwiązania jest to, że do przywrócenia danych z kopii przyrostowej wymagana jest obecność wszystkich kolejnych archiwów.

6.1.1.4 Opcje

Widok opcji umożliwia modyfikowanie globalnych ustawień dla wszystkich zleceń kopii. Zaleca się pozostawienie domyślnych ustawień tworzenia kopii.



Ogólne opcje archiwizacji

- **Ogranicz rozmiar pliku archiwum:** Jeżeli planujesz nagrywanie kopii na płytach CD-ROM, DVD-ROM lub BD-ROM, wprowadź ograniczenie rozmiaru pliku z archiwum do rozmiaru stosowanego nośnika. Lista wyboru umożliwia ustawienie jednego z typowych rozmiarów stosowanych nośników optycznych. Jeżeli rozmiar kopii przekroczy zadaną wartość, kopia zostanie podzielona na fragmenty o zadanym rozmiarze. W trakcie nagrywania program automatycznie poprosi o włożenie do napędu nowego nośnika.

- **Nagraj wielosesyjną płytę CD/DVD:** Program nie zamknie płyty umożliwiając dogranie kolejnych kopii w późniejszym terminie.

- **Usuwaj tymczasowe archiwa:** Pliki tymczasowe zajmują dużą ilość miejsca na dyskach. Zaleca się pozostawienie tej opcji włączonej na stałe.

- **Kopia samorozpakowująca:** Użycie tej opcji powoduje nagranie na płycie z kopią także pliku programu Backup o nazwie AVKBackup.exe.

Dzięki temu możliwe będzie przywrócenie danych z kopii bez udziału całego pakietu. Uruchomienie tego pliku otwiera interfejs składnika Backup, umożliwiający przywrócenie plików.

- **Skanuj pliki na obecność wirusów przed zarchiwizowaniem:** Jeśli w systemie zainstalowany jest składnik AntiVirus, program może skanować pliki przed archiwizacją.

- **Weryfikuj poprawność archiwum**: Włączenie tej opcji wymusza weryfikację poprawności zapisu danych w plikach kopii.

- **Szyfruj archiwum:** Możesz dodatkowo zabezpieczyć pliki kopii za pomocą hasła. Do przywrócenia danych z archiwum niezbędne będzie podanie hasła. Zanotuj lub dobrze zapamiętaj hasło, bez niego nie przywrócisz danych z kopii.

- **Badaj integralność przy kopiach różnicowych:** Włączenie tej opcji wymusza kontrolę poprawności danych po utworzeniu kopii częściowej.

- **Weryfikacja przy przywracaniu z dysku twardego:** Jeśli ta opcja jest włączona, aplikacja sprawdza poprawność danych podczas przywracania z dysku twardego.

Folder plików tymczasowych: Kliknij ten przycisk, aby zmienić lokalizację przechowywania plików tymczasowych programu Backup, niezbędnych do utworzenia kopii zapasowej. Standardowo folder tymczasowy znajduje się na partycji systemowej. Jeżeli nie ma na niej wystarczającej ilości miejsca, wskaż inną partycję.

Opcja **Zastosuj Windows volume shadow copy** umożliwia tworzenie kopii zapasowych napędów (dysków, partycji) zawierających systemy operacyjne.

Obejmij rodzaje plików: Kliknij ten przycisk aby ograniczyć kopiowanie tylko do wybranych rodzajów plików.

Sekcja **Poświadczenia** umożliwia włączenie opcji uruchamiania zleceń kopii przy pomocy konkretnego konta użytkownika systemu Windows. Ustawienie tej opcji i wprowadzenie danych użytkownika jest niezbędne do wykonania automatycznych zleceń kopii zapasowych.

Sekcja **Kompresja** umożliwia ustawienie pożądanego stopnia kompresji kopii zapasowych.

- **Najlepsza kompresja:** Sporządzanie kopii przy tej metodzie kompresji trwa najdłużej, ale pliki archiwów zajmują najmniej miejsca.

- **Średnia kompresja:** Dane są pakowane w niewielkim stopniu, ale tworzenie kopii trwa krócej.

- **Szybkie kopiowanie:** To ustawienie pozwala zrezygnować z kompresji danych i uzyskać najkrótszy czas sporządzania kopii zapasowych.

Sekcja **wykluczenia plików**

Program wykonuje kopie zapasowe plików zapisanych w konkretnych formatach. Część plików w systemie operacyjnym nie musi być uwzględniania w kopiach, np. pliki tymczasowe. W celu przyspieszenia czasu wykonywania kopii i zmniejszenia jej rozmiaru możesz skorzystać z tych ustawień aby pominąć w kopii określone pliki.

- **Foldery z plikami tymczasowymi:** Po zaznaczeniu tej opcji, folder plików tymczasowych danego profilu użytkownika będzie pomijany przy tworzeniu kopii zapasowej.

- **Foldery z tymczasowymi plikami internetowymi:** Po zaznaczeniu tej opcji, folder internetowych plików tymczasowych danego profilu użytkownika nie będzie uwzględniany przy tworzeniu kopii zapasowej.

- **Thumbs.db:** Wykluczenie miniatur spowoduje, że automatycznie tworzone systemowe pliki miniator thumbs.db nie będą brane pod uwagę przy tworzeniu kopii.

- **Pliki tymczasowe (atrybut pliku):** Zaznacz tę opcję, jeśli chcesz pomijać pliki z atrybutem tymczasowe podczas tworzenia kopii.

- **Pliki systemowe (atrybut pliku):** Zaznacz tę opcję, jeśli chcesz pomijać pliki z atrybutem systemowe podczas tworzenia kopii.

Aby utworzyć wyjątki na konkretne formaty plików, kliknij przycisk **Wyklucz rodzajów plików**.

Wpisz w polu **Maska pliku** nazwę lub maskę formatu plików, które chcesz wykluczyć z kopii zapasowej. Kliknij OK i powtórz proces dla wszystkich formatów plików niepożądanych w kopii, przykładowo:. picasa.ini, *.ini, *bak.

Dozwolone jest stosowanie następujących znaków zastępczych.

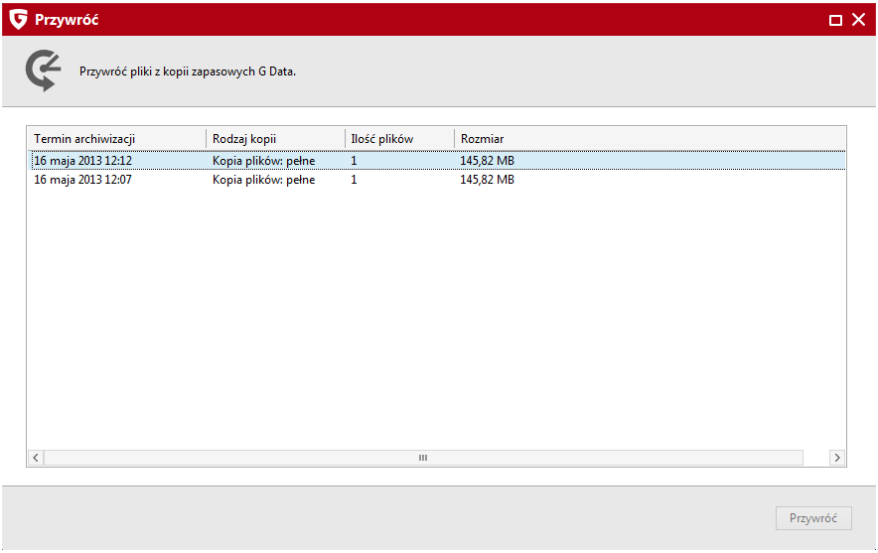
? Symbolizuje dowolny znak.

* Zastępuje dowolny ciąg znaków.

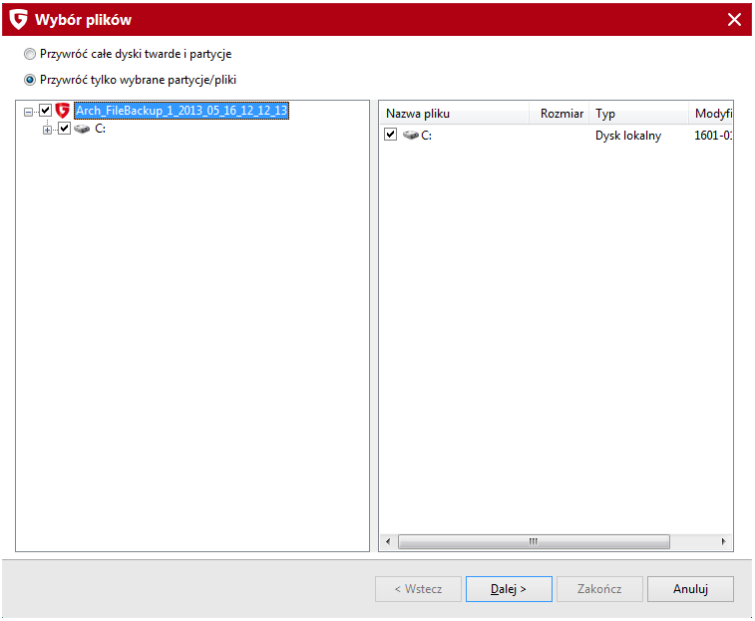
Klikając przycisk **Przywróć domyślne ustawienia** możesz anulować wprowadzone wcześniej zmiany i zastosować fabryczne ustawienia programu.

6.1.2 Przywracanie z kopii

W tym oknie możesz przywrócić dane zapisane w kopii zapasowej. W przypadku kopii standardowej, po prostu zaznacz wybrane archiwum kopii na liście i kliknij przycisk Przywróć.



Aby przywrócić dane z kopii wybierz nazwę zlecenia i wersję kopii zapasowej i kliknij przycisk **Przywróć**. Program spyta, czy chcesz przywrócić wszystkie pliki z archiwum kopii, czy wybrać ręcznie pliki do przywrócenia. Wybierz pożądaną opcję i kliknij przycisk **Dalej**.



Jeśli chcesz przywrócić pliki do lokalizacji źródłowej i nadpisać oryginalne dane, pozostaw zaznaczoną opcję **Przywróć pliki do oryginalnych folderów**. Jeżeli chcesz przywrócić pliki w inne miejsce, wyłącz tę opcję i wskaż folder. Możesz użyć przycisku **Nowy folder...**, aby utworzyć nowy folder w wybranej lokalizacji.

Opcjonalnie wpisz hasło, jeśli kopia była zaszyfrowana. Możesz również zastosować skanowanie antywirusowe danych przed przywróceniem.

W sekcji **Nadpisuj istniejące pliki** możesz określić zasady nadpisywania oryginalnych plików plikami z kopii zapasowej:

- **zawsze:** Wszystkie pliki oryginalne zostaną zastąpione plikami z kopii zapasowej, niezależnie od ich wersji i dat modyfikacji.
- **jeśli zmienił się rozmiar:** Zastąpione zostaną tylko te pliki, które uległy zmodyfikowaniu. Przywracanie kopii potrwa krócej, niż w przypadku zastępowania wszystkich plików.
- **jeśli data modyfikacji jest nowsza niż w archiwum:** Inna możliwość skrócenia czasu przywracania danych. Program zastąpi tylko te pliki, których data modyfikacji jest nowsza, niż data modyfikacji oryginałów.

- **jeśli data modyfikacji uległa zmianie:** Program przywróci tylko te pliki, które mają inną datę modyfikacji niż oryginały.

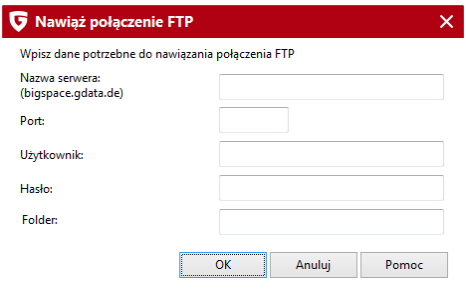
Wybierz pożądane opcje i kliknij przycisk **Zakończ**. Dane zostaną przywrócone we wskazane miejsce zgodnie z zastosowanymi ustawieniami.

6.1.3 Widok Funkcje

W tym widoku możesz uruchomić podstawowe funkcje programu, a także skorzystać z dodatkowych narzędzi - usunąć starsze kopie, nagrać przechowywane obrazy kopii i przeglądać kopie zapisane na serwerach FTP.

6.1.3.1 Kopie online

Jeżeli przechowujesz kopie zapasowe na serwerze FTP, możesz zalogować się na serwer przy użyciu tego polecenia. Po wpisaniu danych dostępu kliknij OK. Otworzy się okno z zawartością foldera na serwerze FTP.



W pakiecie oferujemy również 1 GB miejsca na serwerze FTP na Twoją kopię zapasową. W momencie rejestracji programu otrzymasz dane dostępu do serwera FTP. Dane zostaną automatycznie wpisane w ustawieniach FTP kopii zapasowej. Możesz przechowywać kopie zapasowe na serwerze z dodatkową możliwością zabezpieczenia pliku kopii hasłem. W wersji pudełkowej programu dane dostępu do serwera FTP znajdziesz w opakowaniu z programem. W przypadku zakupu wersji elektronicznej w sklepie internetowym, dane dostępu otrzymasz w wiadomości e-mail z potwierdzeniem rejestracji.

W przypadku wersji na więcej stanowisk każde stanowisko otrzymuje osobne konto rozmiarze 1 GB.

Miejsce na serwerze FTP jest dostępne do końca trwania abonamentu. Standardowo okres ten trwa rok czasu. Po upływie tego terminu pozostawiamy dane na serwerze przez 30 dni w celu umożliwienia odzyskania danych. Po 30 dniach od wygaśnięcia abonamentu dane są usuwane.

Przeglądarka FTP

Aby zalogować się do serwera FTP wpisz w oknie logowania dane dostępu do serwera. Pasek narzędzi przeglądarki oferuje następujące opcje:

Połącz: Jeżeli połączenie zostanie przerwane, kliknij ten przycisk aby je wznowić..

Rozłącz: Kliknij ten przycisk, jeśli chcesz się przerwać sesję FTP.

Nowy folder: Przycisk umożliwia założenie foldera na serwerze FTP.

Usuń: Ten przycisk powoduje usunięcie zaznaczonego archiwum.

Odśwież: Odświeża widok folderu na serwerze FTP.

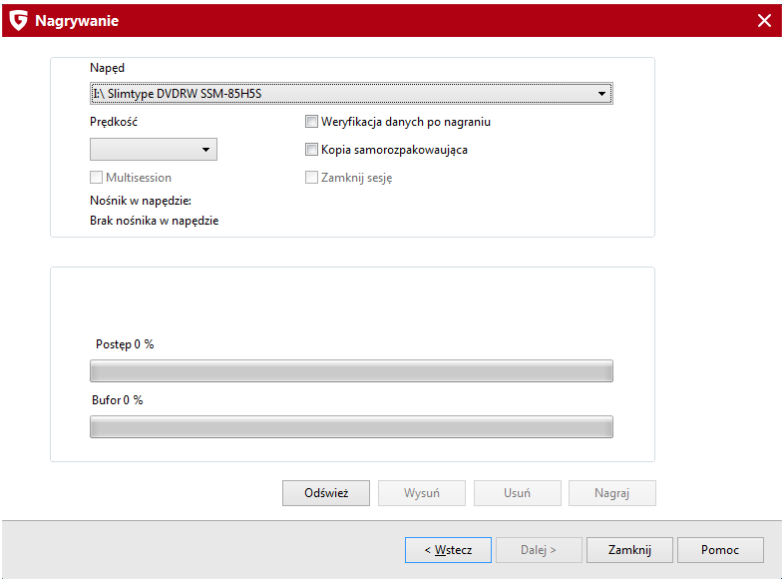
Pobierz: Pobiera zaznaczone archiwum do dowolnej lokalizacji na komputerze.

Wyślij: Wysyła zaznaczone archiwum do folderu na serwerze FTP.

Pomoc: Wyświetla okno pomocy.

6.1.3.2 Nagraj zapisany obraz

W przypadku nagrywania kopii na płyty program umożliwia pozostawienie tymczasowego obrazu płyty na dysku. To polecenie daje możliwość wskazania i ponownego nagrania obrazu kopii na płytę.



Możesz wskazać wybraną nagrywarkę, a także modyfikować prędkość zapisu.

- **Weryfikacja danych po nagraniu:** Włączenie tej opcji wymusza weryfikację poprawności danych po nagraniu płyty. Proces archiwizacji trwa dłużej, ale dzięki weryfikacji zyskujesz pewność, że dane nie zostały nagrane z błędami.

- **Kopia samorozpakowująca:** Użycie tej opcji powoduje nagranie na płycie z danymi także pliku programu Backup o nazwie AVKBackup.exe. Dzięki temu możliwe będzie przywrócenie danych z kopii bez udziału całego pakietu. Uruchomienie tego pliku otwiera interfejs składnika Backup, umożliwiający przywrócenie plików.

Kliknij przycisk **Nagraj**, aby rozpocząć proces nagrywania płyty.

Oryginalny plik obrazu kopii nie jest usuwany automatycznie po nagraniu go

na płytę CD/DVD.

6.1.3.3 Importuj archiwa

Ten widok umożliwia zaimportowanie kopii wykonanej na innym komputerze, lub przed ponownym zainstalowaniem pakietu G Data Software. Wskaż lokalizację pliku archiwum (*.ARC) zapisanego na dysku, płycie lub w folderze sieciowym i kliknij przycisk OK, aby zaimportować plik z kopią zapasową.

Po wykonaniu zadania program wyświetli stosowny komunikat.

Jeśli chcesz wykonać tylko jednorazowe przywrócenie danych z kopii wykonanej na innym komputerze, możesz przejść do widoku Przywróć 38 i ręcznie wskazać plik z kopią w celu przywrócenia danych.

Pliki kopii zapasowych zapisywane są w formacie *.ARC.

6.1.3.4 Klonuj dysk

Klonowanie dysku to nie to samo co kopiowanie danych na inny nośnik. Ta funkcja tworzy pełny obraz dysku bit po bicie. Dzięki temu można utworzyć kopię zapasową dysku z systemem operacyjnym, a w razie potrzeby w prosty sposób przywrócić ją z na dysk wraz z zainstalowanym systemem Windows i programami. Narzędzie umożliwia zatem sporządzenie pełnej zapasowej całego komputera.

Uwaga: Dysk docelowy, na którym zamierzasz zapisać obraz kopii musi mieć co najmniej taki sam rozmiar, jak dysk, który chcesz zabezpieczyć, w innym przypadku kopia po prostu się nie zmieści.

Krok 1: Wybierz dysk źródłowy, czyli dysk, który chcesz sklonować.

Krok 2: Wskaż dysk docelowy, czyli dysk, na którym chcesz przechowywać obraz (klon) zabezpieczanego dysku twardego.

Dopasuj rozmiar partycji do rozmiaru dysku docelowego: Jeśli to pole będzie zaznaczone, program automatycznie dopasuje rozmiary partycji dysku docelowego, powiększając je, o ile będzie to potrzebne do prawidłowego utworzenia obrazu dysku źródłowego.

6.1.3.5 Utwórz nośnik startowy

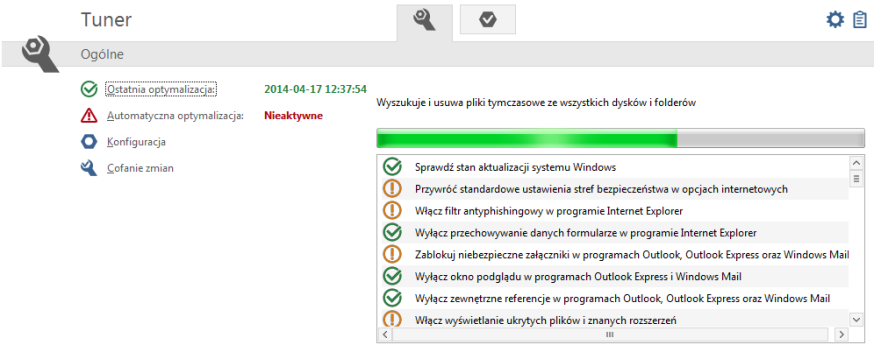
Możesz sporządzić płytę startową umożliwiającą zarówno skanowanie komputera jak i przywrócenie kopii napędu (partycji lub dysku) bez potrzeby uruchamiania systemu Windows. Do utworzenia płyty startowej potrzebna jest czysta płyta. Kreator umożliwia także pobranie sygnatur wirusów przed nagraniem płyty.

Jeśli nie widzisz tej opcji w programie, możliwe, że kreator płyt startowych nie został zainstalowany. Możesz uruchomić polecenie modyfikacji instalacji i doinstalować składnik kreatora płyt startowych.

Szczegóły na temat korzystania z płyty startowej znajdziesz w rozdziale Skanowanie nośnikiem startowym [114].

7 Tuner

Tuner umożliwia wygodną i prostą optymalizację ustawień komputera. Przypomina automatycznie o aktualizowaniu systemu Windows i aplikacji pakietu Microsoft Office, defragmentuje dyski twarde. Można zaplanować także automatyczne usuwanie plików tymczasowych, a także niepotrzebnych elementów z rejestru. Dzięki tym usprawnieniom system Windows zyska na wydajności i przejrzystości.



Kliknij nagłówek sekcji aby rozwinąć menu umożliwiające wykonanie dodatkowych czynności.

Ostatnia optymalizacja: Po wykonaniu pierwszej optymalizacji w tym miejscu pojawi się data ostatniego procesu optymalizacji

wykonanego przez program. Aby ręcznie wymusić rozpoczęcie optymalizacji, kliknij ten wiersz i wybierz polecenie **Optymalizuj teraz**.

Automatyczna optymalizacja: Możesz zautomatyzować proces optymalizacji konfigurując harmonogram działań.

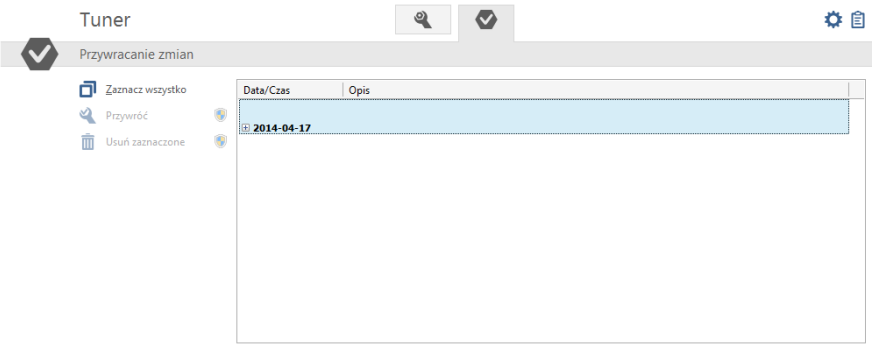
Konfiguracja: Ten widok umożliwia szczegółowy wybór konkretnych opcji optymalizacji pogrupowanych w sekcje:

- **Skuteczność:** Zestaw funkcji optymalizujących bezpieczeństwo systemu operacyjnego.
- **Wydajność:** Funkcje umożliwiające porządkowanie systemu poprzez usuwanie plików tymczasowych, nieużywanych skrótów, plików i wpisów w rejestrze. Dzięki temu system operacyjny uruchamia się szybciej i działa sprawniej.
- **Ochrona danych**: Funkcje usuwające z komputera prywatne informacje. Uniemożliwi to obserwowanie zachowań użytkowników podczas przeglądania internetu, a także podejrzenie wrażliwych danych.

Cofanie zmian: Tuner tworzy punkty przywracania umożliwiające cofnięcie każdej wprowadzonej zmiany. Jeśli masz wrażenie, że program spowodował nieprawidłowe działanie jakiegoś elementu systemu, możesz zastosować ten widok w celu przywrócenia zmian do stanu sprzed optymalizacji. Szczegóły znajdziesz w rozdziale Przywracanie zmian 45.

7.1 Przywracanie zmian

Tuner tworzy punkty przywracania umożliwiające cofnięcie każdej wprowadzonej zmiany. Jeśli masz wrażenie, że program spowodował nieprawidłowe działanie jakiegoś elementu systemu, możesz zastosować ten widok w celu przywrócenia zmian do stanu sprzed optymalizacji



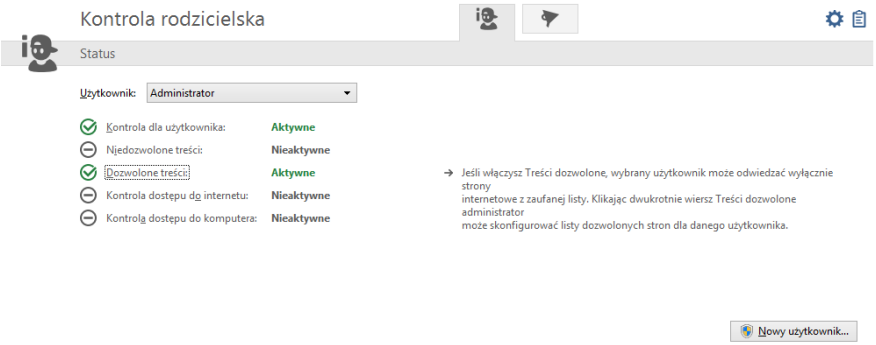
Zaznacz wszystko: Zaznacza do przywrócenia wszystkie zmiany z listy.

Przywróć: Wycofuje wszystkie zaznaczone zmiany, wprowadzone w trakcie optymalizacji systemu.

Usuń zaznaczone: Ten przycisk umożliwia usunięcie niepotrzebnych pozycji z listy zmian.

8 Kontrola rodzicielska

Moduł kontroli rodzicielskiej umożliwia ograniczenie użytkownikom dostępu do stron internetowych zawierających niepożądane treści, a także zarządzanie czasem dostępu do internetu oraz komputera.



Wybierz z listy dostępnych kont użytkowników konto, które chcesz kontrolować. Pamiętaj, że kontrola zafunkcjonuje poprawnie tylko dla kont z ograniczonymi uprawnieniami. Administratorzy komputera będą ją mogli po prostu wyłączyć. Możesz założyć nowe konto Windows z ograniczeniami bezpośrednio w oknie Kontroli rodzicielskiej, klikając przycisk Nowy użytkownik...[48].

- **Kontrola dla użytkownika:** Tutaj możesz włączyć lub wyłączyć kontrolę dla wybranego z listy konta.

- **Niedozwolone treści:** Kliknij ten wiersz, a następnie wybierz polecenie Edytuj...[49], aby otworzyć okno dialogowe, w którym można blokować dla danego użytkownika strony zawierające niedozwolone treści. Po wybraniu i zaznaczeniu blokowanych kategorii kliknij OK, aby włączyć kontrolę w trybie treści niedozwolonych. Strony internetowe, które swoją treścią odpowiadają wybranym kryteriom zostaną zablokowane.

- **Dozwolone treści:** Kliknij ten wiersz, a następnie wybierz polecenie Edytuj...[51], aby otworzyć okno dialogowe, w którym można zezwolić na przeglądanie wybranych treści w Internecie. W tym celu należy wybrać kategorie treści, które mają być dozwolone, a następnie kliknąć OK. Strony internetowe, które odpowiadają danym kryteriom, zostaną wówczas odblokowane.

- **Kontrola dostępu do internetu:** Kliknij ten wiersz, a następnie wybierz

polecenie Edytuj...52, aby otworzyć okno dialogowe umożliwiające ograniczenie czasu spędzanego przez użytkownika na przeglądaniu stron internetowych.

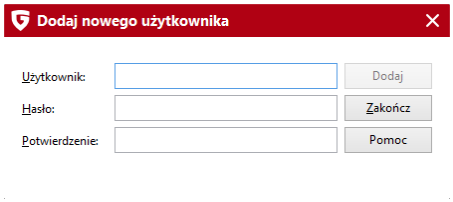
- **Kontrola dostępu do komputera:** Kliknij ten wiersz, a następnie wybierz polecenie Edytuj...54, aby otworzyć okno dialogowe umożliwiające ograniczenie czasu spędzanego przez użytkownika przed komputerem.

Ustawienia: Otwiera okno ustawień protokołowania kontroli rodzicielskiej.

Protokół: Otwiera listę wszystkich raportów z działań zapory. Klikając nagłówki poszczególnych kolumn, możesz posortować raporty.

8.1 Nowy użytkownik...

Jeśli chcesz ograniczyć użytkownikom dostęp do Internetu, utwórz nowe konto użytkownika z ograniczonymi uprawnieniami bezpośrednio w programie Kontrola rodzicielska klikając przycisk Nowy użytkownik.... Otworzy się okno dialogowe, w którym należy wpisać nazwę i ewentualnie hasło.

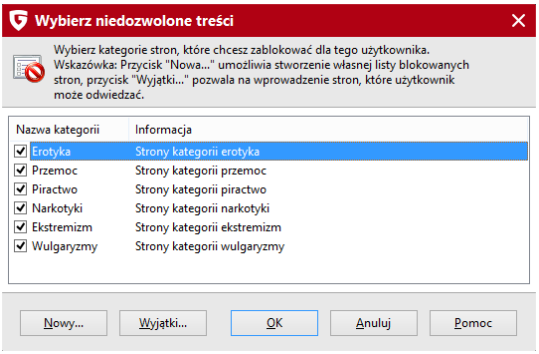


Wskazówka: Ze względów bezpieczeństwa hasło powinno mieć co najmniej 8 znaków, zawierać duże i małe litery jak i cyfry. W przypadku komputerów domowych, nie ma potrzeby zabezpieczania kont użytkowników hasłem.

Nowo założony profil dostępny będzie w liście rozwijanej Użytkownik. System Windows założy konto użytkownika o tej samej nazwie i haśle. Oznacza to, że kontrola rodzicielska z poczynionymi ustawieniami będzie automatycznie aktywna dla osoby, która przy starcie komputera zaloguje się w systemie Windows używając nazwy i hasła założonego profilu.

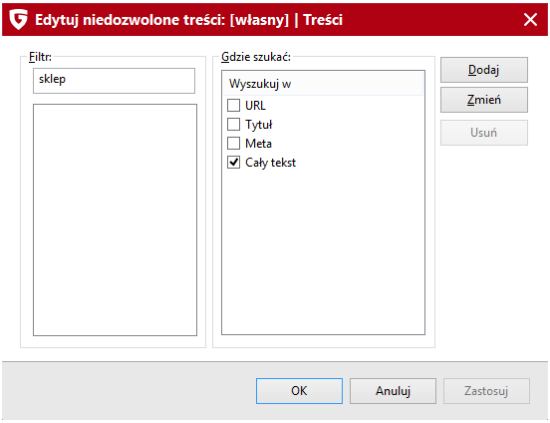
8.2 Treści niedozwolone

Po dwukrotnym kliknięciu otwiera się okno dialogowe, w którym można blokować dla danego użytkownika strony zawierające niedozwolone treści. Po wybraniu i zaznaczeniu blokowanych kategorii należy kliknąć przycisk OK. Strony internetowe, które swoją treścią odpowiadają wybranym kryteriom zostaną zablokowane.



Klikając przycisk **Nowy...**, otworzysz okno dialogowe, w którym możesz definiować własne filtry stron internetowych (tzw. czarna lista). W polach Nazwa i Opis wpisz nazwę i opis tworzonego filtra.

Po kliknięciu przycisku OK otwiera się okno, w którym można wpisywać słowa kluczowe, które mają być filtrowane. W tym celu w polu Filtr trzeba wpisać pojęcie, które ma zostać zablokowane a w sekcji Wyszukuj w wybrać obszar witryny internetowej, w której kontrola rodzicielska ma szukać danego pojęcia.



Dostępne ustawienia:

- URL: Jeśli zaznaczone zostanie pole URL, wówczas dane pojęcie treści niedozwolonej będzie szukane w adresie strony internetowej. Jeśli zatem chcesz blokować strony internetowe zawierające w adresie np. słowo "czat", wystarczy jako filtr wprowadzić słowo "czat", zaznaczyć pole URL i kliknąć Dodaj. Zablokowane zostaną wszystkie strony, które w nazwie domeny, a więc w adresie internetowym zawierają ciąg liter "czat".

- Tytuł: Jeśli zaznaczone zostanie pole Tytuł, blokowany tekst będzie szukany w tytule strony internetowej. Jest to ten obszar strony, widoczny np. po dodaniu stron do Ulubionych. Jeśli zamierzasz zablokować strony zatytułowane np. "czat warszawa"; "czat nastolatki" itd., wówczas wystarczy wpisać jako filtr słowo "czat", zaznaczyć pole Tytuł i kliknąć Dodaj. Zablokowane zostaną wszystkie te strony, które w tytule zawierają ciąg liter "czat".

- Meta: Metatagi są to ukryte na stronie internetowej słowa kluczowe ułatwiające wyszukiwanie strony internetowej w wyszukiwarkach. Słowa "sex" czy "czat" są tu często używane w celu podwyższenia ilości wejść na stronę. Jeśli zamierzasz zablokować strony internetowe, które w metatagu mają wpisane słowa kluczowe takie jak "czat", wystarczy wpisać słowo "czat", zaznaczyć pole Meta i kliknąć Dodaj. Zablokowane zostaną wówczas wszystkie strony, które w metatagach zawierają słowo kluczowe "czat".

- Cały tekst: Jeśli filtrowany ma być tekst strony internetowej, należy wpisać słowo kluczowe, które ma być blokowane, np. "czat", zaznaczyć pole Tekst i kliknąć Dodaj. Zablokowane zostaną wówczas wszystkie

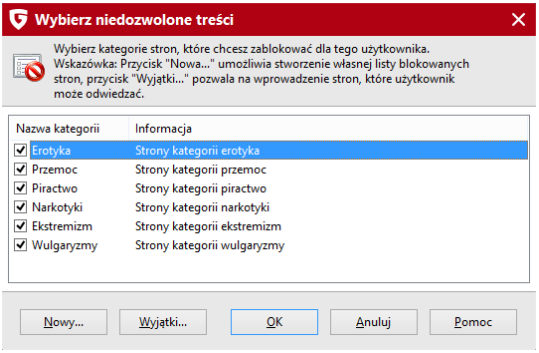
strony, które w tekście zawierają hasła "czat".

Może się zdarzyć, że przez użycie zbyt ogólnych określeń zablokowane zostaną również strony, które są zupełnie nieszkodliwe. I tak np. w przypadku hasła kluczowego "dom" zablokowane zostaną również strony zawierające słowo "domena". Filtr rozpoznaje w słowie "domena" element "dom" i uruchamia blokadę.

Jeżeli filtr blokuje także pożądane strony ze względu na zawarte treści można ponownie skonfigurować wyjątki filtra. W tym celu należy kliknąć przycisk Wyjątki i wpisać adresy stron, które nie mają być blokowane zatwierdzając każdy adres przyciskiem Dodaj.

8.3 Treści dozwolone

W oknie dialogowym Treści dozwolone administrator może zezwolić danemu użytkownikowi na przeglądanie wybranych treści w Internecie. W tym celu należy wybrać kategorie treści, które mają być dozwolone, a następnie kliknąć OK. Strony internetowe, które odpowiadają danym kryteriom, zostaną wówczas odblokowane.



Po kliknięciu przycisku **Nowy...**, otwiera się okno dialogowe, w którym można zdefiniować własne dozwolone treści (tzw. biała lista). Wpisz w polach Nazwa i Opis nazwę oraz opis własnego filtra.

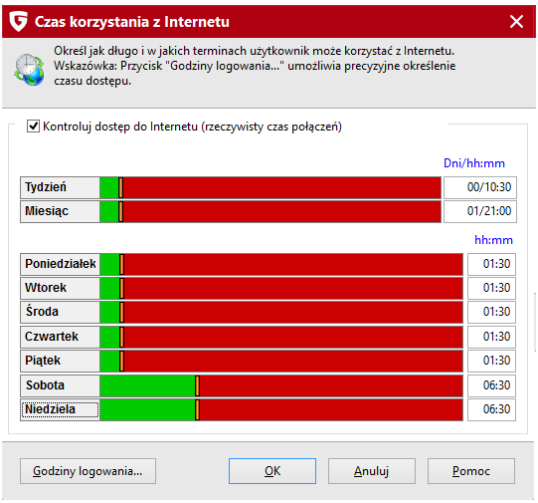
Po kliknięciu przycisku OK otwiera się okno dialogowe, w którym filtr (białą listę) można wypełnić np. odpowiednimi adresami stron internetowych.

W tym celu w polu Filtr można wpisać nazwę filtra. W polu Opis wpisz opis ułatwiający identyfikacje tworzonego filtra w przyszłości. W polu Link wpisz

dokładny adres internetowy dozwolonej strony; np www.interia.pl. Kiedy użytkownik spróbuje wejść na stronę, która nie jest udostępniona, zamiast niej pojawi się na ekranie strona HTML, która zaprezentuje wszystkie dozwolone strony internetowe znajdujące się na białej liście wraz z ich opisami. W ten sposób dziecko może bezpośrednio wejść na te strony, klikając wybrane linki. Po wypełnieniu pól kliknij przycisk Dodaj. Proces można powtarzać wielokrotnie, np. do momentu utworzenia kompletnej listy odblokowanych stron np. danej kategorii.

8.4 Kontroluj czas dostępu do Internetu

W tym oknie możesz skonfigurować czasową blokadę dostępu danego użytkownika do Internetu. W tym celu zaznacz pole Kontroluj czas dostępu do Internetu. Korzystając z suwaków zdecyduj, jak długo użytkownik może korzystać z połączenia Internetowego ogółem w miesiącu, a jak długo w tygodniu. Dodatkowo możesz ustalić przez ile godzin w danym dniu tygodnia. Umożliwia to udostępnienie dzieciom Internetu w różne dni o różnych porach. Z prawej strony suwaków znajdują się pola edycyjne umożliwiające zdefiniowanie tych samych wartości poprzez wpisanie liczb w formacie dni/godziny:minuty. Wpis 04/20:05 oznacza możliwość korzystania z Internetu przez 4 dni, 20 godzin i 5 minut.



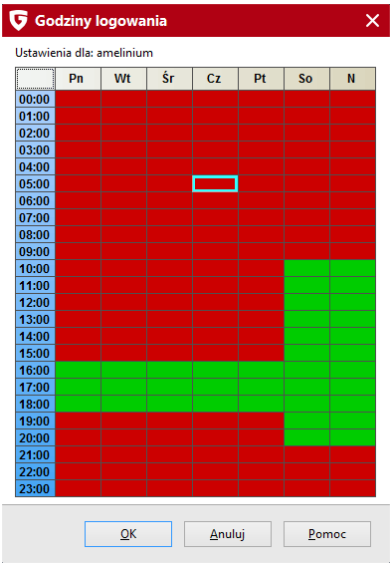
W przypadku ustawienia niezgodnych wartości dla miesiąca i tygodnia, brana pod uwagę będzie tylko wartość mniejsza. Przykładowo, jeśli

zezwolimy na korzystanie z Internetu przez 4 dni w miesiącu, ale przez 5 dni w tygodniu, program automatycznie zaakceptuje tylko mniejszą wartość zezwalając na korzystanie z Internetu w ciągu tygodnia przez 4 dni.

W momencie próby połączenia z Internetem po upływie zdefiniowanego czasu, przeglądarka wyświetli komunikat informujący o wyczerpaniu limitu.

8.4.1 Godziny logowania

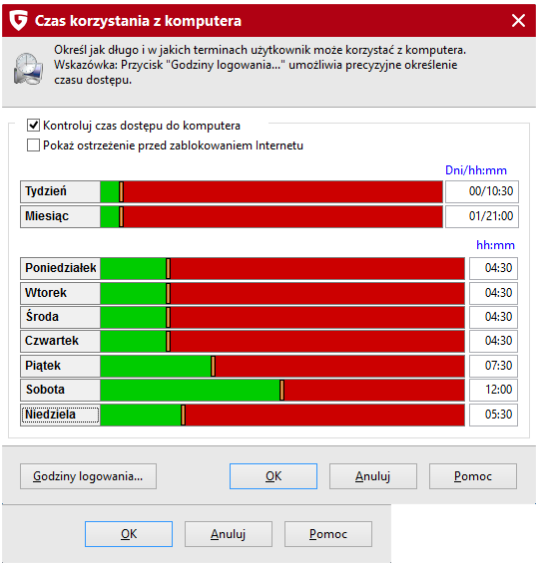
Kliknij przycisk **Godziny logowania...** aby precyzyjnie ustalić godziny korzystania z Internetu w konkretne dni tygodnia. Na zielono zaznaczone są godziny korzystania z Internetu. W kolorze czerwonym przedstawione są godziny, w których korzystanie z połączenia Internetowego jest zabronione.



Zaznacz wybrany przedział godzin myszką. Pojawi się menu kontekstowe oferujące dwie możliwości - **Blokuj** i **Zezwalaj**. Po wybraniu jednej z opcji program oznaczy wybrany przedział odpowiednim kolorem. W momencie próby połączenia z Internetem w niedozwolonych godzinach, przeglądarka wyświetli odpowiedni komunikat.

8.5 Kontroluj czas dostępu do komputera

W tym oknie możesz skonfigurować czasową blokadę dostępu danego użytkownika do Internetu. W tym celu zaznacz pole Kontroluj czas dostępu do komputera. Korzystając z suwaków zdecyduj, jak długo użytkownik może korzystać z komputera ogółem w miesiącu, a jak długo w tygodniu. Dodatkowo możesz ustalić przez ile godzin w danym dniu tygodnia. Umożliwia to udostępnienie dzieciom komputera w różne dni o różnych porach.

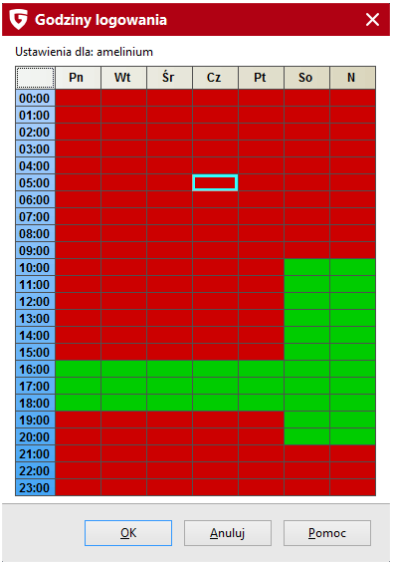


Z prawej strony suwaków znajdują się pola edycyjne umożliwiające zdefiniowanie tych samych wartości poprzez wpisanie liczb w formacie dni/godziny:minuty. Wpis 04/20:05 oznacza możliwość korzystania z komputera przez 4 dni, 20 godzin i 5 minut.

W przypadku ustawienia niezgodnych wartości dla miesiąca i tygodnia, brana pod uwagę będzie tylko wartość mniejsza. Przykładowo, jeśli zezwolimy na korzystanie z komputera przez 4 dni w miesiącu, ale przez 5 dni w tygodniu, program automatycznie zaakceptuje tylko mniejszą wartość zezwalając na korzystanie z komputera w ciągu tygodnia przez 4 dni.

8.5.1 Godziny logowania

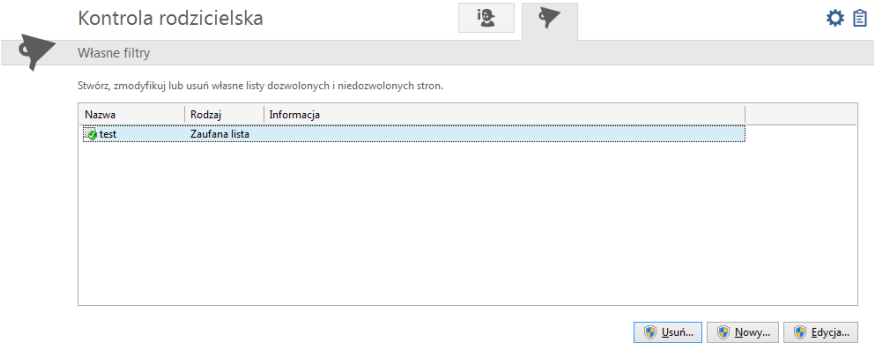
Kliknij przycisk **Godziny logowania...** aby precyzyjnie ustalić godziny korzystania z komputera w konkretne dni tygodnia. Na zielono zaznaczone są godziny dostępności komputera. W kolorze czerwonym przedstawione są godziny, w których logowanie do komputera będzie zablokowane.



Zaznacz wybrany przedział godzin myszką. Pojawi się menu kontekstowe oferujące dwie możliwości - **Blokuj** i **Zezwalaj**. Po wybraniu jednej z opcji program oznaczy wybrany przedział odpowiednim kolorem. W momencie próby zalogowania w niedozwolonych godzinach, system wyświetli odpowiedni komunikat.

8.6 Własne filtry

Uruchamiając widok **Własne filtry** można modyfikować stworzone wcześniej białe i czarne listy, a także tworzyć nowe filtry.



Białe i czarne listy różnią się od siebie zasadniczo:

- **Treści dozwolone:** Jeśli dla określonego użytkownika wybrana zostanie biała lista, będzie on mógł przeglądać w Internecie tylko te strony, które znajdują się na białej liście. Administrator można przyporządkować użytkownikom wszystkie lub tylko wybrane białe listy. Przydatne jest to w celu udostępniania młodszym tylko konkretnych stron internetowych odpowiednich dla danego etapu rozwoju.

- **Treści niedozwolone:** Za pomocą czarnych list można zablokować dostęp do konkretnych stron internetowych. Poza tym użytkownik może odwiedzać wszystkie inne strony internetowe. Czarna lista adresów internetowych nie daje zupełniej ochrony przed niepożądanymi treściami.

Nie da się używać białej i czarnej listy jednocześnie. Już sama biała lista powoduje największe ograniczenia dostępu do treści pochodzących z Internetu.

Do edycji list służą następujące funkcje programu kontroli rodzicielskiej:

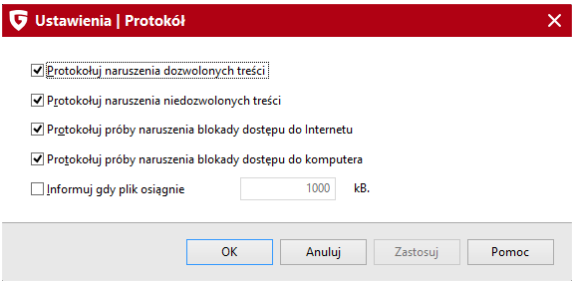
- **Usuń:** Przy pomocy tej funkcji można usunąć wybraną listę.

- **Nowy...:** Przycisk umożliwia utworzenie nowej białej lub czarnej listy. Procedura jest tu taka sama jak opisano w rozdziałach Treści niedozwolone 49 i Treści dozwolone 51.

- **Edycja...:** Ten przycisk pozwala modyfikować zawartość istniejącej listy.

8.7 Ustawienia|Protokół

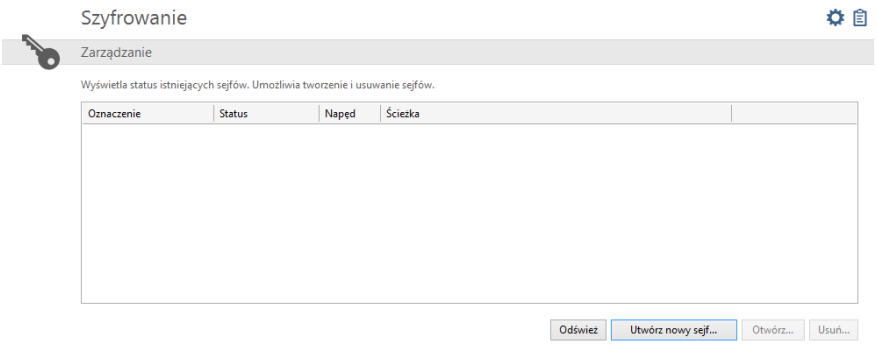
Okno umożliwia wybór raportowanych informacji. Można tu ustalić, jakie naruszenia ustalonych zasad kontroli mają być protokołowane. Zapisane raporty można przeglądać w widoku Protokół.



Pliki protokołów przy regularnym użytkowaniu mogą osiągać dość duże rozmiary, program kontroli rodzicielskiej może przypominać, że dany plik protokołu osiągnął podaną wielkość gdy zaznaczysz Informuj gdy plik osiągnie ... kB. Wówczas w widoku protokołu można usunąć zbędne raporty.

9 Szyfrowanie

Ten składnik pakietu umożliwia przechowywanie danych w wirtualnych sejfach. Można utworzyć dowolną ilość sejfów do których dostęp chroniony jest hasłem. Każdy sejf może mieć kilka różnych haseł dostępu na różnym poziomie uprawnień. Można przykładowo założyć hasło, które umożliwi jedynie odczyt danych z sejfu.

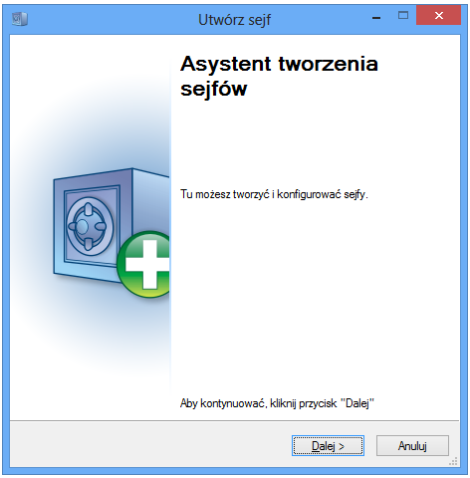


Do zarządzania sejfami służą 4 następujące przyciski:

- **Odśwież:** Odświeża informacje na temat stanu i ilości sejfów w systemie.
- **Otwórz/Zamknij:** Te przyciski umożliwiają otwarcie lub zamknięcie zaznaczonego sejfu. Do otwarcia sejfu wymagane jest podanie wcześniej ustalonego hasła.
- **Utwórz nowy sejf...:** To polecenie otwiera okno asystenta tworzenia nowego sejfu. Szczegóły znajdziesz w rozdziale Tworzenie sejfu 59.
- **Utwórz sejf przenośny...:** Zaznacz istniejący sejf kliknięciem myszy. Pojawi się przycisk umożliwiający przeniesienie sejfu wraz z zawartością na dowolny nośnik (napęd USB, płyta CD/DVD). Szczegóły znajdziesz w rozdziale Tworzenie sejfu przenośnego 63.
- **Usuń...:** Po zaznaczeniu niepotrzebnego sejfu możesz użyć tego polecenia do jego usunięcia. Sejf zostanie usunięty wraz z zawartością. Usunięcie sejfu nie wymaga podania hasła.

9.1 Tworzenie sejfu

Asystent tworzenia nowego sejfu zgromadzi informacje na temat sejfu i utworzy wirtualną partycję, do której dostęp będzie zabezpieczony hasłem.



9.1.1 Lokalizacja i rozmiar sejfu

Pierwsze okno umożliwia wskazanie lokalizacji zapisu sejfu oraz ustalenie jego maksymalnego rozmiaru.

Lokalizacja sejfu

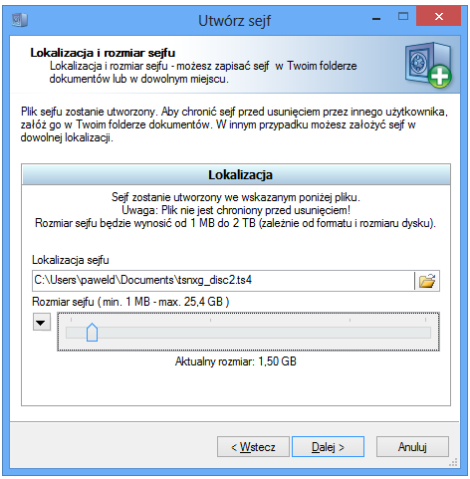
Domyślnie program utworzenie sejfu w folderze dokumentów bieżącego użytkownika. Można też umieścić sejf w dowolnie wybranym folderze.

Wskazówka: Sejf tworzony jest w postaci pliku powiązanego z wirtualną partycją na dysku. Po otwarciu sejfu, w oknie eksploratora Windows pojawia się nowy napęd. Przenoszenie folderów i plików do sejfu, a także operacje na plikach i usuwanie elementów z sejfu wykonuje się tradycyjnie w eksploratorze tak jak w przypadku zwykłego napędu dysku twardego lub pendrive'a. Po zamknięciu sejfu napęd znika samoistnie.

Rozmiar sejfu

Poniżej znajduje się suwak umożliwiający ustawienie rozmiaru sejfu.

Klikając strzałkę po lewej stronie suwaka otworzysz menu umożliwiające dokładniejsze ustawienie rozmiaru. Można podać wartość liczbową w MB lub wybrać jedną z proponowanych wartości.



Uwaga: Utworzenie sejfu na danej partycji spowoduje zarezerwowanie określonego w rozmiarze sejfu miejsca tylko na potrzeby sejfu. Jeśli utworzysz sejf o maksymalnym rozmiarze, program zarezerwuje dla sejfu całe wolne miejsce na wybranej partycji. Zaleca się tworzenie sejfów o rozmiarach dostosowanych do potrzeb, na partycjach z dostępną odpowiednią ilością miejsca.

9.1.2 Parametry sejfu

Dostępne są następujące parametry określające właściwości sejfu:

- **Nazwa sejfu:** Nazwa pod którą sejf będzie widoczny w programie G Data i w eksploratorze Windows.
- **Opis:** Dodatkowy opis ułatwiający identyfikację sejfu.
- **System plików:** Program G Data automatycznie może dobrać rozmiar sejfu w zależności od wskazanego wcześniej rozmiaru. W razie potrzeby można wybrać ręcznie system plików FAT lub NTFS. Zaleca się pozostawienia domyślnego ustawienia.

- **Automatycznie wybierz literę sejfu:** Sejf pojawi się w oknie eksploratora Windows jako kolejny napęd z przypisanym oznaczeniem literowym (jak nowa partycja). Zaleca się pozostawienie automatycznego wyboru litery (Tak), ale w razie potrzeby można ręcznie wskazać jedną z dostępnych liter.

- **Wybierz:** Po przełączeniu na ręczny wybór litery sejfu ta lista zostanie odblokowana i umożliwi wybór litery dla sejfu z listy niezarezerwowanych liter.

9.1.3 Dostęp do sejfu

Dla każdego hasła można nadać inne uprawnienia sejfu. Kliknij przycisk **Dodaj** aby dodać nowe hasło.

Wpisz i powtórz hasło, które umożliwi otwieranie sejfu. Jeśli chcesz nadać specjalne uprawnienia dla danego hasła otwierającego sejf, kliknij przycisk **Uprawnienia**. Dostępne są następujące ustawienia dodatkowe:

- **Przetwarzaj autostart:** W każdym sejfie znajduje się folder o nazwie Autostart. Podczas otwierania sejfu program uruchomi wszystkie pliki wykonywalne znajdujące się w tym folderze, jeżeli ta opcja będzie włączona.

- **Otwieraj w trybie "Tylko do odczytu":** Po otwarciu sejfu tym hasłem nie będzie można zapisywać ani modyfikować plików w sejfie.

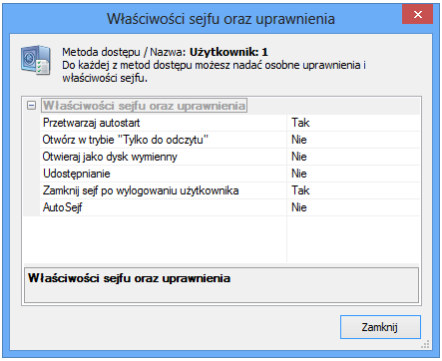
- **Otwieraj jako dysk wymienny:** Domyślnie program otwiera sejfy widoczne w Eksploratorze Windows jako dyski lokalne. Jeżeli chcesz, żeby sejf po otwarciu tym hasłem był widziany jako dysk wymienny, zaznacz tę opcję.

- **Udostępnianie:** Po zaznaczeniu tej opcji będzie można, po otwarciu tym hasłem, udostępnić sejf w systemie Windows dla innych komputerów w sieci.

  Uwaga: Jeśli sejf zostanie udostępniony, po jego otwarciu użytkownicy innych komputerów będą mieli do niego dostęp bez potrzeby podawania hasła!

- **Zamknij sejf po wylogowaniu użytkownika:** Zaleca się, aby ta opcja pozostała włączona. W innym przypadku po wylogowaniu użytkownika inne osoby korzystające z komputera będą miały swobodny dostęp do sejfu.

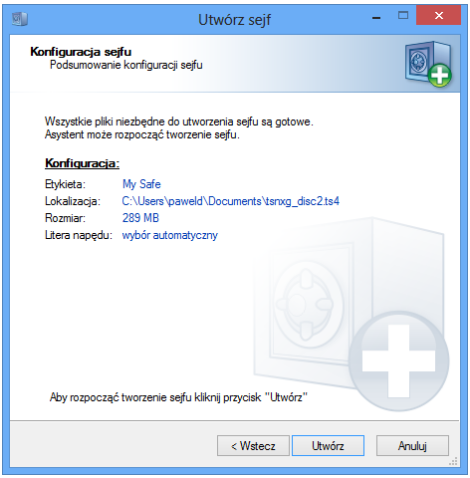
Po wybraniu uprawnień sejfu dla danego hasła kliknij przycisk **Zamknij**.



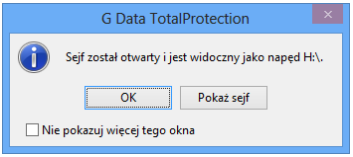
W oknie dostęp do sejfu kliknij **Dalej**.

9.1.4 Konfiguracja sejfu

W ostatnim oknie asystenta tworzenia sejfu widać spis wszystkich ustawionych parametrów sejfu. Jeśli chcesz zmienić ustawienia kliknij przycisk **Wstecz**. Jeżeli wszystko się zgadza kliknij **Utwórz** aby zbudować sejf.



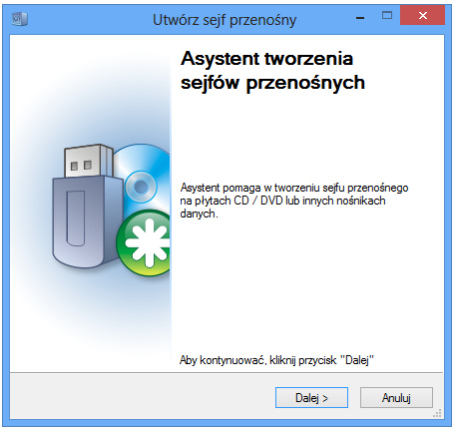
Sejf zostanie utworzony i zapisany na dysku. Po zakończeniu procesu masz możliwość zamknięcia okna przyciskiem OK lub wyświetlenia zawartości sejfu za pomocą przycisku **Pokaż sejf**.



9.2 Tworzenie sejfu przenośnego

Zaznacz istniejący sejf kliknięciem myszy. Pojawi się przycisk umożliwiający przeniesienie sejfu wraz z zawartością na dowolny nośnik (napęd USB, płyta CD/DVD).

Kliknij przycisk **Dalej** aby rozpocząć.



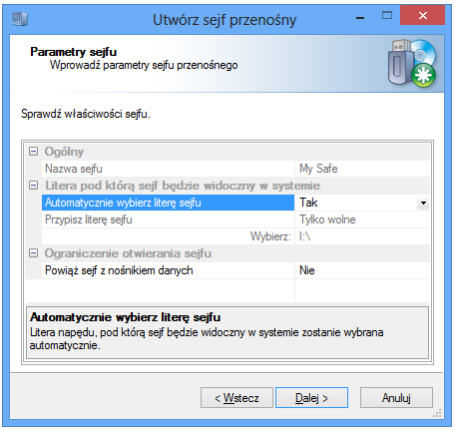
9.2.1 Parametry sejfu przenośnego

Okno przedstawia wszystkie parametry określające właściwości sejfu przenośnego. Modyfikować można tylko niektóre z nich:

- **Automatycznie wybierz literę sejfu:** Sejf pojawi się w oknie eksploratora Windows jako kolejny napęd z przypisanym oznaczeniem literowym (jak nowa partycja). Zaleca się pozostawienie automatycznego wyboru litery (Tak), ale w razie potrzeby można ręcznie wskazać jedną z dostępnych liter.

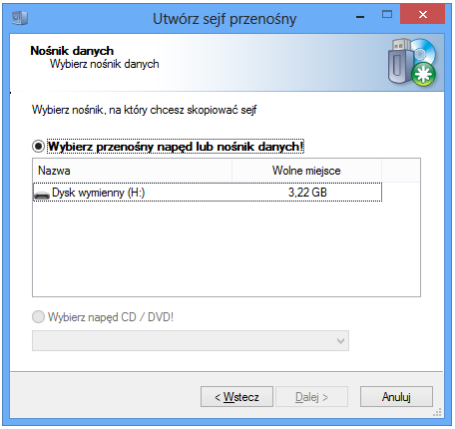
- **Wybierz:** Po przełączeniu na ręczny wybór litery sejfu ta lista zostanie odblokowana i umożliwi wybór litery dla sejfu z listy niezarezerwowanych liter.

- **Powiąż sejf z nośnikiem danych:** Po włączeniu tej opcji, sejf da się otworzyć tylko pod warunkiem, że będzie się znajdował na dysku twardym lub napędzie USB, do którego zostanie przypisany podczas tworzenia. Jeśli sejf nie jest powiązany z nośnikiem, można go otworzyć po przeniesieniu/skopiowaniu pliku sejfu (plik z rozszerzeniem *.ts4) na inny komputer lub nośnik.



9.2.2 Nośnik danych

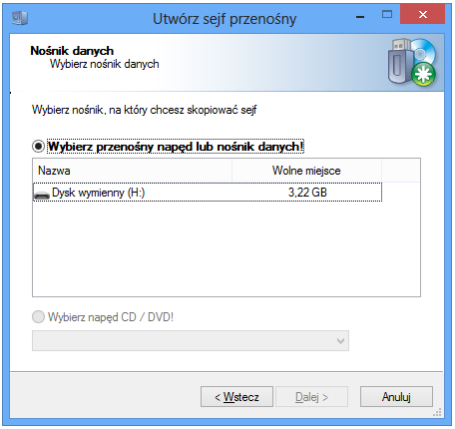
Wybierz nośnik, na który chcesz przenieść sejf. Może to być dysk lub pendrive USB lub też płyta CD/DVD.



Wskazówka: Jeśli przeniesiesz sejf na płytę, nie będzie oczywiście możliwe modyfikowanie jego zawartości.

9.2.3 Rozmiar sejfu

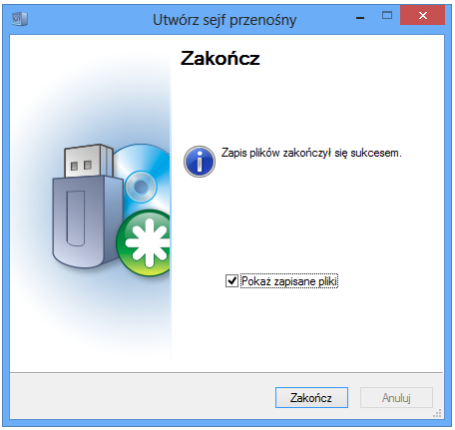
Okno wyświetla rozmiar potrzebny na zapisanie sejfu na nośniku wymiennym. W tym oknie można anulować proces tworzenia nośnika.



Wskazówka: Rozmiar całkowity sejfu powiększony jest o ok 6 MB niezbędnych do umieszczenia na nośniku sterowników do jego obsługi. Bez sterowników sejfu system Windows bez programu G Data nie będzie w stanie otworzyć sejfu przenośnego.

9.2.4 Zakończ

Po kliknięciu przycisku **Zakończ** sejf zostanie utworzony. Jeśli zaznaczysz opcję **Pokaż zapisane pliki**, po zakończeniu procesu tworzenia sejfu otworzy się okno zawierające pliki sejfu.



9.3 Otwieranie sejfu przenośnego

Aby skorzystać z sejfu przenośnego, umieść nośnik z nagranym sejfem w napędzie lub gniazdku USB komputera. Nośnik uruchomi się automatycznie i zainstaluje w komputerze sterowniki i inne elementy niezbędne do obsługi sejfu i metod dostępu. Po zainstalowaniu elementów obsługi może poprosić o zgodę na ponowne uruchomienie komputera. Ten krok jest niezbędny, aby sejf przenośny działał poprawnie.

Po ponownym uruchomieniu komputera ponownie uruchomić sejf przenośny. Pojawi się okno umożliwiające otwarcie lub zamknięcie sejfu. Domyślnie sejf jest zamknięty.

Po kliknięciu przycisku **Otwórz sejf** pojawi się okno logowania do sejfu. Sejf przenośny nie oferuje zabezpieczenia przed podsłuchiwaniem haseł. W oknie logowania do sejfu przenośnego nie będzie zatem informacji o ochronie haseł przed programami szpiegowskimi.

Po otwarciu sejf pojawi się w Eksploratorze Windows obok dysków lokalnych

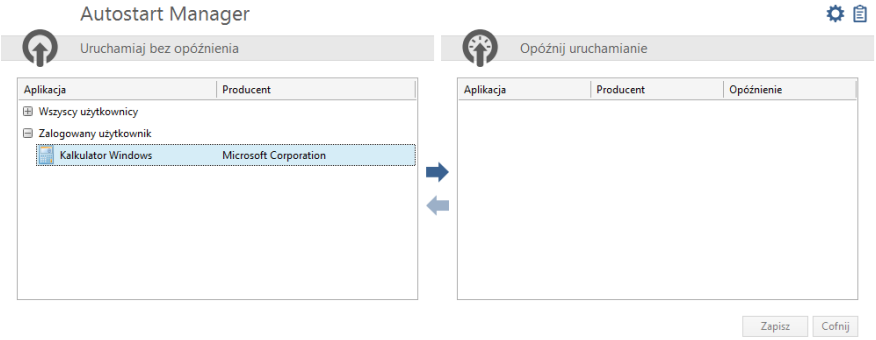
jako dysk wymienny o nazwie sejfu z odpowiednią literą. Każdy użytkownik sejfu przenośnego może skopiować dane z sejfu na komputer. W przypadku sejfu przenośnego nagranego na napęd USB FLASH, użytkownik z odpowiednimi uprawnieniami może również kopiować pliki z komputera do sejfu.

Zamykanie sejfu przenośnego przebiega podobnie jak zamykanie sejfu w programie G Data. Można kliknąć dwukrotnie literę sejfu w Eksploratorze Windows, lub kliknąć ją prawym klawiszem i wybrać odpowiednie polecenie z menu kontekstowego.

Uwaga: Zaleca się zamknięcie sejfu po wykonaniu potrzebnych działań przed wyjęciem nośnika z napędu. W tym celu należy otworzyć na nośniku z sejfem odpowiedni folder uruchomić plik Start.exe. Pojawi się okno umożliwiające zamknięcie sejfu.

10 Autostart Manager

Moduł Autostart Manager umożliwia wybiórcze opóźnianie uruchamiania programów, które włączane są przy starcie systemu operacyjnego. Dzięki tej funkcji komputer może uruchamiać się szybciej i nie jest obciążony przy starcie.



Po lewej stronie widoku Autostart Manager wyświetlone są wszystkie aplikacje uruchamiane wraz ze startem systemu.

 Zaznacz wybrane pozycje i przenieś je na listę opóźnionego uruchamiania klikając klawisz strzałki w prawo.

Zaznacz wybrane pozycje i usuń je z listy opóźnionego uruchamiania klikając klawisz strzałki w lewo.

Opóźnienie

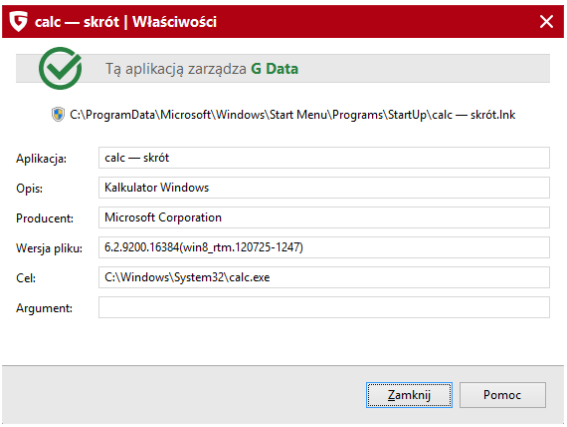
Rozwijając listę w kolumnie **Opóźnienie** możesz zmodyfikować czas i metodę opóźnienia uruchamiania danej aplikacji.

Nie uruchamiaj: Aplikacja nie będzie uruchamiać się automatycznie.

- **1 - 10 min.:** Uruchamianie aplikacji będzie opóźnione o zadaną ilość minut.
- **Automatycznie:** Program sam zadecyduje o sposobie uruchamiania aplikacji w zależności od bieżącego obciążenia procesora i dysku. Aplikacje uruchamiane automatycznie będą dopuszczane do uruchomienia kolejno po zwolnieniu zasobów przerobowych komputera.

10.1 Właściwości

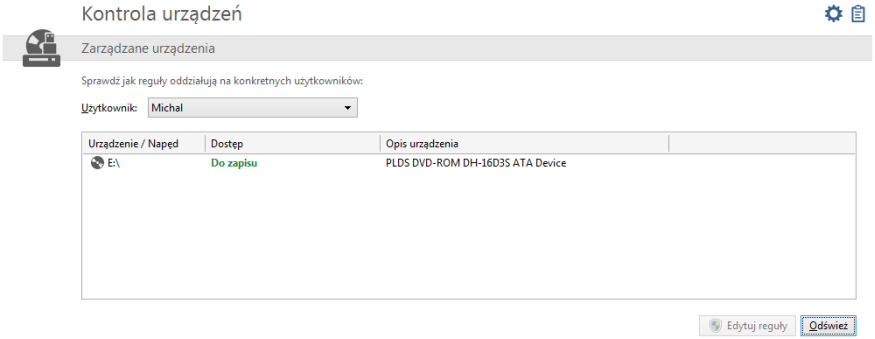
Dwukrotne kliknięcie danej pozycji na liście otwiera okno właściwości uruchamianej aplikacji.



11 Kontrola urządzeń

Kontrola urządzeń umożliwia ograniczenie użytkownikom bez praw administratora dostępu do urządzeń pamięci masowej komputera. Można blokować dostęp do napędów USB, CD/DVD oraz tradycyjnych dyskietek.

Widok przedstawia listę ograniczeń ustawionych dla konkretnego użytkownika systemu Windows. Przycisk **Edytuj reguły** otwiera okno ustawień danej reguły.



12 Ustawienia

Przycisk **Ustawienia** otwiera okno umożliwiające dokonania modyfikacji w konfiguracji wszystkich składników pakietu. Opcje pogrupowane są w tematyczne grupy opisane w kolejnych rozdziałach. Domyślnie program jest ustawiony w sposób gwarantujący maksymalną ochronę. Modyfikowanie ustawień programu nie jest niezbędne.

Zapisz ustawienia: To polecenie umożliwia wyeksportowanie wszystkich ustawień programu do pliku GDataSettings.gds. Możesz zastosować te ustawienia korzystając z opcji wczytania ustawień również na innych komputerach z programem G Data.

Wczytaj ustawienia: Ten przycisk umożliwia zaimportowanie do programu wybranych ustawień z wcześniej utworzonego pliku GDataSettings.gds. Można wybrać konkretne sekcje ustawień do zaimportowania.

Przywróć ustawienia: Ten przycisk umożliwia wybiórcze przywrócenie ustawień do stanu fabrycznego. Tu również Można wybrać konkretne sekcje ustawień do zaimportowania.

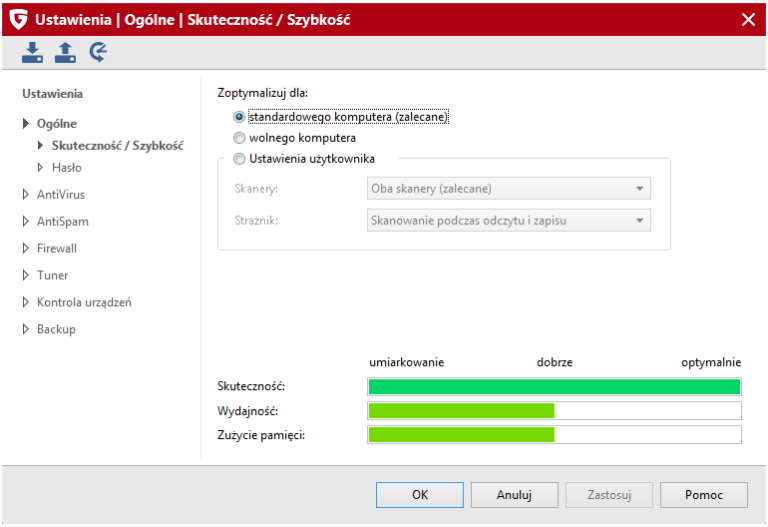
12.1 Ogólne

12.1.1 Skuteczność/szybkość

Program umożliwia dokonanie szybkiej zmiany w konfiguracji programu w celu zoptymalizowania wydajności słabszych komputerów. Wybierz pożądane ustawienie.

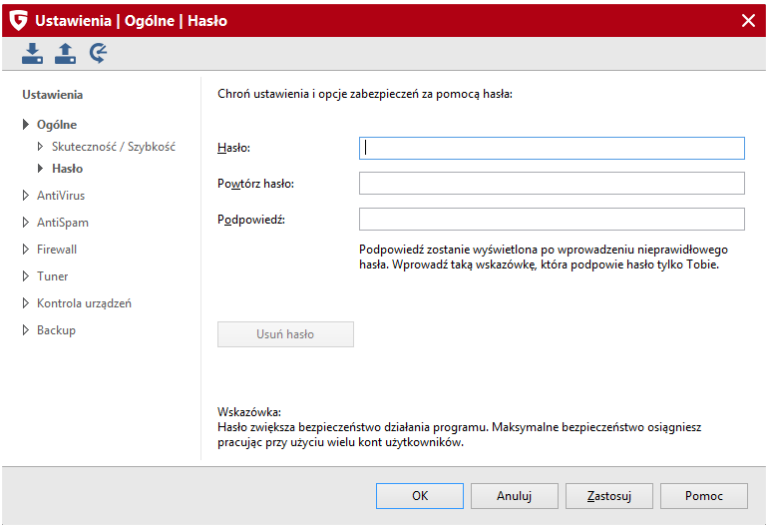
Zoptymalizuj dla:

- **standardowego komputera (zalecane):** Domyślne ustawienie programu. Oba skanery są włączone, skanowane są wszystkie próby odczytu i zapisu.
- **wolnego komputera:** Jeśli dysponujesz starszym komputerem, może zastosować to ustawienie w celu uzyskania większej wydajności systemu operacyjnego. Włączony będzie tylko jeden skaner antywirusowy (podobnie jak w przypadku większości programów antywirusowych, które stosują tylko jeden skaner). Skanowane będą tylko próby uruchomienia plików. Wykrywalność i skuteczność ochrony pozostaną na wysokim poziomie.
- **Ustawienia użytkownika:** Możesz samodzielnie skonfigurować opcje wydajności stosując to ustawienie.



12.1.2 Hasło

Ta sekcja umożliwia ustawienie hasła dostępu do zaawansowanych ustawień programu G Data. Tylko użytkownik znający hasło będzie mógł modyfikować opcje wpływające na skuteczność ochrony.



Wpisz dowolne hasło i powtórz je w polu **Powtórz hasło**. Możesz również wprowadzić tekst podpowiedzi.

Wskazówka: Podpowiedź zostanie wyświetlona po wprowadzeniu nieprawidłowego hasła.

Ochrona ustawień hasłem to dodatkowe zabezpieczenie oferowane przez program G Data. Maksymalne bezpieczeństwo system uzyskasz wymuszając stosowanie do pracy kont użytkowników z ograniczonymi uprawnieniami.

Wskazówka: Jeśli w komputerze stosowane są konta z ograniczonymi uprawnieniami, nie musisz stosować hasła do ustawień. Użytkownicy bez praw administratora nie będą mogli modyfikować ustawień. Klikając przycisk **Usuń hasło** możesz wyłączyć zabezpieczenie hasłem.

12.2 AntiVirus - Ustawienia

12.2.1 Ochrona w czasie rzeczywistym

Okno opcji Strażnika pozwala skonfigurować sposób monitorowania systemu plików przez Strażnika.

- **Włączony (zalecane):** Opcja umożliwia całkowite wyłączenie monitora dostępowego (niezalecane).

- **Skanery:** Strażnik może korzystać z dwóch niezależnych skanerów antywirusowych. Optymalną ochronę zapewnia zastosowanie dwóch skanerów. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor. Jednak jeśli dysponujesz starszym sprzętem lub mniejszą ilością pamięci, spróbuj wyłączyć skaner dodatkowy. Wydajność pracy komputera na pewno wzrośnie. Sam skaner podstawowy również zapewnia skuteczną ochronę przed wirusami.

- **Zarażone pliki:** Wybierz reakcję Strażnika na wykrycie wirusa. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Jeśli nie chcesz korzystać z domyślne go ustawienia (Dialog z użytkownikiem), zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: do Kwarantanny) umożliwia podjęcie decyzji o dalszych działaniach w późniejszym terminie.

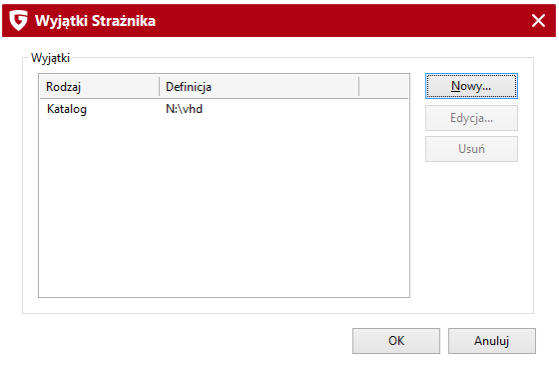
- **Zainfekowane archiwa:** Wybierz reakcję Strażnika na wykrycie wirusa w archiwach. Zalecamy wybranie opcji Dialog z użytkownikiem. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty skrzynek pocztowych lub ważnych danych.

Uwaga: Nie należy usuwać ani przenosić do Kwarantanny całych skrzynek pocztowych ani archiwów w przypadku wykrycia wirusa w jednej z wiadomości lub którymś pliku archiwum. Usunięcie pojedynczej wiadomości, można wykonać ręcznie w programie pocztowym.

- **Kontrola zachowania (inteligentne rozpoznawanie nieznanych szkodników)**: Jeżeli opcja kontroli zachowania jest włączona, oprogramowanie pyta użytkownika o potwierdzenie każdej modyfikacji kluczowych ustawień rejestru lub plików systemowych np. przez instalowane aplikacje. Dzięki włączeniu tej opcji, złośliwe aplikacje nie są wstanie zmodyfikować treści pliku systemowego hosts bez wiedzy użytkownika. Mechanizm kontroli zachowania reaguje również, jeśli uruchomiona aplikacja zachowuje się podobnie jak złośliwe oprogramowanie.

12.2.1.1 Wyjątki

W razie potrzeby można wyłączyć spod kontroli Strażnika wskazane napędy, foldery i pliki. Kliknij przycisk **Wyjątki** aby otworzyć okno wyjątków Strażnika. Aby dodać nowy wyjątek kliknij przycisk Nowy. Wskaż rodzaj obiektu, który chcesz pomijać przy kontroli (napęd, folder lub plik). Przycisk ... otworzy okno wyboru katalogu lub napędu.



Aby utworzyć wyjątek, wykonaj następujące kroki:

1 Kliknij przycisk Wyjątki.

2 W oknie wyjątków kliknij przycisk **Nowy**:

3 Wybierz rodzaj wyjątku. Można tworzyć wyjątki dla napędów, folderów lub plików.

4 W oknie wyboru wskaż obiekt, który chcesz wyjąć spod ochrony Strażnika. Jeżeli tworzysz wyjątek dla pliku, wpisz ręcznie jego nazwę lub zastosuj maskę pliku używając znaków zastępczych.

Dozwolone jest stosowanie następujących znaków zastępczych.

? Symbolizuje dowolny znak.

* Zastępuje dowolny ciąg znaków.

Przykładowo wykluczenie wszystkich plików z rozszerzeniem exe można zdefiniować stosując maskę pliku *.exe. Wyjątki dla różnych plików arkuszy kalkulacyjnych (xlr i xls) można ustawić wpisując tekst *.xl?. Jeżeli nie chcesz, żeby Strażnik skanował pliki, których nazwy rozpoczynają się od konkretnego słowa, np. tekst, wprowadź maskę tekst*.*.

5 Kliknij przycisk OK. Wyjątek pojawi się na liście.

6 Kliknij OK, aby zamknąć okno wyjątków.

Proces można powtarzać wielokrotnie. Można również usuwać i modyfikować zdefiniowane obiekty wyjątków.

12.2.1.2 Zaawansowane

Kliknij przycisk **Zaawansowane...**, aby otworzyć okno zaawansowanych ustawień Strażnika.

- **Tryb:** Domyślnie Strażnik skanuje pliki zarówno podczas odczytu jak i zapisu. Jest to najbezpieczniejsza opcja. Na żądanie można ograniczyć Strażnika do weryfikowania jedynie podczas odczytywania, lub jedynie podczas uruchamiania plików.

- **Nadzorowanie krytycznych folderów:** Jeśli **Strażnik** pracuje w trybie skanowania tylko w trakcje uruchamiania, dostępna jest dodatkowo opcja nadzorowania wybranych folderów. Zaznacz opcję, a następnie wskaż w oknie wyboru foldery, które chcesz objąć szczególną ochroną. W przypadku wybrania innego trybu pracy **Strażnika**, opcja nadzoru krytycznych folderów nie jest dostępna.

- **Skanuj zasoby sieciowe:** Jeśli komputer jest połączony w sieci z innymi stanowiskami, nie chronionymi przez program antywirusowy, (np. notebook), warto uruchomić opcje kontroli zasobów sieciowych. Strażnik będzie kontrolował zapis i odczyt plików znajdujących się na podłączonych w sieci komputerach. Nie musisz uruchamiać tej opcji, jeżeli Twój komputer nie jest połączony z innymi lub też jeżeli na podłączonych do sieci innych komputerach zainstalowana jest ochrona przed wirusami.

- **Heurystyka:** Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmaga skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.

- **Skanuj archiwa:** Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.

- **Skanuj pliki e-mail:** Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.

- **Skanuj obszary systemowe przy starcie komputera:** Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią niezwykle ważny element każdego systemu operacyjnego.

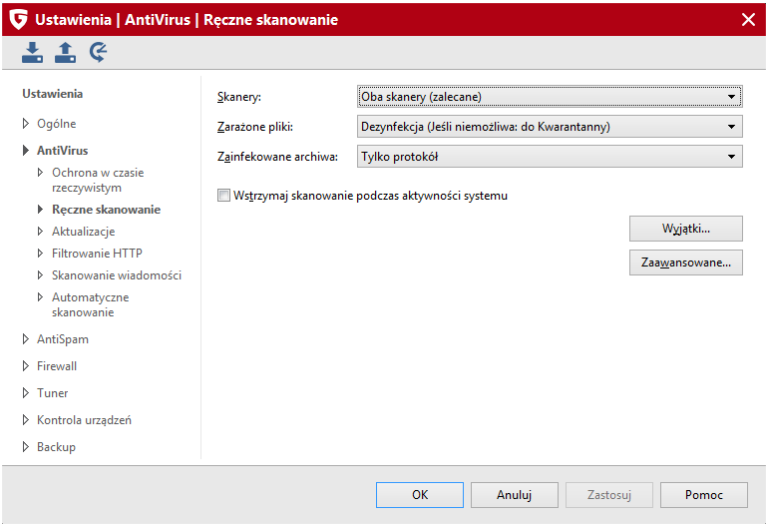
- **Skanuj obszary systemowe przy zmianie nośnika:** Obszary systemowe powinny być kontrolowane przy każdej sposobności. Ta opcja uruchomi skanowanie sektorów startowych przy każdej zmianie nośnika (np. włożenie do napędu nowej płytki CD-ROM).

- **Wykrywaj dialery / spyware / adware / riskware:** To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie może obniżyć poziom bezpieczeństwa systemu.

- **Skanuj tylko nowe i zmodyfikowane pliki:** Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji.

12.2.2 Ręczne skanowanie

Okno opcji skanowania pozwala dopasować parametry skanowania danych. Najlepiej przeprowadzać skanowanie komputera w chwili, kiedy nie jest obciążony innymi zadaniami. Umożliwi to wykorzystanie do skanowania wszystkich zasobów systemowych komputera, a tym samym nie będzie przeszkadzać użytkownikowi w pracy.



Do dyspozycji są następujące opcje i parametry:

- **Skanery:** Program korzysta z dwóch niezależnych skanerów antywirusowych. Optymalne efekty daje zastosowanie obu skanerów. Przy użyciu tylko jednego z nich, proces sprawdzania trwa krócej, ale jest mniej dokładny. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciąża procesor.

- **Zarażone pliki:** Wybierz reakcję skanera na wykrycie wirusa. Automatyczne usuwanie wirusów wraz z plikami może doprowadzić do utraty ważnych danych lub plików systemowych. Zastosowanie opcji **Dezynfekcja (Jeśli niemożliwa: przenieś do Kwarantanny)** umożliwia podjęcie decyzji o dalszych działaniach w późniejszym terminie.

- **Zarażone archiwa:** Wybierz reakcję skanera na wykrycie wirusa w archiwach. Wirusy w plikach archiwalnych mogą stanowić zagrożenie dopiero w momencie rozpakowania archiwum. Strażnik wykryje i zablokuje wirusa w momencie uruchomienia dekompresji. Skanowanie archiwów zalecane jest przed przekazaniem lub przesłaniem spakowanych plików innym użytkownikom, jeżeli nie masz pewności, że stosują skuteczne oprogramowanie antywirusowe.

- **Wstrzymaj skanowanie podczas aktywności systemu:** Ta funkcja spowoduje wstrzymanie skanowanie w momencie przeprowadzania przez

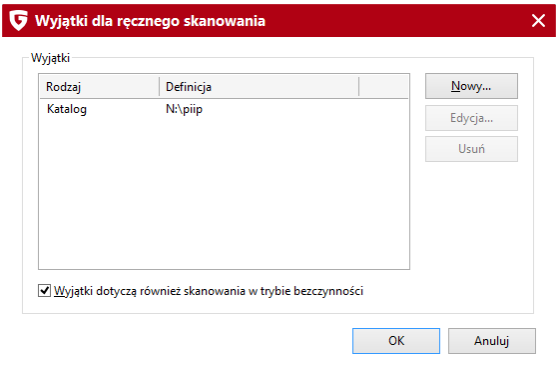
system operacyjny innych działań. Skanowanie zostanie automatycznie wznowione w momencie, kiedy komputer znów będzie bezczynny.

12.2.2.1 Wyjątki

Kliknij ten przycisk, jeśli chcesz ustawić foldery i pliki wykluczeń.

Uwaga: Wyjątki funkcjonują tylko w przypadku wybrania opcji skanowania całego komputera.

Wyjątki są stosowane również dla skanowania w trybie bezczynności.



1. Kliknij przycisk **Wyjątki...**.

2. Kliknij przycisk **Nowy...**

3. Wybierz rodzaj wyjątku.

4. Wskaż napęd, wybierz foldery lub wpisz maskę pliku stosując znaki zastępcze.

   Dozwolone są następujące znaki zastępcze:

- Znak zapytania (?) zastępuje dowolny znak.
- Gwiazdka (*) zastępuje dowolny ciąg znaków.

Aby pomijać przy skanowaniu wszystkie pliki z rozszerzeniem .sav wpisz maskę *.sav. Aby pomijać pliki o nazwach tekst1.doc, tekst2, doc, tekst3.doc), wpisz maskę tekst?.doc.

12.2.2.2 Zaawansowane

Kliknij przycisk **Zaawansowane**, aby otworzyć okno zaawansowanych ustawień skanowania:

- **Rodzaje plików:** Strażnik może skanować wszystkie pliki, lub tylko pliki programowe i dokumenty.
- **Heurystyka:** Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmaga skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.
- **Skanuj archiwa:** Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.
- **Skanuj pliki e-mail:** Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.
- **Skanuj obszary systemowe:** Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią podstawę systemu operacyjnego, zaleca się skanowanie obszarów systemowych co jakiś czas.
- **Wykrywaj dialery / spyware / adware / riskware:** To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie może obniżyć poziom bezpieczeństwa systemu.
- **Wykrywaj rootkity:** Opcja włącza dodatkowy skaner wykrywający rootkity, czyli mechanizmy służące do ukrywania złośliwych programów

przed oprogramowaniem zabezpieczającym.

- **Skanuj tylko nowe i zmodyfikowane pliki:** Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji.

- **Twórz raport:** Jeśli zaznaczysz pole Twórz raport, program będzie protokołował każdy proces skanowania.

- **Proponuj skanowanie nośników wymiennych:** Po podłączeniu pendrive'a lub dysku USB, program wyświetli komunikat umożliwiający przeskanowanie napędu.

12.2.3 Aktualizacje

W tym oknie można zmodyfikować ustawiania aktualizacji, wprowadzić inne dane dostępu do aktualizacji, a także przeprowadzić rejestrację programu przez Internet.

Wpisz w oknie aktualizacji dane dostępu (nazwę użytkownika i hasło) otrzymane w potwierdzeniu rejestracji programu.

Jeżeli korzystasz ze sprzętowej zapory sieciowej lub serwera proxy wymagającego wprowadzenia ustawień połączenia Internetowego, kliknij przycisk **Ustawienia Internetu...** i dokonaj wymaganych zmian.

Import/eksport sygnatur wirusów...: Ta funkcjonalność umożliwia aktualizowania sygnatur wirusów programu G Data bez potrzeby ponownego ich pobierania na kolejnych komputerach. Ułatwia to procedurę aktualizacji np. w przypadku wolnych łącz internetowych. Po wyeksportowaniu pobranych sygnatur wirusów, można udostępnić archiwum w sieci lub przenieść na dowolnym nośniku. Ta funkcjonalność nie umożliwia zautomatyzowania procesu aktualizacji. Użytkownik musi w takim przypadku samodzielnie wykonywać jak najczęstsze aktualizacje poprzez eksportowanie i importowanie sygnatur wirusów.

Uwaga: Do zaimportowania zapisanych sygnatur wirusów niezbędne jest połączenie z internetem w celu zweryfikowania licencji.

Automatyczna aktualizacja sygnatur wirusów

W razie potrzeby możesz wyłączyć opcję automatycznej aktualizacji sygnatur wirusów. Nie jest to jednak zalecane. Aktualne bazy wirusów to

kluczowy aspekt skutecznej ochrony przed zagrożeniami.

Standardowo harmonogram aktualizacji ustawiony jest na cogodzinne pobieranie aktualizacji. W razie potrzeby możesz zmienić ustawienie na codzienną aktualizację po pierwszym połączeniu z Internetem lub każdorazowo po nawiązaniu połączenia z Internetem.

Sporządź raport: Jeśli ta opcja jest włączona, program tworzy raport z każdej przeprowadzonej aktualizacji. Raporty można przejrzeć klikając w głównym oknie programu G Data ikonę protokołu.

12.2.3.1 Aktywuj licencję...

W formularzu rejestracyjnym wpisz numer rejestracyjny produktu i wypełnij wymagane pola. Jeżeli chcesz wprowadzić więcej danych, np. o miejscu zakupu oprogramowanie, wybierz opcję pełnej rejestracji. Numer rejestracyjny znajdziesz w opakowaniu z dostarczonym produktem lub w e-mailowym potwierdzeniu zakupu produktu w przypadku dokonania zakupu wersji elektronicznej.

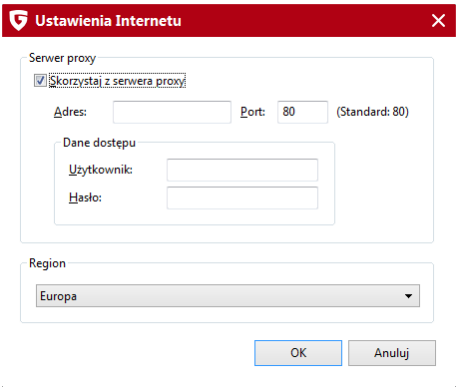
Kliknij przycisk **Zarejestruj...** aby przesłać formularz do serwera aktualizacji.

Po poprawnym przeprowadzeniu rejestracji pojawi się stosowny komunikat, który można zamknąć przyciskiem **Zamknij**. Dane dostępu zostaną automatycznie wpisane do programu i przesłane na wskazany w formularzu adres e-mailowy.

W przypadku wystąpienia problemów z rejestracją, sprawdź czy połączenie z Internetem działa prawidłowo.

12.2.3.2 Ustawienia Internetu...

Jeśli korzystasz z zapory sprzętowej lub serwera proxy, włącz opcję korzystania z serwera proxy i wprowadź dane do autoryzacji, jeżeli serwer ich wymaga.



Dodatkowo poniżej możesz ustawić region świata, w którym się znajdujesz w celu automatycznego przydzielenia do odpowiedniego serwera aktualizacji. Domyślnie ustawiony jest region Europa.

12.2.4 Filtrowanie HTTP

Filtr działa w trakcie otwierania stron przy pomocy przeglądarki internetowej. Okno opcji umożliwia modyfikowanie parametrów skanowania stron internetowych.

- **Sprawdzaj zawartość HTTP:** Ta opcja umożliwia globalne włączenie/wyłączenie filtra zawartości HTTP. Filtr jest potrzebny do wykrywania wirusów na stronach internetowych, a także do działania funkcji kontroli rodzicielskiej.

Jeśli wyłączysz monitorowanie zawartości stron internetowych, a w tym czasie gdy dojdzie do próby uruchomienia zainfekowanych plików znajdujących się już w folderach tymczasowych komputera, monitor dostępowy (Strażnik) będzie w stanie powstrzymać infekcję. Wyłączenie obu tych składników jednocześnie nie jest zalecane.

Możesz utworzyć listę stron internetowych, które nie będą skanowane. Służy

do tego przycisk **Wyjątki...**.

- **Ochrona przed phishingiem:** Ten mechanizm służy do ujawniania prób dokonania oszustw i naciągania przez Internet. Na takie ataki narażeni są klienci banków i sklepów internetowych. Ataki polegają na publikowaniu lub przesyłaniu w mailach linków do sfałszowanych stron internetowych, nakłaniających do podania danych dostępu do konta bankowego lub karty płatniczej. Filtr powinien być włączony podczas korzystania z bankowości internetowej lub zakupów online.

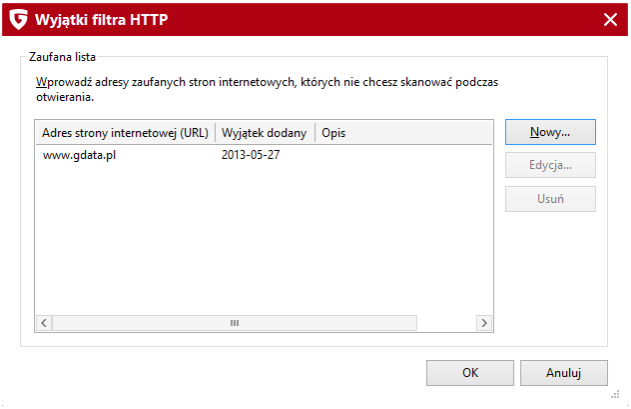
- **Zgłaszaj adresy zarażonych stron internetowych:** Jeżeli ta opcja jest włączona, program automatycznie przesyła do G Data Software adresy stron, na których wykryte zostały złośliwe programy. Zezwalając na wysyłanie danych o wirusach poprawiasz jakość ochrony oferowanej przez zakupiony program.

- **BankGuard (ochrona bankowości online i zakupów internetowych):** Technologia wykrywania szkodników atakujących zaszyfrowane sesje online uchroni Cię przed atakiem nowoczesnych zagrożeń nawet, jeśli szkodnik nie będzie wykrywany przez sygnatury wirusów. Czas życia tych szkodników jest zazwyczaj celowo bardzo krótki. Szybko powstają nowe wersje zagrożeń, a tradycyjne metody wykrywania nie są w stanie zablokować skutecznie ich działalności. Moduł BankGuard stosuje unikalną technologię opracowaną przez G Data specjalnie do neutralizowania zagrożeń związanych z bankowością online i zakupami internetowymi.

- **Ochrona przed keyloggerami:** Niezależnie od sygnatur wirusów, program wykrywa w tle wszelkie próby przechwycenia znaków wprowadzanych z klawiatury. Zapobiega to próbom przejęcia haseł i wrażliwych danych służących np. do logowania w serwisach internetowych. Zaleca się, aby ta funkcja była zawsze włączona.

12.2.4.1 Wyjątki HTTP

W niektórych przypadkach, skanowanie HTTP może spowodować nieprawidłowe wyświetlanie danej strony Internetowej lub blokowanie usługi dostępnej przez stronę. Program umożliwia konfigurację wyjątków HTTP. Strony ustawione jako wyjątki nie są skanowane. W celu dodania adresu strony do listy wyjątków wykonaj następujące kroki:



1 Kliknij przycisk **Wyjątki...**.

Pojawi się okno stron ustawionych jako wyjątki.

2 Aby dodać nowy adres do listy wyjątków, kliknij przycisk **Nowy...**. W polu URL wpisz nazwę strony. Wyjątek możesz opatrzyć dowolnym komentarzem.

Kliknij przycisk OK, aby zatwierdzić wyjątek.

3 Pojawi się komunikat o dodaniu adresu do listy. Kliknij OK w celu zamknięcia okna.

Aby usunąć wyjątek z listy, zaznacz go myszką i kliknij przycisk **Usuń**.

12.2.4.2 Zaawansowane

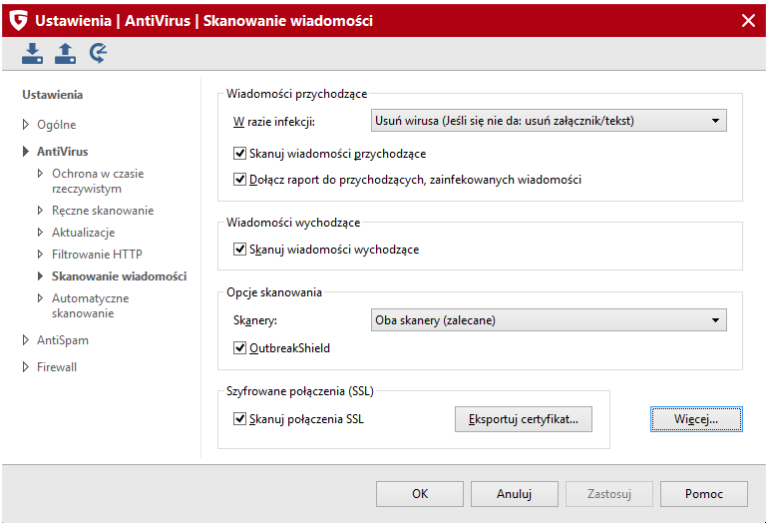
Jeśli korzystasz z niestandardowego portu HTTP (domyślnie 80), możesz w tym miejscu wprowadzić jego numer.

Ignoruj przekroczenie limitu czasu w przeglądarce: Skanowanie zawartości stron może spowodować opóźnienie ich wyświetlania w przeglądarkach Internetowych. Po włączeniu tej opcji, przeglądarka zaczeka dłużej na przekazanie danych strony z programu i nie wyświetli komunikatu o błędzie.

Ograniczenie rozmiaru skanowania pobieranych plików:
Ograniczenie rozmiaru skanowanych plików pozwala uniknąć długotrwałego skanowania dużych plików zawartych na sprawdzanej stronie internetowej. Skanowanie wszystkich plików znacznie spowalnia czas otwierania niektórych stron.

12.2.5 Skanowanie wiadomości

W przypadku wykrycia wirusa w wiadomości skaner może usunąć załącznik, spróbować zdezynfekować wiadomość lub usunąć niebezpieczną treść wiadomości.



Dodatkowo aplikacja instaluje w programie Microsoft Outlook wtyczkę skanującą przychodzące i wychodzące wiadomości. Po zainstalowaniu modułu (przebiega to automatycznie podczas instalacji programu), na pasku zadań Microsoft Outlook pojawia się ikona umożliwiająca skanowanie poszczególnych folderów poczty.

12.2.5.1 Wiadomości przychodzące

- **W razie infekcji:** Zdecyduj jak program ma postąpić z wykrytym wirusem. Wybierz stosowną reakcję w zależności od przeznaczenia komputera i ważności danych. Zalecane jest stosowanie opcji Dezynfekcja (Jeśli niemożliwa: usuń załącznik/treść).

- **Skanuj wiadomości przychodzące:** Jeśli opcja jest włączona, program sprawdza wszystkie przychodzące wiadomości.

- **Dołącz raport do przychodzących, zainfekowanych wiadomości:** Jeśli opcja ta jest aktywna, program dołączy do każdej zainfekowanej wiadomości stosowny komunikat.

12.2.5.2 Wiadomości wychodzące

Skanuj wiadomości wychodzące: Aby przypadkiem nie wysłać wiadomości z wirusem możesz zlecić programowi kontrolowanie wiadomości przed wysłaniem. Jeśli program wykryje wirusa, pojawi się komunikat: Wiadomość [Temat] zawiera wirusa: [Nazwa wirusa] Nie można wysłać wiadomości, a wiadomości zostanie zablokowana.

12.2.5.3 Opcje skanowania

- **Skanery:** Program korzysta z dwóch niezależnych skanerów antywirusowych. Optymalne efekty daje zastosowanie obu skanerów. Użycie dwóch skanerów do sprawdzania poczty gwarantuje najwyższą jakość ochrony antywirusowej.

- **OutbreakShield:** Moduł OutbreakShield łącząc się z aktualizowanym na bieżąco serwerem ustala, czy wiadomość stanowi zagrożenie na podstawie jej cech charakterystycznych. Dzięki temu jest w stanie zareagować na zagrożenie wcześniej, jeszcze przed stworzeniem i dostarczeniem do programu odpowiednich sygnatur wirusów.

12.2.5.4 Szyfrowane połączenia (SSL)

Dostawcy usług poczty elektronicznej udostępniają możliwość korzystania z opcji szyfrowania wiadomości. Dzięki temu konta pocztowe i wiadomości użytkowników są o wiele bezpieczniejsze. Aplikacje G Data umożliwiają obecnie ochronę poczty szyfrowanej protokołem SSL obsługiwanej przez

programy pocztowe.

W celu uruchomienia modułu ochrony poczty szyfrowanej niezbedne jest zaimportowanie do systemu operacyjnego lub programu pocztowego specjalnego certyfikatu G Data Software. Dzięki temu możliwe będzie skanowanie poczty pod kątem zagrożeń i niechcianych wiadomości.

Obsługiwane są wszystkie programy pocztowe umożliwiające zaimportowanie certyfikatu lub mające dostęp do magazynu certyfikatów systemu Windows, np.:

- **Outlook 2003** lub nowszy
- **Thunderbird**
- **The Bat**

Jeśli certyfikat nie został zaimportowany automatycznie, wykonaj następujące kroki aby go zainstalować do magazynu certyfikatów systemu Windows:

1. Zamknij wszystkie programy pocztowe.

2. Zaznacz w oknie Szyfrowane połączenia (SSL) opcję **Skanuj połączenia SSL**.

3. Kliknij przycisk **Eksportuj certyfikat**. Program G Data Software wygeneruje plik zawierający certyfikat. Plik nazywa się **GDataRootCertificate.crt**.

4. Otwórz plik **GDataRootCertificate.crt**. Pojawi się okno dialogowe umożliwiające zainstalowanie certyfikatu w systemie Windows.

5. Kliknij przycisk **Zainstaluj certyfikat...** i podążaj za wskazówkami asystenta instalacji.

Gotowe. Teraz programy pocztowe korzystające z magazynu certyfikatów Windows (np. Office Outlook) mają dostęp do certyfikatu G Data i pozwolą na skanowanie poczty szyfrowanej pod kątem zagrożeń i spamu.

Wskazówka: Jeśli korzystasz z programu pocztowego, który nie wykorzystuje magazynu certyfikatów Windows (np. Thunderbird), zaimportuj certyfikat ręcznie i dokonaj niezbędnej konfiguracji. W tym celu przejdź w programie Thunderbird do okna **Opcje > Zaawansowane > Certyfikaty**. Następne kliknij przycisk **Wyświetl certyfikaty** i przejdź do

zakładki **Organy certyfikacji**. Tam znajdziesz przycisk **Importuj...**. Wskaż wygenerowany wcześniej plik certyfikatu G Data **Mail Scanner Root**.

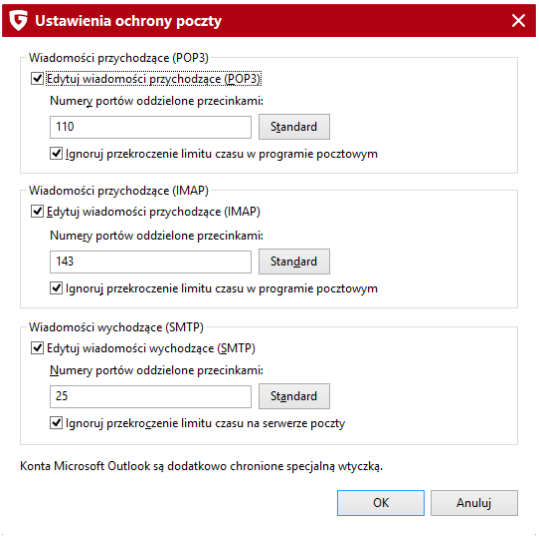
Zaznacz następujące opcje niezbędne do skanowania poczty szyfrowanej:

- Zaufaj temu CA przy identyfikacji witryn internetowych.
- Zaufaj temu CA przy identyfikacji użytkowników poczty.
- Zaufaj temu CA przy identyfikacji twórców oprogramowania.

W przypadku korzystania z innych programów pocztowych skorzystaj z dostępnych w nich opcji importu certyfikatów. W razie wątpliwości, zajrzyj do dokumentacji programu pocztowego.

12.2.5.5 Więcej

Ochrona skrzynek uruchamia się automatycznie po zainstalowaniu programu. W programie Microsoft Outlook pocztę chroni specjalny dodatek. W programach bazujących na protokołach POP3/IMAP (Outlook Express, Mozilla, Opera) poczta chroniona jest przez moduł ochrony kont POP3/IMAP.



Ochronę poszczególnych portów można włączyć lub wyłączyć zaznaczając/ odznaczając opcje **Edytuj wiadomości przychodzące (POP3/IMAP)** i **Edytuj wiadomości wychodzące (SMTP)**.

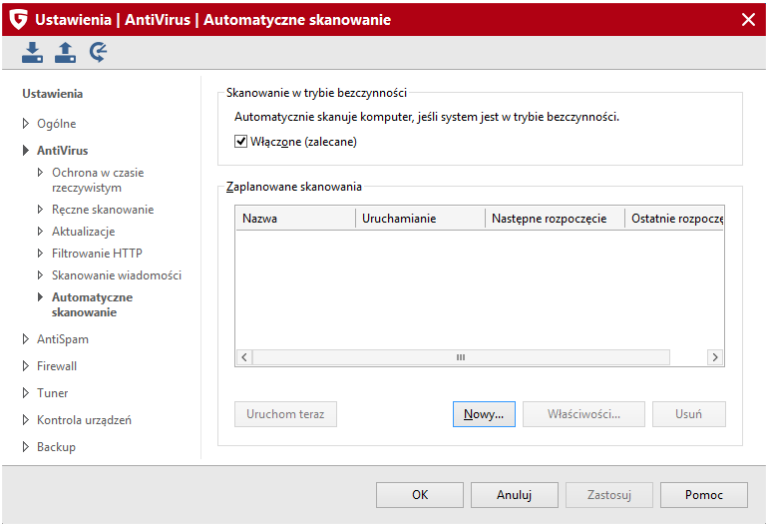
Ponieważ skanowanie poczty przychodzącej odbywa się przed przekazaniem wiadomości do programu pocztowego, może dojść do przekroczenia czasu oczekiwania programu pocztowego na odpowiedź serwera poczty (np. w przypadku odbierania dużej ilości wiadomości jednocześnie). Włączenie opcji **Ignoruj przekroczenie limitu czasu w programie pocztowym** spowoduje, że program pocztowy nie będzie wyświetlał komunikatów błędu przekroczenia limitu czasu oczekiwania.

Jeśli wykorzystujesz niestandardowe numery portów w programie pocztowym, wpisz w polach Numery portów odpowiednie wartości. Klikając przycisk **Standard** przywrócisz wartości domyślne. Jeżeli korzystasz z więcej niż jednego portu, wpisz wszystkie numery portów oddzielając je przecinkami.

Konta programu Microsoft Outlook chronione są dodatkowo przez automatycznie instalowaną wtyczkę umożliwiającą również skanowanie folderów i wiadomości z poziomu programu Microsoft Outlook. Zaznacz folder, który chcesz przeskanować i kliknij ikonę programu w pasku narzędzi programu Microsoft Outlook.

12.2.6 Automatyczne skanowanie

Zadanie automatycznego skanowania najlepiej powierzyć całkowicie innowacyjnej funkcji **Skanowanie w trybie bezczynności**. Nie musisz martwić się o konfigurowanie harmonogramów, czy też o wydajność komputera podczas skanowania. Skanowanie będzie uruchamiane automatycznie i wstrzymywane w momencie wykrycia aktywności systemu lub użytkownika.



Jeśli mimo wszystko chcesz tradycyjnie zaplanować skanowanie, kliknij przycisk **Nowy...** aby utworzyć nowy wpis harmonogramu automatycznego skanowania. Możesz utworzyć różne zlecenia skanowania stosować je jednocześnie.

Jeśli chcesz zmodyfikować daną pozycję harmonogramu, zaznacz ją myszką i kliknij przycisk **Właściwości...**. Pojawi się okno zlecenia umożliwiające modyfikowania parametrów zlecenia. Możesz również zlecić natychmiastowe uruchomienie skanowania przyciskiem **Uruchom teraz** albo usunąć zaznaczone zlecenie skanowania przyciskiem **Usuń**.

12.2.6.1 Ogólne

W polu **Nazwa** wpisz nazwę zlecenia.

Program może wyłączyć komputer po zakończeniu skanowania. Umożliwia to opcja **Wyłącz komputer po zakończeniu skanowania (jeśli nie jest zalogowany żaden użytkownik)**.

12.2.6.2 Rozmiar skanowania

W tym oknie możesz określić zakres skanowania dla zlecenia. Skanowane mogą być wszystkie dyski lokalne, pamięć i autostart lub też konkretne foldery i pliki. Kliknij przycisk **Przeglądaj...** aby wyświetlić okno wyboru folderów.

Po lewej stronie znajduje się drzewo folderów rozwijanych przyciskiem +. Skontrolowany zostanie każdy obiekt zaznaczony haczykiem. Jeśli nie zaznaczysz wszystkich podkatalogów czy plików danego katalogu, wiersz będzie koloru szarego. Czarnymi haczykami oznaczane są foldery skanowane w całości.

12.2.6.3 Planowanie

To okno służy do określenia częstotliwości wykonywania zleceń. W polu Wykonaj wybierz pożądaną częstotliwość i uzupełnij ustawienia korzystając z pól **Planowanie** oraz **Dni tygodnia** (w przypadku ustawienia opcji **Codziennie**).

Ustawienie **Uruchom skanowanie po uruchomieniu komputera, jeśli jest wyłączony** spowoduje wykonanie zaległego skanowania po uruchomieniu komputera, jeśli w czasie przewidzianym w harmonogramie komputer nie będzie uruchomiony.

Opcja **Nie uruchamiaj podczas pracy na baterii** jest aktywna tylko wtedy gdy korzystasz z laptopa działającego na zasilaniu bateryjnym.

12.2.6.4 Ustawienia skanowania

Okno opcji skanowania pozwala dopasować parametry skanowania danych. Najlepiej przeprowadzać skanowanie komputera w chwili, kiedy nie jest obciążony innymi zadaniami. Umożliwi to wykorzystanie do skanowania wszystkich zasobów systemowych komputera, a tym samym nie będzie przeszkadzać użytkownikowi w pracy.

Do dyspozycji są następujące opcje i parametry:

- **Skanery:** Program korzysta z dwóch niezależnych skanerów antywirusowych. Optymalne efekty daje zastosowanie obu skanerów. Przy użyciu tylko jednego z nich, proces sprawdzania trwa krócej, ale jest mniej dokładny. Zalecamy ustawienie Dwa skanery. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciąża procesor.

- **Zarażone pliki:** Wybierz reakcję skanera na wykrycie wirusa. Zastosowanie opcji Dezynfekcja (Jeśli niemożliwa: przenieś do Kwarantanny) umożliwia podjęcie decyzji o dalszych działaniach w późniejszym terminie.

- **Zainfekowane archiwa:** Wybierz reakcję skanera na wykrycie wirusa w archiwach. Wirusy w plikach archiwalnych mogą stanowić zagrożenie dopiero w momencie rozpakowania archiwum. Strażnik wykryje i zablokuje wirusa w momencie uruchomienia dekompresji. Skanowanie archiwów zalecane jest przed przekazaniem lub przesłaniem spakowanych plików innym użytkownikom, jeżeli nie masz pewności, że stosują skuteczne oprogramowanie antywirusowe.

- **Wstrzymaj skanowanie na czas aktywności systemu:** Ta funkcja spowoduje wstrzymanie skanowanie w momencie przeprowadzania przez system operacyjny innych działań. Skanowanie zostanie automatycznie wznowione w momencie, kiedy komputer znów będzie bezczynny.

Kliknij przycisk **Zaawansowane**, aby otworzyć okno zaawansowanych ustawień skanowania:

- **Rodzaje plików:** Strażnik może skanować wszystkie pliki, lub tylko pliki wykonywalne i dokumenty.

- **Heurystyka:** Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując pliki z sygnaturami wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, choć wzmaga skuteczność wykrywania wirusów, jest jednak bardzo czasochłonna. W niektórych przypadkach może także powodować fałszywe alarmy.

- **Skanuj archiwa:** Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne jeśli Strażnik jest włączony. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu rozprzestrzenianiu się.

- **Skanuj pliki e-mail:** Program kontroluje pocztę elektroniczną za pomocą modułu POP3 dla Outlook Express i podobnych oraz wtyczki do programu MS Outlook, nie ma więc potrzeby używania tej opcji.

- **Skanuj obszary systemowe:** Obszary systemowe (boot sektor, Master Boot Record itd.) stanowią podstawę systemu operacyjnego, zaleca się skanowanie obszarów systemowych co jakiś czas.

- **Wykrywaj dialery / spyware / adware / riskware:** To ustawienie włącza moduł wykrywający dialery, a także programy podwyższonego ryzyka, których stosowanie może obniżyć poziom bezpieczeństwa systemu.

- **Wykrywaj rootkity:** Opcja włącza dodatkowy skaner wykrywający rootkity, czyli mechanizmy służące do ukrywania złośliwych programów przed oprogramowaniem zabezpieczającym.

- **Skanuj tylko nowe i zmodyfikowane pliki:** Włączenie tej opcji spowoduje pomijanie podczas skanowania plików, które zostały już wcześniej sprawdzone i zakwalifikowane jako bezpieczne. Jeżeli dany plik uległ modyfikacji, zostanie sprawdzony pomimo włączenia tej opcji.

- **Twórz raport:** Jeśli zaznaczysz tę opcję, program będzie protokołował każdy proces skanowania.

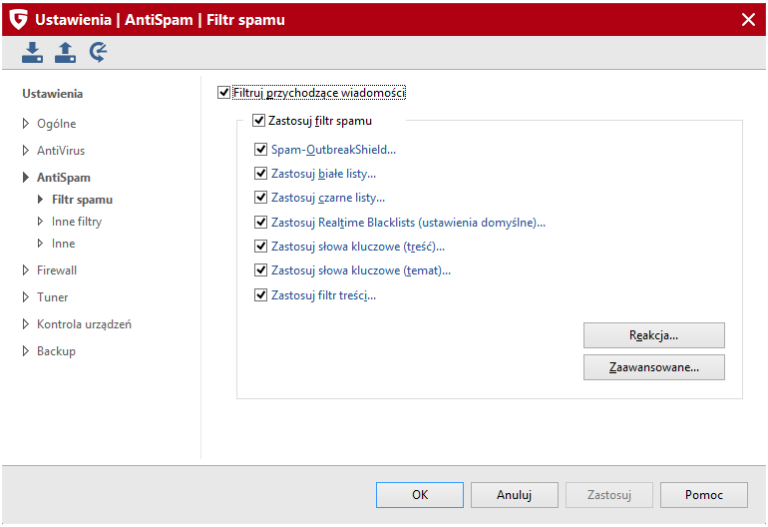
12.2.6.5 Konto użytkownika

W tej zakładce należy wpisać dane dostępu do sieci niezbędne w celu automatycznego skanowania napędów sieciowych.

12.3 AntiSpam - Ustawienia

12.3.1 Filtr spamu

Filtr spamu oferuje możliwość skutecznego blokowania niechcianych wiadomości. Program szuka w wiadomościach typowych dla spamu cech charakterystycznych. Na tej podstawie obliczany jest współczynnik prawdopodobieństwa, że dana wiadomość jest spamem.



Kliknij wiersz wybranego filtra, aby otworzyć okno jego ustawień:

Spam-OutbreakShield...

Umożliwia rozpoznawanie i zwalczanie wirusów w masowych wiadomościach jeszcze zanim sygnatury wirusów zostaną opracowane. System OutbreakShield wykrywa i rejestruje masowo wysyłane wiadomości i w czasie rzeczywistym powstrzymuje wysyłanie spamu. Moduł OutbreakShield jest zintegrowany z ochroną poczty elektronicznej.

Jeśli korzystasz z zapory sprzętowej lub serwera proxy, kliknij dwukrotnie tę pozycję i wybierz przycisk Ustawienia Internetu.... Włącz opcję korzystania z serwera proxy i wprowadź dane do autoryzacji, jeżeli serwer ich wymaga.

Zastosuj białe listy...

Aby wykluczyć konkretnych nadawców lub domeny z kręgu podejrzanych o wysyłkę spamu, można dodać wybrane adresy do listy zaufanych domen i adresów. W polu Adresy/Domeny wpisz adresy np. biuro@firma.pl lub domeny, np. gdata.pl, należące do zaufanych nadawców. Program AntiSpam nie będzie kontrolował wiadomości pochodzących od nadawców z listy. Istnieje też możliwość eksportowania i importowania list adresów i domen. Listy zapisywane są w postaci zwykłych plików tekstowych, a poszczególne adresy wyświetlone są jeden pod drugim.

Zastosuj czarne listy...

Do czarnej listy można dodać adresy i domeny typowych nadawców spamu. W tym celu wpisz w polu adresów i domen adresy mailowe oraz adresy domen, od których zazwyczaj dostajesz masowe, niechciane wiadomości. Program będzie standardowo traktował wiadomości od wskazanych nadawców jako spam. Istnieje też możliwość eksportowania i importowania list adresów i domen. Listy zapisywane są w postaci zwykłych plików tekstowych, a poszczególne adresy wyświetlone są jeden pod drugim.

Zastosuj Realtime Blacklists...

Są to aktualizowane na bieżąco przez Internet, znane w świecie listy domen i adresów wysyłających spam. AntiSpam samoczynnie aktualizuje listy wysyłając zapytania do serwerów zawierających spisy domen wysyłających spam. Zaleca się pozostawienie ustawień domyślnych, jednakże można wpisać własne adresy internetowych list domen wysyłających masowe wiadomości (zalecane tylko zaawansowanym użytkownikom).

Zastosuj słowa kluczowe (treść)...

Filtr słów kluczowych wyszukuje w treści wiadomości zadanego tekstu lub ciągu znaków. W momencie wykrycia słowa kluczowego, program zwiększa indeks prawdopodobieństwa, że dana wiadomość jest spamem. Edycja listy następuje przy użyciu przycisków Dodaj, Zmień i Usuń. Istnieje też możliwość eksportowania oraz importowania list słów kluczowych. Listy zapisywane są w postaci zwykłych plików tekstowych, a poszczególne wyrażenia wyświetlone są jeden pod drugim. Zaznaczenie opcji Wyszukuj tylko całe wyrazy (zalecane) spowoduje, że AntiSpam będzie szukał w treści wiadomości tylko całych wyrażeń j. np. ręka, a pominie wyrazy zawierające w sobie słowa kluczowe, np. rękawica.

Zastosuj słowa kluczowe (temat)...

Filtr słów kluczowych wyszukuje w tematach wiadomości zadanego tekstu lub ciągu znaków. W momencie wykrycia słowa kluczowego, program zwiększa indeks prawdopodobieństwa, że dana wiadomość jest spamem. Edycja listy następuje przy użyciu przycisków Dodaj, Zmień i Usuń. Istnieje też możliwość eksportowania oraz importowania list słów kluczowych. Listy zapisywane są w postaci zwykłych plików tekstowych, a poszczególne wyrażenia wyświetlone są jeden pod drugim. Zaznaczenie opcji Wyszukuj tylko całe wyrazy (zalecane) spowoduje, że program będzie szukał w tematach wiadomości tylko całych wyrażeń j. np. ręka, a pominie wyrazy zawierające w sobie słowa kluczowe, np. rękawica.

Zastosuj filtr treści...

Filtr treści zbudowany jest na podstawie samouczącego się algorytmu Bayesa, obliczającego indeks prawdopodobieństwa, że dana wiadomość jest spamem na podstawie słów użytych w treści wiadomości. Listy słów kluczowych powiększają się automatycznie z biegiem czasu. Przycisk Znajdź w tabeli pozwala sprawdzić, czy dane wyrażenie znajduje się już na liście wyuczonych słów kluczowych. Przycisk Wyczyść tabelę spowoduje usunięcie zawartości tabeli z wyuczonymi wyrażeniami, a proces uczenia się zacznie się od nowa.

12.3.1.1 Reakcja

W tym oknie możesz ustalić reakcję programu na wykrycie spamu lub potencjalnego spamu. Program stosuje trzy poziomy klasyfikowania podejrzanych wiadomości.

- **Podejrzenie o spam**: Program klasyfikuje wiadomości, w których wykrył jedną cechę charakterystyczną dla wiadomości masowych. Niekoniecznie wiadomość taka musi być spamem. Wiadomości wysyłane przez serwisy informacyjne, pochodzące z legalnych, zamówionych subskrypcji także wykazują czasem podobieństwo do maili masowych.

- **Wysokie prawdopodobieństwo spamu:** oznacza, że program wykrył w wiadomości więcej cech charakterystycznych dla wiadomości masowych. Tylko w nielicznych przypadkach okazuje się, że wiadomość nie jest spamem.

- **Bardzo wysokie prawdopodobieństwo spamu:** oznacza, że wiadomość spełnia wszystkie możliwe kryteria wiadomości masowych.

Reakcję programu można ustalić oddzielnie dla każdego poziomu prawdopodobieństwa. Kliknij przycisk Zmień przy danej kategorii, aby ustalić reakcję programu na wykrycie lub podejrzenie spamu. Jeśli chcesz aby wiadomość danej kategorii była odrzucana przez program, wybierz opcję Odrzuć wiadomość. Druga możliwość to dodanie komunikatu do tematu i treści wiadomości w celu jej oznaczenia.

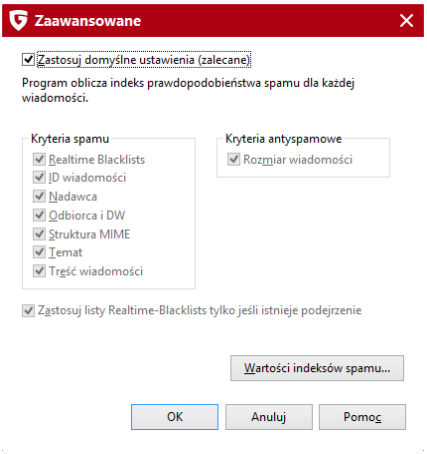
Jeśli używasz programu Microsoft Office Outlook (nie mylić z Outlook Express), program AntiSpam może przenosić niechciane i podejrzane wiadomości do zdefiniowanego folderu w skrzynce pocztowej (Przesuń wiadomość do folderu). Folder można założyć bezpośrednio z programu,

wpisując nazwę w polu Nazwa folderu.

Jeśli używasz innego programu pocztowego, załóż folder o dowolnej nazwie i utwórz regułę przenoszącą do niego wszystkie maile zawierające w temacie słowo [SPAM] tak domyślnie program oznacza masowe wiadomości.

12.3.1.2 Zaawansowane

Opcje zaawansowanej konfiguracji filtra Bayesa pozwalają na dokonanie szczegółowych ustawień i dopasowanie systemu przyznawania indeksów prawdopodobieństwa do przepływu maili w Twojej sieci. Zaleca się używanie ustawień domyślnych. Modyfikowanie ustawień zalecamy tylko zaawansowanym użytkownikom.



12.3.2 Inne filtry

W widoku **Inne filtry** można definiować inteligentne filtry, które blokują przychodzącą pocztę lub automatycznie usuwają z wiadomości potencjalnie niebezpieczną zawartość. Kliknij przycisk **Nowy**, aby utworzyć nową regułę filtra lub przycisk Edycja, aby zmodyfikować definicję istniejącego filtra.

Utworzone filtry wyświetlane są na liście w zakładce **Inne filtry** i można je w każdej chwili włączać lub wyłączać. Aby trwale usunąć filtr, należy go

zaznaczyć kliknięciem myszy, a następnie nacisnąć przycisk **Usuń**.

Możliwości definiowania filtrów w widoku **Inne filtry** dotyczą filtrów, które stanowią uzupełnienie podstawowego filtra antyspamowego programu AntiSpam. W obrębie danego filtra dostępne są również opcje umożliwiające skuteczne blokowanie wiadomości z niepożądaną zawartością lub wysyłanych przez niepożądanych nadawców (np. masowy mailing). Program sprawdza wiele cech charakterystycznych wiadomości. Na podstawie występowania tych cech obliczana jest suma kontrolna, która odzwierciedla prawdopodobieństwo, że dana wiadomość jest spamem. Patrz też rozdział Filtr spamu 94.

Pierwszym krokiem podczas definiowania nowego filtra jest wybór jego typu. Wszelkie modyfikacje utworzonego filtra można następnie wykonywać w oknach opcji powiązanych z wybranym typem filtra. W ten sposób można wygodnie zdefiniować zestaw filtrów zabezpieczający przed spamem.

- **Wyłącz skrypty HTML:** Spora część wiadomości pocztowych wysyłana jest w formacie HTML. Skrypty zawarte w wiadomościach HTML są w stanie uruchomić się już w momencie wywołania podglądu wiadomości w programie pocztowym. Świadomie preparowane skrypty mogą być niebezpieczne dla systemu. mogą prowadzić do stron zawierających złośliwe oprogramowanie, a także umożliwić zdalnemu użytkownikowi przejęcie kontroli nad systemem.

- **Filtr załączników:** Filtr służy do klasyfikowania wiadomości na podstawie właściwości załączonych plików. Większość wirusów komputerowych rozprzestrzenia się właśnie poprzez wysyłanie wiadomości z zarażonym załącznikiem. Może to być uruchamialny plik wirusa z rozszerzeniem .exe, lecz równie często w załącznikach podających się jako pliki graficzne, muzyczne lub wideo umieszczane są skrypty .vbs. Przy otwieraniu załączników zaleca się zachowanie szczególnej ostrożności. W przypadku wątpliwości zawsze można spytać nadawcę wiadomości czy faktycznie wysłał danego maila. W sekcji Rozszerzenia plików wymień typy plików, dla których chcesz zastosować filtr. Najlepiej ustawić filtr dla plików wykonywalnych .exe oraz .com. Jeśli chcesz zatrzymywać duże wiadomości na poziomie filtra załączników, zdefiniuj typowe rozszerzenia plików graficznych (.mpeg, .avi, .mp3, . jpeg, .jpg, .gif) lub archiwów (.zip, .rar, .cab). Poszczególne maski rozszerzeń oddzielaj średnikami, np. *.exe; *.dll. Jeśli chcesz filtrować również wiadomości przesyłane w postaci załącznika do innej wiadomości, zaznacz opcję Filtruj także załączone wiadomości. Użycie opcji Zmień nazwy załączników spowoduje, że program będzie zmieniać nazwy załączników, zamiast je usuwać. Można to zastosować np. w stosunku do plików wykonywalnych (.exe, .com), ale także do plików pakietu Microsoft Office, które mogą zawierać wykonywalne skrypty lub makra. Dzięki

prostej zmianie nazwy załącznika można uniknąć infekcji wirusa, do której wystarczy uruchomienie podglądu wiadomości zawierającej złośliwy skrypt. Jeśli opcja nie zostanie włączona, program będzie usuwać załączniki z wiadomości. W polu Przyrostek wpisz tekst, który program będzie dołączał do nazwy załącznika (np. *.exe.danger). Umożliwi to łatwą identyfikację podejrzanych wiadomości, a także przenoszenie ich do konkretnego folderu np. za pomocą reguł programu pocztowego. Opcja Dodaj komunikat w treści wiadomości pozwala na powiadomienie odbiorcy odfiltrowanej wiadomości o usunięciu lub zmianie nazwy załącznika.

- **Filtr treści:** Moduł filtrowania treści pozwala na blokowanie maili zawierających w temacie lub treści konkretne wyrazy lub ciągi znaków. W sekcji Kryterium wyszukiwania zdefiniuj słowa kluczowe i wyrazy, na które program G Data AntiSpam ma reagować. Wyrażenia można łączyć dowolnie za pomocą operatorów logicznych I oraz LUB. W sekcji Sprawdź, wskaż obszary wiadomości, które mają być sprawdzane. Nagłówek zawiera adres nadawcy, odbiorcy, wiersz tematu, informacje o użytym programie pocztowym i protokołach. Obszar Temat zawiera jedynie temat wiadomości. Treść wiadomości to sam tekst wiadomości a Tekst HTML to kod HTML w wiadomościach wysyłanych w tymże formacie. Włączenie opcji Wiadomości w załączniku spowoduje sprawdzanie także wiadomości przesyłanych w postaci załącznika. W sekcji Reakcja można ustalić procedurę postępowania w przypadku rozpoznania spamu. Opcja Odrzuć wiadomość spowoduje, że mail nie zostanie odebrany przez program pocztowy. Aby dołączyć do wiadomości komunikat (np. SPAM lub UWAGA) zaznacz opcję Dołącz komunikat do tematu wiadomości. Można też ustawić dołączanie komunikatu do treści wiadomości (Komunikat w treści). Jeśli używasz programu Microsoft Office Outlook (nie mylić z Outlook Express), program G Data AntiSpam może przenosić niechciane i podejrzane wiadomości do zdefiniowanego folderu w skrzynce pocztowej (Przesuń wiadomość do folderu). Folder można założyć bezpośrednio z programu, wpisując nazwę w polu Nazwa folderu.

Operator logiczny I wymaga aby obecne były wszystkie elementy (koniunkcja) natomiast operator LUB zakłada obecność przynajmniej jednego elementu (alternatywa).

- **Filtr nadawców:** Dzięki tej opcji można blokować wiadomości pochodzące od konkretnych nadawców lub całych domen. W polu Adresy/ domeny wpisz adresy domen i nadawców od których nie chcesz otrzymywać wiadomości. Poszczególne adresy oddziel średnikami. W sekcji Reakcja można ustalić procedurę postępowania w przypadku rozpoznania spamu. Opcja Odrzuć wiadomość spowoduje, że mail nie zostanie odebrany przez program pocztowy. Aby dołączyć do wiadomości komunikat (np. SPAM lub UWAGA) zaznacz opcję Dołącz komunikat do

tematu wiadomości. Można też ustawić dołączanie komunikatu do treści wiadomości (Komunikat w treści). Jeśli używasz programu Microsoft Office Outlook (nie mylić z Outlook Express), program G Data AntiSpam może przenosić niechciane i podejrzane wiadomości do zdefiniowanego folderu w skrzynce pocztowej (Przesuń wiadomość do folderu). Folder można założyć bezpośrednio z programu, wpisując nazwę w polu Nazwa folderu..

- **Filtr języków:** Filtr języków umożliwia ustawienie powodujące traktowanie wiadomości w danych językach jako spam. Jeżeli przykładowo dana firma nie kontaktuje się z kontrahentami w języku francuskim, można ustawić w programie oznaczanie wiadomości w tym języku jako niechcianych. Wybierz i zaznacz jeden lub więcej języków, o ile wiadomości, które odbierasz zazwyczaj nie zawierają żadnych tekstów w tych językach. W sekcji Reakcja można ustalić procedurę postępowania w przypadku rozpoznania spamu. Opcja Odrzuć wiadomość spowoduje, że mail nie zostanie odebrany przez program pocztowy. Aby dołączyć do wiadomości komunikat (np. SPAM lub UWAGA) zaznacz opcję Dołącz komunikat do tematu wiadomości. Można też ustawić dołączanie komunikatu do treści wiadomości (Komunikat w treści). Jeśli używasz programu Microsoft Office Outlook (nie mylić z Outlook Express), program G Data AntiSpam może przenosić niechciane i podejrzane wiadomości do zdefiniowanego folderu w skrzynce pocztowej (Przesuń wiadomość do folderu). Folder można założyć bezpośrednio z programu, wpisując nazwę w polu Nazwa folderu.

12.3.3 Inne

Ta zakładka zawiera dodatkowe ustawienia dotyczące kontroli kont pocztowych.

- Sprawdź nie przeczytane wiadomości przy starcie programu: Natychmiast po otwarciu programu pocztowego Microsoft Outlook sprawdzone zostaną wszystkie nieprzeczytane wiadomości (tylko Microsoft Outlook).

- Inne programy pocztowe (protokół POP3): Z przyczyn technicznych nie zawsze da się usunąć wiadomość odbieraną przez protokół POP3. Jeżeli wiadomość jest odrzucana, filtr ma możliwość zastąpić ją informacją o odrzuceniu wiadomości. Standardowy komunikat programu brzmi: Wiadomość odrzucona przez program AntiSpam. Możesz także osobiście skomponować tekst powiadomienia. Edytor tekstu rozpoznaje następujące znaki zastępcze (definiowane małymi literami poprzedzonymi znakiem %):

%s Nadawca

%u Temat

W programie pocztowym możesz ustalić regułę usuwającą wiadomości zawierające zadany tekst.

12.4 Firewall - Ustawienia

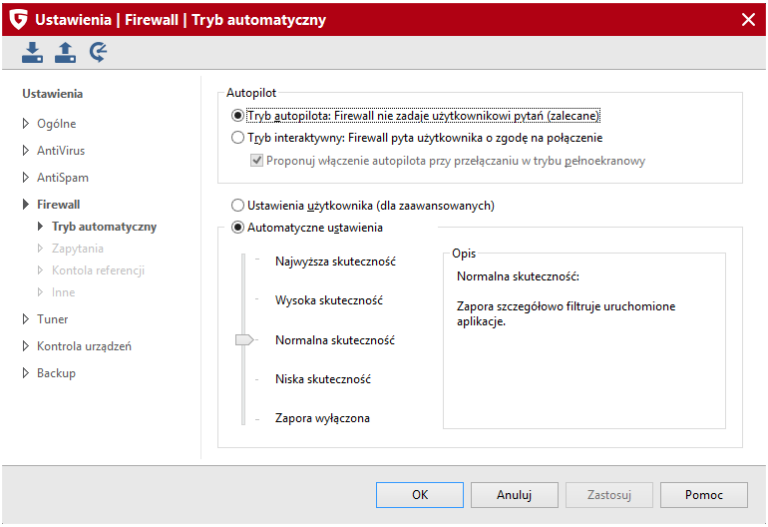
12.4.1 Tryb automatyczny

Autopilot

W tej sekcji możesz ustalić, czy zapora ma pracować automatycznie (autopilot), czy też w trybie ręcznego zatwierdzania reguł.

Tryb autopilota: Zapora działa automatycznie i nie wymaga ingerencji użytkownika. Odpowiednie reguły dostępu są tworzone automatycznie (zalecane).

Tryb interaktywny: Wyłączenie autopilota spowoduje, że zapora będzie wymagała od użytkownika potwierdzenia każdej tworzonej reguły dostępu do Internetu dla aplikacji lub usługi.



Po przełączeniu zapory w tryb ręczny dostępne będą kolejne sekcje ustawień zapory opisane w następnych rozdziałach.

Wskazówka: Poziomy zabezpieczeń umożliwiają szybką konfigurację programu bez dużego wkładu pracy.

- **Najwyższa skuteczność:** Reguły zapory są definiowane bardzo szczegółowo. To ustawienie wymaga zaawansowanej znajomości zagadnień sieciowych (TCP/IP, porty, itd.). W trybie konfiguracji zapora bardzo często wyświetla zapytania.

- **Wysoka skuteczność:** Reguły zapory są definiowane bardzo szczegółowo. To ustawienie wymaga dobrej znajomości zagadnień sieciowych (TCP/IP, porty, itd.). Zapora wyświetlać zapytania częściej niż przy ustawieniu normalnej skuteczności.

- **Normalna skuteczność:** Reguły zapory działają tylko na poziomie aplikacji. W trybie konfiguracji program wyświetla zapytania tylko w sytuacjach krytycznych dla bezpieczeństwa systemu.

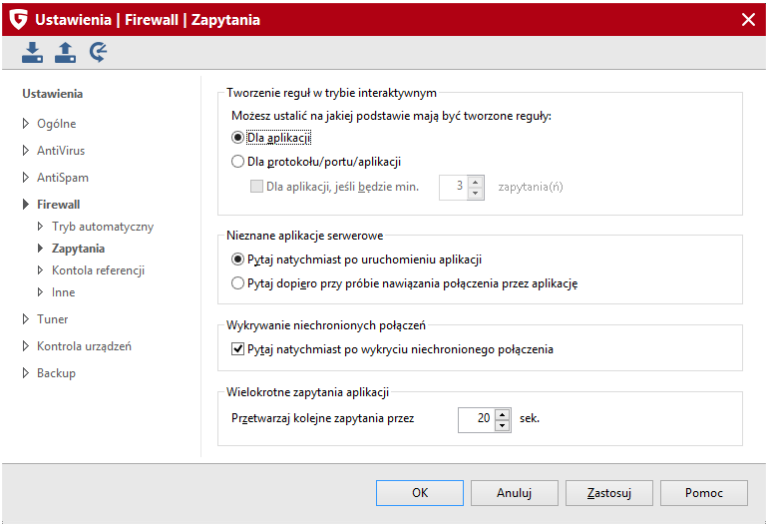
- **Niska skuteczność:** Reguły zapory działają tylko na poziomie aplikacji. W trybie konfiguracji program wyświetla zapytania tylko w sytuacjach krytycznych dla bezpieczeństwa systemu. To ustawienie zapewnia skuteczną ochronę tylko połączeń przychodzących.

- **Zapora wyłączona:** W razie potrzeby można zaporę wyłączyć. Komputer będzie wówczas nadal połączony z Internetem i inną siecią lokalną, ale zapora nie będzie filtrować połączeń ani chronić komputera przed atakami.

Aby skonfigurować zaawansowane opcje zapory wybierz Ustawienia użytkownika. Jest to zalecane tylko doświadczonym użytkownikom dysponującym wiedzą z zakresu bezpieczeństwa sieci komputerowych.

12.4.2 Zapytania

Konfiguracja generowania automatycznych zapytań przeznaczona jest dla zaawansowanych użytkowników. Zalecamy pozostawienie domyślnych ustawień.



Tworzenie reguł w trybie interaktywnym: W momencie nawiązania połączenia z siecią zapora wyświetla okno z zapytaniem. Reguła zatwierdzana przez użytkownika może być utworzona:

Dla aplikacji: Taka reguła zablokuje lub umożliwi dostęp aplikacji do sieci po każdym porcie oraz przy użyciu dowolnego protokołu (np. TCP lub UDP).

Dla protokołu/portu/aplikacji: Aplikacja, która żąda dostępu do sieci otrzymuje na to zezwolenie jedynie jeśli łączy się przy użyciu wskazanego protokołu i wyłącznie po wskazanym porcie. Jeśli ta sama aplikacja miałaby żądać dostępu do sieci w inny sposób, program wyświetli kolejne okno dialogowe umożliwiające utworzenie odpowiedniej reguły.

Nieznane aplikacje serwerowe: Aplikacje, które nie są administrowane poprzez reguły zapory, mogą być różnie traktowane. Można ustawić wyświetlanie żądania już w momencie uruchomienia danej aplikacji. Alternatywnie można zlecić wyświetlanie żądań dopiero po nawiązaniu połączenia.

Wykrywanie niechronionych połączeń: Jeśli ta opcja jest włączona, zapora będzie automatycznie wykrywać nowe połączenia sieciowe, które pojawią się w systemie operacyjnym.

Wielokrotne zapytania aplikacji: To ustawienie umożliwia zmniejszenie ilości zapytań generowanych przez instalacje, np. w przypadku niezatwierdzenia reguły.

12.4.3 Kontrola referencji

Kontrola referencji polega na wykrywaniu modyfikacji w aplikacjach dopuszczonych do komunikacji z Internetem. Program oblicza sumy kontrolne dla aplikacji na podstawie rozmiaru pliku i innych kryteriów. Jeśli suma kontrolna aplikacji nagle ulegnie zmianie, może to oznaczać ingerencję szkodliwego programu. Zapora wykryje modyfikację i zareaguje zgodnie z ustawieniami.

Kontrola referencji wczytanych modułów

Oprócz aplikacji łączących się z Internetem, program potrafi kontrolować w ten sam sposób również moduły (np. pliki .DLL) wykorzystywane przez aplikacje. Moduły często ulegają zmianie, a aplikacje potrafią wczytywać dodatkowe moduły w trakcie działania. Nadzorowanie sum kontrolnych wszystkich modułów powodowało by wyświetlanie dużej ilości komunikatów ostrzegawczych i zapytań. Z tego względu zapora umożliwia weryfikowanie tylko zmodyfikowanych modułów lub opcjonalnie zmodyfikowanych i nieznanych modułów.

12.4.4 Inne

Sekcja inne pozwala na dostosowanie następujących parametrów:

- **Ustawienia tworzenia reguł:** Możesz określić, czy tworzenie nowych reguł ma się odbywać za pomocą Asystenta tworzenia reguł 23 czy poprzez tryb zaawansowany 26. Początkującym użytkownikom zalecamy korzystanie z asystenta tworzenia reguł.

- **Wykrywanie połączeń przy uruchamianiu programu:** Program może wykrywać nieznane aplikacji serwerowe usiłujące nawiązać połączenie sieciowe. Nie zaleca się wyłączania tej opcji podczas pracy w Internecie.

- **Protokołowanie połączeń:** Możesz ustalić, jak długo zapora ma przechowywać informacje o połączeniach.

12.5 Tuner - Ustawienia

12.5.1 Ogólne

Sekcja ogólnych ustawień umożliwia zaplanowanie automatycznego usuwania niepotrzebnych danych z komputera (stare foldery tymczasowe, punkty przywracania programu Tuner oraz nieużywane skróty pulpitu.

Poniżej widoczna jest opcja uruchamiająca wyszukiwanie aktualizacji pakietu Microsoft Office podczas sprawdzania dostępności aktualizacji systemu Windows.

Opcja ma zastosowanie tylko w przypadku, kiedy na komputerze zainstalowane są produkty z pakietu Microsoft Office.

Tworzenie szczegółowych raportów można wyłączyć za pomocą opcji **Nie raportuj szczegółowo informacji o usuniętych elementach**. Użycie opcji **Usuń trwale pliki tymczasowe przeglądarek** (czyli plików cookie, tymczasowych plików internetowych) spowoduje, że nie będzie można ich przywrócić poleceniem Przywróć.

Użycie opcji **Nie zezwalaj na automatyczne ponowne uruchamianie systemu** zapobiega automatycznemu restartowaniu komputera bez ostrzeżenia po wykonaniu zlecenia optymalizacji.

Opcja **Zezwól na tworzenie pojedynczych punktów przywracania**

umożliwia cofanie konkretnych zmian wykonanych przez Tuner.

Opcja **Nie uwzględniaj rodzaju napędu podczas defragmentacji** spowoduje, że defragmentowane będą wszystkie dyski twarde, niezależnie od rodzaju. Producenci dysków SSD odradzają defragmentowanie takich nośników. Jeśli dysponujesz dyskiem SSD, możesz wyłączyć tę opcję.

12.5.2 Ustawienia

Widok Ustawienia umożliwia szczegółowy wybór czynności wykonywanych podczas optymalizacji systemu. Ustawienia dotyczą zarówno ręcznych jak i automatycznych procesów optymalizacji. Opcje podzielone są na 3 sekcje

- Skuteczność: Zróżnicowane funkcje umożliwiające automatyczne pobieranie danych z Internetu mają duży wpływ na bezpieczeństwo systemu. Optymalizacja ustawień zebranych w tej sekcji pomaga chronić system przed atakami z zewnątrz i dbać o aktualność systemu operacyjnego.

- Wydajność: Pliki tymczasowe, niepotrzebne kopie zapasowe, raporty i nieużywane pliki instalacyjne zajmują miejsce na dysku i potrafią spowalniać działanie systemu. Opcje sekcji Wydajność pomagają w automatycznym usuwaniu niepotrzebnych zasobów z systemu.

- Ochrona danych: Zestaw narzędzi do usuwania śladów po aktywności użytkownika w Internecie pomaga chronić prywatność, a także minimalizować zagrożenie utraty wrażliwych danych, np. haseł do serwisów internetowych.

12.5.3 Ochrona folderów

Zakładka Ochrona folderów służy do definiowania folderów oraz napędów pomijanych przy wyszukiwaniu plików tymczasowych.

Aby zdefiniować folder wyjątku, kliknij ten przycisk, a następnie wskaż w oknie wyboru napęd lub folder.

Aby usunąć folder z listy wyjątków zaznacz go, a następnie kliknij ten przycisk.

12.5.4 Ochrona plików

Dodanie pliku do listy plików chronionych zapobiega usunięciu pliku podczas automatycznych procesów optymalizacji systemu.

Aby dodać plik do wyjątków, kliknij ten przycisk i wpisz nazwę pliku. Dozwolone jest używanie znaków zastępczych.

Aby usunąć maskę z listy wyjątków zaznacz ją, a następnie kliknij ten przycisk.

Możesz zastosować następujące znaki zastępcze.

? Symbolizuje dowolny znak.

* Zastępuje dowolny ciąg znaków.

Przykładowo wykluczenie wszystkich plików z rozszerzeniem exe można zdefiniować stosując maskę pliku *.exe. Wyjątki dla różnych plików arkuszy kalkulacyjnych (xlr i xls) można ustawić wpisując tekst *.xl?. Jeżeli nie chcesz, żeby Strażnik skanował pliki, których nazwy rozpoczynają się od

konkretnego słowa, np. tekst,wpisz text*.*.

Kliknij ten przycisk aby ręcznie wskazać plik, który chcesz chronić przed usuwaniem.

12.5.5 Planowanie

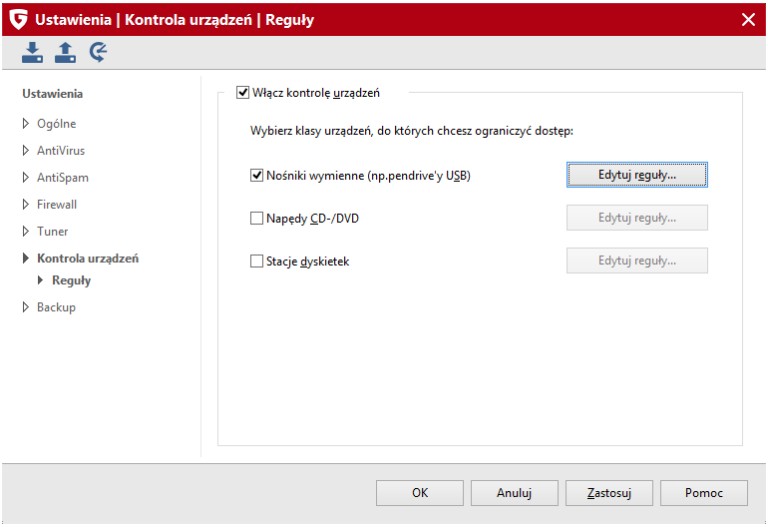
Ten widok umożliwia zaplanowanie automatycznego optymalizowania systemu zgodnie z ustawieniami.

Codzienna optymalizacja umożliwia wybór dni tygodnia wykonywania procesu. W sekcji Planowanie możesz wskazać precyzyjny czas wykonywania optymalizacji.

Możliwe jest również wyłączenie automatycznych optymalizacji poprzez usunięcie zaznaczenia w górnej części okna.

12.6 Kontrola urządzeń

Funkcjonalność kontroli urządzeń umożliwia ograniczenie użytkownikom bez praw administratora dostępu do urządzeń pamięci masowej komputera. Można blokować dostęp do napędów USB, CD/DVD oraz tradycyjnych dyskietek.



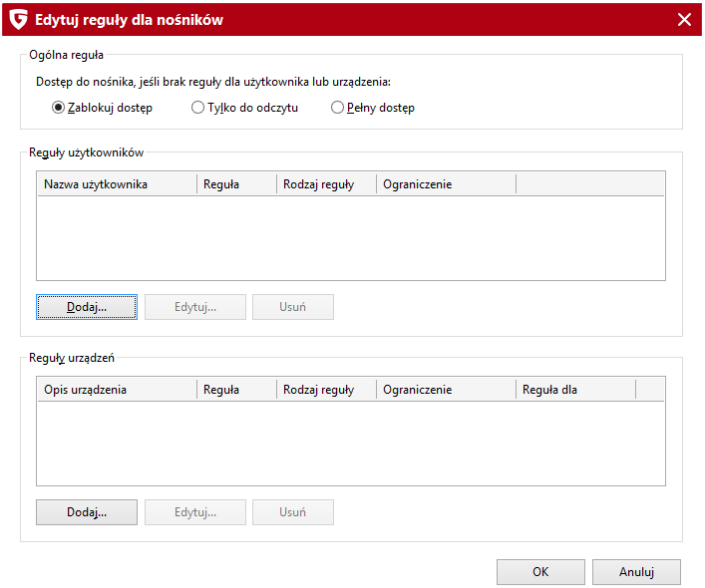
Zaznacz rodzaj urządzeń, do których dostęp chcesz kontrolować:

- Nośniki wymienne (np. pendrive'y USB)
- Napędy CD/DVD
- Stacje dyskietek

Program umożliwia zdefiniowanie szczegółowych reguł dostępu dla każdego z rodzajów urządzeń.

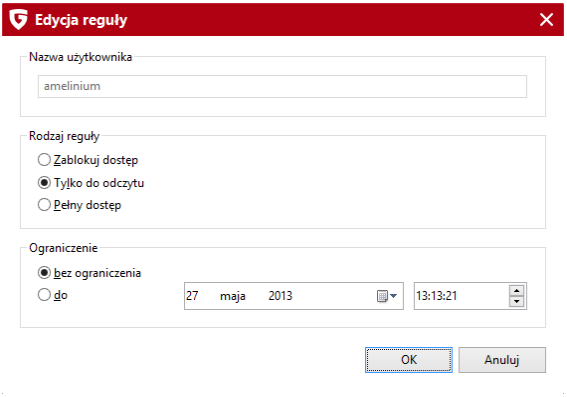
Ogólna reguła

Ta sekcja umożliwia globalne zablokowanie dostępu do urządzeń lub ograniczenie dostępu tylko do odczytu. Dotyczy to wszystkich użytkowników komputera.



Reguły użytkowników

Ta sekcja umożliwia ograniczenie dostępu do urządzeń konkretnym użytkownikom. Kliknij przycisk **Dodaj...** aby utworzyć nową regułę. Wybierz użytkownika i zatwierdź przyciskiem OK.

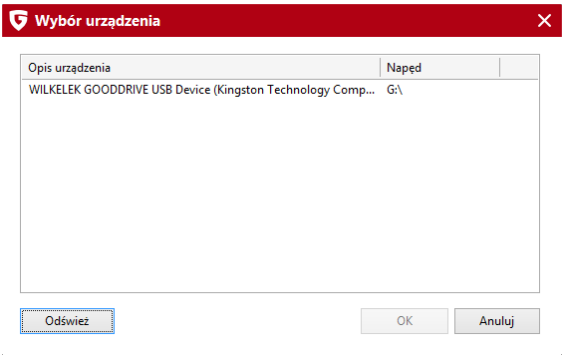


Wybierz formę kontroli i ew. ustaw ograniczenie czasowe dla reguły. Reguła automatycznie przestanie działać po przekroczeniu zadanego terminu.

Dzięki spersonalizowanym regułom masz możliwość udostępniania urządzeń tylko konkretnym użytkownikom, podczas gdy inny nie będą mieć do nich dostępu ze względu na regułę globalną.

Reguły urządzeń

Reguły urządzeń działają na zasadzie wyjątków od reguł globalnych dotyczących konkretnych urządzeń lub nośników USB.



12.6.1 Raporty kontroli urządzeń

Ten widok rejestruje wszystkie zdarzenia związane z pracą modułu kontroli urządzeń.

12.7 Backup - Ustawienia

Ta sekcja umożliwia modyfikowanie globalnych ustawień kopii zapasowych.

- **Folder plików tymczasowych:** W trakcie tworzenia lub odzyskiwania danych z kopii pliki są tymczasowo umieszczane w tym folderze. Jeśli dysponujesz ograniczoną ilością miejsca na partycji systemowej, możesz wskazać inną lokalizację klikając przycisk ....

- **Sprawdzaj, czy źródło i cel są na tym samym dysku:** Domyślnie

program ostrzega przed sporządzeniem kopii danych na tym samym dysku, na którym znajdują się oryginalne dane. Uszkodzenie lub zgubienie nośnika spowoduje w takim przypadku jednoczesne uszkodzenie lub utratę kopii zapasowej. Jeśli wyłączysz tę funkcję, program nie będzie wyświetlał ostrzeżenia.

13 Protokół

W zależności od otwartego modułu programu po kliknięciu ikony protokołu otworzy się odpowiednie okno z raportami.

13.1 Protokół - AntiVirus

Widok zawiera listę wszystkich raportów z działań modułu AntiVirus. Klikając nagłówki poszczególnych kolumn, możesz posortować je według czasu rozpoczęcia, rodzaju, tytułu lub statusu. Dostęp do okna raportów jest też możliwy poprzez ikonkę **Raporty** z prawej strony górnej części okna programu.

Aby obejrzeć raport, zaznacz jego wiersz. Zawartość raportu pojawi się w dolnej części okna. Istnieje możliwość wydrukowania lub zapisania protokołu do pliku za pomocą przycisków **Zapisz jako...** i **Drukuj...**. Dostępne formaty to ASCI (txt) oraz HTML.

Aby usunąć raport, zaznacz jego nazwę i kliknij przycisk **Usuń**. Przycisk **Usuń wszystkie** spowoduje wyczyszczenie listy raportów.

13.2 Protokół - Firewall

Widok zawiera listę wszystkich połączeń komputera z Internetem i siecią lokalną. Można sortować listę klikając nagłówki kolumn. Kliknij przycisk **Szczegóły...** aby zobaczyć szczegółowe informacje na temat przesyłanych pakietów danych.

13.3 Protokół - Backup

Widok zawiera listę raportów z czynności wykonanych przez program G Data Backup. Każdy raport zawiera informacje na temat zastosowanego rodzaju kopii zapasowej, silników antywirusowych zastosowanych do skanowania danych. Każdy raport można otworzyć podwójnym kliknięciem, a po otwarciu wydrukować lub zapisać do pliku tekstowego.

13.4 Protokół - Kontrola rodzicielska

Widok przedstawia zestawienie prób przekroczenia ustalonych uprawnień przez użytkownika wybranego z listy. Informacje można podejrzeć zaznaczając raport i klikając przycisk **Szczegóły...**. Przycisk **Usuń raporty** spowoduje usunięcie zaznaczonych pozycji.

13.5 Protokół - Kontrola urządzeń

W tym miejscu znajdziesz raporty z funkcjonowania modułu kontroli urządzeń.

14 FAQ

14.1 Skanowanie nośnikiem startowym

Dzięki płycie startowej można przeprowadzić skanowanie lokalnych napędów, wykazujące ewentualną obecność wirusa lub rootkita na dysku lub w pamięci. Skanowanie odbywa się bez udziału systemu Windows.

Płyta startowa umożliwia również przywrócenie partycji lub dysku, jeśli wcześniej sporządzona została kopia zapasowa (dostępne w pakiecie G Data TotalProtection).

W celu rozpoczęcia skanowania uruchom komputer z oryginalnej płyty z oprogramowaniem G Data Software lub z płyty startowej sporządzonej przy pomocy programu G Data.

Upewnij się, że komputer automatycznie startuje z płyty CD-ROM. Jeśli nie, zmień kolejność uruchamiania urządzeń w menu BIOS. Jako pierwsze urządzenie bootujące (1st Boot Device) należy ustawić napęd CD-ROM,

dysk twardy z systemem operacyjnym jako drugie (2nd Boot Device). Jeżeli płyta startowa znajduje się w napędzie, uruchomiona zostanie wersja programu oparta o system Linux. Jeżeli płyty nie ma w napędzie, komputer uruchomi automatycznie system Windows z dysku twardego.

Wskazówka: Niektóre płyty główne umożliwiają zmianę kolejności uruchamiania urządzeń po wciśnięciu klawisza F11, F8 lub F2. W przypadku wątpliwości dotyczących sposobu zmiany kolejności uruchamiania, zapoznaj się z dokumentacją dołączoną do płyty głównej. Po przeprowadzeniu skanowania wstępnego i zainstalowaniu programu, zaleca się przywrócenie pierwotnej kolejności uruchamiania.

1. Włóż płytę startową do napędu CD/DVD. Uruchom komputer ponownie. Komputer sam odnajdzie na i uruchomi moduł płyty startowej. Wybierz z wyświetlonego menu pożądaną metodę uruchomienia płyty startowej:

- Microsoft Windows: Jeżeli nie chcesz uruchamiać modułu skanującego, wybierz tę opcję aby uruchomić Twój system operacyjny Windows.

- Płyta startowa G Data: To polecenie uruchamia moduł płyty startowej w standardowym trybie graficznym.

- Płyta startowa G Data - tryb bezpieczny: Jeżeli standardowy moduł płyty startowej powoduje problemy z wyświetlaniem, lub Twój komputer nie obsługuje prawidłowo modułu płyty startowej, możesz wybrać uproszczony moduł płyty startowej pracujący w trybie tekstowym.

2. Wybierz pożądaną opcję przy pomocy klawiszy strzałek i wciśnij przycisk Enter.

3. Płyta startowa uruchomi się system operacyjny Linux z wbudowanym oprogramowaniem G Data Software działającym bez udziału systemu operacyjnego Windows.

4. Przeprowadź skanowanie komputera i usuń wszystkie wykryte wirusy używając opcji oferowanych przez program.

6. Uruchom komputer ponownie wybierając opcję Microsoft Windows, aby uruchomił się Twój system operacyjny.

Skanowanie wstępne przy użyciu płyty startowej to najskuteczniejsze narzędzie do wykrywania rootkitów uruchomionych w systemie.

14.2 Ikonka paska zadań

Ikona programu znajduje się w zasobniku systemowym, czyli w prawym, dolnym rogu pulpitu Windows (obok zegarka).

Tak wygląda ikonka, jeżeli wszystkie niezbędne funkcje programu są włączone.

Jeżeli któryś z kluczowych składników ochrony jest wyłączony lub nie działa prawidłowo na ikonce pojawia się znak ostrzeżenia.

Wygląd ikony podczas pobierania aktualizacji.

Dwukrotne kliknięcie ikony powoduje uruchomienie interfejsu programu. Klikając ikonę prawym klawiszem myszy otworzysz menu kontekstowe zawierające kilka podstawowych poleceń.

Menu umożliwia między innymi wyłączenie Strażnika na określony czas. Polecenie **Aktualizuj sygnatury wirusów** pozwala pobrać najnowsze sygnatury wirusów bez potrzeby uruchamiania okna programu. Z tego miejsca możesz również przejrzeć Statystyki dotyczące wykrytych wirusów, przeskanowanych wiadomości pocztowych i stron internetowych.

Jeśli Twoje oprogramowanie wyposażone jest w składnik Firewall, w menu ikony widnieją dodatkowo polecenia **Wyłącz Firewall** i **Wyłącz autopilota**.

Polecenie **Wyłącz Firewall** pozwala na czasowe wyłączenie zapory sieciowej. Po wyłączeniu zapory komputer nie jest chroniony przed atakami z Internetu. Przy pomocy tej opcji można wyłączyć zaporę maksymalnie do ponownego uruchomienia komputera.

Kliknięcie polecenia **Wyłącz autopilota** wyłącza mechanizm, który automatycznie zezwala aplikacjom na łączenie się z Internetem. Zapora przełączy się w tryb ręczny i przestanie automatycznie zezwalać programom na łączenie się z internetem.

14.3 Jak przeprowadzić skanowanie?

Skanowanie polega na porównywaniu wszystkich plików objętych skanowaniem z wzorcami wirusów (sygnaturami), którymi dysponuje program antywirusowy. Jeżeli program wykryje w pliku zgodność z jedną z sygnatur, zarejestruje ten fakt jako wykrycie wirusa.

W trakcie trwania skanowania wyświetlone jet okno skanowania.

W górnej części okna, w sekcji Postęp wyświetlane są statystyki dotyczące procesu skanowania. Pasek postępu wskazuje procent wykonania skanowania komputera. W sekcji status wyświetlana jest ścieżka dostępu oraz nazwa skanowanego w danym momencie pliku. Środkowa część okna przedstawia wyniki skanowania oraz wykryte zagrożenia.

Przycisk **Anuluj** umożliwia przerwanie skanowania w dowolnym momencie. Użycie przycisku **Wstrzymaj** powoduje tymczasowe wstrzymanie skanowania.

Zaznaczenie opcji **Wstrzymaj skanowanie na czas aktywności systemu** spowoduje wstrzymanie skanowanie w momencie wykonywania przez system innych działań. Skanowanie zostanie wznowione w momencie, kiedy komputer znów będzie bezczynny.

Opcja **Wyłącz komputer po skanowaniu** spowoduje wyłączenie komputera, jeśli skanowanie nie wykryje niebezpiecznych plików.

W sekcji Pokaż więcej możesz zdecydować czy chcesz także oglądać wyniki skanowania dotyczące archiwów, plików, do których program nie ma dostępu i archiwów zabezpieczonych hasłem.

W przypadku wykrycia wirusa program odnotuje ten fakt na liście w oknie skanowania. Po zakończeniu skanowania, można ustalić co program ma zrobić z danym zagrożeniem. Kliknij pole w kolumnie **Akcja** i wybierz z listy rozwijanej czynność, którą chcesz wykonać. Można ustalić inną akcję dla każdego wykrytego zagrożenia. Po dokonaniu wyboru kliknij przycisk **Wykonaj czynności**.

Po wykonaniu wybranych czynności odblokuje się przycisk **Zamknij**. Kliknij go, aby zamknąć okno skanowania.

14.4 Wykrycie wirusa

W przypadku wykrycia wirusa program wyświetla okno zawierające nazwę wirusa, a także lokalizację i nazwę pliku z wykrytym wirusem.

Okno umożliwia podjęcie wybranego działania. W większości przypadków najlepszym rozwiązaniem jest wybranie opcji **Przenieś do Kwarantanny**). Plik z wirusem zostanie przeniesiony do zaszyfrowanego folderu Kwarantanny. Bezpośrednie usuwanie całego pliku z wirusem może spowodować usunięcie ważnego pliku systemowego lub istotnych danych. Wybranie opcji Zablokuj dostęp do pliku spowoduje że program uniemożliwi uruchamianie i kopiowanie pliku.

Kwarantanna i skrzynki pocztowe

Nie zaleca się przenoszenia do Kwarantanny plików programów pocztowych zawierających całe skrzynki pocztowe (np *.PST, *.DBX). Po przeniesieniu plików poczty do Kwarantanny program pocztowy nie odnajdzie ich w domyślnych lokalizacjach i nie będzie w stanie wyświetlić pobranych wcześniej wiadomości, lub też przestanie działać prawidłowo.

14.5 Komunikat Firewall

Jeżeli zapora przełączona jest w tryb ręczny, przy każdej próbie połączenia się aplikacji sieciowej z siecią lokalną lub Internetem program prosi o utworzenie reguły. Okno automatycznego tworzenia reguł umożliwia podgląd szczegółów na temat danej aplikacji lub procesu. W zależności od wybranej reakcji program utworzy regułę blokującą lub akceptującą aktywność sieciową aplikacji lub procesu.

Do wybory są następujące przyciski:

- **Zawsze akceptuj:** Tworzy dla danej aplikacji (np. Opera.exe, Explorer. exe czy WINWORD.exe) regułę, która danej aplikacji na stałe zezwala na aktywność sieciową. Ta reguła znajdzie się w aktywnym zestawie reguł jako reguła generowana przez zapytanie.

- **Akceptuj teraz:** Przycisk zezwala danej aplikacji tylko jednorazowe połączenie. Przy następnej próbie dostępu do sieci, np. po ponownym uruchomieniu komputera, zapora zapyta ponownie o pozwolenie.

- **Zawsze blokuj:** Tworzy regułę dla danej aplikacji, która blokuje na stałe aktywność sieciową aplikacji. Reguła ta znajdzie się aktywnym zestawie reguł jako generowana przez zapytanie.

- **Blokuj teraz:** Przycisk zablokuje jednorazowo aktywność sieciową danej aplikacji. Przy następnej próbie dostępu do sieci, np. po ponownym uruchomieniu komputera, zapora zapyta ponownie o pozwolenie.

Kliknij przycisk **Szczegóły** aby wyświetlić dodatkowe informacje na temat protokołu, portu i adresu IP lub nazwy serwera.

14.6 Komunikat "not-a-virus"

W ten sposób oznaczane są pliki programów, które choć nie są wirusami, stanowią teoretyczne zagrożenie dla komputera. Same w sobie nie są groźnie, ale ich stosowanie może ułatwić przeprowadzenie ataku na komputer. Do takich programów należą między innymi aplikacje do zdalnego zarządzania komputerami przy pomocy protokołu VNC (RealVNC, TightVNC), aplikacje do korzystania z komunikacji IRC, serwery FTP.

Jeżeli są to świadomie używane aplikacje, nie zalecamy usuwania takich plików, ani przenoszenia ich do Kwarantanny, gdyż spowoduje to, że przestaną one funkcjonować poprawnie.

14.7 Deinstalacja programu

Najprostszą metodą usunięcia programu z systemu jest skorzystanie z polecenia Usuń w grupie programowej G Data menu Start systemu Windows. Sam proces instalacji przebiega automatycznie.

Alternatywną metodą jest deinstalacja poprzez Panel sterowania systemu Windows.

- **Windows XP:** Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Dodaj/Usuń programy. Znajdź na liście nazwę zainstalowanego produktu G Data Software, zaznacz ją myszką i kliknij przycisk Usuń.

- **Windows Vista, 7, 8:** Uruchom polecenie menu Start > Panel sterowania. W Panelu sterowania otwórz aplet Programy i funkcje. Znajdź na liście nazwę zainstalowanego produktu G Data Software, kliknij ją prawym klawiszem myszki i wybierz polecenie Usuń.

Podczas instalacji program zapyta, czy usunąć ustawienia i raporty programu. Jeżeli zamierzasz zainstalować nowszą wersję programu, pozwól na usunięcie tych elementów.

Jeśli w Kwarantannie programu znajdują się zarażone pliki, program zapyta podczas deinstalacji, czy chcesz je usunąć. Jeżeli ich nie usuniesz, będą dostępne w Kwarantannie po zainstalowaniu nowszej wersji programu G Data.

14.8 Licencje wielostanowiskowe

Licencje wielostanowiskowe umożliwiają korzystanie z jednej licencji na większej ilości komputerów. Rejestracja odbywa się tylko raz - na pierwszym komputerze. Na pozostałych stanowiskach należy wpisać dane dostępu uzyskane w potwierdzeniu rejestracji.

Rejestracji można dokonać tylko raz. Na każdym kolejnym komputerze wystarczy wpisać dane dostępu otrzymane w potwierdzeniu pierwszej rejestracji.

Nie da się zarejestrować danego numeru po raz drugi. Wpisz dane dostępu i kliknij OK, nie otwierając okna aktywacji licencji. W razie problemów, skontaktuj się z pomocą techniczną G Data 1.

14.9 Kontynuacja licencji

Na niedługo przed upłynięciem licencji na korzystanie z programu, ikonka w zasobniku systemowym pokazuje komunikat o nadchodzącym terminie upływu ważności licencji.

Kliknij dymek, jeżeli chcesz dokonać przedłużenia licencji przez sklep internetowy. Jeśli chcesz zostać przeniesiony na stronę internetową sklepu, kliknij przycisk Zamów.

Jeśli chcesz wcześniej dokonać przedłużenia lub rozszerzenia licencji na większą ilość stanowisk, skontaktuj się ze sprzedawcą lub skorzystaj ze sklepu internetowego G Data klikając przycisk Rozszerz licencję... w lewej części okna programu G Data Security.

14.10 Przeniesienie licencji

Po prostu odinstaluj program z jednego komputera i zainstaluj na drugim. Przy próbie aktualizacji program sam zapyta, czy przenieść licencję. Po przeniesieniu licencji poprzedni komputer utraci możliwość pobierania aktualizacji.

14.11 Copyright