

# **G Data ClientSecurity Business**

Podręcznik użytkownika

Wszystkie prawa zastrzeżone. Oprogramowanie oraz pisemny materiał informacyjny chronione są prawami autorskimi. Dozwolone jest wykonanie jednej kopii bezpieczeństwa oprogramowania, która nie może być udostępniania osobom trzecim.

G Data Software Spółka z ograniczoną odpowiedzialnością zastrzega sobie wszelkie prawa, a w szczególności do publikacji, powielania, edycji i korzystania z oprogramowania. Żadna część niniejszego podręcznika nie może być w żadnej formie powielana, ani przechowywana w bazach danych lub też jakichkolwiek innych systemach przechowywania danych bez pisemnej zgody wydawcy. Wyjątkiem są cytaty w artykułach recenzujących.

G Data Software Sp. z o.o. nie ponosi odpowiedzialności za szkody spowodowane użytkowaniem oprogramowania. Treść podręcznika może ulec zmianie. Aktualna pomoc znajduje się na stronie internetowej [www.gdata.pl](http://www.gdata.pl).

**ISBN 978-83-61624-09-7**

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](mailto:biuro@gdata.pl)  
Bank Zachodni WBK S.A.  
63 1090 1711 0000 0001 0987 7149

G Data Software Sp. z o.o.

# Spis treści

<b>I Wstęp</b>	<b>1</b>
1 Pomoc techniczna .....	1
2 Kontynuacja licencji .....	2
3 Ambulans G Data .....	2
4 Warunki licencji .....	3
<b>II Przed instalacją</b>	<b>6</b>
1 Wymagania programu .....	6
2 Płyta startowa .....	7
<b>III Instalacja</b>	<b>8</b>
<b>IV G Data AntiVirus ManagementServer</b>	<b>10</b>
1 Instalacja składnika ManagementServer .....	10
2 Internet Update .....	14
<b>V G Data AntiVirus Administrator</b>	<b>15</b>
1 Instalacja składnika Administrator .....	16
2 Logowanie .....	16
3 Pierwsze uruchomienie (Asystent konfiguracji) .....	17
4 Obsługa składnika Administrator .....	20
<b>VI G Data AntiVirus Klient</b>	<b>62</b>
1 Instalacja składnika G Data AntiVirus Klient .....	63
2 Instalacja składnika Klient w systemach Linux .....	63
3 Konfiguracja składnika Klient w systemach Linux .....	65
4 Ikona Klienta .....	68

**VII G Data AntiVirus WebAdministrator 72**

- 1 Instalacja składnika WebAdministrator ..... 73
- 2 Obsługa składnika WebAdministrator ..... 74

**VIII G Data Firewall 75**

- 1 Instalacja składnika Firewall ..... 76
  - 2 Obsługa składnika Firewall ..... 76
-

---

# 1 Wstęp

Rozwój usług internetowych i samego Internetu pociąga za sobą także drastyczny wzrost zagrożeń. Tematyka ochrony antywirusowej zaczyna być popularna nie tylko w gronie fachowców. Problem ten dotyczy obecnie każdego użytkownika komputera.

Ataki wirusów są najdotkliwsze dla firm i instytucji działających w oparciu o wewnętrzne sieci komputerowe połączone z Internetem. Skutki mogą być rozmaite: utrata danych, zawieszanie systemów operacyjnych, czasem wręcz utrata kluczowych kanałów komunikacyjnych. Wirusy są w stanie wyrządzić szkody, których czasem nie da się naprawić. Oprogramowanie oferuje wysokiej klasy ochronę przed wirusami. W testach wykrywalności produkt od lat zajmuje czołowe miejsca.

Działanie programu nastawione jest konsekwentnie na centralną konfigurację i zarządzanie oraz szeroko pojętą automatyzację ochrony. Procesy przebiegają w tle, a użytkownicy nie mogą wyłączyć ochrony bez zgody administratora. Automatyczne aktualizacje internetowe umożliwiają opanowanie infekcji najnowszych wirusów. Zdalne sterowanie przy pomocy modułu G Data AntiVirus ManagementServer umożliwia instalację, konfigurację, aktualizację oraz automatyzację ochrony sieci. Wielokrotnie nagradzany moduł Firewall chroni stacje robocze przed atakami z zewnątrz i kontroluje ruch sieciowy.

G Data Software

## 1.1 Pomoc techniczna

Pomoc techniczna przysługuje wszystkim zarejestrowanym użytkownikom przez rok czasu od rejestracji programu lub wykupienia abonamentu. Zgłoszenia problemów z programem przyjmujemy telefonicznie, pocztą elektroniczną i faksem.

telefon:	094 3729 650
----------	--------------

e-mail:	helpdesk@gdata.pl
---------	-------------------

W rozwiązaniu wielu problemów pomoże konfrontacja z tekstami pomocy lub podręcznikiem, prosimy więc najpierw tam poszukać odpowiedzi na pytania. Wiele odpowiedzi można znaleźć na stronie pomocy technicznej:

<http://www.gdata.pl>.

Przed rozmową prosimy o przygotowanie danych na temat sieci i komputerów ze zwróceniem szczególnej uwagi na:

- numery wersji modułów G Data AntiVirus ManagementServer i G Data AntiVirus Klient,
- Numer Klienta otrzymany w potwierdzeniu rejestracji,
- wersje systemów operacyjnych,
- dodatkowo zainstalowane oprogramowanie i sprzęt.

Przygotowanie powyższych informacji ułatwi i przyspieszy korespondencję lub rozmowę z serwisantem.

## 1.2 Kontynuacja licencji

W momencie zarejestrowania zakupionej licencji otrzymujesz prawo do korzystania z aktualizacji sygnatur wirusów i plików produktu, jak i z usługi pomocy technicznej w odniesieniu do używanego oprogramowania przez okres jednego roku, lub dłuższy, w zależności od wniesionej opłaty licencyjnej. W każdej chwili możesz dokonać przedłużenia wykupionej licencji kontaktując się z nami:

telefon: 094 3729 650

W sprawach problemów technicznych zapraszamy do kontaktu z działem pomocy technicznej. Patrz rozdział Pomoc techniczna.

## 1.3 Ambulans G Data

Program G Data AntiVirus ManagementServer ma możliwość wysyłania wykrytych wirusów drogą poczty elektronicznej do Ambulansu G Data. Gwarantujemy pełną dyskrecję i przestrzeganie zasad przechowywania danych osobowych dotyczących przesyłanych plików.

---

Przed wysłaniem pliku niezbędne jest skonfigurowanie ustawień poczty elektronicznej. Szczegółowy opis znajdziesz w rozdziale Ustawienia e-mail.

## 1.4 Warunki licencji

G Data Software Sp. z o.o.

Ogólne warunki użytkowania programu G Data ClientSecurity Business.

### 1. Przedmiot umowy

Przedmiotem umowy zawartej między firmą G Data Software Sp. z o.o., zwaną dalej Producentem, a Użytkownikiem jest program G Data ClientSecurity Business zwany dalej Oprogramowaniem. Producent dostarcza Użytkownikowi Oprogramowanie na nośniku danych lub w postaci pliku pobranego ze strony internetowej Producenta. Producent zwraca uwagę na fakt, że technicznie nie jest możliwe wyprodukowanie Oprogramowania współpracującego bezbłędnie z wszystkimi aplikacjami i z każdą kombinacją sprzętowo-programową.

### 2. Zakres stosowania

Użytkownik otrzymuje proste, niewyłączne i osobiste prawo, zwane dalej Licencją, do używania Oprogramowania na każdym kompatybilnym komputerze pod warunkiem, że Oprogramowanie będzie użytkowane na nie większej niż uzgodniona z Producentem ilości komputerów, maszyn wirtualnych lub sesji terminali. Jeżeli z komputera korzysta więcej niż jedna osoba, Licencja obejmuje wszystkie osoby korzystające z komputera. Użytkownik ma prawo przenieść Oprogramowania z jednego komputera na drugi, przy zachowaniu uzgodnionej z Producentem maksymalnej ilości komputerów.

### 3. Szczególne ograniczenia

Użytkownik nie może modyfikować Oprogramowania bez pisemnej zgody Producenta.

### 4. Prawo własności

Zakupując Oprogramowanie Użytkownik nabywa prawo własności do

nośnika z zapisanym Oprogramowaniem, a także czasowe prawo do otrzymywania aktualizacji i pomocy technicznej. Zakup Oprogramowania nie wiąże się z zakupem praw do Oprogramowania. Producent zastrzega sobie w szczególności wszystkie prawa do publikowania, powielania, modyfikacji i eksploatacji Oprogramowania.

#### 5. Powielanie

Oprogramowanie i dokumentacja pisemna chronione są prawem autorskim. Dozwolone jest sporządzenie jednej kopii bezpieczeństwa Oprogramowania; kopia nie może zostać przekazana osobom trzecim.

#### 6. Czas trwania umowy

Umowa zostaje zawarta na czas nieokreślony. Czas trwania umowy nie obejmuje prawa do otrzymywania aktualizacji i pomocy technicznej. Prawo do użytkowania Oprogramowania wygasa automatycznie bez okresu wypowiedzenia w momencie złamania przez Użytkownika któregokolwiek z postanowień tej umowy. Wraz z wygaśnięciem umowy Użytkownik jest zobowiązany do zniszczenia oryginalnego nośnika z Oprogramowaniem oraz dokumentacji pisemnej.

#### 7. Złamanie warunków umowy

Użytkownik ponosi odpowiedzialność za wszystkie szkody poniesione przez Producenta w związku z naruszeniem praw autorskich, wynikłe ze złamania warunków tej umowy.

#### 8. Zmiany i aktualizacje

Obie strony obowiązują najnowsza wersja tej umowy. Warunki umowy mogą ulec zmianie w każdej chwili, bez powiadamiania Użytkownika i podawania przyczyn.

#### 9. Gwarancja i odpowiedzialność Producenta:

a) Producent gwarantuje, że w momencie przekazania Oprogramowania pierwotnemu Użytkownikowi, jest ono pozbawione błędów i zdadne do użytku w myśl dołączonej specyfikacji programu.

b) W przypadku stwierdzenia wady nośnika lub pobranego pliku, Użytkownik zobowiązany jest do zgłoszenia reklamacji wraz z dowodem zakupu w terminie do sześciu miesięcy od dnia zakupu.

c) Z przyczyn podanych w punkcie 1. Producent nie gwarantuje

---

bezbłądności Oprogramowania, w szczególności w przypadku niespełnienia przez Oprogramowanie wymogów i oczekiwań użytkownika lub niekompatybilności z wybranymi aplikacjami oraz systemami operacyjnymi. Skutki decyzji zakupu i wyniku zamierzonego oraz niezamierzonego działania Oprogramowania ponosi Użytkownik. Zapis odnosi się również do dołączonej dokumentacji pisemnej. Jeśli Oprogramowanie nie jest zdatne do użytku w myśl punktu 1., Użytkownikowi przysługuje prawo odstąpienia od umowy. Takie samo prawo przysługuje Producentowi, jeżeli wyprodukowanie Oprogramowania użytecznego w myśl punktu 1. nie jest możliwe.

d) Producent odpowiada tylko za szkody spowodowane umyślnie lub przez rażące zaniechanie ze strony Producenta. Sprzedawca Oprogramowania nie odpowiada także za szkody spowodowane umyślnie lub przez rażące zaniechanie sprzedawcy. Maksymalna kwota odszkodowania równa jest kwocie poniesionej przez Użytkownika na zakupienie Oprogramowania.

## 10. Właściwość sądu

Sądem właściwym dla wszystkich kwestii spornych wynikających bezpośrednio lub pośrednio z warunków umowy jest sąd odpowiedni dla siedziby Producenta.

## 11. Postanowienia końcowe

Unieważnienie tylko niektórych postanowień tej umowy, nie pociąga za sobą unieważnienia pozostałych postanowień. W miejsce unieważnionego postanowienia stosowane jest inne, aktualne postanowienie o najbardziej zbliżonym celu gospodarczym.

Instalując Oprogramowanie Użytkownik akceptuje powyższe warunki licencji. Akceptując warunki licencji użytkownik zgadza się na przetwarzanie danych osobowych przez Producenta.

Copyright © 2009 G Data Software AG

Skaner A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2009 BitDefender SRL.

Skaner B: © 2009 Alwil Software

OutbreakShield: © 2009 Commtouch Software Ltd.

## 2 Przed instalacją

- Przed zainstalowaniem programu należy zweryfikować sprzętowe i programowe zabezpieczenia sieci i komputerów. Szczególnie ważne jest uaktualnienie wszystkich systemów operacyjnych w sieci. Jeśli istnieje podejrzenie, że dany komputer jest zainfekowany, warto rozważyć przeprowadzenie skanowania wstępnego przy użyciu startowej płyty z programem.
- Pierwszy krok to instalacja składnika ManagementServer. Jest to możliwe w systemach operacyjnych Windows XP SP2/Vista/2003 Server/Server 2008. Ten składnik zdalnie steruje ochroną stacji roboczych i przekazuje im sygnatury wirusów pobierane przez Internet z serwera aktualizacji. Razem z nim instaluje się automatycznie składnik Administrator, interfejs graficzny obsługi składnika ManagementServer.
- Po zainstalowaniu serwera zarządzającego przeprowadź rejestrację online. Zarejestrowanie produktu online umożliwia pobieranie aktualizacji oprogramowania i sygnatur wirusów przez Internet.
- Pierwsze uruchomienie składnika Administrator na komputerze z zainstalowanym składnikiem ManagementServer odbywa się pod nadzorem asystenta konfiguracji. Asystent umożliwia zainstalowanie oprogramowania Klienta na stacjach roboczych sieci, a także konfigurację podstawowych ustawień ochrony.

### 2.1 Wymagania programu

Program działa prawidłowo na komputerach o następującej konfiguracji:

Klient

- System Windows Vista, Windows XP SP2, Windows 2000, Windows Server 2008, Windows 2003 Server (także wersje 64-bit)
- 128 MB RAM

Serwer

- System Windows Vista, Windows XP SP2, Windows Server 2008, Windows 2003 Server (także wersje 64-bit)
-

- 256 MB RAM
- Platforma Microsoft.NET Framework 3.5

Oprogramowanie wykorzystuje protokół TCP/IP do komunikowania stacji roboczych z serwerem oraz do łączenia z Internetem w celu uaktualniania baz wirusów i plików programu.

Istnieje możliwość zainstalowania specjalnej wersji Klienta na stacjach roboczych z systemem Linux, a także na komputerach z systemem Linux udostępniających udziały komputerom z systemem Windows przy użyciu serwera plików Samba poprzez protokół SMB.

## 2.2 Płyta startowa

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

W tym celu należy uruchomić komputer z oryginalnej płyty CD/DVD z programem lub z płyty startowej sporządzonej przez moduł Kreator płyt startowych.

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

- Włóż płytę z programem do napędu CD/DVD-ROM.

- Wyłącz komputer na około 5 sekund. Istnieją wirusy, które są w stanie przetrwać tzw. miękki reset komputera (CTRL+ALT+DEL).
- Uruchom komputer. Komputer sam odnajdzie na płycie startowej moduł skanujący oparty na systemie Linux.

Wskazówka: Skanowanie wstępne odbywa się przy pomocy specjalnego modułu antywirusowego opartego na systemie operacyjnym Linux.

- Usuń wszystkie znalezione wirusy używając opcji oferowanych przez program.
- Po zakończeniu skanowania uruchom komputer ponownie z dysku twardego wybierając przycisk Zakończ.

Jak utworzyć płytę startową?

Możesz sporządzić płytę startową z aktualnymi bazami wirusów przy pomocy modułu Kreator płyt startowych. Moduł należy zainstalować z płyty instalacyjnej z zakupionym programem. Program nagra na płytę bazy wirusów jakimi w danej chwili dysponuje program zainstalowany na komputerze.

Do przeprowadzenia skanowania wstępnego nie jest potrzebny zainstalowany program. Po uruchomieniu komputera z płyty startowej uruchomi się osobny system operacyjny, w którym zostanie przeprowadzone skanowanie lokalnych dysków.

Do utworzenia płyty startowej potrzebna jest czysta płyta.

## 3 Instalacja

Instalacja wszystkich modułów programu jest prosta nawet dla początkujących administratorów. W uruchomionym systemie Windows włóż do napędu płytkę z zakupionym programem. Okno instalacyjne otworzy się automatycznie.

Uwaga: Przed zainstalowaniem programu należy zweryfikować sprzętowe i programowe zabezpieczenia sieci i komputerów. Szczególnie ważne jest uaktualnienie wszystkich systemów operacyjnych w sieci.

Przed zainstalowaniem składników zamknij wszystkie inne aplikacje systemu Windows.

---

Wskazówka: Jeśli funkcja autostartu napędu CD/DVD-ROM nie jest aktywna, instalacja nie rozpocznie się automatycznie. W takim przypadku można uruchomić instalator np. klikając dwukrotnie ikonę napędu CD/DVD-ROM w oknie Mój komputer.

Wybierz w oknie instalacji element, który chcesz zainstalować na tym komputerze:

- **G Data AntiVirus ManagementServer:** Pierwszy krok to instalacja składnika ManagementServer. Jest to możliwe w systemach operacyjnych Windows XP SP2/Vista/2003 Server/Server 2008. Ten składnik zdalnie steruje ochroną stacji roboczych i przekazuje im sygnatury wirusów pobierane przez Internet z serwera aktualizacji. Razem z nim instaluje się automatycznie składnik Administrator, interfejs graficzny obsługi składnika ManagementServer.
- **G Data AntiVirus Administrator:** Jest to moduł sterujący modulem ManagementServer. Osoba znająca hasło dostępu może uruchomić program z każdej stacji roboczej.
- **G Data AntiVirus Klient:** Jest to oprogramowanie chroniące stacje robocze i wykonujące zadania składnika ManagementServer.
- **Kreator płyt startowych:** Aplikacja umożliwiająca tworzenie startowych płyt CD służących do wstępnego skanowania dysków komputera. Szczegóły w rozdziale Płyta startowa.
- **G Data AntiVirus WebAdministrator:** Aplikacja umożliwiająca sterowanie modulem ManagementServer przez przeglądarkę internetową.
- **G Data Firewall:** Zdalnie instalowana aplikacja chroniąca połączenia przychodzące i wychodzące stacji roboczej. Blokuję ataki sieciowe i umożliwi ukrywanie adresu IP komputera. Ręczna instalacja tego składnika wymaga uprzedniego zainstalowania składnika G Data AntiVirus Klient.

Szczegóły na temat instalacji poszczególnych składników znajdziesz w kolejnych rozdziałach.

## 4 G Data AntiVirus ManagementServer

G Data AntiVirus ManagementServer to serce całego systemu ochrony. Serwer pobiera aktualizacje i przekazuje je automatycznie na stacje robocze. Służy do sterowania ochroną antywirusową w sieci. Serwer zarządzający komunikuje się ze stacjami roboczymi używając protokołu TCP/IP. Dla mobilnych stacji roboczych, którzy są często odłączeni od sieci zadania są gromadzone i synchronizowane podczas kolejnej sesji online. Serwer zarządza też centralnym katalogiem Kwarantanny. Pliki Kwarantanny przechowywane są w postaci zaszyfrowanej. Moduł Administrator umożliwia wysłanie plików do Ambulansu G Data za pomocą poczty elektronicznej. Składnikiem G Data AntiVirus ManagementServer administruje się za pomocą modułu Administrator.

Zamknięcie modułu Administrator nie powoduje wyłączenia składnika ManagementServer. Pozostaje on aktywny w tle i steruje ochroną stacji roboczych.

### 4.1 Instalacja składnika ManagementServer



Do zainstalowania składnika ManagementServer wymagany jest system operacyjny Windows Vista, XP, Server 2008 lub 2003 Server. Włóż do napędu płytę z zakupionym oprogramowaniem lub uruchom plik instalacyjny pobrany przez Internet. W celu rozpoczęcia instalacji kliknij przycisk Instaluj w menu automatycznego startu.

#### 4.1.1 Powitanie

Okno powitalne informuje, że zamierzasz zainstalować w systemie operacyjnym składnik ManagementServer. Najpóźniej teraz zamknij wszystkie aplikacje systemu Windows. Kliknij przycisk Dalej aby kontynuować instalację.

---

## 4.1.2 Warunki licencji

Zapoznaj się z warunkami korzystania z oprogramowania. Jeżeli akceptujesz warunki licencji, zaznacz odpowiednie pole i kliknij przycisk **Dalej**.

## 4.1.3 Folder docelowy

Kolejne okno umożliwia wybór docelowego folderu instalacji składnika **ManagementServer**. Jeśli nie chcesz zainstalować programu w domyślnej lokalizacji, kliknij przycisk **Zmień** aby wskazać wybrany folder.

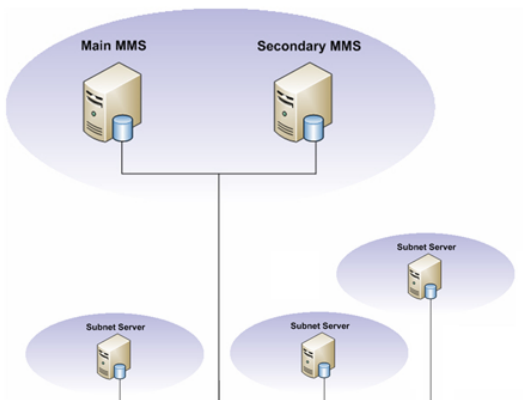
## 4.1.4 Rodzaj serwera

Do wyboru masz trzy rodzaje instalacji składnika ManagementServer:

- **Serwer główny:** W przypadku pierwszej instalacji tego składnika należy zainstalować go jako serwer główny. Będzie to centralna instancja konfiguracyjna i zarządzająca sieciowej architektury ochrony antywirusowej. Wszystkie pozostałe serwery, zarówno zapasowe, jak i podrzędne korzystają z bazy danych serwera głównego.
- **Serwer zapasowy:** W przypadku zastosowania bazy danych typu SQL, program umożliwia zainstalowanie drugiej, awaryjnej instancji serwera. W razie awarii serwera głównego lub segmentu sieci zawierającego serwer główny, stacje robocze łączą się automatycznie i synchronizują z serwerem zapasowym. W momencie przywrócenia działania serwera głównego, stacje znów się z nim łączą. Serwer zapasowy tworzą osobne repozytorium baz wirusów.
- **Serwer podrzędny:** W przypadku dużych sieci, warto rozważyć zainstalowanie serwerów podrzędnych w mniejszych segmentach lub podsieciach. Spowoduje to rozłożenie obciążenia sieci powodowanego przez użytkowanie oprogramowania. Do danego serwera podrzędnego można przyporządkować konkretne stacje robocze w celu odciążenia serwera głównego. Serwery podrzędne pozostają w pełni funkcjonalne nawet w momencie, kiedy serwer główny i serwer zapasowy nie są dostępne.

Dzięki wprowadzeniu hierarchizacji serwerów, można dostosować architekturę ochrony do logicznej topografii sieci. Serwery podrzędne mogą

grupować stacje robocze w podsieciach i synchronizować ustawienia i aktualizacje z serwerem głównym. W razie awarii lub potrzeby konserwacji serwera głównego, jego funkcję przejmuje automatycznie serwer zapasowy.



### 4.1.5 Rodzaj bazy danych

Wybierz rodzaj bazy danych, w której chcesz przechowywać ustawienia składnika ManagementServer. Możesz podłączyć się do istniejącej w sieci instancji serwera SQL, zainstalować bazę Microsoft SQL Express, lub zastosować zintegrowaną bazę danych (np. dla mniejszych sieci).

Do zainstalowania serwera zarządzającego nie jest wymagany typowo serwerowy system operacyjny. Zalecamy stosowanie baz danych opartych o język SQL dla sieci powyżej 50 stacji roboczych.

W przypadku instalacji bazy Microsoft SQL Express, istniejąca starsza baza ustawień zostanie automatycznie przekonwertowana.

---

### 4.1.6 Nazwa komputera

Sprawdź poprawność nazwy komputera, na którym instalujesz składnik ManagementServer. Ta nazwa będzie stosowana do komunikacji między serwerem, a stacjami roboczymi. Jeśli automatycznie podstawiona nazwa nie jest prawidłowa, popraw ją i kliknij przycisk Dalej.

### 4.1.7 Rozpoczęcie instalacji

Teraz rozpocznie się instalacja składnika ManagementServer. Kliknij przycisk Instaluj.

### 4.1.8 Rejestracja online

Najpóźniej przed przeprowadzeniem pierwszej aktualizacji programu, należy zarejestrować produkt przez Internet. Jeżeli produkt został zarejestrowany wcześniej, rejestracja nie jest potrzebna.

Możesz zarejestrować produkt pod koniec instalacji, lub później uruchamiając program Start > (Wszystkie) programy > G Data Software > G Data AntiVirus Business > Internet Update i klikając przycisk Rejestracja online.

Do rejestracji potrzebny jest klucz rejestracyjny, który znajduje się w opakowaniu programu, lub w wiadomości z realizacją zamówienia w przypadku zakupu online.

Do poprawnego przeprowadzenia rejestracji niezbędne jest połączenie z Internetem.

Wprowadź numer rejestracyjny produktu i wypełnij wszystkie pola oznaczone gwiazdką. Wpisz aktualny adres e-mail. Na ten adres wysłane zostanie potwierdzenie rejestracji oraz numer klienta uprawniający do korzystania z pomocy technicznej przez okres 1 roku.

Bezpośrednio po zarejestrowaniu produktu pojawi się okno informacyjne zawierające dane dostępu do aktualizacji (użytkownik i hasło).

Uwaga: Na wszelki wypadek zapisz dane dostępu do aktualizacji i przechowuj w bezpiecznym miejscu. Mogą być przydatne w przypadku ponownej instalacji oprogramowania lub systemu operacyjnego.

Aktualizacje można przeprowadzać bezpośrednio z okna składnika Administrator. Możliwe jest także skonfigurowanie dowolnych schematów automatycznych aktualizacji.

### 4.1.9 Konfiguracja bazy danych

Zmiana tych ustawień niezbędna jest tylko wtedy, gdy jest to ponowna instalacja składnika ManagementServer, lub jeśli na komputerze zainstalowana jest jeszcze inna instancja bazy SQL. W przypadku standardowych ustawień lub pierwszej instalacji serwera zarządzającego po prostu kliknij przycisk Zamknij.

### 4.1.10 Zakończenie instalacji

Po zainstalowaniu usługa systemowa G Data ManagementServer będzie uruchamiać się automatycznie przy każdym uruchomieniu komputera. Aby dokonać zmian w ustawieniach programu G Data AntiVirus ManagementServer, uruchom składnik Administrator poleceniem menu Start > (Wszystkie) Programy > Admin > G Data AntiVirus ManagementServer > G Data AntiVirus Administrator.

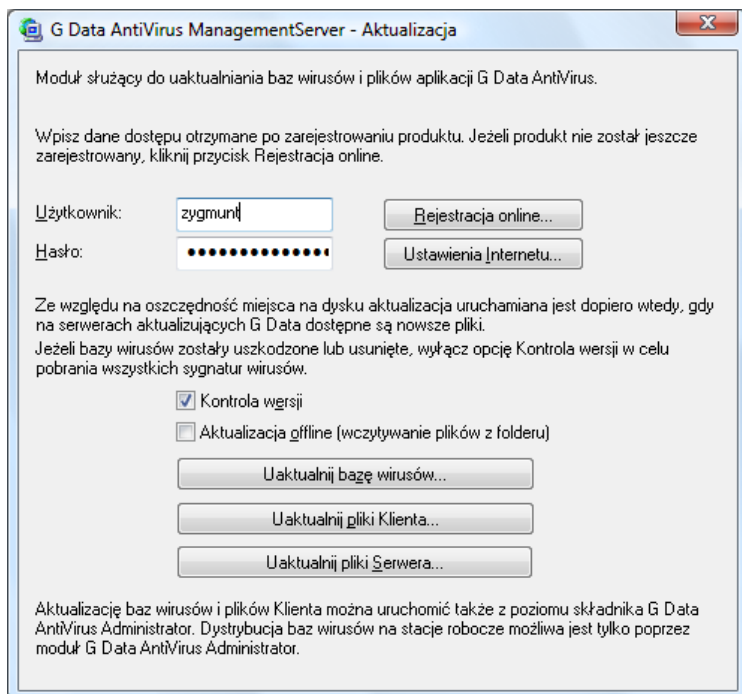
## 4.2 Internet Update

Aplikacja Internet Update umożliwia uaktualnienie sygnatur wirusów i plików składnika Klient w repozytorium serwera zarządzającego oraz w szczególności aktualizację samego składnika ManagementServer.

Składnik ManagementServer, nie aktualizuje się automatycznie. Aby uaktualnić pliki serwera zarządzającego uruchom polecenie menu Start > (Wszystkie) programy > G Data AntiVirus ManagementServer > Internet

---

Update i wciśnij przycisk Aktualizuj pliki Serwera.



Uwaga: Jest to jedyna metoda aktualizacji plików serwera zarządzającego.

## 5 G Data AntiVirus Administrator

Składnik Administrator to graficzny interfejs obsługi składnika ManagementServer. Instaluje się automatycznie podczas instalacji składnika ManagementServer. Umożliwia sterowanie procesami zdalnych instalacji i aktualizacji oprogramowania klienckiego na stacjach roboczych, a także planowanie procesów aktualizacji i skanowania. Z poziomu okna Administratora można modyfikować ustawienia ochrony stacji roboczych.

## 5.1 Instalacja składnika Administrator



Administrator instaluje się automatycznie podczas instalacji składnika ManagementServer. Nie jest wymagana dodatkowa ręczna instalacja Administratora. Aby zainstalować ręcznie moduł administrujący na końcówce sieci, włóż do napędu końcówki płytę z programem i uruchom instalację składnika Administrator.

Przed rozpoczęciem instalacji zamknij wszystkie aplikacje Windows.

Składnik Administrator uruchamia się poleceniem menu Start > (Wszystkie) Programy > Admin > G Data AntiVirus ManagementServer > G Data AntiVirus Administrator.

## 5.2 Logowanie

Po uruchomieniu składnika G Data AntiVirus Administrator program zapyta o nazwę (adres IP) serwera, metodę uwierzytelniania, użytkownika oraz hasło. Wpisz w polu Serwer nazwę lub adres IP komputera z zainstalowanym składnikiem G Data AntiVirus ManagementServer.

Logowanie

Serwer: SBS\_2003

Uwierzytelnianie: Uwierzytelnianie Windows

Użytkownik: Administrator

Hasło: ●●●●●●●●●●●●

OK Anuluj Pomoc

Następnie wybierz metodę uwierzytelniania:

Uwierzytelnianie Windows

Ta metoda uwierzytelniania pozwala na zalogowanie się do składnika

---

---

G Data AntiVirus Administrator przy pomocy poświadczeń konta administratora systemu Windows.

### Zintegrowanie uwierzytelnianie

Ta metoda umożliwia utworzenie wbudowanych kont użytkowników programu G Data AntiVirus Administrator. Możliwe jest utworzenie konta bez uprawnień do modyfikacji ustawień programu. Tworzenie i modyfikowanie kont użytkowników możliwe jest dzięki poleceniu Zarządzanie użytkownikami w menu Plik.

Uwaga: Pierwsze logowanie do składnika Administrator musi odbyć się przy zastosowaniu uwierzytelniania Windows, ponieważ w bazie ustawień oprogramowania nie ma założonych żadnych kont zintegrowanego uwierzytelniania.

## 5.3 Pierwsze uruchomienie (Asystent konfiguracji)

Przy pierwszym uruchomieniu programu automatycznie otwiera się okno asystenta. Asystent pomaga w instalacji i konfiguracji Klientów. Można go wywołać także później z menu Plik > Asystent konfiguracji.

### 5.3.1 Aktywacja

W pierwszej kolejności należy uaktywnić wszystkie komputery, które mają zostać objęte ochroną. Zaznacz stację roboczą na liście i kliknij przycisk Uaktywnij. Jeśli jakiegoś komputera nie ma na liście, np. mógł przez dłuższy czas pozostawać wyłączony, wpisz w polu Komputer jego nazwę i kliknij przycisk Uaktywnij. Komputer zostanie wciągnięty na listę. Kiedy wszystkie końcówki są już aktywne, kliknij Dalej.

### 5.3.2 Metoda instalacji

W kolejnym oknie możesz zrezygnować z automatycznej instalacji oprogramowania klienckiego na aktywnych stacjach roboczych. Jeżeli preferujesz ręczną instalację lub używasz oprogramowania w grupie roboczej zamiast w domenie, wyłącz opcję automatycznego instalowania

składnika Klient.

### 5.3.3 Ustawienia standardowe

W tym oknie możesz zdefiniować standardowe ustawienia z jakimi chcesz domyślnie instalować oprogramowanie klienckie na stacjach roboczych. Program umożliwia grupowanie stacji roboczych i definiowanie różnych ustawień standardowych dla poszczególnych grup. Ustawienia w tym oknie dotyczą ogólnej grupy zwanej Cała sieć.

### 5.3.4 Ustawienia aktualizacji

ManagementServer może pobierać aktualizacje plików i sygnatur wirusów z Internetu. Proces aktualizacji można zautomatyzować. Wpisz w odpowiednie pola dane dostępu otrzymane po zarejestrowaniu programu. Szczegółowy opis planowania aktualizacji i ustawień z nią związanych znajdziesz w rozdziale Aktualizacja.

### 5.3.5 Ustawienia e-mail

ManagementServer ma możliwość wysyłania podejrzanych plików drogą poczty elektronicznej do Ambulansu G Data. W tym celu należy skonfigurować ustawienia w poniższym oknie. Należy podać nazwę i numer portu serwera SMTP, a także adres nadawcy. Adres ten zostanie użyty w celu przesłania odpowiedzi z Ambulansu.

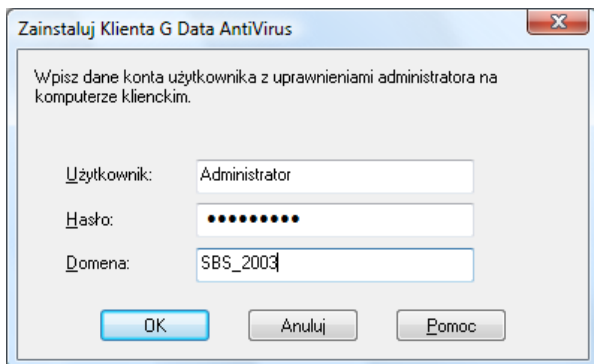
### 5.3.6 Powiadomienia e-mail

ManagementServer może powiadamiać administratora sieci o wykryciu wirusa za pomocą poczty elektronicznej. Można też wysłać podejrzone o infekcję pliki do Ambulansu. Należy wprowadzić w ustawieniach powiadomień nazwę serwera poczty, adres nadawcy oraz adres odbiorcy wiadomości. Można także ograniczyć ilość wysyłanych wiadomości, żeby nie przepełniać skrzynki pocztowej w przypadku infekcji większej ilości plików.

---

### 5.3.7 Automatyczne instalowanie Klienta

Kliknij przycisk Zakończ, aby zakończyć pracę Asystenta konfiguracji. Jeśli wybrana została automatyczna instalacja Klienta na stacjach roboczych, program zażąda podania konta użytkownika, który ma pełne uprawnienia dostępu do napędów serwera i stacji roboczych.



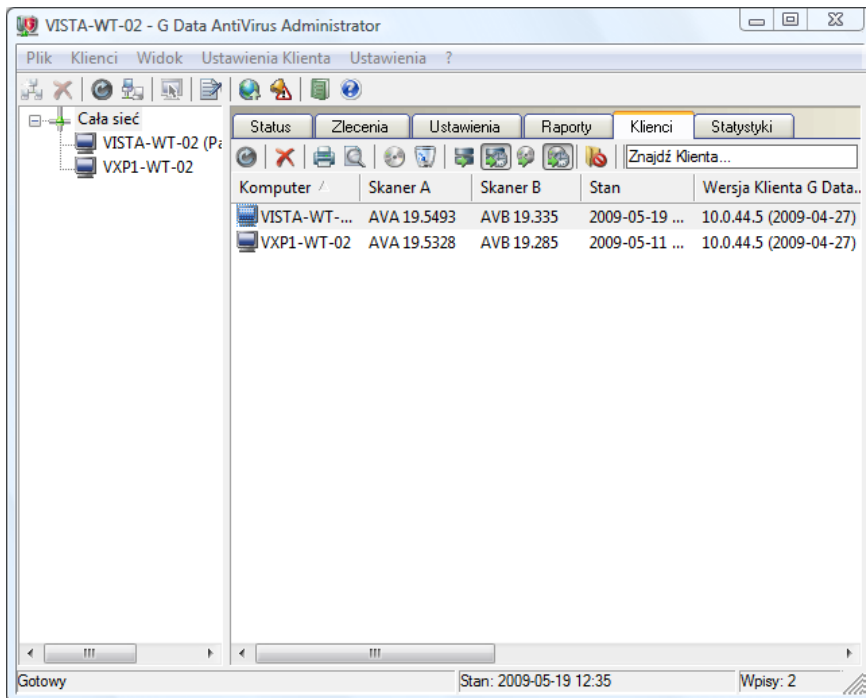
Po potwierdzeniu program spróbuje zainstalować oprogramowanie Klienta na wszystkich aktywnych stanowiskach.

Jeśli wystąpią problemy przy instalacji zdalnej, istnieje też możliwość zainstalowania oprogramowania na komputerach ręcznie lub z udostępnionego folderu. Program umożliwia także utworzenie pakietu cichej instalacji np. przy pomocy logon skryptów. Szczegóły w rozdziale Instalacja składnika G Data AntiVirus Klient.

Istnieje również możliwość zainstalowania specjalnej wersji oprogramowania klienckiego w systemach Linux. Szczegóły w rozdziale Instalacja składnika Klient w systemach Linux.

## 5.4 Obsługa składnika Administrator

Okno składnika Administrator skonstruowane jest w następujący sposób:



W lewej części okna widać drzewko przedstawiające logiczną strukturę domeny lub sieci roboczej. Po prawej stronie znajduje się okno widoku. Zakładki służą do przełączania między poszczególnymi widokami programu. Zawartość okna widoku zmienia się również w zależności od zaznaczenia stacji roboczej lub grupy stacji roboczych w drzewku po lewej stronie. Powyżej umieszczony jest kontekstowy pasek narzędzi z ikonami najczęściej używanych poleceń dla danego widoku. Pasek menu zawiera tematycznie pogrupowane polecenia globalne, do stosowania w każdym widoku programu.

Część funkcji i poleceń, np. dotyczących poczty elektronicznej nie jest dostępna w przypadku zaznaczenia w drzewku komputera

---

systemem Linux z serwerem plików Samba.

## 5.4.1 Pasek menu

Pasek menu zawiera zbiór wszystkich funkcji programu. Zawartość paska menu zmienia się w zależności od wybranej zakładki. Poszczególne funkcje objaśnione zostały w następujących rozdziałach.

### 5.4.1.1 Menu Plik

Menu plik zawiera zestaw poleceń umożliwiających wykonanie podstawowych operacji związanych z obsługą serwera.

### Asystent konfiguracji

Z jego pomocą możesz skonfigurować ochronę antywirusową i zainstalować oprogramowanie na stacjach roboczych. Więcej szczegółów na temat Asystenta konfiguracji znajdziesz w rozdziale Pierwsze uruchomienie (Asystent konfiguracji).

### Pokaż raporty

Plik raportów zawiera raporty działań przeprowadzonych przez składnik ManagementServer. Filtry umożliwiają wyświetlanie wyników według następujących kryteriów:

- **Widok:** Możesz przeglądać wszystkie raporty, albo też tylko raporty serwerów lub tylko stacji roboczych.
- **Stacja robocza/grupa:** Możesz przeglądać raporty pojedynczych stacji roboczych lub całych grup.
- **Czynność:** Możesz przeglądać raporty informacyjne lub komunikaty dotyczące konkretnych procesów związanych z ochroną antywirusową.

- Czas: Kryterium umożliwia wyświetlenie raportów z zadanego okresu czasu.

Przycisk Odśwież odświeża zawartość okna raportu. Widok zamyka polecenie Zamknij. Wiersze raportów wyświetlone są chronologicznie, ich kolejność można jednak zmieniać klikając myszką nagłówki kolumn. Istnieje również możliwość wydrukowania raportów i wyeksportowania ich do pliku w formacie XML. Sortowanie możliwe jest przez kliknięcie nagłówka wybranej kolumny.

## Zarządzanie użytkownikami

Za pomocą tego polecenia, administrator systemu może utworzyć lub zmodyfikować zintegrowane konta dostępu do interfejsu obsługi programu ManagementServer. Aby utworzyć nowe konto kliknij przycisk Nowe, wpisz nazwę użytkownika i hasło, a następnie określ poziom dostępu użytkownika (odczyt/zapis lub tylko odczyt).

## Zarządzanie serwerami

Okno zarządzania serwerami umożliwia przypisanie poszczególnych stacji roboczych do konkretnych serwerów podrzędnych w celu odciążenia serwera głównego. Z tego okna możliwe jest również zdalne zainstalowanie serwera podrzędnego.

Przypisanie stacji roboczych do serwerów w żaden sposób nie wpływa na grupowanie Klientów.

## Synchronizuj serwery podsięci

To polecenie umożliwia ręczne wymuszenie synchronizacji ustawień serwera głównego i serwerów podrzędnych niezależnie od ustawionego interwału automatycznej synchronizacji serwerów.

---

## Szablony wydruku

Funkcja pozwala na zapisanie lub wczytanie szablonów wydruku (marginesy, rozmiar czcionki).

Zawartość okna zależy od wybranego w danym momencie widoku. Opcje dotyczące drukowania nie są dostępne we wszystkich widokach.

## Widok strony

Opcja ta pozwala wybrać elementy, które chcesz wydrukować. W oknie wybory zaznacz elementy, które chcesz wydrukować i kliknij OK. Ukaże się podgląd wydruku. Przycisk Drukuj rozpoczyna drukowanie.

Zawartość okna zależy od wybranego w danym momencie widoku. Opcje dotyczące drukowania nie są dostępne we wszystkich widokach.

## Drukuj

Polecenie to rozpoczyna drukowanie ustawień Klienta lub raportów. W wyświetlonym oknie zaznacz elementy które chcesz wydrukować.

Zawartość okna zależy od wybranego w danym momencie widoku. Opcje dotyczące drukowania nie są dostępne we wszystkich widokach.

## Zakończ

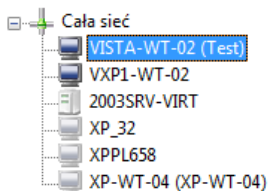
Funkcja ta zamyka składnik Administrator. Oczywiście sieć nadal jest pod ochroną, a wszystkie zlecenia będą wykonywane nawet gdy Administrator nie jest uruchomiony.

### 5.4.1.2 Menu Klienci

Menu Klienci to zestaw poleceń umożliwiających zarządzanie ochroną stacji roboczych lub grup.

#### Nowa grupa

Za pomocą tego polecenia możesz utworzyć nową grupę ustawień stacji roboczych. Grupowanie ustawień ułatwia zarządzanie procesami ochrony. Po kliknięciu polecenia w drzewie Klientów pojawi się nowa grupa, której można nadać dowolną nazwę.



Aby przypisać daną stację roboczą do grupy, kliknij jej nazwę myszką i przeciągnij na folder grupy.

#### Edytuj grupę

Klikając to polecenie otworzysz okno, w którym za pomocą przycisków Dodaj i Usuń można dowolnie grupować stacje robocze. Funkcja jest aktywna po zaznaczeniu dowolnej grupy.

Aby przypisać daną stację roboczą do grupy, kliknij jej nazwę myszką i przeciągnij na folder grupy.

---

## Usuń

Polecenie Usuń z menu Plik usuwa stację roboczą z drzewka (końcówka będzie nieaktywna). Nie oznacza to jednak odinstalowania składnika Klient. Usuwanie grupy przywróci pierwotną hierarchię stacji roboczych. Aby wyświetlić wyłączone stacje robocze można użyć funkcji Pokaż nieaktywne stacje robocze.

## Ustawienia standardowe

Program umożliwia utworzenie standardowych ustawień dla poszczególnych grup stacji roboczych. Dzięki temu wystarczy dodać nową stację roboczą do grupy, aby zastosować na niej wybrane wcześniej ustawienia. Ustawienia standardowe grup lub całej sieci można modyfikować również po przypisaniu stacji roboczych.

Opcja ustawień standardowych uaktywnia się w momencie zaznaczenia grupy lub całej sieci.

Opis ustawień i funkcji znajdziesz w rozdziale Ustawienia.

## Usuń ustawienia standardowe

Funkcja ta usuwa ustawienia standardowe danej grupy. Wszyscy stacje robocze przejmują w takim przypadku standardowe ustawienia całej sieci.

## Odśwież

Funkcja odświeża widok składnika Administrator.

## Pokaż nieaktywne stacje



Za pomocą tego polecenia możesz ujawnić nieaktywne lub usunięte z listy stacje robocze. Ich ikony są półprzezroczyste.



Tak wyglądają ikony aktywnych stacji roboczych - w odróżnieniu od nieaktywnych mają pełne kolory.

## Uaktywnij stację



Kliknij nieaktywną stację roboczą i uruchom to polecenie aby ją uaktywnić.



Samo uaktywnienie stacji roboczej nie oznacza zainstalowania oprogramowania klienckiego. Opcje ochrony dostępne są po zainstalowaniu na stacji roboczej składnika G Data AntiVirus Klient.

## Uaktywnij stację (Dialog)

To polecenie umożliwia uaktywnienie stacji roboczych, których w danej chwili nie ma w widoku drzewa. W oknie należy wpisać nazwę komputera.

## Znajdź komputer

Funkcja ta umożliwia wyszukiwanie komputerów w sieci po ich adresach IP. Wystarczy wpisać początkowy i końcowy adres IP, a program sam znajdzie wszystkie podłączone komputery. Po odnalezieniu stacji można je od razu uaktywnić używając nazw komputerów lub też adresów IP. W tym drugim przypadku, stacja robocza pojawi się w drzewku jako adres IP. Jest to przydatne np. jeśli nie ma w sieci serwera nazw (DNS).

---

## Utwórz pakiet cichej instalacji Klienta G Data AntiVirus

Dzięki tej funkcji można utworzyć instalacyjny plik AvkClientSetupPck.exe, pozwalający na zdalną instalację oprogramowania klienckiego na stacjach roboczych całej domeny bez ingerencji użytkowników np. przy użyciu skryptów logowania.

Pakiet zawiera zawsze aktualną wersję oprogramowania klienckiego.

Podczas instalacji składnika Klient, program pyta, czy w systemie ma zostać zainstalowany również składnik G Data Firewall. Szczegóły na temat składnika zapory połączenia znajdziesz w rozdziale o tym samym tytule.

### 5.4.1.3 Menu Widok

W menu widoku można przełączać między zakładkami programu. Bieżąca zakładka zaznaczona jest haczykiem. Za pomocą polecenia Odśwież lub klawisza F5 można w każdej chwili odświeżyć zawartość okna widoku, aby uaktualnić zmiany, które mogły nastąpić w międzyczasie. Informacje na temat poszczególnych składników programu znajdują się w rozdziałach Zakładki widoków.

### 5.4.1.4 Menu Ustawienia

Menu Ustawienia pozwala skonfigurować parametry pobierania aktualizacji programu i sygnatur wirusów, a także powiadamiania o infekcjach za pomocą poczty elektronicznej.

## Aktualizacja

To okno umożliwia dokonanie ustawień dotyczących aktualizacji plików składnika Klient oraz sygnatur wirusów. W zakładce Dane dostępu i ustawienia wpisz dane dostępu do aktualizacji otrzymane w potwierdzeniu rejestracji programu. Aktualizacje pobierane są z serwera aktualizacji i przechowywane lokalnie przez moduł ManagementServer. Aktualizowanie baz sygnatur wirusów oraz plików programu to podstawa ochrony antywirusowej. Oddzielnym tematem jest aktualizacja plików składnika ManagementServer. Możliwe jest to tylko metodą ręczną poprzez aplikację Internet Update.

## Baza sygnatur wirusów

Klienci wyposażeni są w własne kopie baz sygnatur wirusów. Aktualizacja baz wirusów przebiega w dwóch etapach, oba z nich można zautomatyzować. Pierwszy krok to pobranie plików z serwera aktualizacji do repozytorium składnika ManagementServer. Potem pliki są przekazywane do stacji roboczych (patrz zakładka Klienci).

- **Odśwież:** Przycisk odświeża widok okna. Wczytuje bieżące ustawienia z serwera zarządzającego.
- **Uaktualnij teraz:** To polecenie wymusza ręczne pobranie aktualizacji sygnatur wirusów do repozytorium składnika ManagementServer.
- **Zaplanuj:** Podobnie jak skanowanie, proces aktualizacji sygnatur wirusów można zautomatyzować. W tym celu kliknij przycisk Zaplanuj i skonfiguruj automatyczne pobieranie aktualizacji.

Aby aktualizacja mogła przebiegać automatycznie, serwer musi być połączony z Internetem. Jeżeli jest to konieczne, wprowadź w oknie Dane dostępu i ustawienia dane konta użytkownika i ustawienia proxy.

---

## Pliki programu

Aktualizacja plików składnika Klient również przebiega w dwóch etapach, i także w tym przypadku oba z nich można zautomatyzować.

Pierwszy krok to pobranie plików z serwera aktualizacji do repozytorium składnika ManagementServer. Drugi krok to przekazanie aktualizacji do stacji roboczych.

- **Odśwież:** Przycisk odświeża widok okna. Wczytuje bieżące ustawienia z serwera zarządzającego.
- **Uaktualnij teraz:** To polecenie wymusza ręczne pobranie aktualizacji plików Klienta do repozytorium składnika ManagementServer.
- **Zaplanuj:** Podobnie jak skanowanie, proces aktualizacji plików Klienta można zautomatyzować. W tym celu kliknij przycisk Zaplanuj i skonfiguruj automatyczne pobieranie aktualizacji.

Aby aktualizacja mogła przebiegać automatycznie, serwer musi być połączony z Internetem. Jeżeli jest to konieczne, wprowadź w oknie Dane dostępu i ustawienia dane konta użytkownika i ustawienia proxy.

Uwaga: Aby przeprowadzić aktualizację plików programowych składnika ManagementServer uruchom aplikację Internet Update z grupie programowej składnika ManagementServer w menu Start. Jest to jedyna metoda aktualizacji serwera zarządzającego.

## Dane dostępu i ustawienia

Dane dostępu do aktualizacji baz wirusów i plików programu, czyli użytkownika i hasło otrzymasz pocztą elektroniczną po wykonaniu rejestracji online. Jeżeli bazy wirusów lub pliki programu uległy uszkodzeniu poprzez przerwanie pobierania, wyłącz na czas jednej aktualizacji opcję Kontrola wersji (zalecane) w celu pobrania wszystkich plików. Program pobierze wtedy nie uszkodzone bazy wirusów lub pliki programu Klient.

Przycisk Konto użytkownika i ustawienia proxy otwiera okno, w którym możesz wprowadzić ustawienia serwera proxy.

Uwaga: Wprowadzanie zmian w oknie ustawień serwera proxy zalecane jest tylko w przypadku problemów z połączeniem przy standardowych ustawieniach.

Aby sprawdzić dostępność połączenia z serwerem aktualizacji, wpisz w przeglądarce adres <http://ieupdate.gdata.de/test.htm>, i sprawdź, czy strona zwraca stosowny komunikat.

### **Konto użytkownika i ustawienia proxy**

Jeżeli używasz urządzenia sieciowego wymagającego autoryzacji lub serwera proxy, zaznacz opcję Skorzystaj z serwera proxy. Wpisz adres serwera i port w odpowiednich polach. Jeżeli niezbędna jest autoryzacja, wpisz również nazwę użytkownika oraz hasło.

Aby sprawdzić dostępność połączenia z serwerem aktualizacji, wpisz w przeglądarce adres <http://ieupdate.gdata.de/test.htm>, i sprawdź, czy strona zwraca stosowny komunikat.

### **Powiadomienia**

W przypadku wykrycia wirusa serwer zarządzający może automatycznie wysyłać powiadomienia za pomocą poczty elektronicznej. Niezbędnych w tym celu ustawień dokonujemy w oknie Powiadomienia.

### **Ustawienia e-mail**

Wpisz nazwę serwera poczty oraz numer portu SMTP (zazwyczaj 25). Kliknij przycisk Uwierzytelnianie SMTP aby wpisać dane dostępu do serwera SMTP. Wybierz metodę uwierzytelniania i wpisz dane dostępu.

Następnie potrzebny będzie działający adres poczty elektronicznej, aby można było z niego przysyłać wiadomości. Na ten adres będą nadchodzić odpowiedzi na zgłoszenia plików do Ambulansu.

---

Na ten adres będą nadchodzić odpowiedzi na zgłoszenia plików do Ambulansu.

## Powiadomienia e-mail

Uaktywnij opcję powiadamiania przez e-mail w dolnej części okna i wpisz adres odbiorcy komunikatów. Warto ustalić ograniczenie ilościowe, aby skrzynka nie przepełniła się w przypadku dużej ilości zarażonych plików.

## Cofnij skaner A/B

Serwer zarządzający przechowuje zadaną ilość wersji aktualizacji sygnatur wirusów. W przypadku wystąpienia fałszywych alarmów lub innych problemów z sygnaturami wirusów, jest możliwość zablokowania bieżącej aktualizacji i cofnięcia plików sygnatur do wcześniejszej, poprawnie działającej wersji.

Aby cofnąć stan danego skanera do wcześniejszej wersji, zaznacz w oknie Cofanie aktualizacji bieżącą wersję sygnatur. Jeżeli chcesz cofnąć dany skaner o 2 wersje wstecz, zaznacz bieżącą i poprzednią wersję sygnatur itd.

Jeśli komputer przenośny jest odłączony od sieci z serwerem zarządzającym, operacja cofnięcia sygnatur nie zostanie na nim wykonana. Podobnie nie będzie można anulować cofnięcia sygnatur po odłączeniu komputera od sieci.

Ilość przechowywanych wersji sygnatur wirusów można ustawić w oknie Ustawienia serwera.

## Ustawienia serwera

W tym oknie można skonfigurować ustawienia dotyczące synchronizacji Serwerów podrzędnych, automatycznego czyszczenia raportów, a także przechowywania zarchiwizowanych wersji sygnatur wirusów.

## Ustawienia

W zakładce Ustawienia można modyfikować następujące opcje:

### Cofanie aktualizacji

Ta sekcja umożliwi sprecyzowanie, ile wersji sygnatur wirusów ma być archiwizowanych przed usunięciem.

### Automatyczne usuwanie raportów

W tej sekcji można ustawić parametry automatycznego usuwania raportów skanowania i wierszy pliku raportów.

## Synchronizacja

Ta zakładka umożliwia zdefiniowanie parametrów dotyczących komunikacji między Klientami, serwerami podrzędnymi i serwerem głównym programu:

- **Klienci:** W tej sekcji można określić regularność synchronizacji stacji roboczych z serwerem zarządzającym. Po zaznaczeniu opcji Powiadamiaj stacje robocze o modyfikacjach ustawień, użytkownik stacji będzie informowany komunikatem o każdej zmianie ustawień wykonanej zdalnie.
- **Serwery podrzędne:** W tej sekcji określone są interwały czasowe synchronizacji ustawień i sygnatur wirusów między Serwerem głównym, a Serwerami podrzędnymi. Zaznaczenie opcji Przenoś na bieżąco nowe raporty na serwer główny, spowoduje zsynchronizowanie nowych raportów w momencie ich powstawania, niezależnie od powyższych ustawień.

### 5.4.1.5 Menu ?

Polecenie Informacje wyświetla informacje na temat programu i jego wersji. Polecenie Pomoc powoduje otwarcie pliku pomocy. Polecenie Leksykon wirusów otwiera witrynę internetową z opisami najważniejszych wirusów.

---

## 5.4.2 Pasek narzędzi

Pasek narzędzi umożliwia szybkie uruchomienie ważniejszych poleceń programu.



**Nowa grupa:** Za pomocą tego polecenia możesz utworzyć nową grupę ustawień stacji roboczych. Grupowanie ustawień ułatwia zarządzanie procesami ochrony. Po kliknięciu polecenia w drzewie Klientów pojawi się nowa grupa, której można nadać dowolną nazwę



**Usuń:** Polecenie Usuń z menu Plik usuwa stację roboczą z drzewka (końcówka będzie nieaktywna). Nie oznacza to jednak odinstalowania składnika Klient. Usuwając grupy przywrócisz pierwotną hierarchię stacji roboczych.



**Odśwież:** Funkcja odświeża widok składnika Administrator. Dostępne jest także pod klawiszem funkcyjnym F5.



**Pokaż nieaktywne stacje robocze:** Za pomocą tego polecenia możesz ujawnić nieaktywne lub usunięte z listy stacje robocze. Ich ikony są półprzezroczyste.



**Uaktywnij stację:** Kliknij nieaktywną stację roboczą i uruchom to polecenie aby ją uaktywnić.



**Pokaż raporty:** Plik raportów zawiera raporty działań przeprowadzonych przez składnik ManagementServer.



**Aktualizacja:** To okno umożliwia dokonanie ustawień dotyczących aktualizacji plików składnika Klient oraz sygnatur wirusów.



**Powiadomienia:** W przypadku wykrycia wirusa serwer zarządzający może automatycznie wysyłać powiadomienia za pomocą poczty elektronicznej. Niezbędnych w tym celu ustawień dokonujemy w oknie Powiadomienia.



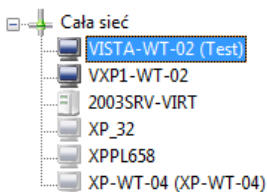
**Leksykon wirusów:** Polecenie Leksykon wirusów otwiera witrynę internetową z opisami najważniejszych wirusów.



**Pomoc:** Polecenie Pomoc powoduje otwarcie pliku pomocy.

### 5.4.3 Drzewo Klientów

Wszystkie komputery oraz zdefiniowane grupy przedstawione są w postaci drzewa. Grupy podzielone na podgrupy wyświetlone są ze znakiem + znanym z Eksploratora Windows. Aby rozwinąć grupę należy kliknąć znak +. Aby zwinąć daną gałąź kliknij znak -.



W oknie drzewa Klientów widoczne są następujące ikony:



Ikona sieci

---



Grupa



Serwer (aktywny)



Serwer (nieaktywny)



Klient (aktywny)



Klient (nieaktywny)



Niedostępne urządzenia, np. drukarki sieciowe

#### 5.4.4 Zakładki widoków

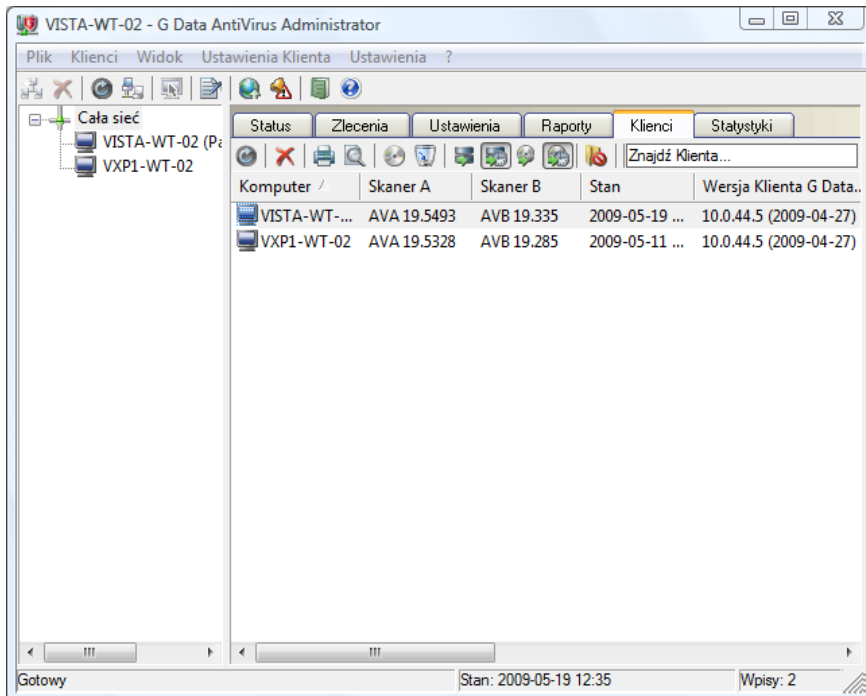
Zakładki służą do przeglądania widoków modułu Administrator. Widoki przedstawiają poszczególne obszary robocze programu.

- Zakładka Status
- Zakładka Zlecenia
- Zakładka Ustawienia
- Zakładka Raporty
- Klienci
- Zakładka Statystyki

Przełączanie widoków jest możliwe także przy użyciu menu Widok.

#### 5.4.4.1 Zakładka Status

Zakładka Status przedstawia zestawienie najważniejszych opcji ochrony antywirusowej danej stacji roboczej, grupy komputerów lub całej sieci.



Symbol zielonego światła oznacza, że ustawienia ochrony antywirusowej skonfigurowane są optymalnie.



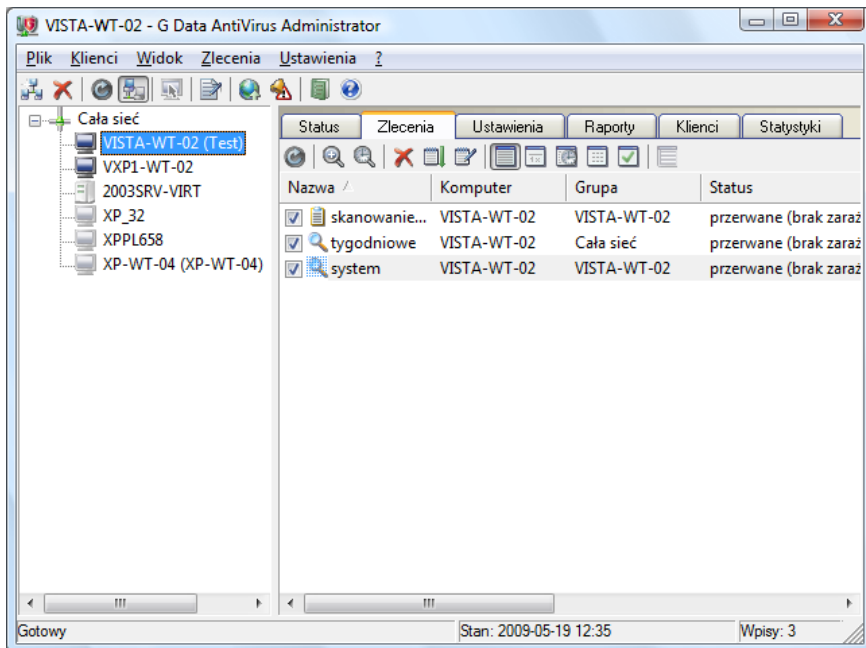
Czerwone światło oznacza, że wymagana jest Twoja ingerencja w ustawienia oprogramowania.

W momencie uruchamiania składnika Administrator, wszystkie ikony pokazują przez moment znaj ostrzeżenia. Nie oznacza to, że program G Data AntiVirus nie działa prawidłowo. W tym momencie mechanizm kontrolny automatycznie sprawdza poprawność ustawień ochrony antywirusowej.

Dwukrotne kliknięcie danego wiersza powoduje otwarcie odpowiedniego okna z ustawieniami, gdzie można dokonać korekty, lub przeprowadzić czynności związane z ochroną antywirusową.

#### 5.4.4.2 Zakładka Zlecenia

W tym widoku definiuje się zlecenia skanowania komputerów z zainstalowanym oprogramowaniem klienckim. Istnieją dwa rodzaje zleceń: jednorazowe i periodyczne. Jednorazowe skanowanie uruchamiane jest natychmiastowo, dla zleceń periodycznych planuje się czas wykonania zlecenia na określony dzień i godzinę.



W widoku Zlecenia widoczne są wszystkie zleczone skanowania. Można je sortować klikając opisy w nagłówkach kolumn:

- **Nazwa:** Nazwa zlecenia nadana przez w trakcie tworzenia zlecenia.
- **Komputer:** To nazwa stacji roboczej. Zlecenia można przydzielać tylko aktywnym stacjom roboczym.
- **Grupa:** Stacje robocze można łączyć w grupy. Jeśli przydzielisz zlecenie grupie, w oknie widoku nie pojawią się nazwy wszystkich stacji roboczych, lecz tylko nazwa grupy.
- **Status:** Informacja o stanie lub wyniku wykonywanego zlecenia. Dowiesz się tu, czy zlecenie jest już wykonane i czy podczas skanowania zostały wykryte wirusy.
- **Ostatnie uruchomienie:** Stąd dowiesz się kiedy ostatnio uruchomione zostało dane zlecenie.
- **Interwał:** Kolumna informuje jak często ma być wykonywane

skanowanie.

- **Rozmiar skanowania:** Zawiera informacje na temat zasobów wybranych do przeskanowania (np. wszystkie dyski lokalne).

Po kliknięciu zakładki Zlecenia, w pasku menu pojawi się dodatkowa pozycja o tej samej nazwie. Menu umożliwia przeprowadzenie następujących działań:

- **Widok:** Jeżeli nie chcesz wyświetlać wszystkich zleceń, wybierz z menu Widok pożądaną opcję. Możesz ograniczyć widok do zleceń periodycznych, jednorazowych, rozpoczętych oraz zakończonych. Dodatkowo można włączyć wyświetlanie szczegółów zleceń grupowych.
- **Uruchom teraz:** To polecenie wymusza natychmiastowe uruchomienie dowolnego istniejącego zlecenia, niezależnie od ustalonego harmonogramu.
- **Anuluj:** Użyj tej funkcji w celu przerwania trwającego skanowania.
- **Usuń:** To polecenie usuwa skonfigurowane zlecenie.
- **Nowy:** Polecenie umożliwia utworzenie nowego zlecenia jednorazowego lub periodycznego.

Możesz utworzyć dowolną ilość różnych zleceń skanowania. Ze względu na obciążenie powodowane przez proces skanowania, najlepiej unikać zleceń zachodzących na siebie w czasie.

## Odśwież



To polecenie odświeża widok okna Zlecenia.

### Nowe zlecenie (jednorazowe)



Ta funkcja umożliwia przeprowadzenie jednorazowego skanowania wybranych zasobów na żądanie. Przed uruchomieniem zlecenia można zdefiniować nazwę zlecenia, parametry skanowania i zasoby, które mają zostać objęte zleceniem.

Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia. Szczegóły na temat konfigurowania zleceń znajdziesz w rozdziale Nowe zlecenie (periodyczne).

### Nowe zlecenie (periodyczne)



Ta funkcja umożliwia przeprowadzenie skanowania periodycznego wybranych zasobów. Przed uruchomieniem zlecenia można zdefiniować nazwę zlecenia, parametry skanowania i zasoby, które mają zostać objęte zleceniem.

Kliknij dwukrotnie nazwę zlecenia, jeżeli chcesz przejrzeć lub zmodyfikować ustawienia zlecenia. Ten sam efekt uzyskasz klikając nazwę zlecenia prawym klawiszem myszki i wybierając polecenie Właściwości...

### Zlecenie

W tej zakładce definiuje się nazwę zlecenia skanowania, a także opcje takie jak możliwość przerywania zlecenia przez użytkownika stacji roboczej, czy wyłączenie komputera po przeprowadzeniu skanowania. Nazwę zlecenia najlepiej dobrać tak, aby mówiła o nim jak najwięcej, np. Skanowanie komputera pani Basi lub Skanowanie folderu Windows w całej sieci. Ułatwi to identyfikację zlecenia.

Można tu zdecydować czy użytkownik ma prawo przerywać zlecenie za pomocą menu kontekstowego ikonki Klienta. Jeśli sieć jest stale pod okiem Strażnika, można zezwolić użytkownikom na przerywanie zleceń, które

---

wpływają na obciążenie komputera. Opcja Odświeżaj postęp skanowania co 2 minuty pozwala na bieżąco informować serwer zarządzający o statusie przebiegającego skanowania.

Wyłącz komputer po zakończeniu skanowania, jeśli nikt nie jest zalogowany to ciekawa opcja umożliwiająca pozostawienie włączonych komputerów np. na noc w celu przeskanowania zasobów bez niepotrzebnego obciążania maszyn w trakcie pracy.

## Czas rozpoczęcia/Planowanie

W zakładce Czas rozpoczęcia, możesz ustawić czas rozpoczęcia skanowania jednorazowego. W tym celu zaznacz opcję Ustaw czas rozpoczęcia i sprecyzuj godzinę rozpoczęcia skanowania.

Zakładka Planowanie służy do określenia częstotliwości wykonywania skanowania. W polu Wykonuj wybierz pożądaną częstotliwość i uzupełnij ustawienia korzystając z sekcji Dokładnie i Dni tygodnia.

Opcja Przy starcie systemu powoduje przeprowadzenie skanowania przy każdym uruchomieniu komputera. Nie jest to wskazane, gdyż komputer przez dłuższy czas po uruchomieniu będzie pracował dużo wolniej niż normalnie.

Wskazówka: Ustawienie Codziennie można zmodyfikować określając dni tygodnia, np. skanowanie w dni robocze, co drugi dzień lub w weekendy, kiedy nikt nie korzysta z komputera.

## Skanowanie

Zakładka Skanowanie pozwala skonfigurować parametry skanowania.

Ponieważ automatyczne zlecenia periodyczne oraz te uruchamiane ręcznie mogą odbywać się w godzinach kiedy komputer nie jest obciążony innymi zadaniami, nie ma potrzeby ograniczania rozmiarów skanowania jak to ma miejsce w przypadku Strażnika.

- Skanery: Program pracuje przy użyciu dwóch niezależnych skanerów. Optymalne efekty daje oczywiście zastosowanie obu skanerów. Przy użyciu tylko klasycznego skanera proces trwa krócej, lecz jest równie skuteczny. Zalecamy ustawienie Dwa skanery. Praca skanerów jest

skoordynowana w ten sposób, że minimalnie obciążają procesor.

- W razie infekcji: W tym polu można ustalić reakcję programu na wykrycie infekcji, w zależności od rodzaju zlecenia. Kwarantanna to specjalny, zaszyfrowany folder, w którym program przechowuje niebezpieczne pliki. Administrator może zlecić dezynfekcję, usunięcie lub wysłanie tych plików do Ambulansu.
- Zainfekowane archiwa: Można ustalić osobną reakcję na wykrycie wirusa w pliku spakowanym. Należy pamiętać, że wirus w takim pliku jest niegroźny do momentu rozpakowania.
- Typy plików: Tu można zdefiniować typy kontrolowanych plików. Z reguły nie ma potrzeby kontrolowania plików, które się nie uruchamiają; kontrola całego systemu plików może zająć dość dużo czasu. Zaleca się ustawienie Automatyczne rozpoznanie plików – sprawdzone zostaną tylko pliki mogące teoretycznie zawierać wirusa.
- Priorytet skanowania: Do wyboru są trzy poziomy priorytetu skanowania: Wysoki, Średni i Niski. Skanowanie o wysokim priorytecie przebiega szybciej, podczas gdy równoczesne procesy innych aplikacji, wolniej. Skanowanie o niskim priorytecie trwa dłużej, ale inne aplikacje działają wtedy bez zakłóceń.

W sekcji Ustawienia można włączać/wyłączać dodatkowe opcje skanowania.

**Heurystyka:** Analiza heurystyczna pozwala na rozpoznawanie wirusów po typowych cechach spotykanych u tego typu programów. Z jednej strony wzmaga to skuteczność skanowania, ale jest to metoda bardzo czasochłonna, a w niektórych przypadkach może powodować fałszywe alarmy.

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

**Skanuj pliki e-mail:** Jeśli opcja jest włączona, skanowane są także pliki programów pocztowych zawierające wiadomości. Nerozważne użycie tej funkcji może spowodować utratę wiadomości pocztowych.

**Skanuj obszary systemowe:** Obszary systemowe (boot sektory, Master Boot Record itd.) stanowią podstawę systemu

---

operacyjnego, dlatego też powinny być skanowane za każdym razem.

Wykrywaj dialery/adware/spyware/riskware: Program wykrywa także programy wysokiego ryzyka, które niekoniecznie są wirusami. W ten sposób wykrywane są np. dialery, programy do zdalnego administrowania (np. RealVNC).

Wykrywaj rootkity: Włączenie tej opcji powoduje zastosowanie skanera wykrywającego grupę wirusów wyposażoną w mechanizmy służące do ukrywania się w systemie operacyjnym.

Zastosuj wszystkie dostępne procesory: Opcja ma zastosowanie w przypadku komputerów wyposażonych w kilka procesorów lub rdzeni (Dual Core lub Quad Core). Użycie opcji spowoduje, że wzrośnie obciążenie systemu, ale skróci się czas skanowania.

## Rozmiar skanowania

Ta zakładka pozwala ograniczyć skanowanie do konkretnych katalogów. Dzięki temu można ustawić kilka osobnych zleceń skanowania dotyczących konkretnych partycji lub folderów.

W przypadku zleceń dla linuksowych serwerów Samba, okno wyboru folderów umożliwia zaznaczenie folderu root (/) lub dowolnych udziałów. Umożliwia to utworzenie osobnych zleceń skanowania dla różnych udziałów.

## Usuń zlecenie



Użycie tego polecenia usuwa zaznaczone zlecenie skanowania.

## Uruchom teraz



Użycie tego polecenia wymusza natychmiastowe wykonanie zaznaczonego zlecenia skanowania niezależnie od ustawionego harmonogramu.

## Raporty



To polecenie otwiera okno raportów dotyczących zleceń dla danej stacji roboczej.

## Opcje wyświetlania

Opcje wyświetlania umożliwiają filtrowanie zleceń:



Pokaż wszystkie zlecenia



Pokaż tylko zlecenia jednorazowe



Pokaż tylko zlecenia okresowe



Pokaż tylko uruchomione zlecenia



Pokaż tylko zakończone zlecenia

---

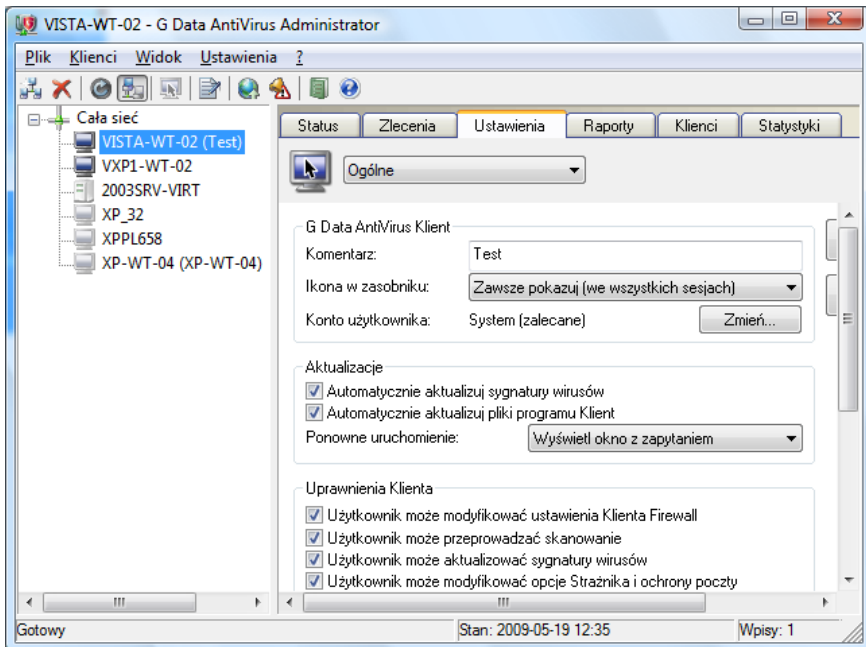


Pokaż szczegóły zleceń grupowych (działa w przypadku zleceń tworzonych dla grup stacji roboczych)

### 5.4.4.3 Zakładka Ustawienia

Zakładka Ustawienia umożliwia modyfikowanie wszystkich opcji ochrony antywirusowej dla konkretnych stacji roboczych, grup lub całej sieci.

Rozwijana lista znajdująca się u góry okna ustawień umożliwia przełączanie między dostępnymi zestawami opcji. Ustawienia dotyczą zawsze stacji roboczej lub grupy zaznaczonej w drzewie Klientów, z lewej strony. Po zakończeniu konfiguracji opcji w danym zestawie kliknij przycisk Zastosuj, aby przekazać ustawienia do stacji roboczych.



## Ogólne

Sekcje ustawień zawarte w zakładce ogólne opisane są w następujących rozdziałach.

## G Data AntiVirus Klient

Pierwsza sekcja zawiera następujące ustawienia:

- **Komentarz:** Jeżeli stacje robocze nie mają komentarzy przypisanych w ustawieniach systemu, możesz przypisać własne komentarze ułatwiające identyfikację komputerów (np. komputer szefa, księgowość, itp.)
- **Ikonka w zasobniku:** Dzięki tej opcji możesz ukryć ikonkę oprogramowania klienckiego na stacji roboczej, jeśli np. nie chcesz aby użytkownik miał świadomość, że program antywirusowy jest zainstalowany. Ustawienie Tylko w pierwszej sesji spowoduje, że ikonka nie będzie widoczna dla kolejnych użytkowników, którzy zalogują się jednocześnie do komputera. Jeżeli planujesz nadanie użytkownikom uprawnień do podglądu lub modyfikowania opcji, ukrywanie ikonki nie ma sensu, gdyż obsługa programu z poziomu stacji roboczej możliwa jest tylko poprzez menu kontekstowe ikonki.
- **Konto użytkownika:** Oprogramowanie klienckie funkcjonuje w kontekście systemu Windows. Jeżeli chcesz wpisać inne konto użytkownika, zastosuj konto z uprawnieniami administratora na stacjach roboczych, aby umożliwić skanowanie.

## Aktualizacje

Sekcja aktualizacje umożliwia ustawienie następujących parametrów:

- **Automatycznie aktualizuj sygnatury wirusów:** Włączenie tej opcji spowoduje automatyczne przekazywanie bieżących aktualizacji z serwera zarządzającego do stacji roboczych.
  - **Automatycznie aktualizuj pliki programu Klient:** Ta opcja umożliwia automatyczne aktualizowanie plików oprogramowania klienckiego na stacjach roboczych.
  - **Ponowne uruchomienie:** Zdarza się, że po uaktualnieniu lub
-

---

odinstalowaniu oprogramowania klienckiego niezbędne jest ponowne uruchomienie systemu operacyjnego stacji roboczej. Można wymusić ponowne uruchomienie bez ostrzeżenia, wyświetlić komunikat o potrzebie restartu lub tylko utworzyć raport.

## Uprawnienia Klienta

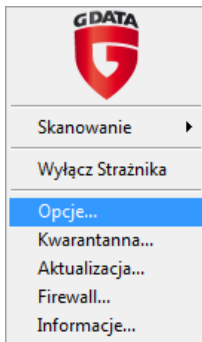
Ta sekcja umożliwia ustawienie uprawnień dla użytkownika oprogramowania klienckiego zainstalowanego na stacji roboczej:

- Użytkownik może modyfikować ustawienia Klienta Firewall: Jeżeli ta opcja jest aktywna, użytkownik stacji roboczej może uruchomić z menu kontekstowego Klienta interfejs programu G Data Firewall i dokonywać zmian w ustawieniach. Jeżeli opcja jest wyłączona, opcja uruchomienia okna Firewall znika z menu kontekstowego.
- Użytkownik może przeprowadzać skanowanie: Jeżeli ta opcja jest włączona, użytkownik może uruchomić skanowanie dowolnych zasobów lokalnych komputera, a także modyfikować opcje skanowania. W menu kontekstowym pojawiają się pozycje Skanuj i Opcje.
- Użytkownik może aktualizować sygnatury wirusów: Jeżeli to uprawnienie jest włączone, użytkownik może aktualizować sygnatury wirusów oprogramowania klienckiego nawet, jeśli komputer nie ma połączenia ze składnikiem ManagementServer. Opcja jest bardzo przydatna w przypadku komputerów przenośnych, które nie zawsze mają połączenie z lokalną siecią przedsiębiorstwa.
- Użytkownik może modyfikować opcje Strażnika i ochrony poczty: Użytkownik z tym uprawnieniem jest w stanie całkowicie wyłączyć ochronę dostępową stacji roboczej, a także poczty elektronicznej. Ustawienie zalecane tylko dla doświadczonych i zaufanych użytkowników stacji roboczych.
- Użytkownik może przeglądać lokalną Kwarantannę: Użytkownik z nadanym uprawnieniem do lokalnej Kwarantanny może samodzielnie usuwać, dezynfekować lub przywracać do systemu zarażone pliki odizolowane w zaszyfrowanym folderze Kwarantanny. Ustawienie zalecane tylko dla doświadczonych i zaufanych użytkowników stacji roboczych.
- Zabezpieczenie ustawień hasłem: Jeżeli do stacji roboczej ma dostęp więcej niż jeden zaufany użytkownik, można zabezpieczyć dostęp do ustawień hasłem, znanym tylko tej osobie. Dzięki temu inni użytkownicy

komputera nie będą mogli modyfikować ustawień narażając system na infekcję.

- Ustawienia aktualizacji: Stacja robocza może uaktualniać sygnatury wirusów z repozytorium serwera zarządzającego, lub bezpośrednio z Internetu. Można również ustawić trzecią opcję, czyli kombinację dwóch pierwszych. W takim przypadku stacja (lub komputer przenośny) pobiera sygnatury z serwera, jeżeli jest w sieci przedsiębiorstwa, a bezpośrednio z Internetu, jeżeli jest poza firmą.

Po włączeniu wszystkich dostępnych uprawnień, użytkownik ma do dyspozycji pełne menu kontekstowe ikonki:



## Wyjątki skanowania

W oknie Foldery wyjątków można zdefiniować pomijane przy skanowaniu pliki, foldery i napędy sieciowe. Kliknięcie przycisku Edycja, a następnie ..., otwiera okno struktury katalogów stacji roboczej.

Wyjątki można definiować dla konkretnych stacji roboczych, grup lub całej sieci. Istnieje też możliwość eksportowania i importowania zestawów wyjątków do pliku tekstowego.

W przypadku wyjątków dla linuksowych serwerów Samba, okno wyboru folderów umożliwia zaznaczenie folderu root (/) lub dowolnych udziałów.

---

## Strażnik

W tym widoku można dostosować ustawienia Strażnika dla wybranych stacji roboczych lub grup. Aby zmienić ustawienia dla całej grupy, należy zaznaczyć grupę na liście komputerów. Strażnik kontroluje wszystkie próby odczytu i zapisu plików zgodnie z ustawieniami. Działanie Strażnika odbywa się w tle, praktycznie niezauważalnie dla użytkownika.

Można skonfigurować Strażnika indywidualnie dla każdej stacji roboczej, grupy komputerów lub całej sieci. Zmiany w ustawieniach zatwierdza się przyciskiem Zastosuj. Przycisk Anuluj przywróci poprzednie ustawienia.

Jeśli w obrębie grupy zmienione zostaną ustawienia niektórych Klientów, w ustawieniach grupy będzie to uwidocznione wypełnionymi kwadracikami przy opisach opcji, które nie są jednolite dla całej grupy lub sieci

Bez ważnej przyczyny, nie powinno się wyłączać Strażnika na żadnym ze stanowisk.

Strażnik może spowolnienie działania niektórych programów lub ich komponentów. Aby tego uniknąć, można dodać foldery lub niektóre pliki tych aplikacji do wyjątków Strażnika.

## Ustawienia

Sekcja Ustawienia umożliwia modyfikację następujących parametrów:

- Status: Strażnik może być włączony, wyłączony. Nie zaleca się wyłączania monitora bez ważnego powodu.
- Skanery: Klient stosuje dwa niezależne skanery antywirusowe. Zalecamy ustawienie Dwa skanery - optymalna wydajność. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor..
- W razie infekcji: Wybierz reakcję programu na wykrycie infekcji, w zależności od rodzaju zlecenia.

Zablokuj dostęp: Program uniemożliwi zapis oraz odczyt danego

pliku.

Dezynfekcja (jeśli niemożliwa: zablokuj dostęp): Jeżeli nie uda się zdezynfekować pliku, program zablokuje do niego dostęp.

Dezynfekcja (jeśli niemożliwa: do Kwarantanny): Jeśli nie uda się zdezynfekować pliku, program przeniesie go do Kwarantanny.

Dezynfekcja (jeśli niemożliwa: usuń plik): Jeśli nie uda się zdezynfekować pliku, program spróbuje go usunąć.

Przenieś plik do Kwarantanny: Plik zostanie umieszczony w zaszyfrowanym folderze.

Usuń zarażony plik: Funkcja ta umożliwia usunięcie pliku wraz z wirusem.

- Zainfekowane archiwa: Można ustalić osobną reakcję na wykrycie wirusa w spakowanym pliku.
  - Rodzaje plików: Zdecyduj, czy chcesz chronić wszystkie pliki, czy tylko pliki wykonywalne i dokumenty.
  - Skanuj w trakcie zapisu: Włączenie tej opcji powoduje sprawdzanie plików podczas zapisywania ich na dysku. Nie zaleca się wyłączenia tej opcji, gdyż jest to w zasadzie podstawowa funkcja Strażnika. Wyłączenie kontroli zapisu znacznie obniża skuteczność ochrony antywirusowej końcówki, a tym samym całej sieci.
  - Skanuj zasoby sieciowe: Przy włączonej opcji Strażnik kontroluje także zamapowane napędy sieciowe. Jeśli cała sieć jest chroniona przez moduły klienckie, opcja ta może być wyłączona.
  - Heurystyka: Analiza heurystyczna różni się od zwykłego skanowania tym, że nie tylko wynajduje wirusy porównując kody plików z kodami stale aktualizowanej bazy znanych wirusów, ale rozpoznaje je po typowych cechach spotykanych u tego typu programów. Ta metoda, z jednej strony wzmacnia skuteczność skanowania, ale jest bardzo czasochłonna i może powodować fałszywe alarmy.
  - Skanuj archiwa: Skanowanie plików spakowanych trwa bardzo długo i nie jest potrzebne dopóki włączony jest Strażnik. Strażnik wychwytuje wirusy w chwili rozpakowywania archiwów i zapobiega ich dalszemu
-

---

rozprzestrzenianiu się. Aby zminimalizować obciążenie procesora rozpakowywaniem dużych plików, można ograniczyć rozmiar kontrolowanych archiwów.

- Skanuj pliki e-mail: Jeśli opcja jest włączona, skanowane są także foldery programów pocztowych zawierające wiadomości. Nerozważne użycie tej funkcji może spowodować utratę wiadomości pocztowych.
- Skanuj obszary systemowe: Włączenie tej opcji powoduje skanowane sektorów rozruchowych dysku twardego oraz dyskietki przy każdym uruchomieniu komputera.
- Skanuj obszary systemowe przy zmianie nośnika: Można kontrolować obszary systemowe przy starcie komputera lub przy zmianie nośnika (np. włożenie do napędu nowej płytki CD-ROM). Zaleca się pozostawienie włączonej przynajmniej jednej z tych dwóch opcji.
- Wykrywaj dialery / adware / spyware / riskware: Strażnik wykrywa także programy wysokiego ryzyka, które niekoniecznie są wirusami. W ten sposób wykrywane są np. dialery, programy do zdalnego administrowania (np. RealVNC).

## Wyjątki

W razie potrzeby można skonfigurować działanie Strażnika tak, aby kontrolując dostęp do plików pomijał określone napędy, katalogi lub pliki.

Możliwe jest definiowanie następujących rodzajów wyjątków:

- Napęd: Kliknij przycisk ..., a następnie wybierz literę napędu (partycji, dysku, napędu CD/DVD), który chcesz wyjąć spod ochrony monitora.
- Katalog: Kliknij przycisk ..., a następnie wybierz folder, który chcesz wyjąć spod ochrony monitora wraz z podfolderami.
- Plik: Wpisz nazwę pliku, który chcesz wyjąć spod ochrony. Dozwolone jest stosowanie znaków specjalnych (? jako dowolny znak, \* jako dowolny ciąg znaków).
- Proces: Kliknij przycisk ..., a następnie wybierz plik wykonywalny (EXE), którego proces chcesz wyjąć spod ochrony monitora.

W ten sposób możesz utworzyć dowolną ilość wyjątków, które później

można zmodyfikować lub usunąć.

Aby wybrać np. wszystkie pliki z rozszerzeniem .exe, wpisz \*.exe.  
Aby wybrać np. wszystkie pliki o formacie arkuszy kalkulacyjnych (np. \*.xlr, \*.xls), wpisz \*.xl?. Jeśli chcesz sprawdzać pliki o takim samym początku nazwy wpisz np. tekst\*.\*

## Powiadomienia

Jeśli chcesz, aby użytkownik otrzymywał komunikaty o wykryciu wirusa w systemie, zaznacz opcję Powiadom użytkownika o wykryciu wirusa. Powiadomienie odbywa się poprzez wyświetlenie okna z komunikatem.

## Status

W przypadku zmodyfikowania ustawień, ta sekcja informuje o fakcie zastosowania zmian na stacji roboczej.

## E-mail

Składnik Klient wyposażony jest w narzędzie umożliwiające ochronę poczty wychodzącej i przychodzącej dowolnego programu pocztowego korzystającego z protokołów POP3, IMAP i SMTP, czyli Outlook Express, Mozilla Thunderbird, The Bat! i inne. Konta programu MS Office Outlook chronione są przez specjalny dodatek.

Ustawienia można skonfigurować indywidualnie dla każdej stacji roboczej, dla grupy komputerów lub też dla całej sieci:

## Wiadomości przychodzące

Ta sekcja umożliwia modyfikowanie następujących ustawień:

- W razie infekcji: Wybierz reakcję programu na wykrycie wirusa w wiadomości.
-

- Skanuj wiadomości przychodzące: Włączenie tej opcji spowoduje sprawdzenie każdej przychodzącej wiadomości pod kątem wirusów i innych zagrożeń.
- Skanuj nieprzeczytane wiadomości podczas uruchamiania Microsoft Outlook: Włączenie tej opcji spowoduje przeskanowanie wszystkich nieprzeczytanych wiadomości we wszystkich folderach programu MS Office Outlook.
- Dołącz raport do zarażonych wiadomości przychodzących: Jeśli program wykryje wirusa w wiadomości, dołączy do tematu słowo WIRUS w nawiasie kwadratowym, a do treści maila komunikat o infekcji.

### Wiadomości wychodzące

Sekcja Wiadomości wychodzące umożliwia modyfikowanie następujących ustawień:

- Skanuj wiadomości wychodzące: Włączenie tej opcji może zapobiec przypadkowemu wysłaniu wirusa lub zarażonego załącznika. Jeżeli program wykryje wirusa w przesyłce, pojawi się stosowny komunikat, a wiadomość nie zostanie wysłana przez program pocztowy.
- Dołącz stopkę do wiadomości wychodzących: Jeżeli opcja Skanuj wiadomości wychodzące, program dołączy do treści wiadomości stopkę informującą o przeprowadzeniu skanowania maila. Dodatkowo można wymusić umieszczenie w podpisie informacji o wersji programu oraz linku do strony G Data Software.

### Opcje skanowania

Do dyspozycji masz następujące opcje skanowania wiadomości:

- Skanery: Zalecamy stosowanie dwóch skanerów. Praca skanerów jest skoordynowana w ten sposób, że minimalnie obciążają procesor.
- OutbreakShield: Jest to dodatkowy skaner poczty, który działa niezależnie od tradycyjnych sygnatur wirusów. Jest w stanie wykryć niebezpieczną wiadomość jeszcze przed sklasyfikowaniem wirusa i dostarczeniem odpowiedniej sygnatury wirusów. Kliknij przycisk Zmień, jeśli chcesz dodatkowo użyć specjalnych sygnatur wirusów tworzonych

na potrzeby skanera OutbreakShield. W takim przypadku program będzie próbował automatycznie nawiązać połączenie z Internetem. Jeżeli połączenie z Internetem wymaga skonfigurowania serwera proxy, skorzystaj z ustawień w sekcjach Serwer proxy i Uwierzytelnianie proxy.

## **Powiadomienia**

Jeśli chcesz, aby użytkownik otrzymywał komunikaty o wykryciu wirusa w wiadomości, zaznacz opcję Powiadom użytkownika o wykryciu wirusa. Powiadomienie odbywa się poprzez wyświetlenie okna z komunikatem.

## **Ustawienia ochrony poczty**

Do dyspozycji są następujące ustawienia:

- Konta programu Microsoft Office Outlook chroni specjalny dodatek: Włączenie tej opcji, oprócz skanowania wiadomości podczas wysyłania/ odbierania, umożliwi dodatkowo skanowanie wiadomości oraz folderów na żądanie, bezpośrednio w programie MS Office Outlook. Skanowanie można wykonać przez zaznaczenie folderu i uruchomienie polecenia Narzędzia > Skanuj folder programem G Data AntiVirus.... Polecenie dostępne jest również jako ostatnia ikonka standardowego paska narzędzi programu MS Office Outlook.
- Chronić porty: Programy pocztowe takie jak Outlook Express, Mozilla Thunderbird, TheBat! korzystające z protokołów POP3, IMAP oraz SMTP chronione są w standardowy sposób. Ochronę poszczególnych protokołów można włączać/wyłączać po kliknięciu przycisku Zmień.

## **HTTP/Komunikatory**

Składnik Klient oferuje funkcje skanowania stron internetowych przed otwarciem, a także ochronę komunikatorów.

---

## Zawartość stron HTTP

- Skanuj zawartość stron HTTP: Filtr działa już w trakcie otwierania stron przy pomocy przeglądarki internetowej. Jeśli chcesz użyć tej funkcjonalności, włącz sprawdzanie zawartości stron i wpisz numer lub oddzielone przecinkiem numery portów HTTP (domyślnie 80).
- Ignoruj przekroczenie limitu czasu w przeglądarce: Skanowanie zawartości strony odbywa się przed otwarciem strony. Może to spowodować błąd w przeglądarce, z powodu niedostarczenia treści strony do przeglądarki w czasie ustawionym w przeglądarce. Włączając tę opcję spowodujesz zignorowanie przekroczenia limitu czasu, dzięki czemu przeglądarka nie wyświetli komunikatu błędu.
- Limit rozmiaru skanowanych plików: Ta opcja pozwala uniknąć długotrwałego skanowania dużych plików zawartych na sprawdzanej stronie internetowej. Skanowanie wszystkich plików w niewielkim stopniu spowalnia czas otwierania obszernych witryn internetowych.

## Komunikatory

- Chroń komunikatory: Używanie komunikatorów internetowych stwarza zagrożenie ze względu na możliwość przesyłania plików przez programy takie jak Windows Messenger itp. Program może zabezpieczyć niektóre z aplikacji służących do komunikacji. Jeżeli Twój komunikator korzysta z innego portu niż standardowy, wpisz numer portu w polu Numery portów.
- Komunikatory (integracja z aplikacjami): Jeżeli używasz programu Microsoft Messenger (powyżej wersji 4.7) lub Trillian (od wersji 3.0), możesz zintegrować program z komunikatorem. Pliki przesyłane przez komunikator będą skanowane na obecność wirusów.

Wyłączenie opcji ochrony komunikatorów nie wpływa na skuteczność ochrony antywirusowej, ponieważ pliki przesyłane przez komunikatory są przed zapisaniem na dysku skanowane przez Strażnika, pod warunkiem, że jest przez cały czas włączony.

## AntiSpam

Składnik Klient ma wbudowany filtr antyspamowy. Dostępne są następujące opcje filtra spamu:

### Filtr spamu

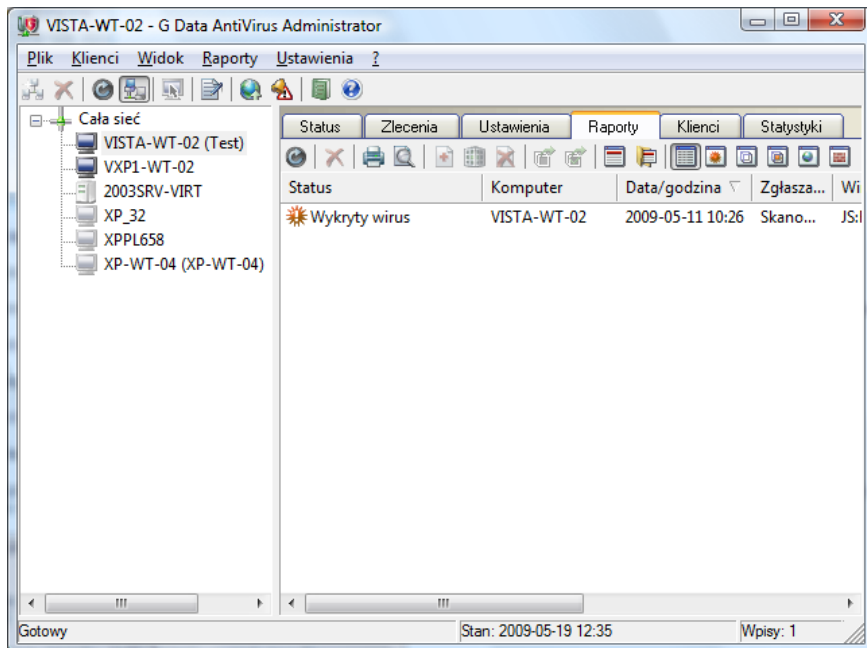
Jeżeli chcesz uruchomić filtr spamu dla poczty elektronicznej, włącz opcję Zastosuj filtr spamu. Po wykryciu podejrzanego, lub potwierdzonej wysyłki masowej, program automatycznie doda zdefiniowany poniżej komunikat do tematu wiadomości.

Dzięki oznaczaniu niechcianych wiadomości w temacie, możesz zdefiniować w aplikacjach pocztowych poszczególne stacje robocze reguły przenoszące wiadomości do utworzonych folderów poczty np. Spam, Prawdopodobnie spam.

#### 5.4.4.4 Zakładka Raporty

W oknie raportów program odnotowuje wszystkie czynności związane z wykryciem wirusów. Administrator programu może wykonać wybraną akcję klikając dwukrotnie raport o wykryciu wirusa lub korzystając z menu kontekstowego prawego klawisza myszy. Można zdezynfekować i przywrócić plik, usunąć go lub przenieść do Kwarantanny.

---



Można sortować raporty klikając nagłówki kolumn:

- Status: To streszczenie raportu. Odpowiednie symbole podkreślają stopień ważności i rodzaj raportu.
- Komputer: Nazwa komputera, z którego pochodzi protokół. W przypadku grupy, uwidocznione są nazwy wszystkich komputerów danej grupy.
- Data/godzina: Data powstania protokołu (wykrycie infekcji lub zlecenie).
- Zgłaszający: Informacja, czy raport sporządził skaner wirusowy, strażnik czy też moduł chroniący pocztę.
- Wirus: Nazwa wykrytego wirusa, o ile jest znana.
- Plik/Wiadomość: Lista zainfekowanych lub podejrzanych plików. W przypadku wiadomości podany jest także adres jej nadawcy.
- Folder: Informacje dotyczące folderu, w którym wykryto wirusa są istotne w przypadku przeniesienia pliku do Kwarantanny – po usunięciu

wirusa będzie można przywrócić plik w pierwotne miejsce.

Wyjaśnienie funkcji paska narzędzi widoku Raport - od lewej do prawej.

- **Odśwież:** Odświeża widok. Wczytuje aktualne raporty z Serwera G Data AntiVirus.
  - **Usuń:** Usuwa wybrane raporty. Jeśli chcesz usunąć raporty Kwarantanny program zapyta, czy wraz z raportami mają zostać usunięte pliki z folderu Kwarantanny.
  - **Drukuj:** Funkcja ta umożliwia wydruk raportów. Przed rozpoczęciem drukowania program zapyta jakie szczegóły chcesz uwzględnić.
  - **Widok strony:** Funkcja ta umożliwia podgląd układu strony przed wydrukiem.
  - **Dezynfekuj plik:** Próbuje usunąć wirusa z pliku.
  - **Przenieś plik do Kwarantanny:** Przenosi plik do folderu Kwarantanny.
  - **Usuń plik:** Usuwa plik z dysku Klienta.
  - **Przywróć z Kwarantanny:** Przywraca plik z folderu Kwarantanny na dysk Klienta. Uwaga: Plik zostanie odtworzony w pierwotnej lokalizacji lecz będzie nadal zainfekowany.
  - **Wyczyść plik i przywróć z Kwarantanny:** Wirus zostaje usunięty z folderu Kwarantanny i przywrócony na dysk Klienta. Program nie przywraca pliku, jeśli wirusa nie da się usunąć.
  - **Ukryj zależne raporty:** Funkcja ukrywa wszystkie wcześniejsze raporty dotyczące tego samego pliku.
  - **Ukryj raporty dotyczące spakowanych plików:** Ukrywa raporty dotyczące wykrycia wirusów w archiwach.
  - **Pokaż wszystkie raporty:** Wyświetla wszystkie dostępne raporty.
  - **Pokaż raporty dotyczące nie usuniętych wirusów:** Wyświetla wszystkie raporty, które sygnalizują, że wirus nie został
-

usunięty.

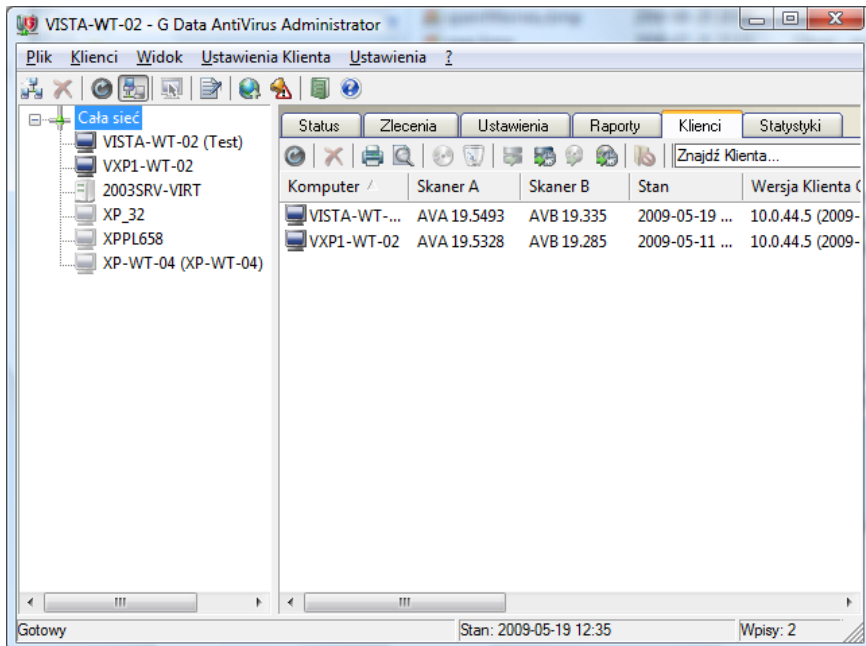
- Pokaż raporty Kwarantanny: Wyświetla raporty dotyczące przeniesienia plików do Kwarantanny.
- Pokaż zawartość Kwarantanny: Wyświetla zawartość folderu Kwarantanny

Dodatkową opcją jest możliwość wyeksportowania raportów do pliku XLS. Eksport dostępny jest po kliknięciu zaznaczonych raportów prawym klawiszem i wybraniu polecenia Eksportuj raporty (infekcje).

Dwukrotne kliknięcie wierszu raportu otwiera okno właściwości raportu. Okno raportu z wykrycia wirusa umożliwia usunięcie pliku, przeniesienie go do Kwarantanny lub dezynfekcję (jeśli plik nie został uszkodzony przez wirusa).

### 5.4.4.5 Zakładka Klienci

Po kliknięciu nazwy stacji roboczej, grupy lub ikony Cała sieć w drzewie po prawej stronie, w widoku Klienci pojawi się spis wszystkich Klientów zainstalowanych w danej grupie.



Można sortować widok klikając nagłówki poszczególnych kolumn:

- Komputer: Nazwa stacji roboczej.
- Skaner A/B: Numer wersji bazy wirusów i data ostatniej aktualizacji.
- Wersja Klienta G Data AntiVirus: Numer wersji składnika Klient.
- Ostatnie logowanie: Data ostatniej próby połączenia Klienta z serwerem zarządzającym.
- Aktualizacja sygnatur wirusów: Stan wykonania aktualizacji baz wirusów.
- Data/godzina: Data rozpoczęcia ostatniej aktualizacji bazy wirusów.

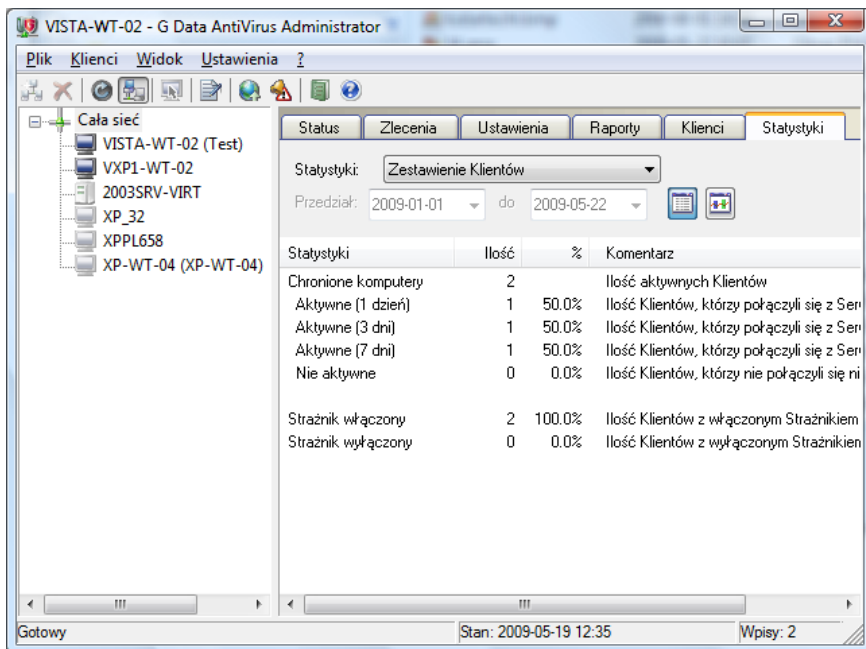
- Aktualizacja plików: Stan wykonania aktualizacji plików modułu Klient.
- Data/godzina: Data rozpoczęcia ostatniej aktualizacji plików modułu Klient.
- Foldery wyjątków: Tu wyświetlane są nazwy folderów pomijanych przy skanowaniu.

Wyjaśnienie ikon paska narzędzi w widoku Klienta - od lewej do prawej:

- Odśwież: Odświeża widok okna. Wczytuje aktualne ustawienia z Serwera G Data AntiVirus.
- Usuń: Przycisk ten usuwa zaznaczonego Klienta z grupy.
- Drukuj: Funkcja ta umożliwia wydruk ustawień. Przed wydrukiem można wybrać elementy do wydruku.
- Widok strony: Funkcja ta umożliwia podgląd układu strony przed wydrukiem.
- Zainstaluj Klienta: Instaluje moduł Klient. Instalacja jest możliwa tylko wtedy, kiedy komputery spełniają określone wymagania.
- Odinstaluj Klienta: Polecenie powoduje odinstalowanie składnika Klient z komputera.
- Aktualizuj sygnatury wirusów: Aktualizuje bazy wirusów Klienta.
- Automatyczna aktualizacja sygnatur wirusów: Uruchamia automatyczną aktualizację baz wirusów składnika Klient.
- Aktualizuj pliki programu: Aktualizuje pliki składnika Klient. Po aktualizacji może być wymagane ponowne uruchomienie komputera.
- Automatyczna aktualizacja plików programu: Uruchamia automatyczną aktualizację plików modułu Klient.
- Edytuj wyjątki: Funkcja pozwala definiować katalogi pomijane przy skanowaniu.

#### 5.4.4.6 Zakładka statystyki

Widok zawiera statystyki dotyczące ataków wirusów. Można przejrzeć ogólne informacje dotyczące relacji składnika ManagementServer i Klientów, a także dane o najczęściej występujących wirusach i najczęściej atakowanych komputerach. Istnieje możliwość graficznego przedstawienia statystyk w postaci wykresów. W tym celu należy kliknąć ostatni przycisk w pasku narzędzi.



## 6 G Data AntiVirus Klient

Składnik Klient chroni stacje robocze w tle i generalnie nie wymaga ingerencji użytkowników. Stacje robocze wyposażone są we własne sygnatury wirusów i mają możliwość samodzielnej aktualizacji (przydatne w przypadku komputerów mobilnych).

## 6.1 Instalacja składnika G Data AntiVirus Klient



Składnik Klient realizuje ochronę antywirusową komputerów wykonując polecenia składnika ManagementServer. Instalacja Klienta może przebiegać zdalnie z modułu Administratora.

Jeśli nie jest to pożądane lub możliwe, można zainstalować oprogramowanie klienckie ręcznie, bezpośrednio na stacjach roboczych. Aby zainstalować Klienta ręcznie, włóż do napędu komputera płytę z zakupionym oprogramowaniem i uruchom instalację składnika Klient. Administrator umożliwia także utworzenie pakietu cichej instalacji do rozdelenia np. przy pomocy skryptów logowania.

W trakcie instalacji ręcznej program zapyta o nazwę lub adres IP komputera, na którym zainstalowany jest składnik ManagementServer. Wskazanie komputera z serwerem zarządzającym jest niezbędne do uzyskania komunikacji między składnikami Klient i ManagementServer.

Opis instalacji składnika Klient w systemach Linux znajdziesz w rozdziale: Instalacja składnika Klient w systemach Linux.

## 6.2 Instalacja składnika Klient w systemach Linux

Produkt umożliwia zainstalowanie ochrony antywirusowej G Data na stacjach roboczych z różnymi dystrybucjami systemu Linux. Podobnie jak Klient dla systemu Windows, linuksowe oprogramowanie klienckie może być zarządzane i aktualizowane zdalnie przez składnik G Data ManagementServer.

Istnieje również możliwość zainstalowania oprogramowania na komputerach z systemem Linux udostępniających udziały komputerom z systemem Windows (wykorzystując protokół SMB). Klient dla serwera Samba nie dopuści do zapisania zawirusowanego pliku w udziale, ani do skopiowania wirusa z udziału na stację roboczą Windows.

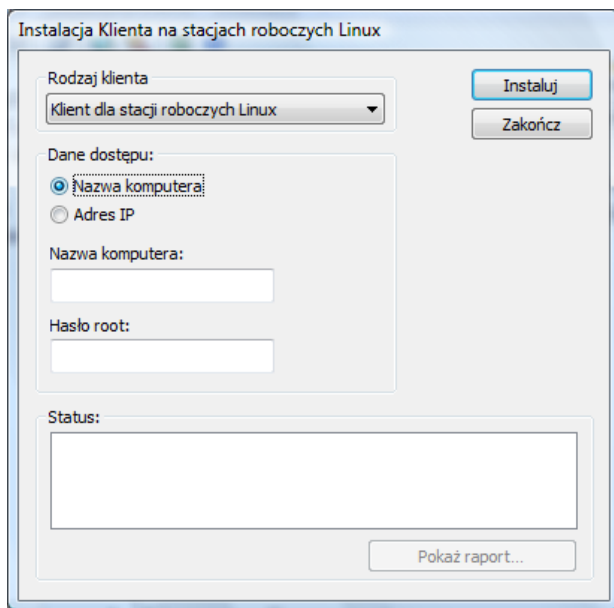
Klient linuksowy dla stacji roboczych funkcjonuje w systemach z

kernelem od wersji 2.6.25 wwyż. (Ubuntu 8.10, Debian 5.0, Suse Linux Enterprise Desktop 11 i inne aktualne dystrybucje).

Klienta dla serwerów plików Samba można zainstalować w każdym dostępnym systemie Linux.

Aby zdalnie zainstalować oprogramowanie w systemie Linux, przeprowadź następujące kroki:

- 1 Uruchom w menu Ustawienia Klienta polecenie Zainstaluj klienta G Data AntiVirus dla systemu Linux. Pojawi się okno umożliwiające wskazanie stacji roboczej lub serwera z systemem Linux.



- 2 Wpisz adres IP komputera, na którym chcesz zainstalować oprogramowanie klienckie. W przypadku instalacji klienta na serwerze Samba, możesz także zastosować nazwę komputera.
  - 3 Wpisz hasło roota systemu Linux. Hasło jest niezbędne do zdalnej instalacji Klienta. Dystrybucje funkcjonujące w oparciu o polecenie
-

sudo, stanowią tu wyjątek.

- 4 Kliknij przycisk Instaluj aby rozpocząć instalację.

Aby zainstalować oprogramowanie ręcznie, na stacji roboczej lub serwerze Samba:

Płyta instalacyjna zawiera specjalny folder z pakietami instalacyjnymi dla systemów Linux.

- installersmb.bin = Instalator dla serwera Samba
- installerws.bin = Instalator dla stacji roboczych

Skopiuj pliki instalacyjne na komputer z systemem Linux i uruchom odpowiedni instalator.

Możesz skopiować na komputer docelowy również plik zawierający sygnatury wirusów. Nie jest to obowiązkowe, ponieważ po połączeniu z serwerem zarządzającym Klient sam pobierze sygnatury wirusów:

- signatures.tar = Archiwum z sygnaturami wirusów

## 6.3 Konfiguracja składnika Klient w systemach Linux

- 1 Aby sprawdzić, czy procesy programu są uruchomione, wykonaj z poziomu wiersza poleceń

```
linux:~# ps ax|grep av
```

Wynik powinien być następujący:

```
...    Ssl    0:07 /usr/sbin/avkserver --daemon
```

```
...    Ssl    0:05 /usr/sbin/avguard --daemon
```

Niezależnie od stosowanej dystrybucji, procesy można uruchamiać i wyłączać poleceniami

```
linux:~# /etc/init.d/avkserver start  
linux:~# /etc/init.d/avkserver stop
```

```
linux:~# /etc/init.d/avclient start  
linux:~# /etc/init.d/avclient stop
```

Do wykonania tych poleceń niezbędne są uprawnienia administratora (root).

- 2 Logi programu znajdują się w folderze /var/log/avk w postaci plików avk.log i remote.log. Plik avk.log rejestruje wyniki skanowania procesu avkserver, plik remote.log rejestruje wyniki działania procesu avkremote, ustanawiającego połączenie z modułem G Data ManagementServer. W przypadku wystąpienia problemów można zajrzeć do tych plików i sprawdzić, czy nie pojawiają się w nich komunikaty o błędach. Pliki mogą rejestrować zdarzenia bardziej szczegółowo niż domyślnie. Aby uzyskać bardziej szczegółowe raporty, należy w plikach etc/gdata/gdav.ini oraz /etc/gdata/avclient.cfg zmienić wartość parametru LogLevel na 7.

Uwaga: Wyższa wartość parametru LogLevel powoduje generowanie dużej ilości raportów i szybki wzrost rozmiarów plików .log. Zaleca się używanie tego trybu tylko w celach diagnostycznych.

- 3 Polecenie avkclient dostępne z wiersza poleceń umożliwia sprawdzenie wersji baz wirusów a także wykonanie skanowania danego folderu lub pliku:

```
linux:~$ avkclient avkversion - zwraca wersję i datę aktualizacji  
baz wirusów
```

```
linux:~$ avkclient version - zwraca numer wersji baz wirusów w  
skrótowej formie
```

```
linux:~$ avkclient scan:<file> - skanuje plik <file> i wyświetla  
wynik skanowania
```

---

- 
- 4 Plik `/etc/gdata/avclient.cfg` jest plikiem konfiguracyjnym składnika służącego do komunikacji z Serwerem zarządzającym. Należy sprawdzić, czy parametr `MainMMS` wskazuje komputer z zainstalowanym składnikiem `ManagementServer`. Parametr można zmodyfikować ręcznie, lub spróbować usunąć i ponownie uaktywnić komputer z serwerem Samba w oknie składnika Administrator.
- 5 Aktywacji ochrony antywirusowej zasobów serwera Samba dokonuje się poprzez wpis:

```
vfs objects = gdvfs
```

w pliku konfiguracyjnym serwera Samba, zazwyczaj `/etc/samba/smb.conf`. Jeżeli wpis znajduje się w sekcji `[global]`, chronione będą wszystkie skonfigurowane zasoby. Aby chronić tylko wybrane zasoby Samba, należy umieścić powyższy wiersz w sekcji każdego zasobu, który ma być chroniony. W przypadku wystąpienia problemów można wyłączyć ten wiersz z użycia stawiając na początku znak `#`, np. po to, żeby stwierdzić, czy zasoby funkcjonują poprawnie bez ochrony antywirusowej. Jeżeli to nie pomaga, trzeba poszukać przyczyn problemów w konfiguracji serwera Samba.

- 6 Aby sprawdzić, czy proces Strażnika jest włączony, uruchom polecenie:

```
ps ax|grep avguard
```

Strażnik potrzebuje modułów kernela `redirfs` i `avflt`. Możesz sprawdzić poleceniem `lsmod`, czy moduły są wczytane: `lsmod|grep redirfs` i `lsmod|grep avflt`...

Moduły muszą być wkompileowane w stosowany kernel.

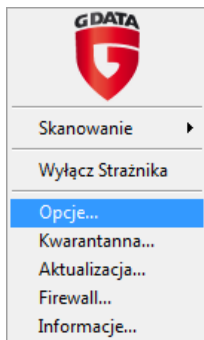
Dbaj o to składnik Dynamic Kernel Module System (DKMS), jeżeli jest zainstalowany wraz z odpowiednimi pakietami Kernel-Header. W takim przypadku, DKMS automatycznie kompiluje i instaluje moduły. Plik dziennika Strażnika znajduje się w lokalizacji `/var/log/gdata/avguard.log`.

## 6.4 Ikona Klienta



Po zainstalowaniu Klienta na stacji roboczej, w zasobniku systemowym Windows pojawi się ikona Klienta pozwalająca użytkownikowi na wykonywanie zadań określonych w ustawieniach składnika Administrator

Kliknij prawym klawiszem ikonę Klienta, aby otworzyć menu kontekstowe.

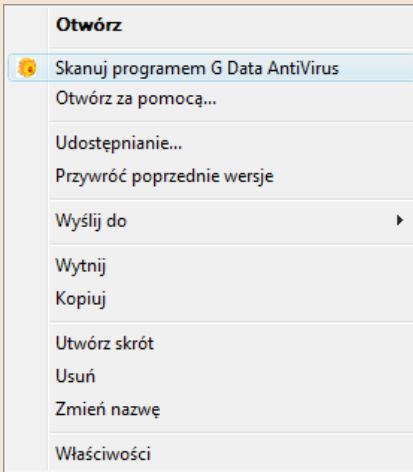


### 6.4.1 Skanowanie

Użytkownik stacji roboczej ma możliwość ręcznego uruchomienia skanowania komputera, napędu, pamięci lub określonych zasobów, o ile w module Administrator włączone jest uprawnienie do samodzielnego skanowania.

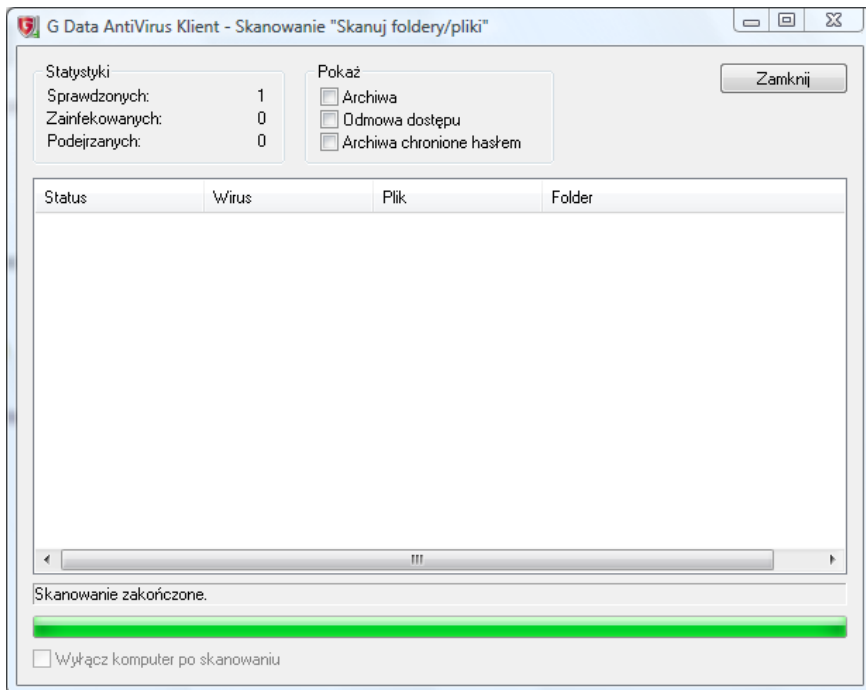
---

Możliwe jest także skanowanie obiektów z menu kontekstowego Eksploratora Windows przy użyciu prawego klawisza myszy.



W trakcie trwania skanowania menu ikonki Klienta powiększa się o następujące pozycje:

- **Priorytet skanowania:** Im wyższy priorytet, tym skanowanie trwa krócej, i tym bardziej obciążony jest system i działanie innych programów. Skanowanie z niskim priorytetem trwa najdłużej, ale w jego trakcie można pracować na stacji bez większych trudności.
- **Wstrzymaj skanowanie:** Po wstrzymaniu skanowania można je wznowić w dowolnym momencie.
- **Przerwij skanowanie:** Jeżeli w module Administrator włączone jest uprawnienie do modyfikacji ustawień, użytkownik może przerwać okresowe lub jednorazowe skanowanie uruchomione zdalnie.
- **Pokaż okno skanowania:** Ta opcja otwiera okno skanowania. Okno wyświetla informacje o przebiegu i postępie skanowania.



## 6.4.2 Wyłącz Strażnika

To polecenie umożliwia czasowe wyłączenie Strażnika składnika G Data AntiVirus Klient (maksymalnie do kolejnego uruchomienia komputera). Jest to możliwe tylko wtedy, gdy w składniku Administrator ustawione jest odpowiednie uprawnienie użytkowników tej stacji roboczej. Zaleca się nadawanie tego uprawnienia tylko zaufanym i odpowiednio przeszkolonym użytkownikom.

### 6.4.3 Opcje...

W zależności od ustawień administratora dla danego komputera, użytkownik ma dostęp do maksymalnie pięciu zakładek okna opcji programu Klient.

Uwaga: Nadanie użytkownikom pełnych uprawnień, umożliwi wyłączenie Strażnika i zatrzymanie procesu skanowania. Zalecamy nadawanie pełnych uprawnień do obsługi oprogramowania Klientkiego tylko zaufanym i przeszkolonym użytkownikom.

Jeżeli do stacji roboczej ma dostęp więcej niż jeden zaufany użytkownik, można zabezpieczyć dostęp do ustawień hasłem, znanym tylko tej osobie. Dzięki temu inni użytkownicy komputera nie będą mogli modyfikować ustawień narażając system na infekcję.

Ustawianie uprawnień możliwe jest w oknie składnika Administrator, w zakładce Ustawienia > Ogólne. Opis poszczególnych uprawnień znajdziesz w rozdziale Uprawnienia Klienta.

Opisy poszczególnych zakładek opcji Klienta znajdziesz w rozdziale Zakładka Ustawienia.

### 6.4.4 Kwarantanna...

W oknie lokalnej Kwarantanny wyświetlone są wszystkie pliki przeniesione do Kwarantanny przez monitor antywirusowy i procesy skanowania. Użytkownik może dokonać próby dezynfekcji i przywrócenia pliku, a także usunąć plik z folderu Kwarantanny.

Uwaga: Przywrócenie zainfekowanego pliku może wywołać wtórną infekcję stacji roboczej. Zaleca się stosowanie tej funkcji tylko w przypadku, kiedy chodzi o potwierdzony fałszywy alarm, lub jeśli system operacyjny wymaga danego pliku do działania.

### 6.4.5 Aktualizacja...

To okno umożliwia przeprowadzenie aktualizacji baz wirusów, nawet gdy komputer (np. laptop) nie jest podłączony do sieci ze składnikiem ManagementServer. Jest to przydatne w przypadku komputerów mobilnych, przebywających czasem dłuższy czas poza firmą.

Przycisk Ustawienia i planowanie umożliwia skonfigurowanie harmonogramu automatycznych aktualizacji sygnatur wirusów.

### 6.4.6 Firewall...

Użytkownik z uprawnieniami do edycji ustawień zapory może tym poleceniem otworzyć interfejs użytkownika składnika Firewall. Szczegóły na temat obsługi zapory znajdziesz w rozdziale G Data Firewall. Nie ma możliwości centralnego zarządzania ustawieniami zapory.

### 6.4.7 Informacje...

Polecenie Informacje pozwala sprawdzić datę sygnatur wirusów i numer wersji składnika Klient.

## 7 G Data AntiVirus WebAdministrator



WebAdministrator to oprogramowanie umożliwiające zarządzanie składnikiem ManagementServer przez przeglądarkę internetową

---

---

## 7.1 Instalacja składnika WebAdministrator

Do zainstalowania składnika WebAdministrator wymagane jest zainstalowanie platformy .NET Framework, a także włączenie następujących funkcji systemu Windows:

- Funkcja Kompatybilność metabazy IIS i konfiguracji IIS 6
- Funkcja Usługi WWW serwera IIS

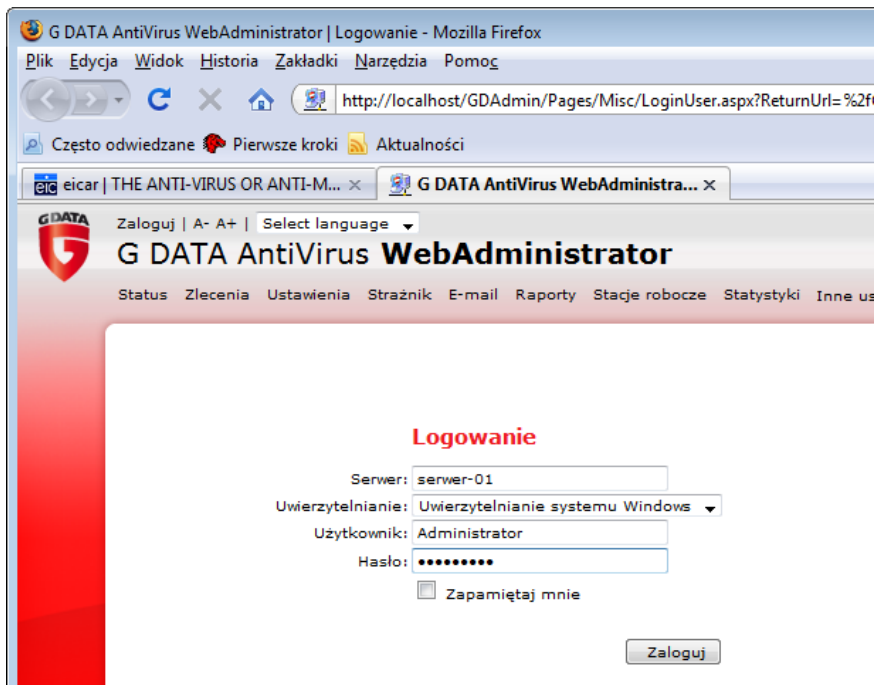
Po zainstalowaniu składnik WebAdministrator wymagane.



Po zainstalowaniu składnika WebAdministrator na pulpicie pojawi się skrót do przeglądarki internetowej otwierający okno logowania do usługi zarządzania programem przez serwis WWW.

## 7.2 Obsługa składnika WebAdministrator

Aby uruchomić składnik, kliknij ikonkę skrótów na pulpicie. Otworzy się strona przeglądarki z oknem logowania do składnika WebAdministrator.



Wpisz te same dane dostępu, których używasz do logowania do standardowego składnika Administrator. Obsługa Web Administratora nie różni się prawie wcale obsługi standardowego składnika G Data AntiVirus Administrator.

G DATA AntiVirus WebAdministrator | Status - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

http://localhost/GDAdmin/Default.aspx

Często odwiedzane Pierwsze kroki Aktualności

Czy Firefox ma zapamiętać wprowadzone hasło?

Wyloguj - Administrator | A- A+ | Select language

## G DATA AntiVirus WebAdministrator

Status Zlecenia Ustawienia Strażnik E-mail Raporty Stacje robocze Statystyki Inne ustawienia ▶

Cała sieć

- VISTA-WT-02

### G DATA AntiVirus Status - Cała sieć

	Klient G DATA AntiVirus jest zainstalowany	1 / 1
	Bazy wirusów aktualne	0 / 1
	Strażnik włączony	1 / 1
	Ochrona poczty włączona	1 / 1
	Skaner OutbreakShield włączony	1 / 1

## 8 G Data Firewall

Klient Firewall jest oprogramowaniem pełniącym funkcje zapory internetowej przeznaczonym na stacje robocze. Zapora chroni komputery działające pod kontrolą systemu operacyjnego Windows przed nieautoryzowanym dostępem do danych oraz przed atakami hakerów działających w sieci lokalnej oraz w Internecie.

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.

## 8.1 Instalacja składnika Firewall



Składnik G Data Firewall instaluje się na stacji roboczej wraz z oprogramowaniem Klientkim. Ręczna instalacja składnika Firewall możliwa jest dopiero po zainstalowaniu składnika Klient.

## 8.2 Obsługa składnika Firewall

Zapora sieciowa instaluje się w trybie autopilota i nie wymaga ingerencji użytkownika w ustawienia. Tryb ręczny wymaga od użytkownika wiedzy z zakresu zagadnień ochrony sieci przed atakami i nie jest zalecany dla użytkowników bez specjalnego przeszkolenia. Jeżeli włączysz użytkownikowi uprawnienie do edycji ustawień zapory, może on otworzyć okno interfejsu graficznego zapory przez polecenie Firewall... w menu kontekstowym ikony Klienta.

### 8.2.1 Widok Status

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

Przez podwójne kliknięcie (lub przez zaznaczenie wpisu i kliknięcie przycisku Edycja) można przejść do okna umożliwiającego modyfikację danego ustawienia programu. Po usunięciu przyczyny ostrzeżenia symbol ostrzeżenia zniknie.

- **Skuteczność:** 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 tworzenie 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.
- Zarejestrowane 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.

## 8.2.2 Widok Sieci

Widok sieci przedstawia połączenia sieciowe (np. LAN, dial-up) Twojego komputera. Okno informuje również o zestawie reguł 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. Szczegóły na temat modyfikacji i tworzenia zestawów reguł znajdziesz w rozdziale Firewall > Zestaw reguł.

### 8.2.2.1 Właściwości połączenia

W oknie właściwości 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, 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.
- 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 Firewall > Zestaw reguł.

### 8.2.3 Widok Zestaw reguł

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

Tryb ukrycia to ustawienie ukrywające adres IP komputera. Ma to na celu utrudnienie potencjalnym hakerom uzyskania informacji o portach otwartych w systemie. Uzyskanie takich informacji umożliwia przeprowadzanie bardziej zaawansowanych ataków na komputer.

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.

#### 8.2.3.1 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 nieznanym 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** i **Tryb zaawansowany**.

Opis działania automatycznego generowania zapytań opisany jest w rozdziale **Firewall > Zestaw reguł > Półautomatyczne tworzenie reguł**.

## **Asystent tworzenia reguł**

Przy pomocy **Asystenta tworzenia reguł** użytkownik może 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 użytkownik może 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:

- Akceptuj lub blokuj dostęp wybranej 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.
  - Udostępnij lub zablokuj określoną usługę internetową (port): 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).
  - Akceptuj lub blokuj dostęp do plików i drukarek (NetBIOS): NetBIOS to specjalny interfejs w sieciach komputerowych, który może być wykorzystywany np. do akceptacji dostępu do plików i drukarek bezpośrednio z komputera do komputera, bez wykorzystywania przy tym protokołu TCP/IP. Jako że nie jest to konieczne w sieciach domowych, a NetBIOS może być wykorzystywany przez hakerów do ataków na komputer użytkownika, zaleca się zablokowanie portów NetBIOS w sieciach niezaufanych.
-

- Akceptuj lub blokuj usługi domen: 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.
- Zezwól na współdzielenie 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.
- Przełącz na tryb zaawansowany: W ten sposób użytkownik może przejść z trybu Asystenta tworzenia reguł do trybu zaawansowanego.

Wyłączenie opcji Uruchamiaj Asystenta reguł również w przyszłości, spowoduje, że program będzie wyświetlał okno zaawansowanej konfiguracji reguł zamiast Asystenta tworzenia reguł.

## 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 aplikacji, 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.
- Ręcznie, poprzez kliknięcie przycisku Nowy w widoku trybu zaawansowanego.
- 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 myszą 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
-

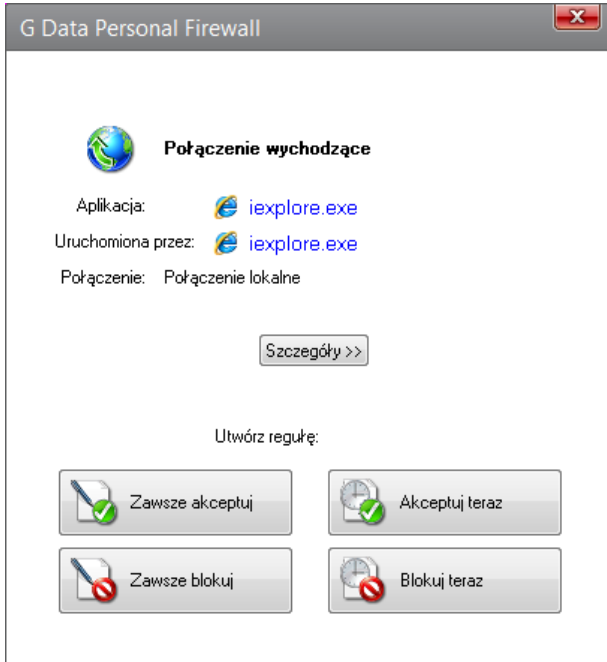
---

komentarz dla reguł generowanych ręcznie.

- **Kierunek połączenia:** To ustawienie definiuje, czy chodzi w danym przypadku o regułę dla połączeń wychodzących, przychodzących czy dla obojgu 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.

### **8.2.3.2 Półautomatyczne tworzenie reguł**

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, znowo zapyta 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, znowo zapyta o pozwolenie.
-

---

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

## 8.2.4 Widok Protokół

Widok Protokół 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.

## 8.2.5 Opcje zapory

Widok Opcje służy do modyfikowania zaawansowanych ustawień funkcji zapory. Jeżeli korzystasz z trybu autopilota, zaporą działa w pełni automatycznie i nie wymaga zaawansowanej konfiguracji.

### 8.2.5.1 Tryb automatyczny

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 zaporą bardzo często wyświetla zapytania.
- **Wysoka skuteczność:** Reguły zapory są definiowane bardzo szczegółowo. To ustawienie wymaga dobrej znajomości zagadnień sieciowych (TCP/IP, porty, itd.). Zaporą 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 zapora 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.

### 8.2.5.2 Zapytania

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

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

Dla protokołu/portu/aplikacji: Dla aplikacji jeśli są przynajmniej \_\_ zapytania: Są aplikacje (jak np. Microsoft Outlook), które podczas żądania odpytują jednocześnie kilka portów względnie korzystają jednocześnie w różnych protokołach. Ponieważ ustawienie Dla protokołu/portu/aplikacji prowadziłyby to do pojawiania się wielu zapytań, można zastosować tę opcję w celu uproszczenia obsługi zapory.

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.

- Bufor: Zapora może wiązać ze sobą stale powtarzające się żądania połączenia jednej aplikacji. Podczas kolejnych prób uzyskania połączenia
-

---

okno dialogowe nie będzie się pojawiać częściej niż ustalona wartość, np. co 20 sekund.

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

Opcja Wykrywaj nieznane aplikacje serwerowe przy uruchamianiu programu powinna być zawsze włączona, ponieważ w przeciwnym przypadku złośliwe aplikacje, które znajdowały się w komputerze jeszcze.

- Niechronione sieci: Zapora może funkcjonować prawidłowo tylko wtedy, gdy wszystkie połączenia, do których chroniony komputer ma dostęp będą przez nią rozpoznane i monitorowane. Zaleca się pozostawienie włączonych opcji Informuj natychmiast o nowych nie chronionych połączeniach oraz Wykrywaj niechronione połączenia sieciowe przy uruchamianiu programu.

### 8.2.5.3 Ataki

Zalecamy pozostawienie poniższych ustawień bez zmian. Po całkowitym wyłączeniu systemu wykrywania ataków spowoduje obniżenie poziomu bezpieczeństwa podczas pracy z Internetem.

Zapora umożliwia wykrywanie metod najczęściej stosowanych ataków DoS (SYN Flood, UDP Flood, ICMP Flood), Ping of death, Land, Helkern oraz SmbDie jak również skanowania portów, które może poprzedzać groźniejszy atak:

- Atak Port Scans (skanowanie portów) obejmuje wykrywanie otwartych portów na komputerze. Poszukiwane są słabe punkty komputera, po wykryciu których zwykle następuje bardziej niebezpieczny atak. Możliwe jest zdefiniowanie następujących ustawień dla ataku tego typu: Liczba portów: - liczba portów, które próbuje otwierać zdalny komputer, oraz Czas (sek), w ciągu którego następuje otwieranie portów.
- Atak Ping of Death polega na wysyłaniu do komputera pakietów ICMP o rozmiarze większym niż 64K (wartość graniczna). Może to spowodować nagłe zakończenie działania systemu operacyjnego.

- Atak Land polega na transmisji do komputera żądań połączenia do samego siebie. W rezultacie zapętlenia się komputera, procesor zostaje obciążony podnosząc prawdopodobieństwo nagłego zakończenia działania systemu operacyjnego.
- Atak SYN Flood polega na wysyłaniu do komputera żądań nawiązania połączenia. System rezerwuje odpowiednie zasoby dla każdego żądania, co powoduje, że system przestaje odpowiadać na żądanie połączeń z innych źródeł. Możliwe jest zdefiniowanie następujących ustawień dla taktu tego typu: Liczba połączeń: - liczba połączeń, które próbuje ustanowić zdalny komputer, oraz Czas (sek), w ciągu którego następują połączenia.
- Atak UDP Flood polega na wysyłaniu specjalnych pakietów UDP, które są w nieskończoność transmitowane pomiędzy zaatakowanymi komputerami. W rezultacie atak absorbuje znaczną część zasobów sieciowych. Możliwe jest zdefiniowanie następujących ustawień dla taktu tego typu: Liczba pakietów UDP: - liczba przychodzących pakietów UDP, oraz Czas (sek), w ciągu którego przychodzą pakiety.
- Atak ICMP Flood polega na wysyłaniu do komputera pakietów ICMP co powoduje wzrost obciążenia procesora atakowanego komputera, ponieważ musi ona odpowiadać na każdy pakiet. Możliwe jest zdefiniowanie następujących ustawień dla taktu tego typu: Liczba pakietów ICMP: - liczba przychodzących pakietów ICMP, oraz Czas (sek), w ciągu którego przychodzą pakiety.
- Atak Helkern polega na wysyłaniu do atakowanego komputera specjalnego pakietu UDP, który może ułatwić uruchomienie złośliwego kodu. Powoduje to spadek szybkości połączenia z Internetem.
- Atak SMB Die polega na próbie ustanowienia połączenia SMB; jeśli atak powiedzie się do komputera przesyłany jest specjalny pakiet powodujący przeładowanie jego bufora. W rezultacie użytkownik musi ponownie uruchomić system. Na ten typ ataku podatne są systemy operacyjne Windows 2k/XP/NT.
- Atak Lovesan wykorzystuje lukę w usługach terminalowych DCOM RPC systemów operacyjnych Windows NT 4.0/2000/XP/2003. Po wykryciu luki na zainfekowany komputer pobierany jest robak internetowy umożliwiający nadawcy nieautoryzowany dostęp do komputera i wykonywanie na nim określonych operacji.

Pola zaznaczenia w pierwszej kolumnie określają, czy atak ma być

---

tylko protokołowany, czy też powinien zostać wyświetlony odpowiedni komunikat.

#### 8.2.5.4 Inne

Ta zakładka umożliwi skonfigurowanie następujących parametrów zapory:

- **Sprawdzanie sum kontrolnych:** Program oblicza sumy kontrolne filtrowanych aplikacji na podstawie rozmiaru pliku oraz innych kryteriów. Jeśli suma kontrolna ulegnie zmianie, może to oznaczać że program został zmodyfikowany przez złośliwą aplikację. W takim wypadku zaporą zadziała wyświetlając alarm. Opcja Sprawdzaj wczytane moduły powoduje, że podobnie jak aplikacje, sprawdzane są także używane przez nie moduły (np. biblioteki DLL). Ponieważ moduły ulegają częstym zmianom i aktualizacjom, konsekwentne sprawdzanie sum kontrolnych wszystkich modułów może powodować dużo niepokojących lecz fałszywych alarmów. Każdorazowa zmiana modułu pociągałaby za sobą zapytania zapory. Na co dzień wystarczy kontrolować tylko sumy zmodyfikowanych modułów.
- **Zmodyfikowane pliki:** To ustawienie pozwala użytkownikowi wybrać reakcję na wykrycie zmian referencyjnych w plikach. Program G Data AntiVirus Klient może automatycznie sprawdzać zmodyfikowane pliki pod kątem zagrożeń. Można również ustawić opcję Zapytaj użytkownika i podjąć decyzję w momencie wykrycia zmian referencyjnych.
- **Zestaw reguł:** Tutaj użytkownik może określić, czy tworzenie nowych reguł ma się odbywać za pomocą Asystenta tworzenia reguł czy poprzez tryb zaawansowany. Początkującym użytkownikom zalecamy korzystanie z Asystenta tworzenia reguł.

Program umożliwia przejście z trybu Asystenta tworzenia reguł na tryb zaawansowany i odwrotnie w dowolnej chwili. W tym celu w trybie asystenta wybierz przycisk Przełącz na tryb zaawansowany. W trybie zaawansowanym kliknij przycisk Asystent... aby przejść do trybu podstawowego.

- **Protokół połączenia:** Tu użytkownik może ustalić, jak długo zaporą ma przechowywać informacje o połączeniach.
- **Autopilot:** W przypadku korzystania z aplikacji działających w trybie

pełnoekranowym - np. gier online, męczące jest zatwierdzanie reguł zapory internetowej w trakcie działania gry lub programu. Funkcja autopilota pozwala na bezproblemowe korzystanie z gier i programów łączących się z Internetem bez potrzeby zatwierdzania reguł w momencie nawiązywania połączenia z Internetem. Jeżeli opcja automatycznego uruchamiania autopilota jest aktywna, program zareaguje w momencie przełączania w tryb pełnoekranowy i zapyta czy uaktywnić autopilota.

---