

The logo for VirusBuster, featuring the word "VirusBuster" in a bold, white, sans-serif font. The letter "V" is stylized with a yellow arrow pointing upwards and to the right, and a yellow underline. The background of the entire page is a dark blue gradient with several light blue, curved, overlapping bands that create a sense of motion or flow.

**VirusBuster**

for Mail Servers - GroupWise

## SPIS TREŚCI

<b>VIRUSBUSTER FOR MAIL SERVERS (GROUPWISE)</b> .....	<b>2</b>
<b>Minimalne wymagania systemowe</b> .....	<b>2</b>
<b>Instalacja</b> .....	<b>3</b>
Instalacja automatyczna .....	3
Instalacja manualna .....	4
<b>Struktura programu</b> .....	<b>6</b>
Interfejs użytkownika .....	6
<b>Szczegółowy opis</b> .....	<b>7</b>
General settings - Ustawienia ogólne .....	7
Internet Agent protection – Ochrona agenta internetowego .....	8
Post Office protection – Ochrona poczty trybu Post Office.....	15
<b>END USER AGREEMENT</b> .....	<b>19</b>
<b>CONTACT</b> .....	<b>20</b>

## VIRUSBUSTER FOR MAIL SERVERS (GROUPWISE)

Obecnie większość wirusów i szkodliwych programów rozprzestrzenia się poprzez pocztę elektroniczną, dlatego filtrowanie poczty firmowej jest niezbędne w celu zabezpieczenia się przed działaniem szkodników. Gwałtowny wzrost liczby spamu przeciąża serwery a usuwanie niechcianych maili bywa czasochłonne, dlatego każdy produkt filtrujący pocztę musi posiadać efektywny filtr spamu.

Program może być zainstalowany jako moduł VirusBuster for NetWare Servers. Zintegrowany z systemem pocztowym, VirusBuster for Mail Servers (GroupWise) zapewnia stałą ochronę sieci przed wirusami, złośliwym kodem oraz spamem. Moduł ochrony serwerów pocztowych Post Office zapewnia zabezpieczenie antywirusowe dla znalezionych w systemie serwerów pocztowych IMAP.

Cechy programu:

- Ogromna wydajność, jaką gwarantuje silnik skanowania wirusów.
- Modułowa architektura ułatwiająca użytkowanie.
- Skanowanie poczty wychodzącej oraz przychodzącej, usuwanie wszystkich pojawiających się wirusów.
- WormBuster natychmiast blokujący robaki internetowe.
- Zamiana załączników zarażonych wirusem na załączniki z ostrzeżeniem.
- Biała lista (lista permisyjna).
- Udoskonalone systemy powiadamiania i rejestru zdarzeń: możliwość wysłania powiadomienia do administratora i/lub nadawcy wiadomości.
- Automatyczna aktualizacja bazy danych poprzez FTP.
- Tradycyjny, łatwy w użytkowaniu interfejs Novell.
- Łatwość integracji z systemem GroupWise.
- Statystyczna filtracja spamu z użyciem wielu metod ewaluacji.

### **Minimalne wymagania systemowe**

Niezbędne do pracy programu elementy systemu:

- Serwer Novell NetWare 5.1+SP8, 6+SP5, 6.5+SP8
- Intel Pentium (lub kompatybilny) co najmniej
- 1024 MB pamięci RAM (Novell NetWare 6.x:: 2048 MB)
- 150 MB wolnego miejsca na twardym dysku
- Novell GroupWise 6.5
- Dla filtrowania Post Office: +100 MB wolnego miejsca na twardym dysku
- VirusBuster for NetWare Servers 2.4.X-X.X.X wersja

## Instalacja

Produkt jest dystrybuowany w postaci samorozpakowującego się pliku (.exe) lub w postaci spakowanego pliku .zip. Użyj wersji samorozpakowującej lub skorzystaj z programu rozpakowującego pliki typu .zip.

**Uwaga!** VirusBuster for Mail Servers (GroupWise) może być używany tylko wtedy, gdy program VirusBuster for NetWare Servers został uruchomiony!

## Instalacja automatyczna

Program dystrybuowany jest w postaci następującego pliku:

`gwise-<product version>-<poa module version>-<language>.exe`

Na przykład:

`gwise-2.2.08-1.0.05-en.exe`

**Uwaga!** Jeśli ochrona serwera jest aktywna, chroni ona domyślnie pliki wykonywane w trakcie zapisu. To może spowodować nieoczekiwane problemy podczas automatycznej instalacji. Dlatego zaleca się, aby w trakcie automatycznej instalacji wyłączyć ochronę zapisu. Najprostszym sposobem jest zatrzymanie serwera ochrony. Po pomyślnej instalacji ochrona zostanie automatycznie wznowiona.

- Po pojawieniu się okna powitalnego wraz z licencją użytkownika, możesz wybrać folder instalacji. Program może być zainstalowany tylko w folderze, w którym zainstalowano wcześniej VirusBuster for NetWare Servers.
- Po wskazaniu docelowego folderu zostanie pokazana wersja modułów do zainstalowania, po to abyś mógł je sprawdzić.
- Na następnym oknie możesz wybrać składniki programu, które chcesz zainstalować. Ochrona agenta internetowego (*Internet Agent*) jest niezbędnym składnikiem ochrony.
- Po naciśnięciu przycisku **[Next>]**, będziesz mógł ustawić zadania, które zostaną automatycznie uruchomione w końcowej fazie instalacji.

**Uwaga!**

Jeśli jakieś z zadań nie będzie mogło być uruchomione, należy uruchomić je ręcznie po zakończeniu instalacji, opierając się na instrukcji *Manualnej instalacji*.

Zadania, które możesz wskazać w tym miejscu są identyczne jak te określone w instrukcji manualnej instalacji (porównaj z sekcją *Manualna instalacja*).

### **Internet Agent protection – Ochrona agenta internetowego**

- *Create domain – Twórz domenę*: Jeśli zostanie zaznaczone, to program spróbuje odszukać na wskazanym woluminie katalog `domain` GroupWise (domena jest taka sama, jak domena ustawiona w serwerze pocztowym). Jeśli nie zostanie ona znaleziona automatycznie, będziesz musiał wpisać ją ręcznie. Po ustawieniu tego parametru, program uruchomi zadania określone w sekcji *Ochrona agenta internetowego* i *Instalacja filtra antyspamowego*.

- *Start protection – Włącz ochronę*: Jeśli zostanie zaznaczone, Ochrona agenta internetowego będzie automatycznie uruchomiona po zakończeniu instalacji.

- *Modify autoexec.ncf – Zmodyfikuj autoexec.ncf*: Jeśli zostanie zaznaczona, zostaną wykonane niezbędne modyfikacje pliku `autoexec.ncf` (porównaj z sekcją *Instalacja ochrony agenta internetowego*).

- *X-Spam-Flag support*: Enables IA-side *Junk Mail* handling. To use this function, other settings are needed which are detailed in the [Spam filter](#) section.

### **Post Offices protection – Ochrona serwerów PostOffice**

- *Certify application to access post offices – Zezwól aplikacji na dostęp do serwerów Post Office* : Jeśli zostanie włączona, program utworzy klucz identyfikacyjny niezbędny do uruchomienia filtra Post Office (porównaj z sekcją *Instalacja ochrony Post Office*).
- *Start module – Uruchom moduł*: Jeśli zostanie zaznaczone, ochrona serwerów Post Office zostanie automatycznie uruchomiona po zakończeniu instalacji.
- *Modify autoexec.ncf – Zmodyfikuj autoexec.ncf*: Jeśli zostanie zaznaczone, zostaną wykonane niezbędne modyfikacje pliku `autoexec.ncf` (porównaj z sekcją *Instalacja filtra poczty Post Office*).

## GroupWise settings – Ustawienia GroupWise

- *Start module – Uruchom moduł*: Jeśli zostanie zaznaczone, moduł ochrony GroupWise będzie automatycznie uruchomiony po zakończeniu instalacji.
- Po ustawieniu tych parametrów, program instalacyjny zostanie uruchomiony, a wskazane zadania zostaną zrealizowane.

## Instalacja manualna

Program dystrybuowany jest w postaci następującego pliku:

`gwise-<product version>-<poa module version>-<language>.zip`

Na przykład:

`gwise-2.2.08-1.0.05-en.zip`

### *Instalacja ochrony agenta internetowego*

Skopiuj pliki `VBGWIA.NLM`, `VBGWISE.SET`, `VBNOTIFY.NLM` i `VBGWSET.NLM` do katalogu, w którym znajdują się `VBSHIELD.NLM` i `VBENGINE.NLM`.

Utwórz katalog komunikacyjny `VBGWIA` wewnątrz katalogu domeny GroupWise Internet Agent (`... \WPGATE \GWIA`). Następnie w tym katalogu (`VBGWIA`) utwórz podkatalogi o nazwach: `QUARANT`, `TEMP`, `SEND`, `RECEIVE`, `RESULT`. Są one wymagane, ponieważ GroupWise będzie przynosił do nich wiadomości w celu skanowania antywirusowego.

Włącz używanie przez agenta internetowego GroupWise katalogu komunikacyjnego. Możesz to uczynić za pomocą programu administracyjnego NetWare Administrator lub za pomocą programu ConsoleOne (odszukaj przycisk *Advanced* w panelu ustawień *Server Directories* właściwości GWIA). Wpisz w polu katalogu SMTP Service Queues na oknie, które się pojawiło, nazwę katalogu komunikacyjnego (`... \WPGATE \GWIA \VBGWIA`). Ustawienie katalogu SMTP Service Queues, powoduje, że GWIA nie prześle dalej wiadomości kanałem SMTP, chyba że pole katalogu SMTP Service Queues zostanie usunięte lub plik `VBGWIA.NLM` jest załadowany.

#### Uwaga!

W momencie określenia katalogu SMTP Service Queues, GWIA nie prześle wiadomości poprzez kanał SMTP, jeśli `VBGWIA.NLM` jest załadowany lub pole katalogu SMTP Service Queues zostanie usunięte!

Zmodyfikuj plik ustawień `VBGWISE.SET` za pomocą programu `VBGWSET.NLM`. Nie zapomnij ustawić katalogu roboczego GroupWise Internet Agent oraz katalogu kwarantanny i katalogu roboczego.

#### Uwaga!

Używając programu `VBNOTIFY.NLM` możesz zastosować nowe ustawienia bez restartu chronionego.

Aby aktywować ochronę GroupWise załaduj program `VBGWIA` (`load vbgwia`). Jeśli postępowałeś zgodnie z instrukcją, odzyskasz przepływ maili w kanale SMTP. Od tego momentu, `VBGWIA.NLM` będzie

„pomocne” w przesyłaniu listów poprzez ich skanowanie.

Jeśli chcesz aby ochrona modułów GroupWise i poczty uruchamiała się automatycznie, razem z systemem, powinieneś dodać do pliku `SYS:SYSTEM/AUTOEXEC.NCF` następującą linię:

```
load vbgwia.nlm
```

## Instalacja filtru spamu

Po zainstalowaniu VirusBuster for NetWare Servers i VirusBuster for Mail Servers (GroupWise) musisz skopiować pliki programu `SPAME.NLM` i bazę danych `VBUSTER.SDB` do katalogu instalacyjnego (na przykład: `SYS:/SYSTEM/VBUSTER`).

Aby zakończyć instalację filtru spamu utwórz katalog w katalogu komunikacyjnym (...`\WPGATE\GWIA\VBGWIA` jak sugerowano powyżej) dla kwarantanny spamu pod nazwą `SPAMQUAR`.

Do zarządzania ustawieniami filtru spamu służy menu *Spam filter*, które odnajdziesz wśród ustawień agenta internetowego (*Internet Agent*).

**Uwaga!**  
Użycie filtru spamu ma wpływ na działanie serwera. Uruchomienie lub zakończenie pracy programu może zająć kilka minut!

## Instalacja filtru poczty Post Office

Skopiuj pliki `VBPOSCAN.NLM` do katalogu instalacyjnego (na przykład: `SYS:/SYSTEM/VBUSTER`).

Aby aktywować moduł ochrony poczty Post Office, należy wygenerować klucz identyfikacyjny, który pozwoli skanerowi poczty na dostęp do listów składowanych w danym serwerze pocztowym. Wygenerowanie klucza musi zostać wykonane w systemie Windows przed pierwszym uruchomieniem skanera POA. Uruchom plik `vbpotapp.exe` (potrzebuje on również biblioteki `gwtapp.dll`) który znajduje się w pakiecie instalacyjnym. Jeżeli istniejący plik został odnaleziony zostaniesz ostrzeżony przed nadpisaniem go.

Aby wygenerować klucz musisz podać następujące ścieżki:

- Bazy danych domeny GroupWise na serwerze Novell (`wpdomain.db`).
- Pliku konfiguracyjnego VirusBuster for Mail Servers (GroupWise) (`vbgwise.set`).

Po wygenerowaniu klucza mechanizm wewnętrznej komunikacji GroupWise skopiuje klucz do innych agentów. W zależności od szybkości komunikacji, może to zająć kilka minut.

Uruchom plik `VBPOSCAN.NLM`, a następnie skonfiguruj filtr poczty Post Office za pomocą programu `VBGWSET.NLM`.

Aby uruchomić ochronę Post Office, załaduj program `VBPOSCAN` (`load vbposcan`).

Jeśli chcesz aby ochrona poczty Post Office uruchamiała się automatycznie, razem z systemem, powinieneś dodać do pliku `SYS:SYSTEM/AUTOEXEC.NCF` następującą linię:

```
load vbposcan.nlm
```

## Struktura programu

VirusBuster for Mail Servers (GroupWise) współpracuje z programem VirusBuster for NetWare Servers. Poprawne działanie będzie zagwarantowane tylko po zainstalowaniu i aktywacji VirusBuster for NetWare Servers.

**Uwaga!** `VBGWIA.NLM` wymaga `VBENGINE.NLM` do skanowania listów i przesyła informacje do `VBSHIELD.NLM`, więc zawsze pamiętaj o wyłączeniu `VBGWIA.NLM` przed wyłączeniem VirusBuster for NetWare Servers!

Jeśli zawartość pliku `VBGWISE.SET` zostanie zmodyfikowana podczas pracy `VBGWIA.NLM`, wówczas `VBGWIA.NLM` może zostać powiadomiony o zmianie poprzez załadowanie `VBNOTIFY.NLM`, które wymusza na `VBGWIA.NLM` ponowne odczytanie ustawień.

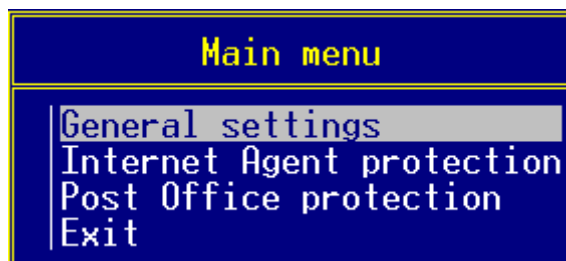
## Interfejs użytkownika

Zmian ustawień programu można dokonać za pomocą menu systemu NetWare's `NWSNUT.NLM`. Następujące klawisze służą do nawigacji w menu systemowym:

- Klawisze kursorów, `PgDn`, `PgUp` - Poruszanie się po pojedynczych elementach menu.
- **Klawisz Enter** - Wybór elementu menu.
- **Klawisz ESC** - Wyjście z menu lub programu.
- **Klawisz F1** - Pomoc.
- **Klawisz Delete** - Usuwanie wpisu/pozycji.
- **Klawisz Insert** - Wstawianie wpisu/pozycji.

## Szczegółowy opis

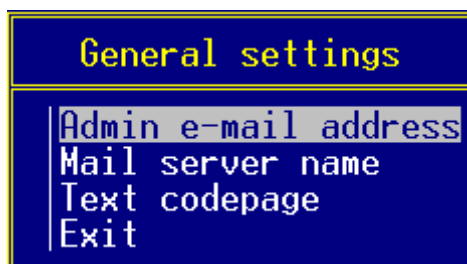
Ustawienia programu dostępne są w pliku **VBGWISE.SET**. Ustawienia mogą być modyfikowane za pomocą menu systemowego **VBGWSET.NLM**. Struktura menu systemowego:



*Menu główne*

Ustawienia ochrony agenta internetowego i ochrony serwerów Post Office znajdują się w dwóch niezależnych pozycjach menu. Opcje zawarte w menu *General settings* odnoszą się zarówno do modułu ochrony IA jak również PO.

## General settings - Ustawienia ogólne



*Menu ustawień ogólnych*

Opcje znajdujące się w tym menu są wspólnymi parametrami dla agenta internetowego i ochrony poczty:

### Admin e-mail address - Adres e-mail administratora

List z powiadomieniem może być przesłany na określony tutaj adres.

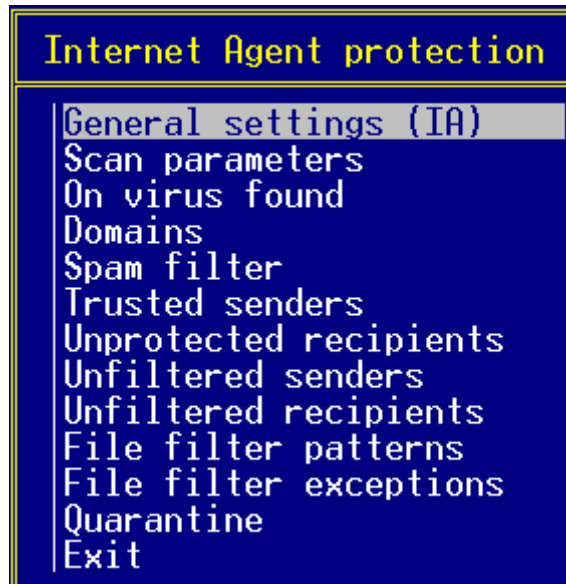
### Mail server name - Nazwa serwera

Nazwa (hostname) serwera SMTP lub jego adres IP wymagany do dostarczenia poczty do odbiorcy.

### Text codepage – Strona kodowa znaków

Tu można określić stronę kodową używaną podczas wysyłania powiadomień.

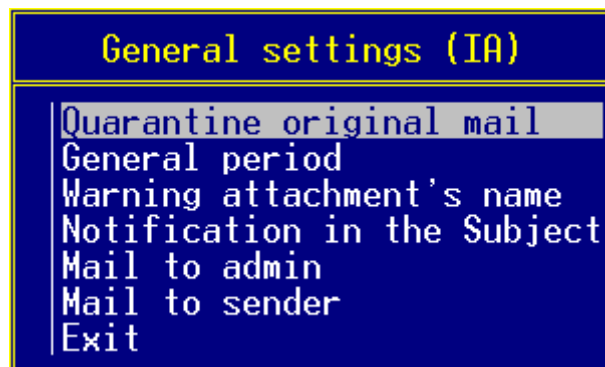
## Internet Agent protection – Ochrona agenta internetowego



*Menu ochrony agenta internetowego*

Agent internetowy jest odpowiedzialny za transmisję poczty i umożliwia komunikację pomiędzy Internetem a siecią lokalną. Tutaj znajdziesz szczegółowe informacje o wirusach i filtrze spamu.

### *General settings (IA) – Ustawienia ogólne (IA)*



*Menu ustawień ogólnych agenta internetowego*

#### Quarantine original mail – Umieść w kwarantannie oryginalną wiadomość

Jeśli wiadomość została zmodyfikowana, oryginalna wiadomość zostanie przez program umieszczona w kwarantannie.

#### General Period – Ogólny okres

Ustawienia okresu dla tych zadań, które nie należą do żadnej z domen. Program uruchamia zadania w określonych odstępach czasowych.

#### Warning attachment's name - Nazwa pliku z ostrzeżeniem

Ustawiana jest tutaj nazwa pliku zawierającego ostrzeżenie, wysłanego w zmodyfikowanym mailu.

## Notification in the subject - Powiadomienie w tytule

Jeśli ta opcja jest włączona, program będzie umieszczał informacje o rezultatach skanowania w tytule listu.

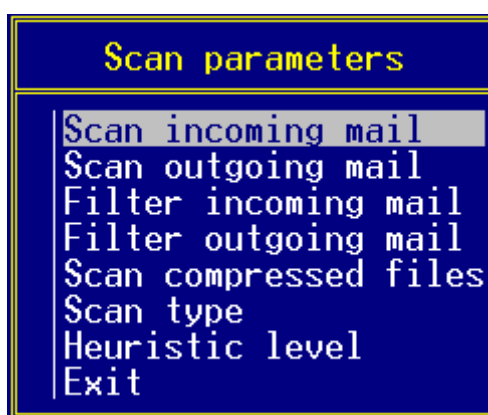
## Mail to admin - Powiadomienie do administratora

Włączenie/wyłączenie opcji wysyłania powiadomienia administratora o występujących incydentach.

## Mail to sender - Powiadomienie do nadawcy

Włączenie/wyłączenie opcji wysyłania powiadomienia nadawcy o występujących incydentach.

## *Scan parameters – Parametry skanowania*



*Menu parametrów skanowania*

## Scan incoming mail - Skanowanie poczty przychodzącej

Włączenie/wyłączenie skanowania poczty przychodzącej.

## Scan outgoing mail - Skanowanie poczty wychodzącej

Włączenie/wyłączenie skanowania poczty wychodzącej.

## Filter incoming mail - Filtr poczty przychodzącej

Po włączeniu tej opcji, w przypadku, gdy wiadomość przychodząca zawiera załącznik, który pasuje do któregoś ze wzorów ustawionych w pliku filtrującym, wówczas program usunie go.

## Filter outgoing mail - Filtr poczty wychodzącej

Jeśli wiadomość wychodząca zawiera załącznik, który pasuje do któregoś ze wzorów ustawionych w pliku filtrującym, wówczas program usunie go, jeśli opcja ta zostanie włączona.

## Scan compressed files - Skanowanie plików skompresowanych

Opcja włączenia/wyłączenia skanowania plików skompresowanych.

## Scan type – Typ skanowania

Silnik skanowania antywirusowego jest zdolny do skanowania i wykrywania wirusów według różnych metod. Zostanie zastosowana metoda określona w tym polu. Dostępne są następujące poziomy ochrony:

- *Fast*  
Skanuje tylko te części pliku, w których prawdopodobieństwo wystąpienia wirusów jest

największe, nie wykrywa wirusów, których wykrycie wymaga zastosowania większej ilości zasobów systemowych (np. wirusy w formułach Excel'a).

- *Strict*  
Zoptymalizowana metoda skanowania, wykrywa wszystkie wirusy zarejestrowane w bazie danych wirusów, skanuje te części pliku, w których prawdopodobieństwo wystąpienia wirusów jest największe.
- *Full*  
Wykrywa wszystkie wirusy zarejestrowane w bazie danych wirusów i skanuje cały plik, nawet te jego części, w których prawdopodobieństwo wykrycia wirusów nie jest duże.

## Heuristic level - Poziom heurystyki (wyszukiwania nieznanego wirusów)

Podczas analizy heurystycznej program próbuje wykryć kod charakterystyczny dla wirusów w plikach, których fragmenty nie znajdują się w bazie wzorców. Skanowanie heurystyczne może być włączone lub wyłączone. Można także ustalać stopień zaawansowania analizy. Użytkownik będzie powiadomiony, jeżeli podejrzany plik zostanie znaleziony.

Dostępne są następujące poziomy analizy heurystycznej:

- *Off - Wyłączony*  
Program nie uruchamia analizy heurystycznej.
- *Normal - Standardowy*  
Ustawienie to powoduje niski poziom fałszywych wskazań przy niewysokim stopniu wyszukiwania nieznanego wirusów.
- *Strong - Wysoki*  
Szansa wykrycia nieznanego wirusa jest wyższa, ale istnieje także wyższe prawdopodobieństwo błędnych ostrzeżeń.

## *On virus found – Akcje po wykryciu wirusa*



*Menu akcji dostępnych w przypadku wykrycia wirusa*

## Virus handling - Postępowanie w przypadku pojawienia się wirusa

Ustalenie procedury postępowania w przypadku wykrycia wirusa. Zainfekowany plik może zostać usunięty, wyleczony, a także można skasować całą wiadomość.

## WormBuster

Jeśli włączysz tę funkcję, wiadomości zainfekowane przez I-robaki zostaną zablokowane bez powiadomienia.

## Suspicious files - Podejrzane pliki

Ustalenie procedury postępowania w przypadku wykrycia przez moduł analizy heurystycznej

podejrzanych plików.

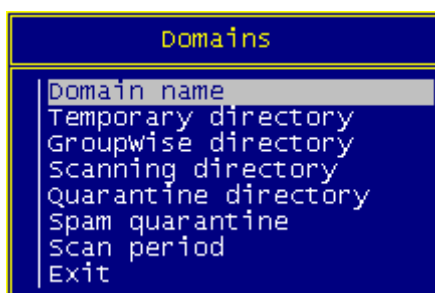
## Password protected archives – Pliki archiwum zabezpieczone hasłem

Po włączeniu tej opcji, program zablokuje pliki, których nie można było sprawdzić z tego powodu, że były one zabezpieczone hasłem.

## On scan error – Co zrobić w przypadku błędu skanowania

W przypadku pojawienia się jakichkolwiek błędów podczas skanowania poczta może zostać zablokowana.

## *Domeny*



*Menu ustawień domen*

## Domain name - Nazwa domeny

Ustawienie nazwy chronionego obszaru.

## Temporary directory - Katalog tymczasowy

Katalog, w którym składowane są pliki tymczasowe.

## GroupWise directory - Katalog GroupWise

Katalogi robocze agenta internetowego GroupWise. Dostępne są: **SEND**, **RECEIVE**, **RESULT**.

## Scanning directory - Katalog skanowania

Ustalenie katalogu roboczego GroupWise dla skanowania protokołu SMTP (**SEND**, **RECEIVE**, **RESULT**, katalogi kwarantanny i tymczasowy muszą być utworzone ręcznie w tym katalogu).

## Quarantine directory - Katalog kwarantanny

Katalog, w którym zamieszczone oryginalne kopie zmodyfikowanych listów.

## Spam quarantine - Kwarantanna spamu

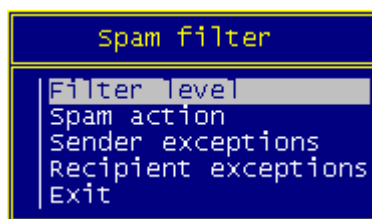
Katalog kwarantanny listów oznaczonych jako spam przez moduł antyspamowy.

## Scan period - Czas skanowania

Ustawiany w bieżącym obszarze ochronnym.

## *Filtr spamu*

VirusBuster for Mail Servers (GroupWise) został stworzony do ochrony systemów pocztowych w celu ochrony przed atakami wirusów. Obecna wersja wyposażona została również w filtr spamu w celu ochrony komputera przed niechcianymi listami.



Menu ustawień filtru spamu

### Filter level - Poziom filtracji

Możesz włączyć lub wyłączyć działanie filtru spamu oraz ustawić jego czułość.

Jeśli wybierzesz opcję bez filtru, filtr spamu wyłączy się. Jeśli użyjesz innych ustawień, filtr spamu włączy się a jego czułość będzie zależała od ustawień, które wybierzesz.

### Spam action - Spam action

Możliwe działania w przypadku wykrycia spamu przez filtr:

- None – Nic nie rób: wiadomość jest przesyłana dalej bez żadnej zmiany, istnieje także możliwość skopiowania poczty do katalogu kwarantanny.
- Mark mail
  - Subject change - Zmień temat: możesz zmienić zawartość pola *Temat* w oknie które się wyświetliło. Możesz wyszczególnić nową zawartość i użyć symbolu tematu `%Subject%` który jest symbolem zawartości oryginalnego pola poczty *Subject*.
  - Insert X-Spam-Flag  
Yes: the "X-Spam-Flag: Yes" field will be inserted in the e-mail's header. The GWIA will identify e-mails which will be forwarded to the *Junk Mail* folder with this flag.
  - Quarantine copy  
Yes: Besides executing one of the above options, the original copy of the e-mail which has been marked as spam will be moved to the quarantine.
- Blocking - Zablokuj: wiadomość nie zostanie przesłana do odbiorcy, zostanie usunięta ale możesz ją także skopiować do katalogu kwarantanny.
- To quarantine – Przenieś do kwarantanny: wiadomość nie zostanie przesłana dalej do odbiorcy, zostanie przesunięta do katalogu kwarantanny.

Pamiętaj, że niezależnie od ustawionych wyjątków w logu `VBUSTER.LOG` zawsze zostanie zarejestrowane zdarzenie, że wykryto spam. Możesz ustawić katalog kwarantanny w menu *Domains*. Zaleca się użycie katalogu `SPAMQUAR`, który został utworzony podczas instalacji.

### *Other Junk Mail folder settings*

If you would like to forward e-mails, which have been marked as spam to the *Junk Mail* folder, and you have selected the option to insert the *X-Spam-Flag*, please check the following settings:

- Select the GWIA object in the ConsoleOne system administration program (usually it is called GWIA).
- After right-clicking on the object, select the *Properties* option from the displayed list.
- Click on the *SMTP/MIME* tab and select *Junk Mail* from the list.
- A dialog will be displayed where the *Flag any messages that contain x-spam-flag: yes or...* option must be checked..

The following settings must also be applied for proper operation:

- On the main page of ConsoleOne, in the left tree, under *GroupWise System* the protection are

(domain) or post office must be selected, where the functionality should be activated (if several protection areas are needed, the settings must be applied to all of them).

- After right-clicking on the selected item, choose *GroupWise Utilities\Client Options* in the list and click on the *Environment* button on the displayed dialog.
- On the *General* tab of the displayed dialog, the *Enable Junk Mail Handling* option must be checked in the *Junk Mail Handling* section.
- Select the *Enable Junk Mail using Junk Mail list* option and other options as well if needed. The settings can be locked by clicking on the lock icon on the right side so that the option for the post office or mailbox which belong to the object cannot be modified.

## Sender exceptions – wyjątki dot. wysyłających

Wiadomości wysłane z wpisanych tutaj adresów i domen nie podlegają filtracji, są przesyłane dalej do odbiorcy bez sprawdzenia spamu. Możesz użyć klawiszy **INSERT** i **DELETE**, aby dodać lub usunąć poszczególne elementy (adresy) listy.

## Recipient exceptions – wyjątki dot. odbiorców

Wiadomości wysłane na wpisane tutaj adresy i domeny nie podlegają filtracji przez moduł antyspamu.

## *Trusted senders - Zaufani nadawcy*

Program nie skanuje wiadomości pochodzących z podanych adresów. Następujące zasady obowiązują podczas określania tych adresów:

- Adres e-mail wpisany w całości, bądź z zastosowaniem wieloznacznych znaków \* i ?. Znak \* zastępuje dowolną liczbę znaków a znak ? zastępuje pojedynczy znak. Znak @ nie może być zastąpiony innym!
- Jeśli adres zaczyna się znakiem @, odnosi się do wszystkich użytkowników z tej domeny.

## *Unprotected recipients – Niechronieni odbiorcy*

Program nie skanuje poczty wysłanej na podane adresy.

## *Unfiltered senders – Niechronieni nadawcy*

The filter settings are not applied to messages incoming from the given addresses.

## *Unfiltered recipients – Odbiorcy dla których filtr jest wyłączony*

Ustawienia filtra nie odnoszą się do wiadomości pochodzących z podanych adresów.

## *File filter patterns – Wzorce filtra plików*

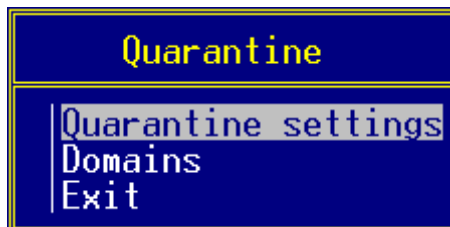
Załączniki, które pasują do podanych wzorów nazw plików są usuwane z wiadomości bez skanowania (np: \*.com, \*.exe, \*.doc).

## *File filter exceptions – Wyjątki filtra plików*

Pliki, które filtr plików będzie pomijał (nie będzie ich usuwał), np. **command.com**.

## Quarantine

You can view the contents of the quarantine folder in this menu and customize the display of the quarantine items with the available options.



Quarantine

## Quarantine settings

The following options can be used to customize the list:

- View  
Quarantined mails will be displayed in the list according to the selected option:  
*Sender + subject*  
*Recipient + subject*
- Sort by  
E-mails will be sorted in the list following these options:  
*Date*  
*Sender/Recipient*  
*Subject*
- Sort order  
E-mails will be sorted in the list following the option selected above, in one of the following orders:  
*Ascending*  
*Descending*

## Domains

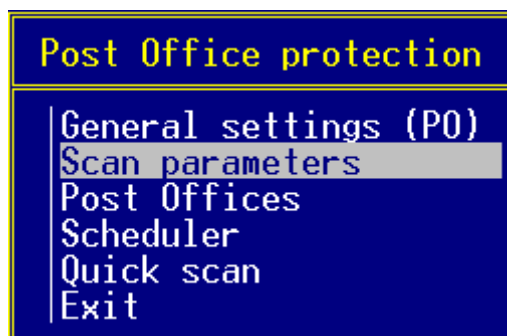
You can select a protection area (domain here) to display a list of items found in its spam or virus quarantine.

The quarantined objects will be displayed in the list (which can take some seconds depending on the length of the list). By pressing **Enter**, details about a specific item in the quarantine can be displayed and the following actions can be performed on the item by pressing **Enter** again:

- *Delete*
- *Forward to admin*
- *Forward to recipient*
- *Skip*

After selecting an action, the details window can be closed by pressing **ESC**. The action will be performed on the selected item after this. Except for the *Skip* option, every action will delete the item from the quarantine.

## Post Office protection – Ochrona poczty trybu Post Office



Menu ochrony poczty Post Office

Moduł ochrony poczty Post Office umożliwia skanowanie antywirusowe poczty w trybie off-line, sprawdzając skrzynki pocztowe użytkowników znajdujące się na serwerach IMAP. System poszukuje wirusów wg ustawionego harmonogramu. Skanowanie w trybie off-line zapewnia większą ochronę poczty uniemożliwiając rozprzestrzenianie się wirusów czy zarażonych listów, które dostały się w jakiś sposób do systemu.

**Ważne!**  
Foldery zawierające więcej niż 5000 elementów nie mogą zostać sprawdzone, ze względu na limit protokołu IMAP!

### General settings (PO) - Ustawienia ogólne (PO)

Ogólne ustawienia modułu:

#### Mail to Admin – powiadomienie do administratora

Za pomocą tej opcji, administrator może zostać poinformowany o zdarzeniach, który wystąpiły w systemie. Jeżeli zdarzenie znajdujące się na liście wystąpi, program wyśle powiadomienie do administratora systemu.

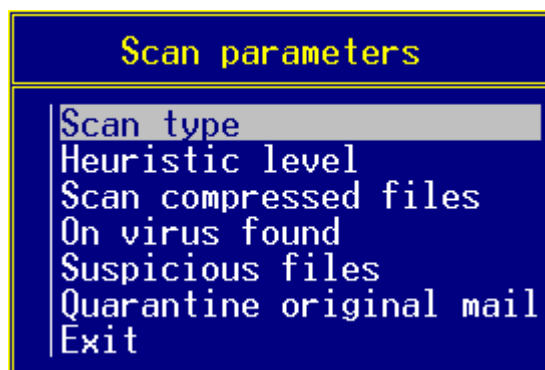
#### Zarządzanie listą:

Lista domyślnie jest pusta. Użyj klawisza **Insert** aby dodać zdarzenie. Po jego naciśnięciu, zobaczysz listę wszystkich możliwych zdarzeń systemu, spośród których wybierzesz te, które będą dla Ciebie interesujące. Użyj klawisza **Enter** do wskazania wybranego zdarzenia. Powtórz tę procedurę, jeśli chcesz być informowany o wielu zdarzeniach. Użyj klawisza **Delete** w celu usunięcia wybranych pozycji.

#### Mail to user – powiadomienie do użytkownika

Za pomocą tej opcji możesz informować użytkowników o różnych zdarzeniach. Tworzenie i zarządzanie listą odbywa się w sposób identyczny, jak zarządzanie powiadomieniami do administratorów.

## Scan parameters – Parametry skanowania



Menu parametrów skanowanie

### Scan type – Typ skanowania

Możesz wybrać te same wartości jak w opcji [Scan type](#) w sekcji Internet Agent.

### Heuristic level – Poziom heurystyki (poziom wyszukiwania nieznanymi wirusów)

Możesz wybrać te same wartości jak w opcji [Heuristic level](#) w sekcji Internet Agent.

### Scan compressed files – Skanowanie skompresowanych plików

Jeżeli wybierzesz tę opcję, skaner będzie sprawdzał także skompresowane pliki.

### On virus found – Postępowanie w przypadku znalezienia wirusa

Wybierz akcję, która zostanie wykonana w momencie wykrycia wirusa. W przypadku niepowodzenia podczas niszczenia wirusa, program podmieni oryginalny plik, na plik tekstowy o nazwie [<nazwa\\_pliku>.txt.](#), w którym będzie więcej informacji o akcji.

### Suspicious files – Podejrzane pliki

Wybierz działanie dla podejrzanych plików.

### Quarantine original mail – Kwarantanna oryginalnych listów

Jeśli włączysz tę opcję, to program umieści w kwarantannie oryginalne kopie listów, które trakcie skanowania zostaną zmodyfikowane. Folder kwarantanny możesz ustawić w opcji [Quarantine IMAP folder](#).

## Post Offices – Ochrona poczty Post Office

Korzystając z tego menu możesz dodać serwery poczty Post Office aby VirusBuster for Mail Servers (GroupWise) okresowo je sprawdzał. Domyślnie lista serwerów jest pusta, o czym program informuje stosownym ostrzeżeniem.

Aby dodać nowy serwer do listy użyj klawisza **Insert**. Po wprowadzeniu nazwy serwera Post Office, musisz wpisać dodatkowe informacje o serwerze, które pojawią się na ekranie. Możesz zmodyfikować te parametry także w przyszłości, wskazując nazwę serwera Post Office za pomocą klawisza **Enter**. Jeśli chciałbyś usunąć serwer Post Office z listy, podświetl jego nazwę, a następnie użyj klawisza **Delete**.



Menu ustawień Post Office

Post Office name – Nazwa serwera Post Office

Identyfikator serwera Post Office w systemie antywirusowym. Możesz odnosić się do określonego serwera Post Office poprzez tę właśnie nazwę.

Host name – Nazwa hosta

Nazwa serwera (hostname) lub jego adres IP, na którym zainstalowano serwer Post Office.

Port – Numer portu

Numer portu serwera pocztowego Post Office.

Scan only new mails – Skanuj tylko nowe listy

Skaner będzie sprawdzał tylko nowo odebrane listy.

Scan all users – Skanuj konta wszystkich użytkowników

Po włączeniu tej opcji będą skanowane konta wszystkich użytkowników serwera Post Office.

User exceptions – Pomijane konta użytkowników

W momencie aktywowania opcji *Scan all users*, tutaj możesz zdefiniować, konta czyich użytkowników nie będą poddawane skanowaniu.

Users to scan – Konta użytkowników do skanowania

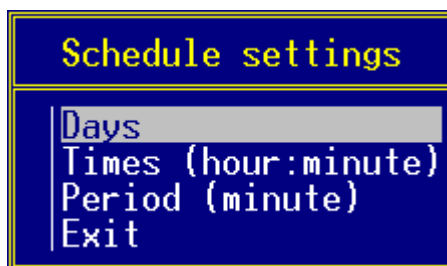
Konta użytkowników do skanowania na aktualnym serwerze Post Office. Nie ma potrzeby wskazywania nazw kont, jeśli opcja *Scan all users* jest włączona.

Quarantine IMAP folder – Folder IMAP kwarantanny

Ustaw folder kwarantanny przechowujący podejrzane obiekty. Nazwa foldera podawana jest w formacie: `<nazwa_użytkownika>/<folder_kwarantanny>` (np. `administrator/kwarantanna`). Możesz utworzyć foldery kwarantanny dla każdego użytkownika oddzielnie, trzeba wtedy zastosować składnię: `%CURRENT_USER%/<nazwa_folderu>`.

### *Scheduler - Harmonogram*

Za pomocą tego menu, możesz określić harmonogram skanowania serwerów Post Office. Wchodząc do menu musisz na początku określić nazwę serwera Post Office, którego będą dotyczyły wprowadzane dane.



*Menu ustawień harmonogramu*

Możesz zdefiniować interwał skanowania lub konkretny czas. Następujące ustawienia są dostępne podczas definiowania harmonogramu skanowania konkretnego serwera Post Office:

#### Days - Dni

Określ dzień lub kilka dni, w których skaner antywirusowy będzie uruchamiany automatycznie. Parametry wpisujesz w taki sam sposób, w jaki wpisywałeś parametry w ustawieniach ogólnych - [General settings \(PO\)](#). Jeśli nie określisz czasu lub okresu, skaner nie uruchomi się.

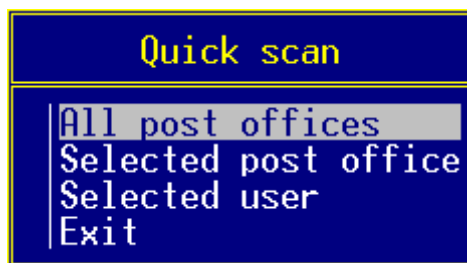
#### Times (hour:minute) – Czas (godzina:minuta)

Wpisz konkretny czas dla wskazanych dni (lub dla każdego dnia, jeśli lista *Days* pozostanie pusta) kiedy chcesz, aby skaner antywirusowy uruchomił się. Wypełnij listę w ten sam sposób, jak było to opisane w ustawieniach ogólnych - [General settings \(PO\)](#). Czas wpisujesz w formacie : **hh:mm** (hh – godzina, mm-minuty).

#### Period (minute) – Okres (w minutach)

Tutaj możesz określić, co ile minut będzie uruchamiany skaner antywirusowy.

#### *Quick scan – Szybkie skanowanie*



*Menu szybkiego skanowania*

#### All post offices – Wszystkie serwery Post Office

Skanuj wszystkie zdefiniowane serwery Post Office. Program będzie skanował tylko dostępne konta użytkowników serwera Post Office.

#### Selected post office – Wybrane serwery Post Office

Możesz wskazać, które serwery Post Office skanować. Program będzie skanował tylko dostępne konta użytkowników serwera Post Office.

#### Selected user – Wybrani użytkownicy

Najpierw musisz wskazać serwer Post Office, a następnie określić czyich użytkowników konta będą skanowane

## END USER AGREEMENT

*THIS SOFTWARE END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU AND VirusBuster Ltd. READ IT CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AND USING THE SOFTWARE. IT PROVIDES A LICENSE TO USE THE SOFTWARE AND CONTAINS WARRANTY INFORMATION AND LIABILITY DISCLAIMERS. BY INSTALLING AND USING THE SOFTWARE, YOU ARE CONFIRMING YOUR ACCEPTANCE OF THE SOFTWARE AND AGREEING TO BECOME BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THESE TERMS THEN DO NOT INSTALL THE SOFTWARE.*

*IMPORTANT NOTICE TO USERS: THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.*

### 1. Definitions

- (a) "Educational Version" means a version of the Software, so identified, for use by students and faculty of educational institutions only. "Home version" means a version of the Software, so identified, for use by individuals on a single computer at home only. Educational and Home Versions may not be used for, or distributed to any party for, any commercial purpose.*
- (b) Henceforward VirusBuster Ltd. means VirusBuster Ltd. and (where interpretable) its suppliers and licensors, if any.*
- (c) "Not For Resale (NFR) Version" means a version of the Software, so identified, to be used to review and evaluate the Software, only.*
- (d) "Software" means the VirusBuster Ltd. (R) VirusBuster(TM) software program supplied by VirusBuster Ltd. herewith, which may also include documentation, associated media, printed materials, and online and electronic documentation.*

### 2. License

*This EULA allows you to:*

- (a) Install and use the Software on a single computer; OR install and store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network, provided you have a license for each separate computer on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers.*
- (b) Educational and Home Version Only. If you have purchased a license for the Educational and/or the Home Version of the Software, then you may install or store the Software on a storage device, such as a network server, used only to run or install the Software on your other computers over an internal network for use by a total number of concurrent users not to exceed the number of user licenses you have been granted; provided, you agree to implement reasonable controls to ensure that your use of the Software does not exceed the number of licenses you have been granted. You agree that VirusBuster Ltd. may audit your use of the Software for compliance with the EULA at any time, upon reasonable notice.*
- (c) Make one copy of the Software in machine-readable form solely for backup purposes. You must reproduce on any such copy all copyright notices and any other proprietary legends on the original copy of the Software.*

### 3. License Restrictions

- (a) Other than as set forth in Section 2, you may not make or distribute copies of the Software, or electronically transfer the Software from one computer to another or over a network.*
- (b) You may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form.*
- (c) You may not sell, rent, lease, transfer or sublicense the Software.*
- (d) You may not modify the Software or create derivative works based upon the Software.*
- (e) You may not use the Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.*
- (f) In the event that you fail to comply with this EULA, VirusBuster Ltd. may terminate the license and you must destroy all copies of the Software.*

### 4. Upgrades

*If this copy of the Software is an upgrade from an earlier version of the Software, it is provided to you on a license exchange basis. You agree by your installation and use of this copy of the Software to voluntarily terminate your earlier EULA and that you will not continue to use the earlier version of the Software or transfer it to another person or entity.*

### 5. Ownership

*The foregoing license gives you limited rights to use the Software. VirusBuster Ltd. and its suppliers retain all right, title and interest, including all copyrights, in and to the Software and all copies thereof. All rights not specifically granted in this EULA, including International Copyrights, are reserved by VirusBuster Ltd. and its suppliers.*

### 6. LIMITED WARRANTY AND DISCLAIMER

- (a) LIMITED WARRANTY. VirusBuster Ltd. warrants that, for a period of ninety (90) days from the date of delivery (as*

evidenced by a copy of your receipt) that the physical media on which the Software is furnished will be free from defects in materials and workmanship under normal use.

(b) NO OTHER WARRANTY. EXCEPT AS SET FORTH IN THE FOREGOING LIMITED WARRANTY, VirusBuster Ltd. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, OR OTHERWISE INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ALSO, THERE IS NO WARRANTY OF NONINFRINGEMENT, TITLE OR QUIET ENJOYMENT. IF APPLICABLE LAW IMPLIES ANY WARRANTIES WITH RESPECT TO THE SOFTWARE, ALL SUCH WARRANTIES ARE LIMITED IN DURATION TO NINETY (90) DAYS FROM THE DATE OF DELIVERY. No verbal or written information or advice given by VirusBuster Ltd. its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of this warranty.

## 7. Exclusive Remedy

Your exclusive remedy under Section 6 is to return the Software to the place you acquired it, with a copy of your receipt and a description of the problem. VirusBuster Ltd. will use reasonable commercial efforts to supply you with a replacement copy of the Software that substantially conforms to the documentation, provide a replacement for defective media. VirusBuster Ltd. shall have no responsibility if the Software has been altered in any way, if the media has been damaged by accident, abuse or misapplication, or if the failure arises out of use of the Software with other than a recommended hardware configuration.

## 8. LIMITATION OF LIABILITY.

NEITHER VirusBuster Ltd. NOR ITS SUPPLIERS SHALL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION OR THE LIKE), ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE OR THIS EULA BASED ON ANY THEORY OF LIABILITY INCLUDING BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF VirusBuster Ltd. OR ITS REPRESENTATIVES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

## 9. Basis of Bargain

The Limited Warranty, Exclusive Remedies and Limited Liability set forth above are fundamental elements of the basis of the agreement between VirusBuster Ltd. and you. VirusBuster Ltd. would not be able to provide the Software on an economic basis without such limitations.

## 10. Consumer End Users Only

The limitations or exclusions of warranties and liability contained in this EULA do not affect or prejudice the statutory rights of a consumer, i.e., a person acquiring goods otherwise than in the course of a business.

## 11. General Provisions

The internal laws of Hungary shall govern this EULA. This EULA contains the complete agreement between the parties with respect to the subject matter hereof, and supersedes all prior or contemporaneous agreements or understandings, whether oral or written. All questions concerning this EULA shall be directed to VirusBuster Ltd.

VirusBuster and VirusBuster logo are trademarks or registered trademarks of VirusBuster Ltd. in Hungary and/or other countries. Other marks are the properties of their respective owners.

## CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address VirusBuster Ltd.  
Budapest 1518,  
Pf. 54.  
Hungary

Phone (+36) 1 382-7000  
Fax (+36) 1 382-7007  
Web <http://www.virusbuster.hu>  
Support <https://support.virusbuster.hu>  
E-mail [sales@virusbuster.hu](mailto:sales@virusbuster.hu)  
[support@virusbuster.hu](mailto:support@virusbuster.hu)