

VIRUS BUSTER

for Mail Servers - GroupWise

TABLE OF CONTENTS

VIRUSBUSTER FOR MAIL SERVERS (GROUPWISE)	1
Minimal system requirements	1
Installation	2
Automatic installation.....	2
Manual installation.....	3
Program's structure	5
Program's user interface.....	5
Detailed overview	6
General settings.....	6
Internet Agent protection	7
Post Office protection	14
END USER AGREEMENT	18
CONTACT	20

VIRUSBUSTER FOR MAIL SERVERS (GROUPWISE)

Nowadays most of the viruses and other harmful programs arrive in e-mail, therefore filtering the e-mail traffic of companies for viruses is crucial to avoid virus infections. The dramatic increase in the number of spam e-mails puts a heavy load on e-mail servers and deleting these e-mails can take a long time therefore every mail filtering product must contain an effective spam filter.

The product can be installed as a module of VirusBuster for NetWare Servers. Integrated into the mail system, the VirusBuster for Mail Servers (GroupWise) provides continuous protection by filtering the e-mail traffic for viruses and other malicious codes and spam. The Post Office protection module provides off-line virus protection for post offices found in the system.

Features:

- Outstanding performance, guaranteed by virus scanning engine
- Modular architecture for ease of use
- Virus scanning of incoming and outgoing messages and the removal of all viruses
- WormBuster for blocking I-Worms instantly
- Replacement of infected attachments with warning attachments
- White list (permissive list)
- Advanced notification and log system: a notification can be sent to the administrator and/or the sender of the message.
- Automatic program and virus database update via FTP
- Traditional, easy-to-use Novell user interface
- Easy integration with the GroupWise system
- Statistical spam filtering with many evaluation methods

Minimal system requirements

The following system components must be available to execute the program:

- Novell NetWare Server 5.1+SP8, 6+SP5, 6.5+SP8
- Intel Pentium (or compatible) processor
- 1024 MB of RAM (2048 MB in case using Novell NetWare Server 6.x)
- 150 MB of free hard disk space
- Novell GroupWise 6.5
- For Post Office filtering: +100 MB of free hard disk space
- VirusBuster for NetWare Servers version 2.4.X-X.X.X

Installation

The product is available in a self-extracting install package (.exe), and in a .zip file. Use the self-extracting version to install the antivirus system automatically or you have to install it manually (.zip version needed).

Important!
 VirusBuster for Mail Servers (GroupWise) can only be used if VirusBuster for NetWare Servers program is installed and activated!

Automatic installation

The following package is available:

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

Example:

`gwise-2.2.08-1.0.05-en.exe`

Important!
 If the server protection is functioning, it protects the executable files against writing by default. This can be a problem during the automatic installation so you are recommended to release write protection until the installation process has finished. The simplest way to do this is to stop the server protection while installing. After successful installation it will be restarted automatically.

- After the welcome panel and accepting the license agreement, you can set the target folder that you want to install the product to. The product can only be installed into such a folder that has the VirusBuster for NetWare Servers program's modules installed before.
- After setting the target folder, the panel displays the version numbers of the modules to be installed so you can check them.
- On the next panel, you can select the components you want to install. The *Internet Agent protection* is essential to install, the others are optional.
- After clicking on the **[Next>]** button, you can set actions which will be executed automatically at the final phase of the installation process.

Important!

If one of the actions can't be executed, it must be performed after the installation manually based on the description of the *Manual installation* section.

Actions that you can select here are the same as the ones you would have to do in the course of manual installation steps (consult the *Manual installation* section for more).

Internet Agent protection

- *Create domain*: If it is checked, the program tries to find the GroupWise's **domain** folder (this is the same as the one that was set when the mail server has been installed) on the selected volume. If it couldn't find the folder automatically, you have to specify it manually. After setting this parameter, the program performs the actions detailed in the *Install Internet Agent protection* and *Install Spam filter* sections.

- *Start protection*: If it is checked, the Internet Agent protection will be started automatically on the server after the installation.

- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the **autoexec.ncf** file (consult the *Install Internet Agent protection* section for more).

- *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

- *Certify application to access post offices*: If it is checked, the program creates the activation key

needed for the Post Office filter (consult the *Install Post Office filter* section for more).

- *Start module*: If it is checked, the Post Office filter will be started automatically on the server after the installation.

- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the [autoexec.ncf](#) file (consult the *Install Post Office filter* section for more).

GroupWise settings

- *Start module*: If it is checked, the GroupWise protection module will be started automatically on the server after the installation.

- After these settings the installation process will be started and the selected actions will be performed.

Manual installation

The following package is available:

[gwise-<product version>-<poa module version>-<language>.zip](#)

Example:

[gwise-2.2.08-1.0.05-en.zip](#)

Install Internet Agent protection

Copy [VBGWIA.NLM](#), [VBGWISE.SET](#), [VBNOTIFY.NLM](#) and [VBGWSET.NLM](#) files into the directory of [VBSHIELD.NLM](#) and [VBENGINE.NLM](#).

Create a [VBGWIA](#) communication directory inside the GroupWise Internet Agent's domain-directory ([...\WPGATE\GWIA](#)). In this directory ([VBGWIA](#)) create the [QUARANT](#), [TEMP](#), [SEND](#), [RECEIVE](#), [RESULT](#) subdirectories. This is needed because messages are moved to these directories for virus scanning from GroupWise's same folders.

Set GroupWise Internet Agent to use the communication directory with the help of NetWare Administrator or ConsoleOne programs (find the *Advanced* button on *Server Directories* setting panel of GWIA properties). You should modify the SMTP Service Queues Directory field in the appeared window to the communication directory ([...\WPGATE\GWIA\VBGWIA](#)). By specifying the SMTP Service Queues Directory, GWIA will not forward messages through the SMTP channel unless the SMTP Service Queues Directory field is deleted or the [VBGWIA.NLM](#) is loaded.

Attention!

By specifying the SMTP Service Queues Directory, GWIA will not forward messages through the SMTP channel if the [VBGWIA.NLM](#) is loaded or the SMTP Service Queues Directory field is deleted!

Modify the [VBGWISE.SET](#) file as required with the help of [VBGWSET.NLM](#)'s menu system. Don't forget to set GroupWise Internet Agent's work directory, and the quarantine and work directory.

Attention!

Using [VBNOTIFY.NLM](#) you can apply new settings without restarting the protection system.

To activate the GroupWise protection, load the VBGWIA program ([load vbgwia](#)). If these steps have been performed in order, mail flow will be recovered in the SMTP channel. From now on, [VBGWIA.NLM](#) will "help" in forwarding mail while it scans mails according to its settings.

If you want the GroupWise protection module to be started automatically together with the server then

you should insert the next line into the `SYS:SYSTEM/AUTOEXEC.NCF` file:

```
load vbgwia.nlm
```

Install spam filter

After you have installed the VirusBuster for NetWare Servers and the VirusBuster for Mail Servers (GroupWise) you, have to copy the `SPAME.NLM` module and the `VBUSTER.SDB` spam database into the installation directory (for example: `SYS:/SYSTEM/VBUSTER`).

To finish spam filter installation create a directory into the communication directory (`...\WPGATE\GWIA\VBGWIA` as suggested) for quarantined spam mails named `SPAMQUAR`.

To control spam filter, find the *Spam filter* menu between the *Internet Agent protection* settings.

! Important!
Using spam filter results performance impact to the server. Starting or stopping of the program may take several minutes!

Install Post Office filter

Copy the `VBPOSCAN.NLM` file into the installation directory (for example: `SYS:/SYSTEM/VBUSTER`).

To activate Post Office module, you need to generate an identifier key that allows the Post Office scanner to access mails stored in the post offices. Key generation must be done on a Windows client before the first run of POA scanner. Run the `vbpotapp.exe` file (it also needs the `gwtapp.dll`) found in the package to generate. If existed key is found, you will be warned about overwriting.

You need to enter the following path to generate the key:

- GroupWise domain database file path on the Novell server (`wpdomain.db`)
- VirusBuster for Mail Servers (GroupWise) configuration file path (`vbgwise.set`)

After key generation, the GroupWise internal communication mechanism replicates the key to the other agents. It can take some minutes according to the network communication speed.

Start the `VBPOSCAN.NLM` then configure the Post Office filter with the help of `VBGWSET.NLM`.

To run Post Office protection, run the `VBPOSCAN` program (`load vbposcan`).

If you want the Post office protection module to be started automatically together with the server then you should insert the next line into the `SYS:SYSTEM/AUTOEXEC.NCF` file:

```
load vbposcan.nlm
```

Program's structure

The VirusBuster for Mail Servers (GroupWise) cooperates with VirusBuster for NetWare Servers. Proper functioning can only be guaranteed if VirusBuster for NetWare Servers is installed and activated.

Attention!

`VBGWIA.NLM` needs `VBENGINE.NLM` to scan letters and forwards its log entries to `VBSHIELD.NLM` so always unload `VBGWIA.NLM` before unloading VirusBuster for NetWare Servers!

If the content of `VBGWISE.SET` is modified while running `VBGWIA.NLM`, the `VBGWIA.NLM` can be warned by loading `VBNOTIFY.NLM` then the `VBGWIA.NLM` will reload settings.

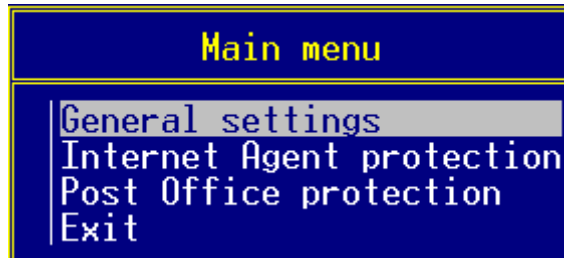
Program's user interface

The program's settings can be managed through NetWare's `NWSNUT.NLM` menu system. The following keys are available to navigate in the menu system:

- Cursor keys, `PgDn`, `PgUp` - Movement among individual menu items.
- `Enter` key - Selecting a menu item.
- `ESC` key - Existing a menu item or the program.
- `F1` key - Displays help.
- `Delete` key - Deleting entry.
- `Insert` key - Inserting entry.

Detailed overview

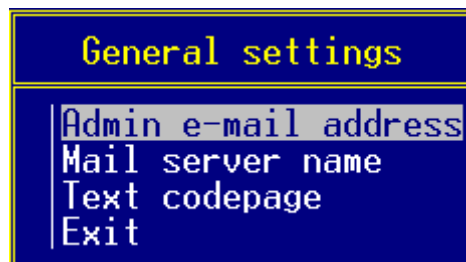
The program's settings can be found in the `VBGWISE.SET` file. The settings can be modified with the help of `VBGWSET.NLM`'s menu system. The menu system's structure:



Main menu

Settings of Internet Agent and Post Office protection could be found in two separated menu item. Options found in the *General settings* are used both IA and PO protection modules. The following lines provides you detailed information about configuration of the anti-virus system.

General settings



General settings

Options found in this menu are common options for the Internet Agent and Post Office protection:

Admin e-mail address

The notification mail will be forwarded to the specified address.

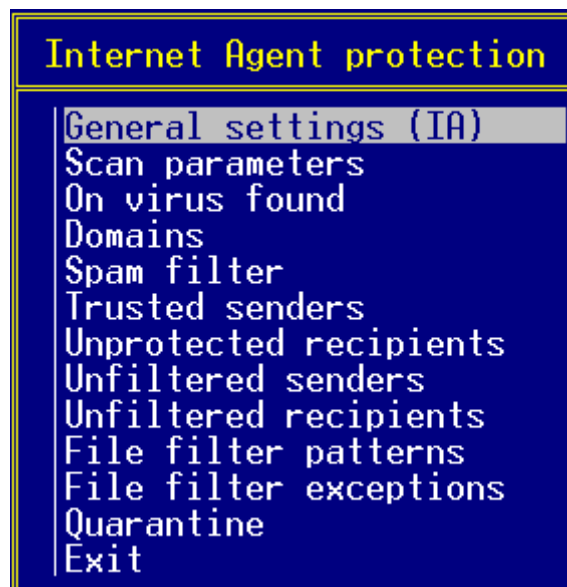
Mail server name

SMTP server's name or IP address needed for mail delivery to the recipient.

Text codepage

The code page of texts connected to event notification can be set here.

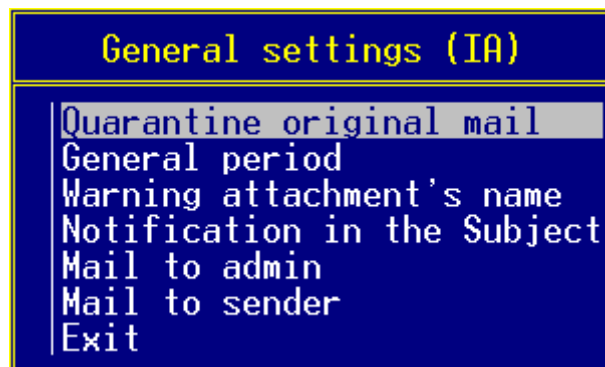
Internet Agent protection



Internet Agent protection

The Internet Agent is responsible for e-mail transmission and makes connection between the Internet and local networks. Detailed information about virus and spam filter could be found hereafter.

General settings (IA)



General settings (IA)

Quarantine original mail

If an e-mail is modified, the original one will be moved to the quarantine.

General Period

Time period setting for those tasks which do not belong to either of domains. The program executes the tasks by the specified interval.

Warning attachment's name

The warning attachment's name, which will be sent with the modified e-mail can be set here.

Notification in the subject

If this option is enabled, the program inserts information in the mail's subject line to inform the user on the results of scanning.

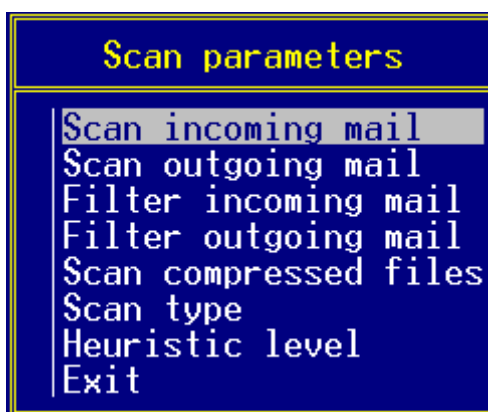
Mail to admin

Enable/disable sending notification mail to the administrator on incidents.

Mail to sender

Enable/disable sending notification mail to the user on incidents.

Scan parameters



Scan parameters

Scan incoming mail

Scanning of incoming mail can be enabled or disabled.

Scan outgoing mail

Scanning of outgoing mail can be enabled or disabled.

Filter incoming mail

If the incoming e-mail has an attachment, which matches any of the patterns set in file filter patterns, the program will remove it if this option is enabled.

Filter outgoing mail

If the outgoing e-mail has an attachment, which matches any of the patterns set in file filter patterns, the program will remove it if this option is enabled.

Scan compressed files

The scanning of compressed attachments can be enabled or disabled.

Scan type

The virus scanning engine is able to scan for and detect viruses according to the set methods/levels. It is possible to choose the needed scanning method in the components in the software. The following levels are available:

- Fast
Scans only those parts of the file, which are most likely to contain a virus and does not detect viruses, which can only be detected by using a major amount of system resources (e.g. Excel

FORMULA viruses).

- Strict
Optimized scanning method, which detects all viruses registered in the virus database and scans those parts of the file, which are most likely to contain a virus.
- Full
Detects all viruses registered in the virus database and scans the whole file, even those parts, where viruses are not likely to be found.

Heuristic level

During the heuristic analysis, the software tries to detect codes and programs, which have virus-like characteristics but are not registered in the virus database. If such a suspicious file is found, the user is notified. The following levels of heuristic analysis are available:

- Off
No heuristic analysis.
- Normal
The depth of the analysis is limited, the possibility of false positives is low, but the chance of detecting unknown viruses is not too high.
- Strong
The chance of detecting unknown viruses is higher, but there is a higher possibility of false positives.

On virus found



Actions in case of virus found

Virus handling

The action, which will be performed on the infected file can be set here. The infected file can be deleted, disinfected or you can also delete the whole mail, if you want.

WormBuster

If you enable this function then the mails infected by I-Worm-type will be blocked without notification.

Suspicious files

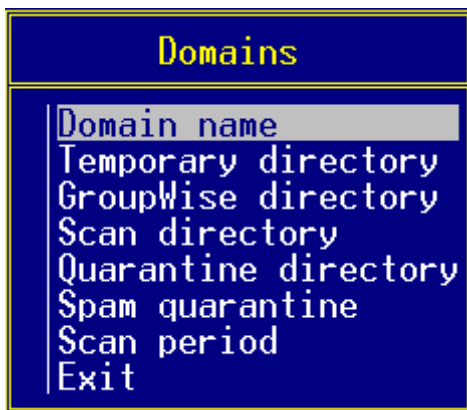
The action, which will be performed on files that are considered suspicious by the heuristic scan can be set here.

Password protected archives

If a compressed file is fail to scan because it is protected by password then the program will block it if this option is enabled.

On scan error

If any errors occur during scanning the certain mail can be blocked if this option is enabled.

Domains

Domain settings

Domain name

The protection area's name can be specified here.

Temporary directory (e.g. `... \WPGATE\GWIA\VBGWIA\TEMP`)

Temporary files will get into this directory.

GroupWise directory (e.g. `... \WPGATE\GWIA`)

The GroupWise Internet Agent's work directory can be specified here. GroupWise's `SEND`, `RECEIVE`, `RESULT` directories can be found here.

Scan directory (e.g. `... \WPGATE\GWIA\VBGWIA`)

The GroupWise's work directory for SMTP scan can be specified here (`SEND`, `RECEIVE`, `RESULT`, quarantine and temporary directories must be created manually in this directory).

Quarantine directory (e.g. `... \WPGATE\GWIA\VBGWIA\QUAR`)

Specify a directory, into which the modified mail's original instances will be placed.

Spam quarantine (e.g. `... \WPGATE\GWIA\VBGWIA\SPAMQUAR`)

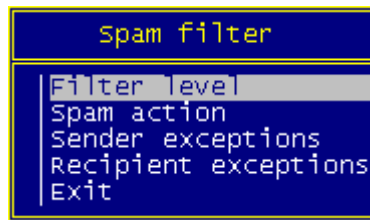
Quarantine directory for that mails' original instances marked as spam by the active spam filter.

Scan period

A scan period can be set inside the current protection area.

Spam filter

VirusBuster for Mail Servers (GroupWise) made for mailing systems to protect them against virus attacks and now it is provided with spam filtering as well to protect you and your computer against unsolicited mails.



Spam filter settings

Filter level

You can enable or disable the activity of the Spam filter and set its sensibility.

If you select the No filter item, the Spam filter will be disabled. If the other settings are used, the Spam filter will be activated and its sensibility depends on your selection.

Spam action

The following options can be performed on the mails which are declared as spam by the filter:

- None: the mail is forwarded without any interaction and you can have the mail copied into the quarantine directory.
- Mark mail:
 - Subject change
You can change the content of the *Subject* field of the mail in the appeared window. You are allowed to specify the new content and use the `%Subject%` token representing the content of the original *Subject* field of the mail.
 - 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: the mail will not be forwarded to the recipient(s), it will be deleted. But you can have the mail copied into the quarantine directory, as well.
- To quarantine: the mail will not be forwarded to the recipient(s), it is moved to the quarantine directory.

Keep in mind, if spam mail is detected, log message is got into the `VBUSTER.LOG` file without exception. You can set the quarantine directory in the *Domains* menu item. It is recommended to use the `SPAMQUAR` directory which having been created in the course of installation.

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 area (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

Mails sent from that address (domain name) enumerated in this settings are not filtered by the spam filter, these are forwarded to their recipients without any spam checking. You can use the **INSERT** and the **DELETE** keys to add or remove items (address) from the list.

Recipient exceptions

Mails received by that address(es) (domain name(s)) enumerated in this settings are not filtered by the spam filter.

Trusted senders

The program will not scan messages coming from the given addresses. The following rules are applied to the addresses:

- The address is a common e-mail address in which ***** and **?** characters can be used as wild cards, the ***** substitutes an undefined number of characters whilst the **?** only substitutes a single character. The **@** sign can't be substituted!
- If the address begins with **@**, it is applied to all users on the given host.

Unprotected recipients

The program does not scan mail sent to the given addresses.

Unfiltered senders

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

Unfiltered recipients

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

File filter patterns

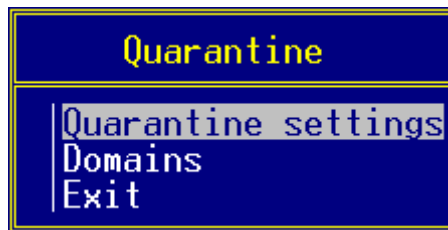
Attachments, which match the given file name patterns are removed from messages without scanning (for example: ***.com**, ***.exe**, ***.doc**).

File filter exceptions

That files can be given here to which filter patterns should not be applied (for example: [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

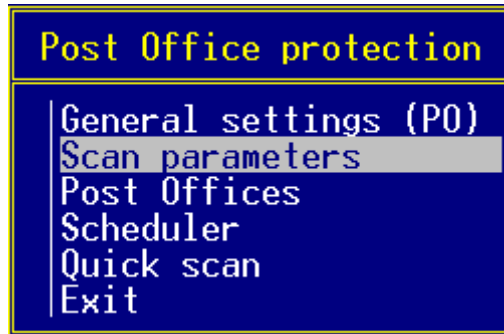
You can select a protection area (domain here) to display a list of items found in its spam or virus quarantine.

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



Post Office protection

The Post Office protection module allows off-line virus scanning of Post offices storing users' mailbox. The system scans for viruses according to the settings at the scheduled dates. The off-line virus scan provides more security for the mail-database preventing virus spreading and blocking infected mails that have managed to get in the system.

Important!
If the folder to be scanned contains more than 5000 items, it can't be opened to check because of the limit of IMAP protocol!

General settings (PO)

General settings of Post Office module:

Mail to Admin

Entering this option you will get a list including system events. If the event(s) found in the list occurs, the program will send a message to the system administrator.

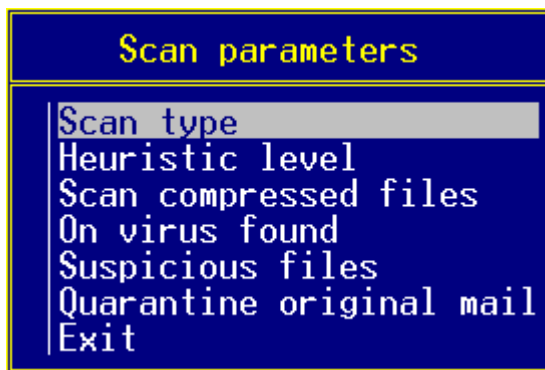
Handling the list:

The list is empty by default, use the **Insert** key to add events. If you press the key, you will get a new list including system events. Use the **Enter** key to select one of them then you will get back to the main list extended with the selected event. Repeat this if you want to set several events to be reported. Use the **Delete** key to delete events from the list.

Mail to user

User notification when the selected event(s) occurs. You have to fill the same list as described above.

Scan parameters



Scan settings

Scan type

These values are the same as you can select in the [Scan type](#) options of Internet Agent section.

Heuristic level

These values are the same as you can select in the [Heuristic level](#) options of Internet Agent section.

Scan compressed files

If you select this option, the scanner will scan also the compressed files.

On virus found

Select action for virus incidents. On failed kill attempt, the program changes the file to a text file named: [<filename>.txt](#). You can find more information in this text file about action taken.

Suspicious files

Select action for suspicious files.

Quarantine original mail

If the mail is modified during the scan and you have activated this function, the program will move the original instance of the mail to the quarantine. Set the quarantine folder in the [Quarantine IMAP folder](#) option.

Post Offices

In this menu you can add Post Offices to be protected by VirusBuster for Mail Servers (GroupWise). Entering the menu a list window appears including the Post Offices selected by you. This list is empty by default which is announced by a warning message.

To add new Post Offices to the list, use the **Insert** key.

! Figyelem!

Alapértelmezett telepítés esetén az IMAP protokollon keresztüli kommunikáció nincs engedélyezve a Post Office Agent-ben, ezért Console One segítségével, a Post Office Agent beállításainál a *GroupWise/Agent Settings* opcióban engedélyezzük. A *GroupWise/Network Address* pontban állítsuk be, hogy a POA mely porton keresztül kezelje az IMAP protokollt. Ügyeljünk arra, hogy ez az érték nem egyezhet meg a GWIA-hoz használt hasonló beállítással (ez az érték általában a 143-as port, a POA-hoz ettől eltérőt állítsunk be).

After entering a name for the Post Office, you need to specify additional data to complete Post Office

definition in the appearing window. You can modify these data at any time you want later selecting the name of the Post Office with the **Enter** key. If you want to delete an existed Post Office from the list, select it and use the **Delete** key.



Post Office settings

Post Office name

ID of Post Office in the antivirus system. You can refer to the specified Post Office by this name.

Host name

Server computer's name or IP address the Post Office is found on.

Port

Enter the port number for the Post Office.

Scan only new mails

If you launch a scan and this option is active, the scanner will only scan the recently received mails.

Scan all users

All users of the current Post Office will be scanned if this function is active.

User exceptions

If *Scan all users* option is active, you can define user(s) who will be skipped from the scanning.

Users to scan

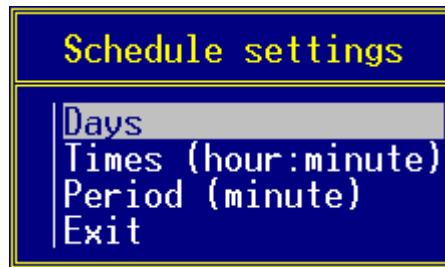
Set users to scan in the current Post Office. There is no reason for setting this option if *Scan all users* option is active.

Quarantine IMAP folder

Set the quarantine folder for storing quarantined objects. Name this folder as `<user>/<folder>` (e.g.: `admin/quar`) which is a common quarantine folder. It is possible to create quarantine folder for each user, use the following form: `%CURRENT_USER%/<folder>`

Scheduler

Schedule the scanning of Post Offices in this menu. Entering the menu, first you have to select a Post Office then specify the schedule settings for the selected one.



Schedule settings

You can define period or exact time to schedule virus scanning. The following settings are available to customize automatic scanning for the selected Post Office:

Days

Define a day or days on which you want to launch virus scan automatically. You can select days from a list the same way as it is described in the [General settings \(PO\)](#) section. If you don't set time or period for the day(s) the scanner will not be run.

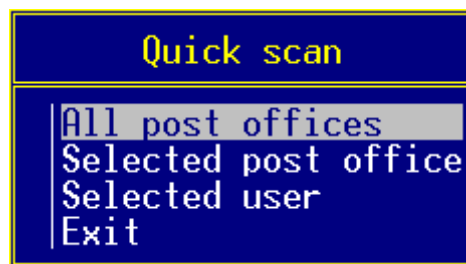
Times (hour:minute)

Set exact time(s) for the selected days (or for every day if the *Days* list is left empty) when you want the virus scan to be launched. A list includes the times, use this list the same way as it is described in the [General settings \(PO\)](#) section. You have to specify the time in the following form: **hh:mm** (hh – hour, mm-minute).

Period (minute)

In this setting you can enter a time period in minute. Always when this period expires, the program will start the virus scan.

Quick scan



Quick scan

All post offices

Scans all the Post Offices protected by the anti-virus system (listed in the *Post Offices* menu). It will only scan the allowed users of Post Offices.

Selected post office

You can select one from the protected Post Offices to scan. It will only scan the allowed users of Post Offices.

Selected user

First you have to select a Post Office then select the user you want to scan.

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
support@virusbuster.hu