

VIRUS BUSTER

for NetWare Servers

TABLE OF CONTENTS

VIRUSBUSTER FOR NETWARE SERVERS	1
Minimal system requirements	1
Installation.....	2
Automatic installation.....	2
Manual installation	2
Program's structure	3
Scanning possibilities	3
Protection units.....	4
Program's user interface.....	4
Detailed overview	5
Engine options.....	5
Domain management	8
Message redirection	10
Global options.....	13
Quarantine.....	14
Information.....	15
Runtime options.....	15
Registration.....	15
UPDATE MANAGER	17
Settings	17
Module versions	18
Manual update	18
Information.....	19
END USER AGREEMENT	20
CONTACT	21

VIRUSBUSTER FOR NETWARE SERVERS

In a network environment, the protection of servers is crucial as most of the data used for our everyday work is stored and transferred by servers. Therefore the effective protection of these servers does not only secure the stored data, but provides a secondary defense line for clients connected to them.

VirusBuster for NetWare Servers provides resident protection for data, systems and therefore for the everyday work, optimized to the increased data traffic of servers. The easy-to-use, traditional NetWare-based user interface, the clear settings and continuous updates ensure, that the protection of the company's NetWare servers operate automatically and effectively.

Main features:

- Effective resident protection against viruses for servers
- Separate protection areas to handle servers' storage disks or their smaller areas individually
- Intelligent file protection, extended write protection to prevent infections
- Manual and scheduled virus scans
- Automatic updates
- Intelligent quarantine for storing infected files
- Incremental virus database update

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

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).

Automatic installation

The following package is available:

`nwshield-<product version>-<engine version>-<language>.exe`

Example:

`nwshield-2.2.08-4.2.13-en.exe`

- After the welcome panel and accepting the license agreement, you can set the target folder that you want to install the product to.
- 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 main component is essential to install, the Update Manager is 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).

VirusBuster for NetWare Servers

- *Start protection*: If it is checked, the antivirus protection will be started automatically after the installation.

- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the `autoexec.ncf` file (consult the *Manual installation* section for more).

- *Registration*: If it is checked, the registration data can be entered during the installation.

VirusBuster Update Manager

- *Start module*: If it is checked, the Update Manager module will be started after installation.

- If you have selected the *Registration* action before, you have to enter the valid registration data in the following panel.
- After these settings the installation process will be started and the selected actions will be performed.

Manual installation

The following package is available:

`nwshield-<product version>-<engine version>-<language>.zip`

Example:

`nwshield-2.2.08-4.2.13-en.zip`

The product can be run on Novell NetWare servers and must be placed on the server's SYS: volume in a subdirectory so that it can be launched from console. The installation should be performed in domain administrator security context.

Steps when installing the product for the first time:

- Log on to a workstation using a domain administrator account. Create a subdirectory named **vbuster** in the **SYS:\SYSTEM** directory for the program. The configuration file, log file and the **QUAR** (quarantine) and **TEMP** (folder of temporary files) directories will be created here automatically. Add this new directory to the **search path** list by using the **search add sys:system/vbuster** command.
- Copy the program's files (**VBSHLD4.NLM**, **VBENGINE.NLM**, **VBUSTER.INI** and the virus database (the **DATABASE** directory and its content)). Also copy the **VBUPDATE.NLM** and **VBUPDASC.NLM** files for automatic updating.
- Insert the **search add 1 sys:system/vbuster** line into **SYS:SYSTEM/AUTOEXEC.NCF** file. If you want the protection to be started automatically together with the server then you should insert the next line, too: **load vbshld4.nlm**. The **SYS:SYSTEM/AUTOEXEC.NCF** file can be modified with any editor from a workstation or with **INSTALL.NLM** from the server (NCF files options/ Edit **AUTOEXEC.NCF** file).
- Create a new user with system administrator security context in Novell NetWare's system administration program (NetWare Administrator or ConsoleOne) exclusively for virus protection. Recommended user name: **vbuster**. This user should be added to the program's special user group.
- Launch the program on the server with the **load vbshld4** command and perform the program's configuration.

If everything is all right, the modules will be loaded and two new entries will be displayed in the console screen's list (VBSShield Screen and VBSShield Console).

Program's structure

VirusBuster for NetWare Servers is a general Novell NetWare loadable module (NLM) that should be run on the server. After it having been loaded, it checks the server's every operation and scans every file before performing an operation on them.

If it finds a virus in the scanned file, it initiates the actions specified in the settings. It can deny the operation, put the infected file into the quarantine, disinfect the virus, and send a message to the users concerned, domain administrators or any other users. It puts all information gathered during its operation into a log file.

It is possible to define a file access rights system above Novell NetWare's possibilities. Writing of specified network directories or files can be banned easily this way preventing virus infection too.

Scanning possibilities

VirusBuster for NetWare Servers scans files in two ways. On the one hand it monitors every file operation on the server, in other words, it checks every incoming request and only allows access to virus-free files. On the other hand full virus scans can be requested, at a given time, for a specific protection area which can either be scheduled or can be launched manually from the console.

- On access scan
In case of on access scan, the program automatically scans a file for viruses when its reading is requested. The types of files, which should be scanned, can be set in every domain. There are two lists for this purpose; the first of this contains file-masks of what should be scanned whilst the other contains excluded file-masks.

- Periodical scan
In case of a periodical scan every file in the domain will be scanned. The periodical scan can be started manually or automatically at times specified for each domain.
- Write protection of files
The program is able to provide write protection for files by complementing the Novell NetWare network file access protection system. Write protection is users independent in other words it applies to all users. In every domain it can be set whether write protection is enabled or disabled similarly, the mask for files that should be protected or should be excluded can also be set for each domain.

Protection units

Similarly to the Novell NetWare security context system, the scanning and protection options for VirusBuster for NetWare Servers can be set individually in every domain. One subdirectory structure of the server belongs to each of the protection units. If this subdirectory does not contain further protection units, the unit will be applied to all subdirectories and files in that directory. If the subdirectory contains further protection units, the upper unit will not be applied to its subdirectories. That is to say a file only belongs to one protection unit and the same settings are applied to every file inside a protection unit.

Program's user interface

The functions and settings of the product can be accessed through Novell NetWare's regular menu system. After having started the program its functions and settings can be accessed through menus.

Using menus

- Cursor keys - Movement between menu items
- **Enter** key - Selection of the menu item
- **ESC** key - Exiting a sub-menu item or the program
- **F1** key - Displays program help

In the program the basic unit for configuration is the list. Items in the list can be modified, deleted, added or an item can be configured in more detail with the help of the following keys:

Using lists

- Cursor keys, **PgDn**, **PgUp** - Movement between list items
- **Enter** key - Selection of one or more list entries
- **F5** key - Highlighting entries or disabling highlight
- **Delete** key - Removal of an entry
- **Insert** key - Adding a new entry
- **F3** key - Renaming an entry

When specifying the date worksheet the required dates should be marked with a * (star) in the table which appears.

Specifying dates

- Cursor moving keys, with which you can move in the sheet
- It is possible to select an interval by pressing **F5** key
- By pressing **Ins** or the star (*) key the actual date or interval can be selected
- By pressing **Delete** or **Space** key the actual date or interval can be deselected
- By pressing **Enter** key the selection of the actual date or interval can be inverted

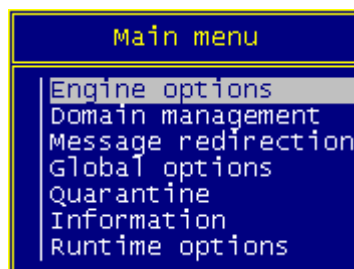
Detailed overview

The product can be launched by the **VBSHLD4.NLM**. The program creates two screens:

- VBShield Screen - The programs operations and logged events can be monitored here.
- VBShield Console – The program can be configured here, individual options can be set here and periodical scans can be launched from here manually.

Note!

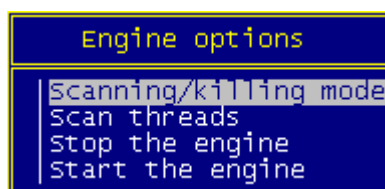
If you leave or exit the screens, the protection will also be terminated. After exiting, scans and periodical scans will not be executed!



Main menu

A more detailed insight of the program can be gained by going through the menu items.

Engine options



Engine options

Scanning/killing mode

```
Scanning/killing mode
Scan packed/MIME files: Enabled
  Temporary directory: SYS:\SYSTEM\vbuster_ ...
          Scan: Strict
          virus killing: Disabled
          Non-killable viruses: Keep file
In case of protection error: Access enabled
          General heuristics: Normal
          suspicious programs: Keep file
```

Scanning/killing mode

Scan packed/MIME files

If it is activated, the program will perform a virus scan on compressed files.

Temporary directory

During scanning the program temporarily places the content of a compressed and MIME files into the specified directory.

Scan

Scan method can be set under this point:

- Strict: Optimized scanning method searches for viruses in those parts of a file where they are likely to be found.
- Fast: Optimized scanning method will only scans for viruses in those parts of a file, where they are likely to be found. This scanning method is the one recommended in most cases.
- Full: Scans the whole file, even places where under normal circumstance viruses are not found, thereby increasing the chance of false alarms. This method is very time-consuming.

Virus killing

The program will remove the virus from the infected file, if possible, if this option is enabled.

Non-killable viruses

Some viruses cannot be removed even if they are recognized. The action, which will be performed when such a virus is found can be set here:

- Rename file: renames the infected file.
- File to quarantine: moves the infected file to the quarantine directory.
- Keep file: does nothing with the infected file.
- Delete file: deletes the infected file.

In case of protection error

It can be set whether the program should prohibit an access request in case of file access error or not.

General heuristics

Heuristic scan mode can be enabled or disabled and its sensitivity can be set here. 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:

- *Disabled*
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.

Suspicious programs

The action set here will be performed when a program file is considered suspicious during the heuristic scan:

- Rename file: renames the infected file.
- File to quarantine: moves the infected file to the quarantine directory.
- Keep file: does nothing with the infected file.
- Delete file: deletes the infected file.

Scan threads

The number of parallel scanning threads can be set here.

```
Scan threads
-----
Total number of scanner threads: 16
                               (Max.: 16, min.: 2!)
Reserved for on-access scan: 13
                               (Max.: total-1, min.: 1!)
```

Scan threads

Note!
The value must be between 2 and 16. The new value will be applied when the scan engine is restarted!

The program operates with four threads by default. Two threads are always kept for receiving incoming requests, for on-access scan. Increasing the number of threads can reduce system performance although more files can be scanned this way.

Stop the engine

It is seldom that we only want to stop the scan engine independently from the rest of the program, however, it can be rather useful during program update as like this the engine can be changed on the fly.

Note!
By stopping the scan engine, the defense still remains active, but no scans can be performed. This can result in the inaccessibility of certain files!

Start the engine

Starting the engine and loading the actual VDB with the set scan number.

Note!
Always check if the proper VBENGINE.NLM and virus database files are available in the search path. VBENGINE.NLM will only be launched if it exists and if the version of the virus database and VBENGINE.NLM is proper!

Domain management

All protection units (domains) are listed in the "Domain entries list" window. Units can be created, deleted or renamed in this list.

The / (root) protection unit cannot be deleted or renamed. If a unit is renamed (**F3** key), all entries connected to it will be renamed as the new domain. If a unit is deleted (**Delete** key), entries will be deleted and if any messaging system would be terminated this way, the program will warn the user. If a periodical scan is running on the unit, which is renamed or deleted, the scan stops immediately. If a new unit is created, it will inherit all characteristics of the unit, which has been selected when having pressed the **Insert** key.

Note!
The protection unit is inactive while configuring it. Do not leave the configuration window open!

The following modifications can be made inside a protection unit settings:

```
SYSTEM
Domain path: SYS:SYSTEM
On-access scan: Enabled
Virus found action: Access denied
Periodic scan: (time table)
Files to be scanned: (list)
Exceptions: (list)
Write protection of files: Enabled
Write protected files: (list)
Exceptions: (list)
```

Domain's settings

Domain path

Every protection unit has a subdirectory. This subdirectory can be set here. The full path must be set in **volume name:path** form. When specifying a path, directories can be divided either by the "/" or "\" sign.

On-access scan

On-access scan of files stored on the server can be enabled or disabled. The program scans files on access if this option is enabled.

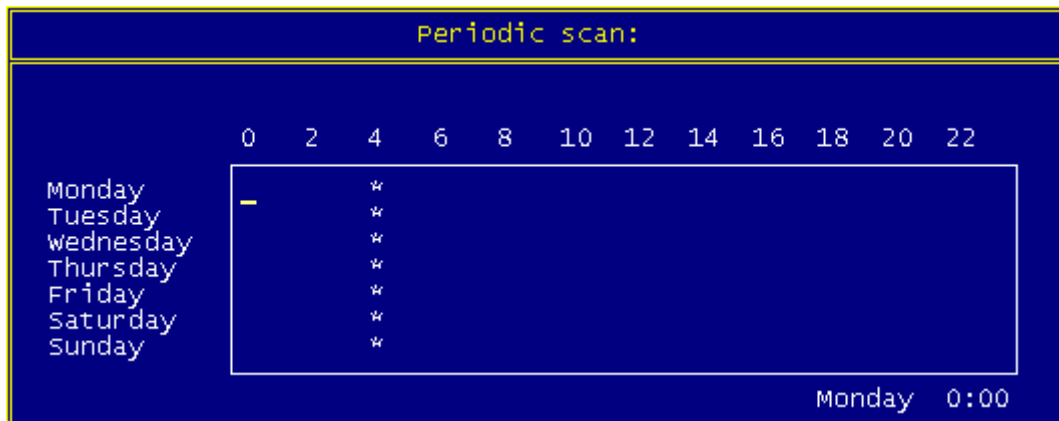
Virus found action

If on-access scan is enabled, the action, which will be performed when a virus is found during an on-access scan, can be set here:

- File to quarantine: the infected file will be moved to the directory set in Global options/Virus collector.
- Access denied: denies access to infected files.
- No action: does nothing with the infected file.
- Delete file: deletes the infected file.

Periodic scan

Periodic scans can be set in 30 minute long intervals in this window so that the program would perform scans weekly in the given domain's directories at given times. If the program detects that it has to perform a scan in the interval when it is started it will perform the scan immediately.



Periodic scanning

Files to be scanned

The masks of files, which should be scanned when accessed, can be selected here (e.g: `*.com`, `*.exe`, `*.doc`).

Exceptions

The masks of files, which should not be scanned when accessed, can be selected here (e.g: `command.com`).

Write protection of files

The write protection can be enabled or disabled here. This protection is not applied to special users.

Write protected files

The masks of files, which are protected can be selected here.

Exceptions

The masks of files that should not be write-protected can be selected here.

! Note!

If the configuration file (`VBUSTER.CFG`) does not exist in VirusBuster for NetWare Servers' directory, the entries of protection units will be created, with default settings, when the program is started. According to these entries on-access scan is performed on all executable files that are stored on the server. Periodical scan is performed every day at 4:00 am all executable files each on domain. Write protection is only applied to files under `SYS:LOGIN`, `SYS:PUBLIC` and `SYS:SYSTEM` by default.

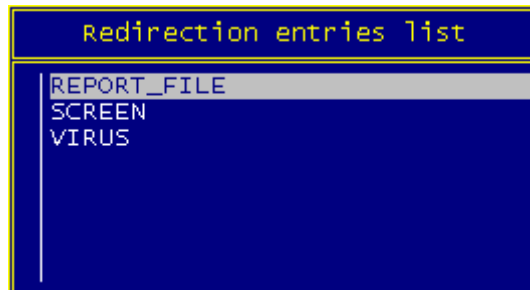
Message redirection

The program displays the name of the redirection entry in this menu. Redirection entries can be created, deleted or renamed in this list. The options of a unit can be accessed by selecting the unit.

Note!
The unit will remain inactive during configuration!

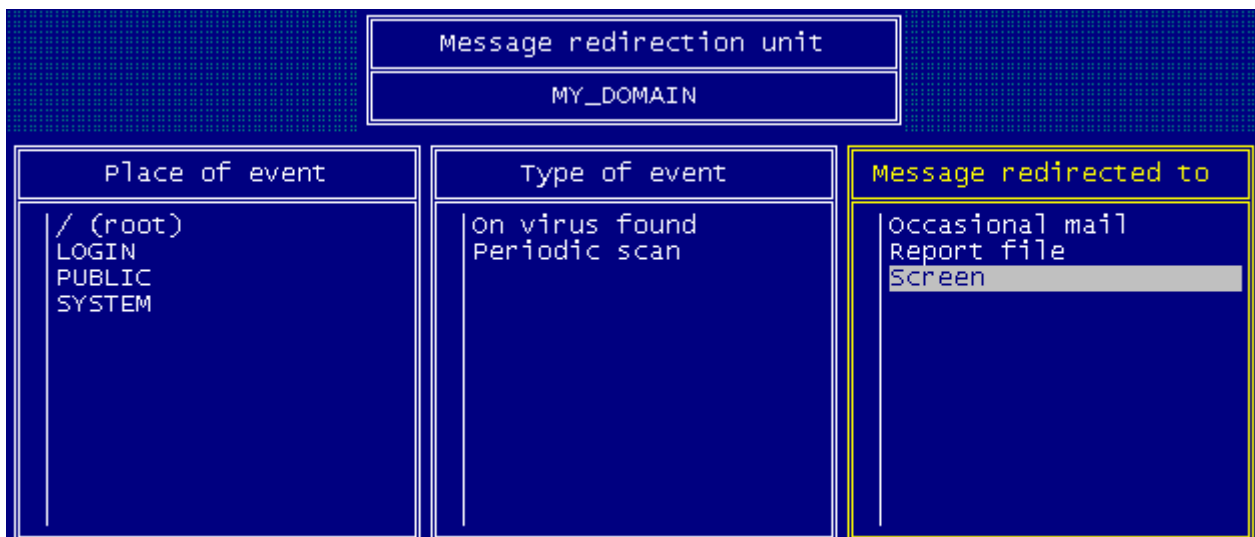
During redirection configuration you have to specify where the messages should be forwarded which were created at a given location as a consequence of a given event. Three units are present in the program by default:

- Report file - A log file, in which all events are stored that occurred during the system's operation.
- Screen - The program's screen messages.
- Virus - A unit, which contains several addresses and is activated when a virus is found.



Redirection entries

When configuring a Message redirection unit, you have to specify the following data: Where was the message to be forwarded created, what was it triggered by and where should it be forwarded to.



Message unit panel

Place of event

The message redirection unit's place of creation contains the following settings:

General

Describes the place of creation of those messages, which cannot be connected to any protection units. If a message control unit contains the "general" place of creation description, than the unit was created inside VirusBuster for NetWare Servers, which means that it can forward messages that cannot be connected to any protection units.

Domain name

If a domain's name can be found in a message control unit's place of creation field, the unit will be applied to messages created in the given protection unit. When creating a new protection unit, it will inherit the characteristics of the unit, which has been selected when pressing the **Insert** key. These settings can be modified.

Type of event

The message control unit classifies events into four main groups:

File protection

Describes events made by VirusBuster for NetWare Servers' file protection system. If enabled, the message control unit will forward messages, which have been created when performing an illegal writing process in any domain included in the place of creation list.

Information

Describes events, which has been caused by VirusBuster for NetWare Servers, but are not connected to the program's scanning or protection system. The message control unit will forward the following messages if enabled:

- Occasional mail has been sent: The program generates a confirmation message when an occasional mail is sent. If the option is enabled, the unit also forwards this message.
- Component: If the option is enabled, messages created by an external component will be registered.
- Engine events: The program generates a message on every event, which occurs connected to the engine.
- File changed: If a virus had been found and the infected file has been moved to a given folder or has been renamed, it sends a message. By logging these, it is possible to recover these files.
- Error: All errors, which occur inside the program generates a message. If the option is enabled, the unit forwards this message it also forwards a message describing the error.
- Error message from engine: The program generates a message on every error, which occurs connected to the engine.
- Configuration has changed: If the option is enabled, messages created when the program's configuration had been modified are forwarded.
- VirusBuster for NetWare Servers has started: If the option is enabled, the message created on program launch will be forwarded.
- VirusBuster for NetWare Servers has stopped: If the option is enabled, the message created on program stop will be forwarded.
- Periodic mail has been sent: The program generates a confirmation message when a regular mail is sent. If the option is enabled, the unit also forwards this message.

Periodic scan

Describes events caused by VirusBuster for NetWare Servers' periodical scan system. The message control unit will forward the following messages describing the status of periodical scans in the given

protection units:

- File to be scanned: The program has arrived at a new file during periodical scan. The message contains the name of the protection unit and the file.
- Scan sub-directory: The program has arrived at a new subdirectory during periodical scan. The message contains the name of the protection unit and the directory.
- Scan started: The program's periodical scan system has initiated a periodical scan on a protection unit. The message contains the name of the protection unit.
- Scan stopped: The program's periodical scan system has finished a periodical scan on a protection unit. The message contains the name of the protection unit.
- Scan aborted: The program's periodical scan system has aborted one of the running periodical scans on a protection unit due to user intervention. The message contains the name of the protection unit.

On virus found

Describes events caused by VirusBuster for NetWare Servers' virus scanning system. The message control unit will forward a message if a virus is found in the listed protection units regardless of the fact whether it was a periodical or an on-access scan. Depending on the scan result the messages can be the following:

- Suspicious: The virus scanning system has found a suspicious code part indicating the presence of a virus when scanning a file.
- Immuniser: The program has found a file, which has been disinfected by a virus scanner.
- Internet worm (I-Worm): The program found an Internet worm-type malware.
- Mutant: The virus scanning system has found a code part similar to a known virus when scanning a file.
- Sequence: The virus scanning system has found a byte sequence, which can be found in a virus.
- Non-killable: The program has found a file, which has been ruined by a virus so it cannot be disinfected.
- Packed: The program has found a compressed file, which contains a virus.
- Trojan program: The program has found a file, which contains a Trojan program.
- Virus: The virus scanning system has found a virus.

Messages' recipients

The message control unit can send messages to the following recipients:

Occasional mail

Sends an occasional mail to recipients given in global options.

ErrorLog

Writes the message into Novell NetWare's error log file (`SYS:SYSTEM/SYS$LOG.ERR`).

User

If the event, which has caused the message, can be connected to a user, the program sends a broadcast message to the user.

Screen

The message will be displayed on the server, on the VBShield Screen.

Console

The message will be displayed on the server, on the System Console screen.

Operator

The message will be broadcasted to every operator, which can be given optionally. The message will only be sent to operators, who are logged on to the network when the event occurs. Operators must be added to the operator list before activating the message sending unit.

Periodic mail

Sends periodic mail (at given times) to recipients given in global options.

Report file

Writes the message into the file, which can be given optionally (the default is `vbuster.log`).

Type of message

The language of the message and the level of details can be given in case of every output. The level of details can be one of the following:

Short

The message contains only one line. Broadcast messages can only be sent as a short message.

Normal

The message contains all information on the event except for:

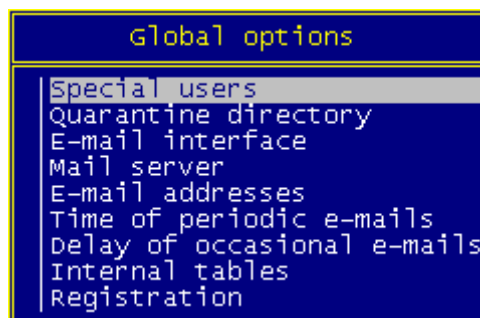
- If the event can be connected to a file, its path is displayed in a shortened form.
- The date of the event is not included.
- Does not contain the physical base address connected to the event.

Detailed

The message contains information on the event including.

Global options

The programs general settings can be found in the Global options menu.



Global options

Special users

The list of users, who can write or read protected files, can be specified here. These users can perform disinfection while VirusBuster for NetWare Servers is running. In this case, users using the server, do not have to log out from the network.

Quarantine directory

If a virus is found and it must be moved according to the program's settings, the infected file will be moved to this directory.

E-mail interface

The e-mail interface, which is used when sending periodical or single messages, can be set here.

- None: The program does not send mails.
- Socket: E-mails are forwarded with the aid of a socket.

Mail server

You can specify the domain name of IP address of the SMTP server used for message forwarding

E-mail addresses

The following users will receive the message, which can be a periodical or an occasional e-mail.

Time of periodic e-mails

The times, when periodical messages are sent can be given in this table in 30 minute intervals weekly.

Delay of occasional e-mails

If the appropriate delay is set, than it is here that it can be specified that the sending of an occasional e-mail should be delayed for a certain time.

Internal tables

The size of VirusBuster for NetWare Servers' internal tables can be set here. The size of tables is given in bytes. The size of the following tables can be set:

- On-access file cache size: The program places the names of the files, which were considered virus-free during the on-access scan in this table. In case of repeated access the file will not be scanned if its name is in this table. In case of writing, the file's name will be automatically removed from the table. If you do not want to use this option, set the size of file cache to 0.
- Redirection table: The size for storing message control units can be set here.
- Domain table: The size for storing protection units can be set here.

Quarantine

The task of the quarantine is to store infected or suspicious files and handle them according to the settings.

If you select a quarantined item you will get some information on the selected file in a new window and you can choose from the actions performed on the file by using the *Quarantine actions* menu item.

- Keep: The program keeps the file as it is.
- Save as: The program saves the file coded, so it can be sent for analysis.
- Delete: The program deletes the selected file permanently.
- Rescan: The program performs a scan on the file and removes the virus from it if it is possible.
- Restore: The program restores the file to its original location if the given path exists and if a file with the same name does not exist at the said location.

The selected action will be performed after closing the window!

Information

In this menu you can request information on units known by the program.

About

The addresses and phone numbers connected to the program's distribution and support and version numbers are displayed here. The status of the scan engine can be checked here (loaded or unloaded).

Runtime options

The following options are displayed:

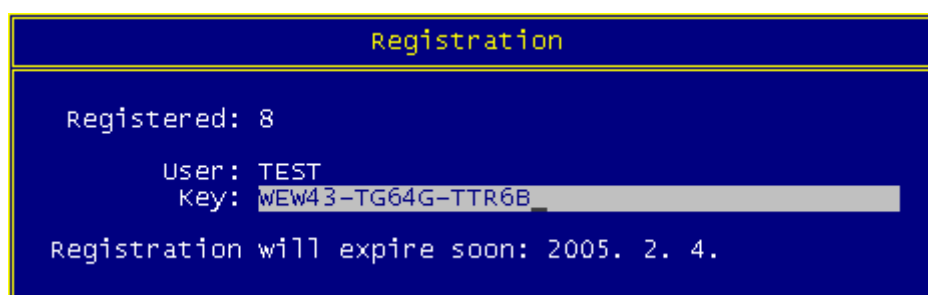
- Start scanning: Displays the list of domains, where a scan can be performed (no scans are running, the domain entry is valid). After having selected the domain(s), a scan will be initiated.
- Stop scanning: Displays the list of domains, where a scan is running or a periodical scan is due to start. In the second case, the domain's name is in a bracket. After having selected the domain(s), scans will be stopped.
- Report file listing: Displays the name of log files, which can be displayed. If a file is selected, its content will be displayed. If the display is at the end of the file, it will switch to tracking mode so that new entries will be displayed automatically.

Registration

You will only be able to launch the product if you have a user name and a valid registration key for the program.

Based on the VirusBuster's registration policy, the purchased VirusBuster product version can be used as long as the user wants to without any restriction. So, the purchased license has not time limit, if the registration has expired the current product version can be used for any length of time. But if any of the program components is updated after expiring, the program cannot be started anymore (user needs to renew the license to use the product again). The update restriction does not affect the database updates, these files can be updated without any consequence at any time – even the registration has expired (but we cannot guarantee the continual compatibility).

After the registration has expired the product stops the automatic program update so that it doesn't have to terminate its operation because of the new (updated) program modules. When it is happening, the product is notifying the user by a message window (and log record) which is displayed every time the user tries to start a manual update. If the registration has expired, the update of the program modules is not allowed. After renewing the license, the program automatically reset the module update settings to the former status.



Registration windows

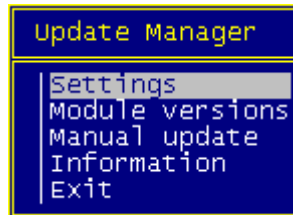
Registration process

During the registration process the user will receive a registration key for the name and number of server users given by the said user. The name and the registration key can be entered after selecting the *Global Options/Registration* menu item. A window will appear in which information can be found on the registration status, the number of server user as well as the number of users registered.

! Note!
Please take care of case sensitivity when you are entering the registration data!

UPDATE MANAGER

Novell-based VirusBuster products can be updated easily with the help of *Update Manager*. In order to install the updater, from the installation CD, copy the `VBUPDATE.NLM`, `VBUPDASC.NLM` files and the `VBUSTER.INI` file if this does not already exist into VirusBuster for NetWare Servers directory. The update can be started with the `load vbupdate` command. The following options are listed in the console window:



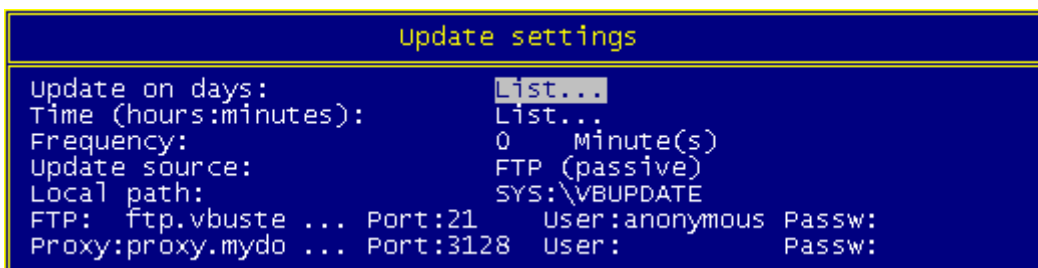
Main menu

The product uses incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program doesn't need to download the whole virus database file every time (its size is several MBs) but usually only a small additional database package including the virus signatures processed and released recently. Using this mechanism, the download time is decreased to a minimal level so we can release additional virus database packages several times a day to improve the defence. Users can obtain protection against new malware without spending long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses have been processed in our virus lab.

Settings

The general settings that will affect both the automatic and the manual updates can be viewed here.

By the default update setting, the product tries to update the program- and database modules by two hours to keep the protection up-to-date.



Update settings

Update on days

It is through this option that the days on which the program should perform the updates can set. New days can be added with the aid of the `Insert` key and days already on the list can be removed through the use of the `Delete` key.

Time

This list contains the times when the program should perform the updates. The times must be given in hh:mm format (for example 22:30 stands for half past ten p.m.). The specified value is only valid, if 0 (zero) value is given in the next menu item (*Frequency*).

Frequency

The frequency of updates can be set here in minutes. The program will perform an update in every x minutes if this option is set.

Update source

The type of the source from where the program will execute the update can be specified here. It can either be a local, a passive or active FTP path or a Proxy FTP.

Local path

It is here that you can enter the server path where the installation kits can be found.

FTP/Port/User name/Password

This is where you can enter the details of the FTP server. We suggest using the default setting; update.virusbuster.hu/pub12 for sever name, using of port 21 and *anonymous* as user name with no password.

Proxy/Port/User name/Password

These fields have to be completed if the FTP update is carried out through a proxy server. As default we suggested using the port 3128.

Module versions

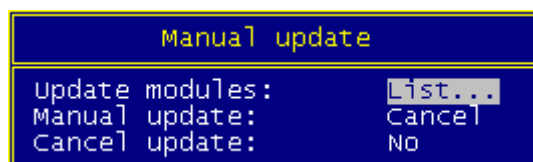
The module versions of the program and the dates they were created are displayed here. It also here that you can set as to which modules should be updated.

Under the name of the installed products we can see the modules belonging to it as well as the module version number and the date it was created.

On the field next to the product name it can be set whether or not the modules of the program should be updated.

Manual update

Manual updates can be initiated in this window:



Manual update

Update modules

This list contains all modules that will be updated during the update process. The modules listed here are those that were selected for updating in the Module versions window.

Manual update

Choosing the Start option in this window will start the update process. It is very important, that the process will only be started, if no other tasks are running.

Cancel update

It is with the aid of this option that a running update process can be cancelled.

Information

This menu contains the address of the VirusBuster Ltd.

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