

VirusBuster
for Windows Servers

TABLE OF CONTENTS

VIRUSBUSTER FOR WINDOWS SERVERS	3
Minimal system requirements	3
Installation.....	4
Normal installation	4
Installation with parameters	6
If the installation has not started... ..	6
Remove, modify, repair.....	6
Starting from the Start menu	6
System tray	7
Pop-up windows	8
MMC console information.....	9
Starting the console	9
Handling installed products	9
Options, setting parameters	10
Structure.....	13
PROGRAM COMPONENTS	14
Quarantine.....	14
Quarantine entries	14
Settings panel.....	15
Virus scanner	16
Add new task	16
Scanner settings.....	16
Heuristics.....	17
Scan areas.....	17
Files to be scanned.....	17
Scan areas.....	18
Interactivity.....	18
Resident protection (Server Shield)	19
Settings panel.....	19
Virus scan areas.....	19
COMMON COMPONENTS	22
General settings	22
Security context for network connections	22
General settings.....	22
SMTP clients.....	23
Tray icon settings.....	23
Global settings for detection	23
Log	24
Log message	24
Settings panel.....	25
Central alert	25
Task manager	27
Tasks and task settings	27
Registration.....	30
Updater	31
Source settings.....	31
Tasks	32
ADDITIONAL INFORMATION	33

Virus scanning methods	33
Heuristics	33
Actions	33
How to test virus scanning engine	34
Windows, messages	35
Virus scan window	35
Message window	36
END USER AGREEMENT	38
CONTACT	39

VIRUSBUSTER FOR WINDOWS 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 Windows Servers provides resident protection for data, systems and therefore for the everyday work, optimized to the increased data traffic of servers. The task oriented operation, the flexible settings, the wizard style and advanced user interfaces provide ease of use with the highest level of security in the most flexible way.

Main features:

- Effective resident protection for servers against viruses and other harmful codes
- Separate protection areas to handle servers' storage disks or their smaller areas individually
- Manual, automatic and scheduled virus scans
- Incremental virus database update
- Easy to use, wizard style user interface
- Advanced interface for advanced settings
- Task oriented operation, modular updates
- Intelligent quarantine for infected files
- Supports Windows Security Center

Minimal system requirements

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

Processor	400 MHz (x86/x64)
Supported operating system - memory	Windows 2000 server - 256 MB Windows 2003/2008 server - 512 MB <i>Recommended to install the latest Service Pack and use at least 1024 MB memory depending on other applications running on the system.</i>
Free hard disk space	100 MB
Browser	Internet Explorer 5
Other	If you need more information, check the readme.txt file – it is in the installation kit.

Installation

Please make sure, that your computer is virus free before installing the software! The anti-virus software can only operate properly if it was installed on a virus free computer. Perform a virus scan on the computer with the help on VirusBuster Scanner's latest version, which can scan the whole system for viruses in a fast and easy way.

Note!

If an anti-virus software is already installed on the computer, it has to be removed before installing VirusBuster. If an older version of VirusBuster is installed on the computer, it should be removed as well!

The product can be installed from a self-extracting archive ([winsrv.exe](#)). After executing the file, the installation package will be decompressed and installation will be started.

Normal installation

Install instructions should be followed, which will guide you through the installation process.

Welcome panel

You can move forward from the welcome screen by clicking on the **|Next >|** button. The end user licence agreement will be displayed in the next window. Generally, on the bottom of every window, you can step back with the **|< Back|** button and quit the installation process with the **|Cancel|** or **|Exit|** buttons.

Displaying and accepting the license agreement

Please overview the agreement and select the **|Yes|** button, if you accept the term and conditions and would like to continue the installation process. If you do not accept the terms and conditions of the above agreement, choose the **|No|** button, which will terminate the installation process and exit from the wizard.

Information about the product

You can step forward with the **|Next >|** button, and specify the installation path.

Choosing the installation path

By default, the product will be installed on the system partition in the `Program files\VirusBuster\` directory, which can be changed by clicking on the **|Browse...|** button, where you can browse through the drives and directories available on you computer and choose the needed path for installation. After having selected the installation path, you can move forward by clicking on the **|Next >|** button.

Choosing the installation mode

The most suitable installation mode in most cases is the *Typical*, and if there is no reason to choose one of the other two options, this one should be selected. The *Compact* installation mode only installs basic components. The product will be operational, but some of the extra functions may not be accessible if this option is selected. The following panel will be: [Specifying registration information](#) window.

The *Custom* installation mode is only advised for experienced users. The user can specify the

components, which should be installed, if this option is selected.

After selecting install modes you can continue the installation by clicking on the **|Next >|** button.

Choosing components (Custom)

Information will be displayed about the selected module on the right side of the window under *Description* by clicking on one of the components. The *MS Office* and *MS Outlook* protection components can only be selected (installed) if the product, which can be protected by these components is installed on the computer. After selecting the needed components, you can move forward by clicking on the **|Next >|** button. Display of the following panels depends on the selected components.

Update settings (Custom)

Update tasks help keep your product up to date automatically. By default, the product contains tasks for the automatic update of the virus database and the software itself. You can step forward by clicking on the **|Next >|** button, to set the update source. If you don't want to create the default tasks, a warning window will inform you about the importance of regular updates.

Specifying the update source (Custom)

Select the suitable update source types for your system and network. You can set additional proxy settings in case selecting the *HTTP* source.

Specifying registration information

The software can be registered during the installation process by typing the user name and the registration key in the appropriate fields. The software can be installed without registration by selecting the *Register later* option and by clicking on the **|Next >|** button. Detailed information about this topic can be found in the [Buy, register, activate](#) section.

Security data

Enter user name and password to specify a Windows account: the updater tasks will be run with the permission that belongs to the specified account by default. This setting can be modified later in the *General settings* option.

Additional data

You can enable/disable displaying the product's icon on the Desktop or select the language of the program.

Start copying

Finally, you can overview the settings and components, which will be used during the product's installation. The files' copying will be started by clicking on the **|Next >|** button.

Successful installation

If the installation was finished without any problems, you can exit the installer after all files have been copied by clicking on the **[Finish]** button, the software has been installed successfully. Finally, you can overview the settings and components, which will be used during the product's

Installation with parameters

By specifying parameters after the installation executable, other installation modes can be accessed, which are not available on the installation interface. You can find detailed information about these parameters and installation modes in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product.

If the installation has not started...

Please check, that your computer fits all minimal system requirements. Check, if your system has all needed system and program components. Without these, installation cannot be performed and an error message will inform you about the needed system component, which should be present in your computer before installing the anti-virus software. You can find detailed information about this topic in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product..

Remove, modify, repair

If you want to remove VirusBuster from you computer, or you want to modify the installed components or reinstall installed components, you have to perform the following:

- Click on the *Add/remove program* icon on the *Control panel!*
- Search for the product, which should be removed in the list, and select it.
- Click on the **[Modify/remove]** button!

You can select the needed operation in the window, which is displayed:

- *Modify*
If you select this option, a component list will appear after clicking on the **[Next >]** button. By selecting or deselecting components in the list, you can add new components, or remove installed ones. The needed operations (installation/removal) will be performed after clicking on the next button.
- *Repair*
Reinstalls installed components.
- *Remove*
Uninstalls all installed components from the computer.

Starting from the Start menu

VirusBuster products will be registered under Start / Programs / VirusBuster during installation. All the shortcuts related to the product are placed here, the software can be started here and product-related documentation can also be opened from this menu.

System tray

VirusBuster can be accessed from the system tray. A VirusBuster icon will be displayed in the tray after installation, indicating that the VirusBuster product is present in the system.



VirusBuster icon on the system tray

The little shield on the icon indicates the status of the *Shield (Resident protection)*, which provides continuous virus protection for the system (if this function is not installed, the shield is not displayed). The shield's colour indicates the protection's status:

- *Green*
The *Shield* is active, the computer is protected against viruses (if the product is registered or is in a trial period).
- *Grey*
The *Shield* is not functioning, there is no resident virus protection.

The most important functions of the program can be accessed from the system tray easily, the most commonly used components and tasks can be started from here. By clicking on the VirusBuster icon (1) with the right mouse button, a local menu will appear where the needed function can be selected. If a menu has a sub-menu, it will be indicated with a little arrow in front of the menu item's name (2).



VirusBuster icon on the system tray – local menu

The following items are always listed in the menu:

- *Registration*
This menu item contains all function related to purchasing or registering the software. Detailed information about this topic can be found under the [Buy, registration, activation](#) section.
- *Support*
This menu item contains three items, which are the following:
 - Help*
The installed products' documentation files can be accessed here.
 - Contact us*
With the help of this function you can send an e-mail to VirusBuster about the product, if the *Mailer* component is installed (detailed description under the [Mail sending](#) section).
 - Information*

Opens VirusBuster's home page.

After registering the software or during the trial period, the most important installed components and the available scanning or update tasks can be accessed from the menu. The VirusBuster Console can be started by clicking twice on the menu with the left mouse button.

Pop-up windows

Through the little information boxes – pup-up windows – displayed above the System Tray users get quick and immediate information about the status of the antivirus system and events occurred during the program operation.



Pop-up window

The title highlighted with bold characters shows the „sender” of the displayed message. The message informs users about this module's operation or message. Certain cases there is a button placed between the message lines. Clicking on it users can navigate to the offered function directly (for example if the message warns user of virus database update, the action could be started immediately by clicking on the **|Update|** button).

The pop-up window will close itself after a while, users can also do it by clicking on the **|X|** button placed on the right-upper corner of the pop-up window.

MMC console information

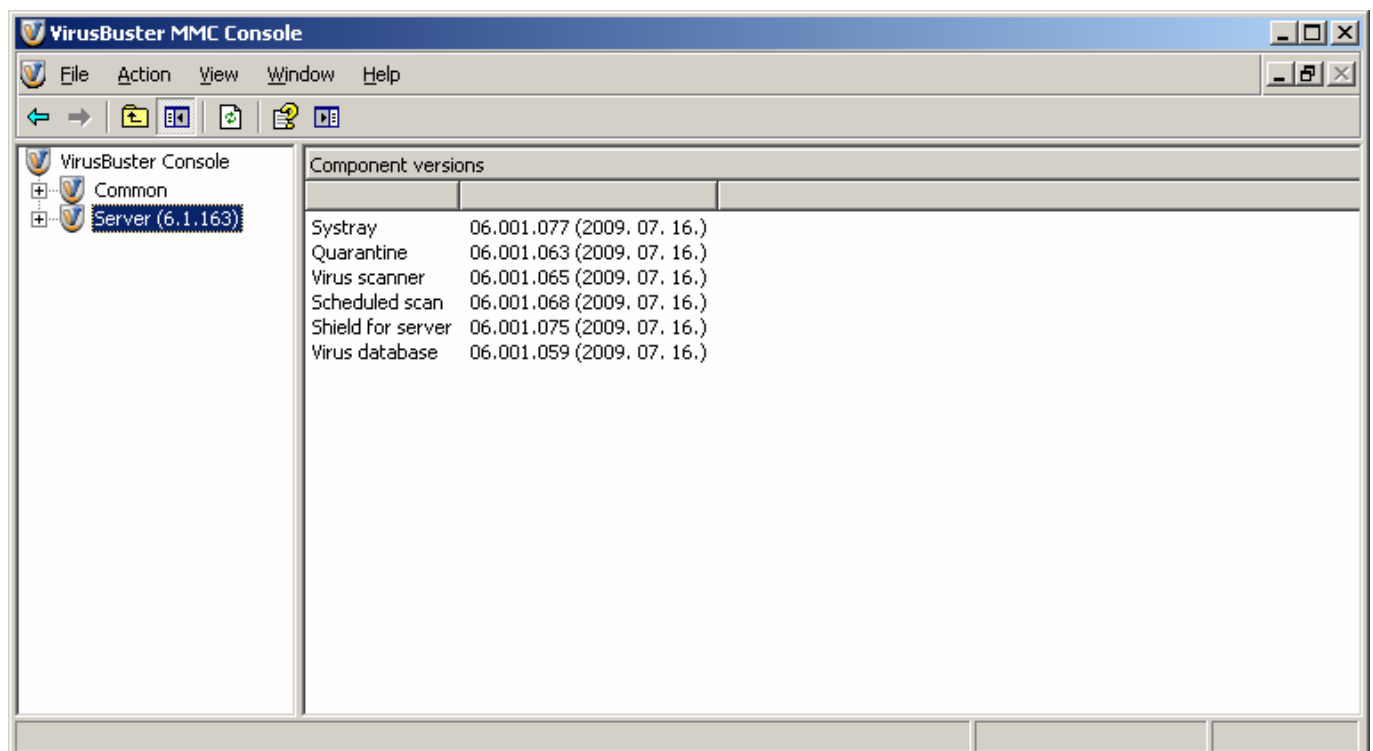
The advantage of MMC (Microsoft Management Console) is that experienced users can perform tasks in the hierarchic system in a matter of minutes and modifying settings and configuration is much easier.

Starting the console

To start the MMC user interface start the 'VirusBuster MMC Console' program from the *Start menu* (Start menu / Programs / VirusBuster MMC Console), and the MMC console elements will be displayed, which are gathered in a parent window (VirusBuster MMC Console). This window contains the menu and the toolbar, which contain commands to open or create additional consoles and to save them. After starting this parent window contains the 'VirusBuster console' window, where you can access the product(s)'s settings.

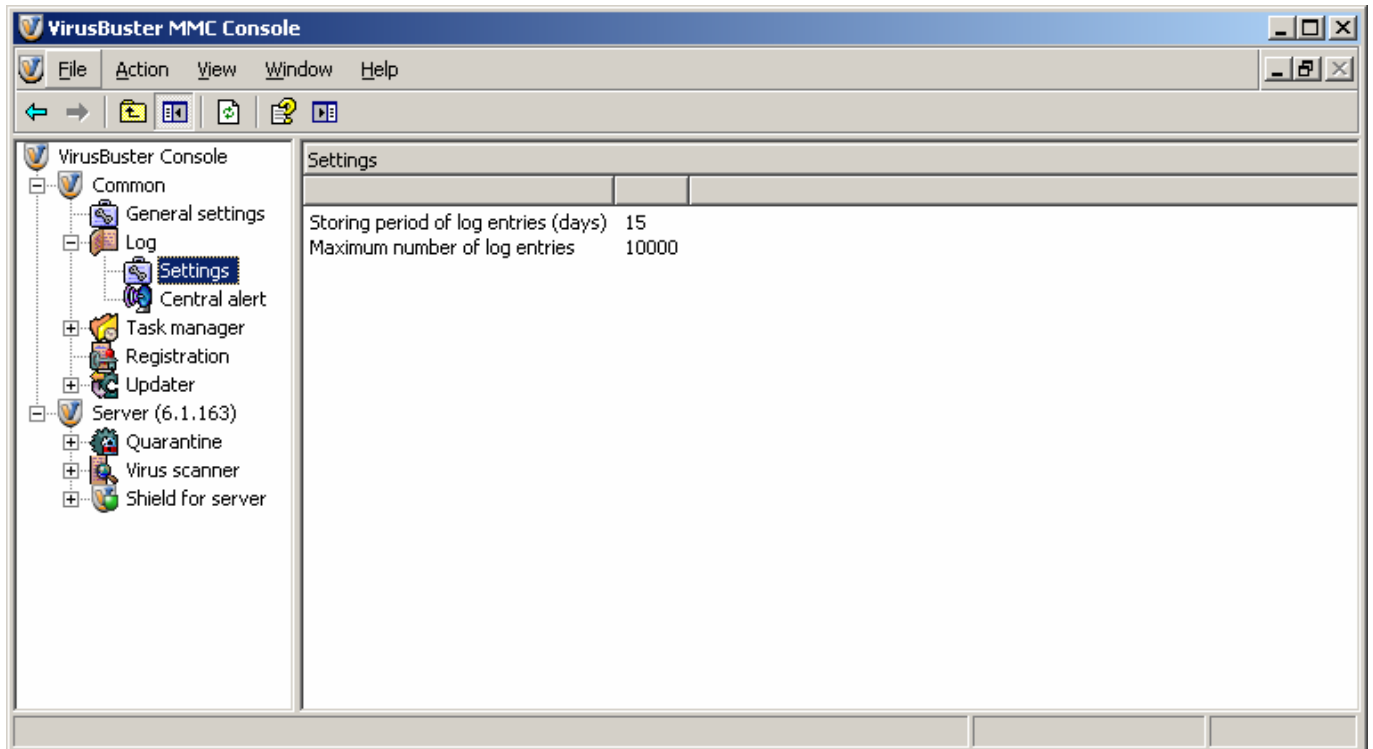
Handling installed products

The settings of the products are shown in the console tree. General modules of the product are located in the *Common* node. Click on the product name to display the product's modules and their version numbers in the right-hand (details) window.



An installed product and its module versions

To access module settings click on the plus sign in front of the module's name and the settings groups will be displayed under the module.



Settings of a module

By clicking on the settings groups under the module, the module's settings will be displayed in the details window. You can modify these by clicking twice on the selected option or by using the right mouse button on the option and choosing Modify from the local menu. Other functions in the local menu are detailed in the description of each module.

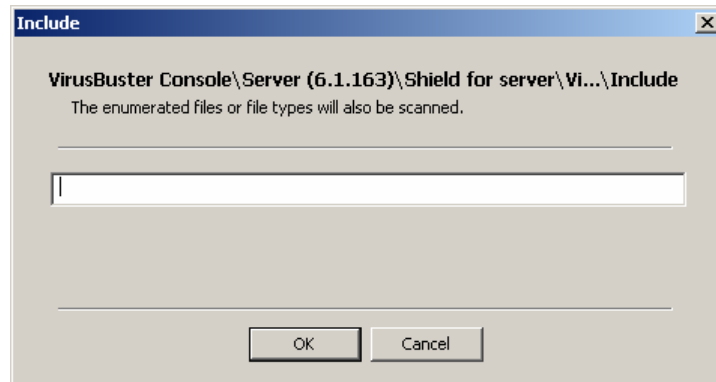
Important! Some of the settings or options above general options can only be accessed in the local menus.

Options, setting parameters

You can access the settings of each module by specifying the needed options in the details window. The options can be modified in two ways:

- Double click on the setting's name
- Right click on the setting's name and select the Modify option.

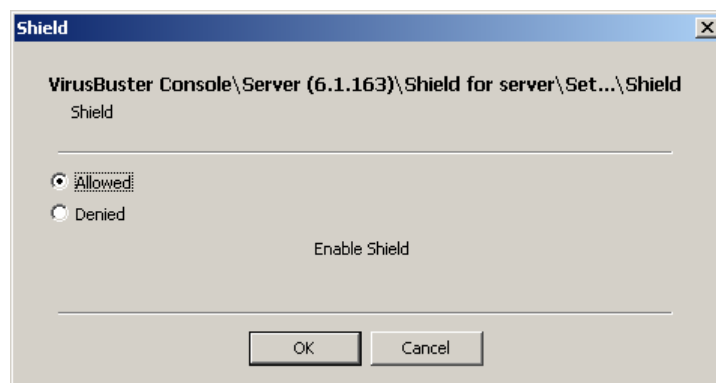
The values of the options can be set in the input dialogs. The most simple setting is when the user has to specify the value in an input field.



Simple input dialog

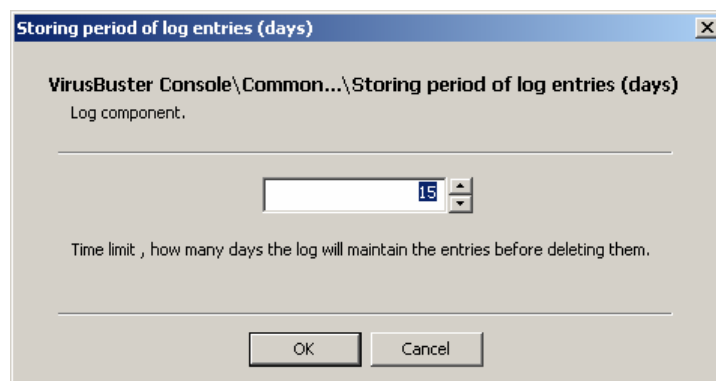
In some cases, the needed value can be specified by clicking on the **[Browse ...]** button. After having specified or selected the needed value, the window can be closed with the **[Ok]** button and the setting's value will be the parameter specified in the input field. If you do not want to specify a value, or you do not want to modify the value, use the **[Cancel]** button. The above are valid for all dialog windows.

In some cases, the option can only be enabled or disabled. In this case, the program offers these two options in a dialog window and the needed one should be selected.



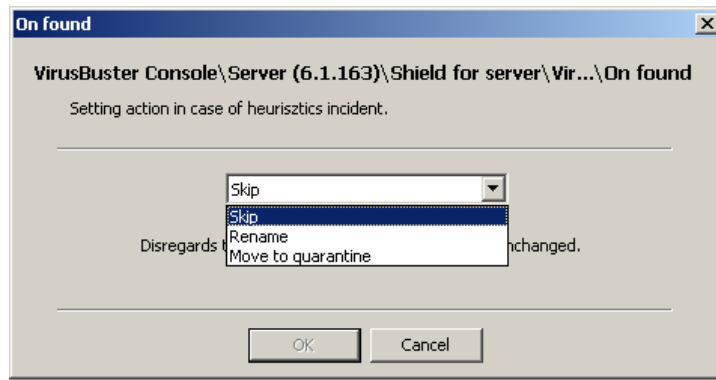
Enable/disable option

The values can be set with arrows, which increase or decrease the value of the parameter. In this case, you can only specify values between the allowed values. The needed value can be set by typing as well.



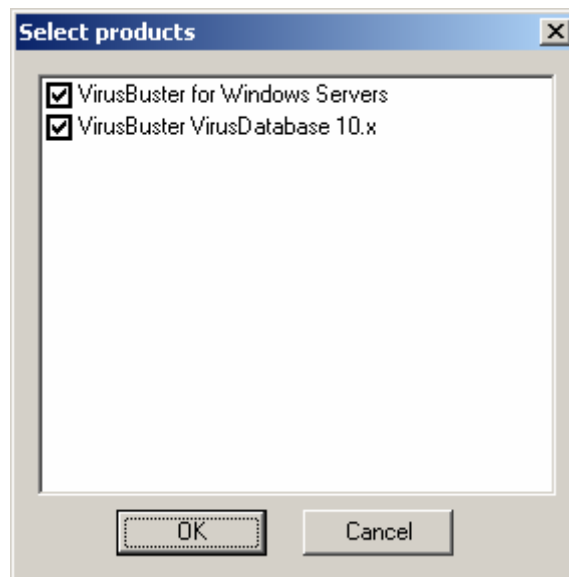
Parameter settings window

In the following window, the value of the settings can only be a pre-defined parameter, in this case these can be selected from a drop-down list:



Selecting a value from a drop-down list

The settings group may only be modified on a comprehensive dialog window (like selecting products for an update task). In this case, the comprehensive window will be displayed if any of the options is modified, where you can specify the value of all the settings in the group.



Comprehensive settings window

Structure

The product's modules can be found under the 'VirusBuster for Windows Servers' group in the MMC interface. The following list only contains components, which belong to this product. For their detailed description, select one of the components:

- [Quarantine](#)
- [Virus scanner](#)
- [Server Shield](#)

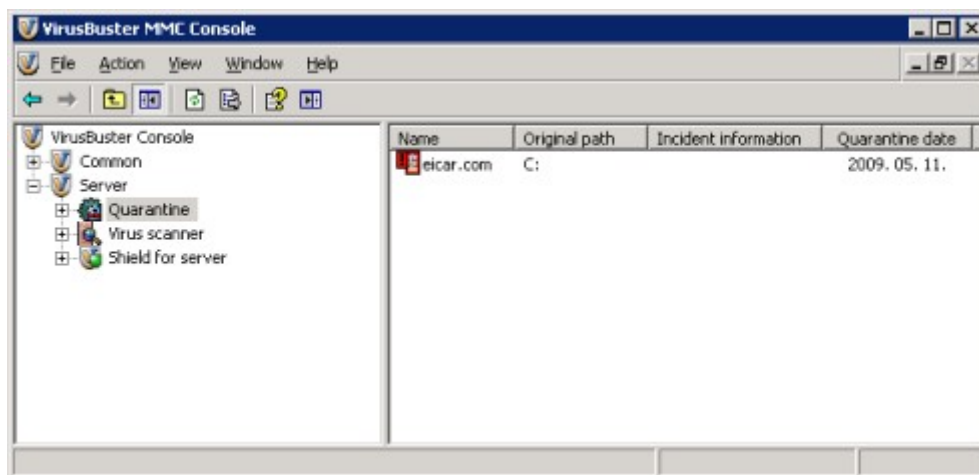
Other components of the product can be found in the MMC tree in the 'Common' group, which are detailed in the [Common components](#) section.

PROGRAM COMPONENTS

Quarantine

The component's task is to store and process non-killable viruses according to the settings.

By clicking on the Quarantine component, the items, which have been placed in it will be displayed in the right-side details window. By clicking on the plus sign in front of the component, you can display the icon of the panel, which contains the Quarantine's other settings and options.



Quarantine

Quarantine entries

The following information is displayed in the quarantine window:

- *Name*
The original name of the quarantined file.
- *Original path*
The file's original path, before it was moved to the quarantine.
- *Incident information*
It displays the detected malware and its path.
- *Quarantine date*

Several actions can be performed on files, which are stored in the quarantine, which are available in the local menu. To access the local menu, please click on the needed entry with the right mouse button.

- *Rescan*
The software scans the selected file(s) again and kills all viruses if it is possible.
- *Restore*
The program restores the file to its original path and status, if the *Restore infected files* function is enabled on the component's *Settings* panel (only if the file is infected with a virus), if the original path exists and there is no file with the same name on the path. If there is a file with the same name on the original path, or the path does not exist, the quarantine will restore the file to the program's temporary folder.
- *Save as...*
Saves the file with the specified name. The program encodes the file so that the virus is inactive

and the file can be sent for virus analysis.

- *Send...*
Sends the selected file(s) to VirusBuster for analysis. Proper SMTP settings are needed for sending a file, which can be specified on the Common/General settings panel's [SMTP client](#) setting. You can modify these data before sending by clicking on the **[Mailer settings ...]** button in the sending window.
- *Delete*
The program deletes the selected file(s) permanently.

Settings panel

Other settings, which affect the operation of the quarantine can be specified on this panel. You can enable the quarantine's restore function with the help of the *Restore infected files* option. If it is enabled, infected files can be restored from the quarantine.

If the *Automatic rescanning after virus database has been updated* option is enabled, the program will rescan all files in the quarantine after a virus database update and kills all viruses in them if it is possible.

The following options can only be modified if automatic rescanning is enabled:

- *Automatic killing of killable viruses*
If this option is enabled, the program will kill all viruses in the quarantined files after a virus database update if it is possible.
- *Automatic restoration of disinfected files*
If this option is enabled, the program will restore all files, which have been disinfected automatically after a virus database update.

! Important!

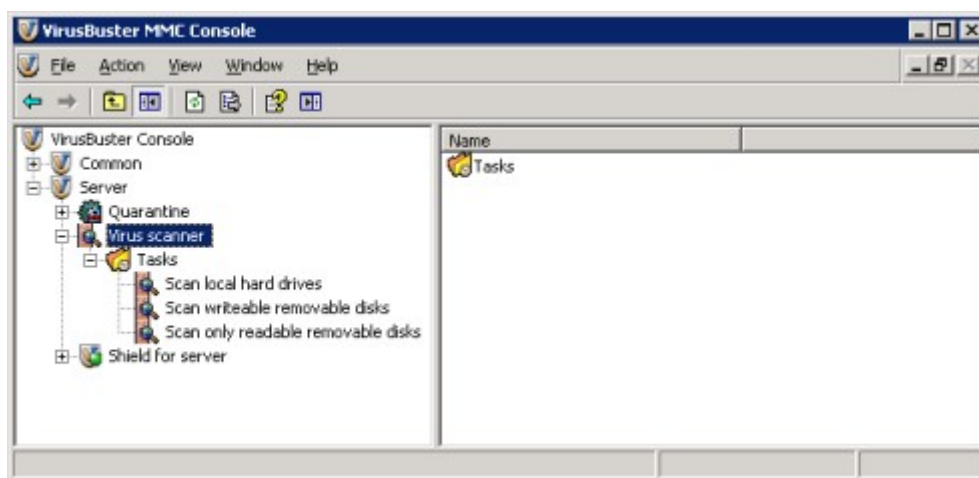
It is not needed to specify a quarantine directory, the program uses the installation directory's **Quarantine** folder automatically.

Virus scanner

Virus scanning tasks can be added and modified and virus scans can be initiated in this component. Virus scanning is based on tasks: the virus scan can be started with a few mouse clicks or can be scheduled for a specific date or a trigger event with the pre-set parameters.

After having clicked on the Virus scanner component, the *Tasks* folder will be displayed in the right-side details window. By clicking on it twice, you can overview the existing virus scanning tasks. This folder can also be displayed by clicking on the plus sign in front of the component in the list on the left panel. In this case, the *Tasks* folder will be displayed in the left-side tree as well and tasks can be displayed by clicking on it.

The icon in front of the task's name in the details window indicated the task's status (started, stopped or paused).



Virus scanner

Tasks can be modified, deleted or scheduled in the local menu, which is detailed in the [Using tasks and task settings](#) section.

Add new task

A new task can be added in the local menu. Click on the *Tasks* folder in the left-side list or anywhere in the details window with the right mouse button and choose the *Add* option.

When adding a new task, first the task's name must be specified. After specifying a name, the task will be created with default settings. To modify these, select the new task's name from the left-side task list or click on the task's name twice in the right side details window.

Scanner settings

The *Scanning method* can be specified on the following levels:

- [Fast/Extensive/Full](#)

You can specify the actions, which will be performed (automatic mode), or which will be suggested (interactive mode) when a virus is found on the Virus found settings panel. The selected primary action

can be set in the Virus found option. If this cannot be performed (e.g. the virus cannot be killed), then the secondary action, which is set at the In case of unsuccessful disinfection option will be performed or suggested. When a virus is found, all actions can be performed on the file except for Kill, therefore it is not needed to set a secondary action, if the set value is other than Kill in case of the primary action. You can set an action for heuristic detections

The available actions *On virus found*:

- [Kill/Move to Quarantine/Skip/Delete/Rename](#)

Available secondary actions:

- [Move to Quarantine/Skip/Delete/Rename](#)

Heuristics

Heuristics *Sensitivity* settings:

- [Off/Medium/High](#)

Available actions in case of heuristics found:

- [Move to Quarantine/Skip/Rename](#)

Scan areas

You can specify the areas, which should be scanned here. The following areas can be selected (*Enabled*) or deselected (*Disabled*):

- *Memory*
Scans the computer's memory.
- *Master boot record*
Scans the computer's first boot record.
- *Boot sector*
Scans the current boot sector.
- *Compressed files*
Scans all files, which have been compressed with known compression methods.
- *Folders*
Scans the selected folders.
- *Selected files*
Scans the selected files

Files to be scanned

If the *Scan all files option is enabled*, all file types (all extensions) will be scanned. If this option is disabled, you can specify the file types, which should be scanned. These can be set based on pre-defined groups. If the *Allowed* value is selected, the specified file type will be scanned.

- Jet database engine files
- Sheet files

- Document files
- Power Point files
- Program files
- Script files

You can specify file types, which should be or should not be scanned individually. To be able to do this, the *Included file types* or the *Excluded file types* option must be selected. In this case, the files, which should be or should not be scanned must be specified in the *Include* or *Exclude* fields separated with a semicolon (;) (e.g. *.rxx; *.qqq). When specifying file types, joker characters can be used (e.g. *.qwe, *.?ab).

Scan areas

The drives and network shares or their individual directories which should be scanned can be set here. Click with the right button in this option then you can add, modify and delete scan areas.

You can enter or browse a new scan area in the browser window. More scan areas can also be added.

Selecting the *Recursive* check box, the selected folder with all its subfolders and files will be scanned.

If you would like to scan all the available drives on the client, enter the #ALLHARDDRIVES keyword as path.

Interactivity

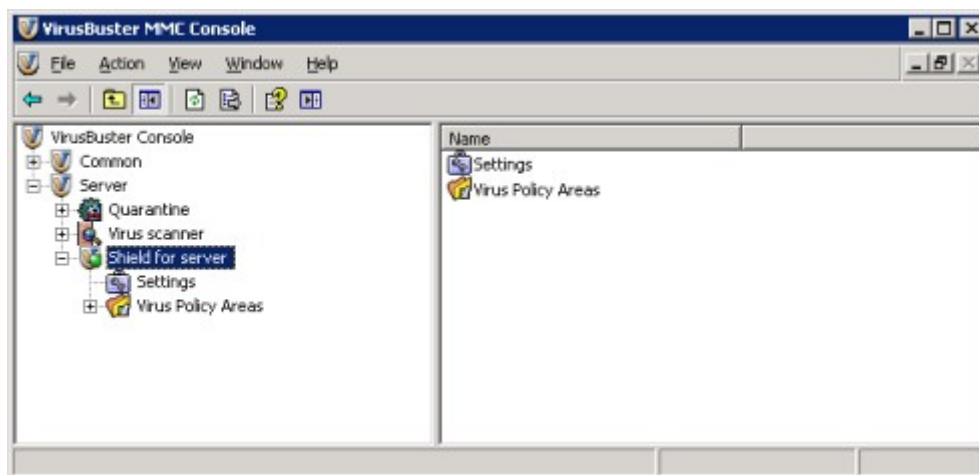
If the *Interactive communication* option is enabled, the program will prompt the user for further instructions in case of every incident and will offer the set actions as default. If the option is disabled, the set actions will be performed automatically on the infected file.

If the *Status window* option is enabled, you can overview the monitor the scanning process on a [virus scanning process status window](#).

Resident protection (Server Shield)

This component provides resident protection against viruses. Its main task is to search for viruses and disinfect them by working in the background. The protection will scan files when they are accessed (e.g. reading and writing).

After having clicked on the Server Shield component the icon of the *Settings* panel and the *Scan areas* folder will be displayed in the right side details window. If you click on these twice, you can view their contents. You can display these two options by clicking on the plus sign in front of the component in the left side list. In this case, the panel's icon and the folder will be displayed in the tree.



Server Shield

Settings panel

The Server Shield can be switched on or off in the *Resident protection* option (*Enabled/Disabled*).

You will be notified about virus incidents if the *Display warning* option is enabled. If it is disabled, the program will perform the set actions, but the user will not be informed about the incident; it will only be stored in the log.

Virus scan areas

One of the important functions of the server resident protection that it is possible to create separate virus policy areas (VPAs), which can have different virus scanning settings. For example, two different directories on the computer can be protected with different settings against viruses. For this, two different virus scan areas must be added with the needed individual settings.

The protection areas can be found in the *Virus policy areas* folder. Click on the folder with the left mouse button and existing protection areas will be displayed in the details window on the right. If you click on the plus sign in front of the folder, the same list will appear in left side tree structure. By default, only the *Default VPA* scan area is added to the system, which cannot be removed, but its settings can be modified.

To view the settings of a scan area, click on its name in the left side tree structure once, or in the details windows twice. The settings of the scan area will be displayed in the right side details window.

New scan areas can be added by using the local menu. Click on the *Virus policy areas* folder on the left side or on any of the set protection settings or anywhere in details window with the right mouse button and select *New*.

When adding a new scan area, you have to specify its name first. After having specified a name, the needed area will be created with default settings.

To modify the settings of a scan area, select the area's name in the left side list or click on the name twice in the right side details window.

To delete a scan area, click on its name and select *Delete* from the local menu.

Virus scan areas settings

General settings

You can enable or disable the selected protection area in the *Resident protection* option. If it is disabled, the virus protection options will not be used and the path specified in the *VPA path* field will not be protected.

You can specify the path or drive which should be protected in the *VPA path* field. The protection is recursive, therefore the selected directory and all of its sub-directories and all files in them will be protected according to the settings.

File access settings

You can specify whether the following files can be accessed in the system or not:

- *Access to infected files*
Disabled: Local or remote users cannot access files, which have been marked as infected by the protection.
- *Access to suspicious files*
Disabled: Files, which have been found suspicious during the heuristic analysis cannot be accessed.
- *Access in case of scanning error*
Disabled: If there is an error during scanning (it cannot be determined whether the file is clean or not), the protection will deny access to the file.

Scan settings

Scan settings are the same as detailed in the [Scan settings](#) section.

Heuristics

The heuristics levels and the performed actions are the same as detailed in the Virus scanner component's [Heuristics](#) section.

Protection of file groups

Files or groups of files can be specified inside a VPA path (in case of non-server protection: globally),

which have special limitations or exceptions. When specifying file groups, joker characters can be used ('*', '?') so that file groups can be added flexibly. To form file groups, file masks, which should be included or excluded must be typed in the field separated by a semicolon (;).

Protection types, which can be activated by selecting them:

- *Delete protection of file group*
You can specify files or file groups in the *Include* option, which cannot be deleted as the resident protection will prevent it.
- *Write protection of file group*
You can specify files or file groups in the *Include* option, which cannot be written as the resident protection will prevent it.
- *Rename protection of file groups*
You can specify files or file groups in the *Include* option, which cannot be renamed as the resident protection will prevent it.

File, or file types specified in the *Exclude* option will not be excluded from the file group protection.

For example: if you want to prevent writing of **.exe** files beginning with **va** and **ve** characters, but you don't want to protect **.exe** files beginning with the **val** characters, you have to set the following values in the *Write protection of file group* option:

- Include: **va*.exe; ve*.exe**
- Exclude: **val*.exe**

Important!

If you set delete, write or rename protection for a file group, please consider, that if an application tries to delete, write or rename the protected file it may cause several log records showing the actions. It is because different file managers perform the requested action on the file repeatedly to try delete, write or rename it. Each attempt is registered into the log.

Scanning of file types

The settings of file types which are selected for scanning are the same as detailed in the Virus scanner component's [Files to be scanned](#) section.

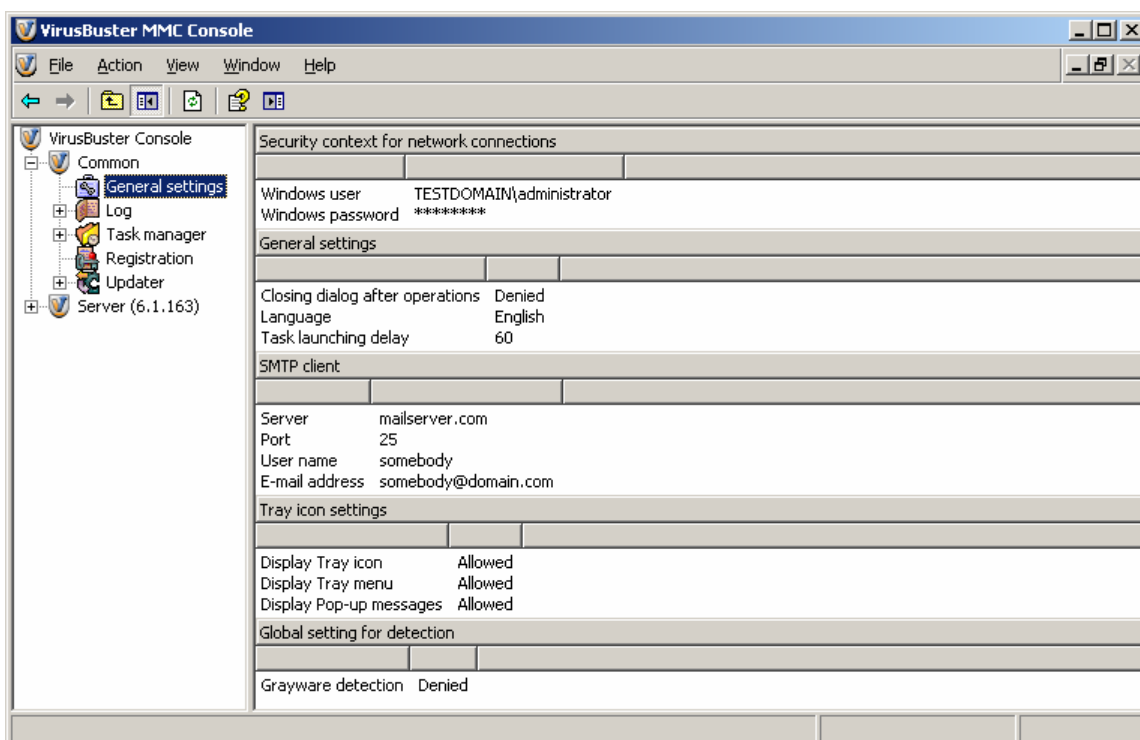
COMMON COMPONENTS

The modules which are grouped under the 'Common' node provide general functions for the current product.

General settings

Security context for network connections

Enter user name and password to specify a Windows account: the updater tasks will be run with the permission that belongs to the specified account by default. The account has to be specified in the format NETWORK\User (e.g. WORKGROUP\Admin).



General settings

General settings

If the *Close dialog after operations* option is enabled, the dialog window will be closed automatically after an operation, if there is one. If it is disabled, the program will wait for the user to close the window.

You can change the language of the product by selecting a new language from the available values of the *Language* setting*. After selecting a new language, you need to restart the product to apply the new setting. For changing the language also in the tray menu, you have to restart the computer.

Task launching delay: If the starting of a task is triggered by an event, it may be needed to delay the starting of the task, so that it can be performed. A task can be scheduled to be started at system startup for example. In this case it may be needed to delay it for a while after the login process so that initialization

processes can be performed and applications can be loaded. The delay can be set in seconds.

SMTP clients

It is possible to send a direct message to VirusBuster from the program if you have a question or a problem. Proper SMTP settings must be specified for this, the following values must be set:

- *SMTP server*
Name of the server which delivers the e-mails, usually this name is given by the ISP (Internet Service Provider) or it is the name of the Exchange server (this information can be found in the mailer client settings /Outlook, Thunderbird, etc./ or you can ask your system administrator or ISP).
- *Port number*
The mail server's port number (25 by default).
- *User name*
This name will be displayed in the mail you sent us as 'sender'. Tokens can also be used in this field:
%m% - computer name
%u% - user name
- *E-mail address*
This is your e-mail address the response will be sent for.

Tray icon settings

These options allow you to customize the operation of the System Tray menu and the Pop-up windows.

- *Display Tray icon*
Denied: The System Tray icon will not be shown on the Tray.
- *Display Tray menu*
Denied: The local menu of the System Tray icon will not be displayed even if right clicking on the icon.
- *Display Pop-up messages*
Denied: The application will not warn the user by Pop-up windows (displayed right above the System Tray) about problems and events occurred during operation. This setting doesn't have an effect on displaying other information windows (virus alerts, warnings) of the product.

Global settings for detection

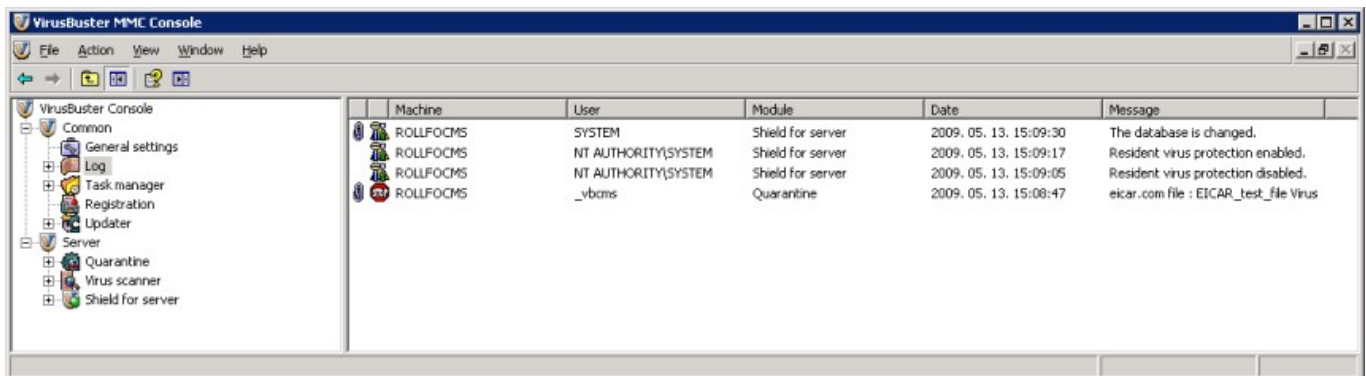
- *Grayware detection*
If this switch is enabled, the program will detect products in the *grayware* category, and will perform the action specified for the applications detected.
Grayware is software which may fall into different categories, depending on its use. Normally, if the user approved the installation and use of these applications, they cannot be considered malware. However, they may also be installed without the user's consent, and their functionalities may be abused for malicious activities. Such software may include ftp server programs and remote access applications. Thus the presence of such a program in itself is not necessarily harmful. Whether it is harmful or not on a given machine is determined by the circumstances of its installation.

Log

Its main task is to store the messages generated by the various parts (modules) of the software and to forward these to the user if needed.

Physically, the log file is located in the *Bin* folder of the installation path. Called *local.db*, it is an SQLITE type database file.

The log entries will be displayed in the right side details window by clicking on the component. By clicking on the plus sign in front of the component, you can display the panel's icon, which contain the Log's other settings.



Log

Log message

Structure of the messages:

- *Machine*
The name of the computer, where the message was created.
- *User*
The name of the user, who started the application, which generated the message.
- *Module*
The name of the module, which created the message.
- *Date*
The date, when the message was created
- *Message*
The message's content.

The icon in front of the *Machine* value indicates the message's type and the paper clip at the end of the line indicates if the message has a detailed description.

The program refreshes the list automatically if the new message is created or deleted. The refresh will not modify the selected item provided it is not the one which has just been deleted.

A local menu will appear by clicking with the right mouse button on the items, in which the separate fields of the messages can be switched on or off and the following actions can be performed:

- *Save as...*
Saves the message's content to the specified file.

- *Send...*
Sends the message and the log file to VirusBuster support. You can finish sending the message in the *Mailer component* window.
- *Refresh*
Refreshes the list.
- *Delete*
Deletes all messages from the list.

If you click on a message twice, the details of the message will be displayed and you can view its detailed description.

Settings panel

You can specify the display's chronological order in the *Log display* option by clicking on the panel.

The *Database directory* contains the path of the log database file. By default this path is the VirusBuster directory's *Log* sub-directory.

Store log messages in the system: The program will delete messages older than the specified value (days).

Database size limitation: You can maintain the log database's size by limiting it. You can set the maximum value (Mbytes) and the program will delete old messages continuously to limit the size to this value.

Central alert

The task of the component is to send a warning upon any new log entry it was registered for (i.e. in the case of any event for which such notification was enabled). In order to work, the Central alert component requires the Log component, and correct e-mail settings.

Central alert operation is based on rules, i.e. notification settings can be specified in (several) rules. In order to manage rules, select the *Central alert* component in the left-hand tree, and then use the local menu (right click) in the right-hand window. The options are *Add rule*, *Modify rule*, and *Clone rule* (cloning means to create a new rule from an existing one with identical settings).

When adding a new notification rule, the following settings have to be specified

- *Rule name*
A unique name to identify the rule.
- *Send detailed message*
When enabled, the alert message will contain the detailed content of the log entry. When the option is disabled, only a brief message will be sent. Default: enabled.
- *Type of notification*
E-mail – alerts will be sent to the e-mail address specified (e-mail settings should be checked).
Event log – alerts will be entered into the *Event log*.
- *Filters*
Filters are used to select the types of events the log entries of which are sent out by the Central alert. Whenever a new entry of a specified type is created in the product's log, the Central alert will send it to the given address.
- *Central alert settings – Active*
If these settings are not enabled (i.e. there is no checkmark in the corresponding checkboxes),

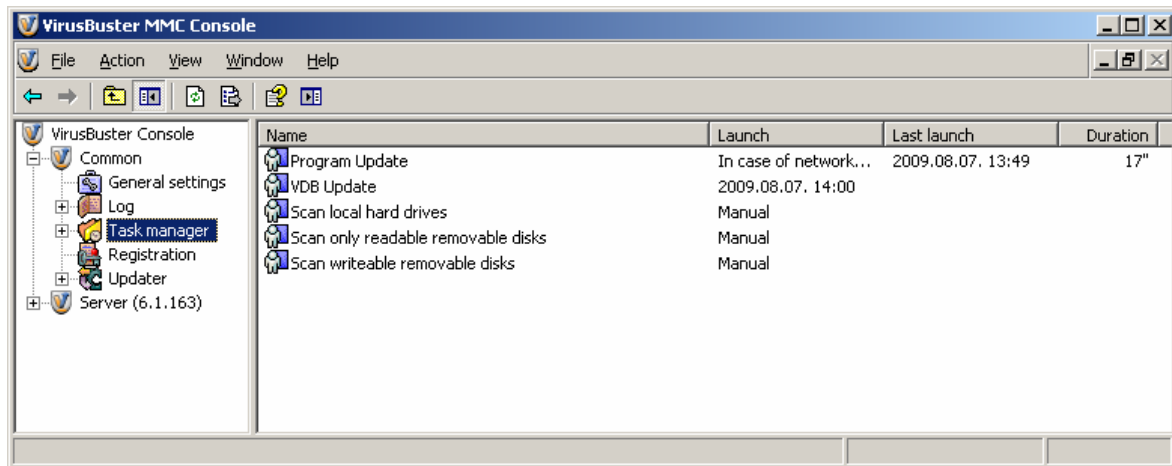
then alert messages are sent to the specified address at the moment when they are created. If these settings are enabled (i.e. the corresponding checkboxes are checked), then alerts will be scheduled based on the settings listed below.

- *Period*
Alerts are not sent immediately (i.e. when they are created). Rather, they are sent in a single message (in a batch) once the period of time specified here has elapsed.
- *Send if queue length is ...*
When the total quantity of new alerts reaches the amount specified here, the messages will be sent immediately (i.e. they may be sent earlier than the time specified in *Period*).
- *Sending messages at startup*
If there are unsent messages when the product or the computer is shut down, and this setting is enabled, then they will be sent out upon the program's startup.

Task manager

This component gathers all the tasks of the system's modules. All tasks added in the program can be managed in this component.

By clicking on the component, all existing – added and default – tasks will be displayed in the right side details window. By clicking on the plus sign in front of the component, these tasks will be displayed and their types are indicated with the icons in front of them. The icon in front of the task's name in the details window indicates its status (started, stopped or paused).



Task manager

Tasks and task settings

You can display a task's settings by clicking on it once in the left side list or by clicking on it twice in the details window. The detailed explanation of the settings you can find in the related component own section.

The following information is displayed next to the task's name in the details window:

- **Launch**
The method of starting the task. You can read detailed information about this topic in the [Scheduling](#) section.
- **Last launch**
The date, when the task was started for the last time.
- **Duration**
The duration of the task's operation during the last launch.

Functions in the local menu

By clicking on the task with the right mouse button either in the tasks list or in the details window, the local menu will appear, which contains the following functions:

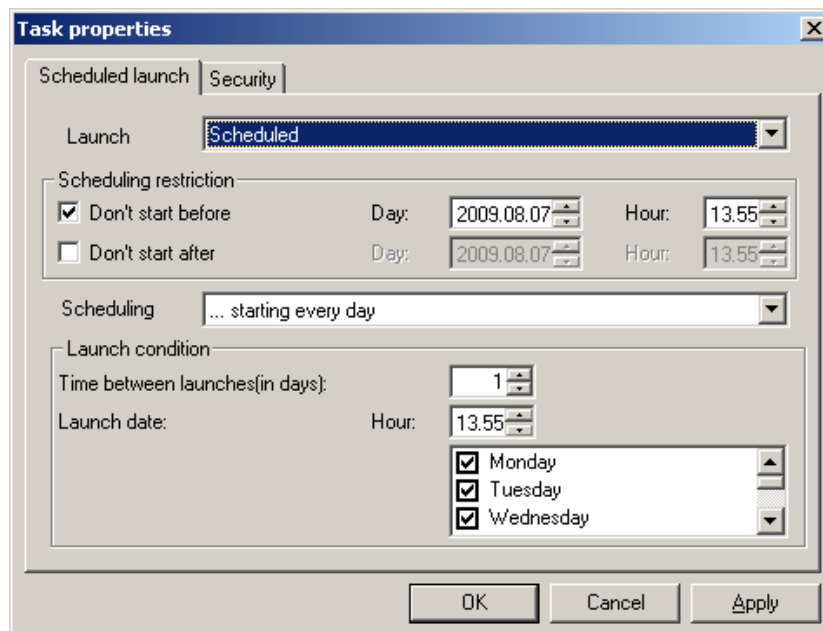
- **Start/Pause/Resume/Stop**
You can start a selected task, pause it, resume a paused task or stop a running task.
- **Disable/Enable**
If is possible to disable a task. In this case it cannot be started manually or scheduled until it has

been enabled again.

- *Manual operation*
It can be used, if the task is not started by the user. If you choose this option, the task will be set to manual and the user has to start it manually. All set scheduling parameters will be invalid. You can read about scheduling in the [Scheduling](#) section.
- *Modify*
You can modify the selected task's settings here. If you select this option, the task's settings will be displayed in the details window. Default tasks cannot be modified.
- *Delete*
Deletes the selected task from the system.
- *Schedule*
Scheduling of the selected task.

Scheduling

You can schedule the task in the local menu. The settings can be specified in a dialog window.



Scheduling

You can select several scheduling options like rarity or a specified date or event. Depending on the task's type (update or virus scanning task) the following options can be selected:

- Manual, the task can be started by the user.
- Started in case of a network connection (only in case of virus scanning tasks)
- Scheduled, the time of starting can be specified in this case
- Started in case of user login (only in case of virus scanning tasks)
- Started in case of user login and network connection

The *Schedule type* can be selected from a drop-down list:

- Once
- minutes

- hours
- days
- weeks
- months
- years

You can set the intervals, after which the task must be started on the specified days using the *Time between launches*, *Day and Hour* (hour.minute) settings. For example, if the scan must be started every third week, the *Schedule type* will be weekly, the *Time between launches* will be three.

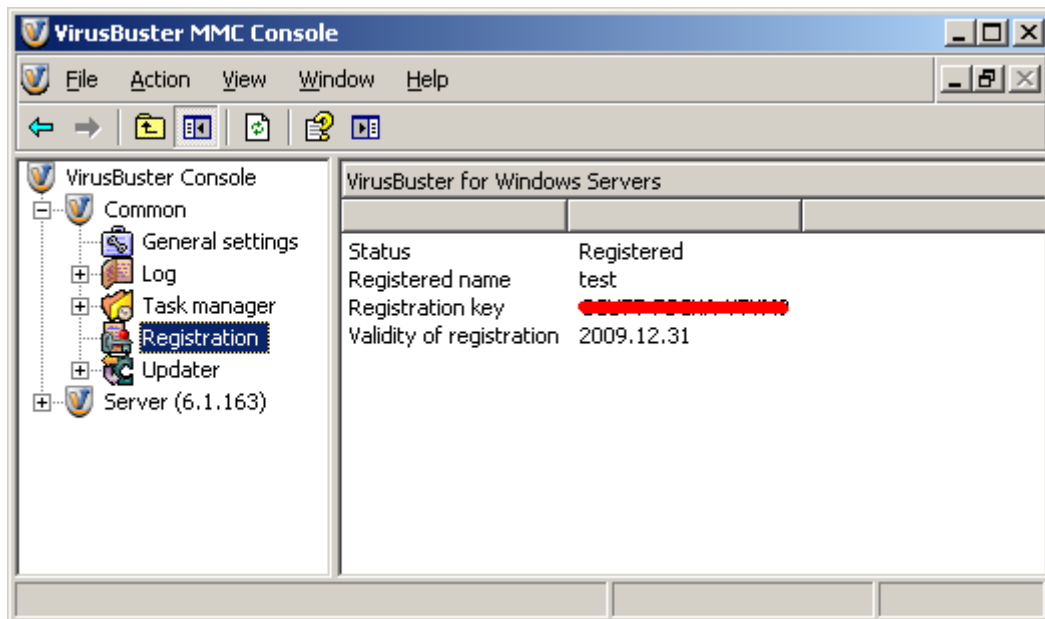
You can assign a user profile to individual schedule settings on the *Security* panel and the task will be performed with the specified user's security context and only if that user is logged in.

- *Anyone*
The tasks will be started in case of any user.
- *Default*
The security context of the user defined in the Common/General settings panel will be used.
- *Custom*
You can specify a custom user.

Registration

The component's task is to check and store the registration data specified by the user. The registration data includes a user name and a registration key.

After clicking on the Registration component the installed VirusBuster products and their registration data will be displayed. To modify these, click on the registration data of the needed product with the right mouse button and select Registration from the local menu.



Registration

Select the needed product in the registration window – this is only needed if several VirusBuster products are installed – and specify the registration data in the appropriate fields and click on the **OK** button. In case of a successful registration, the following will be displayed under the product's name:

- *Status*: Registered
- *Registered name*: the specified name
- *Registration key*: the specified registration code
- *Validity of registration*: the date of expiry, the product will be registered until this date.

Clicking on the *Activation...* menu item in the local menu you can start the activation module. After entering your activation code you will receive the product's registration key at the end of the activation process. After successful activation the product will be registered automatically. If CMS is used, the key will be put into the Licence manager as well. For more information on activation please read the product's manual.

Updater

Updating the software and the virus database is vital for maintaining the effectiveness of the protection. The software update is based on tasks: the update can be started with a few clicks or can be scheduled for a date or an event and it will be performed with the pre-set settings.

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.

By clicking on the Update component, the *Last started update task* and the *Last performed update* information will be displayed, which are the following:

- *Task name*
- *Task started*
The date, when the task was started
- *Task source*
The update source assigned to the task
- *Tasks result/updated product*
The result of the task/The name of the updated product.

The difference between the two groups is that the last started task may not have been successful, but the last performed update was a successful update process.

By clicking on the plus sign in front of the component, the Source panel's icon and the Tasks folder will be displayed, with the help of which the module's settings can be modified.

Source settings

By selecting the Source panel, the available update sources will be displayed in the details window. The sources can be activated by selecting the checkbox next to them. If a source is selected, it will be possible to perform update from it, and it can be selected when adding or modifying a task.

The possible update sources and their settings are the following:

- HTTP
Update through the HTTP protocol. You have to specify the HTTP server's name, the used port (default is 80) and path, where the descriptor file can be found. The default setting is:
update.virusbuster.hu:80/pub11
If the connection needs proxy server to access the update source, you can specify additional settings:
 - Proxy
 - *None* – There is no need proxy to access the network.
 - *Specified in Explorer* – Application gets predefined proxy settings from Windows Internet Explorer.
 - *Customized proxy* – If this option is selected, you can manually set proxy settings.
 - Proxy server/port – Address and port settings required to access to the proxy server.
 - Proxy user/password – User name and password if the proxy server needs

authentication.

- FTP
Update through the FTP protocol. The FTP server's name, the port used by the server (default is 21) and the path, where the descriptor file can be found and the user name and password for logging in must be specified. If you are using the 'Anonymous' user name, please type your own e-mail address in the password field. The default setting is: [anonymous@update.virusbuster.hu:21/pub11](mailto:anonymous@update.virusbuster.hu)
- NetWare path
The update can be performed from a Novell NetWare server if the needed path is typed in the field in UNC format (`\\servername\sharename`).
- Path
The update can be performed from a local or a network drive. The path can be specified by clicking on the `[...]` button.
- CD drive
If the update is performed from a CD, please select the drive's letter from the drop-down list.

Important!

The update can only be performed from a local or a network path, if the user is logged in to the domain!

The update can only be performed from a Novell NetWare network path if the user is logged in to the server!

Tasks

After clicking on the Tasks group all the existing – default and added – tasks will be displayed in the details window. The icon in front of the task's name indicates its status (started, stopped, paused).

Tasks can be modified, deleted or scheduled from the local menu, which is detailed in the [Tasks and task settings](#) section. The method of adding a new task is detailed in the [Add new task](#) section.

Update task settings

You can select the update source in the *Type* option, where the program will check if there is a new version available. Only active sources can be selected, which can be set on the [Source](#) panel.

You can select the products, which should be updated in the *Products to be updated* option.

If the *Dialog window* option is enabled, you can overview the update process. You can overview the process step-by-step and the program will prompt you at every step if the *Interactivity option* is enabled.

If the update source can be accessed through the network, you can specify the information needed for the network connection in the *Network connection parameters* option. If the *Continuous network connection* option is selected, the task will not try to create a connection and it will generate an error if the connection is not available. If the *Dial-up connection* option is selected, the task will try to establish a connection and will terminate it after it has been performed if the task created the connection. In this case, you can specify a password for the connection.

The *Restart computer* option controls the system restart. If you deny it, the computer will never be restarted after update process have been finished.

Important!

Please do not disable computer restart unless you have a relevant reason to do it, because there may be changes performed during the update process that need computer restart to be activated. If it is disabled, it is possible that the computer's resident protection may not be activated and your computer will not be protected!

ADDITIONAL INFORMATION

Virus scanning methods

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:

- *Quick*
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).
- *Extensive*
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.

Heuristics

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.

Actions

In case of a virus infection, several actions can be performed on the infected file. The following actions are available:

- *Kill*
Removes the virus from the infected file, the file will be disinfected and restored to its original status.
- *Move to quarantine*
Moves the file to the quarantine directory. Viruses moved to the quarantine are not functional, they are not dangerous for the system.
- *Skip*
No action is performed on the infected file.
- *Delete*
Deletes the infected file permanently.
- *Rename*

Renames the extension's first letter to v in the infected file.

The following actions can be performed on e-mail attachments:

- *Delete attachment*
Deletes the infected attachment from the e-mail.
- *Rename attachment*
Renames the extension's first letter to w in the infected attachment.

How to test virus scanning engine

In order to see what happens, when our virus scanning engine finds an infected file, you can use the EICAR (European Institute of Computer Anti-virus Research) Standard Anti-virus Test file, which naturally is not a virus, but is detected by our engine as if it were. To create a file that contains the EICAR sequence, type the following string and save it in a file having a **.COM** extension (like **EICAR.COM**):

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To check the operation of the virus scanning engine, perform a virus scan on the created file, or execute the file if the resident protection (Shield) is active. If the engine is operating correctly, the result of the scan or the execution will be a warning window.

Note
If executed, this small COM file will display the "EICAR-STANDARD-ANTIVIRUS-TEST-FILE" message, and will exit.

Windows, messages

VirusBuster displays its messages and information in message windows on the screen to inform the user about viruses, or events, which occur in the system.

Virus scan window

When a virus scan is started, the process of the scanning and its parameters are displayed in a window to inform you about the status of the scanning.



Virus scan window

In the upper part of the window, the main settings of the scanning process and the method of scanning and disinfection are displayed. The *Scanning process* section contains the name of the file, which is currently scanned and its path, the elapsed time and a status indicator bar. The *Scan statistics* section contains the number of scanned files, the number of infected files, the number of disinfected files and the number of suspicious files. The *Last found virus* – where the last found infected file and its path are displayed – and the *Virus name* fields informs you about the last found virus. The log entries, which have been generated during the scanning process are displayed in a window at the bottom of the panel. You can access detailed information about each entry, by clicking on an item twice with the left mouse button.

Virus scans can be started in many ways, therefore the displayed scan windows basically contain the same information, but there are some differences between different types of scans. The above mentioned general information types are always displayed in the window, other displayed settings and buttons depend on the starting method of the virus scanning process.

Message window

The program uses message window to display information about virus incidents, the effects of operations started by the users or other functionality problems, which occur in the system.

Recognizing a virus infection

During the virus scan, if a file is infected, the program will display a message window.

Infection types:

- *Infected - killable*
The virus scanning engine has found an infected file, which can be disinfected.
- *Infected – non-killable*
The virus scanning engine has found a virus in the file, but has no information in its database about the method of disinfection.
- *Suspicious*
The virus scanning engine has found a virus-suspicious file. This means, that the file contains code, or a code segment, which indicates the presence of a virus. You can read detailed information about this topic in the [Heuristics](#) section.

The virus found window can be displayed during the operation of the following modules (if the module is available for the product):

- Scanning task, during a quick scan
- If the Shield is active (not interactive)
- MS Office protection
- MS Outlook protection
- Rescanning of quarantined files

Individual *Virus found settings* can be assigned to all of these modules and the method of disinfection can be set for the found viruses for each module separately.



Virus found window

At the top of the window the icon and the name of the module is displayed, which has sent the message. This informs you, which module has found the virus. The red bar in the middle informs you about the type of the infection and above it, you will receive information about the method of disinfection and possible further activities. Below the red bar, the infected file's name and its path are displayed and next to it – if this information is available, the found virus's name can be found.

In the bottom of the interactive panel, there are buttons, with the help of which you can specify actions.

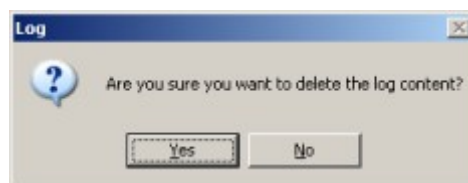
The program can only send a warning message about incidents, which are reported by the *Shield* module, infections will be handled as set in the module's *Virus found settings* section.

By clicking on the **|X|** button in the top right corner of the window, the *Skip* action will be performed on the current incident.

By enabling the *Apply to all* option, the system will not notify you about found viruses of this type and the set actions will be performed on the same type of virus incidents.

Warning

These messages provide information about changes and effects or results of an operation which have been initiated by a user.



Warning message

This window is similar to the virus found window. At the top of the window the icon and the name of the module is displayed, which has sent the message. The orange bar contains the message itself and you can read a detailed description in the details window, which can be viewed by clicking on the arrow on the right side of the *Details* bar.

The **|OK|** button is for confirming the message and the operation will be continued. If there is a **|Cancel|** button on the panel, you can delete the execution of the started task.

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