

VIRUS **BUSTER**

Personal

TABLE OF CONTENTS

VIRUSBUSTER PERSONAL	1
Minimal System Requirements	1
Installation	2
Normal Installation	2
Installation with Parameters	3
If the Installation Has Not Started...	3
Removal, Modification, Reparation	3
Starting from the Start Menu	4
System Tray	4
Pop-up Windows	6
Purchase, Registration, Activation	6
Purchase	6
Registration	6
Activation	7
User Interface	8
The Structure of the Interface	8
Testing the Virus Scan Engine	11
The Structure of Antivirus Protection	12
Shield	12
Settings	12
Scan Areas	14
Statistics	15
Software Updates	16
Creating a New Task	18
Modifying an Update Task	22
Starting an Update Task	22
Quick Database Update	29
Scanner	30
Tasks	30
Starting a Scan	36
Quick scan	36
Quarantine Module	37
Items	37
Settings	38
Log Component	40
Entries	40
Settings	41
Administration	43
Access Settings	44
General Settings	44
Mailer Settings	46
Central alert	46
Rights Management	48
Activation	51
Sending mails	52
Virus Scanning Methods	53
Heuristics	53
Actions	54
Windows, Messages	55
Virus Scan Window	55

Message Window	56
END USER AGREEMENT	59
CONTACT	61

VIRUSBUSTER PERSONAL

VirusBuster Personal provides comprehensive protection for every personal computer. On the one hand it provides continuous protection with the help of the resident protection (Shield) component, which operates effectively against both program viruses and macro viruses. On the other hand further components (described later) provide both automation and adjustability of virus scans and program updates. Log is made of the events occurring while the software is run. For greater protection, the program creates a quarantine directory into which the infected or suspicious files are moved. These are only a few of the various functions of VirusBuster listed and described later in the document.

The main features of the product are the following:

- Effective protection for your computer against viruses
- Easy to use, wizard-style user interface
- Advanced user interface for experienced users
- Task-oriented operation
- Incremental virus database update
- Manual, automatic, and scheduled scanning
- Resident protection with pre-defined protection levels
- Task-oriented, modular updates
- Intelligent quarantine for infected files
- Support of 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 XP/2000 (SP4) - 256 MB Windows 7/Vista - 512 MB <i>It is recommended to install the latest Service Pack and use at least 512 MB memory (1024 MB when using Vista) depending on other applications running on the system.</i>
Free hard disk space	200 MB
Browser	Internet Explorer 6
Other	If you need more information, check the readme.txt file – it is in the installation kit.

Installation

Make sure that your computer is virus free before installing the software. The antivirus software can only operate properly if it is installed on a virus free computer. Perform a virus scan on the computer with the help of VirusBuster Scanner's latest version that can scan the whole system for viruses in a fast and easy way.

Note!
If an antivirus software is already installed on the computer, it must be removed before installing VirusBuster. If an older version of VirusBuster is installed on the computer, it must be removed as well.

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

Normal Installation

Install instructions must be followed that guides you through the installation process.

Welcome Panel

You can start the process from the welcome screen by clicking on the **|Next >|** button. The end user license agreement is displayed in the next window. Generally, at the bottom of every window, you can return with the **|< Back|** button and quit the installation process with the **|Cancel|** or **|Exit|** buttons.

Displaying and Accepting the License Agreement

Read the agreement and select the **|Yes|** button if you accept the terms 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 to terminate the installation process and exit the wizard.

Information about the Product

You can specify the installation path after clicking on the **|Next >|** button.

Choosing the Installation Path

By default, the product is installed on the system partition in the `Program files\VirusBuster\` directory that 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 selecting the installation path, you can continue 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 *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

After selecting *Custom* mode, program components can be selected to be installed or not. After selecting

the needed components, you can continue by clicking on the **|Next >|** button. The display of the following panels depends on the selected components.

Additional Data

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

Starting the Installation

Finally, you can check the settings and components to be used during the installation of the product. Copying files is started by clicking on the **|Next >|** button.

Successful Installation

If the installation is finished without any problems, you can exit the installer after all files are copied by clicking on the **|Finish|** button. The software is installed successfully.

Installation with Parameters

By specifying parameters after the installation file, other installation modes can be enabled that are not available during regular installation. You can find 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...

Check that your computer fits all minimal system requirements. Check if your system has all the needed system and program components. Without these, installation cannot be performed and an error message informs you about the needed system component that is required in your computer before installing the antivirus 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.

The product can also not be installed if another antivirus product can be found on the computer. In this case, you have to remove the existing av application before installing the VirusBuster.

Removal, Modification, Reparation

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

1. Click on the *Add/remove program* icon on the *Control panel*.
2. Search for the product to be removed from the list and select it.
3. Click on the **|Modify/remove|** button.

You can select the needed operation in the window that is displayed:

- *Modify*
If you select this option, a component list appears 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) are 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 Personal is available under Start / Programs / VirusBuster Personal after 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

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

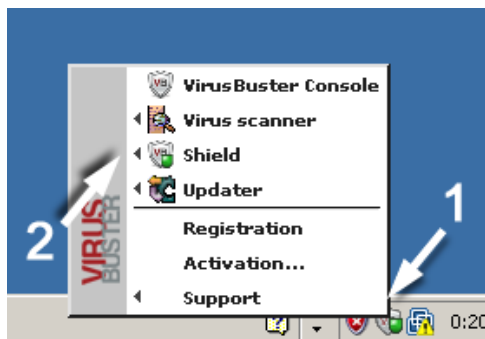


VirusBuster Icon on the System Tray

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 color of the shield indicates the status of the resident protection:

- *Green*
Shield is active, the computer is protected against viruses (if the product is registered or is in a trial period).
- *Gray*
Shield is not working, 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 right-clicking on the VirusBuster icon (1), a local menu appears where the needed function can be selected. If a menu has a sub-menu, it is indicated with a little arrow in front of the name of the menu item (2).



VirusBuster Icon on the System Tray – Local Menu

The following items are always listed in the menu:

- *Support*
This menu item contains three items which are the following:

Help

The documentation files of the installed product 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.

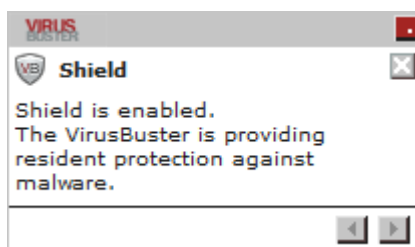
Information

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 double-clicking on the menu.

Pop-up Windows

Through pop-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 operation of the software.



Pop-up Window

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

The pop-up window closes after a short period of time, but users can also do it by clicking on the [|X|](#) button placed in the top-right corner of the pop-up window.

Purchase, Registration, Activation

The installed antivirus software can be used for 30 days with full functionality after the first installation. During this 'Trial period', the user can access all functions and settings, and all virus removal functions are available. The software has full functionality for virus protection during this period; the only difference between the registered and the trial version is that it regularly warns the user in a message window (when starting components) that it is a trial period and the software can be registered using several methods. Several options are available: the product can be purchased, registered, activated, or – only during the trial period – the [|Continue|](#) button can be used to start the software (and to postpone the purchase, registration, activation of the product). The [|Exit|](#) button closes the program.

Purchase

The purchase function is available in the pop-up window by clicking on the [|Buy ...|](#) button. The software redirects the user to VirusBuster's home page, through which the product can be bought online – this is an e-mail-based license order – and the user receives the registration information to be used for registering the product.

Registration

The product can be used with full functionality for 30 days after installation, this is the trial period. After this period, the software cannot be used without registering it with a valid license key. The panel where the program can be registered can be opened by clicking on the [|Register ...|](#) button in the pop-up window or by accessing this function from the menu of the VirusBuster icon in the system tray.

On the registration panel, the product to be registered can be selected from the *Product's name*: drop-down menu (several products can be installed on one computer at the same time). The registration

information must be typed in the *User name:* and *License key:* fields accordingly. Then the software can be registered by clicking on the [|Register|](#) button if valid registration information was supplied and the date of expiry is displayed on the panel. A green line appears with *Registered* written on it.

When registration expires, the product can be used with full functionality until the next software update. According to the license agreement of the product, the right to use product updates is only valid during the license period. According to this, the product can only be updated after the registration expired if a new license is bought and the software is registered again. If a new license is not bought and the product is not registered again, an update ceases all functionality. This is not valid for the virus database, the database can be updated without any limitations, but the vendor does not provide any guarantee for the compatibility of the software with the new database updates.

Activation

During the activation process, the user can request the product license key (3x5 characters) with the help of the activation key (3x4 characters) online. The activation is not the registration itself, but the process of acquiring the license key. The beginning of the registration period is the day of activation and is valid for the period set in the license agreement.

The activation panel can be accessed in a pop-up window by clicking on the [|Activation ...|](#) button.

User Interface

VirusBuster products have a unified appearance, which provides a comprehensive control interface for the programs. The installed products can be started with the same icon ([Starting from the Start Menu](#)), all of the installed components are available on the joint user interface.

Important!
If the user is logged into the system without administrator rights (low level user), most of the settings are not available for this user on the user interface.

VirusBuster products have a wizard-based user interface that is used to modify the settings of the product easily. The settings of the functions can be modified step by step with the help of the detailed description on each settings panel.

The settings of the protection components on the wizard-based interface can be modified on the following two levels:

- *Simple* user interface
This interface is for beginner users. Only the basic settings are listed, and only the most important parameters can be modified. The product can be customized to the user's needs with the pre-defined settings combinations.
- *Advanced* user interface
This interface was designed for experienced users. All settings are available on this interface and the system can be totally customized for unique needs.

You can switch between the two interfaces with the **Simple** – **Advanced** buttons at the bottom of each settings panel.

Important!
In case of switching from the *Advanced* user interface to the *Simple* user interface, there may be some settings that cannot be associated with any of the settings combinations on the simple interface. In this case (that is, if switching is done), all the settings modified on the advanced interface are lost and are replaced with a settings combination that can be displayed on the simple interface.

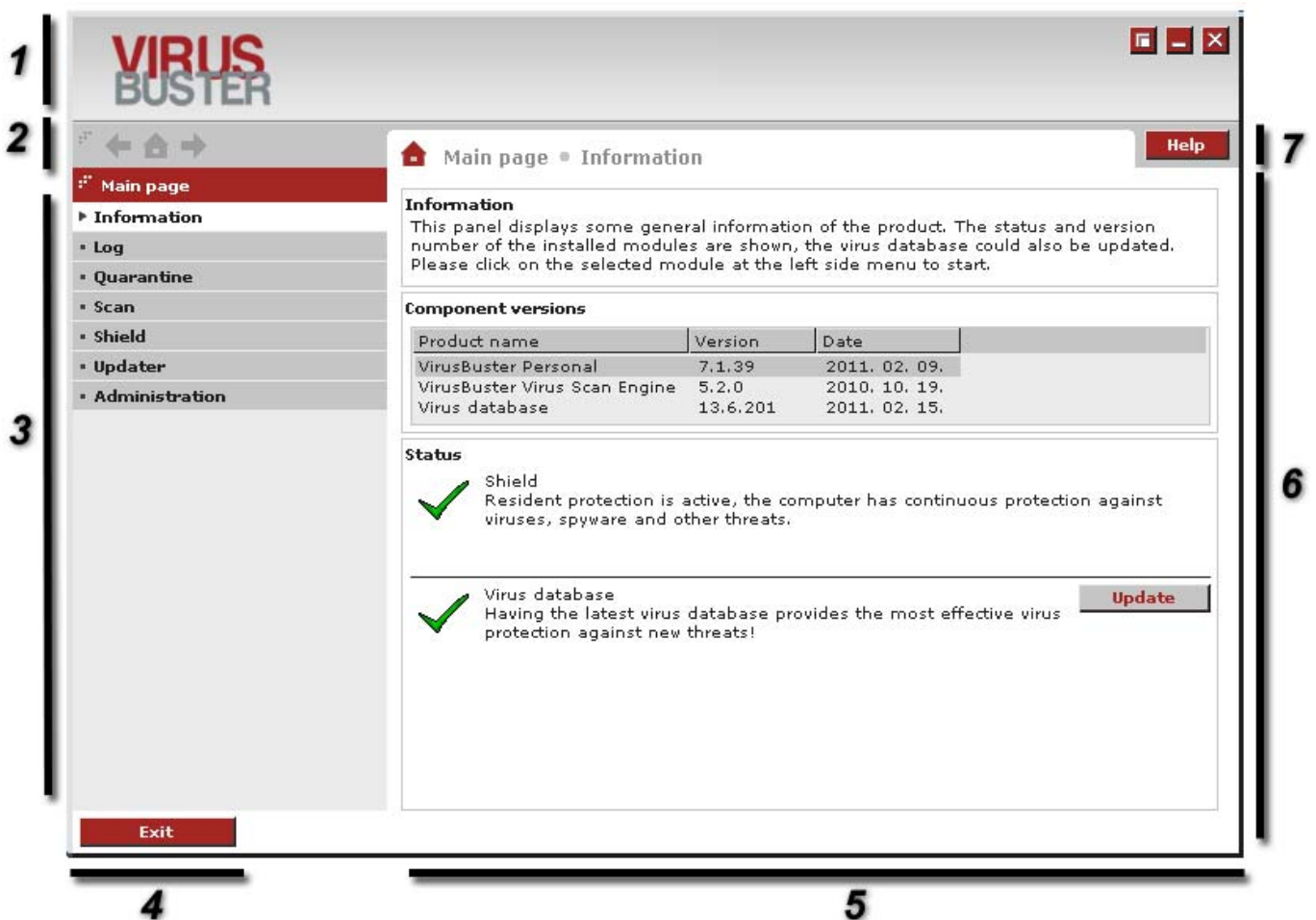
The Structure of the Interface

VirusBuster's user interface can be displayed by starting the product from the *Start menu* with the *VirusBuster Personal -> VirusBuster Console (Personal)* shortcut. On this interface, the needed settings can be modified, a virus scan can be started, messages can be sent, and so on, with the help of menus and panels.

After the console is started, the *Main page* appears containing basic information about the program. You can check the status and version numbers of the installed VirusBuster products and the most important components. The virus database update can be started by clicking on the **Update** button. You can check the status of the *Shield* and the version of the virus database. The used icons and their meanings are the following:

- ✓ The service is active. / In case of the virus database: the database is newer than two days, it is up-to-date.
- ! The service is stopped. / In case of the virus database: The database is older than seven days.
- ! The service is not installed. / In case of the virus database: There is a virus database error.

You can check the settings of each component with the menus (3) on the console. By clicking on one of the menus, the options and settings of the component are displayed on the settings panel (6). In this case, the sub-menus of the selected component are displayed in the menu (3). With the help of the menu, you can access other functions and settings of the component or you can see the step you are currently at in a multi-step settings process. You can return to the Main page by clicking on the house icon of the navigation panel (2). Each step of the navigation can be accessed with the right and left arrows.



Wizard-based User Interface

The structure of the interface:

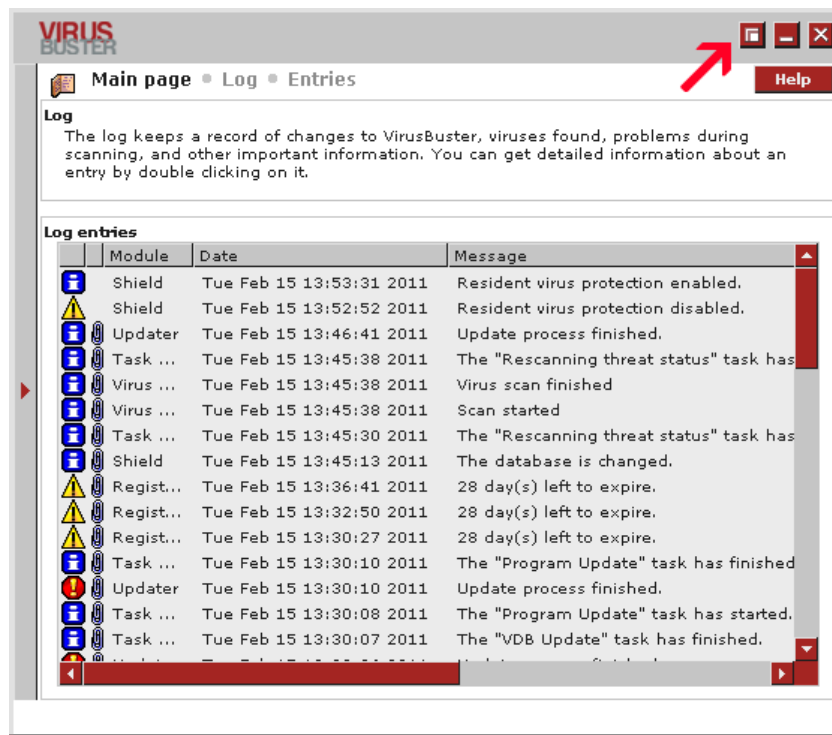
- 1 *Header*
The window header, VirusBuster logo
- 2 *Navigation panel*
Navigation through the selected menu items and the panels
You can access the previously viewed panel(s) and menu(s) with the left arrow, and you can access the last step from which you stepped back with the right arrow. You can access the main page by clicking on the house icon. The lock symbol shows if the main options can be changed or not ([Administration](#)).
- 3 *Menu*
You can access the settings panels of the installed components with the menu items.
- 4 *Exit*
You can exit the program any time by clicking on the **|Exit|** button.
- 5 *Panel control buttons*
There are several buttons to help the settings process or to start a process on most of the settings panels. With the help of these buttons, you can switch between the simple and advanced user interfaces, go through a settings process, or start the selected task.
- 6 *Settings panel*
The settings panel of the component, option, or operation that was selected in the menu (3) is displayed here. Settings can be modified and tasks can be added or started on this panel.
- 7 *Help*
You can view help in connection with the settings of the active panel.

Switching to Compact User Interface

If the product is run on an operating system with low screen resolution, some parts of the panels may be invisible for the users, because there is no place to display the window as a whole. In such a case, some menu items or options cannot be entirely seen. If this happens, you are recommended to switch the VirusBuster product interface to *Compact view* with the first control button in the right upper corner of the user interface. To switch back to normal view, click on the same button again.

| Important!

If the screen resolution is 640X480 pixels, only the *Compact view* is available for the product. In such a case, the switch button is not displayed on the screen.



Compact Mode

In *Compact view*, the left side menu disappears saving place on the screen. Click on the side bar that you can find instead of the regular menus on the left to select modules. It appears covering the settings panel. After selecting the required module, you can make it disappear by clicking on the same side bar button.

Testing the Virus Scan Engine

In order to see what happens when our virus scanning engine finds an infected file, you can use the European Institute of Computer Antivirus Research (EICAR) Standard Antivirus 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 with the **.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 is a warning window.

Note
If executed, this small COM file displays the "EICAR-STANDARD-ANTIVIRUS-TEST-FILE" message and it exits.

The Structure of Antivirus Protection

VirusBuster products consist of modules and the software components together create the antivirus protection. The following sections describe the operation and the structure of each component.

Shield

This component provides resident protection against viruses. Its main task is to scan the machine for viruses and remove them in the background. The component scans files when they are accessed (when writing or reading the file). The settings of the Shield can be modified in the following panels:

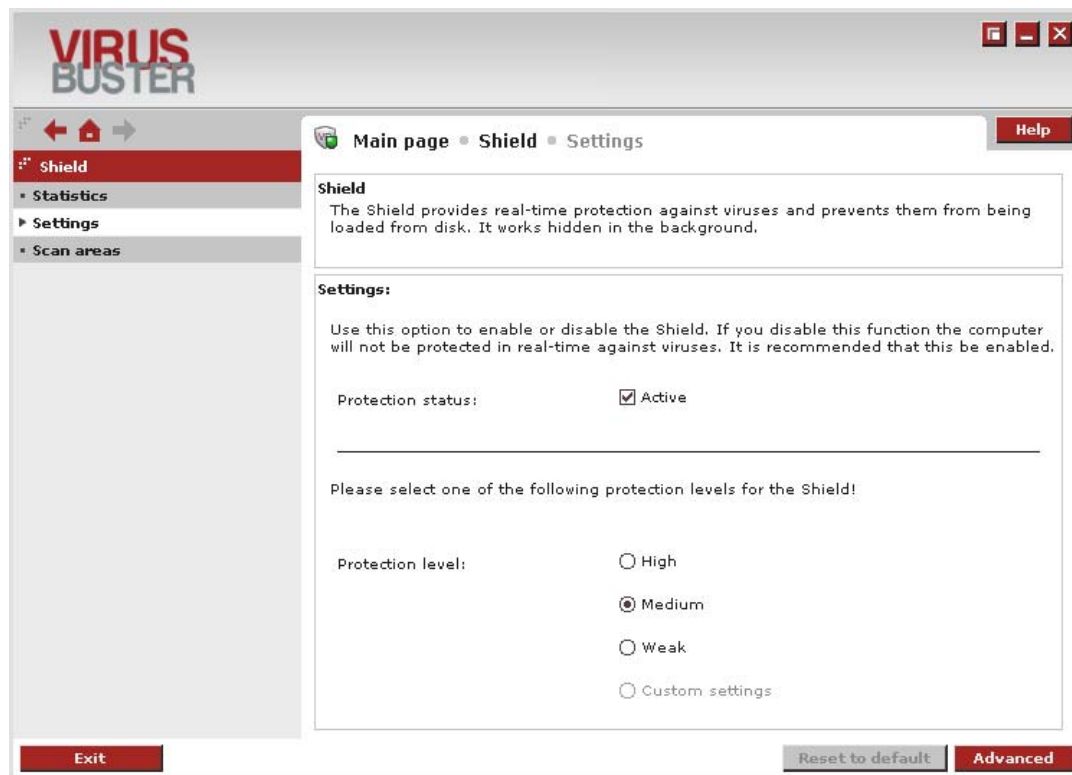
- *Settings*
- *Scan areas*
- *Statistics*

If the resident protection is enabled, the attached removable devices (such as USB stick) can also be scanned quickly. When you are plugging a new device, a pop-up window will be displayed above the tray on which you can click to start scanning. If you don't click it, the window will disappear automatically after a while.

Settings

The settings of the resident protection can be modified in the *Settings* panel. It can be configured in a matter of seconds on the simple user interface or in details on the Advanced panel, which can be displayed by clicking on the [Advanced](#) button.

Simple Settings



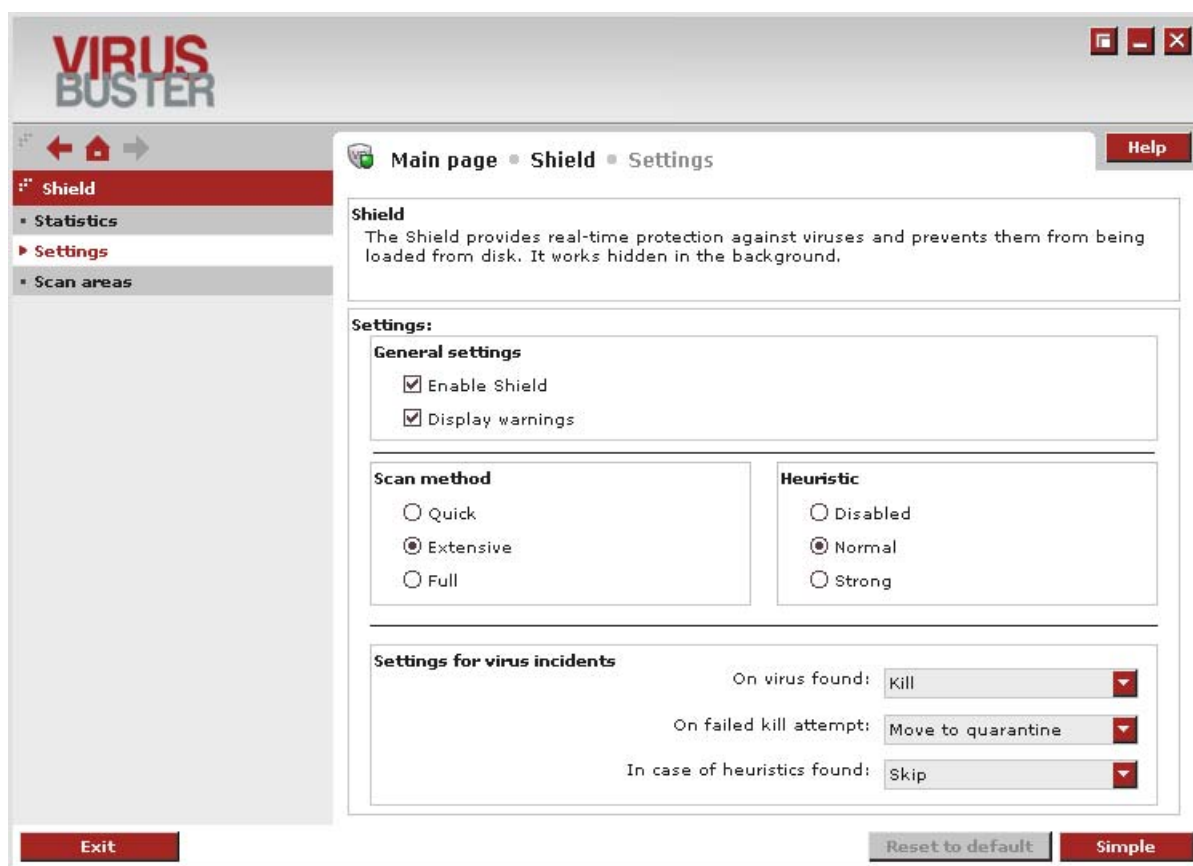
Shield - Settings

The resident protection is active if the *Active* option is selected. The level of the resident protection can be easily set by choosing from the pre-defined levels in the panel. The protection levels are a combination of settings that can be displayed by switching to the *Advanced* panel.

The protection levels and their settings are the following:

- *High*
Uses the *Full* virus scanning option, high heuristics; killable viruses are disinfected, non-killable viruses are moved to the quarantine.
- *Medium*
Uses the *Extensive* virus scanning option, medium heuristics; killable viruses are disinfected, non-killable viruses are skipped.
- *Weak*
Uses the *Fast* virus scanning option, no heuristics; killable viruses are disinfected, non-killable viruses are skipped.
- *Custom settings*
This option cannot be selected. It is enabled if a combination of settings that is not present in any of the pre-defined levels is created on the *Advanced* panel.

Advanced Settings



Shield - Advanced Settings

The resident protection can be activated by enabling the *Enable Shield* option on the *Advanced* panel.

By enabling the *Display warnings* option, the user receives a warning message when a virus is found. Otherwise, if this function is disabled, the program performs the selected actions, but the user does not

receive any messages, only the log entries.

The scanning method can be set to the following levels:

- [Quick/Extensive/Full](#)

Heuristic analysis can be set to the following levels:

- [Disabled/Normal/Strong](#)

The description of the *Virus found settings* can be found in the *Scanner* [section](#).

Available actions when a virus is found are the following:

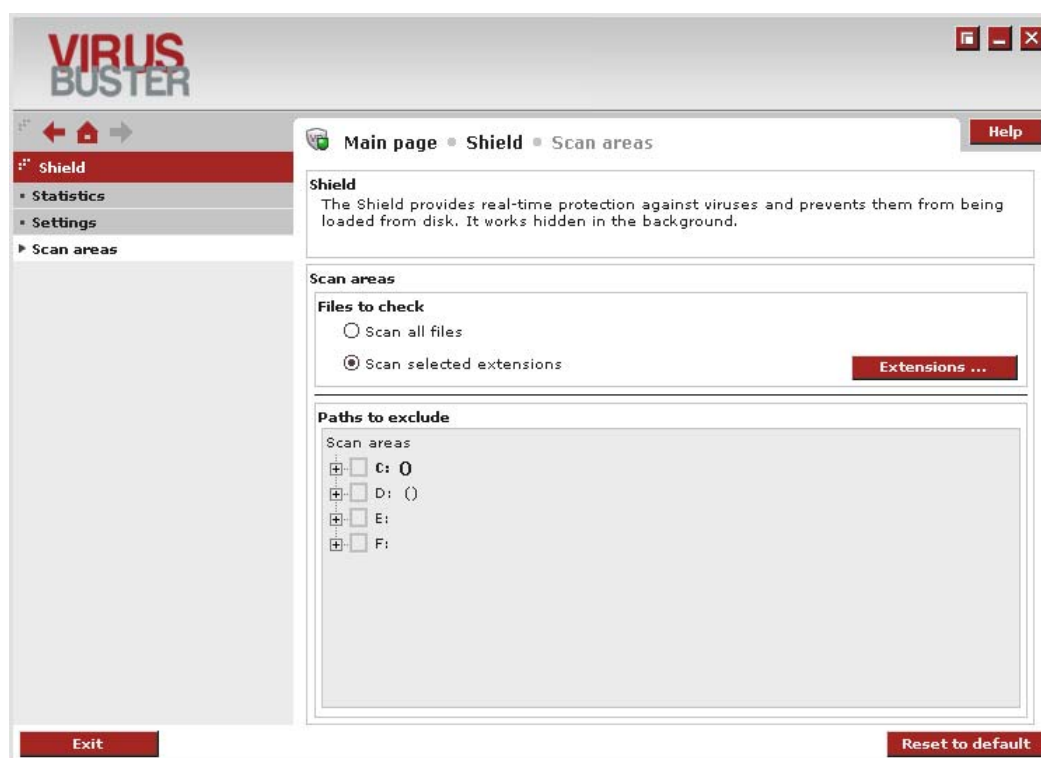
- [Kill/Skip/Rename/Move to quarantine/Delete](#)

Available secondary actions and actions for heuristic detections are the following:

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

Scan Areas

In this panel, you can specify the file types to be scanned and the paths not to be scanned.



Shield – Scan Areas

If the *Scan all files* option is enabled, all file types (extensions) are scanned when they are accessed.

If the *Scan specified file types* option is enabled, only the specified file types (extensions) are scanned when they are accessed. The extensions can be set as described in the [Extension settings](#) subsection of the section about the Scanner component.

In the *Excluded paths window*, the drives and directories on the computer are displayed in a tree

structure. The user can select the paths not to be protected, and files under these paths are not scanned when they are accessed. A plus (+) sign indicates if a directory has sub-directories. The plus (+) sign is changed to a minus (-) sign if the directory is open and its sub-directories are displayed. A directory can be opened by clicking on its name or on the plus (+) sign. If the checkbox in front of the directory is selected, the files in the directory are not scanned. The opened or closed status of the directory is very important when selecting checkboxes: because if it is open, its sub-directories are scanned, or if it is closed, all the sub-directories are selected recursively. Directories selected recursively are marked with an asterisk (*).

There are three options for selecting a directory:

- The checkbox is selected.
The selected directory and all its sub-directories are selected, and the files in these are not scanned when they are accessed.
- The checkbox is not selected, the name of the directory is bold.
There is a sub-directory in the directory to be checked. The files in this directory are not scanned when they are accessed.
- The checkbox is not selected, the name of the directory is not bold.
Neither the directory nor any of its sub-directories are checked, all files in these directories are scanned when they are accessed.

Statistics

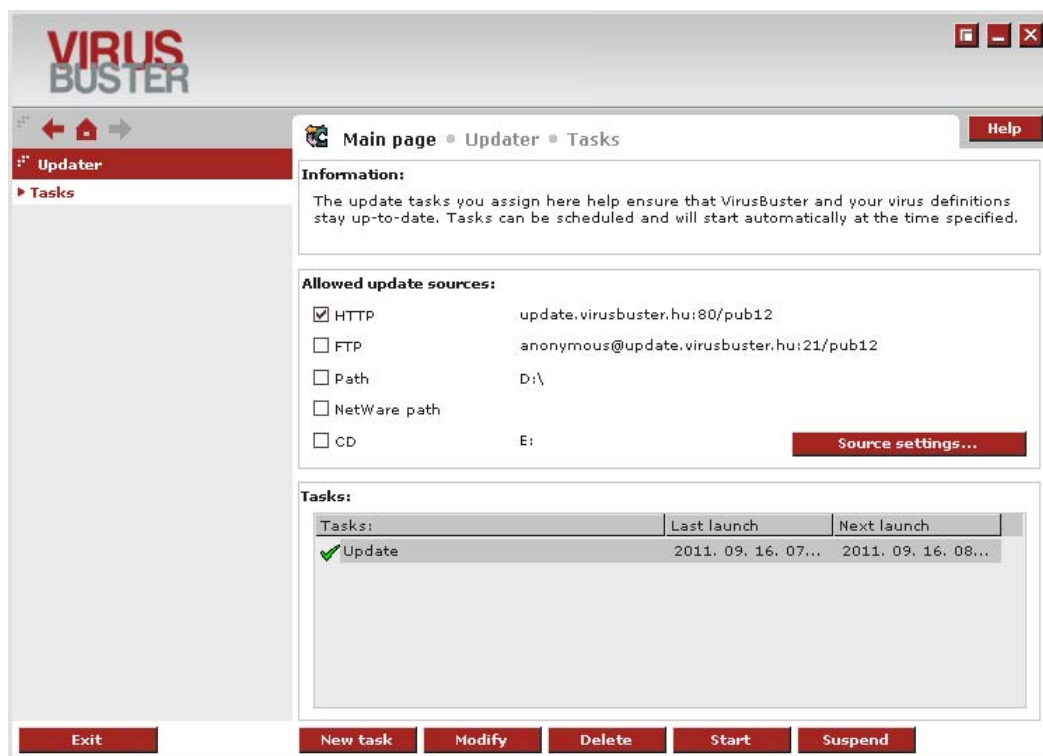
Comprehensive information about files scanned by the Shield and the detected infections are available. The name of the last found virus and the path where it was found are also displayed in this panel.

Software Updates

Updating the software and the virus database is essential for maintaining the efficiency of the antivirus 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 is performed with the pre-defined settings. Software update tasks can be added or modified in the *Updater* module, which provides an interface for creating tasks step by step to set the options and parameters needed for the update.

The product uses an incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program does not 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. With this mechanism, the download time is decreased to a minimal level, so additional virus database packages can be released several times a day to improve security. Users can obtain protection against new malware without spending a long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses were processed in our virus lab.



Updater

The needed source can be activated (after this, updates can be performed from the source) by selecting the checkbox in front of an update source in the *Tasks* menu item in the *Allowed update sources* settings. After this, the source can be selected when adding a new task or modifying it. Information about a source is displayed next to its name, these can be modified by clicking on the [Source settings ...](#) button. In this window, the settings for each source can be modified. The settings of the item selected from the drop-down list can be modified at the bottom of the panel. Keep in mind that each task tries to perform the update via the assigned update source only.

Important!

If a source selected for a task is inactivated, the task cannot be started until the source is reactivated.

The possible update sources and their settings are the following:

- **HTTP**
Update through the HTTP protocol. Specify the name of the HTTP server, the used port (default is 80) and the path where the descriptor file can be found. The default setting is:
update.virusbuster.hu:80/pub12
If the connection needs a proxy server to access the update source, you can specify additional settings:
 - Proxy
 - *None* – There is no need for a proxy to access the network.
 - *Specified in Explorer* – Application gets pre-defined proxy settings from Windows Internet Explorer.
 - *Customized proxy* – If this option is selected, you can manually set the proxy settings.
 - Proxy server/port – Address and port settings required to access the proxy server.
 - Proxy user/password – Username and password if the proxy server needs authentication.
- **FTP**
Update through the FTP protocol. The name of the FTP server, the port used by the server (default is 21) and the path where the descriptor file can be found and the username and password for logging in must be specified. If you are using the 'Anonymous' user name, type your own e-mail address in the password field. The default setting is:
[anonymous@update.virusbuster.hu:21/pub12](ftp://anonymous@update.virusbuster.hu:21/pub12)
- **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, select the letter of the drive 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.

New tasks can be added or existing ones can be viewed, modified, started, or stopped at the bottom of the panel. In the first column of the task list, the task name is displayed, then the date of the last start, and the date of the next start or the trigger event. The last column indicates if the task is stopped.

The product contains a task called *Update* by default which checks the update source in every hour for new product version or virus database and if it is available, the update process will be started.

The following operations can be performed by clicking on the appropriate buttons at the bottom of the panel:

- **|New task|**
For creating a new task and specifying its settings
- **|Modify|**
For [modifying the settings of a selected task](#)
- **|Delete|**
For deleting a selected task
- **|Start|**
For [running a selected task](#)
- **|Suspend|**

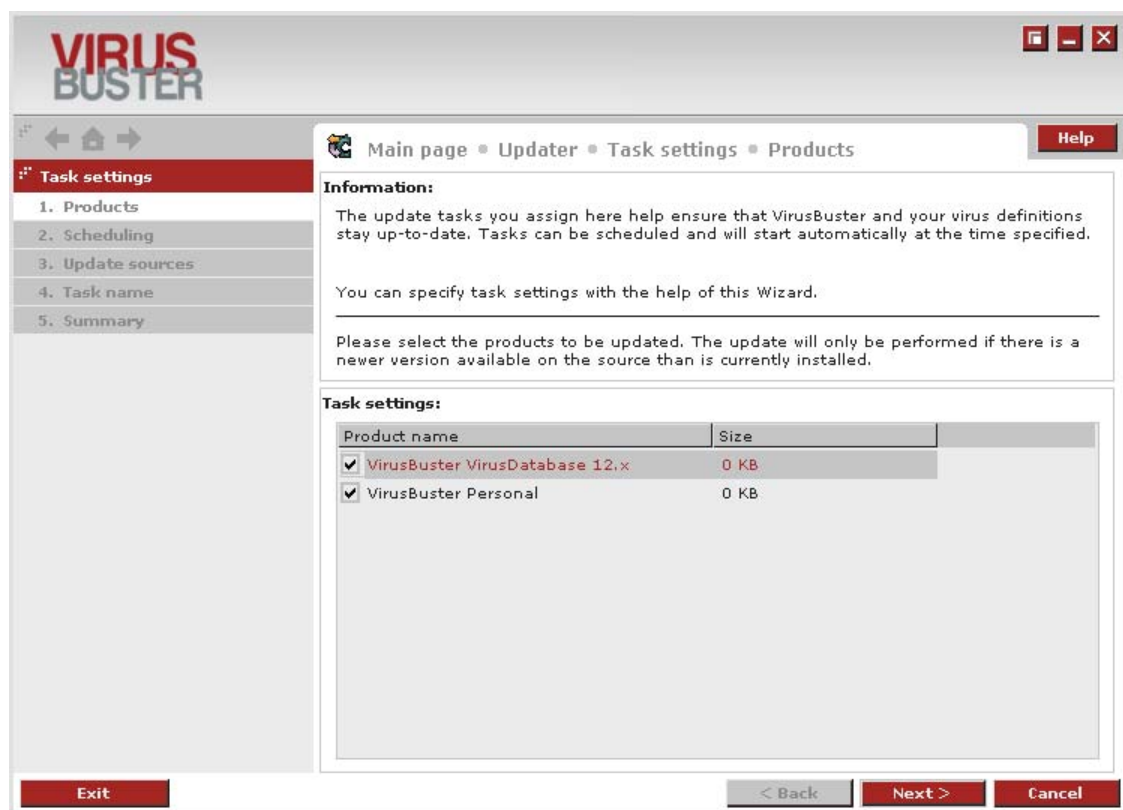
For suspending the selected task: the task cannot be started and does not start until it is authorized again.

Creating a New Task

The settings for a new task can be added step by step, and the attributes of the task can be modified during the steps.

Products

The first step is to select the product(s) for the update task. The task checks if the selected product(s) are up-to-date and if there is a newer version of the product(s), it downloads them and updates the system. The list contains the installed products and the virus database file that can be chosen by selecting the checkbox in front of them. At least one item must be selected to be able to continue with the wizard.



Updater – Selecting Products

Scheduling

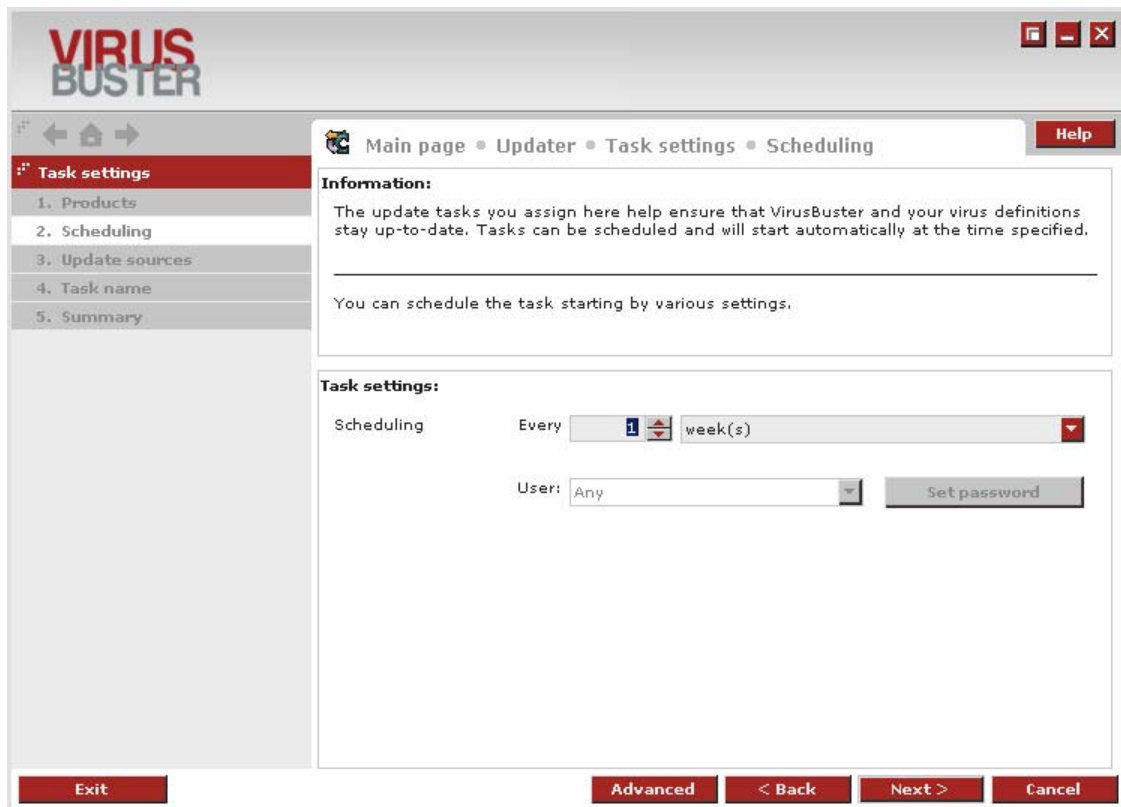
The beginning of the update process can be scheduled in this panel by specifying the needed date or an event as a trigger.

The update task is started and performed using the user privileges of the user profile set in the *User:* field. The password needed for logging in can be specified by clicking on the [\[Password ...\]](#) button.

Simple Settings

The following periods can be selected to schedule the starting of a task:

- Day(s)/week(s)
A number can be specified here and the software starts the update every x days or weeks. On the required date, the task is started when the user logs in to the system and the network is online. If the task starting was not successful, the program always tries starting the task in every login time until it can be performed successfully.
- Manual start
The task must be started by the user manually. The task can be started after it was selected.



Scanner - Scheduling

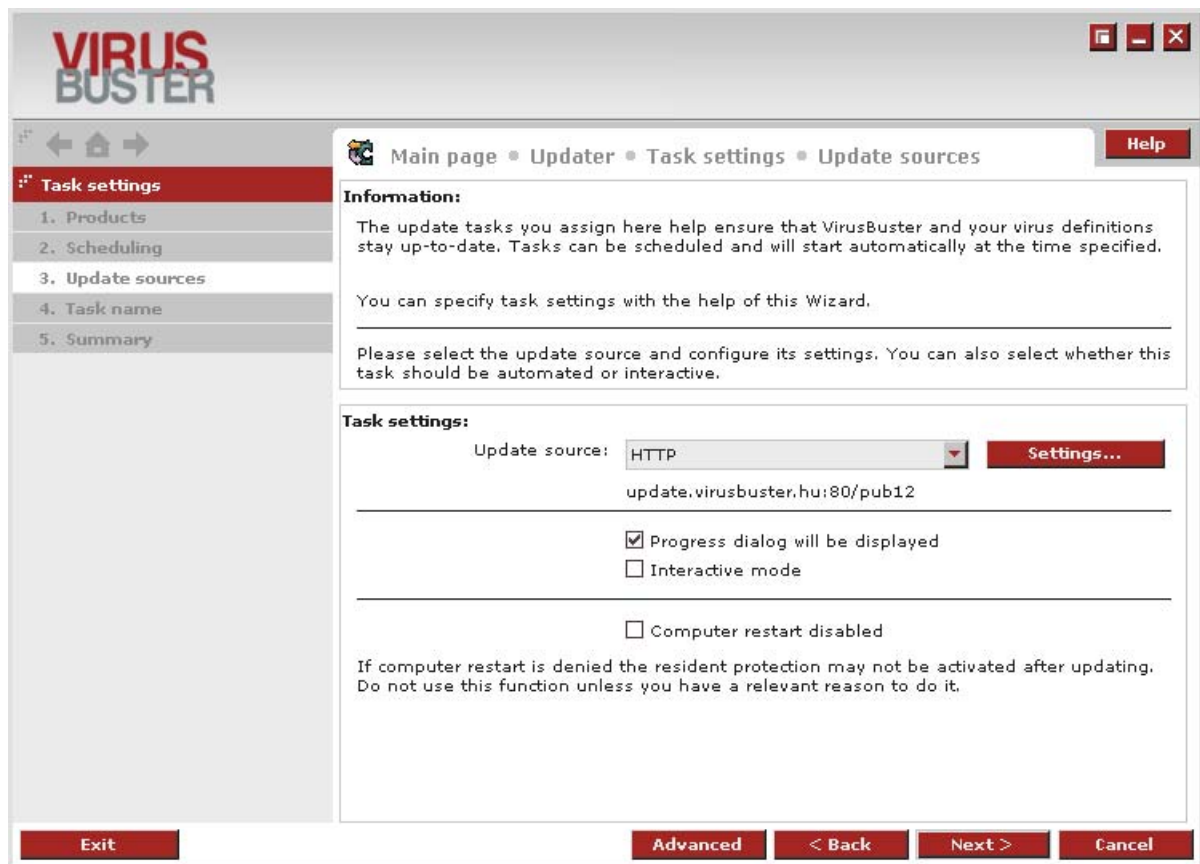
Advanced Settings

The following settings are available on the detailed scheduling panel:

- Day(s)/week(s)/hour(s)
- Manual
- Scheduled
An exact date can be specified for starting the task (hours, minutes), then the days when the task must be started can be selected.
- Every quarter-hour / every half-hour
The task is started at the specified periods on the selected day(s).

Update Sources

Simple Settings



Update Sources, Simple Interface

You can select the update source from the drop-down list where the software checks for new updates at the given time. Only the active update sources are available that can be set on the main panel of the *Updater* under [Allowed update sources](#). The settings of the update sources can be modified globally by clicking on the [Settings ...](#) button.

If you check in the *Progress dialog will be displayed* setting, you can follow the update process, otherwise, the task runs in the background without the window displayed.

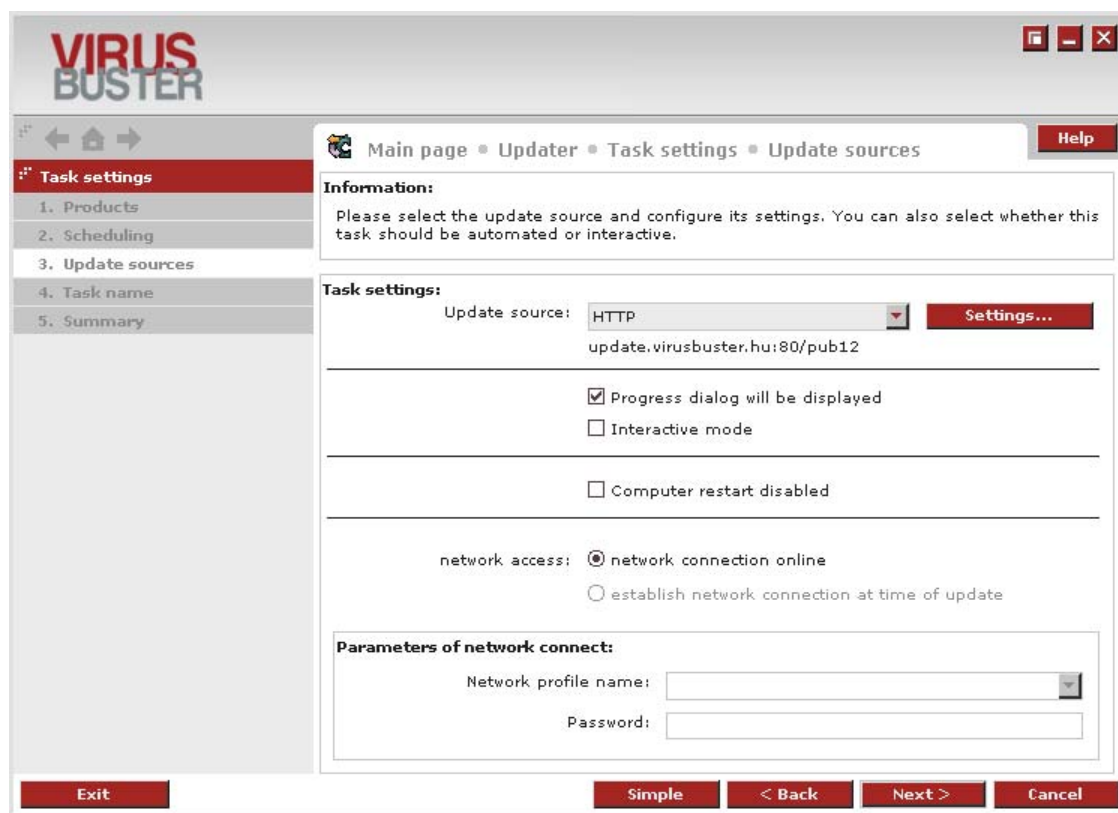
By enabling *Interactive mode* if the *Progress dialog will be displayed* setting is checked, the user can follow the whole update process step by step and can change the settings of the task temporarily.

The *Computer restart disable* option controls the system restart. If you select this setting, the computer is never restarted after the update process is finished.

Important!

Do not disable computer restart unless you have a relevant reason to do so, because there may be changes performed during the update process that require computer restart to be activated. If it is disabled, it is possible that the resident protection of the machine may not be activated and your computer is not protected.

Advanced Settings



Update Sources, Advanced Interface

The above options can be all found on the advanced interface, and with the help of the *Network access* setting, you can specify the *Updater's* network handling.

If the *Network connection online* is selected, the started task does not try to create a network connection, and if the network cannot be accessed, it generates an error. If the *Establish network connection at time of update* option is selected (if the network connection is not available continuously, for example, in case of a dial-up connection), the task creates a network connection and terminates it if the task is performed and the connection was established by the software. The second option activates the *Parameters of network connect* where you can select the needed network profile from a drop-down list and specify the appropriate password.

Task Name

To specify a name for the task, type the needed name in the field. You can refer to the needed task on the *Tasks list* window of the *Tasks* panel with this name in the future. It is not possible to add two tasks with the same name and the \ (backslash) character cannot be used in the task name.

Summary

The settings specified during the steps above can be checked on this panel. If the settings are correct, the task settings can be saved by clicking on the **Finish** button. You can return to the last settings panel by clicking on the **Back** button. You can return to the *Updater's* main panel by clicking on the **Cancel** button and all settings are lost (the new task is not created or modifications are not saved).

Modifying an Update Task

When modifying a task, the same steps are present like in case of adding a new task.

- *Summary*
You can check the settings of the task.
- *Products*
You can modify the list of products to be updated ([Products](#) panel).
- *Scheduling*
You can modify the scheduling of the task ([Scheduling](#) panel).
- *Update source*
You can select a new update source for the task ([Update source](#) panel).
- *Task name*
You cannot modify the task name. This setting identifies the task being modified.
- *Summary*
A summary of the modified settings ([Summary](#) panel).

Starting an Update Task

An update task – according to its settings – can be started at a specified time (scheduled), or can be triggered by an event (system startup), or the user can start it manually.

The steps of the update task can be checked if it is interactive – this can be specified when adding the task or modifying its settings in the [Update Sources](#) panel.

The operation of the tasks can be automated during any step if you select the *Automatic operation* option at the bottom of the panels. In this case, the product automatically performs the steps of the update and you can check a summary of the update process in the *Summary* panel.

When the update process starts, the program collects the version information of products and components, then compares these to the information stored in the specified update source, and if an update is needed (new versions are available in the update source), it downloads these to the computer and the updates the programs and modules.

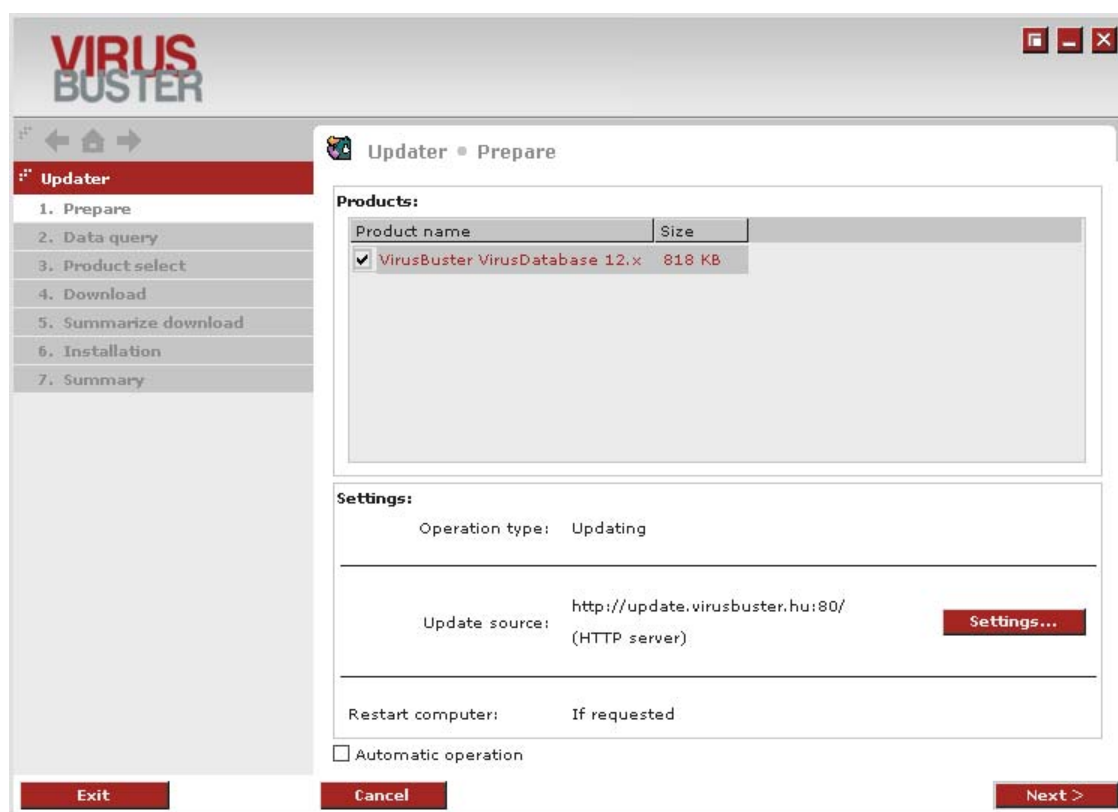
During interactive operation, the update process can be followed and the results are displayed in the Summary panel.

Preparation

The main settings of the update task are displayed here.

! Important!

It is possible to modify the settings to be valid temporarily for the started task before running the task.



Update Process - Information

The Updater tries to update the products displayed in the *Products* window. The list has two columns, the first contains the name of the product, the second contains its size (in MBs). In front of the items displayed in the first column, there are checkboxes, and by selecting them, you can disable the products not to be updated.

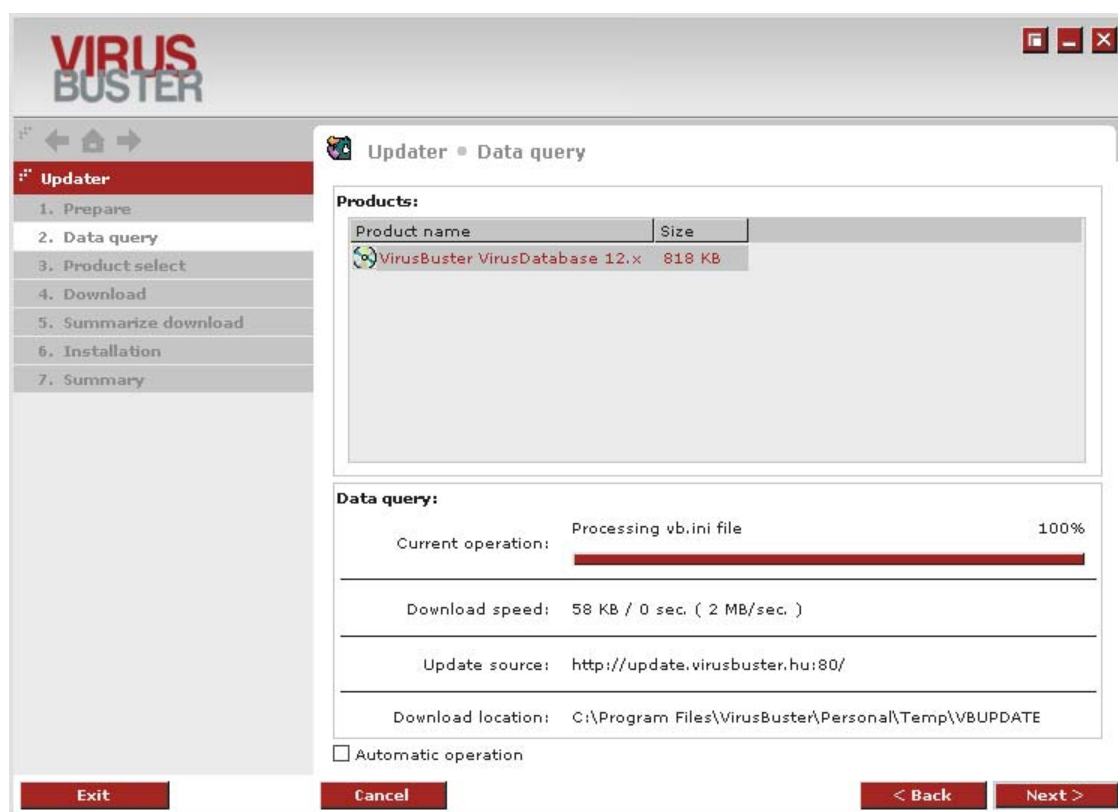
At the bottom of the panel, the most important program settings are displayed, the update source can be modified by clicking on the **[Settings ...]** button. The setting for each source can be modified in the window displayed.

After the task ended, the program restarts the computer if needed.

You can move to the next panel by clicking on the **[Next]** button and you can terminate the update by clicking on the **[Cancel]** button.

Data Query

During this step, the Updater collects information about the selected items from the update source. The items selected for update are displayed at the top of window, and the bottom of the window contains information about the status of the data query.



Update Process – Data Query

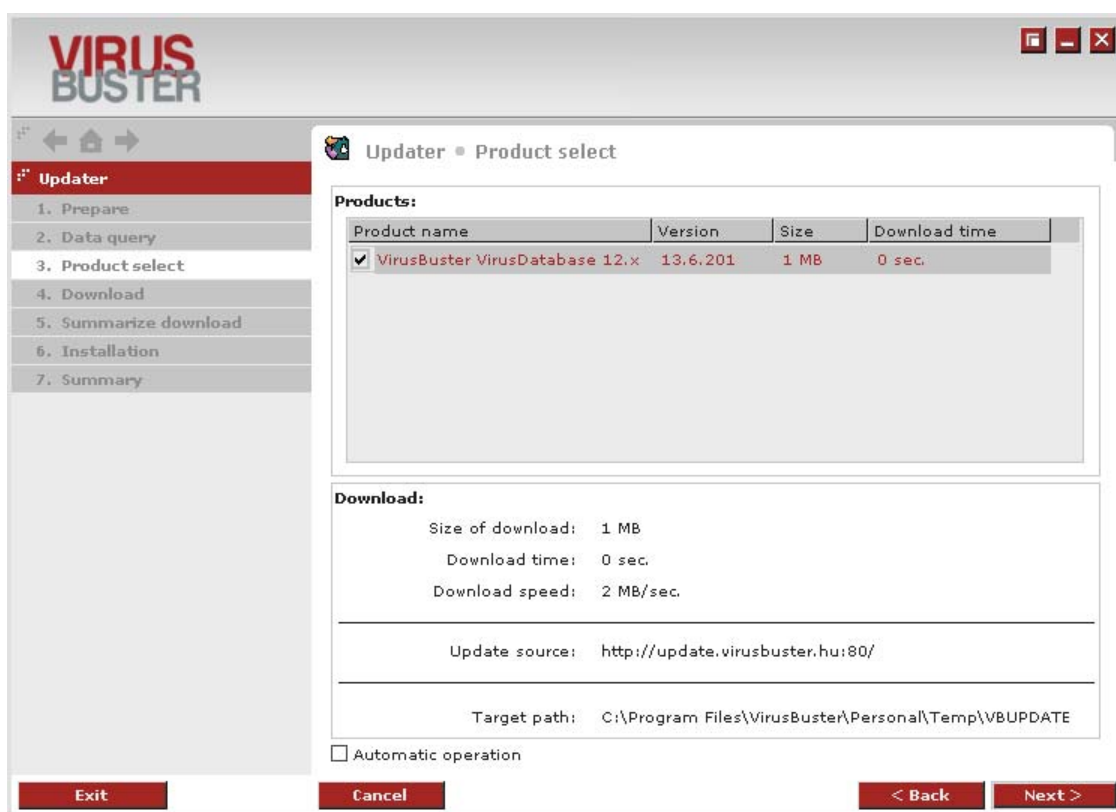
The *Current process* status bar indicates the status of collecting information. You can check the download speed, the update source, and the path for the download where the information files are stored temporarily.

If a problem occurs, you can view detailed information about the cause of the problem by clicking on the **[Next]** button to access the [Summary](#) panel. If the update process was performed without any problems, you can proceed by clicking on the **[Next]** button to the next panel, return by clicking on the **[Back]** button, or terminate the update process by clicking on the **[Cancel]** button.

Product Selection

You can modify the list of products to be updated on this panel at the top of the *Products* window.

The version number of the product, size, and the estimated download time is displayed next to the name of the product.



Update Process – Product Selection

The following information is displayed at the bottom of the *Download* section:

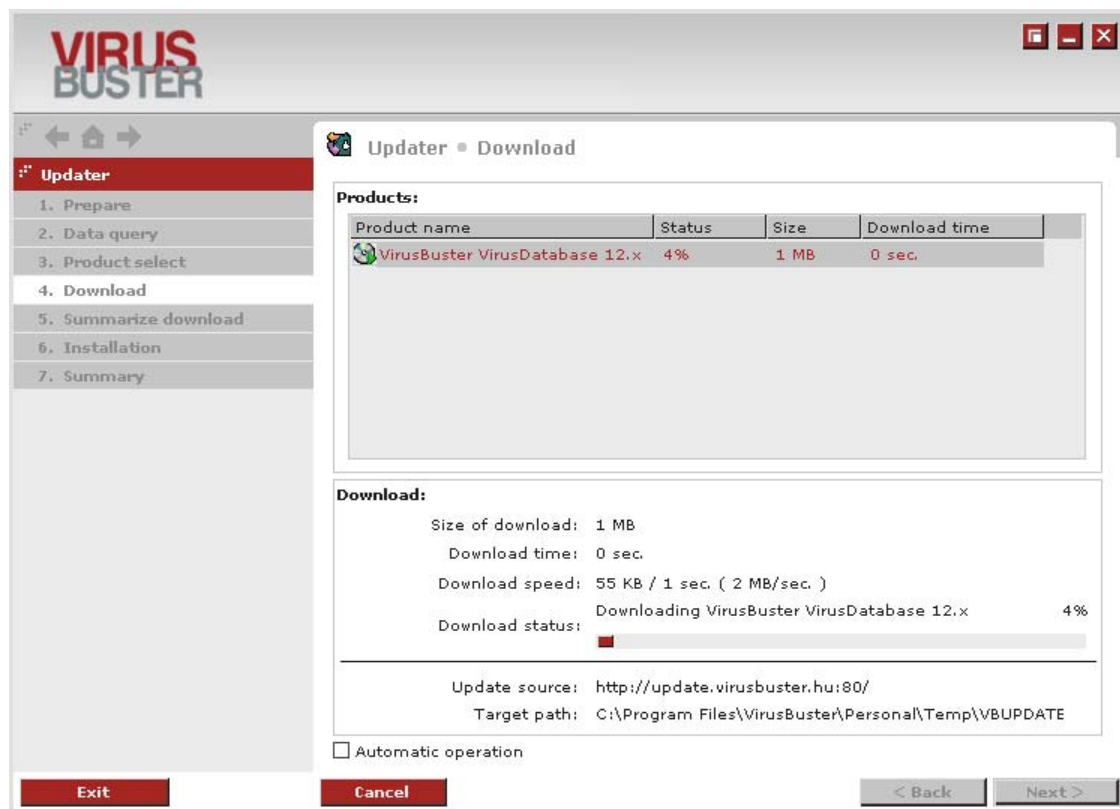
- *Download size*
The size of the selected program components
- *Estimated download time*
The estimated time required to download all components
- *Download speed*
The estimated speed of downloading files

Automatic operation can be enabled by selecting it.

After the download is finished, you can continue by clicking on the **|Next|** button to the next panel, return by clicking on the **|Back|** button, or terminate the update process by clicking on the **|Cancel|** button.

Download

At the top of the panel, the products to be downloaded are displayed in the Products window.



Update Process - Download

The little green arrow on the CD icon in front of the products indicates which product is downloaded currently. The current status and information about this product is displayed at the bottom of the *Download* section. Successful downloads are indicated by a green tick on the icon. The red exclamation mark indicates that there was a problem during the download. If a problem occurs, you can view detailed information about the cause of the problem by clicking on the [\[Next\]](#) button to access the [Summary](#) panel.

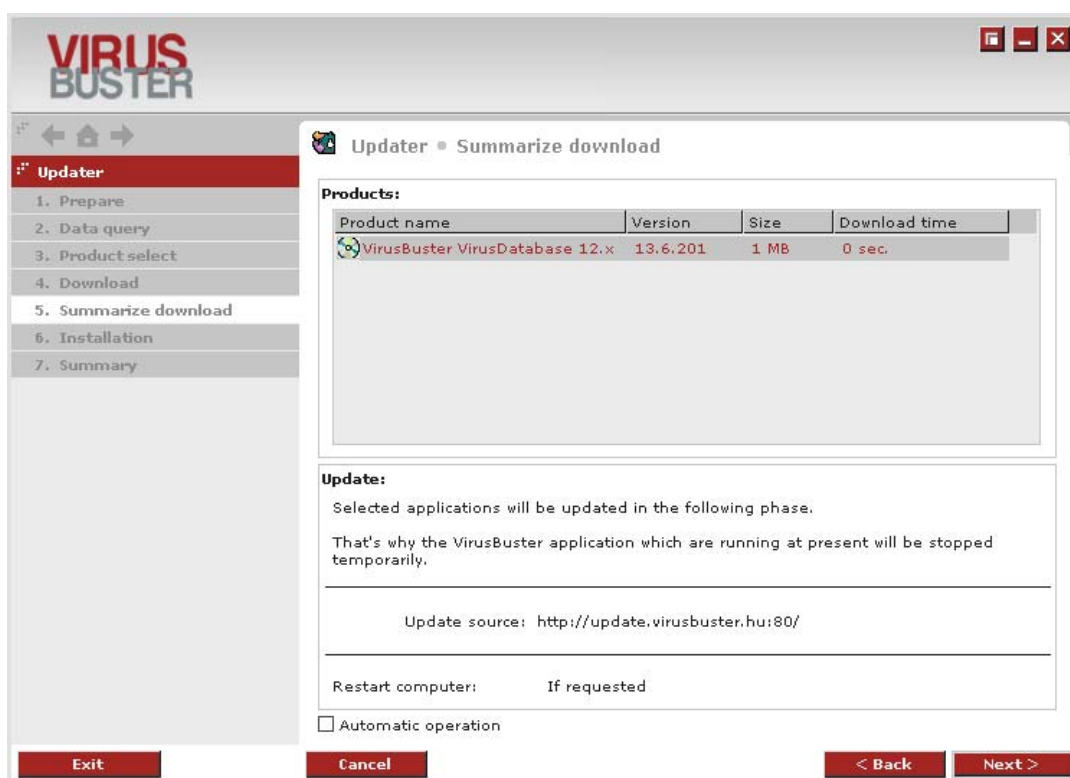
If the download was performed without any problems, you can go to the next panel by clicking on the [\[Next\]](#) button.

Download Summary

In case of a successful file download, the downloaded program components with their sizes and version numbers can be checked in the summary panel.

At the bottom of the window, you are informed that the updates of the selected programs and components are performed during the next step.

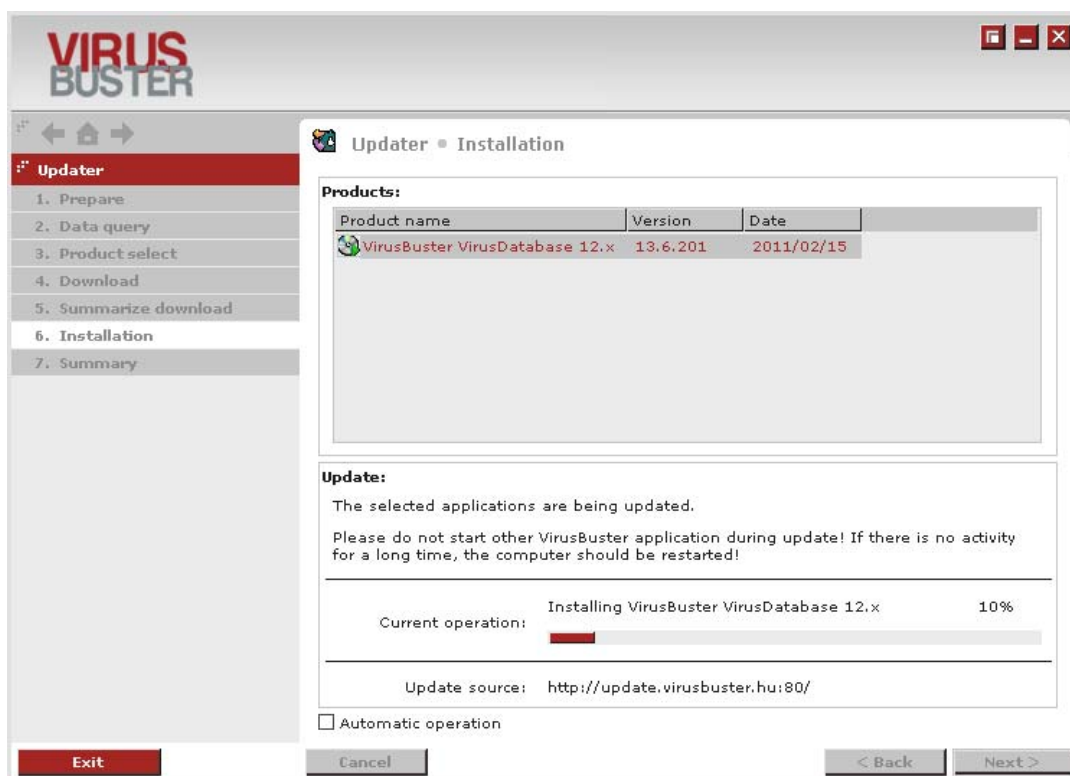
Below the update source, the status of the computer restart is displayed and you can also switch to automatic operation by enabling it.



Update Process – Download Summary

Installation

The selected and downloaded components are installed during this step.



Update Process - Installation

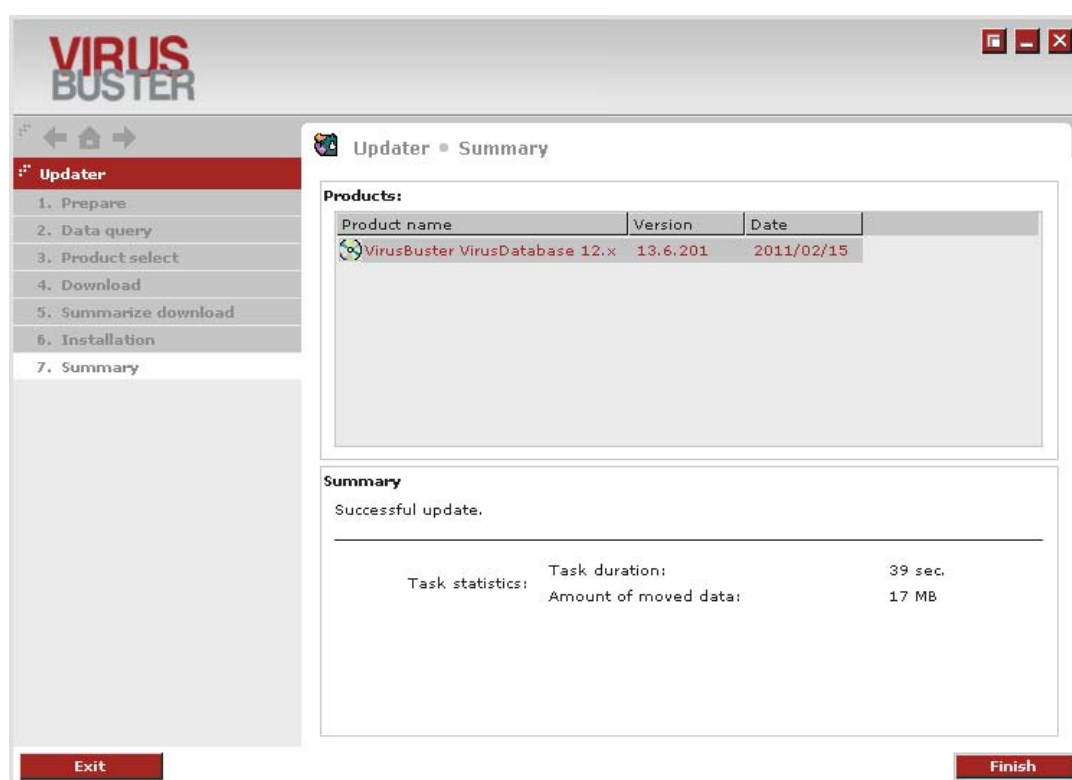
The little CD icon in front of the products indicates the status of the update as described earlier, and the status bar indicates the current status of the update at the bottom of the panel.

When updating, the program stops running applications while the installation is performed and new versions are updated. This can take several minutes.

You can only continue if the update is finished or a problem occurred.

Summary

The last step of the update process is the summary informing you about the successful update or the problems occurred during the update. The process can be ended by clicking on the **Finish** button.



Update Process – Summary, Successful Update

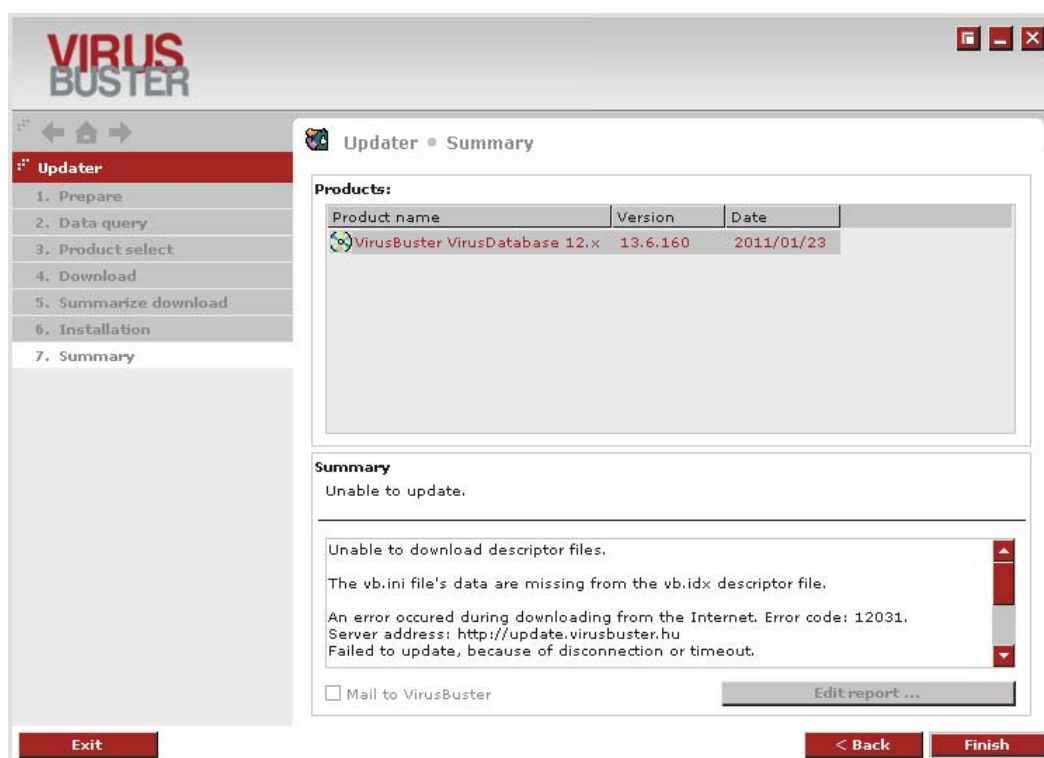
Successful Update

In case of a successful update, the new version numbers of the updated applications and the date of the update are displayed at the top of the window. Statistics are displayed about the time needed for performing the task and the transferred data size at the bottom of the window.

If automatic restart is set, the panel contains a status bar indicating the one-minute-long period after which the computer is restarted. It is possible to terminate the restart or to restart the computer immediately.

Update with Problems

If a problem occurred, you can read detailed information about the problem and its possible resolution at the bottom of the panel.



Update Process – Summary, Update with Problems

By selecting the *Mail to VirusBuster* and clicking on the **Finish** button, you can send a notification about the problem to VirusBuster, it will be analyzed by our staff, and you will be notified about the possible resolution of the problem.

If this option is unavailable (you cannot select it), specify the mailer settings. Correct mailer settings are essential to send messages.

If you want to send an e-mail, its content and settings can be viewed by clicking on the **View problem report...** button. This panel contains the address of the sender and the recipient, the **report.zip** file to be attached to the mail. This file can be viewed by clicking on the **Browse ...** button in this panel. This compressed file contains files needed for finding and analyzing the problem.

Quick Database Update

By clicking on the **Update** button on the main page of the graphical user interface (*Information* menu), you can initiate a "quick" database update (if this function is available). In such a case, the program selects an update source from the active update sources and tries to download and update the database from that source. The different update sources are grouped by their availability and the active one on the highest level is always selected for database download.

Level of the update sources (from the highest to the lowest one):

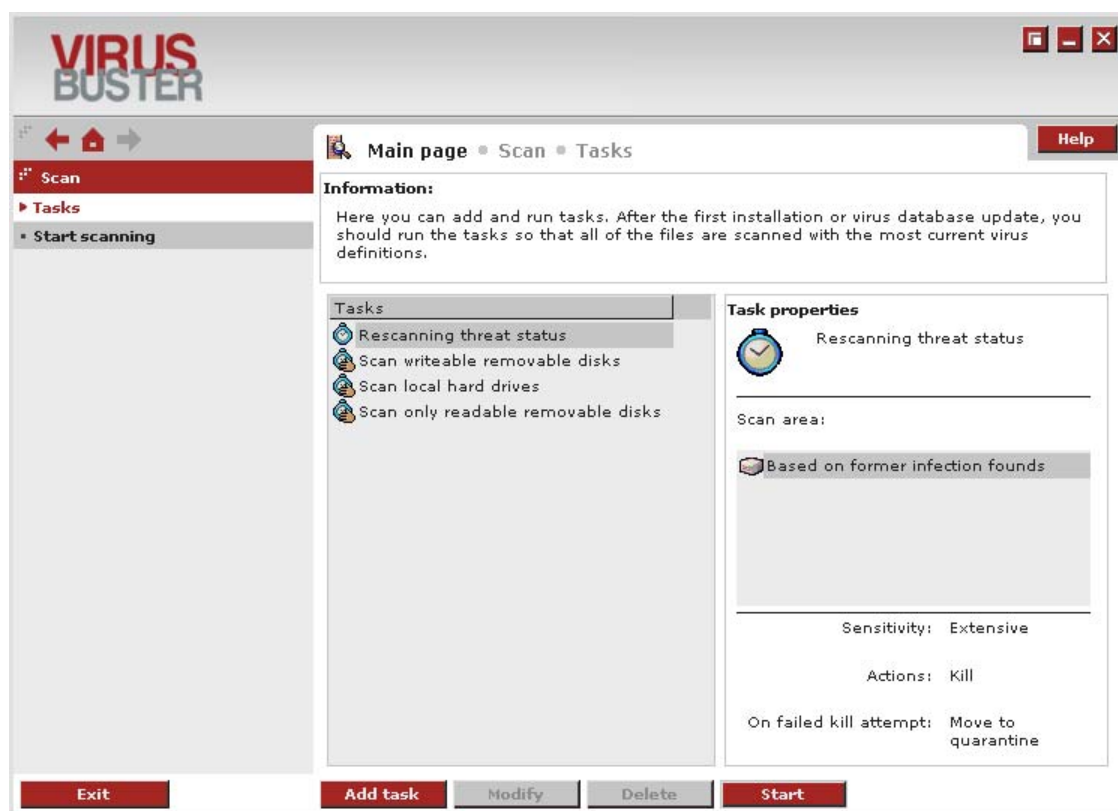
- Path
- NetWare path
- CD
- HTTP
- FTP

Scanner

This component performs all virus scanning tasks and provides manual virus scans. Task-oriented operation allows the user to perform scans according to one of the set tasks in which the scanning method and other options are pre-defined, therefore, scanning is possible at once without having to determine individual settings for the scan. The settings of a scanning task can be modified in the *Tasks* menu, manual scans can be started using the *Start scan* function.

Tasks

Default and user-defined scan tasks can be displayed, started, or modified in the *Tasks* panel.



Scanner - Tasks

The available tasks are displayed in the Tasks window. After installation, only the default tasks are available, but they can be extended with tasks specified by the user.

The main settings of the selected task are displayed on the right side of the panel in the *Tasks* windows. This information cannot be modified here.

The task type is indicated by the icons in front of them, the following icons are used:



The task is triggered by an event (system startup).



The task is started manually by the user.



The task is scheduled: it is started at a set time or periodically.

By clicking on the following buttons, the following options are available:

- **|Add task|**
Creates an individual scan task with the defined scan settings.
- **|Modify|**
Modifies the settings of the selected task.
- **|Delete|**
Deletes the selected task.
- **|Start|**
Starts the selected task.
The description of the window displaying the scanning process can be found in the Virus [Scan Window](#) section.

Creating a New Task

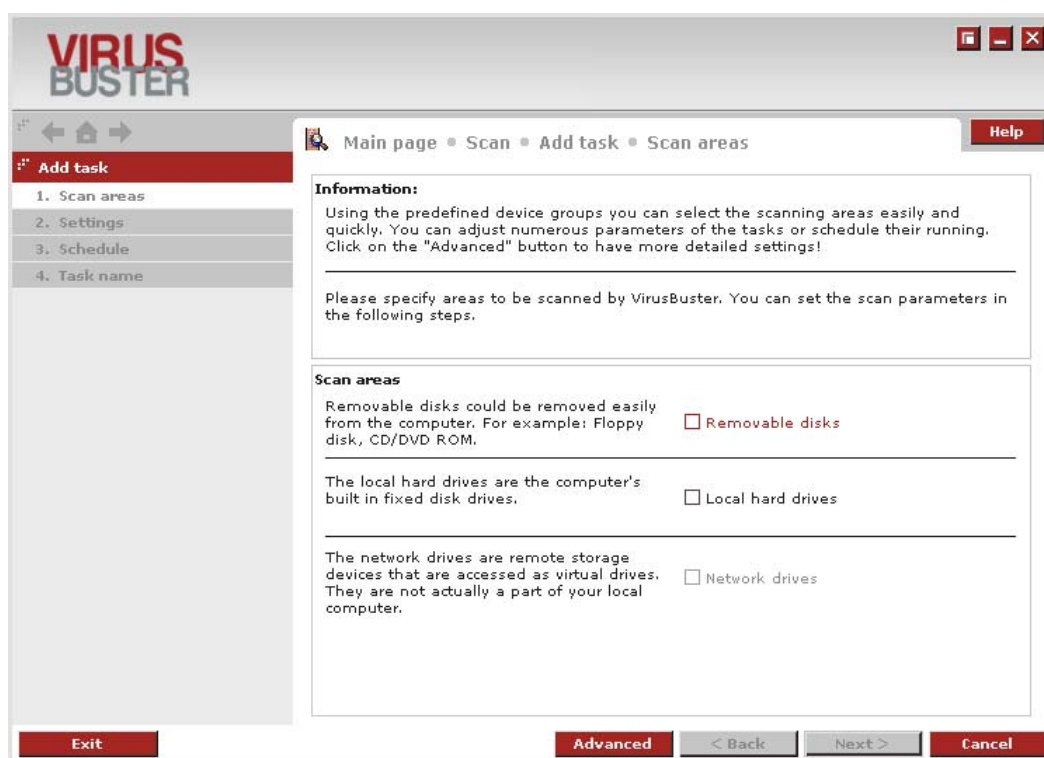
By clicking on the **|Add task|** button, a wizard-style interface appears where settings for the new task can be defined step by step with detailed descriptions. You can go to the next step by clicking on the **|Next|** button. Adding the new task can be stopped by clicking on the **|Cancel|** button. The settings can be easily defined in the simple settings panels or can be adjusted in details by clicking on the **|Advanced|** button.

Scan Areas – Selecting the Drives To Be Scanned

Simple Settings

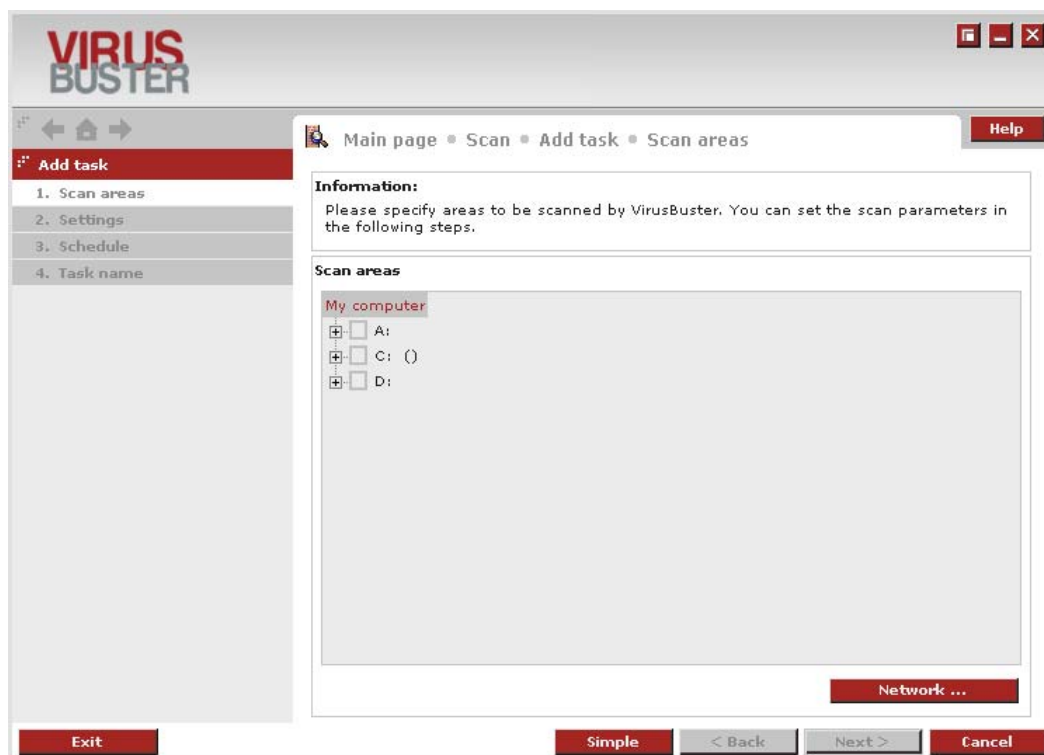
By selecting the needed drive types, you can define the drives to be scanned. The *Next* button is only active if at least one type is selected. The following settings are available:

- *Removable disks*
Removable disks can be removed easily from the computer. For example: floppy disk, CD/DVD ROM.
- *Local hard drives*
The local hard drives are the built-in, fixed disk drives of the computer.
- *Network drives*
The network drives are remote storing drives that can be used through a network. They are not part of the local computer physically.



Scanner – Scan Areas

Advanced Settings



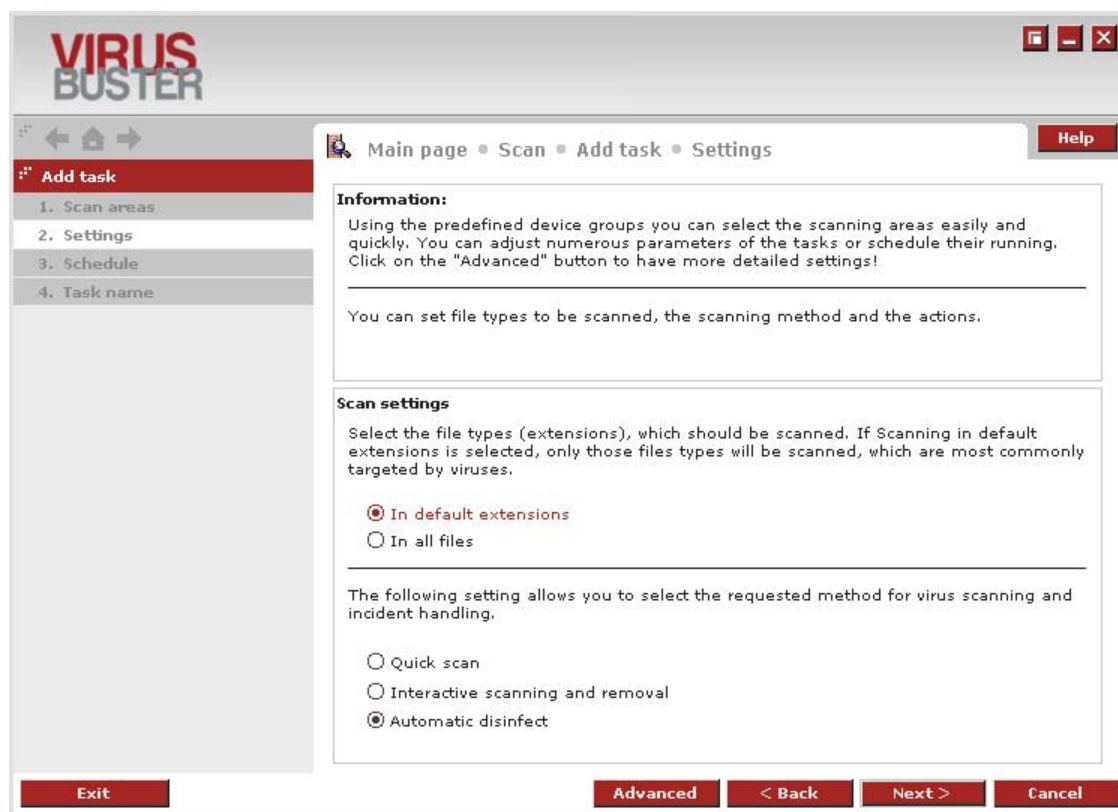
Scanner – Scan Areas, Advanced Interface

The drives or individual directories to be scanned can be set in the *Advanced* panel. The available drives and directories on the computer are displayed in the *Scan areas* window. A plus (+) sign indicates if a directory has sub-directories. The plus (+) sign is changed to a minus (-) sign if the directory is open and its sub-directories are displayed. A directory can be opened by clicking on its name or on the plus (+) sign. If the checkbox in front of the directory is selected, the files in the directory are scanned. The opened or closed status of the directory is very important when selecting checkboxes, because if it is open, its sub-directories are not scanned. If it is closed, all the sub-directories are selected recursively. Directories selected recursively are marked with an asterisk (*).

If your computer is a member of a network, you can add network shares to scan by clicking on the [\[Network...\]](#) button. Select the desired path in the appeared window, then click on the [\[Add\]](#) button. The selected path is added to the existing ones.

Settings – Specifying the Scanning Method

Simple Settings



Scanner - Settings

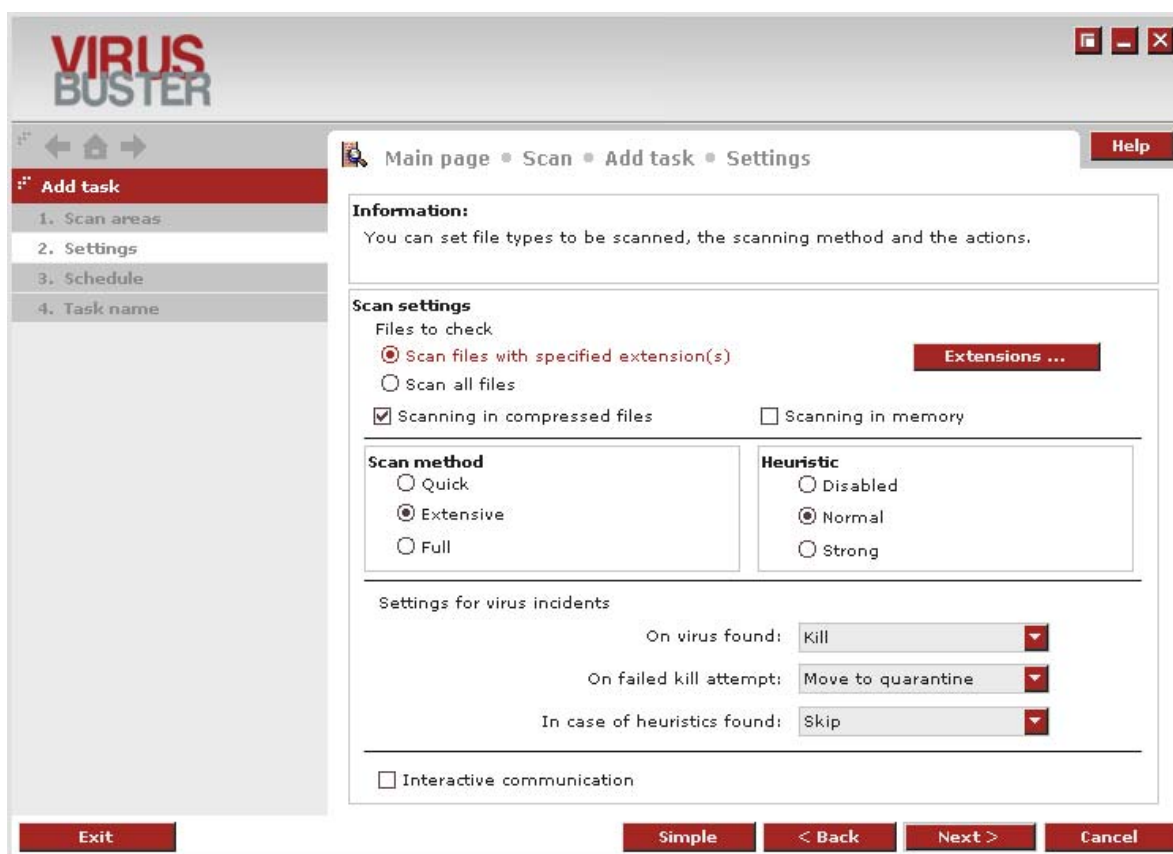
When selecting scanning *In default extensions*, the scanner only scans file types set by default. These are described in the [Extension settings](#) section.

All files can be scanned by selecting the *In all files* option. In this case, all files are scanned regardless of their extensions.

In the next panel, the method of scanning and disinfection and other settings of the scanner can be adjusted by choosing from the pre-defined scanning methods. These methods are a set of settings that can be displayed by using the *Advanced* panel.

- **Quick scan**
Uses the *Fast* scanning method and no heuristics; all viruses are *Skipped*. The process is automatic, no user interaction is needed. The set actions are performed on infected files.
- **Interactive scanning and removal**
Uses the *Extensive* scanning method and *Medium* heuristics, killable viruses are *Killed*, non-killable viruses are *Quarantined*. User interaction is needed when a virus is detected, the set actions must be confirmed.
- **Automatic disinfection**
Uses the *Full* scanning method, *Medium* heuristics; killable viruses are *Killed*, non-killable viruses are *Quarantined*. The process is automatic, no user interaction is needed, the set actions are performed on infected files.

Advanced Settings



Scanner – Settings, Advanced Panel

If the *Scan all files* option is enabled, all file types (extensions) are scanned. If the *Scan files with specified extension(s)* option is enabled, only files with extensions specified by the user are scanned. The default values can be modified by clicking on the [Extensions ...](#) button.

Extension Settings

The following file types are scanned by default:

- Jet engine files
- Table files
- Compressed files
- Document files
- PowerPoint files
- Program files
- Script files

Individual files can be set to be scanned or not to be scanned. For this, the *Files to be scanned* or the *Files not to be scanned* options must be enabled, and the needed file types must be specified in the given fields (for example: *.rx). Special characters can be used (for example, *.qwe, *.?ab).

The program scans all compressions if the *Scan compressions* option is enabled. If the *Scan memory* option is enabled, it starts scanning by checking the contents of the memory, then the specified scan areas.

The scanning method can be set on the following levels:

- [Quick/Extensive/Full](#)

Heuristics can be set on the following levels:

- [Disabled/Normal/Strong](#)

You can specify the actions to be performed (automatic mode) or to 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 (for example, the virus cannot be killed), the secondary action set in the *In case of unsuccessful disinfection* option is 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 for the primary action. You can set an action for heuristic detections.

The available actions when a virus is found are the following:

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

Available secondary actions and actions in case of a heuristic detection are the following:

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

If *Interactive communication* is enabled, the software prompts the user for interaction in case of every incident and the set actions are displayed by default. If this option is not enabled, the set actions are automatically performed on the infected files.

Scheduling Panel – Setting the Time for Starting the Scan

The scheduling of a scanning task – the beginning of a virus scan – can be easily executed in this panel. You can select the needed frequency or a specific date or event from the various scheduling options. The settings of this panel are the same as described in the [Scheduling](#) subsection of the *Updater* section.

Task Name

To specify a name for the task, type the name in the appropriate text field. A name must be specified, otherwise, the task cannot be added.

After pressing the **[Finish]** button, the scanning task with the specified settings is created and you can refer to it with its name in the list window of the *Tasks* panel. It is not possible to create two tasks with the same name, and the \ (backslash) character cannot be used in the task name.

Modifying a Scanning Task

Modification consists of the same steps and settings to be used during adding a task.

- *Modification of the scan area*
You can modify the target areas of the selected scanning task (the [Scan areas](#) panel).
- *Settings – specifying the scanning method*
You can modify the settings of the scanning task (the [Settings – specifying the scanning method](#) panel).
- *Scheduling*
It is possible to modify the scheduling settings (the [Scheduling](#) panel).
- *Task name*
The task name cannot be modified, because this is the only settings that can identify a task. You can return the *Tasks* panel by clicking on the **[Finish]** button.

Starting a Scan

If you do not want to add a task for scanning, but want to run a simple virus scan, you can specify the needed settings in the *Start scan* menu. After having selected the menu item, it is important to specify scan areas before starting the scan. After this, scanning can be started immediately by clicking on the **[Scan button]** at the bottom of the window (in this case, parameters not specified are handled with their default value). The following settings are available for the configuration of the manual scan:

- *Scan areas*
First the drives must be specified to be scanned for viruses. The function of the panel and settings are the same as described in the section about adding a new task in the [Scan areas](#) panel.
- *Settings*
You can set the file types to be scanned and you can specify the actions to be performed when a virus is found. The panel is the same as described in the section about adding a new task under [Settings](#).
- *Start scan*
You can check major scan settings on this panel and start scanning by clicking on the **[Start]** button. The description of the scan window indicating the status of the scan can be found in the [Scan window](#) section.

Quick scan

The scanning of files and folders can be started not only from the user interface and the system tray, but from anywhere in the windows system with the help of local menus. In *My Computer*, you can scan a whole drive, or in *Explorer*, you can scan a whole directory or just one file.

By right-clicking on the needed item (drive, folder, or file), a local menu appears on which the *Scan with VirusBuster* option must be selected to start scanning the selected item(s). The description of the scan window indicating the status of the scan can be found in the [Scan Window](#) section.

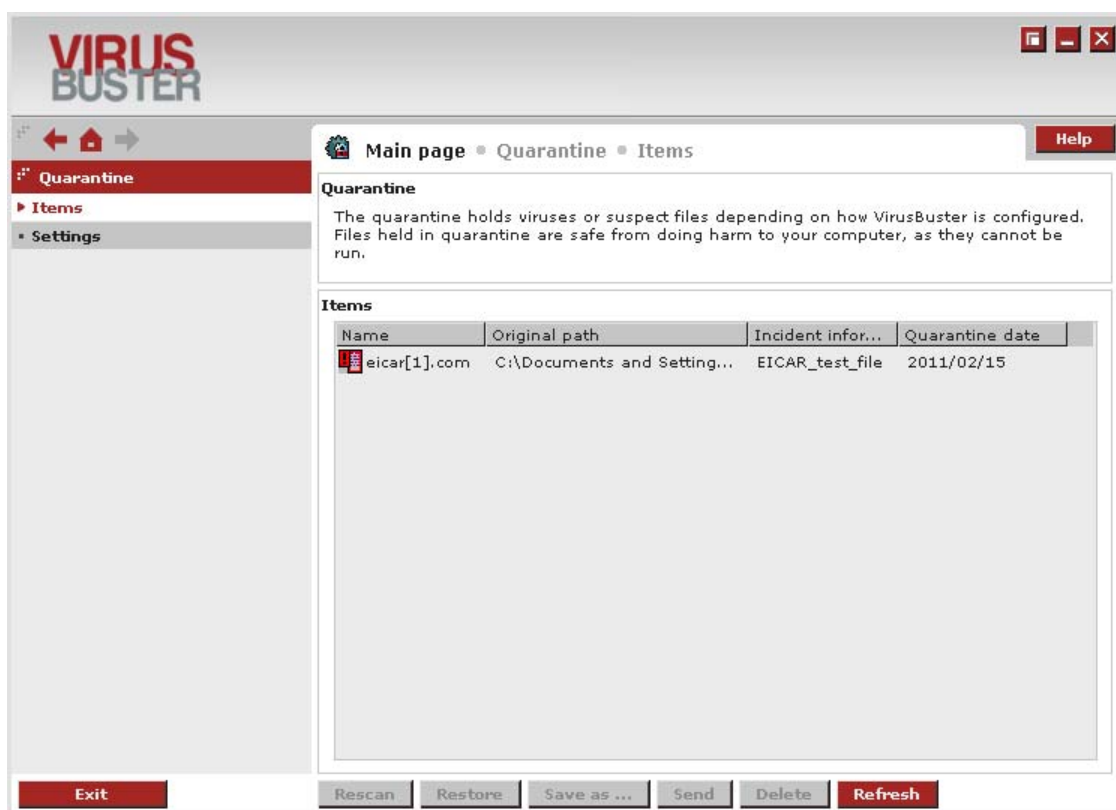
Quarantine Module

This component stores and processes infected files that cannot be disinfected according to the settings. Quarantine settings can be modified in the following panels:

- *Items*
- *Settings*

Items

The *Entries* list provides information about all files stored in the quarantine.



Quarantine - Entries

The following information is displayed in the quarantine window:

- *Name*
The original name of the file
- *Original path*
The original path of the file before it was moved to the quarantine
- *Virus name*
The name of the virus that infected the file
- *Quarantine Date*
The date when the file was moved to the quarantine

Several actions can be performed on the quarantined files that can be activated by clicking on the buttons at the bottom of the panel.

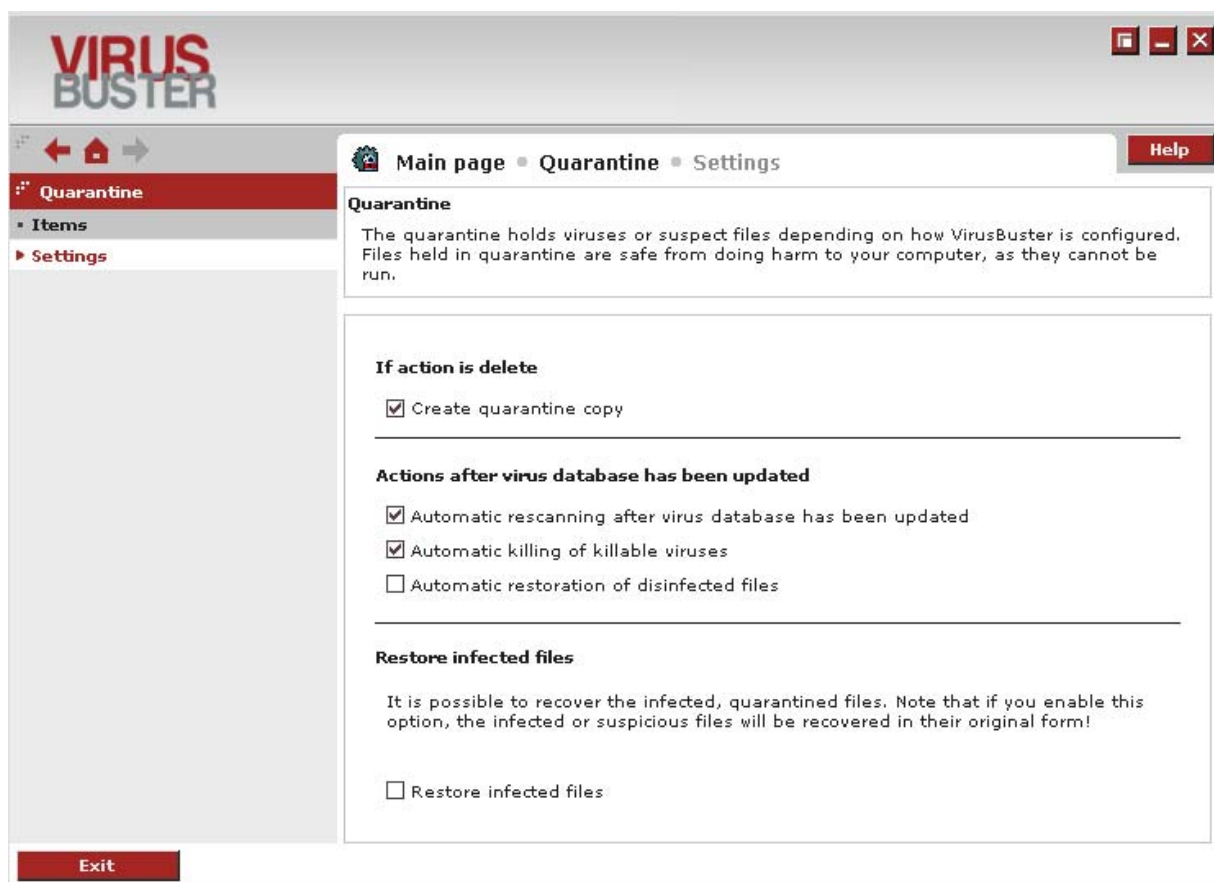
- [|Rescan|](#)

The software performs an additional scan on the selected file(s) and removes the virus, if it is possible.

- **|Restore|**
The software restores the file to its original location and status if the *Restore infected files* option is enabled in the *Settings* panel of the component, but only if the file is infected, the original path exists, and there is no file on the path with the same name. If a file with the same name can be found on the original path or the original path does not exist, the quarantine restores the file to the temporary directory.
- **|Save as...|**
It saves the file with the specified name. The software encodes the file, so that the virus cannot be activated and the file can be sent for virus analysis.
- **|Send|**
It sends the selected file to VirusBuster for analysis. This option is functioning only if SMTP settings are proper in the Mailer component. You can send the message in the [Mailer component](#) after clicking on the button.
- **|Delete|**
The program permanently deletes the selected file(s).
- **|Refresh|**
It refreshes the list of items in the quarantine.

Settings

Other quarantine settings can be found on this panel.



Quarantine - Settings

In *If action is delete* option, If *Create quarantine copy* is allowed then the infected file will be backed up in case it has to be deleted during the disinfection method.

- *Automatic rescan after virus database has been updated*
If the option is enabled, the software rescans every file in the quarantine after every virus database update and removes all viruses, if it is possible.
- *Automatic killing of killable viruses*
If this option is enabled, viruses that can be disinfected after the virus database update are automatically removed from the files stored in the quarantine. This option can only be enabled if the *Automatic rescan after virus database updates* option is enabled.
- *Automatic restoration of disinfected files*
If the option is enabled, the software restores all files that were automatically disinfected after a virus database update. This option can only be enabled if the *Automatic rescan after virus database updates* option is enabled.

By enabling the *Restore infected files* option, the restore function of the quarantine can be used in case of infected files and the **Restore** button becomes active in the *Entries* panel.

Important!

It is not needed to specify a path for the quarantine directory, the software uses the **Quarantine** subdirectory in the installation directory.

Log Component

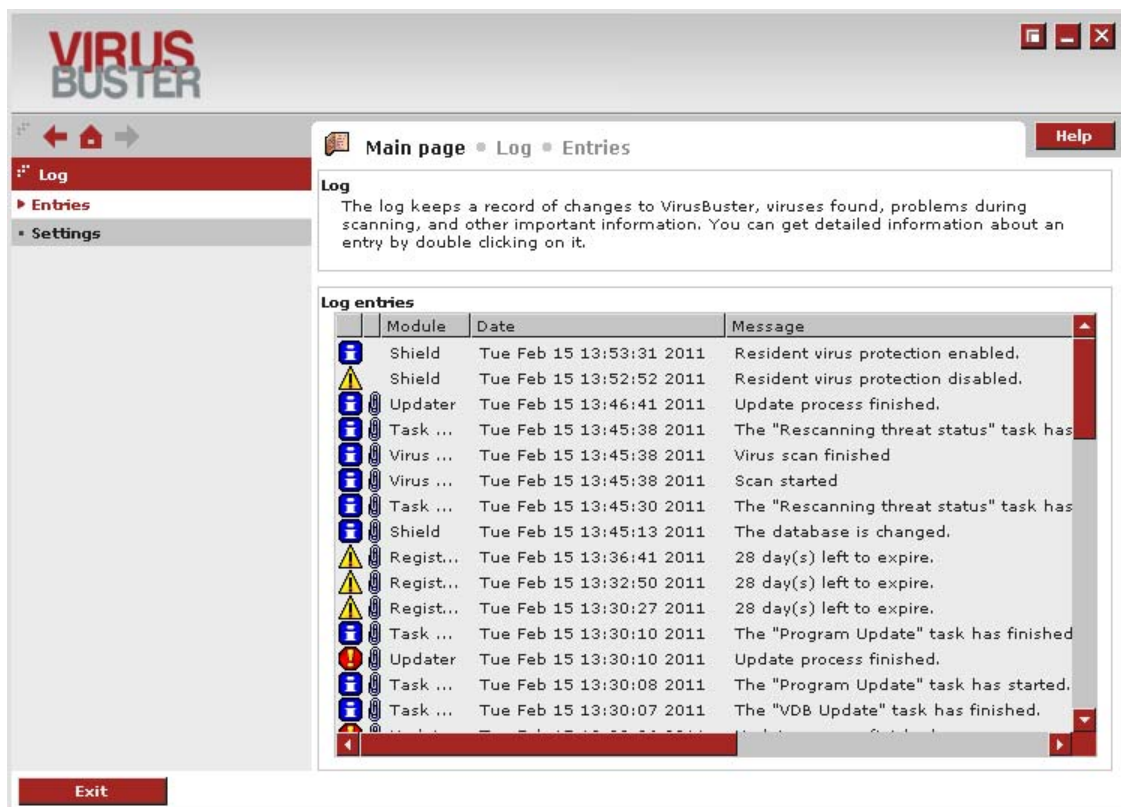
This component stores messages generated by different parts (modules) of the software and forwards them to the user if needed.

To view the log entries and to change the settings, the following menu items must be used:

- *Entries*
- *Settings*

Entries

With the help of log messages, you can check the operation of the antivirus protection or reveal the cause of possible errors and view other messages created by the software.



Log - Entries

In the *Log entries* panel, the following information is displayed:

- *Module*
The name of the module that generated the message
- *Date*
The date when the message was generated
- *Machine*
The name of the computer that created the message
- *User*
The name of the user who started the application that generated the message

The software refreshes the list automatically if a new message is generated or a message is deleted. Refreshing does not modify the selected entry if it is not the one that has just been deleted from the list.

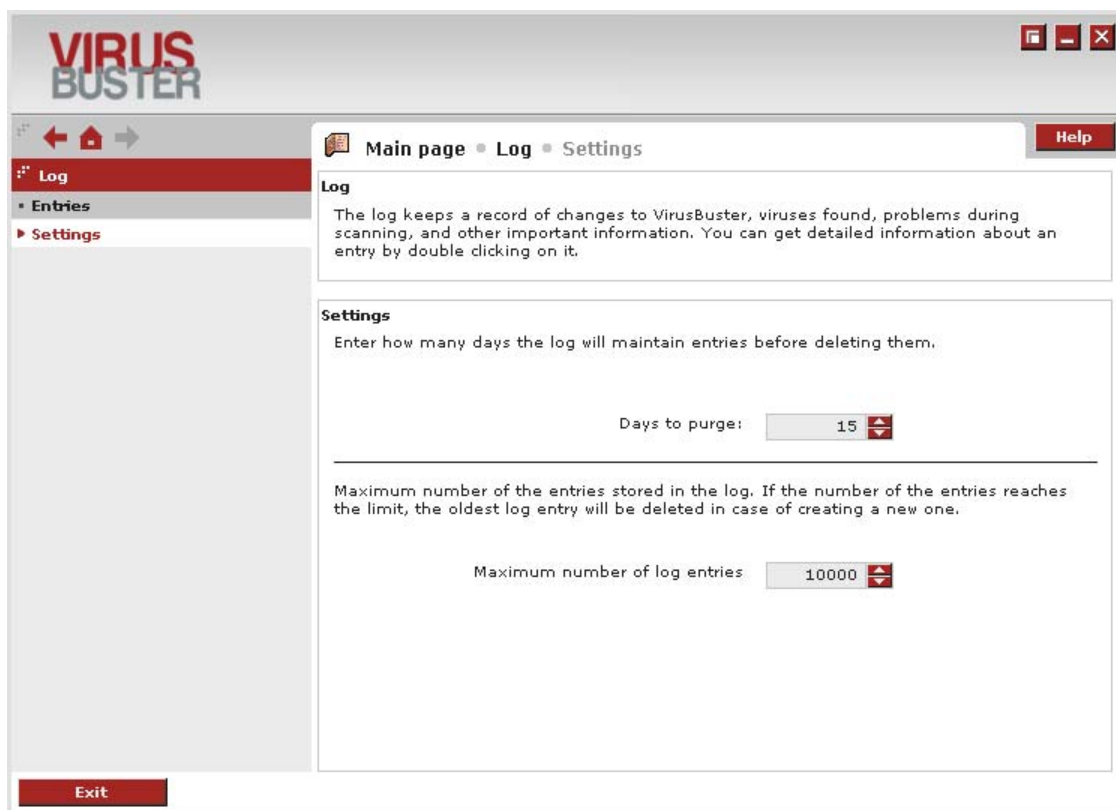
By right-clicking on the list panel, a pop-up menu appears where it is possible to switch the various fields of messages on or off or to perform the following actions:

- *Save log...*
It saves the content of the message to the desired file.
- *Send...*
It sends a message and a log file to VirusBuster Support. After selecting it, you can send the message in the window of the *Mailer component* (if installed).
- *Reload*
It refreshes the list.
- *Delete*
It deletes ALL the messages from the list.

By double-clicking on any entry, the message details appear and the whole content of the message can be checked.

Settings

The display and handling settings of the log entries can be modified in this panel.



Log - Settings

The size and time limit can be set for the log entries:

- *Days to purge*
Entries older than the set value (days) are automatically deleted from the database.
- *Maximum number of log entries*
If the number of log entries reaches the set value, older entries are deleted from the end of the log database.

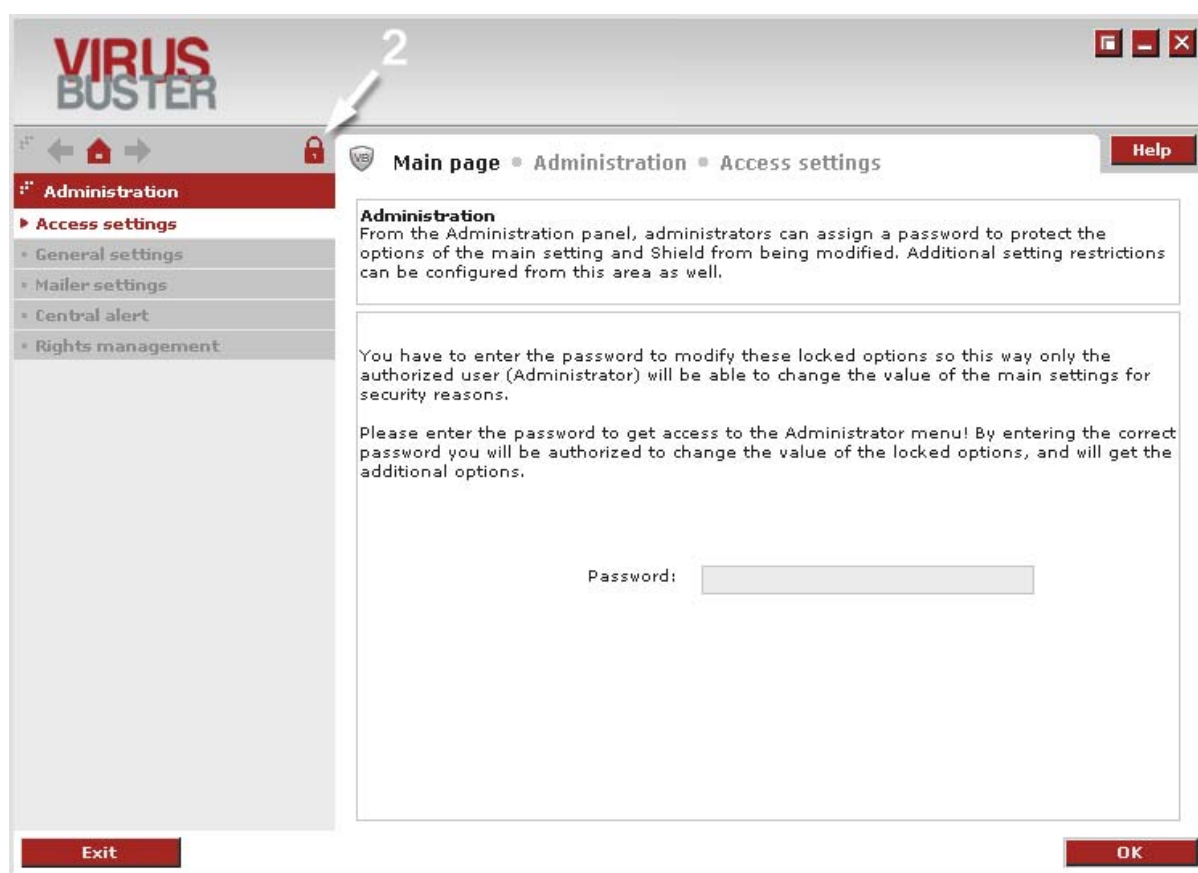
The modified values are applied every half hour by a transparent and automatic maintenance task.

Administration

In the Administration panel, Administrators are allowed to lock the modification level of the main settings and are authorized to set some additional options to customize the program operation. Administrators can set a password to limit the access to the main settings of the application to ensure that only the authorized users can modify the values of the important options and the Administrator settings.

There is a lock symbol in the *Navigation panel* to display the modification status of the settings. If the lock is open (1), users can modify all the settings of the application; if it is locked (2), the modification is not possible (arrows show the two statuses of the symbol in the following figures).

After clicking on the Administration menu, enter your password – if it was specified before – to access the administrator panel and to be able to modify the value of the locked options. Enter your password into the *Password* field, then click on the **[OK]** button to get the administration settings (see the description of the [Administrator mode](#)).



Enter Password

If there is no password specified, all the settings can be modified by the users. Click on the **[Set password]** button to set your Administrator password on the *Access settings* panel.

Depending on whether there is a password set for the product or the user is logged in or not, the product can be used in two operation modes:

- Administrator mode: the user logged into the product on the *Administration* panel (it is shown by a little lock symbol being unlocked on the menu bar).
- Normal mode: there is no need to enter a password to get the *Administration* panel or the user is

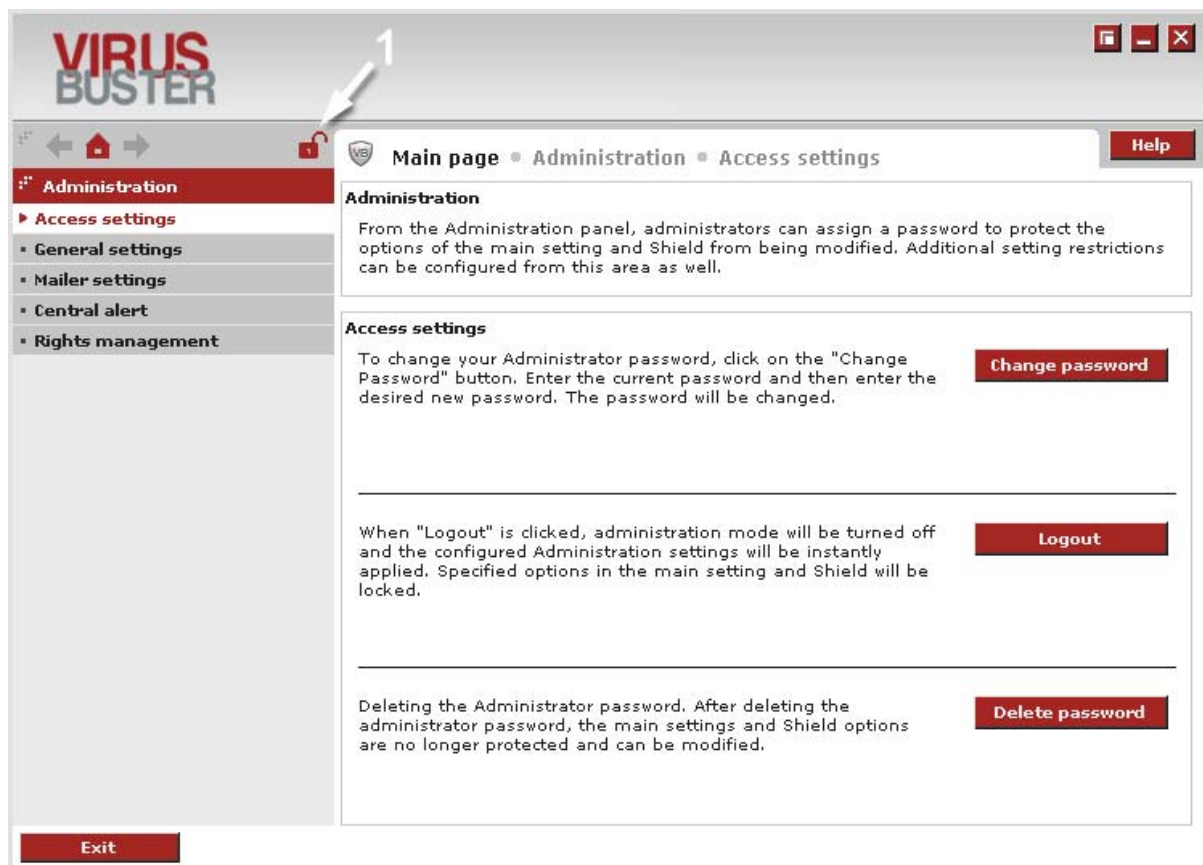
not logged in yet with the password set for the product (in such a case there is no lock symbol displayed or (for the second case) it is shown as locked).

Access Settings

If a password is not set for the product, only the [\[Set password\]](#) button is available in this panel to set the password. After setting the password, modification of some important options are not allowed when using the product without entering the specified password (see the description of the [Administrator mode](#)), so that unauthorized users cannot change important settings of the product.

If you set your administrator password, the following options are available in this panel:

- *Change password*
- *Logout*
- *Delete password*



[Access Settings](#)

General Settings

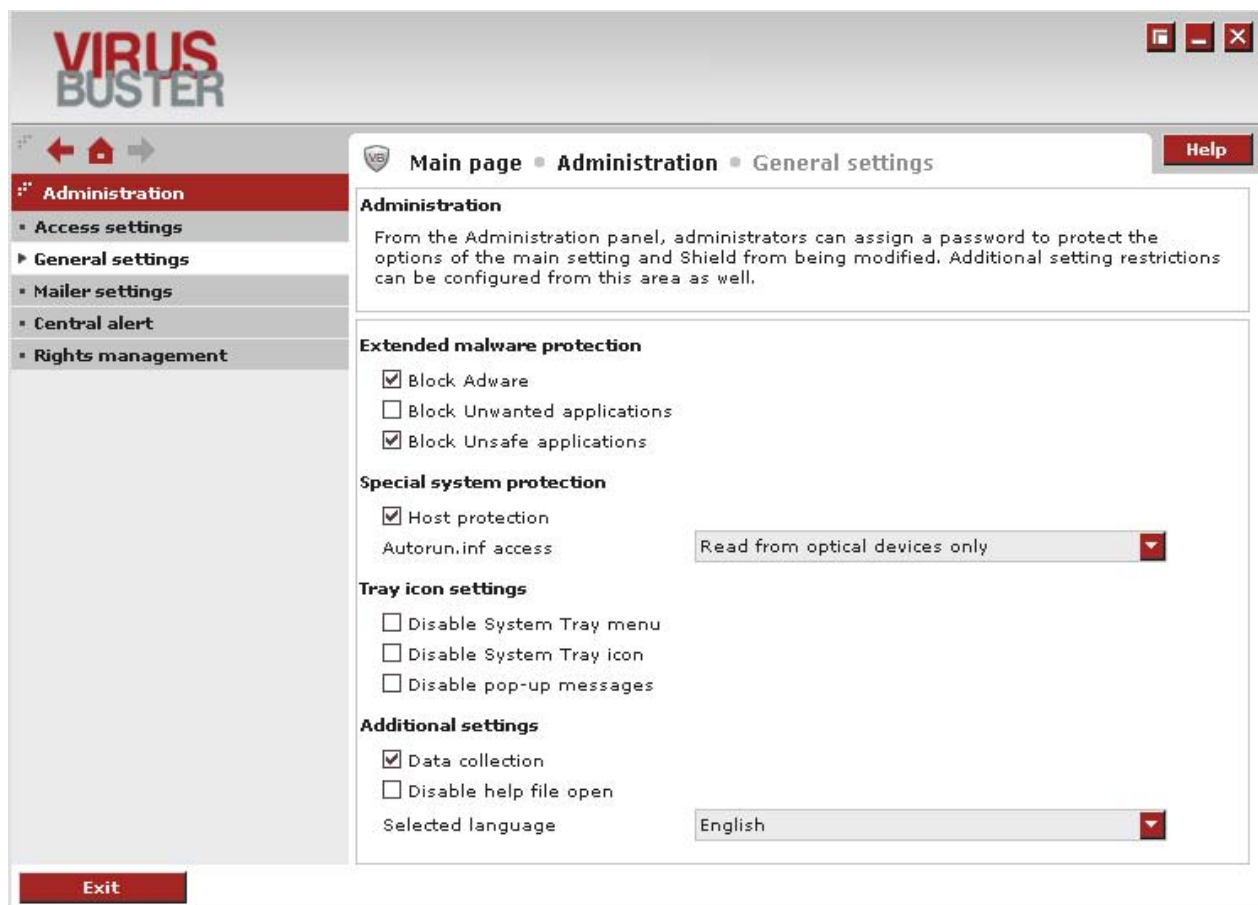
You can control the general operation of the product by enable/disable various functions.

Below *Extended malware protection*, you can adjust grayware detections in three categories. Grayware is a kind of 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. So 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.

Description of categories:

- *Block adware: detection of adware applications*
- *Block unwanted applications: this category includes cracks, keygens and other applications which are not real malware (based on their operation), but they can be undesirably for most users*
- *Block unsafe applications: includes dangerous applications (based on their operation) but, at the same time, they are also commercial products (keyloggers or password recovery products)*



General Settings

Special system protection

- *Hosts protection*
With the help of this option, the protection of the hosts file of a machine (that is in the System32\drivers\etc folder inside the Windows system folder) can be specified. It is enabled by default and works in case active resident protection.
- *Autorun.inf access*
Using this option, you can protect autorun.inf files (running software automatically) on plug-in

(e.g. pen-) drives and CDs/DVDs from unauthorized access.

The level of protection can be set by selecting one of the following options from the corresponding dropdown list:

- *No restriction*
The autorun.inf file is available with no restrictions, it is not protected.
- *Read only*
The autorun.inf file can be read only; it cannot be modified.
- *Read from optical devices only*
The autorun.inf file can be read from CDs or DVDs only; however, it cannot be modified. This is the default setting.
- *Disabled*
The autorun.inf file is read- and write-protected.

Autorun.inf protection is working in case of resident protection enabled.

The *Tray icon settings* options allow you to customize the operation of the System Tray menu and the pop-up windows.

- *Disable System Tray menu*
If you check this option, the local menu of the System Tray icon is not displayed even when right-clicking on the icon.
- *Disable System Tray icon*
When selecting this option, the System Tray icon is not shown on the Tray.
- *Disable Pop-up messages*
The application does not warn the user with the help of pop-up windows (displayed right above the System Tray) about problems and events occurred during operation. This setting has no effect on displaying other information windows (virus alerts, warnings) of the product

Options in *Additional settings* group:

- *Data collection*
With the help of this option, the software can send reports about virus incidents to VirusBuster to further improve antivirus protection. Information only about the installed product and the detected malware incidents, but no personal data are sent.
- *Disable help file open*
When set, Help is not available on the user interface.
- *Selected language*
It can be used to change the language of the user interface by selecting one from a dropdown list. In order to make the change effective, the software must be restarted. Changing the language of the VirusBuster icon on the Tray to the new setting requires reboot.

Mailer Settings

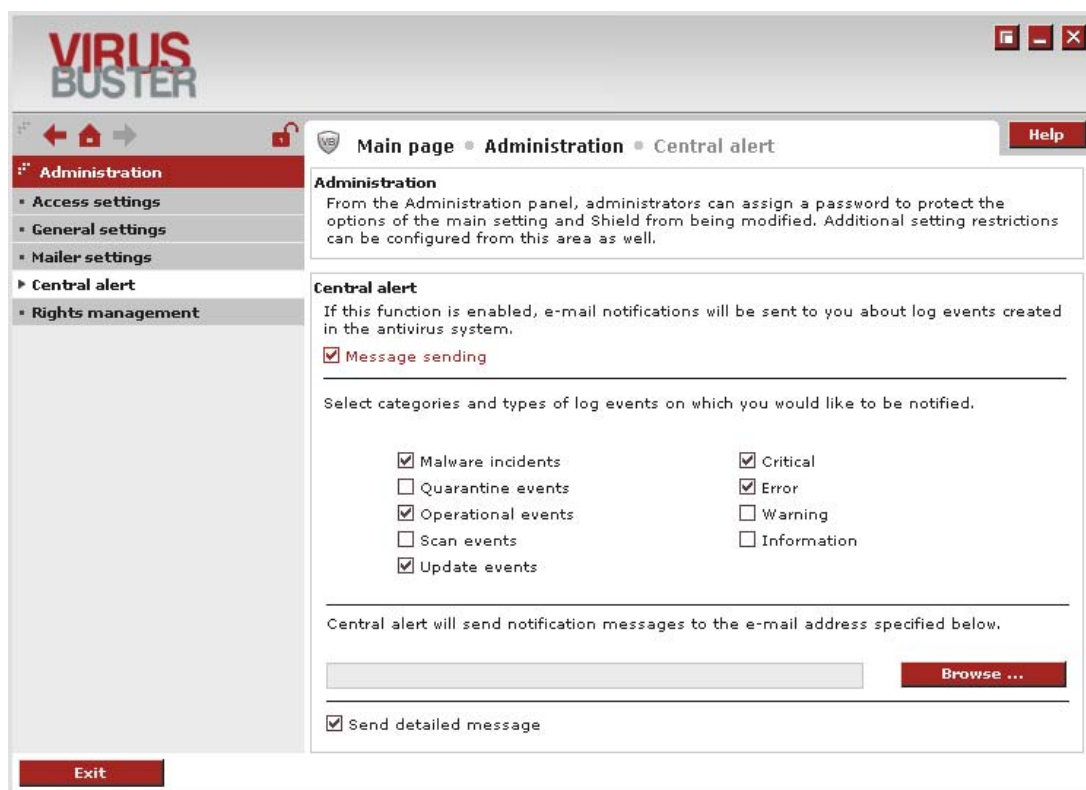
This menu is only available if the *Mailer* component is installed. Here you can set some mail sending parameters needed for VirusBuster to be able to deliver messages. See the [Mailer](#) section for more information.

Central alert

Central Alert is a useful function for administrators who would like to be notified about various events and actions that occurred on the client's computer. The only thing administrators must do is to specify the types of events they are notified about and set the e-mail address(es).

This function is disabled by default. It can be enabled by selecting the checkbox in front of the Sending

message option.



Central Alert

Select the event categories and types you want to be notified about by the central alert module under the *Message sending* option. You can specify the message group that you would like to receive notification about according to the event categories and types if they occur in your system.

The event categories can be one of the following:

- *Malware incidents*
It contains messages about malware incidents (every malware detected, suspicious files).
- *Quarantine events*
It contains messages about the quarantine (for example, restoring, rechecking, saving the quarantine, and so on).
- *Operational events*
It contains messages created during the operation of the antivirus software (for example, enabling/disabling modules, modifying settings, changing the status of the antivirus protection, and so on).
- *Scan events*
It contains messages about virus scanning (for example, corrupt file, starting/stopping scanning, attachment type not supported, and so on).
- *Update events*
It contains messages about antivirus software updates (for example, outdated virus database, update does not start/started/stopped, update with errors, and so on).

The event types can be one of the following:

- *Critical*
An event that requires immediate interference (for example, virus database error, scan engine problem, malware detection, and so on)
- *Error*
An event that requires interference (for example, problems with update and installation, lack of license key, and so on)
- *Warning*
An event with lower importance that may cause problems (for example, disabling resident protection, suspicious file detected, file access denied, and so on)
- *Information*
Event not causing any problem (for example, tasks/installation executed successfully)

At the bottom of the panel, enter a valid e-mail address where you want VirusBuster to forward the messages. You can enter several e-mail addresses where you would like to send the messages of the *Central Alert*. Separate the e-mail addresses by commas or semicolons. Use the **Browse ...** button to select the address from the address book.

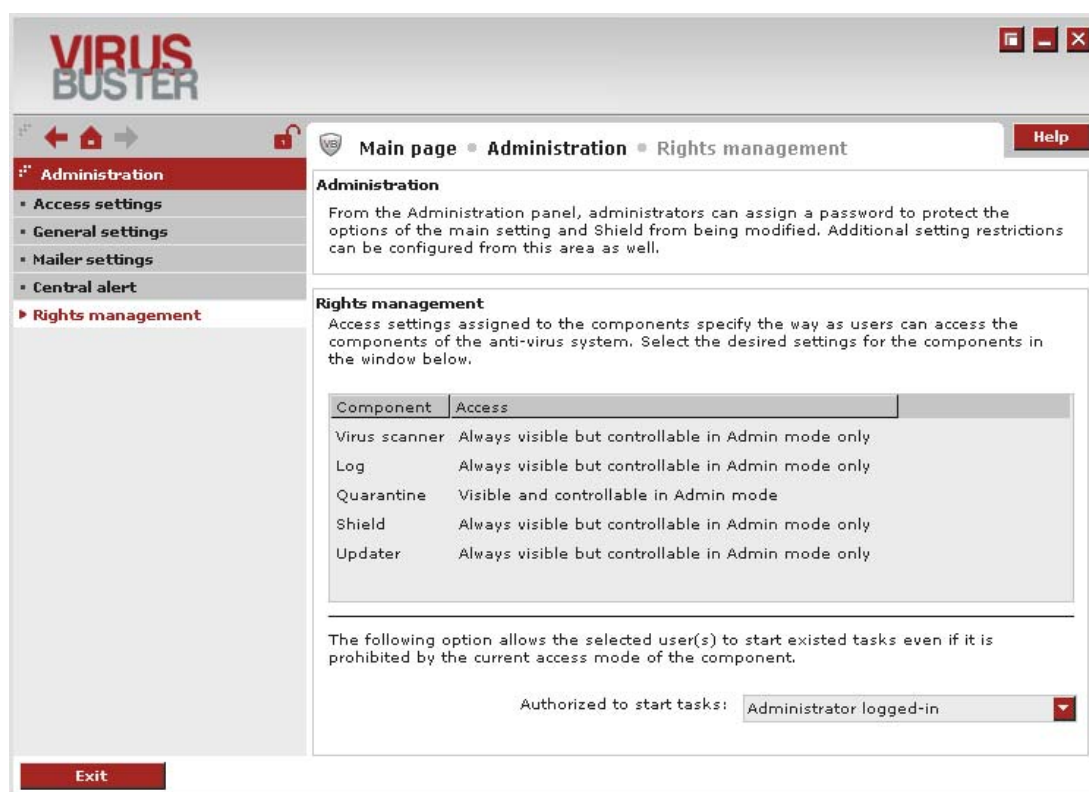
Checking the *Send detailed message* checkbox, the program sends the messages in more detailed format if extra information is available.

Rights Management

Rights management provides comprehensive options to specify the access and control rights for each installed module. Accessibility depends on whether the product is used by an administrator (*Admin mode*) or a normal user (*Normal mode*).

Important!

Admin mode of the antivirus software is not the same as the Windows user having Administrator rights in the operating system. *Admin mode* means that a user has high-level permissions to control the module settings in the antivirus product.



Rights Management

It is possible to restrict some operations (for example, running tasks) or locking the module settings against modification.

There is a window in the middle of the panel with two columns. The first one contains the installed components (*Component*), the second one contains the access settings that belong to the modules (*Access*). The required setting can be selected from a drop-down list.

Access settings that are available to assign to the modules:

- *Hidden*
The module settings are available neither in *Admin mode* nor in *Normal mode* while this value is assigned.
- *Visible in Admin mode but not controllable*
The module settings are visible in *Admin mode* only, but changing the settings is not possible even in *Admin mode*.
- *Visible and controllable in Admin mode*
The module settings are visible and can be changed in *Admin mode* only.
- *Always visible but not controllable*
The module settings are visible in both *Admin* and *Normal modes*, but they cannot be changed.
- *Always visible but controllable in Admin mode only*
The module settings are visible in both *Admin* and *Normal modes*, but they are only controllable in *Admin mode*.
- *No restriction*

Important!

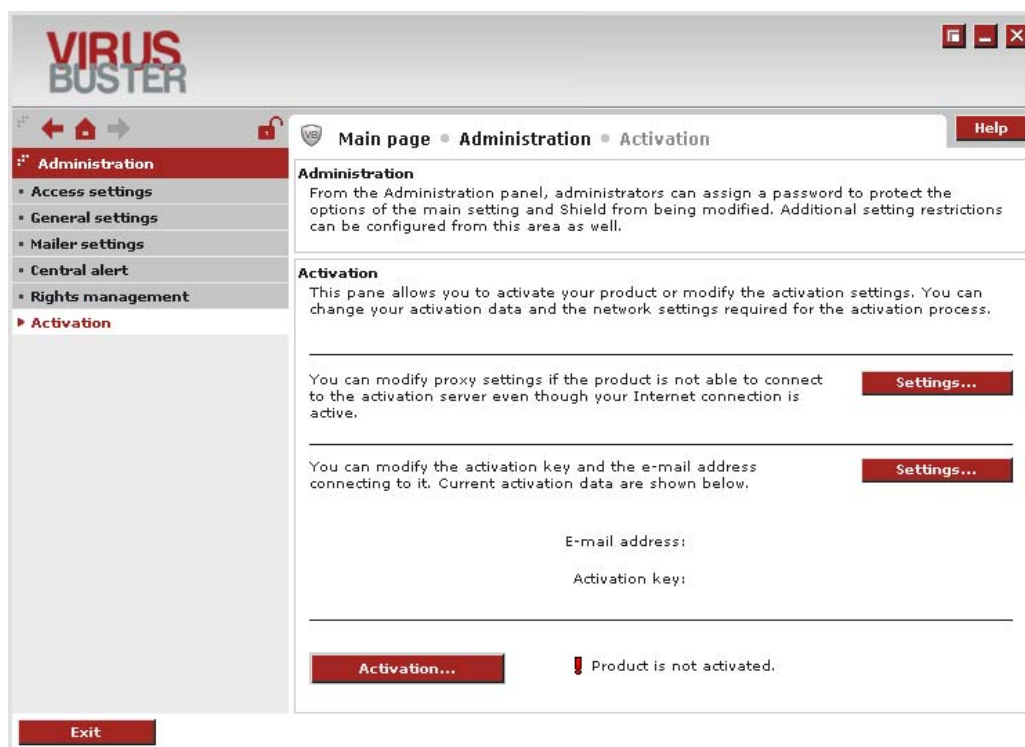
If there is no password set for the product, only the *Hidden* value has an effect. It is pointless to select any of the other options, because nothing happens (as they can only set with other user right levels).

If the access of the *Scan* or *Update* modules is restricted, the current tasks of the modules are not accessible and they cannot be started manually (the restriction does not affect the scheduled tasks, of course). You can select a value from the list of the *Authorized to start tasks* settings and users belonging to the selected category can start tasks manually despite of the restriction.

- *Everybody*
Every user can start tasks manually in the product.
- *Administrator logged-in*
Users with *Admin mode* login can start tasks manually (if starting the task is disabled, users with *Normal mode* login cannot do it).
- *Nobody*
Nobody can start tasks manually (if starting the task is disabled, users cannot do it).

Activation

The *Activation* menu is displayed only if the product is registered using the [activation process](#). In this case, you can check your activation data, reactivate your product, change your activation data and network settings in case of a communication problem on this page.



Activation Settings

You can start the activation process by clicking on the **|Activate...|** button at the bottom of the page. In case of an already activated product, this is only needed if your activation data changed (in most cases the e-mail address), or the registration of the product expired and you want to reactivate it manually. The current activation status is displayed next to the button.

To modify your activation data, specify a new e-mail address and/or the new activation key and start the activation process with the **|Activate...|** button. In case of a successful activation, the modified data is saved and the product is registered with the supplied activation code.

In case of a failed activation, if there is a communication problem, it can be solved by modifying the proxy settings. The following options are available:

- *Internet connection without Proxy*
The program does not use proxy.
- *Using system settings for Internet connection*
The program uses the settings of the operating system.
- *Manual Proxy settings*
The user can set the proxy settings manually.

| Important!
The modification of default proxy settings is only advised for advanced users.

Sending mails

It is possible to send a mail directly to VirusBuster from the program if you have a question or request.

The Mailer component can be accessed:

- From the system tray by right-clicking on the VirusBuster icon and selecting the *Support/Contact us* option)
- From the [Log](#) component
- From the [Quarantine](#) component

VIRUS BUSTER

Information
This function helps you to contact the VirusBuster Support, collects the required information to be sent and allows you to enter your comments and experiences.

Sender:
Name:
E-mail address:

Mail information
To: support@virusbuster.hu
Attached: C:\Program Files\VirusBuster\Personal\Temp\vb13.tmp.zip

Mail content
Registration data:
[Redacted text]

Comment
In this field please enter your questions, the description of any errors that might have occurred, and any details that led up to your problem. We need these specific details to best analyze the problem.
[Large text area]

Mailer settings ... OK Cancel

[Sending the Log](#)

When sending the log or items selected from the quarantine, an information window appears. At the top of the window, the data of the sender is displayed. The data specified by the sender can be modified – along with the SMTP settings – by clicking on the **[Mailer settings ...](#)** button. The following fields must be filled in the panel (specifying appropriate SMTP settings is vital for the operation of the Mailer):

- **SMTP server**
Name of the server delivering the e-mails, usually this name is given by the Internet Service Provider (ISP) or it is the name of the Exchange server (this information can be found in the mailer client settings /Outlook, Thunderbird, and so on/ or you can ask your system administrator or ISP)

- *Port number*
The port number of the mail server (25 in most cases)
- *User name*
This name is displayed in the mail you sent us as 'sender'. Tokens can also be used in this field:
%m% - computer name
%u% - username
- *E-mail address*
This is the e-mail address the response is sent to.

In the center of the panel in the *Mail information* section, the header of the mail to be sent is displayed, but it cannot be edited. The recipient is VirusBuster's support division. Under this, the subject of the mail and the attached files are displayed, then the name of the attached log file is displayed in case of sending the log, or a reference to the attached files in case of sending quarantined files. Fill the *Comments* text field in which you can describe your problem or write your questions and comments.

You can send the e-mail by pressing the **OK** button or you can terminate the process by clicking on the **Cancel** button.

Virus Scanning Methods

The virus scanning engine can scan for and detect viruses according to the set methods/levels. You can choose the needed scanning method in the components of the software. The following levels are available:

- *Quick*
Scans only the parts of a file that are most likely to contain a virus and does not detect viruses that can only be detected by using a large amount of system resources (for example, Excel FORMULA viruses).
- *Extensive*
Optimized scanning method that detects all viruses registered in the virus database and scans those parts of the file that are most likely to contain a virus.
- *Full*
Detects all viruses registered in the virus database and scans the whole file, even the parts where viruses are not likely to be found.

Heuristics

During a heuristic analysis, the software tries to detect codes and programs that 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*
There is 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 becomes disinfected and is restored to its original status.
- *Move to quarantine*
It 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*
It deletes the infected file permanently.
- *Rename*
It changes the first letter of the name of the extension to v in the infected file.

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

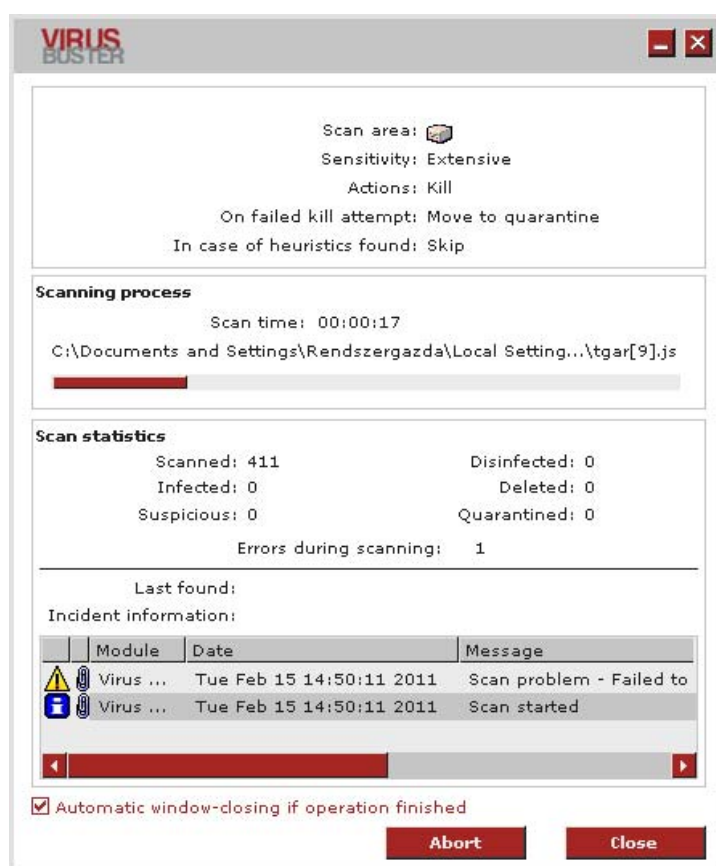
- *Delete attachment*
It deletes the infected attachment from the e-mail:
- *Rename attachment*
It renames the first letter of the name of the extension to w in the infected attachment.

Windows, Messages

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

Virus Scan Window

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



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 currently scanned, 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 inform you about the last found virus. The log entries 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 double-clicking on an item.

Virus scans can be started in many ways, so 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.

Virus Scan Window During a Scanning Task and During a Manual Scan

In case of these scanning methods, the virus scan window is not displayed as a separate window, but on the console interface. Above basic information, several buttons are available to control the scanning process:

You can terminate scanning by clicking on the **|Cancel|** button to return to the scanning [Tasks](#).

During scanning:

- **|Stop|**
You can stop scanning any time during the process. After stopping the process, the buttons displayed when scanning is finished become available.
- **|Pause|**
If scanning is paused, the process is stopped temporarily, not permanently. You can continue scanning by clicking on the **|Continue|** button.

After scanning:

- **|Rescan|**
It restarts the scanning task.
- **|Save as ...|**
It saves the log entries of the virus scan to a log file.
- **|Add|** (Only in case of *Manual scanning!*)
The scan with the adjusted settings can be saved as a scanning task that can be started later by clicking on a button. Set [Scheduling](#) and [Task's name](#) to be able to create the new task.

Virus Scan Window During a Quick Scan

In case of a quick scan, a window appears which informs the user about the status of the scan. By enabling the *Automatically close the window after the operation* option at the bottom of the panel, the scan window is automatically closed after scanning is finished. This can also be performed by clicking on the **|Close|** button. The scanning process can be terminated by clicking on the **|Abort|** button.

Message Window

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

Recognizing a Virus Infection

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

Infection types:

- *Infected - killable*
The virus scanning engine found an infected file that can be disinfected.
- *Infected – non-killable*
The virus scanning engine found a virus in the file, but has no information in its database about the method of disinfection.
- *Suspicious*
The virus scanning engine found a virus-suspicious file. This means that the file contains code or a code segment indicating 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 (only in case of using VirusBuster Professional)
- MS Outlook protection only in case of using VirusBuster Professional)
- 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 that sent the message are displayed. This informs you which module found the virus. The red bar in the middle informs you about the type of the infection and you also receive information about the method of disinfection and possible further activities. Below the red bar, the name of the infected file and its path are displayed and next to it – if this information is available, the name of the detected virus can be found.

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

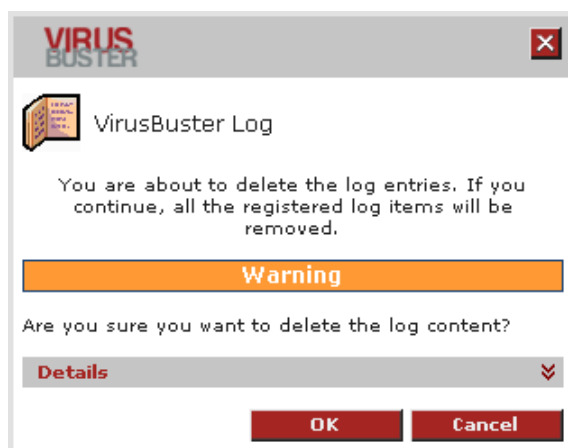
The program can only send a warning message about incidents reported by the *Shield* module, infections are handled as set in the *Virus found settings* section of the module.

By clicking on the **[X]** button in the top right corner of the window, the *Skip* action is performed on the current incident.

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

Warning

These messages provide information about changes and effects or results of an operation initiated by the 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 that sent the message are displayed. 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.

You can confirm the message by clicking on the **|OK|** button, and the operation is 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