Dr.WEB
for Kerio Control firewall

Administrator Manual

Жасағаның
دافع عن إبداعاتك
Защити созданное
Defend what you create
Protégez votre univers
Verteidige, was du erschaffen hast
Захисти створене
保护您创建的一切
Proteggi ciò che crei
Защити созданное
Защити созданное
Жасағаныңды қорға
Verteidige, was du erschaffen hast
Proteggi ciò che crei
Захисти створене
Defend what you create
脅威からの保護を提供します
Protégez votre univers
Proteggi ciò che crei
Захисти створене
دافع عن إبداعاتك
脅威からの保護を提供します
Defend what you create
Жасағаныңды қорға
دافع عن إبداعاتك
دافع عن إبداعاتك
Protégez votre univers
保护您创建的一切
Защити созданное
脅威からの保護を提供します
Захисти створене
Verteidige, was du erschaffen hast

Dr.Web for Kerio Control firewall
Version 9.0.0
Administrator Manual
5/24/2017

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: http://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of contents

Introduction

Thank you for purchasing Dr.Web for Kerio Control firewall. This product is a plug-in that integrates into Kerio Control and protects the Internet traffic against viruses and all the types of malware by checking the files transferred via HTTP, FTP, SMTP and POP3 protocols.

With the use of the plug-in, Kerio Control incorporates the latest and most advanced anti-virus technologies of Doctor Web aimed to detect the malicious objects which may present a threat to network operation and information security.

Dr.Web for Kerio Control firewall checks the Internet traffic for viruses, dialer programs, adware, riskware, hacktools and joke programs. On detection of a security threat, they are treated according to Kerio Control settings.

This guide helps administrators to install and configure Dr.Web for Kerio Control firewall plug-in to work with Kerio Control.

For detailed information on Kerio Control settings and traffic checks, see the Kerio official web site.

Document Conventions

This guide utilizes the following content conventions and signs (see Table 1).

Table 1. Document Conventions and Signs

Convention	Comment
	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

Main Features

Dr.Web for Kerio Control firewall performs the following functions:

- Anti-virus check of the files transferred via HTTP, FTP, SMTP and POP3 protocols, including the following:
  - Attachments of e-mails
  - Web traffic files downloaded via HTTP and FTP protocols
- Malware detection
- Isolation of the infected objects in Dr.Web quarantine
- Heuristic analyzer for additional protection against unknown viruses
- Fast and efficient check
- Automatic update of virus databases

Dr.Web for Kerio Control firewall does not check the files transferred via the HTTPS protocol.

Licensing

The use rights for the purchased product are regulated by the *license key* file.

License Key File

The license key has the .key extension and contains, among other, the following information:

- Licensed period for the product
- List of components the user is allowed to use
- Users number limitation for the license

A *valid* license key file satisfies the following criteria:

- License period has started and is not expired
- The license applies to all components of the product
- Integrity of the license key file is not violated

If any of the conditions is violated, the license key file becomes *invalid*, Dr.Web for Kerio Control firewall stops detecting the malicious programs and transmits the traffic unchanged.

Acquire License Key File

You can receive a license key file in one of the following ways:

- By e-mail in an archived attachment
- With the plug-in distribution kit
- On separate media

To acquire a license key file by e-mail

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. The license key file is archived and sent to the e-mail address you specified in the registration form.
5. Extract the license key file and copy it to the computer where Kerio Control resides and where Dr.Web for Kerio Control firewall is planned to be or is already installed.

For demonstrative purposes you may be provided with a *trial license key file*. Trial license allows you to access the full functionality of Dr.Web for Kerio Control firewall for a short-term period. No support is provided during trial period. On the expiration of the trial license, you will need to purchase a full license to continue working with the product.

To receive a trial license key file by e-mail, fill in the registration form at http://download.drweb.com/demoreq/.

For more information on licensing and types of license key files, visit the Doctor Web official web site.

Update License

When license expires or security of your system is reinforced, you may need to update the license. The new license then should be registered with the product. Dr.Web for Kerio Control firewall supports hot license update without stopping or reinstalling the plug-in.

To update the license key file

1. To update the license key file copy the new license key file to the /etc/opt/drweb.com/etc folder.
2. Restart the configuration daemon **configd** to switch the application to the new license.

For more information on license types, visit the Doctor Web official web site.

Use License Key Files

Dr.Web for Kerio Control firewall requires a key file for correct operation. The path to this file is specified during the installation.

During the operation of Dr.Web for Kerio Control firewall the plug-in searches for the first valid key file in the /etc/opt/drweb.com/etc folder, where it is copied during the installation of the program. If no valid key is found, the plug-in stops functioning.

Do not edit or otherwise modify the file to prevent the license from compromise.

Licensing Parameters

The license key file regulates the use of Dr.Web for Kerio Control firewall.

To view license details

1. View the license key file. (For instance, open the file with the text editor.)

The license key file is secured with digital signature. Do not edit or otherwise modify the file to prevent the license from compromise.

2. Review the following licensing parameters (see Table 2).

Table 2. Licensing Parameters

Parameter	Description
`[Key] | Applications`	Determines the application components licensed with the key.  To use the key with Dr.Web for Kerio Control firewall the component KerioPlugin should be in the list determined by this parameter.
`[Key] | Expires`	Determines the license expiration date.
`[User] | Name`	Determines the license owner.
`[User] | Computers`	Determines the number of users which the plug-in is licensed to protect simultaneously.

3. Close the file without saving.

Installation

Dr.Web for Kerio Control firewall resides on computers where Kerio Control is installed. It operates as an external anti-virus integrated via the plug-in interface.

Dr.Web for Kerio Control firewall is distributed as a single self-extracting archive **drweb-kerio-control_9.0.0.*[patch]*-*[build]*~linux_x86.run** (where *[patch]* is the number of patch, *[build]* is the number of program build, e.g., drweb-kerio-control_9.0.0.0-1312241911~linux_x86.run) and can be installed via console.

For more information on use of anti-virus within Kerio Control see the Kerio official web site at http://www.kerio.com/.

System Requirements

Before beginning installation, review the following system requirements and instructions (see Table 3).

Table 3. System Requirements

Component	Requirement
Disk Space	Minimum 290 MB of disk space
Operating System	• Kerio Control VMware Virtual Appliance • Kerio Control Software Appliance • Kerio Control Hyper-V Virtual Appliance
Firewall	Kerio Control, versions 8.x, 9.0 or 9.1

This section reflects requirements for the Dr.Web for Kerio Control firewall only. See Kerio Control guides for firewall requirements. Dr.Web for Kerio Control firewall operates successfully on computers which meet the Kerio Control requirements.

Dr.Web for Kerio Control firewall supports installation and operation in Kerio Control VMware Virtual Appliance and Kerio Control Software Appliance. For information on this environment see Kerio official web site at http://www.kerio.com/.

Program Components

Dr.Web for Kerio Control firewall is an anti-virus package that consists of several complimentary components interacting with each other to ensure the anti-virus protection. Below is a list of these components with their short descriptions:

- Configuration daemon (**configd**) controls activity of all components of Dr.Web for Kerio Control firewall depending on the specified settings, stores information on license and settings and provides application components with it, if necessary.
- Scanning engine (**drweb-se**) is used to perform anti-virus scanning.
- Updater (**drweb-update**) is designed to automatically update the virus databases. This component downloads the copies of the virus databases via Internet.

Install Plug-in

Before beginning installation, review the system requirements.

To install Dr.Web for Kerio Control firewall you must have the Administrator privileges.

Ensure to perform the following actions before installing Dr.Web for Kerio Control firewall:

1. Enable SSH on Kerio Control VMware Virtual Appliance:
   - Open the terminal, press Alt+F2 on the terminal.
   - Login as "root".
   - Execute the following command: `start-ssh`.
2. Copy the **drweb-kerio-control_9.0.0.*[patch]*-*[build]*~linux_x86.run** archive and Dr.Web for Kerio Control firewall license key file on Kerio Control VMware Virtual Appliance.

To install Dr.Web for Kerio Control firewall

1. Allow execution of the `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run` archive (where *[patch]* is the number of patch, *[build]* is the number of program build, e.g., `drweb-kerio-control_9.0.0.0-1401221455~linux_x86.run`). You can use the following command:

```
# chmod +x drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run
```

2. Execute the file by the command:

```
# ./drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run
```

You can also specify the path to the license key file using the `-k` option:

```
# drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86.run -- -k <path>
```

3. The `drweb-kerio-control_9.0.0.[patch]-[build]~linux_x86` directory will be created. Then the installer will start.
4. To continue installation of Dr.Web for Kerio Control firewall enter `Y` or `Yes` (values are case insensitive) and press ENTER. This will start the installation of the components. Otherwise type `N` or `No`.
5. If you have not specify the path to the license key file when running the run-file, you will be asked to specify it.
6. The message informing about completing the installation of program components will open.

Uninstall Plug-in

To uninstall Dr.Web for Kerio Control firewall you must have the Administrator privileges.

To uninstall Dr.Web for Kerio Control firewall

3. Disable the use of anti-virus Dr.Web for Kerio Control firewall by Kerio Control. To do this:
   - Launch the administration console for Kerio firewall.
   - Open the **Configuration** -> **Antivirus** section.
   - Clear the checkbox **Use an external antivirus** for Dr.Web for Kerio Control firewall;
   - Click **Apply** to disable the use of Dr.Web for Kerio Control firewall.
5. Execute the command `# /opt/dweb.com/bin/remove-kerio-control.sh`.
6. To continue Dr.Web for Kerio Control firewall removal, enter *Y* or *Yes* (values are case insensitive) and press *ENTER*. This will start the components uninstall process. Otherwise enter *N* or *No*.
7. The message informing about the removal of the selected components will open.

The license key file and quarantine are not deleted by default. You can delete them.

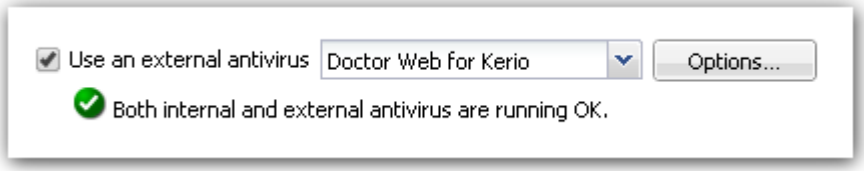
In addition, the specified check settings are saved and automatically used if you reinstall the plug-in.

Configuration

Dr.Web for Kerio Control firewall is enabled and operates as an external anti-virus software within Kerio Control and provides the check of different traffic types according to the settings of Kerio Control.

To integrate Dr.Web for Kerio Control firewall into Kerio Control:

1. Open the administration console for Kerio firewall.
2. Open the **Configuration** -> **Antivirus** section.
3. In the **Antivirus Software** group of the **Antivirus Engine** tab, select the checkbox **Use an external antivirus** and then select **Doctor Web for Kerio** in the drop-down list.
4. Specify the antivirus options.
5. Specify the protocols for scanning.
6. Click **Apply**. If the plug-in was integrated successfully, the corresponding message will appear under the anti-virus software selection option (see illustration below).



If the integration failed and an error is reported, check the installation of the plug-in and check the error log of Kerio Control. Consult the Kerio Control Administrator's Guide as well to resolve the problem.

A valid key file is required for Dr.Web for Kerio Control firewall operation. In case license is missing or an error occurred in configuration daemon **configd** operation, the Internet traffic is not scanned for viruses! Information on the encountered problem is fixed in the error log of Kerio Control.

The detailed information on possible errors of anti-virus integration is available in the Kerio Control Administrator's Guide and at Kerio official web site.

Anti-virus Options

The options of Dr.Web for Kerio Control firewall specify the program operation These options can be set up by means of administration console for Kerio firewall on the **Configuration** -> **Antivirus** section:

1. Click **Options** to the right of anti-virus name in the **Antivirus Software** group of **Antivirus Engine** tab.
2. The list of options to configure the anti-virus check and quarantine managing will open.
3. Click **OK** in **Antivirus Options** window when you finish setting up the anti-virus plug-in options.
4. Click **Apply** on the **Antivirus Engine** tab to apply the changes.

Scanned Protocols

Dr.Web for Kerio Control firewall scans for viruses and other malware the traffic going through the protocols that can be specified on the **Configuration** -> **Antivirus** section of administration console for Kerio firewall.

To specify protocols for scanning:

1. In the **Protocols** group of **Antivirus Engine** tab select the protocols that you want be scanned by Dr.Web for Kerio Control firewall. You can select the following protocols for scanning: HTTP, FTP, SMTP and POP3.
2. If desired, you can also enable the limitation of the maximum size of scanned files and specify this maximum (in kilobytes) in corresponding text field. The default value is 4096 KB.

For detailed information on scanning of different types of protocols and its settings available via administration console for Kerio firewall see the Kerio Control Administrator's Guide.

Virus Check

Dr.Web for Kerio Control firewall detects the following malicious objects:

- Infected attachments in e-mails
- Infected objects transmitted via HTTP and FTP protocols.

Dr.Web for Kerio Control firewall checks the internet traffic for the following types of malicious objects and malware:

- Infected archives
- Bomb viruses in files or archives
- Adware
- Hacktools
- Dialer programs
- Joke programs
- Riskware

You can specify the protocols that would be scanned for viruses by Dr.Web for Kerio Control firewall and set up the anti-virus options determining the types of detected malicious objects.

Dr.Web for Kerio Control firewall uses different detection methods and scans the traffic transferred via selected protocols. In case a virus is detected by Dr.Web for Kerio Control firewall it is processed according to the settings of Kerio Control (see Table 4). These settings are specified on the tabs of the **Configuration** -> **Antivirus** section in administration console for Kerio firewall.

Table 4. Settings of traffic scanning and actions applied to detected malware.

Tab	Description
HTTP, FTP scanning	If a virus is detected in traffic going through HTTP and FTP protocols, its transmission is denied and the firewall performs the actions specified on this tab by administrator. Using this tab administrator can also specify the actions of firewall in case the transferred file cannot be checked for viruses and the scanning rules determining which types of objects would be checked by Dr.Web for Kerio Control firewall.
Email scanning	On this tab the settings of anti-virus check of SMTP and POP3 protocols can be specified as well as the actions in case a virus is detected in the attached files or anti-virus check fails (due to corruption or encryption of the file).

In case Dr.Web for Kerio Control firewall detects a virus or other malware, the administrator can de notified about it by e-mail or SMS. Besides, information on all detected malicious objects is accumulated in alert log of Kerio Control.

For detailed information on scanning of different types of traffic and sending notifications see the Administrator's Guide of Kerio Control.

The anti-virus check of large files (larger than 50 Mb) may take considerable time. As a result, in some cases the data transferred via Kerio Control is not delivered to the recipients. this should be taken into consideration when configuring the timeout for data delivery for the corresponding applications and the scanned file size limits for Kerio Control.

For security reasons, it is recommended to enable the Forbid resume due to antivirus scanning rule in the FTP policy section of the Kerio firewall administration console, otherwise, the infected objects can get into the client computers in an attempt to re-download them.

Check Settings

The following anti-virus options allow you to specify the program actions for different types of malware and enable heuristic analyzer and the use of quarantine (Table 5).

Table 5. Anti-virus check settings.

Option	Description
Detect adware (Yes/No) Detect dialers (Yes/No) Detect hacktools (Yes/No) Detect jokes (Yes/No) Detect riskware (Yes/No)	These options allow to enable/disable the detection of adware, dialers, hacktools, jokes and riskware in the Internet traffic. Each parameter may have one of the following values: • **No** to disable detection of corresponding malware type. Therefore, the objects containing such malware will be ignored. • **Yes** to enable detection of corresponding malware type. In this case, the transmission of the objects with such type of malware will be denied. By default, this value is set for all options in this group. When configuring these options please note that their values are case sensitive.
Enable heuristic (Yes/No)	This option enables/disables the heuristic analyzer that allows to detect the unknown viruses. Two values are possible: • **No** to disable the heuristic analyzer • **Yes** to enable the heuristic analyzer By default, the heuristic analyzer is enabled. When configuring this option please note that its values are case sensitive.
Quarantine directory	This option specifies the path to the quarantine directory. The default path is **/var/lib/drweb/quarantine**.

Option	Description
Quarantine enabled (Yes/No)	This option allows to enable/disable moving the infected objects to quarantine. By default, it is disabled. Two values are possible: • **No** to disable the use of quarantine • **Yes** to enable moving the infected objects to quarantine  When configuring this option please note that its values are case sensitive.

 The specified parameters are saved when reinstalling Dr.Web for Kerio Control firewall.

Detection Methods

The Dr.Web Anti-virus solutions use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behavior.

Signature analysis

The scans begin with signature analysis which is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the Dr.Web Anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

On completion of signature analysis, the Dr.Web Anti-virus solutions use the unique Origins Tracing™ method to detect new and modified viruses which use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing™ mechanism allows to considerably reduce the number of false triggering of the heuristics analyzer. Objects detected using the Origins Tracing™ algorithm are indicated with the .Origin extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an emulator – a programming model of the processor and runtime environment. The emulator operates with protected memory area (emulation buffer), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristics analyzer is based on certain knowledge (heuristics) about certain features (attributes) than might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the FLY-CODE™ technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers Dr.Web is aware of, but by also new, previously unexplored programs. While checking packed objects, Dr.Web Anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious".

While performing any of the abovementioned checks, the Dr.Web Anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web Virus Laboratory discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the Dr.Web resident guards and penetrates the system, then after an update the virus is detected in the list of processes and neutralized.

Quarantine

The infected attachments can be moved to Quarantine – a special directory (`/var/lib/drweb/quarantine`,), where the malicious objects are isolated from the rest of the system.

By default, the quarantine is disabled and all infected ojects are deleted. To enable it, set the value **Yes** for the **Quarantine enabled** anti-virus parameter.

If a file moved to quarantine has the same name as a file that is already in quarantine, an index will be added to the name of the new file. For example, the file `file.com` will be renamed to `file.com.drwebq.1524482643`, where `1524482643` is the file creation timestamp.

Manage Quarantine

The quarantined files can be reviewed and processed only by the superuser (root). The files can be removed from quarantine or saved on the disk.

Update

Dr.Web for Kerio Control firewall uses virus databases to detect malicious software. These databases contain details and signatures for all viruses and malicious programs known at the moment of the plug-in release. However modern computer viruses are characterized by the high-speed evolvement and modification. More than that, within several days and sometimes hours, new viruses emerge which can infect millions of computers around the world. To mitigate the risk of infection during the licensed period, Doctor Web provides you with regular updates to virus databases and plug-in components.

A special component Dr.Web Updater is used to update virus databases. Updater is a part of Dr.Web for Kerio Control firewall and can be installed via the **drweb-updater** packet of the installation archive. It is started automatically by configuration daemon **configd** and checks the availability, downloads and installs updates every 30 minutes.

Logging

Dr.Web for Kerio Control firewall registers errors and application events in debug, error and security protocols of Kerio Control.

Debug Log

The debug log of Kerio Kerio Control contains the information that is used for search and analysis of errors in operation of Dr.Web for Kerio Control firewall.

To enable the debug logging

1. Launch the administration console for Kerio firewall.
2. On the **Logs** section click **debug**.
3. Right-click the window of debug log, and then click **Messages**.
4. In the **Logging Messages** window select the option **Antivirus plugin** and then click **OK**.

Troubleshooting

If you're experiencing trouble protecting the Internet traffic from virus threats, follow the steps below to ensure that Dr.Web for Kerio Control firewall is installed and configured properly:

- Check installation
- Check plug-in operation

If the errors are reported and the problems of Dr.Web for Kerio Control firewall operation persist, contact Dr.Web Technical Support for help and assistance.

Check Installation

To check whether the plug-in is correctly installed:, ensure that during the plug-in installation the following folders have been created and contain all necessary files (see Table 6):

Table 6. Check the installed files and folders

Directory	File name	Description
/opt/dweb.com/bin	drweb-configd	Configuration daemon
	drweb-update	Updater
	drweb-se	Scanning engine
/etc/opt/drweb.com	drweb32.key	Key file
/opt/kerio/winroute/avirplugins	avir_drweb.so	The library of anti-virus application Dr.Web for Kerio Control firewall

Check Functionality

To make sure the plug-in operates properly, it is recommended to check the program's virus detection capabilities.

To check plug-in operation

1. Open the page http://www.eicar.org/download/eicar.com using the Internet browser to download the test virus EICAR-Test-File. The mentioned page must not open, and the information on the attempt to download the infected file must be fixed in the alert log of Kerio Control.

2. Send an e-mail with EICAR-Test-File in attachment via server protected by Kerio Control. Check the received e-mail. The infected object must be deleted. The message subject may contain the prefix informing about the detected malicious object.

Appendices

Technical Support

If you encounter any issues installing or using company products, take advantage of the following Doctor Web support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Browse the Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from Doctor Web Technical Support by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, see the Doctor Web official web site at http://company.drweb.com/contacts/moscow.