



Dr.WEB®

for Kerio WinRoute

Defend what you create

Administrator Manual

© 2003-2013 Doctor Web. All rights reserved.

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk and Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

**Dr.Web for Kerio WinRoute
Version 6.00.2
Administrator Manual
10.06.2013**

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site 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

| | |
|---|-----------|
| Chapter 1. Introduction | 6 |
| Conventions | 8 |
| Contacting Support | 9 |
| Chapter 2. Licensing | 10 |
| License Key File | 10 |
| Acquire License Key File | 11 |
| Update License | 12 |
| Use License Key Files | 12 |
| Licensing Parameters | 13 |
| Chapter 3. Installation | 14 |
| System Requirements | 14 |
| Compatibility | 15 |
| Install Plug-in | 16 |
| Uninstall Plug-in | 17 |
| Configure Internet Connection for Updater | 19 |
| Chapter 4. Configuration | 20 |
| Anti-virus Options | 21 |
| Check Settings | 21 |
| Notifications Settings | 24 |
| Scanned Protocols | 26 |
| Chapter 5. Virus Check | 27 |
| Detection Methods | 28 |
| Quarantine | 30 |



| | |
|---|-----------|
| Chapter 6. Web Console | 33 |
| Program Information | 34 |
| Program Statistics | 34 |
| Chapter 7. Update | 35 |
| Chapter 8. Logging | 37 |
| Event Log | 37 |
| Text Log | 38 |
| Debug Log | 39 |
| Chapter 9. Troubleshooting | 40 |
| Check Installation | 40 |
| Check Functionality | 41 |
| Appendices | 43 |
| Appendix A. Updater Command Line Parameters | 43 |
| Appendix B. Collect Information for Troubleshooting | 46 |
| Appendix C. Operation in Central Protection Mode | 49 |
| Index | 52 |



Chapter 1. Introduction

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

With the use of the plug-in, Kerio WinRoute Firewall and Kerio Control incorporate 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 WinRoute 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 WinRoute Firewall/Kerio Control settings.

Main Features

Dr.Web for Kerio WinRoute 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
 - Files transferred over the web-service Kerio Clientless SSL VPN
- 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 WinRoute does not check the files transferred via the HTTPS protocol.

This guide helps administrators to install and configure **Dr.Web for Kerio WinRoute** to work with Kerio WinRoute Firewall/Kerio Control.


For detailed information on Kerio WinRoute Firewall/Kerio Control settings and traffic checks, see the Kerio official web site at http://www.kerio.com/kwf_home.html.



Conventions

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

Table 1. Document Conventions and Signs

| Convention | Description |
|---|--|
| Bold | Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide. |
| Green and bold | Names of Doctor Web products and components. |
| <u>Green and underlined</u> | Hyperlinks to topics and web pages. |
| Monospace | Code examples, input to the command line and application output. |
| <i>Italic</i> | Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition. |
| CAPITAL LETTERS | Names of keys and key sequences. |
| Plus sign ('+') | Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key. |
|  | A warning about potential errors or any other important comment. |



Contacting Support

Support is available to customers who have purchased a commercial version of **Doctor Web** products. Visit **Doctor Web Technical Support** web site at <http://support.drweb.com/>.

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/>
- Look for the answer in **Dr.Web** knowledge database at <http://wiki.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-form 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>.



Chapter 2. 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 WinRoute** stops detecting the malicious programs and transmits the traffic unchanged. License violation is registered in the Windows Event Log and in the text log of plug-in.

See [Logging](#) for detailed information about events logging.



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 WinRoute Firewall/Kerio Control resides and where **Dr. Web for Kerio WinRoute** 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 WinRoute** 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 at <http://www.drweb.com>.



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 WinRoute** 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 program installation folder (by default, %ProgramFiles%\DrWeb for Kerio WinRoute\).
2. **Dr.Web for Kerio WinRoute** automatically switches to the new license.

For more information on license types, visit the **Doctor Web** official web site at <http://www.drweb.com>.

Use License Key Files

Installation Wizard copies and registers the license key file to the plug-in installation folder (usually, %ProgramFiles%\DrWeb for Kerio WinRoute).

During the operation of **Dr.Web for Kerio WinRoute** the plug-in searches for the first valid key file in the installation folder (by the *.key mask) starting with the key file indicated while installing 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 WinRoute**.

To view license details


1. View the license key file. (For instance, open the file with the Notepad 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 WinRoute 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. |
| [Settings] MailServer | Determines if the license can be used on mail servers. |

3. Close the file without saving.



Chapter 3. Installation

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

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

System Requirements

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

Table 3. System Requirements

| Component | Requirement |
|------------------|--|
| Disk Space | Minimum 350 MB of disk space |
| Operating System | One of the following: <ul style="list-style-type: none">• Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server or Datacenter Server) with SP4 and Update Rollup 1• Microsoft® Windows® XP (Home Edition or Professional Edition)• Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition or Datacenter Edition)• Microsoft® Windows Server® 2003 R2• Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition or Datacenter Edition)• Microsoft® Windows Server® 2008 R2 |



| | |
|---------------------|--|
| | <ul style="list-style-type: none">• Windows Vista® (Starter, Home Basic, Home Premium, Business, Enterprise or Ultimate)• Microsoft® Windows 7® (Starter, Home Basic, Home Premium, Business, Enterprise or Ultimate) Both 32-bit and 64-bit versions of operating systems are supported. |
| Firewall | If you're installing Dr.Web for Kerio WinRoute for the first time, the following firewall versions can be used: <ul style="list-style-type: none">• Kerio WinRoute Firewall 6.2 or higher• Kerio Control, versions from 7.0.0 to 7.4.2 |
| Additional software | Dr.Web Agent 6.0 or higher (for operation in central protection mode) |

Before installation of **Dr.Web for Kerio WinRoute** please review the information on plug-in [compatibility](#).

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

Compatibility

Before installation of **Dr.Web for Kerio WinRoute** please review the following information on product compatibility:

- Version 6.00.2 of **Dr.Web for Kerio WinRoute** is compatible only with **Dr.Web** products of version 6.
- If anti-virus solutions of other vendor are operating in the system besides **Dr.Web for Kerio WinRoute** the proper operation of the plug-in cannot be guaranteed.



- In case an anti-virus file guard **Spider Guard** operates in the system besides **Dr.Web for Kerio WinRoute**, it is necessary to add to exclusions the Kerio firewall file upload path (usually, % ProgramFiles%\Kerio\WinRoute Firewall\tmp\) in anti-virus file guard settings to enable the anti-virus check by **Dr.Web for Kerio WinRoute**.
- All critical updates issued for the operating system should be installed before installation of **Dr.Web for Kerio WinRoute**.

Install Plug-in

Before beginning installation, review the [system requirements](#).



To install **Dr.Web for Kerio WinRoute** you must have the Administrator privileges.

To install Dr.Web for Kerio WinRoute

1. Stop the Kerio WinRoute Firewall/Kerio Control service.
2. Copy the following files to the computer where Kerio WinRoute Firewall/Kerio Connect resides:
 - Installation file
 - License key file
2. Run the installation file depending on the type of the operating system that is used on the computer:
 - **drweb-KerioWinRoute-600-windows-nt-x86.exe** in case the 32-bit operating system is used
 - **drweb-KerioWinRoute-600-windows-nt-x64.exe** if the operating system is 64-bit
3. The window with a suggestion to choose the language of installation will appear. You can choose English or Russian language of installation. Click **OK**.
4. InstallShield Wizard for Kerio WinRoute will open. Click **Next**.
5. On the **License Agreement** page read the Dr.Web License Agreement, select **I accept the terms in the license agreement** and click **Next**.



6. Select the licensing type. You can use either the key file from **Dr.Web Control Center** or a local key file. Click **Next**.
7. If you have selected to use the local key file on the previous step, enter the path to the license key file or click **Browse** to select the file on the **License Key** page. Click **Next**.
8. On the **Kerio WinRoute Path** page specify the path to the Kerio WinRoute installation folder. Click **Next**.
9. On the **Destination Folder** page enter the path to the folder where the plug-in will be installed. By default, it is the folder **%ProgramFiles%\DrWeb for Kerio WinRoute**. If you want to choose another folder click **Change** and specify the path to it. Click **Next**.
10. On the **Ready to Install the Program** page click **Install** to start installation of **Dr.Web for Kerio WinRoute** on your computer.
11. After the installation of **Dr.Web for Kerio WinRoute** is completed you can launch the virus databases update by selecting the checkbox **Run update**. Then click **Finish** to exit the wizard.

This completes the plug-in installation. You need to [configure](#) Kerio WinRoute Firewall/Kerio Control to use the plug-in.

Uninstall Plug-in



To uninstall **Dr.Web for Kerio WinRoute** you must have the Administrator privileges.

To uninstall Dr.Web for Kerio WinRoute

1. Disable the use of anti-virus **Dr.Web for Kerio WinRoute** by Kerio WinRoute Firewall/Kerio Control. To do this:
 - Launch the administration console for Kerio firewall.
 - Open the **Configuration** -> **Content Filtering** -> **Antivirus** section.



- In the group **Antivirus Software** on the **Antivirus Engine** tab clear the checkbox **Use external antivirus** for selected anti-virus **Dr.Web for Kerio WinRoute**.
 - Click **Apply** to disable the use of **Dr.Web for Kerio WinRoute**. The caption «**Disabled**» under the checkbox **Use external antivirus** indicates that the selected anti-virus is not used by the firewall.
2. Use one of the following methods to uninstall **Dr.Web for Kerio WinRoute**:
 - On the **Control Panel**, double-click **Add or Remove Programs**, then in the programs list select **Dr.Web for Kerio WinRoute** and click **Remove**. At the prompt, click **Yes**.
 - Launch the installation file of the plug-in. Choose the language of the dialog (English or Russian) and click OK. The InstallShield Wizard will open. Click **Next**. On the **Remove the Program** page click **Remove** to uninstall **Dr.Web for Kerio WinRoute**. On completion of program removal click **Finish** to exit the wizard.
 3. The plug-in files and update task will be removed.



The license key, program statistics and log files are not deleted by default. You have to delete the files manually from the program installation folder (by default, %ProgramFiles%\DrWeb for Kerio WinRoute).



Configure Internet Connection for Updater

If the computer where Kerio WinRoute Firewall/Kerio Control resides connects to the Internet via proxy, you need to configure the **Dr.Web for Kerio WinRoute Updater** to connect to the proxy server.

To configure connection to a proxy server

1. In the **Dr.Web for Kerio WinRoute** installation folder (usually, %ProgramFiles%\DrWeb for Kerio WinRoute), double-click drwebupw.exe.
2. In the dialog window, click **Settings**.
3. In the **Settings** window open the **Proxy** tab.
4. Enter the IP-address and the port number that the proxy server uses.
5. If required, enter user name and the password needed for connection to the proxy server or leave blank if the proxy server allows anonymous access.
6. Click **OK**.

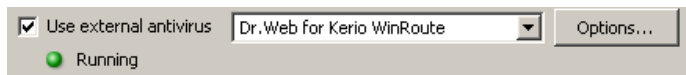


Chapter 4. Configuration

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

To integrate **Dr.Web for Kerio WinRoute** into Kerio WinRoute Firewall/Kerio Control:

1. Open the administration console for Kerio firewall.
2. Open the **Configuration -> Content Filtering -> Antivirus** section.
3. In the **Antivirus Software** group of the **Antivirus Engine** tab, select the checkbox **Use external antivirus** and then select **Dr.Web for Kerio WinRoute** 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 caption «**Running**» will appear near the name of anti-virus (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 WinRoute Firewall/Kerio Control. Consult the Kerio WinRoute Firewall/Kerio Control Administrator's Guide as well to solve the problem.

For detailed information on use of anti-virus software with Kerio WinRoute Firewall/Kerio Control and possible errors of integration, see Kerio WinRoute Firewall/Kerio Control Administrator's Guide and Kerio official web site at http://www.kerio.com/kwf_home.html.



Anti-virus Options

The options of **Dr.Web for Kerio WinRoute** specify the program operation and logging. These options can be set up by means of a administration console for Kerio firewall on the **Configuration** -> **Content Filtering** -> **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](#), the [program logging](#), the [notifications sending](#) and also the [port](#) to work with the web console will open. To change the value of each option, select it in the list and click **Edit**. In the window **Edit value**, specify the value of the selected option.
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.

Check Settings

The following options allow to configure the check of archives, specify the program actions for different types of malware and enable the use of quarantine ([Table 4](#)).



Table 4. Anti-virus check options.

| Option | Description |
|---|---|
| Engine: Check archives (0, 1) | <p>This option enables/disables the scanning of archives. Two values are possible:</p> <ul style="list-style-type: none">• 0 to disable scanning of archives• 1 to enable scanning of archives <p> For correct archive check the value of this parameter must correspond to the scanning rules for archive scanning in Kerio WinRoute Firewall/ Kerio Control.</p> |
| Engine: Detect adware (0, 1) Engine: Detect dialers (0, 1) Engine: Detect hacktools (0, 1) Engine: Detect jokes (0, 1) Engine: Detect riskware (0, 1) | <p>These options allow to enable/disable the detection of adware, dialers, hacktools, jokes and riskware in web traffic. Each parameter may have one of the following values:</p> <ul style="list-style-type: none">• 0 to disable detection of corresponding malware type. Therefore, the objects containing such malware will be ignored.• 1 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. |
| Engine: Enable heuristic (0, 1) | <p>This option enables/disables the heuristic analyzer that allows to detect the unknown viruses. Two values are possible:</p> <ul style="list-style-type: none">• 0 to disable the heuristic analyzer• 1 to enable the heuristic analyzer <p>By default, the heuristic analyzer is enabled.</p> |
| Quarantine: Enabled (0, 1) | <p>This option allows to enable/disable moving the infected objects to quarantine. By default, it is enabled.</p> |




| Option | Description |
|-------------------------------|---|
| Engine: Max archive level | <p>This option specifies the maximum level of embedding in archives. If the number of embedding levels of a scanned object is bigger than the specified one, the object will be treated as if the check failed according to the corresponding settings of Kerio firewall.</p> <p>The default value is 16.</p> |
| Engine: Max archive size (KB) | <p>This option defines the maximum file size (in kilobytes) of an archive. If the size of an archive exceeds the specified value, the object will be treated as if the check failed according to the corresponding settings of Kerio firewall.</p> <p>The default value is 0 KB (corresponds to the unlimited file size).</p> |
| Engine: Max scan time (ms) | <p>This parameter defines the maximum time (in milliseconds) for object check. If the time of an object check exceeds the specified one, the object will be treated as if the check failed according to the corresponding settings of Kerio firewall.</p> <p>The default value is 0 ms (corresponds to the unlimited check time).</p> |

The following options allow to configure the program logging ([Table 5](#)).



Table 5. Program logging settings.

| Option | Description |
|-----------------------------|--|
| Logging: Log level (0, 1) | <p>By setting this option you can turn on/off plug-in logging. By default, logging is turned off. Two values are acceptable:</p> <ul style="list-style-type: none">• 1 to turn on logging• 0 to turn off logging <p> To apply changes of this setting you need to reconfigure Kerio firewall to use the anti-virus Dr.Web for Kerio WinRoute.</p> |
| Logging: Max file size (KB) | <p>This setting allows to specify the maximum file size (in kilobytes) for the log text file. The default value is 50000 KB.</p> |

Notifications Settings

The following options allow to select the notifications types ([Table 6](#)) and also specify the parameters of the server used to send the notifications ([Table 7](#)).

Table 6. Mail notifications parameters.

| Option | Description |
|-----------------------------|--|
| Notify: Check failed (0, 1) | <p>This option allows to enable/disable sending the notifications on check failure (e.g. in case a checked object is corrupter or password-protected).</p> <p>By default, this notification type is enabled.</p> |



| Option | Description |
|----------------------------------|---|
| Notify: Bases out of date (0, 1) | This option allows to enable/disable sending the notifications on virus databases becoming outdated. By default, this notification type is disabled. |
| Notify: Daily statistics (0, 1) | This option allows to enable/disable sending the information on the program statistics for the last 24 hours. By default, this notification type is disabled. |
| Notify: Key not found (0, 1) | This option allows to enable/disable sending the notifications on the event of missing license key file. By default, this notification type is disabled. |
| Notify: License expires (0, 1) | This option allows to enable/disable sending the notifications on the forthcoming license expiration. By default, this notification type is disabled. |
| Notify: Start error (0, 1) | This option allows to enable/disable sending the notifications on the application start error. By default, this notification type is disabled. |
| Notify: Threat detected (0, 1) | This option allows to enable/disable sending the notifications on threats detection while checking e-mail attachments. By default, this notification type is disabled. |

Table 7. Notifications server parameters.

| Option | Description |
|-----------------------|---|
| SMTP Notify: From | This option allows to specify the e-mail address of the notifications sender. |
| SMTP Notify: Password | This option allows to specify the user password to access to the notifications server. |
| SMTP Notify: Server | This option allows to specify IP-address and port of the notifications server. Example: 192.168.0.1:25. |



| Option | Description |
|-----------------------|---|
| SMTP Notify: To | This option allows to specify the e-mail addresses of the notifications recipients. You can enter one or several addresses separated by commas or semicolons. |
| SMTP Notify: Username | This option allows to specify the user name to access to the notifications server. |

Scanned Protocols

Dr.Web for Kerio WinRoute scans for viruses and other malware the traffic going through the protocols that can be specified on the **Configuration -> Content Filtering -> Antivirus** section of a dministration 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 WinRoute**. You can select the following protocols for scanning: HTTP, FTP, SMTP and POP3. By default, all indicated protocols are selected.
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 WinRoute Firewall/Kerio Control Administrator's Guide.



Chapter 5. Virus Check

Dr.Web for Kerio WinRoute detects the following malicious objects:

- Infected attachments in e-mails and infected objects transmitted via HTTP and FTP protocols or using the web-service Kerio Clientless SSL VPN, including:
 - 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 WinRoute** and set up the [anti-virus options](#) determining the types of detected malicious objects.

Dr.Web for Kerio WinRoute uses different [detection methods](#) and scans the traffic transferred via selected protocols. In case a virus is detected by **Dr.Web for Kerio WinRoute** it is processed according to the settings of Kerio WinRoute Firewall/Kerio Control (see [Table 8](#)) that are specified on the tabs of the **Configuration** -> **Content Filtering** -> **Antivirus** section in administration console for Kerio firewall.



Table 8. 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 WinRoute . |
| 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). |
| SSL-VPN scanning | This tab allows to set up the scanning of the files transferred via the Kerio Clientless SSL VPN web-service. You can enable scanning for the uploaded and/or downloaded files and specify the actions in case the transferred file cannot be checked for viruses. |

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

For detailed information on scanning of different types of traffic and sending notifications see the Administrator's Guide of Kerio WinRoute Firewall/Kerio Control available on the Kerio official web site at http://www.kerio.com/supp_kwf_manual.html.

Detection Methods

The **Doctor Web** anti-viruses simultaneously use several malware detection methods, which allow them to perform thorough checks on suspicious files and control software behaviour:



1. 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 **Doctor Web** anti-viruses use signature checksums instead of using complete signature sequences. Checksums uniquely identify signatures which preserves correctness of virus detection and neutralization. The **Dr.Web** signature databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.
2. On completion of signature analysis, the **Doctor Web** anti-viruses use the unique **Origins Tracing** method to detect new and modified viruses which use the known infection mechanisms. Thus the **Dr.Web** users are protected against such viruses as notorious blackmailer Trojan.Encoder.18 (also known as [gpcode](#)). In addition to detection of new and modified viruses, the Origins Tracing mechanism allowed to considerably reduce the number of false triggering of the **Dr.Web** heuristics analyser.
3. The detection method used by the *heuristics analyser* is based on certain knowledge about attributes that characterize malicious code. Each attribute or characteristic has weight coefficient which determines the level of its severity and reliability. Depending on the sum weight of a file, the heuristics analyser calculates the probability of unknown virus infection. As any system of hypothesis testing under uncertainty, the heuristics analyser may commit type I or type II errors (omit viruses or raise false alarms).

While performing any of the abovementioned checks, the **Doctor Web** anti-viruses use the most recent information about known malicious software. As soon as experts of the Doctor Web virus laboratory discover new threats, the update for virus signatures, behaviour characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore the automatic [update of virus databases](#) provides the detection of even the newest viruses.



Quarantine

The infected attachments can be moved to **Quarantine**, where the malicious objects are isolated from the rest of the system.

By default, the quarantine is enabled. To disable it, set the value **0** for the **Quarantine enabled** [anti-virus parameter](#). In case quarantine is disabled, the infected objects will be deleted.

The quarantined files can be reviewed and processed using the special utility **Dr.Web Quarantine**. To launch the utility, select **Start -> Programs -> Dr.Web for Kerio WinRoute -> Dr.Web Quarantine**. The list of objects in quarantine will be displayed (see [Figure 1](#)).

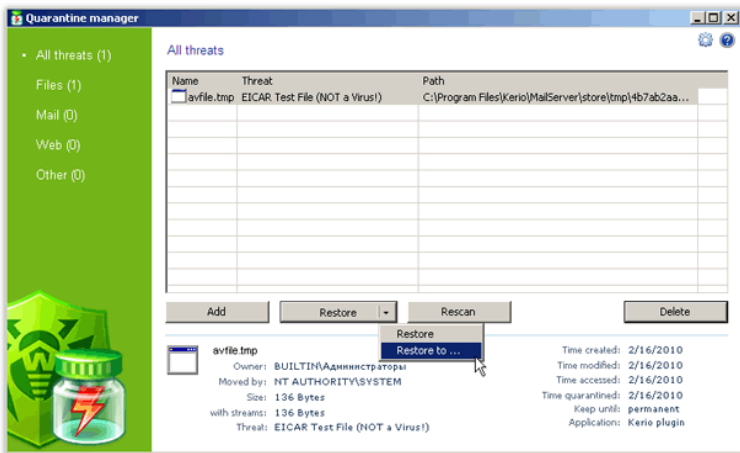


Figure 1. Quarantine

For each object in the list the information on the infected file name and size, the name of the virus and the path to the storage folder is displayed. You can specify the types of the information that is displayed in the list. To do this, right-click any column in the table and select **Customize columns**. Then select the types of the information you want to be displayed.




You can remove the quarantined objects or restore them. To do this:

- Select one or several objects in the list.
- To delete the selected file(s) click the **Delete** button.
- To restore the selected file(s) select **Restore** -> **Restore to** and then specify the folder the file(s) will be restored to.

You can also scan the quarantined objects, e.g. the suspicious files, again, after [updating Dr.Web virus databases](#). To check the files again, click the **Rescan** button.

The **Add** button is used to add files from the local or removable disk to quarantine. Then you can scan these files for viruses. Please take note that in this case the file can be restored to the initial folder only using the **Restore** button.

Quarantine properties

To access to quarantine properties click the **Properties**  button in the top part of the **Quarantine** window. In the **Quarantine properties** window (see [Figure 2](#)) you can specify the following settings:

1. You can set up the quarantine size. To do this, specify the amount of the disk space for the quarantine in the **Set quarantine size** section (see [Figure 2](#)).
2. Before the infected file is cured, its backup is saved in the quarantine to allow restoring the file in case it is corrupted during its curing. To enable viewing backups in quarantine list, select the **show backup files** check box in the **View** section (see [Figure 2](#)).

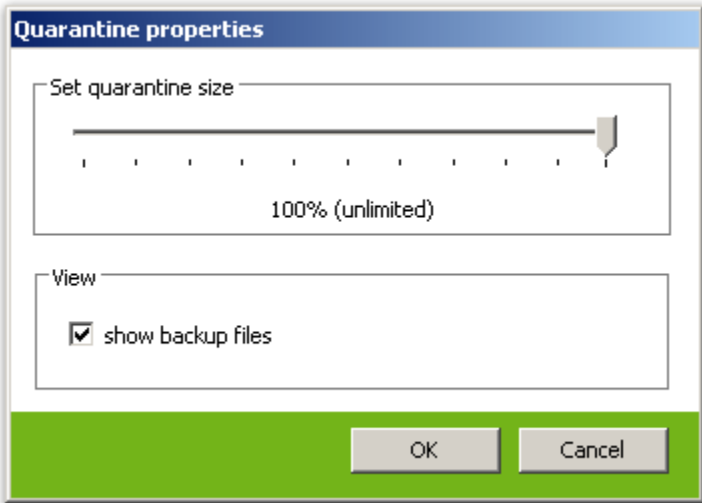


Figure 2. Quarantine properties

The objects in quarantine are saved on the hard disk section the Kerio firewall is installed on. If there is no free space for saving the file or the specified maximum quarantine size is exceeded, the file is not moved to quarantine.



In case Kerio WinRoute versions from 6.2 to 6.7.1 inclusive are used, the cyrillic file names may be displayed incorrectly in logs and quarantine list. If the name of infected file that is moved to **Dr.Web** quarantine contains cyrillic symbols, these symbols are deleted from the file name. However, this error do not influence the messages delivery.



Chapter 6. Web Console

Web Console allows you to view the information on the **Dr.Web for Kerio WinRoute** operation, particularly, on the license and updates, as well as the program statistics via browser (see [Figure 3](#)).

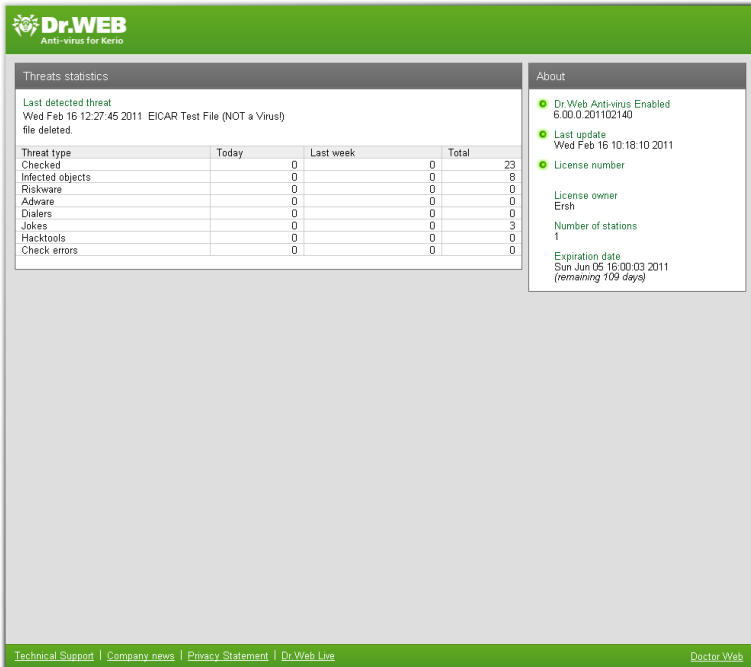


Figure 3. Web console

Access to web console

To access to the web console, enter the IP address and the port of the Kerio firewall in the address bar of the browser (e.g., <http://127.0.0.1:8091>). Port is specified by the **Web console: Port** parameter and may fall into the range from 1024 to 65536. The default value is 8091.



Program Information

The **About** section of web console (see [Figure 3](#)) contains the following information on the program activity, license and virus databases updates:

- Version of the anti-virus engine
- Date and time of the last update of the virus databases
- License number
- Name of the license owner
- Number of the protected stations
- License expiration date

Program Statistics

The program statistics is displayed in the **Threats statistics** section of the web console (see [Figure 3](#)). The following information is compiled in the table of statistics:

- Date and time of the last threat detection and the name of the virus
- Number of checked files and detected threats during different periods of time (the last 24 hours, the last week and all the time since the program installation):
 - Total number of checked objects
 - Number of infected objects
 - Number of detected riskware, adware, dialers, jokes and hacktools
 - Number of errors when checking e-mail attachments

To clear statistics

The statistics is saved in `drw-kerio-stat.dat` file, located in the program installation folder. If the plug-in stops functioning, the statistics for the last 24 hours and for the last week is deleted automatically. To clear the statistics for the whole period of the plug-in operation, you need to delete the `drw-kerio-stat.dat` file.



Chapter 7. Update



The Updater component (drwebupw.exe) may be launched just on the completion of the plug-in installation by selecting the corresponding checkbox at the last step of [installation](#). This component updates the scanning engine (drweb32.dll) and virus databases (*.vdb).

Dr.Web for Kerio WinRoute 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 evolution 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. The Updater component of **Dr.Web for Kerio WinRoute** helps you download the updates via Internet and automatically installs them.




If your computer connects to the Internet via proxy, [configure Updater](#) to connect to the proxy server.

For computers without access to the Internet, you can configure updates from the central storage of update files.

When you install **Dr.Web for Kerio WinRoute**, the installation wizard creates a task which schedules Updater to check for new updates at the **Doctor Web** global update server. You can change the schedule using the standard Windows Scheduled Tasks utility. You can also configure the update process using the command line parameters listed in the [Appendix A](#).



To modify update schedule

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **Dr.Web Update for Kerio WinRoute Plugin**  and select **Properties**.
3. On the **Schedule** tab, modify the task schedule. By default, the plug-in checks for updates each 30 minutes.
4. Click **OK**.


To configure update without Internet connection

1. Create a central storage for the update files.



You can use folder available through UNC paths only, which include:

- Local folder on the computer
 - Shared network folders
-

2. Copy the new updates for plug-in components and virus databases from the **Doctor Web** official download site at <http://download.drweb.com/bases/> to the storage. You can view the list of updatable components in the drweb32.lst file which is located in the installation folder of **Dr.Web for Kerio WinRoute** (usually, %ProgramFiles%\DrWeb for Kerio WinRoute).
3. On the local computer where you want to configure updates from the central storage, open the Control Panel and double-click **Scheduled Tasks**.
4. Right-click **Dr.Web Update for Kerio WinRoute Plugin**  and select **Properties**.
5. On the **Task** tab, add the following command line parameter to the command string in the **Run** field:
/URL:<storage> where <storage> is the path to the central updates storage.
5. Click **OK**.



Chapter 8. Logging

Dr.Web for Kerio WinRoute registers errors and application events in the following logs:

- Windows Event Log
- Debug, error and security protocols of Kerio WinRoute Firewall/Kerio Control
- Text Dr.Web debug log (if the value of the [antivirus parameter](#) Logging: Log level is 1)

By default, the text Dr.Web debug log is stored in the DrWebForKWF.log file in the %ProgramFiles%\DrWeb for Kerio WinRoute\ folder.

The update information is logged in a separate drwebupw.log file, which is located in the %AllUsersProfile%\Application Data\Doctor Web\Logs\ folder.

Event Log

Dr.Web for Kerio WinRoute registers the following information in the Windows Event Log:

- Plug-in starts and stops
- License key file parameters including validity, licensed period (information is registered each time the plug-in checks the license or when the license file changes)
- Parameters of the plug-in components including scanner, core, virus databases (information is registered when the plug-in starts or components are updated)
- License invalidity notifications if the license key file is missing, some of the plug-in components are not licensed, license is blocked or license key file is corrupted (information is registered when the plug-in checks the license.)
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)



To view Event Log

1. On the Control Panel, double-click **Administrative Tools** and then double-click **Event Viewer**.
2. In the tree view, select **Application**.
3. The application Event Log displays in the right pane. The Source for the plug-in events is **Dr.Web for Kerio WinRoute**.

Text Log

Dr.Web for Kerio WinRoute registers the following information in the text log:

- License validity status
- Malware detection reports per each detected malicious object
- Errors while scanning for archives or password-protected files
- Core failures
- License expiration notifications (A message is registered in 30, 15, 7, 3, 2 and 1 days before expiration.)



Enabling the program logging in the Log file decreases server performance, therefore it is recommended to enable logging only in case of errors occurrence in operation of **Dr.Web for Kerio WinRoute**.

The text log file is cyclic. When the log size reaches the maximum (defined by the [option](#) Logging: Max file size (KB), the default is 50000 KB), the plug-in creates a new file and deletes the old one.



Debug Log

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

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**.



Chapter 9. Troubleshooting

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

- [Check installation](#)
- [Check plug-in operation](#)
- [Check Updater module](#)

If the errors are reported and the problems of **Dr.Web for Kerio WinRoute** operation persist, contact [Dr.Web Technical Support](#) for help and assistance. [Collect the full information](#) on the problem to send to the Technical Support with the problem description.

Check Installation

To check whether the plug-in is correctly installed:

1. Ensure that during the plug-in installation the following folders have been created and contain all necessary files:
 - %ProgramFiles%\DrWeb for Kerio WinRoute\

| File name | Description |
|----------------|---|
| drwebupw.exe | Executable file of Updater |
| update.drl | List of URLs for updating |
| drweb32.key | License key file |
| dwqrui.exe | Utility to access to Dr.Web quarantine |
| locale.ini | Localization file |
| drwmsg.dll | Service library |
| WebConsole.exe | Executable file of web console |



- %ProgramFiles%\DrWeb for Kerio WinRoute\html\ with files used by the web console
- %CommonProgramFiles%\Doctor Web\Scanning Engine\

| File name | Description |
|--------------|--------------------------------|
| drweb32.dll | Anti-virus engine |
| dwinctl.dll | - |
| dwengine.exe | Dr.Web Scanning Engine service |

- %AllUsersProfile%\Application Data\Doctor Web\Bases\

| Имя файла | Описание |
|-------------|-------------------------------------|
| *.vdb | Virus databases |
| drweb32.lst | List of files downloaded by Updater |

2. On the Control Panel, double-click **Administrative Tools** and then double-click **Services**. Ensure that the service Dr.Web Scanning Engine (DrWebEngine) is running.
3. [View Event Log](#) and ensure that there is no errors which originate from the application Dr.Web for Kerio WinRoute.
4. In the %ProgramFiles%\DrWeb for Kerio WinRoute\ folder, view the DrWebForkWF.log text log and ensure that it contains no errors.

Check Functionality


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



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. For information on EICAR test virus see http://en.wikipedia.org/wiki/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 WinRoute Firewall/Kerio Control.
2. Send an e-mail with EICAR-Test-File in attachment via server protected by Kerio WinRoute Firewall/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.

To check Updater

1. On the Control Panel, double-click **Scheduled Tasks** and ensure that the **Dr.Web Update for Kerio WinRoute Plugin**  task is created.
2. Check that last update succeeded. The plug-in updates virus databases after installation completes. If update completes successfully, the ERRORLEVEL environment variable is set to 0. Other values indicate an error.
3. In the %AllUsersProfile%\Application Data\Doctor Web\Logs\ folder, view the drwebupw.log update log and ensure that it contains no errors.




Appendices

Appendix A. Updater Command Line Parameters

The Updater can operate in command line mode. You can use parameters to configure the update process.

To configure update task

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **Dr.Web Update for Kerio WinRoute Plugin**  and select **Properties**.
3. In the **Run** field add command line parameters.

Available Parameters

Below is the list of command line parameters which can be used to configure the updating process:

| Parameter | Description |
|--|--|
| /DBG | Sets detailed logging in the %AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log file. |
| /URL:<url> | Specifies location of the updates server. Only UNC-paths are accepted. |
| /USER: <name> | Specifies the user name to use when connecting to the updates server. |
| /PASS: <password> | Specifies the password to use when connecting to the updates server. |



| Parameter | Description |
|------------------------------|---|
| /UPM: <mode> | Configures connection via proxy. You can set one of the following values: <ul style="list-style-type: none">• direct – direct connection without proxy• ieproxy – connection via proxy, system settings are used• userproxy – connection via proxy, user-defined settings are used |
| /PURL: <address> | Specifies location of the proxy server. |
| /PUSER: <name> | Specifies the user name to use when connecting to the proxy server. |
| /PPASS: <password> | Specifies the password to use when connecting to the proxy server. |
| /UA | Sets the Update All mode when Updater downloads all files specified in the updating list regardless of the operating system used and the product components installed. This mode allows you to download all updates from the Doctor Web global update server. This mode cannot be used to update the anti-virus installed on a computer. |
| /ST | Sets the Updater to run in stealth (invisible) mode. |
| /LNG: <filename> | Specifies the language resources file name. The default language is English. |
| /GO | Sets the package operation mode when Updater does not display dialogs. |
| /QU | Sets compulsory closure of Updater after finishing an update regardless of its results. Update result is returned in the ERRORLEVEL environment variable. If update completes successfully, the ERRORLEVEL environment variable is set to 0. Other values indicate an error. |



| Parameter | Description |
|--|--|
| /DIR: <folder> | Specifies the folder where to store the update files. The default is the directory where Updater runs. |
| /URM: <mode> | Sets the Restart mode. In this mode the computer is restarted when update finishes. You can set one of the following values: <ul style="list-style-type: none">• prompt – prompt for reboot if needed• noprompt – reboot without prompting if needed• force – always reboot• disable – disable reboot |
| /REG | Launches Updater to register the product or request a license key file. |
| /UPD | Sets the Usual mode. Use this parameter together with /REG to update the product after completing registration. |
| /UVB | Sets update of virus databases and the core (drweb32.dll) only. This option disables /UA parameter. |
| /RP <file> or /RP+ <file> | Specifies the log file. The default is %AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log. Use /RP+ to append new records to the file. Use /RP to overwrite the file. |
| /INI: <path> | Specifies an alternative configuration file to use. |
| /NI | Sets Updater to ignore parameters specified in the configuration file (drweb32.ini). |
| /NR | Sets Updater to work without logging. |
| /SO | Enables sound notifications on errors. |



Appendix B. Collect Information for Troubleshooting

In case you experience problems while using or installing **Dr.Web for Kerio WinRoute** contact [Dr.Web Technical Support](#).

To help you to fix the problems as soon as possible, please provide to the **Doctor Web** specialists the full information on the problem. You can review the recommendations listed below. This information should be sent with your request to the Technical Support.

Recommendations

1. Save the report file with system information in the .nfo format. To do this:
 - Run the `msinfo32` command from the **Start -> Run** menu.
 - Select **File -> Save**.
 - Enter the file name and click **OK**.
2. Include the full version of Kerio WinRoute/Kerio Control (e.g., 6.7 build 6399). To view the version the firewall do the following:
 - Open the Control Panel and select **Add or Remove Programs**.
 - In the **Add or Remove Programs** window select Kerio WinRoute Firewall/Kerio Control.
 - Click the link **Click here for support information**. A window containing the product information will open. The full product version is also indicated in this window.
3. Save the **Application** and **System** logs in the .evt format. To do this:
 - Run the `eventvwr` command from the **Start -> Run** menu.
 - Right-click the **Application/System** log and select **Save log file as**.
 - Enter the file name and select the **Event Log (.evt)** file type, then click **Save**.



4. If the problem persists, enable the [Dr.Web debug log](#) end reproduce the problem. Then you can disable the debug log. By default, the Dr.Web debug log is created in the %ProgramFiles%\DrWeb for Kerio WinRoute\DrWebForKWF.log folder.
5. Include the Dr.Web update log. To do this:
 - Copy the drwebupw.log file from the %AllUsersProfile%\Application Data\Doctor Web\Logs\ folder.
6. If **Dr.Web for Kerio WinRoute** is installed and operates on a virtual machine, include the full version of the virtualization system and the report file with system information (.nfo) on the host virtual machine.

If you experience problems on the program installation or removal:

1. Include the version of the installation file you experience problems with (e.g., 6.00.0.07120). To view the installation file version do the following:
 - Find the program installation file in Windows Explorer (e.g., drweb-KerioWinRoute-600-windows-nt-x86.exe).
 - Right-click the installation file name end select **Properties**.
 - In the **Properties** window open the **Version** tab and select **Product version**.
2. Verify the digital signature of **Dr.Web for Kerio WinRoute** installation. To do this:
 - Find the program installation file in Windows Explorer (e.g., drweb-KerioWinRoute-600-windows-nt-x86.exe).
 - Right-click the installation file name and select **Properties**.
 - In the **Properties** window open the **Digital signatures** tab, then select the digital signature in the list and click **Details**.
 - The **Digital Signature Details** window should contain an inscription "This digital signature is OK". If this inscription is missing, try to reload the installation file from the **Doctor Web** server and repeat the digital signature verification procedure.



3. Attach the drweb-kerio-setup.log file located in the temporary folder. To do this:
 - Open the temporary folder %Temp% from the **Start** -> **Run** menu and copy the drweb-kerio-setup.log file.
4. Attach the following information on the license key file:
 - Applications, Created and Expired parameters' values. Example:
Applications=Update, Scheduler,
KerioPlugin
Created=2010-01-05 (12:00) UTC
Expires=2010-07-05 (12:00) UTC
 - The [Settings] section. Example:
MailServer=Yes
FileServer=No
InetGateway=No
SpamFilter=No
LotusSpamFilter=No
EmailAddresses=Unlimited
TrafficLimit=Unlimited



Appendix C. Operation in Central Protection Mode

Dr.Web for Kerio WinRoute can operate in the central protection mode in a network managed by **Dr.Web Control Center**. The central protection helps automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one *anti-virus network* which security is monitored and managed from central server (**Dr.Web Control Center**) by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

Solutions for central protection from **Doctor Web** use client-server model (see [Figure 4](#)).

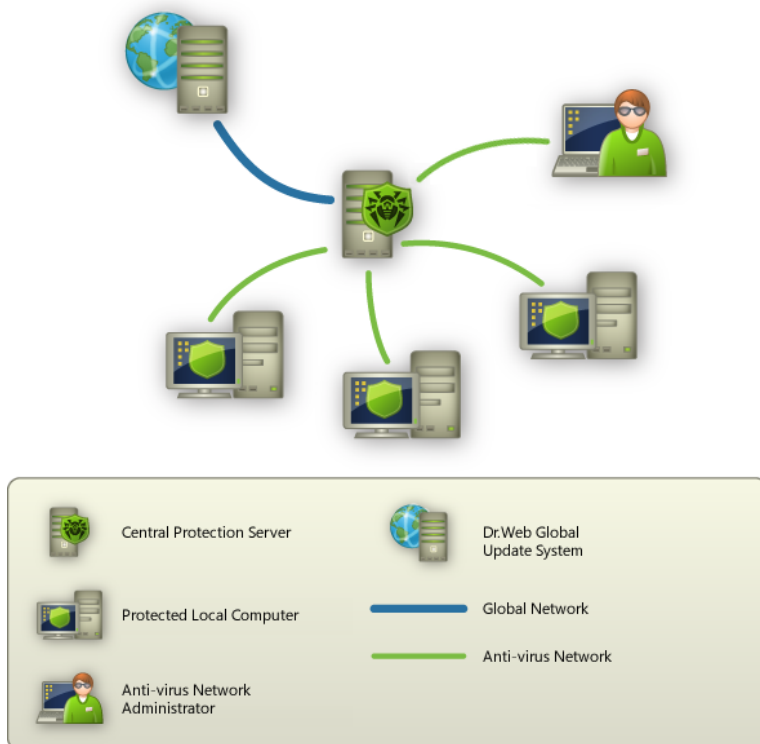
Workstations and servers are protected by *local anti-virus components* (clients; herein, **Dr.Web for Kerio WinRoute**) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.

Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.



Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.



Picture 4. Logical structure of anti-virus networks.



Operation of Dr.Web for Kerio WinRoute in Central Protection Mode

For operation of **Dr.Web for Kerio WinRoute** in central protection mode, version 6 of **Dr.Web Agent** is required to be installed and operate correctly on the same operating system.



The version 6.00.2 of **Dr.Web for Kerio WinRoute** is not compatible with **Dr.Web Agent** of version other than 6.

Dr.Web for Kerio WinRoute operating in the central protection mode provides the following possibilities:

- Recording the start events of Kerio firewall with the installed plug-in **Dr.Web for Kerio WinRoute**. Start events are displayed in the **Start/Stop** table of **Dr.Web Control Center**. The stop event of Kerio firewall is not recorded.
- Sending statistics of **Dr.Web for Kerio WinRoute** operation. The statistics is displayed in the **Statistics** and **Summary statistics** tables of **Dr.Web Control Center**.
- Sending notifications on detected viruses with information on the infections and performed actions. These events are displayed in the **Infection** table of **Dr.Web Control Center**.
- Virus databases and anti-virus engine updates from **Dr.Web Control Center** repositories. This action allow disabling the standard updater of **Dr.Web for Kerio WinRoute** which starts by default according to a schedule. In this case components update starts from **Dr.Web Control Center** repositories according to its schedule.
- Using a license key file for **Dr.Web for Kerio WinRoute** that is registered at anti-virus network. On the start of Kerio firewall with the installed plug-in **Dr.Web for Kerio WinRoute** the license key file for the station in anti-virus network will be used. If this key is invalid, the plug-in will use the local key file stored in the program installation folder.



Index

A

- anti-virus check 27
- appendix 43, 49

C

- central protection 49
- check 41
 - detection methods 28
 - for viruses 27
 - installation 40
 - integration with Kerio WinRoute Firewall 41
 - updater 41
- command line parameters 43
- compatibility 15
- configure 20
 - anti-virus check 21
 - firewall 20
 - internet connection 19
 - logging 21
 - notifications 24
 - proxy 19
 - server parameters 24
 - work with Kerio WinRoute Firewall/Kerio Control 20
- connect to Internet via proxy 19
- contact support 9

D

- debugt log 39

- detection methods 28
- document conventions 8
- Dr.Web for Kerio WinRoute
 - check operation 41
 - install 16
 - main features 6
 - options 21, 24
 - quarantine 30
 - statistics 34
 - uninstall 17
 - update 35
 - web console 33, 34

E

- event log 37

F

- firewall 14

G

- get key file 11

I

- install Dr.Web for Kerio WinRoute 14, 16
 - check 40
- integration 20
 - check 41
- internet connection 19



Index

K

- Kerio Control 14
- Kerio WinRoute Firewall 14
- key file 10
 - format 13
 - get 11
 - parameters 13
 - update 12
 - use 12

L

- license 34
 - get 11
 - update 12
 - use 12
 - validity 10
- license key file
 - update 12
 - validity 10
- licensing 10
 - parameters 13
- logging 37
 - configure 21
- logs 37
 - debug log 39
 - event log 37
 - text log 38

N

- notifications 24

O

- operating system 14
- operation mode 49
- options 20
 - anti-virus 21, 24
 - check 21
 - Dr.Web for Kerio WinRoute 21
 - logging 21
 - notifications 24
 - server 24

P

- protocols 26
- proxy 19

Q

- quarantine 30

R

- requirements 14

S

- scanning
 - configure 20
 - protocols 26
 - settings 26
- statistics 34



Index

support 9
system requirements 14

T

technical support 9
text log 38
troubleshooting 40

U

uninstall Dr.Web for Kerio WinRoute
14, 17
update 35
 check 41
 parameters 43
 virus databases 34
update license 12

V

virus check 27

W

web console 33, 34
 access 33
 license 34
 statistics 34
 update 34

