Dr.WEB®

for Kerio MailServer

Defend what you create

# Administrator Manual

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 MailServer**
**Version 6.00.2**
**Administrator Manual**
**07.03.2013**

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

# 1. Introduction

Thank you for purchasing **Dr.Web for Kerio MailServer**. This product is an anti-virus plug-in designed to protect corporate mail systems against viruses. The plug-in integrates into Kerio mail servers and checks the attached files of e-mails.

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

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

## Main Features

**Dr.Web for Kerio MailServer** performs the following functions:

- The anti-virus check of e-mail attachments according to Kerio mail server rules
- Malware detection
- Isolation of the infected objects in Dr.Web quarantine
- Heuristic analysis for additional protection against unknown viruses
- Fast and efficient check
- Automatic update of virus databases

This guide helps administrators of corporative networks which use Kerio mail server to install and configure **Dr.Web for Kerio MailServer**.

For detailed information on Kerio mail servers settings and mail checks, see Kerio official web site at http://www.kerio.com/kms_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. |
| Green and underlined | Hyperlinks to topics and web pages. |
| `Monospace` | Code examples, input to the command line and application output. |
| *Italic* | Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values.<br>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-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.

# 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
- Possibility to use the license on mail servers
- 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 MailServer** stops detecting the malicious programs. If the key file became invalid during the operation of Kerio mail server then the server stops delivering the e-mails to the recipients. The delivery without check for viruses can be restored by disabling the use of **Dr.Web for Kerio MailServer**. For restoration of the mail anti-virus check the correct key file is required.

License violation is registered in the system 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 mail server is installed and the installation of **Dr.Web for Kerio MailServer** is planned or has been already completed.

For demonstrative purposes you may be provided with a *trial license key file*. Trial license allows you to access full functionality of the **Dr.Web for Kerio MailServer** 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 MailServer** supports hot license update without stopping or reinstalling the plug-in.

### To update the license key file

1. To update the license key file, do one of the following:
   - Replace an old license key file with the new one in the folder specified by `LicenseFile` parameter located in `[StandaloneMode]` section of `/etc/drweb/agent.conf` configuration file.
   - Specify the path to the new key file as the value of `LicenseFile` parameter located in `[StandaloneMode]` section of `/etc/drweb/agent.conf` configuration file.

   Note that the path to file is case sensitive, e.g., the paths /opt/drweb/ and /opt/DrWeb/ are different.

2. Enable the use of the new key file by the following command:

   ```
   /etc/init.d/drweb-monitor reload
   ```

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

# Use License Key File

For operation of **Dr.Web for Kerio MailServer** a license key file is required, the path to the key file can be defined by `LicenseFile` parameter located in `[StandaloneMode]` section of `/etc/drweb/agent.conf` configuration file.

The value of `LicenseFile` parameter located in `[StandaloneMode]` section of `/etc/drweb/agent.conf` configuration file can contain several paths to different key files, The paths should be separated by commas.

During the operation of **Dr.Web for Kerio MailServer** the plug-in searches for the first valid key file in the folder specified by one of the values of `LicenseFile` parameter located in `[StandaloneMode]` section of the configuration file `/etc/drweb/agent.conf`. 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.

## To change license key file location

1. To change the path to the key file, specify the new path as the value of `LicenseFile` parameter located in `[StandaloneMode]` section of program configuration file `/etc/drweb/agent.conf`.

   Note that the path to file is case sensitive.

2. To start using the key file located by the specified path, use the following command:

```
/etc/init.d/drweb-monitor reload
```

# Licensing Parameters

The license key file regulates the use of **Dr.Web for Kerio MailServer**.

## To view license details

1. View the license key file.

> 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.<br>To use the key with **Dr.Web for Kerio MailServer** the component KerioPlugin should be in the list determined by this parameter.<br>If the license key is used both for anti-virus daemon **drwebd** and for **Dr.Web for Kerio MailServer**, then the components MailDaemonUnix and FileDaemonUnix should be also included in the list. |

| Parameter | Description |
|---|---|
| `[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.<br>⚠ If the key file is used with **Dr. Web for Kerio MailServer**, the value of this parameter should be **Yes**, otherwise the key will be considered as invalid. |

3. Close the file without saving.

# 3. Installation and Removal

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

**Dr.Web for Kerio MailServer** is distributed as a single self-extracting archive **drweb-kerio_6.0.2.*[patch]*-*[build]*~linux_x86.run** archive (where *[patch]* is the number of patch, *[build]* is the number of program build, e.g., drweb-kerio_6.0.2.0-1109201904~linux_x86.run) and can be installed using GUI installer or via console. The archive contains the following packets (see Table 3):

**Table 3. Packets included into the application installation archive.**

| Name | Description |
|---|---|
| drweb-common | Contains:<br>• Main configuration file `drweb32.ini`<br>• Libraries<br>• Documentation<br>• Directory structure<br>When this packet is installed, it creates:<br>• **drweb** user<br>• **drweb** group |
| drweb-bases | Contains:<br>• Anti-virus scanning engine<br>• Virus databases (vdb)<br>Requires the drweb-common packet for installation. |
| drweb-updater | Contains the updater of the anti-virus scanning engine and virus databases.<br>Requires the drweb-common packet for installation. |

| Name | Description |
|---|---|
| drweb-daemon | Contains the **Dr.Web Daemon** executable files and documentation.<br>Requires drweb-bases for installation. |
| drweb-scanner | Contains the **Dr.Web Scanner** executable files and documentation.<br>Requires drweb-bases for installation. |
| drweb-kerio-plugin6 | Contains the avir_drweb.so library of anti-virus application **Dr.Web for Kerio MailServer**. Suitable for installation and operation with Kerio MailServer of version 6.x.x. |
| drweb-kerio-plugin7 | Contains the avir_drweb.so library of anti-virus application **Dr.Web for Kerio MailServer**. Suitable for installation and operation with Kerio Connect of version 7.x.x. |
| drweb-kerio-plugin-doc | Contains the **Dr.Web for Kerio MailServer** documentation. |
| drweb-agent | Contains the executable files, libraries and documentation of **Dr.Web Agent**.<br>Requires drweb-boost144 and drweb-common packets for installation. |
| drweb-boost144 | Contains the libraries that are used by **Dr.Web Agent**.<br>Requires drweb-libs packet for installation. |
| drweb-libs | Contains the common libraries for product components. |
| drweb-epm6.0.0-libs | Contains the libraries for graphic installer and uninstaller.<br>Requires drweb-libs packet for installation. |
| drweb-epm6.0.0-uninst | Contains the files of the graphic uninstaller.<br>Requires drweb-epm6.0.0-libs packet for installation. |

| Name | Description |
|---|---|
| drweb-monitor | Contains the executable files, libraries and documentation of **Dr.Web Monitor**.<br>Requires drweb-boost144 and drweb-common packets for installation. |

# System Requirements

Before beginning installation, review the following system requirements and instructions (Table 4):

**Table 4. System Requirements**

| Component | Requirement |
|---|---|
| Disk space | Minimum 290 MB of disk space |
| Operating system | One of the following:<br>• Red Hat 9.0<br>• Red Hat Enterprise Linux 4/5<br>• Fedora Core 7 / 8<br>• SUSE Linux 10.0, 10.1, 10.2, 10.3, 11.0 и 11.1<br>• CentOS Linux 5.2 и 5.3<br>• Debian 5.0<br>• Ubuntu 8.04 LTS |
| Mail server | If you're installing **Dr.Web for Kerio MailServer** for the first time, the following versions of the mail server can be used:<br>• Kerio MailServer 6.2 or higher<br>• Kerio Connect, versions from 7.0.0 to 7.4.3<br>If **Dr.Web for Kerio MailServer** is already installed on your computer, the mail server can be updated up to Kerio Connect 8.0. **Dr.Web for Kerio MailServer** will be operating correctly without any additional actions. |

| Component | Requirement |
|---|---|
| Additional software | **Dr.Web Agent** 6.0 or higher (for operation in central protection mode) |

⚠ The operation of **Dr.Web for Kerio MailServer** and particularly of the anti-virus daemon **drwebd** requires disabling the Security-Enhanced Linux system.

This section reflects requirements for the **Dr.Web for Kerio MailServer** only. See Kerio guides for mail server requirements. **Dr.Web for Kerio MailServer** operates successfully on computers which meet the Kerio mail server requirements.

**Dr.Web for Kerio MailServer** supports installation and operation in Kerio MailServer VMware Virtual Appliance. For information on this environment see company's official web site at http://www.kerio.com/mailserver.

# Program Components

**Dr.Web for Kerio MailServer** 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:

- **Anti-virus daemon** (**drwebd**) is used to perform anti-virus scanning.
- **Console scanner** (file to launch is `/opt/drweb/drweb`) detects and cures the viruses while checking the files on the local computer, including shared directories. It is launched by schedule or manually and performs the predefined actions to the infected and suspicious objects.

- **Updater** (`update.pl`) is a Perl script included into **Dr.Web for Kerio MailServer** anti-virus package. It is designed to automatically update the virus databases. Updater downloads the copies of the virus databases via Interner or from a local network folder or server.
- **Dr.Web Monitor** (file to launch is `/opt/drweb/drweb-monitor`) is a resident component which controls the fault-safety of the whole anti-virus system. It provides the correct starts and stops of the anti-virus modules and their components as well as the restarts in case of their failure.
- **Dr.Web Agent** is a component which constantly resides in the memory and sends the configuration parameters to other components. **Dr.Web Agent** also controls the anti-virus check politics which is subject to active **Dr.Web** license.
- **Web console** is used to view via browser the information on Dr.Web for Kerio MailServer operation, more specifically, on the license, updates and statistics of the plug-in.

# Install Plug-in

Before beginning installation, review the system requirements.

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

## Using the GUI Installer

To install **Dr.Web for Kerio MailServer**, do the following:

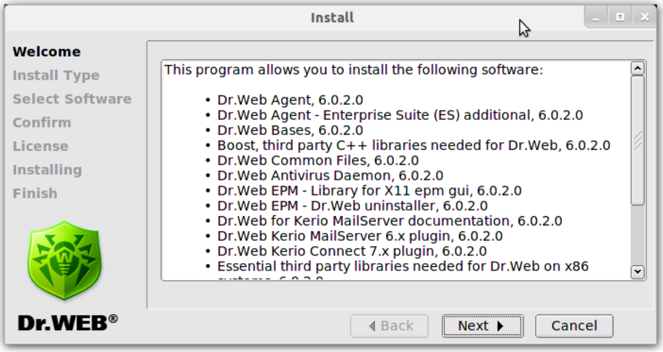
1. Allow execution of the **drweb-kerio_6.0.2.*[patch]*-*[build]*~linux_x86.run** archive (where *[patch]* is the number of patch, *[build]* is the number of program build, e.g., drweb-kerio_6.0.2.0-1109201904~linux_x86.run). You can use the following command:

   ```
   #    chmod    +x    drweb-kerio_6.0.2.[patch]-[build]
   ~linux_x86.run
   ```

2. Execute the file by the command:

   ```
   # ./drweb-kerio_6.0.2.[patch]-[build]~linux_x86.run
   ```

3. The drweb-kerio_6.0.2.[patch]-[build]~linux_x86 directory will be created. This directory contains a set of installation files. Then the GUI installer will start (see Figure 1).



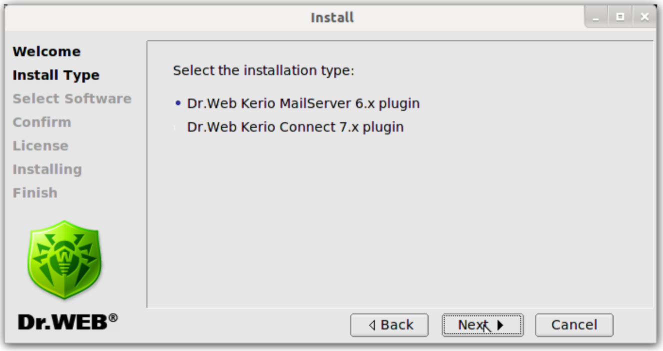
This program allows you to install the following software:

- Dr.Web Agent, 6.0.2.0
- Dr.Web Agent - Enterprise Suite (ES) additional, 6.0.2.0
- Dr.Web Bases, 6.0.2.0
- Boost, third party C++ libraries needed for Dr.Web, 6.0.2.0
- Dr.Web Common Files, 6.0.2.0
- Dr.Web Antivirus Daemon, 6.0.2.0
- Dr.Web EPM - Library for X11 epm gui, 6.0.2.0
- Dr.Web EPM - Dr.Web uninstaller, 6.0.2.0
- Dr.Web for Kerio MailServer documentation, 6.0.2.0
- Dr.Web Kerio MailServer 6.x plugin, 6.0.2.0
- Dr.Web Kerio Connect 7.x plugin, 6.0.2.0
- Essential third party libraries needed for Dr.Web on x86

**Figure 1. GUI installer welcome page**

To navigate between installation pages, use the **Back** and **Next** buttons. To cancel the installation, click **Cancel** on any step.

4. On the **Install type** page (see Figure 2), select the installation package depending on the Kerio mail server version. Click **Next**.



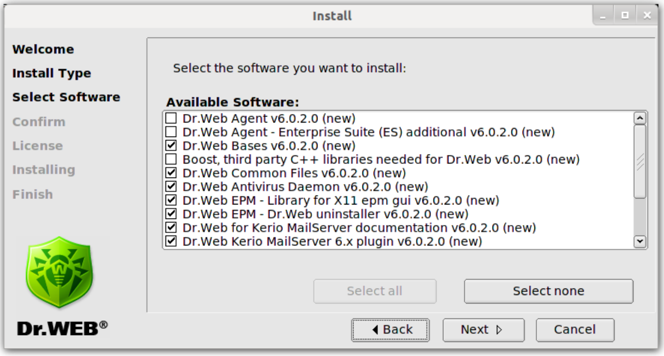
Select the installation type:

● Dr.Web Kerio MailServer 6.x plugin

○ Dr.Web Kerio Connect 7.x plugin

**Figure 2. Installation package type selection**

5. On the **Select Software** page (see Figure 3), select the components to install.



Select the software you want to install:

**Available Software:**

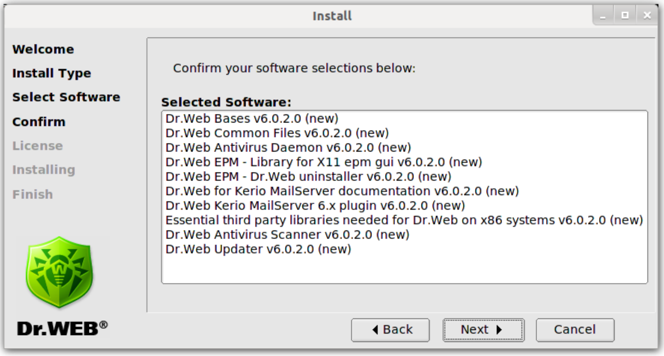
☐ Dr.Web Agent v6.0.2.0 (new)
☐ Dr.Web Agent - Enterprise Suite (ES) additional v6.0.2.0 (new)
☑ Dr.Web Bases v6.0.2.0 (new)
☐ Boost, third party C++ libraries needed for Dr.Web v6.0.2.0 (new)
☑ Dr.Web Common Files v6.0.2.0 (new)
☑ Dr.Web Antivirus Daemon v6.0.2.0 (new)
☑ Dr.Web EPM - Library for X11 epm gui v6.0.2.0 (new)
☑ Dr.Web EPM - Dr.Web uninstaller v6.0.2.0 (new)
☑ Dr.Web for Kerio MailServer documentation v6.0.2.0 (new)
☑ Dr.Web Kerio MailServer 6.x plugin v6.0.2.0 (new)

**Figure 3. Select components to install**

If the installation of a component requires other components to be previously installed, all corresponding dependencies are selected for installation automatically. For example, if you select to install **Dr.Web Antivirus Daemon**, then **Dr.Web Bases** and **Dr.Web Common Files** are selected and installed automatically.

To select all components, click **Select all**. To clear all check boxes, click **Select none**. Click **Next** when you are done with selecting components to install.

6. On the **Confirm** page (see Figure 4), review the list of selected components and confirm their installation by clicking **Next**.



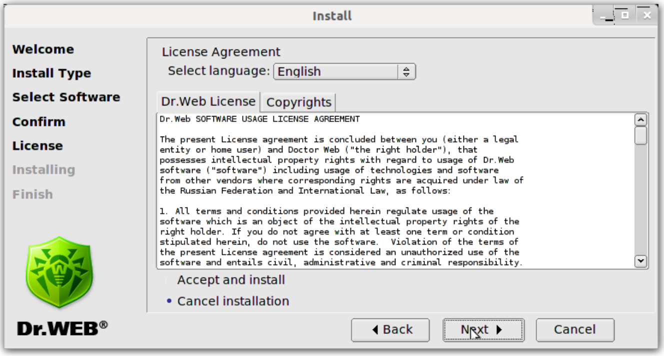
Confirm your software selections below:

**Selected Software:**

```
Dr.Web Bases v6.0.2.0 (new)
Dr.Web Common Files v6.0.2.0 (new)
Dr.Web Antivirus Daemon v6.0.2.0 (new)
Dr.Web EPM - Library for X11 epm gui v6.0.2.0 (new)
Dr.Web EPM - Dr.Web uninstaller v6.0.2.0 (new)
Dr.Web for Kerio MailServer documentation v6.0.2.0 (new)
Dr.Web Kerio MailServer 6.x plugin v6.0.2.0 (new)
Essential third party libraries needed for Dr.Web on x86 systems v6.0.2.0 (new)
Dr.Web Antivirus Scanner v6.0.2.0 (new)
Dr.Web Updater v6.0.2.0 (new)
```

**Figure 4. Confirmation of the components installation**

7. On the **License** page (see Figure 5), read the License Agreement (you can select the License Agreement language in the **Select language** list). Further installation requires the License Agreement acceptance. Click **Next**.



License Agreement

Select language: English

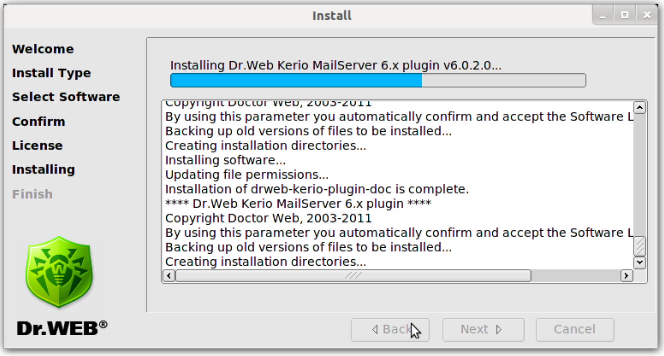
```
Dr.Web SOFTWARE USAGE LICENSE AGREEMENT

The present License agreement is concluded between you (either a legal
entity or home user) and Doctor Web ("the right holder"), that
possesses intellectual property rights with regard to usage of Dr.Web
software ("software") including usage of technologies and software
from other vendors where corresponding rights are acquired under law of
the Russian Federation and International Law, as follows:

1.  All terms and conditions provided herein regulate usage of the
software which is an object of the intellectual property rights of the
right holder. If you do not agree with at least one term or condition
stipulated herein, do not use the software.  Violation of the terms of
the present License agreement is considered an unauthorized use of the
software and entails civil, administrative and criminal responsibility.
```

○ Accept and install

● Cancel installation

**Figure 5. License Agreement**

8. The installation of **Dr.Web for Kerio MailServer** starts. The installation report is shown in the **Installing** window (see Figure 6) in the real-time mode.



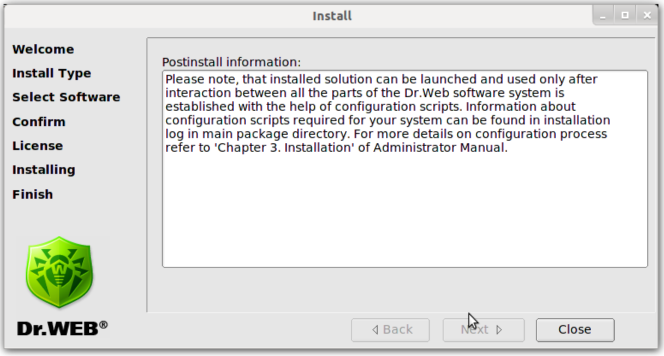
Installing Dr.Web Kerio MailServer 6.x plugin v6.0.2.0...

```
Copyright Doctor Web, 2003-2011
By using this parameter you automatically confirm and accept the Software L
Backing up old versions of files to be installed...
Creating installation directories...
Installing software...
Updating file permissions...
Installation of drweb-kerio-plugin-doc is complete.
**** Dr.Web Kerio MailServer 6.x plugin ****
Copyright Doctor Web, 2003-2011
By using this parameter you automatically confirm and accept the Software L
Backing up old versions of files to be installed...
Creating installation directories...
```

**Figure 6. Installation progress window**

9. If the program is successfully installed, the **Installation complete** notification opens. Then you can agree to configure the program components. The following actions will be performed:
   - The program license key file will be copied to the `/opt/drweb` directory
   - The path to the key file will be written to **Dr.Web Agent** and daemon (**drwebd**) configuration files
   - The automatic launch will be configured for **Dr.Web Monitor** and **drwebd**
   - **Dr.Web Monitor**, **drwebd** and **drweb-kerio-webstatd** daemons will be launched

10. On the **Finish** page (see Figure 7), click **Close** to exit the GUI installer.



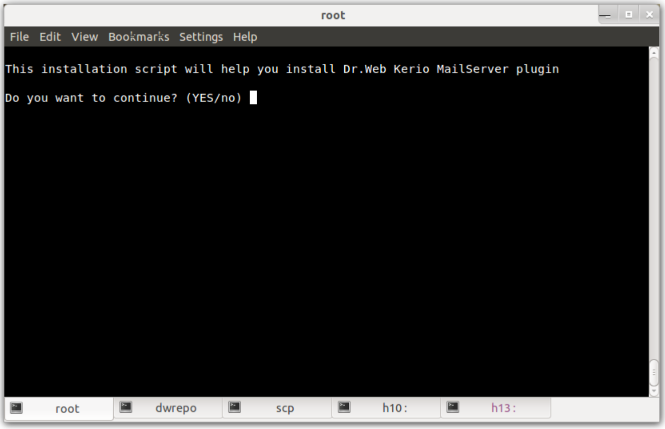
Postinstall information:

Please note, that installed solution can be launched and used only after interaction between all the parts of the Dr.Web software system is established with the help of configuration scripts. Information about configuration scripts required for your system can be found in installation log in main package directory. For more details on configuration process refer to 'Chapter 3. Installation' of Administrator Manual.

**Figure 7. Installation finish window**

## Installation Using the Console

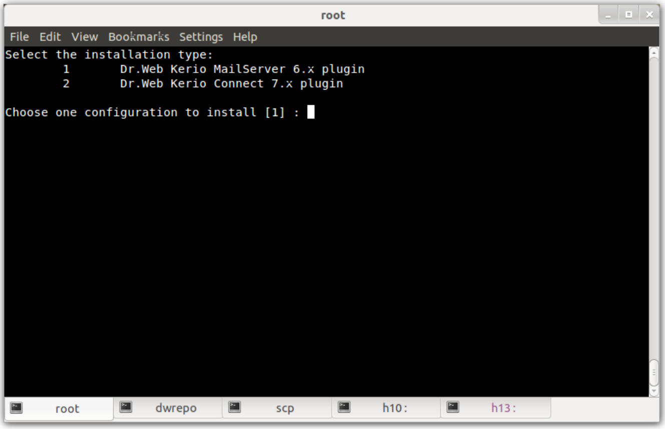
**Dr.Web for Kerio MailServer** can be installed without use of GUI installer. Usually, console installer(see Figure 8) starts automatically is graphical installer fails to start.



```
This installation script will help you install Dr.Web Kerio MailServer plugin

Do you want to continue? (YES/no)
```

**Figure 8. Program installation from the console**

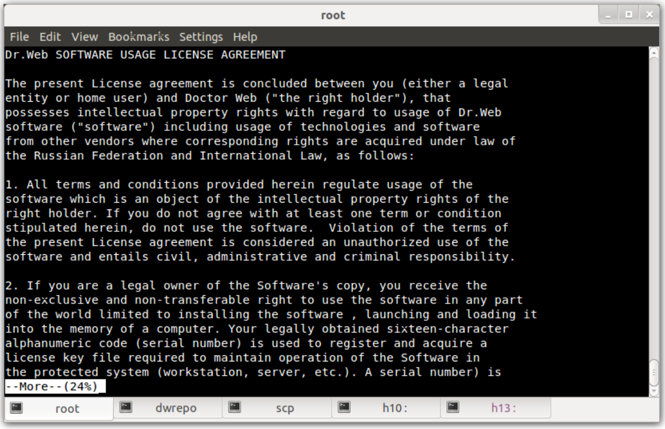
1. To proceed with **Dr.Web for Kerio MailServer** installation, enter `Y` or `Yes` (values are case insensitive), otherwise type `N` or `No`. Press ENTER.
2. Then select the installation package depending on the Kerio mail server version you are using (see Figure 9). Enter the number of the corresponding package and press ENTER.



```
Select the installation type:
        1       Dr.Web Kerio MailServer 6.x plugin
        2       Dr.Web Kerio Connect 7.x plugin

Choose one configuration to install [1] :
```

**Figure 9. Installation package selection**

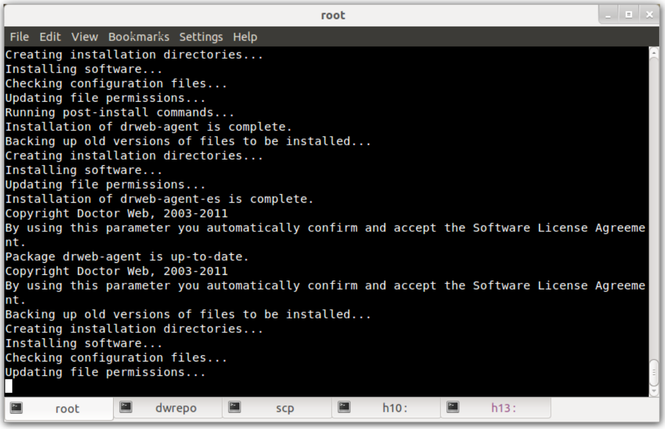
3. Read carefully the License Agreement (see Figure 10). To scroll the text, press SPACEBAR. Further installation requires the License Agreement acceptance. Enter `Y` or `Yes` and press ENTER. Otherwise the installation is canceled.



```
Dr.Web SOFTWARE USAGE LICENSE AGREEMENT

The present License agreement is concluded between you (either a legal
entity or home user) and Doctor Web ("the right holder"), that
possesses intellectual property rights with regard to usage of Dr.Web
software ("software") including usage of technologies and software
from other vendors where corresponding rights are acquired under law of
the Russian Federation and International Law, as follows:

1. All terms and conditions provided herein regulate usage of the
software which is an object of the intellectual property rights of the
right holder. If you do not agree with at least one term or condition
stipulated herein, do not use the software.  Violation of the terms of
the present License agreement is considered an unauthorized use of the
software and entails civil, administrative and criminal responsibility.

2. If you are a legal owner of the Software's copy, you receive the
non-exclusive and non-transferable right to use the software in any part
of the world limited to installing the software , launching and loading it
into the memory of a computer. Your legally obtained sixteen-character
alphanumeric code (serial number) is used to register and acquire a
license key file required to maintain operation of the Software in
the protected system (workstation, server, etc.). A serial number) is
--More--(24%)
```

**Figure 10. License Agreement**

4. The installation of **Dr.Web for Kerio MailServer** starts. The installation progress report is shown on the screen in the real-time mode (see Figure 11).



```
Creating installation directories...
Installing software...
Checking configuration files...
Updating file permissions...
Running post-install commands...
Installation of drweb-agent is complete.
Backing up old versions of files to be installed...
Creating installation directories...
Installing software...
Updating file permissions...
Installation of drweb-agent-es is complete.
Copyright Doctor Web, 2003-2011
By using this parameter you automatically confirm and accept the Software License Agreeme
nt.
Package drweb-agent is up-to-date.
Copyright Doctor Web, 2003-2011
By using this parameter you automatically confirm and accept the Software License Agreeme
nt.
Backing up old versions of files to be installed...
Creating installation directories...
Installing software...
Checking configuration files...
Updating file permissions...
```

**Figure 11. Installation progress**

5. Then you can agree to configure the program components. The following actions will be performed:
   - The program license key file will be copied to the `/opt/drweb` directory
   - The path to the key file will be written to **Dr.Web Agent** and daemon (**drwebd**) configuration files
   - The automatic launch will be configured for **Dr.Web Monitor** and **drwebd**
   - **Dr.Web Monitor**, **drwebd** and **drweb-kerio-webstatd** daemons will be launched
6. The message informing about the installation completion will open.

# Uninstall Plug-in

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

Before uninstalling the plug-in disable the use of anti-virus **Dr.Web for Kerio MailServer** by Kerio mail server. To do this:

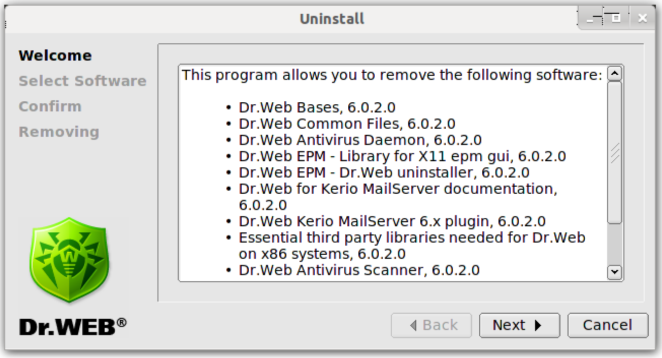
- Launch the **Administration Console for Kerio MailServer**.
- Open the **Configuration** -> **Content Filter** -> **Antivirus** section.
- In the **Antivirus usage** group clear the checkbox **Use external antivirus** for selected anti-virus **Dr.Web for Kerio MailServer**.
- Click **Apply** to disable the use of **Dr.Web for Kerio MailServer**.

The license key is not deleted by default. You have to delete the key file manually.

## Using the GUI Uninstaller

To remove **Dr.Web for Kerio MailServer**, do the following:

1. Launch the GUI uninstaller (see Figure 12) using the command `# /opt/drweb/remove.sh`.



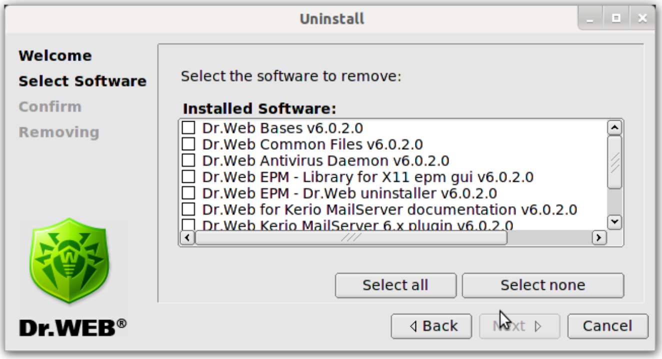
This program allows you to remove the following software:

- Dr.Web Bases, 6.0.2.0
- Dr.Web Common Files, 6.0.2.0
- Dr.Web Antivirus Daemon, 6.0.2.0
- Dr.Web EPM - Library for X11 epm gui, 6.0.2.0
- Dr.Web EPM - Dr.Web uninstaller, 6.0.2.0
- Dr.Web for Kerio MailServer documentation, 6.0.2.0
- Dr.Web Kerio MailServer 6.x plugin, 6.0.2.0
- Essential third party libraries needed for Dr.Web on x86 systems, 6.0.2.0
- Dr.Web Antivirus Scanner, 6.0.2.0

**Figure 12. Graphic uninstaller welcome page**

   To navigate between uninstall pages, use the **Back** and **Next** buttons. To cancel the program removal, click **Cancel** on any step.

2. On the **Select Software** page (see Figure 13), select the components to remove by selecting the corresponding check boxes. The check boxes for the dependant components will be selected automatically.



Uninstall

Welcome
Select Software
Confirm
Removing

Select the software to remove:

**Installed Software:**

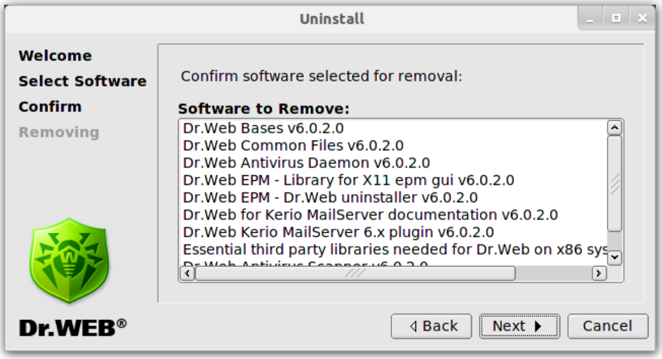
- □ Dr.Web Bases v6.0.2.0
- □ Dr.Web Common Files v6.0.2.0
- □ Dr.Web Antivirus Daemon v6.0.2.0
- □ Dr.Web EPM - Library for X11 epm gui v6.0.2.0
- □ Dr.Web EPM - Dr.Web uninstaller v6.0.2.0
- □ Dr.Web for Kerio MailServer documentation v6.0.2.0
- □ Dr.Web Kerio MailServer 6.x plugin v6.0.2.0

**Figure 13. Select components to remove**

If you installed **Dr.Web for Kerio MailServer** solution on a computer with another **Dr.Web** product installed, then setup lists all **Dr.Web** modules for both **Dr.Web for Kerio MailServer** and the old product. Please, pay attention to the actions you perform and selections you make to avoid accidental removal of the useful components.

To select all components, click **Select all**. To clear the check boxes of all the selected components, click **Select none**. Click **Next** when you are done with selecting components.

3. On the **Confirm** page (see Figure 14), review the list of the selected components and confirm their removal by clicking **Next**.



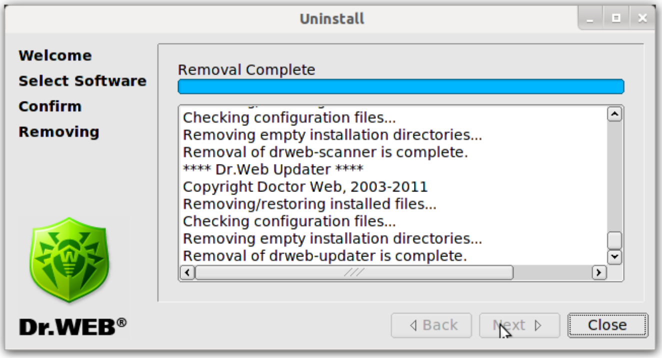
Confirm software selected for removal:

**Software to Remove:**

```
Dr.Web Bases v6.0.2.0
Dr.Web Common Files v6.0.2.0
Dr.Web Antivirus Daemon v6.0.2.0
Dr.Web EPM - Library for X11 epm gui v6.0.2.0
Dr.Web EPM - Dr.Web uninstaller v6.0.2.0
Dr.Web for Kerio MailServer documentation v6.0.2.0
Dr.Web Kerio MailServer 6.x plugin v6.0.2.0
Essential third party libraries needed for Dr.Web on x86 sys
Dr.Web Antivirus Scanner v6.0.2.0
```

**Figure 14. Confirmation of the selected components uninstall**

4. The removal process starts. **Dr.Web for Kerio MailServer**. The progress report is shown in the **Removing** window (see Figure 15) in the real-time mode.



Removal Complete

```
Checking configuration files...
Removing empty installation directories...
Removal of drweb-scanner is complete.
**** Dr.Web Updater ****
Copyright Doctor Web, 2003-2011
Removing/restoring installed files...
Checking configuration files...
Removing empty installation directories...
Removal of drweb-updater is complete.
```

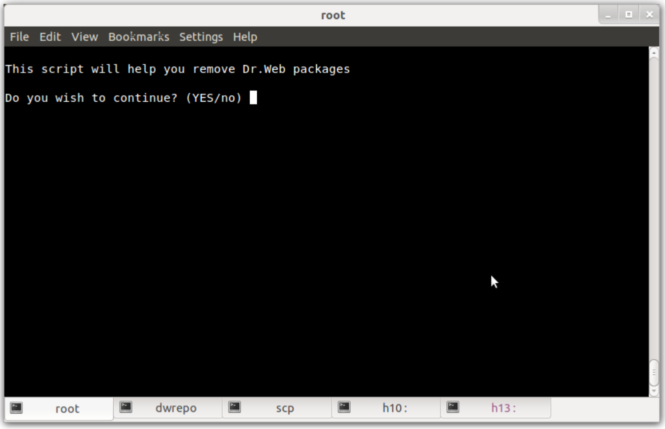
**Figure 15. Removal progress**

On removal completion click **Close** to exit the uninstaller.

## Uninstall Using the Console

To delete **Dr.Web for Kerio MailServer** without use of GUI uninstaller, do the following:

1. Execute the command `# /opt/drweb/remove.sh`. The console uninstaller (see Figure 16) launches automatically id the GUI installer fails to start.

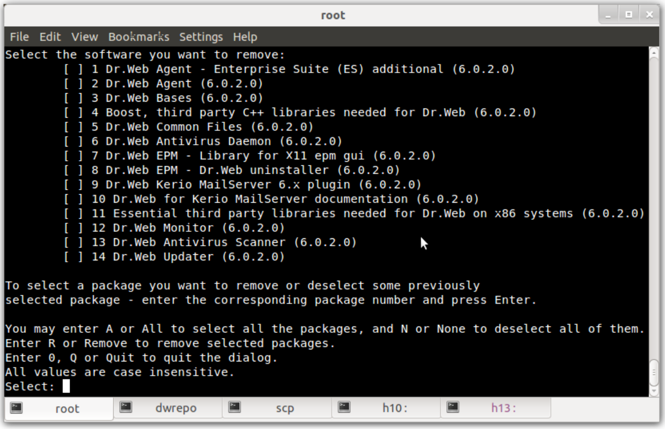


```
This script will help you remove Dr.Web packages

Do you wish to continue? (YES/no)
```

**Figure 16. Program removal from the console**

To continue **Dr.Web for Kerio MailServer** removal, enter `Y` or `Yes` (values are case insensitive) and press ENTER. Otherwise enter `N` or `No`.

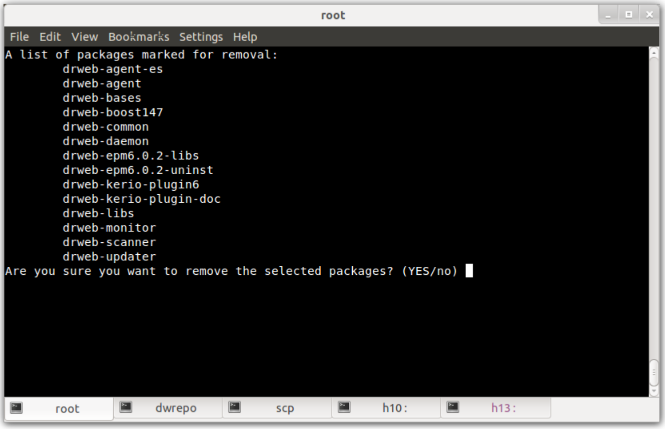
2. On the next step (see Figure 17), select the program components you would like to remove (follow the instructions on the screen).



```
Select the software you want to remove:
        [ ] 1 Dr.Web Agent - Enterprise Suite (ES) additional (6.0.2.0)
        [ ] 2 Dr.Web Agent (6.0.2.0)
        [ ] 3 Dr.Web Bases (6.0.2.0)
        [ ] 4 Boost, third party C++ libraries needed for Dr.Web (6.0.2.0)
        [ ] 5 Dr.Web Common Files (6.0.2.0)
        [ ] 6 Dr.Web Antivirus Daemon (6.0.2.0)
        [ ] 7 Dr.Web EPM - Library for X11 epm gui (6.0.2.0)
        [ ] 8 Dr.Web EPM - Dr.Web uninstaller (6.0.2.0)
        [ ] 9 Dr.Web Kerio MailServer 6.x plugin (6.0.2.0)
        [ ] 10 Dr.Web for Kerio MailServer documentation (6.0.2.0)
        [ ] 11 Essential third party libraries needed for Dr.Web on x86 systems (6.0.2.0)
        [ ] 12 Dr.Web Monitor (6.0.2.0)
        [ ] 13 Dr.Web Antivirus Scanner (6.0.2.0)
        [ ] 14 Dr.Web Updater (6.0.2.0)

To select a package you want to remove or deselect some previously
selected package - enter the corresponding package number and press Enter.

You may enter A or All to select all the packages, and N or None to deselect all of them.
Enter R or Remove to remove selected packages.
Enter 0, Q or Quit to quit the dialog.
All values are case insensitive.
Select: 
```

**Figure 17. Select the program components to remove**

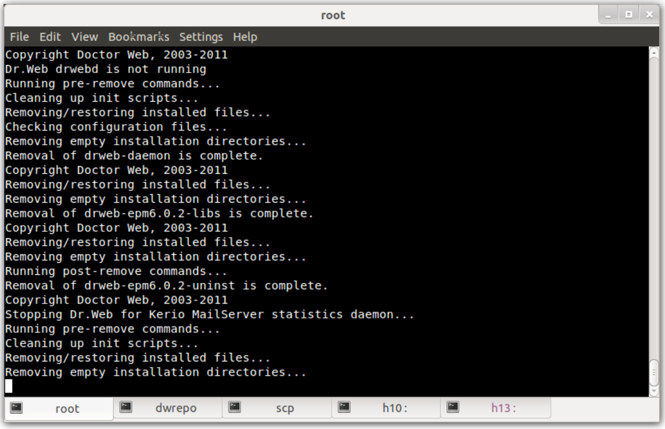
3. Confirm the removal of the selected components (see Figure 18). Enter `Y` or `Yes` (values are case insensitive) and press ENTER.



```
A list of packages marked for removal:
        drweb-agent-es
        drweb-agent
        drweb-bases
        drweb-boost147
        drweb-common
        drweb-daemon
        drweb-epm6.0.2-libs
        drweb-epm6.0.2-uninst
        drweb-kerio-plugin6
        drweb-kerio-plugin-doc
        drweb-libs
        drweb-monitor
        drweb-scanner
        drweb-updater
Are you sure you want to remove the selected packages? (YES/no) 
```

**Figure 18. Confirmation of the removal of the selected components**

4. The removal of the selected components starts. The report on the removal progress is shown on the screen in the real-time mode (see Figure 19).



```
Copyright Doctor Web, 2003-2011
Dr.Web drwebd is not running
Running pre-remove commands...
Cleaning up init scripts...
Removing/restoring installed files...
Checking configuration files...
Removing empty installation directories...
Removal of drweb-daemon is complete.
Copyright Doctor Web, 2003-2011
Removing/restoring installed files...
Removing empty installation directories...
Removal of drweb-epm6.0.2-libs is complete.
Copyright Doctor Web, 2003-2011
Removing/restoring installed files...
Removing empty installation directories...
Running post-remove commands...
Removal of drweb-epm6.0.2-uninst is complete.
Copyright Doctor Web, 2003-2011
Stopping Dr.Web for Kerio MailServer statistics daemon...
Running pre-remove commands...
Cleaning up init scripts...
Removing/restoring installed files...
Removing empty installation directories...
```

**Figure 19. Program components removal progress**

5. The message informing about the removal completion will open.

# Install and Uninstall from Native Packages

You can install **Dr.Web for Kerio MailServer** from native packages for common Linux distributions.

Installation from native packages can be performed only for Kerio Connect 7.0 or higher version.

All packages are located in the **Dr.Web** official repository http://officeshield.drweb.com/drweb/. Once you have added the repository to the package manager of your system, you can install, update or remove necessary packages like any other program from repository. All dependencies will be resolved automatically.

After installing from repository, automatic post-install script for installing license key file will not be initiated. Licence key file must be copied manually. You need to restart all **Dr.Web** services after updating from repository for the updates to take effect.

Below you can find the detailed instructions on how to add **Dr.Web** repository to supported package managers and install **Dr.Web for Kerio MailServer** using console.

All commands for adding repositories, importing keys, installing and removing packages described below must be ran with administrator (root) privileges.

## Debian, Ubuntu (apt)

1. Debian repository is signed by the digital key. For correct operation you need to import the key using on of the following commands:

   ```
   wget -O - http://officeshield.drweb.com/drweb/drweb.
   key | apt-key add -
   ```

   or

   ```
   curl http://officeshield.drweb.com/drweb/drweb.key  |
   apt-key add -
   ```

2. To add the repository to you system, add the following line to /etc/apt/sources.list file:

   ```
   deb http://officeshield.drweb.com/drweb/debian stable
   non-free
   ```

3. To install **Dr.Web for Kerio MailServer**, execute the following commands:

   ```
   apt-get update

   apt-get install drweb-kerio
   ```

4. To uninstall **Dr.Web for Kerio MailServer**, execute the following command:

   ```
   apt-get remove drweb-kerio
   ```

Alternatively, you can use graphical manager (e.g., Synaptic) to install or remove the packages.

Please note, that after installation from native packages, `drwebd.enable` file will be located in the following directories:

- `/etc/defaults` – for deb packages
- `/etc/sysconfig` – for rpm packages

## Red Hat Enterprise Linux, Fedora, CentOS (yum)

1. Add the file with following content to the `/etc/yum.repos.d` directory:

   ```
   [drweb]

   name=DrWeb - stable

   baseurl=http://officeshield.drweb.com/drweb/

   el5/stable/i386/

   gpgcheck=1

   enabled=1

   gpgkey=http://officeshield.drweb.com/drweb/

   drweb.key
   ```

2. To install **Dr.Web for Kerio MailServer**, execute the following command:

   ```
   yum install drweb-kerio
   ```

3. To uninstall **Dr.Web for Kerio MailServer**, execute the following command:

   ```
   yum remove drweb-kerio
   ```

Alternatively, you can use graphical manager (e.g., PackageKit, Yumex) to install or remove the packages.

## SUSE Linux (Zypper)

1. To add the repository, run the following command:

   ```
   zypper ar -t YUM http://officeshield.drweb.com/drweb/
   el5/stable/i386/ drweb
   ```

   or

   ```
   zypper ar -t YUM http://officeshield.drweb.com/drweb/
   el5/stable/x86_64/ drweb
   ```

2. To install **Dr.Web for Kerio MailServer**, execute the following commands:

   ```
   zypper refresh

   zypper install drweb-kerio
   ```

3. To uninstall **Dr.Web for Kerio MailServer**, execute the following command:

   ```
   zypper remove drweb-kerio
   ```

Alternatively, you can use graphical manager (e.g., YaST) to install or remove the packages.

# 4. Configure Program Components

In case the **Run interactive postinstall script** check box has not been selected during the installation of **Dr.Web for Kerio MailServer** and the corresponding script has not run, it is required to configure the anti-virus daemon, drweb-kerio-webstatd daemon and Dr.Web Monitor.

If the proxy server is used for Internet connection, you also need to define its parameters.

## Launch and Configure Daemon drwebd

After **Dr.Web for Kerio MailServer** is installed, you need to launch the anti-virus daemon **drwebd**. To do this:

1. Open the `/etc/drweb/drwebd.enable` file and set the value of the parameter `ENABLE=1`.
2. Copy the key file for **drwebd** daemon in the directory specified by the `Key` parameter of the `[Daemon]` section in the `/etc/drweb/drweb32.ini` configuration file. The default key file is set to **/opt/drweb/drweb32.key**.
3. Launch the daemon by the following command:

   ```
   /etc/init.d/drwebd start
   ```

   Make sure that there were no start up errors.

# Launch and Configure Dr.Web Monitor

To configure **Dr.Web Monitor**, do the following:

1. Open the `/etc/drweb/drweb-monitor.enable` file and set the parameter value `ENABLE=1`.
2. Launch **Dr.Web Monitor** by the following command:

   ```
   /etc/init.d/drweb-monitor start
   ```

   Make sure that there were no start up errors.

# Launch and Configure Daemon drweb-kerio-webstatd

To use the web console you need to launch the daemon **drweb-kerio-webstatd** by the following command:

```
/etc/init.d/drweb-kerio-webstatd start
```

# Configure Proxy

If the computer where Kerio mail server resides connects to the Internet via proxy, you need to configure **Dr.Web for Kerio MailServer** Updater to connect to the proxy server.

The proxy server parameters can be defined in the configuration file (by default, `/etc/drweb/drweb32.ini`) in the `[Updater]` section (Table 5):

**Table 5. Proxy configuration parameters**

| Parameter | Description |
|---|---|
| `ProxyServer =` *<proxy server name or IP-address>* | Name or IP-address of the proxy server. |
| `ProxyLogin =` *<proxy server user name>* | Name of the proxy server user. |
| `ProxyPassword =` *<proxy server user password>* | Password of the proxy server user. |

# 5. Program Integration

**Dr.Web for Kerio MailServer** can be enabled and operates as an external anti-virus software integrated into Kerio mail server and checks the e-mail attachments according to the mail server settings.

**To integrate Dr.Web for Kerio MailServer into Kerio mail server:**

1. Launch the **Administration Console for Kerio MailServer**.
2. Open the **Configuration** -> **Content Filter** -> **Antivirus** section.
3. Select the checkbox **Use external antivirus** and then select **Dr.Web for Kerio MailServer** in the drop-down list.
4. Specify the anti-virus options.
5. Click **Apply**.

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

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

# Anti-virus Options

The options of **Dr.Web for Kerio MailServer** specify the program operation and logging. These options can be set up by means of **Administration Console for Kerio MailServer** on the **Configuration** -> **Content Filter** -> **Antivirus** section:

1. Click **Options** to the right of anti-virus name.
2. The list of options will open (see Table 6). 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 and click **OK**.

**Table 6. Dr.Web for Kerio MailServer options.**

| Option | Description |
|---|---|
| Detect adware (Yes/No)<br>Detect dialers (Yes/No)<br>Detect hacktools (Yes/No)<br>Detect jokes (Yes/No)<br>Detect riskware (Yes/No) | These options allow to enable/disable the detection of adware, dialers, hacktools, jokes and riskware in e-mail attachments. Each parameter may have one of the following values:<br>• **No** to disable detection of corresponding malware type. Therefore, the objects containing such malware will be ignored.<br>• **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. |
| Dr.Web Agent socket path | This setting specifies the socket for interaction with **Dr.Web Agent**. The default value is **pid:/var/drweb/run/drweb-agent.pid**.<br>For detailed information on configuring this component see the **Dr.Web Agent** documentation. |

| Option | Description |
|---|---|
| Dr.Web Daemon socket path | This setting specifies the socket for interaction with anti-virus daemon **drwebd**. The default value is **pid:/var/drweb/run/drwebd.pid**.<br>This setting also allows you to configure the anti-virus check performing on the remote computer with anti-virus daemon **Dr.Web Daemon** (**drwebd**), if the computer where Kerio mail server resides has no access to the internet or the common anti-virus check server is used. In this case you can indicate the IP-address and the port of remote daemon as the value of this setting in the following format: *<ip-address>:<port>*. For example: 192.168.100.10:3000.<br>For detailed information on anti-virus check performing on the remote computer see the **Dr.Web Daemon** documentation. |
| Enable heuristic (Yes/No ) | This option enables/disables the heuristic analyzer that allows to detect the unknown viruses. Two values are possible:<br>• **No** to disable the heuristic analyzer<br>• **Yes** to enable the heuristic analyzer<br>By default, the heuristic analyzer is enabled. |
| Quarantine directory | This option specifies the path to the quarantine directory. The default path is **/var/drweb/infected**. |
| Quarantine enabled (Yes/No) | This option allows to enable/disable moving the infected objects to quarantine. By default, it is enabled. |

3. Click **OK** in **Antivirus options** window when you finish setting up the anti-virus plug-in options.
4. Click **Apply** on the **Antivirus** section to apply the changes.

# 6. Virus Check

**Dr.Web for Kerio MailServer** detects the following malicious objects:

- Infected e-mail attachments including:
    - Infected archives
    - Bomb viruses in files or archives
    - Adware
    - Hacktools
    - Dialer programs
    - Joke programs
    - Riskware

You can determine the types of malicious objects to be detected by setting up the anti-virus options.

**Dr.Web for Kerio MailServer** uses different detection methods while scanning the attached files of e-mail messages. In case a virus is detected by **Dr.Web for Kerio MailServer** it is processed according to the settings of Kerio mail server.

The actions of Kerio mail server for detected malicious objects or in case the attached file cannot be scanned are specified by means of **Administration Console for Kerio MailServer** in the corresponding groups of options on the **Configuration** -> **Content Filtering** -> **Antivirus** section or on the **Action** tab (depends on the version of Kerio mail server).

You can configure server to discard the message with infected attachments, allow the delivery of the message with removed infected files, forward the initial or filtered message to the administrator's e-mail, send a warning notification or bounce the message to the sender.

You can also set up the actions of the server in case the attached file cannot be scanned, for example, when it is encrypted or corrupted. You can configure server to perform the same actions as for the infected files or to pass the file and append to the message a notification that it can probably contain a virus.

For detailed information on configuring Kerio mail server to process the checked messages see the Administrator's Guide of Kerio mail server available on the Kerio official web site at http://www.kerio.com/supp_kms_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** – a special directory (`/var/drweb/infected`), where the malicious objects are isolated from the rest of the system.

By default, the quarantine is enabled. To disable it, set the value **No** for the **Quarantine enabled** anti-virus parameter. In case quarantine is disabled, the infected objects will be deleted.

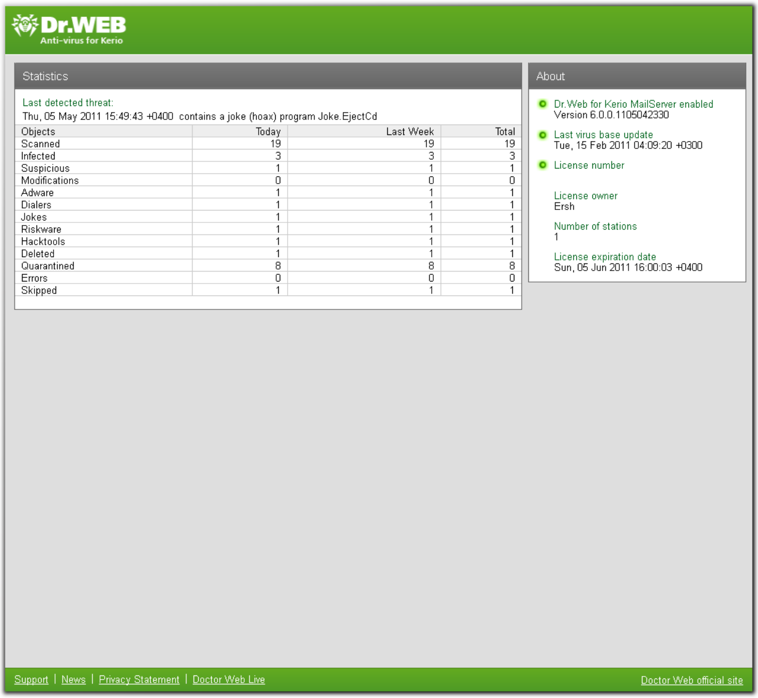
If a file moved to quarantine has the same name as a file that is already in quarantine, an index number will be added to the name of the new file. For example, the file file.com will be renamed to file.com_01, etc.

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.

In case Kerio MailServer versions from 6.2 to 6.7.2 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.

# 7. Web Console

Web console allows viewing the information on the **Dr.Web for Kerio MailServer** operation, particularly, on the license and updates, as well as the program statistics (see Figure 20) via browser.



Statistics

Last detected threat:
Thu, 05 May 2011 15:49:43 +0400 contains a joke (hoax) program Joke.EjectCd

| Objects | Today | Last Week | Total |
|---|---|---|---|
| Scanned | 19 | 19 | 19 |
| Infected | 3 | 3 | 3 |
| Suspicious | 1 | 1 | 1 |
| Modifications | 0 | 0 | 0 |
| Adware | 1 | 1 | 1 |
| Dialers | 1 | 1 | 1 |
| Jokes | 1 | 1 | 1 |
| Riskware | 1 | 1 | 1 |
| Hacktools | 1 | 1 | 1 |
| Deleted | 1 | 1 | 1 |
| Quarantined | 8 | 8 | 8 |
| Errors | 0 | 0 | 0 |
| Skipped | 1 | 1 | 1 |

About

- Dr.Web for Kerio MailServer enabled
  Version 6.0.0.1105042330
- Last virus base update
  Tue, 15 Feb 2011 04:09:20 +0300
- License number

License owner
Ersh

Number of stations
1

License expiration date
Sun, 05 Jun 2011 16:00:03 +0400

**Figure 20. Web console**

### Access to web console

To access to the web console, in the address bar of the browser enter the address in the following format:

`http://localhost:27182/statistics`, where `localhost` is the address of the protected Kerio mail server.

## Program Information

The **About** section of web console (see Figure 20) 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 **Statistics** section of the web console (see Figure 20). 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 suspicious objects

- Number of detected riskware, adware, dialers, jokes, hacktools and modifications
- Number of deleted objects and objects move to quarantine
- Number of errors when checking e-mail attachments
- Number of skipped objects

# 8. Update

It is recommended to use the Updater script (update.pl) to update virus databases. Updater is a part of **Dr.Web for Kerio MailServer** and can be installed via the **drweb-updater** packet of the installation archive.

In case **Dr.Web Agent** operates in the **Enterprise** mode, virus databases and anti-virus engine are updated from the repository of **Dr.Web Control Center**.

The Updater script is written in Perl and is located in the directory of executable files of application (by default, `/opt/drweb/update.pl`). Updater settings are specified in the `[Updater]` section of the main configuration file (by default, `/etc/drweb/drweb32.ini`). To use a different configuration file, it is necessary to specify the full path to it via command line parameter when launching the script.

When installing the **drweb-updater** packet, a task for periodic launch of the `update.pl` script (every half an hour) is created via a standard scheduler (**cron**). This is done by creating the drweb-update file in the `/etc/cron.d` directory. The file contains the following code:

```
*/30 * * * * drweb /opt/drweb/update.pl
```

The `[Updater]` section of the configuration file contains the following parameters (Table 7):

Table 7. Updater parameters

| Parameter | Description |
|---|---|
| `Section` | Specifies the component for update. The following values are possible:<br>• **Daemon** – to update the daemon<br>• **Scanner** – to update the scanner<br>The default value is **Daemon**.<br>The information on the location of the files for update is received from the corresponding sections of the configuration file. The value can de redefined by setting the command line parameter `--what` when launching the updates. |
| `ProgramPath =` *<path to file>* | Path to Daemon/Scanner. This parameter is used by Updater to get the product version and API information on the installed executable file.<br>The default value is %bin_dir/drwebd. |
| `SignedReader =` *<path to program file>* | Path to the program for signed files reading.<br>The default value is %bin_dir/read_signed. |
| `LzmaDecoderPath =` *<path to program file>* | Path to the program for lzma-archives unpacking. |
| `LockFile =` *<path to file>* | Path to lock file designed to prevent certain files share when they are processed by Updater.<br>The default value is %var_dir/run/update.lock. |
| `CronSummary` | This parameter enables/disables use of the standard output mode (stdout) for statistics of update session. The following values are possible:<br>• **Yes** to enable the use of standard output<br>• **No** to disable the use of standard output<br>The default value is **Yes**. |

| Parameter | Description |
|---|---|
| `DrlFile = `*<path to file>* | Path to the file containing the list of update servers. Updater selects the values from this list randomly.<br>The default value is %var_dir/bases/update.drl.<br>⚠ This file is signed by **Doctor Web** and should not be modified by user. It is updated automatically. |
| `Timeout` | Maximum time (in seconds) for updates download.<br>By default it is set to 90 sec. |
| `Tries` | The number of attempts for Updater to establish the connection.<br>The default the value is 3. |
| `LogFileName = `*<full file name>* | The log file name. It can be set as syslog to carry out logging by the system service. The default name is **syslog**. |
| `SyslogFacility = `*<full file name>* | The type of record when the system service syslogd is used. The following values are possible: **Daemon**, **Local0** .. **Local7**, **Kern**, **User**, **Mail**.<br>The default value is **Daemon**. |
| `LogLevel` | Log verbosity level. The following values are possible: **Debug**, **Verbose**, **Info**, **Warning**, **Error**, **Quiet**.<br>The default value is **Verbose**. |

The `[Updater]` section contains also the proxy configuration parameters.

# 9. Logging

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

- Syslog
- Debug log of Kerio mail server.

The update information is also logged by program, to configure logging the Updater events, set up the corresponding parameters in the `[Updater]` section of the configuration file.

## Event Log

**Dr.Web for Kerio MailServer** registers the following information using the system service syslog:

- 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 (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)

The log messages are usually located in the `/var/log/messages` file (RedHat, SUSE) or `/var/log/syslog` file (Debian). For more information on the system log, see your operating system documentation.

# Debug Log

The debug log of Kerio mail server contains the information that is used for search and analysis of errors in operation of **Dr.Web for Kerio MailServer**.

## To enable the debug logging

1. Launch the **Administration Console for Kerio MailServer**.
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 checking** and then click **OK**.

# 10. Troubleshooting

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

- Check installation
- Check plug-in operation

## 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 8):

**Table 8. Check the installed files and folders**

| Directory | File name | Description |
|---|---|---|
| /opt/drweb | drwebd | Anti-virus daemon |
| | update.pl | Update script |
| | drwebd.key | Key file for anti-virus daemon **drwebd** |
| | drweb-agent | **Dr.Web Agent** component |
| | drweb-monitor | **Dr.Web Monitor** component |
| /etc/drweb | drwebd.enable | Enable/Disable the daemon **drwebd** |
| | drweb-monitor.enable | Enable/Disable **Dr.Web Monitor** |
| /opt/drweb/kerio | avir_drweb.so | The library of anti-virus application **Dr.Web for Kerio MailServer** |
| /opt/kerio/mailserver/plugins/avirs | avir_drweb.so | Link to the /opt/drweb/kerio/avir_drweb.so file |

| Directory | File name | Description |
|---|---|---|
| /opt/drweb | drweb-kerio-webstatd | Web console daemon |

# Check Functionality

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

### To check plug-in operation

1. Send an e-mail with EICAR-Test-File in attachment via Kerio mail server. For information on EICAR test virus see http://en.wikipedia.org/wiki/EICAR_test_file.
2. Check the received e-mail. The infected object should be deleted.

# 11. Appendices

## Appendix A. Operation in Central Protection Mode

**Dr.Web for Kerio MailServer** 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 21).

Workstations and servers are protected by *local anti-virus components* (clients; herein, **Dr.Web for Kerio MailServer**) 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.

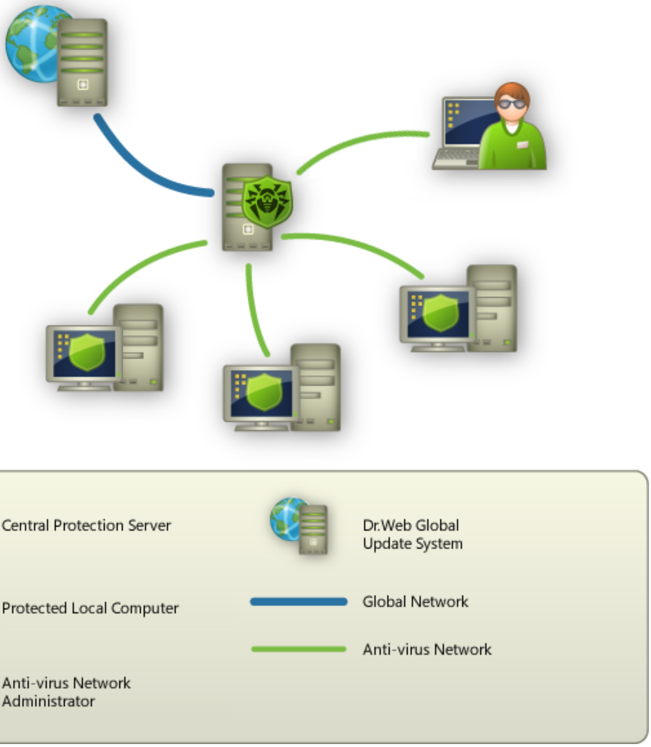

Central Protection Server
Dr.Web Global Update System
Protected Local Computer
Global Network
Anti-virus Network
Anti-virus Network Administrator

**Figure 21. Logical structure of anti-virus networks.**

## Operation of Dr.Web for Kerio MailServer in Central Protection Mode

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

The version 6.00 of **Dr.Web for Kerio MailServer** is not compatible with **Dr.Web Agent 5**.

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

- Recording the start and stop events of Kerio mail server with the installed plug-in **Dr.Web for Kerio MailServer**. Start and stop events are displayed in the **Start/Stop** table of **Dr.Web Control Center**.
- Sending statistics of **Dr.Web for Kerio MailServer** 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 MailServer**, 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 MailServer** that is registered at the anti-virus network. To use this key, you need to switch **Dr.Web Agent** to the **Enterprise** mode by specifying the **Yes** value for the `UseEnterpriseMode` parameter in the `/etc/drweb/agent.conf` configuration file.

⚠ In the **Enterprise** mode **Dr.Web for Kerio MailServer** does not use the local license key file specified in the `/etc/drweb/agent.conf` configuration file as `LicenseFile` parameter value in the `[StandaloneMode]` section. In the **Enterprise** mode the key file is requested from **Dr.Web Control Center**, and if it is not received, the plug-in does not perform the anti-virus check.

# Index

# Index

# Index