Dr.WEB

for Kerio Connect

Administrator Manual

Dr.Web for Kerio Connect
Version 11.1
Administrator Manual
1/22/2020

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125040

Website: https://www.drweb.com/

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

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

Doctor Web

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

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

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

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

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

Table of Contents

Introduction

Thank you for purchasing the Dr.Web for Kerio Connect application. This product is an anti-virus plug-in designed to protect corporate email traffic against viruses. The plug-in integrates into the Kerio Connect email server and scans the email attachments sent to the server.

This software product incorporates the latest and most advanced anti-virus technologies of Doctor Web designed to detect different types of malicious objects which may pose a threat to the email system operation and information security.

This manual will help administrators of corporate networks using the Kerio Connect email server install and configure the Dr.Web for Kerio Connect plug-in and learn its basic functions.

For more information on the anti-virus scans of the email for the Kerio Connect email server, see Kerio official website at http://www.kerio.ru/products/kerio-connect.

Conventions

The following symbols and text conventions are used in this guide:

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

Command-line commands, entered with a keyboard (in the terminal or terminal emulator), are marked with the command prompt character `$` or `#` in the current manual. The character indicates the privileges required for the specified command:

`$`—indicates that the command can be executed with user rights.

`#`—indicates that the command can be executed with superuser (usually *root*) privileges. To elevate privileges, use the `su` or `sudo` commands.

About the Product

Dr.Web for Kerio Connect scans the email traffic for viruses, dialer programs, adware, riskware, hacktools and joke programs. On detection of security threats, they are treated according to the Kerio Connect email server settings.

Program Main Features

Dr.Web for Kerio Connect performs the following functions:

- anti-virus scan of email attachments according to the Kerio Connect email server rules,
- malware detection;
- isolation of infected objects in quarantine;
- heuristic analysis for additional protection against unknown viruses;
- constant update of virus databases

Program Components

Dr.Web for Kerio Connect consists of several components interacting with each other.

- The configuration daemon `drweb-configd` controls activity of all Dr.Web for Kerio Connect components depending on the specified settings, stores information on license and settings, and provides application components with this information, if necessary.
- The Dr.Web Scanning Engine (`drweb-se`) is used to perform anti-virus scanning.
- The updating module `drweb-update` (Dr.Web Updater) serves for automatic update of virus virus databases. This component downloads them from Doctor Web update servers via the Internet.
- The Dr.Web Ctl utility (`drweb-ctl`) provides you with the command-line interface for managing the product.

Licensing

Permissions to use Dr.Web for Kerio Connect are granted by the license purchased from the Doctor Web company or from its partners. License parameters determining user rights are set in accordance with the License Agreement (see https://license.drweb.com/agreement/), which the user accepts during the product installation.

The license contains information on the user and the vendor as well as usage parameters of the purchased product, including:

- the list of components licensed to the user;
- Dr.Web for Kerio Connect licensed period;
- availability of technical support;
- other restrictions (for example, number of computers on which you are allowed to use Dr.Web for Kerio Connect).

For evaluation purposes users can also activate demo period. Having fulfilled the activation conditions, users can take advantage of full functionality of Dr.Web for Kerio Connect for the whole demo period.

Each Doctor Web product license has a unique serial number associated with a special file stored on the user computer. This file regulates operation of product components in accordance with the license parameters and is called a *license* key file. Upon activation of a demo period, a special key file, named a *demo* key file, is automatically generated.

If a license or a demo period are not activated on the computer, Dr.Web for Kerio Connect components are blocked. Moreover, updates for virus databases and components cannot be downloaded from the Doctor Web update servers.

License Registration and Activation

License purchasing, registration and activation

After a license is purchased, updates to product components and virus databases are regularly downloaded from the Doctor Web update servers. If users have issues with installing or using the purchased product, they can contact technical support provided by Doctor Web or its partners.

You can purchase any Doctor Web product, as well as obtain a product serial number either via the online store or from our partners. For details on license types, visit the Doctor Web official website at https://license.drweb.com/.

License registration is required to prove that you are a legal user of Dr.Web for Kerio Connect and to activate the functions of the anti-virus, including the regular updates of virus databases.

To activate the product, enter the serial number of the purchased license. The serial number is supplied with the product or via email when purchasing or renewing the license online. A purchased license can be activated on the Doctor Web official website at https://products.drweb.com/register/.

If you have used the product in the past, you may be eligible for a 150-day extension to your new license. To enable the bonus, enter your registered serial number or provide the license key file.

If you have several licenses for using Dr.Web for Kerio Connect on several servers, but choose to use the product only on one server, you can specify this and, hence, license validity period will be automatically extended.

Subsequent Registration

If a key file is lost but the existing license is not expired, you should register again by providing the personal data you specified during the previous registration. You can use a different email address. In this case, the license key file will be sent to the newly specified address.

The number of times you can request a key file is limited. One serial number can be registered no more than 25 times. If the limit is exceeded, no key file is sent. To receive a lost key file, contact Doctor Web technical support, describe your problem in detail, and state personal data you entered upon serial number registration. The license key file will be sent by email.

After the key file is sent to you by email, you need to install it manually.

Demo Period Request

A demo period for your copy of the Dr.Web for Kerio Connect product can be obtained by sending a request via the Doctor Web official website at https://download.drweb.com/demoreq/biz/. After you select the product and fill in the registration form, you will receive an email with a serial number or a key file required to activate the demo period.

Another demo period for the same computer can be obtained after a certain time period.

You can also use the `license` command of the Dr.Web Ctl management utility, which allows you to get a demo or a license key file for a serial number of a registered license automatically.

Key File

User rights for the Dr.Web for Kerio Connect product are stored in the special *key file*. The file contains information on the purchased license or a demo period and regulates usage rights in accordance with it.

A *valid* key file satisfies the following criteria:

- license period is not expired,
- the key file applies to all components of Dr.Web for Kerio Connect,
- integrity of the key file is not violated.

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

The key file is digitally signed to prevent its editing. The edited key file renders invalid. It is not recommended to open your key file in text editors in order to avoid its accidental invalidation.

Key File Installation

Dr.Web for Kerio Connect requires a valid key file for correct operation. The path to this file is specified after the plug-in installation.

During the Dr.Web for Kerio Connect operation, the key file must be located in the default directory `/etc/opt/drweb.com` under the name `drweb32.key`.

Plug-in components regularly check the key file for availability and validity. If no valid key file (license or demo) is found, or if the license is expired, operation of the anti-virus components is blocked until a *valid* key file is installed.

It is recommended that you keep the license key file until it expires, and use it to reinstall the product or install it on a different computer. In this case, you can use the same product serial number and customer data that you provided during the registration.

If you have a key file corresponding to the valid license for Dr.Web for Kerio Connect (for example, if you obtained the key file by email or if you want to use the program on another server), you can activate the product by specifying the path to the key file. For that, do the following:

1. Unpack the key file if archived and save it in any available directory (for instance, a local directory or removable media).

In email messages, key files are usually transferred in ZIP archives. The archive containing the key file for product activation usually named `agent.zip` (note that if the message contains several archives, then it is necessary to use the `agent.zip` archive).

2. Then copy the key file to the `/etc/opt/drweb.com` directory and rename the file to `drweb32.key` if necessary.
3. To accept the changes, restart Dr.Web for Kerio Connect with the `reload` command from the Dr.Web Ctl utility.

Licensing Parameters

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

Licensing Parameters

1. To view licensing parameters stated in the license key file, open the file using the text editor.

The license key file is protected from being edited. File editing makes it invalid. Do not save the file when you close the text editor to prevent the file from being compromised.

2. Review the following licensing parameters:

Parameter	Description
The `[Key]` group, the `Applications` parameter	It determines the components that the license owner can use.  The KerioPlugin component must be listed to use the key file with Dr.Web for Kerio Connect.
The `[Key]` group, the `Expires` parameter	Determines the license key file expiration date (`Year-Month-Day` format is used).
The `[User]` group, the `Name` parameter	Determines the license owner registration name.
The `[User]` group, the `Computers` parameter	Determines the number of users protected by the plug-in.

3. Close the file without saving.

License Update

In some cases, for example, when the license expires or security of your system is reinforced, you may need to buy a new Dr.Web for Kerio Connect license or an extended one. In this case, you should replace your license key file that is already registered in the system. You do not need to reinstall or interrupt Dr.Web for Kerio Connect operation to update the license.

To replace the license key file

1. To update the license, copy your new license key file to the `/etc/opt/drweb.com` directory.
2. Restart the configuration daemon (drweb-configd), so that Dr.Web for Kerio Connect starts using the new license key file.

For more information on license types, visit the Doctor Web official website at https://license.drweb.com/products/biz.

Plug-in Installation and Uninstallation

Dr.Web for Kerio Connect is installed on computers where the Kerio Connect email server is installed. It operates as an external anti-virus software via the plug-in interface.

Dr.Web for Kerio Connect is distributed as a single self-extracting archive `drweb-kerio-connect_[version]-[build]~linux_amd64.run`, where `[version]` is the product version and `[build]` is the build number. The archive contains the following packages:

Name	Description
`drweb-common`	Contains: • uninstallation program (`uninst.sh`), • license agreement files, • directory structure, During the installation of this package, a group named `drweb` and a user named `drweb` are created.
`drweb-bases`	Contains anti-virus databases (`.vdb`). Requires the `drweb-common` package for installation.
`drweb-update`	Contains the updater of the anti-virus scan engine and virus databases. Requires the `drweb-common` package for installation.
`drweb-configd`	Contains Dr.Web for Kerio Connect configuration daemon files.
`drweb-ctl`	Contains command-line interface tool for Dr.Web for Kerio Connect and documentation.
`drweb-se`	Contains the Dr.Web Scanning Engine executable files and documentation. Requires `drweb-bases` for installation.
`drweb-kerio-connect-plugin`	Contains the `avir_drweb.so` library of the Dr.Web for Kerio Connect plug-in. Suitable for installation and operation with the Kerio Connect email server version 7.x.x. or later
`drweb-kerio-connect-doc`	Contains documents on the Dr.Web for Kerio Connect application.
`drweb-libs`	Contains the common libraries for product components.

For more information on using the anti-virus software with Kerio Connect email servers, see the Kerio official website at http://www.kerio.com/products/kerio-connect.

System Requirements

The computer where you want to install Dr.Web for Kerio Connect should meet the following system requirements:

Parameter	Requirement
Disk space	Minimum 290 MB of disk space, not including the disk space for quarantine files storage
Operating system	One of the following 64-bit versions: • Red Hat Enterprise Linux 6 and 7 • CentOS 6 and 7 • Ubuntu 12.04 LTS, 14.04 LTS • Debian 7 and 8
Email server	If you install Dr.Web for Kerio Connect for the first time, Kerio Connect version 7.0.0 and later ones can be used.

This section reflects requirements for the Dr.Web for Kerio Connect only. The application can operate on computers with the installed Kerio Connect email server. System requirements to the email server can be found in the documents to Kerio Connect.

Dr.Web for Kerio Connect also supports installation and operation in the Kerio Connect VMware Virtual Appliance environment. For information on this software see Kerio official website at http://www.kerio.com/support/kerio-connect.

Program Installation

This section describes how to install Dr.Web for Kerio Connect. It also contains a description of how to upgrade the version, if the previous version of Dr.Web for Kerio Connect is already installed on your computer.

Before installation, make sure the computer meets the minimum system requirements.

Program Installation

To install Dr.Web for Kerio Connect components

1. If necessary, download the installation file from the Doctor Web official website at https://download.drweb.com/.

2. Enable SSH access on the email server. For that,
   - open the **Status** tab on the admin console of the Kerio Connect email server, pressing and holding SHIFT, then open the **System Status** section and click **Enable SSH**;
   - then select **Yes** in the popup window.
3. Copy the `drweb-kerio-connect_[version]-[build]~linux_amd64.run` archive and the license key file of Dr.Web for Kerio Connect on a computer with the installed Kerio Connect email server.
4. Allow the archive to be executed, for example, by using the following command:

   ```
   # chmod +x <file_name>.run
   ```

5. Execute the archive using the following command:

   ```
   # ./<file_name>.run
   ```

   At this, an integrity check of the archive is performed. Archived files are then unpacked to a temporary directory and the installation program that uses the command line is automatically started.

   

   If the path to the temporary directory in the file system has not enough free space for the unpacked files, the installation process is aborted and a corresponding message is displayed. In this case, change the value of the `TMPDIR` system environment variable so that it specifies to a directory with enough free space and repeat the installation. You can now use the `--target` option to unpack files in the specified directory.

6. Follow the installer instructions.

All unpacked installation files are deleted once the installation process is completed.

Installation program may be launched automatically in the silent mode, that is, without displaying a user interface (including dialogs that are normally displayed in the command-line mode). For this, you need to execute the following command during step 5:

```
# ./<file_name>.run -- --non-interactive
```

Note that using this option means that you *accept* the terms of the Dr.Web License Agreement. You can find the text of the License Agreement in the */var/opt/drweb.com/opt/share/doc/LICENSE* file. The file extension indicates the language of the License Agreement. If the `LICENSE` file does not have any extension, the Dr.Web License Agreement is written in English. If you *do not accept* the terms of the License Agreement, you must uninstall the product after its installation.

Installing from Command Line

Once you start the program for the command-line-based installation, a message is be displayed inviting you to install the product.

1. To proceed with Dr.Web for Kerio Connect installation, enter `Y` or `Yes` (values are case insensitive), otherwise type N or `No`. Press `ENTER`.
2. The License Agreement will open. Click ENTER to scroll the text down line by line or SPACEBAR to scroll it down one screenful at a time. Note that you cannot scroll the License Agreement up. To continue installation, you need to accept the terms of the License Agreement. To do it, enter `Y` or `Yes` in the input field and click ENTER. Otherwise, the installation will be aborted.
3. After you accept the terms of the License Agreement, Dr.Web for Kerio Connect installation automatically starts. During the procedure, the information about the installation process, including the list of installed components, is displayed on the screen.
4. If the installation was successful, if the product requires automatic configuration before starting, the interactive product configuration script will automatically start.

   If an error occurs, a message describing the error is displayed on the screen and then the installer exits. When the installation process fails due to an error, resolve the problems that caused this error and start the installation again.

After installation, the Dr.Web for Kerio Connect plug-in may be connected with the email server.

Interactive Configuration Program

The interactive configuration program allows you to install the product license key file.

1. If you want to configure the plug-in, enter `Y` or `Yes` as the answer to the question “Do you want to continue?”. If you enter `N` or `No`, configuration program exits.
2. If a valid key file is not available on your computer (in the product standard directory for keeping the key file), the script offers you to specify the path to a valid key file.
   If a valid key file is already available on your computer, specify the path to it and click ENTER. The file will be copied to the product standard directory.

   If a valid key file is in the product standard directory, this step is automatically skipped.

   To skip this step, enter `0`. You can install a key file manually later.
3. After you finish adjusting the settings, click ENTER to exit the configuration program.

If the configuration program has not been executed for some reason, copy the license key file to the `/etc/opt/drweb.com/` directory, and then restart the service using the `reload` command of the Dr.Web Ctl utility.

Upgrading to a Newer Version

Complete installation of the new version of Dr.Web for Kerio Connect. Then, for the update to take effect, disable the plug-in using the admin console of the Kerio Connect email server, and then enable it again.

When upgrading the product, the existing license key file will be automatically saved to the appropriate location, that is, to the standard directory for the new version of the product.

If any problem occurs during the automatic installation of the key file, you can install it manually.

If a valid license key file was lost, contact Doctor Web technical support.

Installation Check

To check if the program is correctly installed, ensure that during the installation the following directories were created and contain all necessary files:

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

If errors occurred during the program installation or operation, contact Doctor Web technical support.

Program Uninstallation

To uninstall Dr.Web for Kerio Connect, you must have administrator privileges.

Before uninstalling Dr.Web for Kerio Connect, disable its usage by the Kerio Connect email server. To do this,

1. Open the administration console of the email server.
2. Open the **Configuration** → **Content Filter** → **Anti-virus** section.
3. Clear the check box **Use external anti-virus program** for the selected anti-virus, **Dr.Web for Kerio Connect**.
4. Click **Apply**.
   Dr.Web for Kerio Connect will be disabled.

Uninstalling Dr.Web for Kerio Connect

To uninstall the program using the automatic uninstallation tool,

1. Execute the following command:

```
# /opt/drweb.com/bin/uninst.sh
```

2. To start uninstalling Dr.Web for Kerio Connect enter `Y` or `Yes` and click ENTER. Otherwise, enter `N` or `No`, and the automatic uninstallation tool exits.

Note that the tool for automatic uninstallation removes not only Dr.Web for Kerio Connect, but also all other Dr.Web products installed on your computer. If you want to uninstall only Dr.Web for Kerio Connect, use the Zypper package manager instead of automatic uninstallation tool.

3. After you confirm uninstallation, uninstallation process of all anti-virus products of Doctor Web packages will start. At that, entries of uninstallation progress registered in the log will be displayed.
   The software will automatically terminate after removing all components.

The license key file is not deleted automatically. However, you can delete it manually.

Moreover, scanning settings are saved and are used automatically during the Dr.Web for Kerio Connect reinstallation.

For custom component uninstallation, please use the Zypper package manager. It is automatically installed together with the product. To uninstall the selected components

1. Switch to the `/opt/drweb.com/bin` directory and execute the following command:

   ```
   # ./zypper rm <package_name>
   ```

2. Following the instruction on the screen, select the components you would like to uninstall.
3. Confirm uninstalling the selected components. For that, enter `Y` or `Yes` and click ENTER.
4. The uninstallation process of the selected components starts. The report on the uninstallation progress is displayed on the screen in the real-time mode.
   After the uninstallation process is completed, you will see the message that the selected components are successfully uninstalled.

To reinstall any component, you can uninstall the component, then install it again.

Uninstallation of Dr.Web for Kerio Connect may be launched automatically in the silent mode, that is, without displaying a user interface (including dialogs that are normally displayed in the command-line mode). For this, you need to launch the program as follows:

```
# env DRWEB_NON_INTERACTIVE=yes /var/opt/drweb.com/opt/bin/uninst.sh
```

Program Integration

Dr.Web for Kerio Connect can be connected to the Kerio Connect email server as an external anti-virus software that scans email attachments according to the mail server settings.

To connect Dr.Web for Kerio Connect

1. Open the administration console of the email server.
2. Open the **Configuration** → **Content Filter** → **Anti-virus** section.
3. Select the check box **Use external anti-virus program**.
4. Select **Dr.Web for Kerio Connect** in the dropdown menu.
5. Configure the application options.
6. Click **Apply**.

If the plug-in was connected successfully, the corresponding message appears under the anti-virus software selection option.

If the integration failed and an error is reported, check the error log of the email server. Consult the Kerio Connect email server Administrator manual to solve the problem.

If the computer with Dr.Web for Kerio Connect installed is connected to the Internet via a proxy server, configure the proxy server connection parameters.

For more information on use of anti-virus software with email server and possible connection errors, see the administrator manual for the Kerio Connect email server at the official Kerio website at http://www.kerio.com/products/kerio-connect.

Configure Anti-Virus Program

The Dr.Web for Kerio Connect application options specify its operation and logging of its events. The options can be set up via the admin console of the email server, in the **Configuration → Content Filter → Anti-virus** section or on the **Actions** tab (depending on the Kerio Connect server version). To edit options of perform the following steps:

1. Click the **Options** button to the right from the app name **Dr.Web for Kerio Connect**. You will see the list of options to configure antimalware scanning and quarantine operations:

Parameter	Description
Detect adware, **Detect dialers**, **Detect hacktools**, **Detect jokes** **Detect riskware**	With these options, you can configure email scanning for adware, dialers, hacktools, jokes, and riskware in email attachments. Each option may have one of the following values: • `No`—disable detection of the corresponding malware type. Therefore, the objects containing such malware will be ignored. • `Yes`—enable detection of the 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.
Enable heuristic	With this option, you can enable/disable the heuristic analyzer that allows to detect unknown viruses. This option may have one of the following values: • `No`—to disable the heuristic analyzer. • `Yes`—to enable the heuristic analyzer. By default, the heuristic analyzer is enabled.
Quarantine directory	This option specifies the path to the quarantine directory. By default, the default path is `/var/lib/drweb/quarantine`.
Quarantine enabled	With this option, you can enable/disable moving the infected objects to the quarantine. This option may have one of the following values: • `No`, to disable moving the infected objects to the quarantine. • `Yes`, to enable moving the infected objects to the quarantine. This value is set by default.

2. To edit 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. Then click **OK**.

When setting these parameters, note that the `No`/`Yes` values are case-sensitive.

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

When reinstalling Dr.Web for Kerio Connect previously set parameters are kept.

Configure Proxy

If the computer with Dr.Web for Kerio Connect installed is connected to the Internet via a proxy server, you should also configure the Dr.Web Updater (`drweb-update`) module to connect to the proxy server.

The proxy server connection parameters can be defined in the configuration file (by default, `/etc/opt/drweb.com/drweb32.ini`) in the `[Update]` section:

Parameter	Description
`Proxy` *<connection string>*	It stores parameters for connecting to a proxy server that is used by the Dr.Web Updater component to connect to the Doctor Web update servers (for example, if direct connection to external servers is prohibited by your network security policy). If the parameter value is not specified, the proxy server is not used. **Allowed values** <*connection string*> is a string to connect to the proxy server. The string has the following format (URL): `[`<*protocol*>`://[`<*user*>`:`<*password*>`@]`<*proxyhost*>`:`<*port*>, where • <*protocol*> is a type of the used protocol (in the current version, only http is available); • <*user*> is a user name for connection to the proxy server; • <*password*> is a password for connection to the proxy server; • <*proxyhost*> is an address of the host where the proxy server operates (IP address or domain name, for example FQDN); • <*port*> is the used port. The <*protocol*> and <*user*>`:`<*password*> parameters can be empty. If the <*user*> or <*password*> parameters contain the following characters: “@”, “%” or “:”, these characters must be changed to the following codes: “%40”, “%25” and “%3A” respectively. The <*proxyhost*>`:`<*port*> proxy server address is mandatory. **Default value**: (not specified). **Examples**: 1. In the configuration file, • Connection to the proxy server on the host “proxyhost.company.org” using the port 123: `Proxy = proxyhost.company.org:123` • Connection to the proxy server on the host “10.26.127.0” using the port 3336 via the HTTP protocol as the user “legaluser” with the password “passw”: `Proxy = http://legaluser:passw@10.26.127.0:3336` • Connection to the proxy server on the host “10.26.127.0” using the port 3336 as the user “user@company.com” with the password “passw%123:”:

Parameter	Description
	`Proxy = user%40company.com:passw%25123%3A@10.26.127.0:3336` 2. Set the same values using the `cfset` command for the Dr.Web Ctl utility: `# drweb-ctl cfset Update.Proxy proxyhost.company.org:123` `# drweb-ctl cfset Update.Proxy http://legaluser:passw@10.26.127.0:3336` `# drweb-ctl cfset Update.Proxy user%40company.com:passw%25123%3A@10.26.127.0:3336`

Operation Check

To make sure the application operates properly, it is recommended to check the virus detection capabilities of Dr.Web for Kerio Connect. To perform the check, do the following:

1. Send an email with the EICAR test file attached via the Kerio Connect mail server. For information on the EICAR test virus, see http://en.wikipedia.org/wiki/EICAR_test_file.
2. Check the received email. The infected object must be deleted. The message subject may contain the prefix informing about the detected malicious object.

If errors occurred during the program installation or operation, contact Doctor Web technical support.

Virus Scan

Dr.Web for Kerio Connect detects infected email attachments.

Dr.Web for Kerio Connect scans the email traffic for the following types of malicious objects and malware:

- infected archives;
- bomb viruses in files or archives;
- adware;
- hacktools;
- dialers;
- jokes;
- riskware;

Dr.Web for Kerio Connect uses various threat detection methods during the scanning.

By configuring the anti-virus application via the admin console of the Kerio Connect email server you can determine the types of the detected malicious objects and actions applied to them.

When a malicious object is detected, you can

- discard message delivery,
- remove infected attachments and allow message delivery,
- forward an original message or a message where infected attachments have been removed to the server administrator,
- forward a message back to the sender or send a warning to the sender about infected objects in the message.

If Dr.Web for Kerio Connect cannot scan the attachment, for example, if the file is password protected or corrupted, you can

- apply actions for infected files and discard the file delivery,
- allow message and the attachment delivery informing about possible viruses.

For detailed information on configuring email traffic and actions that the email server applies to detected malicious objects, see the administrator manual of Kerio Connect email server.

Detection Methods

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which allows them to perform thorough scans on suspicious files and control software behavior.

Signature Analysis

The scans begin with signature analysis that 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, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

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

Execution Emulation

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

Heuristic Analysis

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

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

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

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

Quarantine

The infected email attachments sent to the server can be moved to the *quarantine,* a special directory (`/var/lib/drweb/quarantine`), where malicious objects are securely stored in isolation from the rest of the system.

By default, the option to move the infected objects is enabled. To disable it, set the value `No` for the anti-virus application option **Quarantine enabled**. If you disable quarantine, infected attachments will be removed.

If a file moved to the quarantine has the same name as a file that is already in quarantine, a numeral index will be added to the name of a new file. For example, the file `file.com` will be renamed to `file.com_01` and so on.

Managing quarantine

The quarantined files can be reviewed and processed only with *root* privileges. To remove files from the quarantine or save them on disk, use the `quarantine` command of the Dr.Web Ctl management utility.

Working With the Dr.Web Ctl Utility

You can manage the Dr.Web for Kerio Connect operation from the command line using a special command-line tool—Dr.Web Ctl (`drweb-ctl`).

You can perform the following actions from the command line:

- run the update of virus databases,
- view and change parameters of Dr.Web for Kerio Connect configuration,
- view component status and statistics on detected threats,
- view the quarantine and manage quarantined objects.

User commands for Dr.Web for Kerio Connect management can have an effect only if the Dr.Web for Kerio Connect service components are running (by default, they are automatically run on a system startup).

The Dr.Web Ctl utility supports auto-completion of commands for managing Dr.Web for Kerio Connect operation if the auto-completion option is enabled in the used command shell. If the command shell does not support auto-completion, you can configure the shell. For that, refer to the instruction manual for the used operating system.

When the utility finishes its operation, it returns an exit code according to the conventions for POSIX compatible systems: `0` (zero)—if the operation is completed successfully, non-zero—in case an error occurred.

Note that the utility returns a non-zero exit code only if an internal error has occurred (for example, the utility cannot connect to some component or the requested operation cannot be executed). If the utility detects (and, maybe) neutralizes a threat, it will return the `zero` exit code, as the requested operation (`scan`, and so on) is completed successfully.

If you want to learn more about detected threats and actions applied to them, examine messages that the utility displays in the console.

Utility Call Format

The command-line utility that manages Dr.Web for Kerio Connect operation has the following call format:

```
$ drweb-ctl [<general options> | <command> [<argument>] [<command options>]]
```

Utility call options:

- *<general options>*—options that can be applied on the start when the command is not specified or can be applied for any command. Not mandatory for the startup.
- *<command>*—command to be performed by Dr.Web for Kerio Connect (for example, start scanning, output the list of quarantined objects, and other commands).
- *<arguments>*—command arguments. The arguments depend on the specified command. Some commands do not have any arguments.
- *<command options>*—options that regulate performing the specified command. The arguments depend on the command. Some commands do not have any options.

The following general options are available:

Option	Description
`-h, --help`	To display general help information and exit. To output help information on any command, use the following call: `$ drweb-ctl <command> -h`
`-v, --version`	To display the module version and exit.
`-d, --debug`	The option instructs to display the debug information upon execution of the specified command. It cannot be executed if no command is specified. Use the following call: `$ drweb-ctl <command> -d`

To request help about this utility from the command line, use the following command:

```
$ man 1 drweb-ctl
```

drweb-ctl Commands

Commands to manage Dr.Web for Kerio Connect can be divided into the following groups:

- commands to manage configuration,
- commands to manage detected threats and the quarantine,
- commands to manage updates,
- information commands.

Commands to manage configuration

The following commands to manage configuration are available:

Command	Description
`cfset` <*section*>`.`<*parameter*> <*value*>	**Function**: Change the active value of the specified parameter in the current configuration. Note that the equals sign is not allowed. **Arguments**: • <*section*> is a name of the configuration file section with a configurable parameter. The argument is mandatory. • <*parameter*> is a name of the configurable parameter. The argument is mandatory. • <*value*> is a value that should be assigned to the configurable parameter. The argument is mandatory. The following format is always used to specify parameter values: <*section*>`.`<*parameter*> <*value*>. **Options**: `-a [--Add]`—do not substitute the current parameter value but add the specified value to the list (allowed only for parameters that can have several values specified as a list). You should also use this option to add new groups of parameters with a tag. `-e [--Erase]`—do not substitute the current parameter value but remove the specified value from its list (allowed only for parameters that can have several values, specified as a list). `-r [--Reset]`—reset the parameter value to the default one. At that, <*value*> is not required in the command and it is ignored if specified. The options are not mandatory. If they are not specified, the current parameter value (or the value list) is substituted with the specified value.

Command	Description
`cfshow [<section>[.<parameter>]]`	**Function**: Display parameters of the current Dr.Web for Kerio Connect configuration. The following format is used to display default parameters: <*section*>.<*parameter*> = <*value*>. Sections and parameters of non-installed components are not displayed. **Arguments**: • <*section*> is a name of the configuration file section which parameters are to be displayed. The argument is optional. If not specified, parameters of all configuration file sections are displayed. • <*parameter*> is a name of the displayed parameter. The argument is optional. If not specified, all parameters of the section are displayed. Otherwise, only this parameter is displayed. If a parameter is specified without the section name, all parameters with this name from all of the configuration file sections are displayed. **Options**: `--Uncut`—display all configuration parameters (not only those that are used by the currently installed set of components). Otherwise, only parameters used by the installed components are displayed. `--Changed`—display only those parameters which values differ from the default ones. `--Ini`—display parameter values in the ini file format (one file per line): at first, the section name is specified in square brackets, then, the section parameters listed as the <*parameter*> = <*value*> pairs. `--Value`—display only value of the specified parameter (the <*parameter*> argument is mandatory in this case).
`reload`	**Function**: Restart the Dr.Web for Kerio Connect service components. At that, logs are opened again, the configuration file is reread, and the attempt to restart abnormally terminated components is performed. **Arguments**: None. **Options**: None.

Commands to manage detected threats and the quarantine

The following commands for managing threats and the quarantine are available:

Command	Description
`threats [<action> <object>]`	**Function**: Apply the specified action to detected threats, selected by their identifiers. Type of the action is specified by the command option.

Command	Description
	If the action is not specified, display information on the detected but not neutralized threats. For each threat, the following information is displayed: • identifier assigned to the threat (an ordinal number); • full path to the infected file; • information about the threat (threat name and threat type according to the classification used by the Doctor Web company); • information about the file: size, the file owner, the time of the last modification; • history of operations applied to the threat: detection, actions applied, and so on. **Arguments**: None. **Options**: `--Directory` <*directory list*>—display only threats detected in the files from the specified directory list. `-f [--Follow]`—wait for new messages about threats and display the messages once they are received (CTRL+C interrupts the waiting). `--Format "`<*format string*>`"`—display information on threats in the specified format. ⚠ Each listed option will be ignored if it is specified together with on of the *action options*. Action options `--Cure` <*threat list*>—try to cure the listed threats. `--Delete` <*threat list*>—delete the listed threats. `--Ignore` <*threat list*>—ignore the listed threats. `--Quarantine` <*threat list*>—move the listed threats to the quarantine. The <*threat list*> parameter contains threat identifiers separated with commas. If it is required to apply the command to all detected threats, specify `All` instead of <*threat list*>. For example, to move all detected threats to the quarantine, use the command `$ drweb-ctl threats --Quarantine All`
`quarantine [`<*action*> <*object*>`]`	**Function**: Apply an action to the specified quarantined object.

Command	Description
	If an action is not specified, information on quarantined objects and their identifiers together with brief information on the original files moved to quarantine is displayed. The optional `--Format` option determines the format of the displayed information on isolated objects. If the `--Format` option is not specified, the following information is displayed for each isolated file: • identifier assigned to the quarantined object; • original path to the file moved to the quarantine; • date when the file was moved to the quarantine; • information about the file: size, the file owner, the time of the last modification; • information about the threat (threat name and threat type according to the classification used by the Doctor Web company). **Arguments**: None. **Options**: `-a [--Autonomous]`—start a separate scanner copy to perform the specified action with the quarantine and shut down the scanner copy after the action is performed. This option can be applied along with any options mentioned below. `--Format "<format string>"`—display information on the quarantined objects in the specified format. `-f [--Follow]`—wait for new messages about threats and display the messages once they are received (CTRL+C interrupts the waiting). ⚠ If the `--Format` or `-f [--Follow]` option is applied along with any action options mentioned below, it is ignored. `--Delete <object>`—delete the specified object from the quarantine. ⚠ Note that objects are deleted from the quarantine permanently—this action is irreversible. `--Cure <object>`—try to cure the specified object in the quarantine. ⚠ If the object is successfully cured, it will remain in the quarantine. To restore the cured object from the quarantine, use the `--Restore` option.

Command	Description
	`--Restore` <*object*>—restore the specified object from the quarantine to the original location.  You can restore the file from the quarantine even if it is infected. `--TargetPath` <*path*>—restore an object from the quarantine to the specified directory • as a file with the original name if the <path> parameter contains only a directory; • as a file with a new name if the <path> parameter contains not only a directory, but also a name under which the file is restored.  Note that this option can be used only with the `--Restore` option. As the <*object*> parameter, the quarantine object identifier is used. To apply this command to all quarantined objects, specify *All* instead of `<object>`. For example, to restore all objects from the quarantine, use the command `$ drweb-ctl quarantine --Restore All`  If the additional option `--TargetPath` is specified for the `--Restore All` variant, the option must set a path to a directory, not a path to a file.

Formatted output for the threats and quarantine commands

The output format is defined by the format string, specified as an argument of the optional option `--Format`. The format string must be specified in quotes. The format string can include common symbols (displayed "as is") as well as special markers that are changed for certain information during output.

The following markers are available:

- common for the `threats` and `quarantine` commands:

Marker	Description
`%{n}`	New string
`%{t}`	Tabulation
`%{threat_name}`	The name of a detected threat (virus) according to the classification used by the Doctor Web company
`%{threat_type}`	Threat type («known virus», and so on) according to the classification used by the Doctor Web company
`%{size}`	Original file size
`%{origin}`	The full name of the original file with the path to its location
`%{path}`	Synonym for `%{origin}`
`%{ctime}`	Date/time when the original file was modified in the following format: `%Y-%b-%d %H:% M:%S` (for example, `2018-Jul-20 15:58:01`)
`%{timestamp}`	Similar to `%{ctime}`, but in the UNIX timestamp format
`%{owner}`	Username of the original file owner
`%{rowner}`	The remote user, an owner of the original file. If the marker cannot be applied or the value is unknown, it is replaced with the "?" symbol.

- specific for the `threats` command:

Marker	Description
`%{hid}`	The identifier of a threat record in the history of events related to a threat
`%{tid}`	The threat identifier
`%{htime}`	Date/time of the event related to a threat
`%{app}`	The identifier of the component which processed a threat

Marker	Description
`%{event}`	The latest event related to a threat: • `FOUND`—a threat was detected; • `Cure`—a threat was cured; • `Quarantine`—a file with a threat was moved to quarantine; • `Delete`—a file with a threat was deleted; • `Ignore`—a threat was ignored; • `RECAPTURED`—a threat was detected again by another component.
`%{err}`	Error message text. If there is no error, the marker is replaced with an empty string.

- specific for the `quarantine` command:

Marker	Description
`%{qid}`	The identifier of a quarantined object
`%{qtime}`	Date/time of moving an object to the quarantine
`%{curetime}`	Date/time of an attempt to cure the quarantined object. If the marker cannot be applied or the value is unknown, it is replaced with the "?" symbol.
`%{cureres}`	The result of curing a quarantined object • `cured`—a threat is cured; • `not cured`—a threat was not cured or there was no attempt to cure it.

Commands to manage updates

The is one command to manage updates

Command	Description
`update`	**Function**: Instruct Dr.Web Updater to download and install updates of virus databases and scan engine from Doctor Web update servers or terminate a running update process. **Arguments**: None. **Options**: `--Stop`—terminate the running updating process.

Information commands

The following information commands are available:

Command	Description
`appinfo`	**Function**: Display information on active Dr.Web for Kerio Connect modules. The following information is displayed for every module: • internal name; • GNU/Linux process identifier (PID); • state (running, stopped, and so on); • error code, if the component operation has been terminated because of an error; • additional information (optionally). For the configuration daemon (`drweb-configd`), the following additional information is displayed: • the list of installed components (Installed); • the list of components that must be launched by the configuration daemon (Should run). **Arguments**: None. **Options**: `-f [--Follow]`—wait for new messages on module status change and display the messages once they are received (CTRL+C interrupts the waiting).
`baseinfo`	**Function**: Display information on the current version of the scan engine and of virus databases status. The following information is displayed: • scan engine version, • date and time when the current virus databases were issued, • number of available virus records, • time of the last successful update of the virus databases and the scan engine, • time of the next scheduled automatic update. **Arguments**: None. **Options**: `-l [--List]`—display the full list of downloaded files of virus databases and the virus records number in each file.
`license`	**Function**: Display information about the current license, or get a demo license or a key file for the license that has already been registered (for example, that has been registered on the Doctor Web website).

Command	Description
	If no option is specified, the following information is displayed in the standalone mode: • license number, • license expiration date and time. If you are using a license provided to you by the central protection server (for the use of the product in the central protection mode or in the mobile mode), the following information will be displayed: **Arguments**: None. **Options**: `--GetDemo`—request a demo key file that is valid for one month, and receive this key, if the conditions for the provision of a demo period have not been breached. `--GetRegistered` <*serial number*>—get a license key file for the specified serial number, if the conditions for the provision of a new key file have not been breached (for example, when the program does not function in the central protection mode while the license is managed by the central protection server).  If the serial number is not the one provided for the demo period, you must first register it on the Doctor Web website. To register a serial number or request a demo period, the Internet connection is required. For more information about the licensing of Doctor Web products, refer to the Licensing section.

Updating Anti-Virus Databases

Doctor Web products use virus databases to detect malicious software. These databases contain details and signatures for all currently known viruses and malicious programs. The Dr.Web for Kerio Connect application gets updates of virus databases online from the Doctor Web update servers. During the licensed period, Doctor Web provides you with regular updates to virus databases and application components, if available.

The special component Dr.Web Updater is used to automatically update virus databases. This plug-in is a part of Dr.Web for Kerio Connect and can be installed from the `drweb-update` package.

Upon startup of the operating system, the configuration management daemon (`drweb-configd`) will automatically launch the updater. Dr.Web Updater checks for available updates every 30 minutes to download and install them upon detection.

Logging

Dr.Web for Kerio Connect registers errors and application events in registration logs of the Kerio Connect email server: the debug log, the error log, and the security log, as well as in the syslog.

Debug Log

The debug log of the Kerio Conect email server contains information that is used for searching and analyzing errors in the Dr.Web for Kerio Connect operation.

To enable the debug logging

1. Open the administration console of the email server.
2. In the **Protocols** section, select the **debug** log.
3. Right-click the window of the **debug** log, and click **Messages**.
4. Select **Anti-virus** in the **Logging Messages** window. Click **OK**.

Operation System Log

The following information is logged in the system service syslog:

- notifications on the program starts and stops;
- license key file parameters including validity, licensed period (information is registered each time the program checks the license or when the license file changes);
- parameters of the program components. The information is logged when the program starts or components are updated;
- license invalidity notifications if the license key file is missing, some of the program components are not licensed, license is blocked or the license key file is corrupted. The information is logged during the program start and its operation;
- license expiration notifications. The information is logged 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 in the `/var/log/syslog` file (Debian). For more information on the system log, refer to your operating system documentation.

Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

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

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at https://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at https://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.