



Руководство администратора



© «Доктор Веб», 2020. Все права защищены

Настоящий документ носит информационный и справочный характер в отношении указанного в нем программного обеспечения семейства Dr.Web. Настоящий документ не является основанием для исчерпывающих выводов о наличии или отсутствии в программном обеспечении семейства Dr.Web каких-либо функциональных и/или технических параметров и не может быть использован при определении соответствия программного обеспечения семейства Dr.Web каким-либо требованиям, техническим заданиям и/или параметрам, а также иным документам третьих лиц.

Материалы, приведенные в данном документе, являются собственностью ООО «Доктор Веб» и могут быть использованы исключительно для личных целей приобретателя продукта. Никакая часть данного документа не может быть скопирована, размещена на сетевом ресурсе или передана по каналам связи и в средствах массовой информации или использована любым другим образом кроме использования для личных целей без ссылки на источник.

Товарные знаки

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA и логотип Dr.WEB являются зарегистрированными товарными знаками ООО «Доктор Веб» в России и/или других странах. Иные зарегистрированные товарные знаки, логотипы и наименования компаний, упомянутые в данном документе, являются собственностью их владельцев.

Ограничение ответственности

Ни при каких обстоятельствах ООО «Доктор Веб» и его поставщики не несут ответственности за ошибки и/или упущения, допущенные в данном документе, и понесенные в связи с ними убытки приобретателя продукта (прямые или косвенные, включая упущенную выгоду).

Dr.Web для Kerio Control

Версия 11.1

Руководство администратора

22.01.2020

ООО «Доктор Веб», Центральный офис в России

Адрес: 125040, Россия, Москва 3-я улица Ямского поля, вл.2, корп.12А

Сайт: <https://www.drweb.com/>

Телефон: +7 (495) 789-45-87

Информацию о региональных представительствах и офисах Вы можете найти на официальном сайте компании.

ООО «Доктор Веб»

Компания «Доктор Веб» — российский разработчик средств информационной безопасности.

Компания «Доктор Веб» предлагает эффективные антивирусные и антиспам-решения как для государственных организаций и крупных компаний, так и для частных пользователей.

Антивирусные решения семейства Dr.Web разрабатываются с 1992 года и неизменно демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности.

Сертификаты и награды, а также обширная география пользователей свидетельствуют об исключительном доверии к продуктам компании.

Мы благодарны пользователям за поддержку решений семейства Dr.Web!



Содержание

Введение	5
Используемые обозначения	6
О продукте	7
Компоненты приложения	7
Лицензирование	8
Регистрация и активация лицензии	8
Запрос демонстрационного периода	10
Ключевой файл	10
Определение параметров лицензирования	11
Обновление лицензии	12
Установка и удаление подключаемого модуля	13
Системные требования	14
Установка приложения	14
Установка в режиме командной строки	16
Переход на новую версию	17
Проверка корректности установки	17
Удаление приложения	18
Подключение и настройка работы приложения	20
Настройка антивирусного приложения	21
Выбор протоколов	22
Проверка работоспособности	22
Проверка на вирусы	24
Методы обнаружения угроз	25
Карантин	27
Работа с утилитой Dr.Web Ctl	28
Формат вызова утилиты	29
Команды drweb-ctl	30
Обновление вирусных баз	39
Регистрация событий	40
Техническая поддержка	41



Введение

Благодарим вас за приобретение приложения Dr.Web для Kerio Control. Данный продукт обеспечивает надежную защиту корпоративного сетевого трафика от вирусных угроз. Приложение подключается к межсетевому экрану Kerio Control и осуществляет антивирусную проверку файлов, передаваемых по протоколам HTTP, FTP, SMTP и POP3.

В данном программном продукте применены наиболее передовые разработки и технологии компании «Доктор Веб», которые позволяют обнаруживать различные типы вредоносных объектов, представляющих угрозу функционирования сети и информационной безопасности пользователей.

Настоящее руководство призвано помочь администраторам корпоративных сетей, использующих межсетевой экран Kerio Control, установить и настроить подключаемый модуль Dr.Web для Kerio Control, а также ознакомиться с основными функциями подключаемого модуля.

Дополнительную информацию о возможностях антивирусной проверки сетевого трафика в рамках межсетевого экрана Kerio Control можно найти на официальном сайте компании «Kerio» по адресу <http://www.kerio.ru/products/kerio-control>.



Используемые обозначения

В данном руководстве используются следующие условные обозначения:

Обозначение	Комментарий
	Предупреждение о возможных ошибочных ситуациях, а также важных моментах, на которые следует обратить особое внимание.
<i>Антивирусная сеть</i>	Новый термин или акцент на термине в описаниях.
<code><IP-address></code>	Поля для замены функциональных названий фактическими значениями.
Сохранить	Названия экранных кнопок, окон, пунктов меню и других элементов программного интерфейса.
CTRL	Обозначения клавиш клавиатуры.
<code>/home/user</code>	Наименования файлов и каталогов, фрагменты программного кода.
<u>Приложение А</u>	Перекрестные ссылки на главы документа или гиперссылки на внешние ресурсы.



Команды, которые требуется ввести с клавиатуры в командную строку операционной системы (в терминале или эмуляторе терминала), в руководстве предваряются символом приглашения ко вводу команды: `$` или `#`. Символ указывает, какие полномочия пользователя необходимы для исполнения данной команды:

`$` – для исполнения команды достаточно обычных прав пользователя;

`#` – для исполнения команды требуются права суперпользователя (обычно – *root*). Для повышения прав можно использовать команды `su` и `sudo`.



О продукте

Dr.Web для Kerio Control проверяет сетевой трафик на вирусы, программы дозвона, рекламные программы, потенциально опасные программы, программы взлома и программы-шутки. При обнаружении угроз безопасности к ним применяются действия согласно настройкам межсетевого экрана Kerio Control.

Основные функции приложения

Dr.Web для Kerio Control выполняет следующие функции:

- антивирусную проверку файлов, передаваемых по протоколам HTTP, FTP, SMTP и POP3, а именно:
 - вложенных файлов почтовых сообщений;
 - файлов веб-трафика, загружаемых по протоколам HTTP и FTP;
- обнаружение вредоносного программного обеспечения;
- изоляцию инфицированных файлов в карантине;
- использование эвристического анализатора для дополнительной защиты от неизвестных вирусов;
- регулярное автоматическое обновление вирусных баз.



Dr.Web для Kerio Control не проверяет файлы, передаваемые по протоколу HTTPS.

Компоненты приложения

Dr.Web для Kerio Control состоит из нескольких дополняющих друг друга компонентов, которые взаимодействуют между собой:

- демон управления конфигурацией (`drweb-configd`). Управляет активностью всех компонентов Dr.Web для Kerio Control в зависимости от выбранных [настроек](#), а также хранит информацию о лицензии и настройках, предоставляя ее тем или иным компонентам при необходимости;
- сканирующее ядро Dr.Web Scanning Engine (`drweb-se`). Осуществляет [антивирусную проверку](#);
- модуль обновления Dr.Web Updater (`drweb-update`). Предназначен для автоматического [обновления вирусных баз](#) путем загрузки их с серверов обновлений компании «Доктор Веб» через сеть Интернет;
- утилита управления [Dr.Web Ctl](#) (`drweb-ctl`). Предоставляет пользователю интерфейс для управления работой приложения из командной строки.



Лицензирование

Права пользователя на использование копии программного продукта Dr.Web для Kerio Control подтверждаются и регулируются [лицензией](#), приобретенной у компании «Доктор Веб» или ее партнеров. Параметры лицензии, регулирующие права пользователя, установлены в соответствии с Лицензионным соглашением (см. <https://license.drweb.com/agreement/>), условия которого принимаются пользователем [при установке](#) программного продукта на компьютер.

В лицензии фиксируется информация о пользователе и продавце, а также параметры использования приобретенной копии продукта, в частности:

- перечень компонентов, которые разрешено использовать;
- период, в течение которого разрешено использование Dr.Web для Kerio Control;
- наличие или отсутствие технической поддержки;
- другие ограничения (например, количество компьютеров, на которых разрешено использовать Dr.Web для Kerio Control).

Имеется также возможность активировать для приобретенной копии продукта демонстрационный период. В этом случае, если не нарушены [условия активации](#), пользователь получает право на полноценное использование Dr.Web для Kerio Control в течение демонстрационного периода.

Каждой лицензии на использование программных продуктов компании «Доктор Веб» сопоставлен уникальный серийный номер, а на локальном компьютере пользователя с лицензией связывается специальный файл, регулирующий работу компонентов продукта в соответствии с [параметрами лицензии](#). Он называется *лицензионным ключевым файлом*. При активации демонстрационного периода также автоматически формируется специальный ключевой файл, называемый *демонстрационным*.

В случае отсутствия у пользователя действующей лицензии или активированного демонстрационного периода, антивирусные функции компонентов Dr.Web для Kerio Control блокируются, кроме того, становится недоступен сервис регулярных [обновлений вирусных баз](#) с серверов обновлений компании «Доктор Веб».

Регистрация и активация лицензии

Приобретение, регистрация и активация лицензии

При приобретении лицензии клиент получает возможность в течение всего срока ее действия получать обновления с серверов обновлений компании «Доктор Веб», а также получать стандартную техническую поддержку компании «Доктор Веб» и ее партнеров.



Приобрести любой антивирусный продукт компании «Доктор Веб» или серийный номер для него можно у наших [партнеров](#) или через [интернет-магазин](#). Дополнительную информацию о возможных вариантах лицензий можно найти на официальном сайте компании «Доктор Веб» <https://license.drweb.com/>.

Регистрация лицензии подтверждает, что вы являетесь полноправным пользователем продукта Dr.Web для Kerio Control, и активирует его функции, включая функции обновления вирусных баз. Рекомендуется выполнять регистрацию и активацию лицензии сразу после установки.

При активации приобретенной лицензии необходимо указать ее серийный номер. Этот номер может поставляться вместе с продуктом или по электронной почте, при покупке или продлении лицензии онлайн. Приобретенная лицензия может быть активирована непосредственно на официальном сайте компании «Доктор Веб» по адресу <https://products.drweb.com/register/>.



В случае регистрации лицензии, продлевающей лицензию с истекшим сроком годности, требуется указать серийный номер или лицензионный ключевой файл предыдущей лицензии, в противном случае срок действия новой лицензии будет сокращен на 150 дней.

Если имеется комплект лицензий, выданных для использования продукта на нескольких серверах, то при регистрации имеется возможность указать, что Dr.Web для Kerio Control будет использоваться только на одном сервере. В этом случае все лицензии из комплекта будут объединены в одну и срок ее действия будет автоматически увеличен.

Повторная регистрация

Повторная регистрация может потребоваться в случае утраты лицензионного ключевого файла при наличии активной лицензии. При повторной регистрации необходимо указать те же персональные данные, которые были введены при первой регистрации лицензии. Допускается использовать другой адрес электронной почты – в таком случае лицензионный ключевой файл будет выслан по новому адресу.

Количество запросов на получение лицензионного ключевого файла ограничено – регистрация лицензии с одним и тем же серийным номером допускается не более 25 раз. Если это число превышено, лицензионный ключевой файл не будет выслан. В этом случае обратитесь в [службу технической поддержки](#) компании «Доктор Веб», при этом в запросе следует подробно описать ситуацию, указать персональные данные, введенные при регистрации, и серийный номер лицензии. Лицензионный ключевой файл будет выслан службой технической поддержки по электронной почте.

После получения ключевого файла по электронной почте, вам необходимо выполнить процедуру [его установки](#).



Запрос демонстрационного периода

Для получения демонстрационного периода на использование продукта Dr.Web для Kerio Control следует отправить запрос с официального сайта компании «Доктор Веб» по адресу <https://download.drweb.com/demoreq/biz/>. После выбора продукта и заполнения анкеты вы получите по электронной почте серийный номер или ключевой файл для активации демонстрационного периода.



Демонстрационный период использования продукта может быть выдан повторно для того же компьютера только по истечении определенного периода времени.

Также можете воспользоваться командой `license` утилиты управления [Dr.Web Ctl](#), которая позволяет автоматически получить демонстрационный или лицензионный ключевой файл для серийного номера зарегистрированной лицензии.

Ключевой файл

Права пользователя на использование программного продукта Dr.Web для Kerio Control хранятся в специальном файле, называемом *ключевым*. В ключевом файле фиксируются параметры использования продукта в соответствии с приобретенной лицензией или активированным демонстрационным периодом.

Ключевой файл является *действительным* при одновременном выполнении следующих условий:

- срок действия лицензии не истек,
- ключевой файл распространяется на все компоненты, используемые Dr.Web для Kerio Control,
- целостность ключевого файла не нарушена.

При нарушении любого из этих условий ключевой файл становится *недействительным*, при этом Dr.Web для Kerio Control перестает обнаруживать вредоносные программы и пропускает объекты электронных сообщений без изменений.



Содержимое ключевого файла защищено от редактирования при помощи механизма электронной цифровой подписи, поэтому редактирование делает ключевой файл недействительным. Не рекомендуется открывать ключевой файл в текстовых редакторах во избежание случайной порчи его содержимого.

Установка ключевого файла

Для работы Dr.Web для Kerio Control необходим действительный ключевой файл, путь к которому указывается [после установки](#) подключаемого модуля.



При работе Dr.Web для Kerio Control ключевой файл по умолчанию должен находиться в каталоге `/etc/opt/drweb.com` и называться `drweb32.key`.

Компоненты подключаемого модуля регулярно проверяют наличие и корректность ключевого файла. При отсутствии действительного ключевого файла (лицензионного или демонстрационного), а также по истечении срока его действия, антивирусные функции всех компонентов блокируются до установки *действительного* ключевого файла.

Рекомендуется сохранять имеющийся лицензионный ключевой файл до истечения срока его действия. В этом случае при переустановке продукта или переносе его на другой сервер повторная регистрация серийного номера лицензии не потребуется. Можно использовать лицензионный ключевой файл, полученный при первом прохождении процедуры регистрации.

При наличии ключевого файла, соответствующего действующей лицензии на Dr.Web для Kerio Control (например, он был получен от продавца по электронной почте после регистрации, или приложение переносится на другой сервер), имеется возможность активировать продукт, просто указав путь к имеющемуся ключевому файлу. Это можно сделать следующим образом:

1. Распакуйте ключевой файл, если он был получен в архиве, и сохраните его в любой доступный каталог (например, в домашний каталог или на съемный носитель).



По электронной почте ключевые файлы обычно передаются упакованными в zip-архивы. Архив, содержащий ключевой файл для активации продукта, обычно имеет имя `agent.zip` (обратите внимание, что если в сообщении содержится несколько архивов, то нужно использовать именно архив `agent.zip`).

2. Далее скопируйте ключевой файл в каталог `/etc/opt/drweb.com` и, если необходимо, переименуйте в `drweb32.key`.
3. Перезапустите Dr.Web для Kerio Control, выполнив команду `reload` утилиты управления [Dr.Web Ctl](#) для применения внесенных изменений.

Определение параметров лицензирования

Лицензионный ключевой файл регулирует использование Dr.Web для Kerio Control.

Определение параметров лицензирования

1. Чтобы определить параметры лицензирования, записанные в вашем ключевом файле, откройте файл для просмотра.



Ключевой файл имеет формат, защищенный от редактирования, поэтому редактирование этого файла делает его недействительным. Чтобы избежать порчи ключевого файла, не сохраняйте его при закрытии текстового редактора.



2. Проверьте следующие параметры лицензирования:

Параметр	Комментарий
Группа [Key], параметр Applications	Указывает компоненты, которые разрешено использовать владельцу лицензии.  Для использования ключевого файла с Dr.Web для Kerio Control в списке компонентов обязательно должен присутствовать компонент KerioPlugin.
Группа [Key], параметр Expires	Указывает срок действия лицензионного ключевого файла в формате: Год-Месяц-День.
Группа [User], параметр Name	Указывает регистрационное имя владельца лицензии.
Группа [User], параметр Computers	Указывает количество пользователей, защищаемых модулем.

3. Закройте файл, не сохраняя изменений.

Обновление лицензии

В некоторых случаях, например, при изменении характеристик защищаемой системы или требований к ее безопасности либо при окончании срока действия лицензии вы можете принять решение о приобретении новой или расширенной лицензии на Dr.Web для Kerio Control. В таком случае потребуется заменить уже существующий и зарегистрированный в системе лицензионный ключевой файл. Приложение поддерживает обновление лицензии «на лету», при котором не требуется переустанавливать Dr.Web для Kerio Control или прерывать его работу.

Замена ключевого файла

1. Чтобы обновить лицензию, скопируйте новый ключевой файл в каталог `/etc/opt/drweb.com/`.
2. Чтобы Dr.Web для Kerio Control переключился на использование нового ключевого файла, необходимо перезапустить демон управления конфигурацией ([drweb-configd](#)).

Дополнительную информацию о видах лицензий можно найти на официальном сайте компании «Доктор Веб» по адресу <https://license.drweb.com/products/biz>.



Установка и удаление подключаемого модуля

Приложение Dr.Web для Kerio Control устанавливается на тот же компьютер, на котором установлен межсетевой экран Kerio Control, и используется им в качестве внешнего антивирусного программного обеспечения через интерфейс подключаемых модулей.

Продукт Dr.Web для Kerio Control поставляется в виде самораспаковывающегося архива `drweb-[version]-av-kerio-control-linux-amd64.run`, где `[version]` – номер версии. В архиве содержатся следующие пакеты:

Название	Описание
<code>drweb-common</code>	Содержит: • программу удаления (<code>uninst.sh</code>), • файлы лицензионного соглашения, • структуру каталогов. В процессе установки данного пакета создаются группа <code>drweb</code> и пользователь <code>drweb</code> .
<code>drweb-bases</code>	Содержит вирусные базы (<code>.vdb</code>). Для установки требуется пакет <code>drweb-common</code> .
<code>drweb-update</code>	Содержит модуль обновления антивирусного ядра и вирусных баз. Для установки требуется пакет <code>drweb-common</code> .
<code>drweb-configd</code>	Содержит файлы демона управления конфигурацией Dr.Web для Kerio Control.
<code>drweb-ctl</code>	Содержит файлы утилиты, обеспечивающей управление Dr.Web для Kerio Control из командной строки, и документацию к ней.
<code>drweb-se</code>	Содержит исполняемые файлы компонента Dr.Web Scanning Engine и документацию к нему. Для установки требуется пакет <code>drweb-bases</code> .
<code>drweb-kerio-control-plugin</code>	Содержит библиотеку <code>avir_drweb.so</code> подключаемого модуля Dr.Web для Kerio Control. Используется для установки и работы с межсетевым экраном Kerio Control версии 9.2.1 и выше.
<code>drweb-kerio-control-doc</code>	Содержит документацию приложения Dr.Web для Kerio Control.
<code>drweb-libs</code>	Содержит библиотеки, общие для всех компонентов продукта.

Дополнительную информацию об использовании антивирусного программного обеспечения межсетевым экраном Kerio Control можно найти на официальном сайте компании «Kerio» по адресу <http://www.kerio.ru/products/kerio-control>.



Системные требования

Компьютер, на который устанавливается Dr.Web для Kerio Control, должен удовлетворять следующим системным требованиям:

Параметр	Требование
Место на жестком диске	Не менее 350 МБ свободного дискового пространства без учета места для хранилища файлов карантина
Операционная система	Одна из следующих: • Kerio Control VMware Virtual Appliance • Kerio Control Software Appliance • Kerio Control Hyper-V Virtual Appliance
Межсетевой экран	Kerio Control версии 9.2.1 или выше

Настоящие требования относятся только к Dr.Web для Kerio Control. Приложение может работать на компьютерах, на которых установлен межсетевой экран Kerio Control. Системные требования к межсетевому экрану содержатся в документации Kerio Control.

Dr.Web для Kerio Control также поддерживает установку и работу в средах Kerio Control VMware Virtual Appliance, Kerio Control Software Appliance и Kerio Control Hyper-V Virtual Appliance. Информацию о данных программных решениях можно найти на официальном сайте компании «Kerio» по адресу <http://www.kerio.ru/support/kerio-control>.

Установка приложения

В этом разделе описывается [процедура установки](#) Dr.Web для Kerio Control, а также рассмотрена возможность [перехода на новую версию](#), если на вашем компьютере уже установлен Dr.Web для Kerio Control предыдущей версии.

Перед установкой приложения удостоверьтесь, что компьютер удовлетворяет минимальным [системным требованиям](#).

Процедура установки приложения

Чтобы установить компоненты приложения Dr.Web для Kerio Control, выполните следующие действия:

1. Если необходимо, загрузите инсталляционный файл с официального сайта компании «Доктор Веб» по адресу <https://download.drweb.com/>.
2. Включите SSH-доступ на межсетевом экране. Для этого:



- на вкладке **Состояние** консоли администрирования межсетевого экрана Kerio Control, удерживая клавишу SHIFT, откройте раздел **Состояние системы** и нажмите **Включить SSH**;
 - в окне предупреждения выберите **Да**.
3. Скопируйте на компьютер с межсетевым экраном Kerio Control архив `drweb-[version]-av-kerio-control-linux-amd64.run` и лицензионный ключевой файл Dr.Web для Kerio Control.
 4. Разрешите исполнение архивного файла, например, командой:

```
# chmod +x <имя_файла>.run
```

5. Запустите архивный файл на исполнение командой:

```
# ./<имя_файла>.run
```

При этом будет проверена целостность архива. Затем файлы, содержащиеся в архиве, будут распакованы во временный каталог и автоматически запустится программа установки, использующая режим командной строки.



Если в части файловой системы, содержащей временный каталог, не имеется достаточного количества свободного места для распаковки дистрибутива, то процесс установки будет завершен после выдачи соответствующего сообщения. В этом случае следует повторить распаковку, изменив значение системной переменной окружения `TMPDIR` таким образом, чтобы она указывала на каталог, имеющий достаточное количество свободного места. Также вы можете воспользоваться ключом распаковки в указанный каталог `--target`.

6. Следуйте [инструкциям программы установки](#).

Все установочные файлы, извлеченные из архива, будут автоматически удалены после окончания установки.

Имеется возможность установки в полностью автоматическом режиме (без показа интерфейса пользователя, в том числе диалогов программы установки в режиме командной строки). Для этого необходимо на [шаге 5](#) выполнить команду:

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



Обратите внимание, что использование этой опции означает, что *вы соглашаетесь с условиями Лицензионного соглашения*. С текстом Лицензионного соглашения можно ознакомиться после установки продукта, прочитав файл `/var/opt/drweb.com/opt/share/doc/LICENSE`. Расширение файла указывает язык, на котором написан текст Лицензионного соглашения. Файл `LICENSE` без расширения хранит текст Лицензионного соглашения на английском языке. Если *вы не согласны с условиями Лицензионного соглашения*, вам следует удалить продукт после установки.



Установка в режиме командной строки

После запуска программы установки в режиме командной строки, на экране появится текст приглашения к установке.

1. Для продолжения установки Dr.Web для Kerio Control введите `Y` или `Yes` в строке ввода (значения регистронезависимые) и нажмите клавишу ENTER. В противном случае введите `N` или `No` и установка будет прекращена.
2. Откроется Лицензионное соглашение. Для перелистывания текста лицензионного соглашения пользуйтесь клавишами ENTER (перелистывание текста на одну строчку вниз) и ПРОБЕЛ (перелистывание текста вниз на экран). Обратите внимание, что перелистывание текста Лицензионного соглашения назад (вверх) не предусмотрено. Для продолжения установки требуется принять Лицензионное соглашение. Для этого введите `Y` или `Yes` в строке ввода и нажмите клавишу ENTER. В противном случае установка будет прекращена.
3. После принятия условий Лицензионного соглашения автоматически будет запущен процесс установки Dr.Web для Kerio Control на компьютер. При этом на экран будет выводиться информация о ходе установки, включающая в себя перечень устанавливаемых компонентов.
4. В случае успешного окончания процесса установки, если продукт предусматривает автоматическую настройку перед запуском, будет автоматически запущена [интерактивная программа настройки](#) продукта.

В случае возникновения ошибки на экран будет выведено соответствующее сообщение с описанием ошибки, после чего работа программы установки будет завершена. Если установка была прервана из-за ошибки, следует устранить проблемы, вызвавшие ошибку установки, после чего повторить процесс установки.

После установки подключаемый модуль Dr.Web для Kerio Control может быть [подключен](#) к межсетевому экрану.

Интерактивная программа настройки

Интерактивная программа настройки позволяет установить имеющийся у вас ключевой файл продукта.

1. Если вы желаете выполнить настройку подключаемого модуля, то после запуска программы нужно ответить `Y` или `Yes` на вопрос «Do you want to continue?». Если вы ответите `N` или `No`, работа программы настройки будет завершена.
2. Если в данный момент на компьютере (в стандартном для продукта каталоге) не имеется ключевого файла, программа предложит указать путь к ключевому файлу. Если на вашем компьютере имеется действующий ключевой файл, укажите путь к нему и нажмите ENTER. Ключевой файл будет скопирован в стандартный для продукта каталог.

Если ключевой файл уже размещен в стандартном для продукта каталоге, этот шаг будет автоматически пропущен.



Чтобы пропустить этот шаг, введите 0. В этом случае вы сможете установить ключевой файл вручную позднее.

3. По окончании внесения изменений необходимо нажать клавишу ENTER для завершения работы программы настройки.



Если программа настройки по тем или иным причинам не была выполнена, то необходимо лицензионный ключевой файл скопировать вручную в каталог `/etc/opt/drweb.com/`, после чего перезапустить сервис с помощью команды `reload` утилиты управления [Dr.Web Ctl](#).

Переход на новую версию

Выполните [процедуру установки](#) новой версии Dr.Web для Kerio Control. Далее, чтобы обновление вступило в силу, выключите подключаемый модуль с помощью консоли администрирования межсетевого экрана Kerio Control, после чего снова [включите его](#).

При обновлении продукта уже имеющийся у вас ключевой файл будет автоматически установлен в надлежащее место – в стандартный для новой версии продукта каталог.



В случае возникновения проблем с автоматической установкой лицензионного ключевого файла, вы можете выполнить его [установку вручную](#).

В случае утраты действующего лицензионного ключевого файла обратитесь в [службу технической поддержки](#) компании «Доктор Веб».

Проверка корректности установки

Чтобы проверить корректность установки, удостоверьтесь, что следующие каталоги созданы и содержат все необходимые файлы:

Каталог	Имя файла	Описание
<code>/etc/opt/drweb.com</code>	<code>drweb32.key</code>	Ключевой файл
<code>/opt/dweb.com/bin</code>	<code>drweb-configd</code>	Демон управления конфигурацией
	<code>drweb-se</code>	Сканирующий модуль
	<code>drweb-update</code>	Модуль обновления
<code>/opt/kerio/winroute/avirplugins</code>	<code>avir_drweb.so</code>	Библиотека Dr.Web для Kerio Control

Если в процессе установки приложения возникли ошибки, вы можете обратиться за помощью в [службу технической поддержки](#) компании «Доктор Веб».



Удаление приложения



Для удаления приложения Dr.Web для Kerio Control необходимо иметь права администратора.

Перед удалением Dr.Web для Kerio Control отключите использование антивирусного приложения межсетевым экраном Kerio Control. Для этого:

1. Запустите консоль администрирования межсетевого экрана.
2. Откройте подраздел **Конфигурация** → **Антивирус**.
3. Снимите флажок **Использовать внешнее антивирусное ПО** для выбранного антивируса **Doctor Web for Kerio** на вкладке **Антивирусная программа** в группе настроек **Антивирусное ПО**.
4. Нажмите кнопку **Применить**.
Использование Dr.Web для Kerio Control будет отключено.

Удаление Dr.Web для Kerio Control

Чтобы удалить приложение с помощью программы автоматического удаления выполните следующие действия:

1. Выполните команду:

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

2. Для запуска процесса удаления Dr.Web для Kerio Control введите Y или Yes в строке ввода и нажмите клавишу ENTER. В противном случае введите N или No и работа программы удаления будет завершена.



Обратите внимание, что при запуске программы автоматического удаления она удалит не только приложение Dr.Web для Kerio Control, но и все другие продукты компании «Доктор Веб», установленные на вашем компьютере. Для удаления только Dr.Web для Kerio Control вместо запуска программы автоматического удаления воспользуйтесь [менеджером пакетов](#) Zypper.

3. После подтверждения удаления запустится процедура удаления всех установленных пакетов антивирусных продуктов компании «Доктор Веб». При этом на экран будут выдаваться записи, фиксируемые в журнал и отражающие ход процесса удаления. Программа завершит свою работу автоматически после удаления всех компонентов.



Лицензионный ключевой файл не удаляется автоматически. Но его можно удалить вручную.

Кроме того, установленные [параметры проверки](#) сохраняются и автоматически используются при переустановке Dr.Web для Kerio Control.



Для выборочного удаления компонентов следует воспользоваться менеджером пакетов Zypper, автоматически установленным вместе с продуктом. Для этого:

1. Перейдите в каталог `/opt/drweb.com/bin` и выполните следующую команду:

```
# ./zypper rm <имя_пакета>
```

2. Выберите компоненты, которые хотите удалить, следуя инструкциям на экране.
3. Подтвердите удаление выбранных компонентов. Для этого введите `Y` или `Yes` в строке ввода и нажмите клавишу `ENTER`.
4. Начнется процесс удаления выбранных компонентов. Отчет о результатах прохождения каждого из этапов данного процесса выводится на экран в режиме реального времени.
По окончании процесса удаления будет выведено сообщение о том, что выбранные компоненты успешно удалены.

Для переустановки какого-либо компонента можно сначала удалить его, а потом заново установить.

Имеется возможность удаления Dr.Web для Kerio Control в полностью автоматическом режиме (без вызова интерфейса пользователя, в том числе без диалогов программы удаления в режиме командной строки). Для этого необходимо запустить программу следующим образом:

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



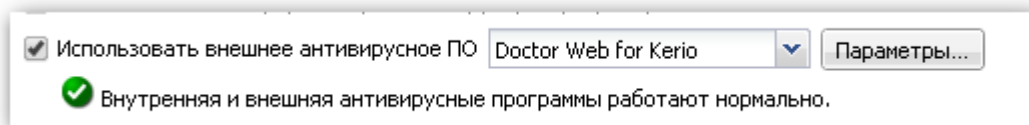
Подключение и настройка работы приложения

Dr.Web для Kerio Control подключается к межсетевому экрану Kerio Control в качестве внешнего антивирусного программного обеспечения и осуществляет проверку различных видов сетевого трафика в соответствии с настройками межсетевого экрана.

Подключение Dr.Web для Kerio Control

1. Запустите консоль администрирования межсетевого экрана.
2. Откройте подраздел **Конфигурация** → **Антивирус**.
3. Установите флажок **Использовать внешнее антивирусное ПО** на вкладке **Антивирусная программа** в группе настроек **Антивирусное ПО**.
4. Выберите **Doctor Web for Kerio** в выпадающем списке.
5. Настройте [параметры приложения](#).
6. [Выберите протоколы](#) для сканирования.
7. Нажмите кнопку **Применить**.

Если подключение прошло успешно, под настройкой выбора антивирусного программного обеспечения появится соответствующее сообщение:



Если при подключении антивирусного приложения возникли ошибки, просмотрите журнал ошибок (error) межсетевого экрана и для решения возникшей проблемы воспользуйтесь руководством администратора межсетевого экрана Kerio Control.

Дополнительную информацию об использовании антивирусного программного обеспечения межсетевого экрана и возможных ошибках подключения можно найти в руководстве администратора межсетевого экрана Kerio Control и на сайте компании «Kerio» по адресу <http://www.kerio.ru/products/kerio-control>.



Настройка антивирусного приложения

Параметры Dr.Web для Kerio Control определяют специфику его работы, а также регистрацию событий приложения. Параметры могут быть изменены с помощью консоли администрирования межсетевого экрана в разделе **Конфигурация** → **Антивирус**. Для изменения настроек выполните следующие действия:

1. Нажмите кнопку **Параметры** на вкладке **Антивирусная программа** в группе настроек **Антивирусное ПО** справа от названия приложения **Doctor Web for Kerio**. Откроется список параметров, с помощью которых можно настроить [антивирусную проверку](#) и [работу с карантином](#):

Параметр	Комментарий
Detect adware, Detect dialers, Detect hacktools, Detect jokes, Detect riskware	Перечисленные параметры позволяют настроить проверку интернет-трафика на наличие рекламных программ, программ дозвона, программ взлома, программ-шуток и потенциально опасных программ. Каждый параметр может принимать одно из следующих значений: • No – объекты, содержащие данный тип вредоносного программного обеспечения, будут пропущены; • Yes – передача подобных объектов запрещена. Данное значение установлено по умолчанию для всех типов вредоносных объектов.
Enable heuristic	С помощью данного параметра можно включить или отключить эвристический анализатор, позволяющий обнаруживать неизвестные вирусы. Параметр может принимать одно из следующих значений: • No – для отключения эвристического анализатора; • Yes – для включения эвристического анализатора. По умолчанию эвристический анализатор включен.
Quarantine directory	Данная настройка задает путь к каталогу карантина. По умолчанию установлено значение <code>/var/lib/drweb/quarantine</code> .
Quarantine enabled	Данный параметр позволяет включить или отключить перемещение инфицированных объектов в карантин. Параметр может принимать одно из следующих значений: • No – для отключения перемещения инфицированных объектов в карантин. Данное значение установлено по умолчанию; • Yes – для включения перемещения инфицированных объектов в карантин.

2. Для того чтобы изменить значение того или иного параметра, выберите его в списке и нажмите кнопку **Редактировать**. В окне **Редактировать значение** укажите значение выбранного параметра, после чего нажмите кнопку **ОК**.



При настройке данных параметров необходимо учитывать, что значения No/Yes зависят от регистра.



3. Нажмите кнопку **ОК** в окне **Параметры антивирусной программы**, когда закончите настройку параметров.
4. Нажмите кнопку **Применить** в разделе **Антивирус** на вкладке **Антивирусная программа** для сохранения сделанных изменений.



При переустановке Dr.Web для Kerio Control заданные параметры проверки сохраняются.

Выбор протоколов

Dr.Web для Kerio Control осуществляет проверку сетевого трафика по нескольким протоколам, которые могут быть выбраны с помощью консоли администрирования межсетевого экрана Kerio Control в разделе **Конфигурация** → **Антивирус** на вкладке **Антивирусная программа**.

Чтобы выбрать протоколы для сканирования:

1. В группе настроек **Протоколы** укажите протоколы, которые Dr.Web для Kerio Control будет подвергать проверке. Можно выбрать следующие протоколы для сканирования: HTTP, FTP, SMTP и POP3.
2. При желании можно включить ограничение на размер сканируемого файла и указать максимальное значение размера файла (в килобайтах) в соответствующем текстовом поле. По умолчанию установлено значение 4096 Кб.

Подробнее о настройках сканирования, определяемых с помощью консоли администрирования межсетевого экрана, можно узнать из руководства администратора межсетевого экрана Kerio Control.

Проверка работоспособности

Для проверки работоспособности приложения необходимо убедиться в способности Dr.Web для Kerio Control обнаруживать вирусы. Для проверки выполните следующие действия:

1. Откройте в браузере страницу <http://www.eicar.org/download/eicar.com>, чтобы скачать тестовый файл EICAR-Test-File. Информацию о тестовом вирусе EICAR можно найти по адресу http://en.wikipedia.org/wiki/EICAR_test_file.
Указанная страница не должна открыться, а в журнале оповещений (alert) межсетевого экрана Kerio Control должна быть зафиксирована информация о попытке скачать инфицированный файл.



2. Отправьте письмо с тестовым инфицированным файлом EICAR-Test-File во вложении через сервер, защищаемый межсетевым экраном Kerio Control.

Проверьте полученное письмо. Инфицированный вложенный файл должен быть удален из письма. Заголовок письма может содержать префикс, оповещающий о найденном вредоносном объекте.

Если в процессе работы приложения возникли ошибки, вы можете обратиться за помощью в [службу технической поддержки](#) компании «Доктор Веб».



Проверка на вирусы

Приложение Dr.Web для Kerio Control обнаруживает инфицированные вложения в электронных письмах и инфицированные объекты, передаваемые по протоколам HTTP и FTP.

Dr.Web для Kerio Control проверяет сетевой трафик на наличие следующих типов вредоносных объектов и программ:

- инфицированные архивы;
- файлы-бомбы или архивы-бомбы;
- рекламные программы;
- программы взлома;
- программы дозвона;
- программы-шутки;
- потенциально опасные программы.

Во время антивирусной проверки Dr.Web для Kerio Control использует различные [методы обнаружения угроз](#).

С помощью настройки [параметров антивирусного приложения](#) через консоль администрирования межсетевого экрана Kerio Control можно определить типы обнаруживаемых вредоносных объектов и действия над ними. Кроме того, вы можете [выбрать протоколы](#), которые Dr.Web для Kerio Control будет проверять.

Настройки сканирования определяются с помощью вкладок раздела **Конфигурация** → **Антивирус** через консоль администрирования межсетевого экрана Kerio Control:

Вкладка	Комментарий
Сканирование HTTP, FTP	При обнаружении вируса, передаваемого по протоколам HTTP и FTP, его передача будет запрещена, и межсетевой экран выполнит действия, установленные администратором на данной вкладке настроек. Здесь же определяются действия в случае, если антивирусу не удалось проверить файл, и правила сканирования, определяющие типы файлов, проверяемых Dr.Web для Kerio Control.
Сканирование электронной почты	На данной вкладке вы можете задать настройки антивирусной проверки протоколов SMTP, POP3 и определить действия в случае обнаружения вирусов во вложениях электронных писем и в случае невозможности проверки файла (например, если файл поврежден или защищен паролем).

В случае обнаружения подключаемым модулем Dr.Web для Kerio Control угроз, администратор может настроить отправку уведомлений по электронной почте или в виде текстового сообщения SMS. Кроме того, информация обо всех обнаруженных угрозах фиксируется в журнале оповещений (alert) межсетевого экрана Kerio Control.



Антивирусная проверка файлов больших размеров (более 50 Мб) может занять продолжительное время. В результате, в некоторых случаях данные, проходящие через межсетевой экран Kerio Control, могут быть не доставлены получателям. Это необходимо учитывать при настройке времени ожидания получаемых данных для соответствующих программных продуктов и максимального размера проверяемых файлов для межсетевого экрана Kerio Control.

Подробнее о настройках антивирусного сканирования сетевого трафика и действиях межсетевого экрана над обнаруженными вредоносными объектами можно узнать из руководства администратора межсетевого экрана Kerio Control.

Методы обнаружения угроз

Все антивирусные продукты, разработанные компанией «Доктор Веб», применяют целый набор методов обнаружения угроз, что позволяет проверять подозрительные объекты максимально тщательно.

Сигнатурный анализ

Этот метод обнаружения применяется в первую очередь. Он выполняется путем проверки содержимого анализируемого объекта на предмет наличия в нем сигнатур уже известных угроз. *Сигнатурой* называется непрерывная конечная последовательность байт, необходимая и достаточная для однозначной идентификации угрозы. При этом сравнение содержимого исследуемого объекта с сигнатурами производится не напрямую, а по их контрольным суммам, что позволяет значительно снизить размер записей в вирусных базах, сохранив при этом однозначность соответствия и, следовательно, корректность обнаружения угроз и лечения инфицированных объектов. Записи в вирусных базах продуктов компании «Доктор Веб» составлены таким образом, что благодаря одной и той же записи можно обнаруживать целые классы или семейства угроз.

Origins Tracing

Это уникальная технология компании «Доктор Веб», которая позволяет определить новые или модифицированные угрозы, использующие уже известные и описанные в вирусных базах механизмы заражения или вредоносное поведение. Она выполняется по окончании сигнатурного анализа и обеспечивает защиту пользователей, использующих антивирусные решения компании «Доктор Веб». Кроме того, использование *технологии Origins Tracing* позволяет значительно снизить количество ложных срабатываний эвристического анализатора. К названиям угроз, обнаруженных при помощи Origins Tracing, добавляется постфикс *.Origin*.



Эмуляция исполнения

Метод эмуляции исполнения программного кода используется для обнаружения полиморфных и зашифрованных вирусов, когда использование поиска по контрольным суммам сигнатур неприменимо или значительно усложнено из-за невозможности построения надежных сигнатур. Метод состоит в имитации исполнения анализируемого кода при помощи *эмулятора* – программной модели процессора и среды исполнения программ. Эмулятор оперирует с защищенной областью памяти (буфером эмуляции). При этом инструкции не передаются на центральный процессор для реального исполнения. Если код, обрабатываемый эмулятором, инфицирован, то результатом его эмуляции станет восстановление исходного вредоносного кода, доступного для сигнатурного анализа.

Эвристический анализ

Работа *эвристического анализатора* основывается на наборе эвристик (предположений, статистическая значимость которых подтверждена опытным путем) о характерных признаках вредоносного или, наоборот, безопасного исполняемого кода. Каждый признак кода имеет определенный вес (т. е. число, показывающее важность и достоверность этого признака). Вес может быть как положительным, если признак указывает на наличие вредоносного поведения кода, так и отрицательным, если признак не свойственен компьютерным угрозам. На основании суммарного веса, характеризующего содержимое объекта, эвристический анализатор вычисляет вероятность содержания в нем неизвестного вредоносного объекта. Если эта вероятность превышает некоторое пороговое значение, то выдается заключение о том, что анализируемый объект является вредоносным.

Эвристический анализатор также использует *технология FLY-CODE* – универсальный алгоритм распаковки файлов. Этот механизм позволяет строить эвристические предположения о наличии вредоносных объектов в объектах, сжатых программами упаковки (упаковщиками), причем не только известными разработчиками продуктов компании «Доктор Веб», но и новыми, ранее не исследованными программами. При проверке упакованных объектов также используется технология анализа их структурной энтропии, которая позволяет обнаруживать угрозы по особенностям расположения участков их кода. Эта технология позволяет на основе одной записи вирусной базы произвести обнаружение набора различных угроз, упакованных одинаковым полиморфным упаковщиком.

Поскольку эвристический анализатор является системой проверки гипотез в условиях неопределенности, то он может допускать ошибки как первого (пропуск неизвестных угроз), так и второго рода (признание безопасной программы вредоносной). Поэтому объектам, отмеченным эвристическим анализатором как «вредоносные», присваивается статус «подозрительные».



Во время любой из проверок все компоненты антивирусных продуктов компании «Доктор Веб» используют самую свежую информацию обо всех известных вредоносных программах. Сигнатуры угроз и информация об их признаках и моделях поведения обновляются и добавляются в вирусные базы сразу же, как только специалисты антивирусной лаборатории компании «Доктор Веб» обнаруживают новые угрозы. Даже если новейшая вредоносная программа проникает на компьютер, минуя резидентную защиту Dr.Web для Kerio Control, то она будет обнаружена в списке процессов и нейтрализована после получения [обновленных вирусных баз](#).

Карантин

Инфицированные объекты, обнаруженные при проверке сетевого трафика, могут быть перемещены в *карантин* – специальный каталог `/var/lib/drweb/quarantine`, предназначенный для изоляции и безопасного хранения вредоносных объектов.

По умолчанию опция перемещения инфицированных объектов в карантин выключена, а все инфицированные объекты удаляются. Для ее включения, установите значение `Yes` для [параметра антивирусного приложения](#) **Quarantine enabled**.



В случае, если в карантин помещается файл, имя которого совпадает с именем уже находящегося в карантине файла, то к имени помещаемого файла будет добавлен буквенно-числовой индекс. Например, `file.com` будет переименован в `file.com.drwebq.1524482643`, где `1524482643` – это временная метка (timestamp) создания файла в карантине.

Управление карантином

Просмотр файлов, находящихся в карантине, и работа с ними доступны только суперпользователю (*root*), который может с помощью команды `quarantine` утилиты управления [Dr.Web Ctl](#) удалить файлы из каталога карантина или сохранить их на диске.



Работа с утилитой Dr.Web Ctl

Dr.Web для Kerio Control позволяет осуществлять управление своей работой из командной строки операционной системы. Для этого в состав приложения входит специальная утилита управления Dr.Web Ctl (`drweb-ctl`).

Имеется возможность выполнять из командной строки следующие действия:

- запуск обновления вирусных баз;
- просмотр и изменение параметров конфигурации Dr.Web для Kerio Control;
- просмотр состояния компонентов и статистики обнаруженных угроз;
- просмотр карантина и управление его содержимым.

Для того чтобы команды управления Dr.Web для Kerio Control, вводимые пользователем, имели эффект, должны быть запущены сервисные **компоненты** Dr.Web для Kerio Control (по умолчанию они автоматически запускаются при старте операционной системы).

Утилита Dr.Web Ctl поддерживает стандартное автодополнение команд управления Dr.Web для Kerio Control при условии, что функция автодополнения включена в используемой командной оболочке. В случае если командная оболочка не поддерживает автодополнение, можете настроить ее при необходимости. Для этого обратитесь к справочному руководству используемой операционной системы.



При завершении работы утилита возвращает код выхода в соответствии с соглашением для POSIX-совместимых систем: 0 (нуль) – если операция выполнена успешно, и не нуль – в противном случае.

Обратите внимание, что утилита возвращает ненулевой код выхода, только когда произошла внутренняя ошибка (например, утилита не смогла подключиться к некоторому компоненту, или запрошенная операция не может быть выполнена и т. п.). Если утилита обнаруживает и, возможно, нейтрализует некоторую угрозу, она возвращает код выхода 0, так как запрошенная операция (такая как `scan` и т. п.) выполнена успешно.

Если необходимо установить перечень обнаруженных угроз и примененных к ним действий, то проанализируйте сообщения, которые утилита выводит на консоль.



Формат вызова утилиты

Утилита управления работой Dr.Web для Kerio Control имеет следующий формат вызова:

```
$ drweb-ctl [<общие опции> | <команда> [<аргумент>] [<опции команды>]]
```

Параметры вызова утилиты:

- *<общие опции>* – опции, которые могут быть использованы при запуске без указания команды или для любой из команды. Не являются обязательными для запуска;
- *<команда>* – команда, которая должна быть выполнена Dr.Web для Kerio Control (например, запустить проверку файлов, вывести содержимое карантина и т. п.);
- *<аргументы>* – аргументы команды. Зависят от указанной команды. У некоторых команд аргументы отсутствуют;
- *<опции команды>* – опции, управляющие работой указанной команды. Зависят от команды. У некоторых команд опции отсутствуют.

Доступны следующие общие опции:

Опция	Описание
-h, --help	Вывести на экран краткую общую справку и завершить работу. Для вывода справки по любой команде используйте вызов: <pre>\$ drweb-ctl <команда> -h</pre>
-v, --version	Вывести на экран версию модуля и завершить работу.
-d, --debug	Предписывает выводить на экран расширенные диагностические сообщения во время выполнения указанной команды. Не имеет смысла без указания команды. Используйте вызов: <pre>\$ drweb-ctl <команда> -d</pre>



Для получения справки об утилите используйте команду:

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



Команды drweb-ctl

Команды управления Dr.Web для Kerio Control разделены на следующие группы:

- [команды управления конфигурацией](#),
- [команды управления угрозами и карантином](#),
- [команда управления обновлением](#),
- [информационные команды](#).

Команды управления конфигурацией

Доступны следующие команды управления конфигурацией:

Команда	Описание
<code>cfset</code> <code><секция> . <параметр></code> <code><значение></code>	Назначение: Изменить активное значение указанного параметра текущей конфигурации. Обратите внимание, что знак равенства не используется. Аргументы: • <code><секция></code> – имя секции конфигурационного файла, в которой находится изменяемый параметр. Обязательный аргумент. • <code><параметр></code> – имя изменяемого параметра. Обязательный аргумент. • <code><значение></code> – значение, которое следует присвоить изменяемому параметру. Обязательный аргумент. Для задания значения параметров всегда используется формат: <code><секция> . <параметр> <значение></code>. Опции: <code>-a [--Add]</code> – не заменять текущее значение параметра, а добавить указанное значение в список значений параметра (допустимо только для параметров, которые могут иметь список значений). Также эту опцию следует использовать для добавления новых групп параметров с тегом. <code>-e [--Erase]</code> – не заменять текущее значение параметра, а удалить указанное значение из его списка (допустимо только для параметров, которые имеют список значений). <code>-r [--Reset]</code> – сбросить параметр в значение по умолчанию. В этом случае <code><значение></code> в команде не указывается, а если указано, оно игнорируется. Опции не являются обязательными. Если они не указаны, то текущее значение параметра (в том числе список значений) заменяется на указанное значение.



Команда	Описание
<code>cfshow</code> <code>[<секция> [. <параметр>]]</code>	Назначение: Вывести на экран параметры текущей конфигурации Dr.Web для Kerio Control. Для вывода параметров по умолчанию используется формат: <code><секция>.<параметр> = <значение></code>. Секции и параметры не установленных компонентов по умолчанию не выводятся. Аргументы: • <code><секция></code> – имя секции конфигурационного файла, параметры которой нужно вывести на экран. Необязательный аргумент. Если не указан, то на экран выводятся параметры всех секций конфигурационного файла. • <code><параметр></code> – имя выводимого параметра. Необязательный аргумент. Если не указан, выводятся все параметры указанной секции, в противном случае выводится только этот параметр. Если указан без имени секции, то выводятся все вхождения этого параметра во все секции конфигурационного файла. Опции: <code>--Uncut</code> – вывести на экран все параметры конфигурации, а не только те, которые используются текущим установленным набором компонентов. В противном случае выводятся только те параметры, которые используются имеющимися компонентами. <code>--Changed</code> – вывести только те параметры, значения которых отличаются от значений по умолчанию. <code>--Ini</code> – вывести значения параметров в формате ini-файла (по одному в строке): сначала в отдельной строке выводится имя секции, заключенное в квадратные скобки, после чего параметры, принадлежащие секции, перечисляются в виде пар <code><параметр> = <значение></code>. <code>--Value</code> – вывести только значение указанного параметра. В этом случае аргумент <code><параметр></code> обязателен.
<code>reload</code>	Назначение: Перезапустить сервисные компоненты Dr.Web для Kerio Control. При этом заново открываются журналы, перечитывается файл конфигурации, и производится попытка перезапустить аварийно завершенные компоненты. Аргументы: Нет. Опции: Нет.



Команды управления угрозами и карантином

Доступны следующие команды управления угрозами и карантином:

Команда	Описание
<code>threats</code> [<действие> <объект>]	Назначение: Выполнить указанное действие с обнаруженными ранее угрозами по их идентификаторам. Тип действия определяется указанной опцией команды. Если действие не указано, то вывести на экран информацию об обнаруженных, но не обезвреженных угрозах. Для каждой угрозы выводится следующая информация: • идентификатор, присвоенный угрозе (порядковый номер); • полный путь к инфицированному файлу; • информация об угрозе (имя, тип по классификации компании «Доктор Веб»); • информация о файле: размер, пользователь-владелец, дата последнего изменения; • история действий с инфицированным файлом: обнаружение, применявшиеся действия и т. п. Аргументы: Нет. Опции: <code>--Directory <список каталогов></code> – выводить только те угрозы, которые были обнаружены в файлах из указанного списка каталогов. <code>-f [--Follow]</code> – ожидать новые сообщения об угрозах и выводить их сразу, как только они поступят (нажатие комбинации клавиш CTRL+C прерывает ожидание). <code>--Format "<строка формата>"</code> – выводить информацию об угрозах в <u>указанном формате</u>.  Каждая из перечисленных выше опций будет проигнорирована, если она указана совместно с какой-либо из <i>опций-действий</i>. Опции-действия: <code>--Cure <список угроз></code> – выполнить попытку лечения перечисленных угроз. <code>--Delete <список угроз></code> – выполнить удаление перечисленных угроз. <code>--Ignore <список угроз></code> – игнорировать перечисленные угрозы. <code>--Quarantine <список угроз></code> – выполнить перемещение в карантин перечисленных угроз.



Команда	Описание
	Параметр <i><список угроз></i> содержит идентификаторы угроз, которые перечисляются через запятую. Если требуется применить данную команду ко всем обнаруженным угрозам, вместо <i><список угроз></i> следует указать All. Например, чтобы переместить в карантин все обнаруженные объекты с угрозами, используйте команду: <pre>\$ drweb-ctl threats --Quarantine All</pre>
quarantine [<i><действие></i> <i><объект></i>]	Назначение: Применить действие к указанному объекту, находящемуся в карантине. Если действие не указано, то вывести на экран информацию об объектах, находящихся в карантине, с указанием их идентификаторов и с краткой информацией об исходных файлах, перемещенных в карантин. Информация об изолированных объектах выводится в соответствии с форматом, заданным необязательной опцией <i>--Format</i>. Если опция <i>--Format</i> не указана, то для каждого изолированного объекта выводится следующая информация: • идентификатор, присвоенный изолированному объекту в карантине; • исходный путь к файлу, перемещенному в карантин; • дата перемещения файла в карантин; • информация о файле: размер, пользователь-владелец, дата последнего изменения; • информация об угрозе: имя, тип по классификации компании «Доктор Веб». Аргументы: Нет. Опции: <i>-a</i> [<i>--Autonomous</i>] – запустить отдельную копию сканера для выполнения заданного действия с карантином, завершив ее работу после окончания действия. Эта опция может быть применена совместно с любой из опций, указанных ниже. <i>--Format</i> "<i><строка формата></i>" – выводить информацию об объектах, находящихся в карантине, в <u>указанном формате</u>. <i>-f</i> [<i>--Follow</i>] – ожидать новые сообщения об угрозах и выводить их сразу, как только они поступят (нажатие комбинации клавиш CTRL+C прерывает ожидание).  Если опция <i>--Format</i> или <i>-f</i> [<i>--Follow</i>] указана совместно с любой из опций-действий, то она игнорируется.



Команда	Описание
	--Delete <объект> – удалить указанный объект из карантина.  Обратите внимание, что удаление из карантина – необратимая операция. --Cure <объект> – попытаться вылечить указанный объект в карантине.  Если объект был успешно вылечен, то он все равно останется в карантине. Для извлечения объекта из карантина следует воспользоваться опцией восстановления --Restore. --Restore <объект> – восстановить указанный объект из карантина в исходное место.  Восстановить файл из карантина можно, даже если он инфицирован. --TargetPath <путь> – восстановить объект из карантина в указанный каталог: • с исходным именем, если в параметре <путь> указан только каталог; • с новым именем, если параметр <путь> содержит не только каталог, но и имя, под которым будет восстановлен файл.  Обратите внимание, что опция применяется только совместно с опцией восстановления --Restore. В качестве параметра <объект> используется идентификатор объекта в карантине. Если требуется применить данную команду ко всем объектам, находящимся в карантине, вместо <объект> следует указать All. Например, чтобы восстановить из карантина все имеющиеся в нем объекты, используйте команду: <pre>\$ drweb-ctl quarantine --Restore All</pre>  Если для варианта --Restore All указана дополнительная опция --TargetPath, то она должна задавать путь к каталогу, а не к файлу.



Форматированный вывод данных для команд `threats` и `quarantine`

Формат вывода задается строкой формата, указанной в качестве аргумента необязательной опции `--Format`. Строка формата обязательно указывается в кавычках. Строка формата может включать в себя как обычные символы, которые будут выведены на экран «как есть», так и специализированные маркеры, которые при выводе будут заменены на соответствующую информацию.

Доступны следующие маркеры:

- общие для команд `threats` и `quarantine`:

Маркер	Описание
<code>%{n}</code>	Перевод строки
<code>%{t}</code>	Табуляция
<code>%{threat_name}</code>	Имя обнаруженной угрозы (вируса) по классификации компании «Доктор Веб»
<code>%{threat_type}</code>	Тип угрозы («known virus» и т. д.) по классификации компании «Доктор Веб»
<code>%{size}</code>	Размер исходного файла
<code>%{origin}</code>	Полное имя исходного файла с путем к его расположению
<code>%{path}</code>	Синоним для <code>%{origin}</code>
<code>%{ctime}</code>	Дата/время модификации исходного файла в формате: <code>%Y-%b-%d %H:%M:%S</code> (например, 2018-Jul-20 15:58:01)
<code>%{timestamp}</code>	То же, что и <code>%{ctime}</code> , но в формате времени UNIX timestamp
<code>%{owner}</code>	Пользователь-владелец исходного файла
<code>%{rowner}</code>	Удаленный пользователь-владелец исходного файла. Если маркер не применим или значение неизвестно, то он заменяется на «?».

- специфические для команды `threats`:

Маркер	Описание
<code>%{hid}</code>	Идентификатор записи об угрозе в реестре истории событий, связанных с угрозой
<code>%{tid}</code>	Идентификатор угрозы
<code>%{htime}</code>	Дата/время события, связанного с угрозой



Маркер	Описание
%{app}	Идентификатор компонента, обработавшего угрозу
%{event}	Последнее событие, связанное с угрозой: • FOUND – угроза была обнаружена; • Cure – угроза была вылечена; • Quarantine – файл с угрозой был перемещен в карантин; • Delete – файл с угрозой был удален; • Ignore – угроза была проигнорирована; • RECAPTURED – угроза была обнаружена повторно другим компонентом.
%{err}	Текст сообщения об ошибке. Если ошибки нет, маркер заменяется на пустую строку.

- специфические для команды quarantine:

Маркер	Описание
%{qid}	Идентификатор объекта в карантине
%{qtime}	Дата/время перемещения объекта в карантин
%{curetime}	Дата/время попытки лечения объекта, перемещенного в карантин. Если маркер не применим или значение неизвестно, то он заменяется на «?».
%{cures}	Результат попытки лечения объекта, перемещенного в карантин: • cured – угроза вылечена; • not cured – угроза не вылечена, либо попыток лечения не было.

Команда управления обновлением

Для управления обновлением доступна одна команда:

Команда	Описание
update	Назначение: Инициировать процесс обновления вирусных баз и антивирусного ядра с серверов обновлений компании «Доктор Веб» с помощью компонента Dr.Web Updater или прервать уже запущенный процесс обновления. Аргументы: Нет. Опции: --Stop – прервать уже идущий процесс обновления.



Информационные команды

Доступны следующие информационные команды:

Команда	Описание
appinfo	Назначение: Вывести на экран информацию о работающих модулях Dr.Web для Kerio Control. Для каждого модуля выводится следующая информация: • внутреннее имя; • идентификатор процесса GNU/Linux (PID); • состояние (запущен, остановлен и т. п.); • код ошибки, если работа компонента завершена вследствие ошибки; • дополнительная информация (опционально). Для демона управления конфигурацией (drweb-configd) в качестве дополнительной информации выводятся: • перечень установленных компонентов (Installed); • перечень компонентов, запуск которых должен быть обеспечен демоном (Should run). Аргументы: Нет. Опции: <code>-f [--Follow]</code> – ожидать новые сообщения об изменении состояния модулей и выводить их на экран сразу, как только они поступят (нажатие комбинации клавиш CTRL+C прерывает ожидание).
baseinfo	Назначение: Вывести на экран информацию о текущей версии антивирусного ядра и состоянии вирусных баз. Выводится следующая информация: • версия антивирусного ядра, • дата и время выпуска используемых вирусных баз, • число доступных вирусных записей, • момент последнего успешного обновления вирусных баз и антивирусного ядра, • момент следующего запланированного автоматического обновления. Аргументы: Нет. Опции: <code>-l [--List]</code> – вывести полный список загруженных файлов вирусных баз и число вирусных записей в каждом файле.



Команда	Описание
license	Назначение: Вывести на экран информацию об активной лицензии, получить демонстрационную лицензию или ключевой файл для уже зарегистрированной лицензии (например, на сайте компании «Доктор Веб»). Если не указана ни одна опция, то при использовании лицензии для автономного режима работы выводится следующая информация: • номер лицензии, • дата и время окончания действия лицензии. Если используется лицензия, выданная сервером централизованной защиты (для работы в режиме централизованной защиты или в мобильном режиме), то выводится соответствующая информация. Аргументы: Нет. Опции: --GetDemo – запросить демонстрационный ключевой файл сроком на месяц и получить его, в случае если не нарушены условия получения демонстрационного периода. --GetRegistered <серийный номер> – получить лицензионный ключевой файл для указанного серийного номера, если не нарушены условия получения нового ключевого файла (например, программа не находится в режиме централизованной защиты, когда лицензией управляет сервер централизованной защиты).  Если серийный номер не является серийным номером демонстрационного периода, то он должен быть предварительно зарегистрирован на сайте компании «Доктор Веб». Для регистрации серийного номера и для запроса демонстрационного периода требуется подключение к сети Интернет. Подробнее о лицензировании продуктов компании «Доктор Веб» см. в разделе Лицензирование.



Обновление вирусных баз

Для обнаружения вредоносных объектов антивирусные продукты компании «Доктор Веб» используют специальные вирусные базы, в которых содержится информация обо всех известных вредоносных программах. В приложении Dr.Web для Kerio Control реализован сервис обновлений вирусных баз через сеть Интернет с серверов обновлений компании «Доктор Веб». В течение срока действия лицензии происходит регулярная загрузка информации о новых вирусах и вредоносных программах, а при наличии обновлений компонентов приложения обеспечивается их установка.

Для автоматизации получения и установки обновлений вирусных баз используется модуль обновления Dr.Web Updater. Данный модуль входит в состав Dr.Web для Kerio Control и содержится в пакете `drweb-update`.

При старте операционной системы демон управления конфигурацией (`drweb-configd`) автоматически запускает модуль обновления. Dr.Web Updater проверяет наличие обновлений каждые 30 минут, а при их обнаружении загружает и устанавливает обновления.



Регистрация событий

Dr.Web для Kerio Control регистрирует ошибки и происходящие события в журналах регистрации межсетевого экрана Kerio Control: журнале отладки ([debug](#)), журнале ошибок (error) и журнале безопасности (security).

Журнал отладки

В журнал отладки межсетевого экрана Kerio Control (debug) заносится информация, используемая при поиске и анализе ошибок в работе Dr.Web для Kerio Control.

Включение регистрации событий приложения в журнале debug

1. Запустите консоль администрирования межсетевого экрана.
2. В разделе **Журналы** выберите журнал **debug**.
3. Нажмите правую кнопку мыши в любой точке окна журнала **debug** и выберите пункт **Сообщения**.
4. Выберите пункт **Antivirus** в окне **Протоколирование сообщений** и нажмите кнопку **ОК**.



Техническая поддержка

При возникновении проблем с установкой или работой продуктов компании, прежде чем обращаться за помощью в службу технической поддержки, попробуйте найти решение следующими способами:

- ознакомьтесь с последними версиями описаний и руководств по адресу <https://download.drweb.com/doc/>;
- прочитайте раздел часто задаваемых вопросов по адресу https://support.drweb.com/show_faq/;
- посетите форумы компании «Доктор Веб» по адресу <https://forum.drweb.com/>.

Если после этого не удалось решить проблему, вы можете воспользоваться одним из следующих способов, чтобы связаться со службой технической поддержки компании «Доктор Веб»:

- заполните веб-форму в соответствующей секции раздела <https://support.drweb.com/>;
- позвоните по телефону в Москве: +7 (495) 789-45-86 или по бесплатной линии для всей России: 8-800-333-7932.

Информацию о региональных представительствах и офисах компании «Доктор Веб» вы можете найти на официальном сайте по адресу <https://company.drweb.com/contacts/offices/>.

